# Provision NAS storage

## ONTAP System Manager

NetApp
April 25, 2020

# Table of Contents

# Provision NAS storage

## NAS overview

ONTAP enables you to serve data to Linux and Windows clients simply, securely, and efficiently.

ONTAP System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using ONTAP System Manager, you can manage NAS services at the component level:

- Protocols – NFS, SMB/CIFS, or both (NAS multiprotocol)
- Name services – DNS, LDAP, and NIS
- Name service switch
- Kerberos security
- Exports and shares
- Qtrees
- Name mapping of users and groups

If you need to learn more about ONTAP NAS features, you can review the *Concepts* guide and *Provisioning for NAS protocols* section in the ONTAP 9 Documentation Center.

## Provision NAS storage for VMware datastores

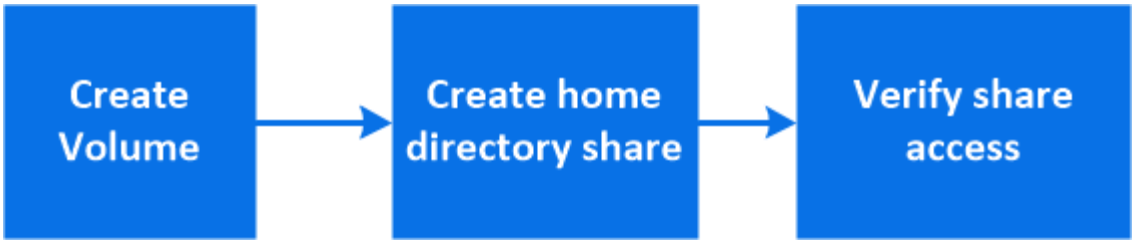
Create volumes to provide VMware datastores using the NFS protocol.

See the NFS Configuration for ESXi using VSC Express Guide for VMware datastore provisioning best practices.

## Provision NAS storage for home directories

Create volumes to provide storage for home directories using the SMB/CIFS protocol.

This procedure creates new volumes for home directories on an existing SMB-enabled storage VM.




*Steps*

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
2. Create a home directory share: click **Storage** > **Shares**, click **Add**, and select **Home Directory**.
3. Switch to a Windows client to verify that the share is accessible.
    a. In Windows Explorer, map a drive to the share in the following format: `\\_SMB_Server_Name__Share_Name_`
    If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.
    b. On the newly created drive, create a test file, and then delete the file.

# Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol.

This procedure creates new volumes on an existing NFS-enabled storage VM.

*Steps*

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
    a. The default export policy grants full access to all users. You can add more restrictive rules to the export policy later.
2. Switch to a Linux system to verify access.
    a. Create and mount the volume using the network interface of the storage VM.
    b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

After verifying access, you might want to restrict client access with the volume's export policy and set any desired UNIX ownership and permissions on the mounted volume.

# Manage access using export policies

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an existing NFS-enabled storage VM.

*Steps*

1. Create or modify an export policy for a volume: click **Storage** > **Volumes**, click an NFS-enabled volume, click **More**, and then click **Edit Export Policy**.
2. Click **Select an existing policy** or **Add a new policy**.

# Provision NAS storage for Windows servers using SMB/CIFS

Create volumes to provide storage for Windows servers using the SMB/CIFS protocol.

This procedure creates new volumes on an existing SMB-enabled storage VM.

*Steps*

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.

   The default share grants full access to all users. You can modify the Access Control List (ACL) later.

2. Switch to a Windows client to verify that the share is accessible.
   a. In Windows Explorer, map a drive to the share in the following format: `\\_SMB_Server_Name__Share_Name_`
   b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you might want to restrict client access with the share ACL and set any desired security properties on the mapped drive.

# Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Create volumes to provide storage for clients using either the NFS or SMB/CIFS protocol.

This procedure creates new volumes on an existing storage VM enabled for both NFS and SMB protocols.


