



# Rehost a volume from one SVM to another SVM

ONTAP 9

NetApp  
August 11, 2023

# Table of Contents

- Rehost a volume from one SVM to another SVM ..... 1
  - Rehost a volume from one SVM to another SVM overview ..... 1
  - Rehost SMB volumes ..... 1
  - Rehost NFS volumes ..... 3
  - Rehost SAN volumes ..... 4
  - Rehost volumes in a SnapMirror relationship ..... 6
  - Features that do not support volume rehost ..... 7

# Rehost a volume from one SVM to another SVM

## Rehost a volume from one SVM to another SVM overview

Volume rehost enables you to reassign NAS or SAN volumes from one storage virtual machine (SVM, formerly known as Vserver) to another SVM without requiring a SnapMirror copy. The volume rehost procedures depend upon the protocol type and the volume type. Volume rehost is a disruptive operation for data access and volume management.

### Before you begin

Several conditions must be met before you can rehost a volume from one SVM to another:

- The volume must be online.
- Protocols: SAN or NAS

For the NAS protocol, the volume must be unmounted.

- If the volume is in a SnapMirror relationship, then the relationship must be either deleted or broken prior to volume rehost.

You can resynchronize the SnapMirror relationship after the volume rehost operation.

## Rehost SMB volumes

You can rehost volumes that serve data over SMB protocol. After rehosting the CIFS volume, to continue accessing data over SMB protocol, you must manually configure policies and the associated rules.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- If the source SVM and destination SVM Active Directory domains differ, you might lose access to the objects on the volume.
- Beginning in ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

- When the source SVM has local users and groups, the permissions for the files and directories (ACLs) that are set are no longer effective after volume rehost operation.

The same is true for audit ACLs (SACLs)

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the

source volume, and must be manually reconfigured on the rehosted volume:

- Volume and qtree export policies
- Antivirus policies
- Volume efficiency policy
- Quality of service (QoS) policies
- Snapshot policies
- Quota rules
- ns-switch and name services configuration export policy and rules
- User and group IDs

### Before you begin

- Volume must be online.
- Volume management operations, such as volume move or LUN move, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The source SVM and destination SVM must have the same Active Directory and realmDNS domain.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.



If local users and groups are configured, and if there are files and directories on that volume with permissions set for those users or groups, these permissions are no longer effective.

### Steps

1. Record information about the CIFS shares to avoid losing information on CIFS shares in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

```
volume unmount
```

3. Switch to the advanced privilege level:

```
set -privilege advanced
```

4. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

5. Mount the volume under the appropriate junction path in the destination SVM:

```
volume mount
```

6. Create CIFS shares for the rehosted volume:

```
vserver cifs share create
```

7. If the DNS domains differ between the source SVM and destination SVM, create new users and groups.
8. Update the CIFS client with the new destination SVM LIFs and junction path to the rehosted volume.

### After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume.

### [SMB configuration](#)

### [SMB and NFS multiprotocol configuration](#)

## Rehost NFS volumes

You can rehost volumes that serve data over NFS protocol. After rehosting the NFS volumes, to continue accessing data over NFS protocol, you must associate the volume with the export policy of the hosting SVM and manually configure policies and associated rules.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- Beginning in ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume, and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

### Before you begin

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.

- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

### Steps

1. Record information about the NFS export policies to avoid losing information on NFS policies in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

```
volume unmount
```

3. Switch to the advanced privilege level:

```
set -privilege advanced
```

4. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver  
destination_svm
```

The default export policy of the destination SVM is applied to the rehosted volume.

5. Create the export policy:

```
vserver export-policy create
```

6. Update the export policy of the rehosted volume to a user-defined export policy:

```
volume modify
```

7. Mount the volume under the appropriate junction path in the destination SVM:

```
volume mount
```

8. Verify that the NFS service is running on the destination SVM.
9. Resume NFS access to the rehosted volume.
10. Update the NFS client credentials and LIF configurations to reflect the destination SVM LIFs.

This is because the volume access path (LIFs and junction path) has undergone changes.

### After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume.

### [NFS configuration](#)

## Rehost SAN volumes

You can rehost volumes that have mapped LUNs. After re-creating the initiator group (igroup) in the destination SVM, volume rehost can automatically remap the volume on the same SVM.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- Beginning in ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

### Before you begin

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- There must be no active I/O on the volumes or LUNs.
- You must have verified that the destination SVM does not have igroup of the same name but different initiators.

If the igroup has the same name, then you must have renamed the igroup in either one of the SVMs (source or destination).

- You must have enabled the `force-unmap-luns` option.
  - The default value of the `force-unmap-luns` option is `false`.
  - No warning or confirmation message is displayed when you set the `force-unmap-luns` option to `true`.

### Steps

1. Record LUN mapping information on target volume:

```
lun mapping show volume volume vserver source_svm
```

This is a precautionary step to avoid losing information about LUN mapping in case the volume rehost fails.

2. Delete igroups associated with the target volume.
3. Rehost the target volume to the destination SVM:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

4. Map LUNs on the target volume to appropriate igroups.
  - Volume rehost preserves LUNs on the target volume; however, LUNs remain unmapped.
  - Use the destination SVM port set while mapping LUNs.
  - If the `auto-remap-luns` option is set to `true`, the LUNs are mapped automatically after rehost.

## Rehost volumes in a SnapMirror relationship

You can rehost volumes in a SnapMirror relationship.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

### Before you begin

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

### Steps

1. Record the SnapMirror relationship type:

```
snapmirror show
```

This is a precautionary step to avoid losing information about the SnapMirror relationship type in case the volume rehost fails.

2. From the destination cluster, delete the SnapMirror relationship:

```
snapmirror delete
```



You must not break the SnapMirror relationship; otherwise, the data protection capability of the destination volume is lost and the relationship cannot be reestablished after the rehosting operation.

3. From the source cluster, remove the SnapMirror relationship information:

```
snapmirror release relationship-info-only true
```

Setting the `relationship-info-only` parameter to `true` removes the source relationship information without deleting the Snapshot copies.

4. Switch to the advanced privilege level:

```
set -privilege advanced
```

5. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

6. If the SVM peering relation is not present, create the SVM peer relationship between the source SVM and destination SVM:

```
vserver peer create
```

7. Create the SnapMirror relationship between the source volume and destination volume:

```
snapmirror create
```

You must run the `snapmirror create` command from the SVM that is hosting the DP volume. The rehosted volume can be the source or destination of the SnapMirror relationship.

8. Resynchronize the SnapMirror relationship.

## Features that do not support volume rehost

There are certain features that do not support volume rehost.

The following features do not support volume rehost:

- SVM DR
- MetroCluster configurations
- SnapLock volumes
- NetApp Volume Encryption (NVE) volumes (in versions of ONTAP before 9.8)

In ONTAP releases prior to 9.8, you must unencrypt the volume before rehosting it. Volume encryption keys depend on SVM keys. If a volume is moved to another SVM and if multitenant key configuration is enabled on either the source or destination SVM, the volume and the SVM keys will not match.

Beginning in ONTAP 9.8, you can rehost a volume with NVE.

- FlexGroup volumes
- Clone volumes

## Copyright information

Copyright © 2023 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.