NAS storage management

ONTAP 9

NetApp
December 18, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/concept_nas_provision_overview.html on December 18, 2022. Always check docs.netapp.com for the latest.

Table of Contents

NAS storage management . . . 1
- Manage NAS protocols with System Manager . . . 1
- Configure NFS with the CLI . . . 19
- Manage NFS with the CLI . . . 87
- Manage NFS over RDMA . . . 197
- Configure SMB with the CLI . . . 202
- Manage SMB with the CLI . . . 242
- Provide S3 client access to NAS data . . . 583
- SMB configuration for Microsoft Hyper-V and SQL Server . . . 593

NAS storage management

Manage NAS protocols with System Manager

NAS management overview with System Manager

The topics in this section show you how to configure and manage NAS environments with System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see these topics:

- NFS configuration overview
- SMB configuration overview

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

- Protocols – NFS, SMB, 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

Provision NFS storage for VMware datastores

Before using Virtual Storage Console for VMware vSphere (VSC) to provision NFS volumes on an ONTAP based storage system for ESXi hosts, enable NFS using System Manager for ONTAP 9.7 or later.

After creating an NFS-enabled storage VM in System Manager, you then provision NFS volumes and manage datastores using VSC.

Beginning with VSC 7.0, VSC is part of the ONTAP Tools for VMware vSphere virtual appliance, which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Be sure to check the NetApp Interoperability Matrix to confirm compatibility between your current ONTAP and VSC releases.

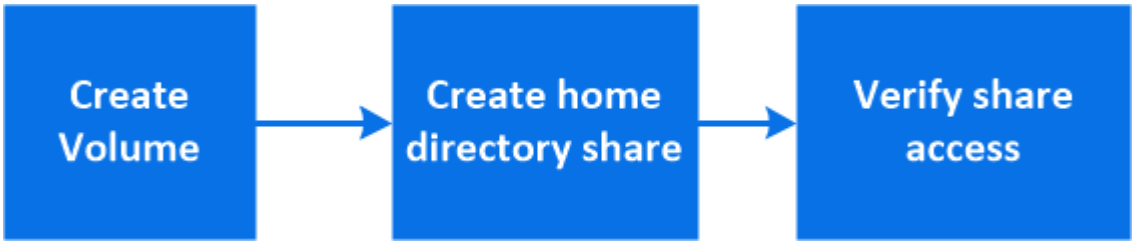
To set up NFS access for ESXi hosts to datastores using System Manager Classic (for ONTAP 9.7 and earlier releases), see NFS configuration for ESXi using VSC overview

For more information, see TR-4597: VMware vSphere for ONTAP and the documentation for your VSC release.

Provision NAS storage for home directories

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

This procedure creates new volumes for home directories on an existing SMB-enabled storage VM. You can accept systems defaults when configuring volumes or specify custom configurations.



You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Steps

1. Add a new volume in an SMB-enabled storage VM.
   a. Click **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

      Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

      - If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.
      - You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.
2. Click **Storage > Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following 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.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete provisioning for home directories.

Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol with ONTAP System Manager (9.7 and later).

This procedure creates new volumes on an existing NFS-enabled storage VM. You can accept system defaults when configuring volumes or specify custom configurations.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

If you want details about the range of ONTAP NFS protocol capabilities, consult the NFS reference overview.

Steps

1. Add a new volume in an NFS-enabled storage VM.
   a. Click **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

Only storage VMs configured with the NFS protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

- If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

  The default export policy grants full access to all users.

- You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.

2. On a Linux client, do the following 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 can restrict client access with the volume's export policy and set any desired UNIX ownership and permissions on the mounted volume.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete provisioning for Linux servers using NFS.

Other ways to do this in ONTAP

To perform this task with…	Refer to…
System Manager Classic (ONTAP 9.7 and earlier)	NFS configuration overview
The ONTAP command line interface (CLI)	NFS configuration overview with the CLI

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. In System Manager, Click **Storage** > **Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

Provision NAS storage for Windows servers using SMB

Create volumes to provide storage for Windows servers using the SMB protocol using System Manager, which is available with ONTAP 9.7 and later.

This procedure creates new volumes on an existing SMB-enabled storage VM and creates a share for the volume root (/) directory. You can accept systems defaults when configuring volumes or specify custom configurations. After initial SMB configuration, you can also create additional shares and modify their properties.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

If you want details about the range of ONTAP SMB protocol capabilities, consult the SMB reference overview.