*Steps*

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
   a. Create an export policy: click **More Options** and check **Share via NFS**.

The default setting grants full access to all users. You can add more restrictive rules to the export policy later.

b. Create a share: check **Share via SMB/CIFS**.
The share is created with a default Access Control List (ACL) set to "Full Control" for the Everyone group. You can add restrictions to the ACL later.

2. Switch to a Linux client to verify that the export is accessible.
   a. Create and mount the volume using the network interface of the storage VM.
   b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
3. Switch to a Windows client to verify that the share is accessible.
   a. In Windows Explorer, map a drive to the share in the following format: `\\_SMB_Server_Name__Share_Name_`
   b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you might want to restrict client access with the volume's export policy, restrict client access with the share ACL, and set any desired ownership and permissions on the exported and shared volume.

# Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for NFS or SMB. It is assumed that you have already configured DNS, NTP, and LDAP on the storage system.


*Steps*

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
   a. Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

      The root volume of the storage VM must have the following configuration:

| Name... | Setting... |
|---|---|
| UID | root or ID 0 |
| GID | root or ID 0 |
| UNIX permissions | 755 |

   b. If these values are not shown, use the `volume modify` command to update them.

2. Set user permissions for the storage VM root volume.
   a. Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

      The storage VM should have the following UNIX users configured:

      | User name | User ID | Primary group ID |
      |---|---|---|
      | nfs | 500 | 0 |
      | root | 0 | 0 |

      **Note:** The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

   b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.
3. Set group permissions for the storage VM root volume.
   a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

      The storage VM should have the following UNIX groups configured:

      | Group name | Group ID |
      |---|---|
      | daemon | 1 |
      | root | 0 |

   b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.
4. Switch to System Manager and configure Kerberos: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, click → under Kerberos, click **Add** under Kerberos Realm, and complete the following sections:
   a. Add Kerberos Realm: enter configuration details depending on KDC vendor.
   b. Add Network Interface to Realm: click **Add** and select a network interface.
5. If desired, add mappings from Kerberos principal names to local user names.
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click → under **Name Mapping**.
   b. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

# Provide client access with name services

Enable ONTAP to look up host, user, group, or netgroup information using LDAP or

NIS to authenticate NAS clients.

This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for NFS or SMB. For LDAP configurations, it is assumed that the LDAP configuration details required in your environment are available and that you are using a default ONTAP LDAP schema.

*Steps*

1. Configure the required service: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ for LDAP or NIS.
2. Include any changes in the name services switch: click ✎ under Name Services Switch.

# Provision NAS storage for large file systems using FlexGroup volumes

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.

*Steps*

1. Click **Storage** > **Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.

# Improve performance for multiple clients with FlexCache

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes are ideal for read-intensive workloads, especially where clients need to access the same data repeatedly.

The FlexCache volume can be on the same cluster as or on a different cluster than that of the remote volume. If the remote volume is on a different cluster, you need to have already peered the clusters and storage VMs.

*Steps*

1. Click **Storage** > **Volumes**.
2. Click **Add**.

3. Click **More Options** and then select **Add as cache for a remote volume**.

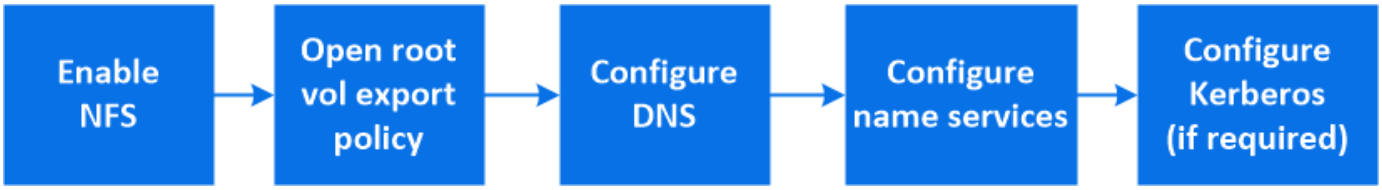
For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