Steps

1. Add a new volume in an SMB-enabled storage VM.
   a. Click **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

      Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

      - If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

        - You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.

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 can restrict client access with the share ACL and set any desired security properties on the mapped drive. See Create an SMB share for more information.

Add or modify shares

You can add additional shares after initial SMB configuration. Shares are created with default values and properties you select. These can be modified later.

You can set the following share properties when configuring a share:

- Access permissions
- Share properties
    - Enable continuous availability to shares that contain Hyper-V and SQL Server over SMB data (beginning with ONTAP 9.10.1). See also:
        - Continuously available share requirements for Hyper-V over SMB
        - Continuously available share requirements for SQL Server over SMB
    - Encrypt data with SMB 3.0 while accessing this share.

After initial configuration, you can also modify these properties:

- Symbolic links
    - Enable or disable symlinks and widelinks
- Share properties
    - Allow clients to access Snapshot copies directory.
    - Enable oplocks, allowing clients to lock files and cache content locally (default).
    - Enable access-based enumeration (ABE) to display shared resources based on the access permissions of the user.

Procedures

To add a new share in an SMB-enabled volume, click **Storage > Shares**, click **Add**, and select **Share**.

To modify an existing share, click **Storage > Shares**, then click the ⋮ and select **Edit**.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8 you can specify a Custom QoS policy or disable QoS, in addition to the default value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

  This option is not available if you previously selected *Manual placement under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.
  Access permission for the protocols for which the volume is configured.
  ***Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.**
  ***Click *Save** to create the volume and add it to the cluster and storage VM.

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.

- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete provisioning for Windows servers using SMB.

Other ways to do this in ONTAP

To perform this task with…	Refer to…
System Manager Classic (ONTAP 9.7 and earlier)	SMB configuration overview
The ONTAP command line interface	SMB configuration overview with the CLI

Provision NAS storage for both Windows and Linux using both NFS and SMB

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

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

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Steps

1. Add a new volume in a storage VM enabled for both NFS and SMB.

   a. Click **Storage > Volumes** and then click **Add**.

   b. Enter a name, select the storage VM, and enter a size. Only storage VMs configured with both the NFS and SMB protocols are listed. If only one storage VM configured with the NFS and SMB protocols is available, the **Storage VM** field is not shown.

   c. Click **More Options** and select **Share via NFS**.

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

   d. Select **Share via SMB**.

      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.

   e. If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

   Alternatively, you can continue to enable any additional required services such as authorization, quality of

service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.

2. On a Linux client, 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. On a Windows client, do the following 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 can 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.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete multiprotocol provisioning for Windows and Linux servers.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (ONTAP 9.7 and earlier)	SMB and NFS multiprotocol configuration overview
The ONTAP command line interface	SMB configuration overview with the CLI NFS configuration overview with the CLI What the security styles and their effects are Case-sensitivity of file and directory names in a multiprotocol environment

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.

Before beginning you should have 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 to configure Kerberos
5. In System Manager, click **Storage > Storage VMs** and select the storage VM.
6. Click **Settings**.
7. Click → under Kerberos.
8. Click **Add** under Kerberos Realm, and complete the following sections:
   - Add Kerberos Realm

     Enter configuration details depending on KDC vendor.

   - Add Network Interface to Realm

     Click **Add** and select a network interface.

9. If desired, add mappings from Kerberos principal names to local user names.

a. Click **Storage > Storage VMs** and select the storage VM.

b. Click **Settings**, and then click → under **Name Mapping**.

c. 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, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

Steps

1. Configure the required service: click **Storage > Storage VMs**.

2. Select the storage VM, click **Settings**, and then click ⚙ for LDAP or NIS.
3. Include any changes in the name services switch: click ✎ under Name Services Switch.

Manage directories and files

Expand the System Manager volume display to view and delete directories and files.

Beginning with ONTAP 9.9.1, directories are deleted with low-latency fast directory delete functionality.

For more information about viewing file systems in ONTAP 9.9.1 and later, see File System Analytics overview.

Step

1. 1. Click **Storage > Volumes**. Then expand a volume to view its contents.

Manage host-specific users and groups with System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage users and groups that are specific to a UNIX or Windows host.