# Enable NAS storage

## Enable NAS storage for Linux servers using NFS

Modify storage VMs to enable NFS servers for serving data to Linux clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



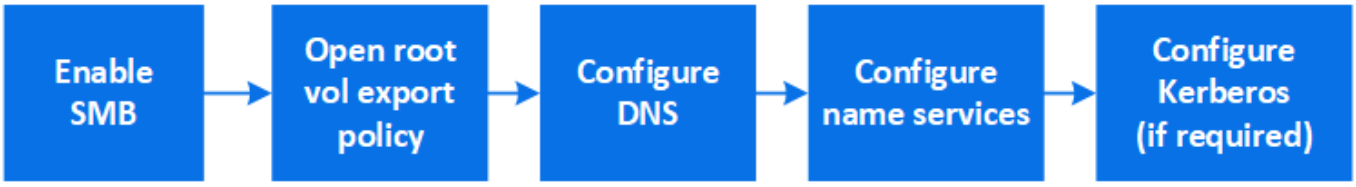

*Steps*

1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **NFS**.
2. Open the export policy of the storage VM root volume:
   a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name* _root), and then click on the policy that is displayed under **Export Policy**.
   b. Click **Add** to add a rule.
      - Client specification = `0.0.0.0/0`
      - Access protocols = NFS
      - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ under **DNS**.
4. Configure name services as required.
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click for ⚙ LDAP or NIS.
   b. Include any changes in the name services switch file: click ✎ in the Name Services Switch tile.
5. Configure Kerberos if required:
   a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
   b. Click → in the Kerberos tile and then click **Add**.

## Enable NAS storage for Windows servers using SMB/CIFS

Modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



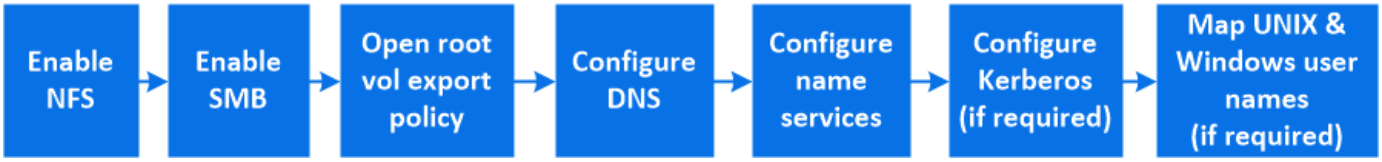

*Steps*

1. Enable SMB/CIFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **SMB/CIFS**.
2. Open the export policy of the storage VM root volume:
   a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.
   b. Click **Add** to add a rule.
      - Client specification = `0.0.0.0/0`
      - Access protocols = SMB/CIFS
      - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ under **DNS**.
   b. Switch to the DNS server and map the SMB server.
      - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
      - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ under **LDAP** or **NIS**.
   b. Include any changes in the name services switch file: click ✎ under **Name Services Switch**.
5. Configure Kerberos if required:
   a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
   b. Click → under **Kerberos** and then click **Add**.

## Enable NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.




*Steps*

1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **NFS**.
2. Enable SMB/CIFS on an existing VM: click ⚙ under *SMB/CIFS".
3. Open the export policy of the storage VM root volume:
   a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.
   b. Click **Add** to add a rule.
      - Client specification = `0.0.0.0/0`
      - Access protocols = NFS
      - Access details = NFS Read-Only
4. Configure DNS for host-name resolution:
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ under **DNS**.
   b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
      - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
      - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
5. Configure name services as required:
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ for LDAP or NIS.
   b. Include any changes in the name services switch file: click ✎ under **Name Services Switch**.
6. Configure Kerberos if required: click → in the Kerberos tile and then click **Add**.
7. Map UNIX and Windows user names if required: click → under **Name Mapping** and then click

**Add**.

You should use this procedure only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. This procedure can be done using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.