You can perform the following procedures:

Windows	UNIX
• View Windows users and groups • Add, edit, or delete a Windows group • Manage Windows Users	• View UNIX users and groups • Add, edit, or delete a UNIX group • Manage UNIX Users

View Windows users and groups

In System Manager, you can view a list of Windows users and groups.

Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

   The **Windows** section displays a summary of the number of users in each group associated with the selected storage VM.

4. Click → in the **Windows** section.
5. Click the **Groups** tab, then click ⌄ next to a group name to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.

Add, edit, or delete a Windows group

In System Manager, you can manage Windows groups by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of Windows groups. Refer to View Windows users and groups.
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action…	Perform these steps…
Add a group	1. Click + Add . 2. Enter the group information. 3. Specify privileges. 4. Specify group members (add local users, domain users, or domain groups).
Edit a group	1. Next to the group name, click ⋮, then click **Edit**. 2. Modify the group information.
Delete a group	1. Check the box next to the group or groups you want to delete. 2. Click Delete . **Note:** You can also delete a single group by clicking ⋮ next to the group name, then clicking **Delete**.

Manage Windows Users

In System Manager, you can manage Windows users by adding, editing, deleting, enabling, or disabling them. You can also change the password of a Windows user.

Steps

1. In System Manager, view the list of users for the group. Refer to View Windows users and groups.
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action…	Perform these steps…
Add a user	1. Click + Add . 2. Enter the user information.
Edit a user	1. Next to the user name, click ⋮, then click **Edit**. 2. Modify the user information.

Delete a user	1. Check the box next to the user or users you want to delete. 2. Click Delete . **Note:** You can also delete a single user by clicking ⋮ next to the user name, then clicking **Delete**.
Change user password	1. Next to the user name, click ⋮, then click **Change Password**. 2. Enter the new password and confirm it.
Enable a user	1. Check the box next to each disabled user you want to enable. 2. Click Enable .
Disable a users	1. Check the box next to each enabled user you want to disable. 2. Click Disable .

View UNIX users and groups

In System Manager, you can view a list of UNIX users and groups.

Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

   The **UNIX** section displays a summary of the number of users in each group associated with the selected storage VM.
4. Click → in the **UNIX** section.
5. Click the **Groups** tab to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.

Add, edit, or delete a UNIX group

In System Manager, you can manage UNIX groups by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of UNIX groups. Refer to View UNIX users and groups.
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action…	Perform these steps…

Add a group	1. Click + Add . 2. Enter the group information. 3. (Optional) Specify associated users.
Edit a group	1. Select the group. 2. Click Edit . 3. Modify the group information. 4. (Optional) Add or remove users.
Delete a group	1. Select the group or groups you want to delete. 2. Click Delete .

Manage UNIX Users

In System Manager, you can manage Windows users by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of users for the group. Refer to View UNIX users and groups.
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action…	Perform these steps…
Add a user	1. Click + Add . 2. Enter the user information.
Edit a user	1. Select the user you want to edit. 2. Click Edit . 3. Modify the user information.
Delete a user	1. Select the user or users you want to delete. 2. Click Delete .

Monitor NFS active clients

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:
* Time of last access
* Network interface IP address
* NFS connection version

* Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and a count of NFS clients is includes in the **Dashboard** display.

Step

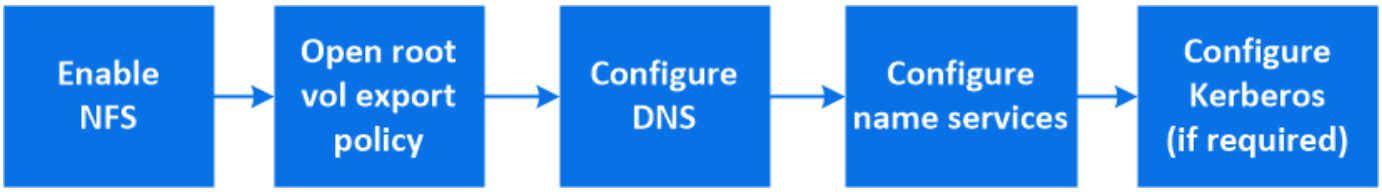
1. Display NFS client activity: Click **Hosts > NFS Clients**.

Enable NAS storage

Enable NAS storage for Linux servers using NFS

Create or modify storage VMs to enable NFS servers for serving data to Linux clients.

This procedure enables a new or existing storage VM for the NFS protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



Steps

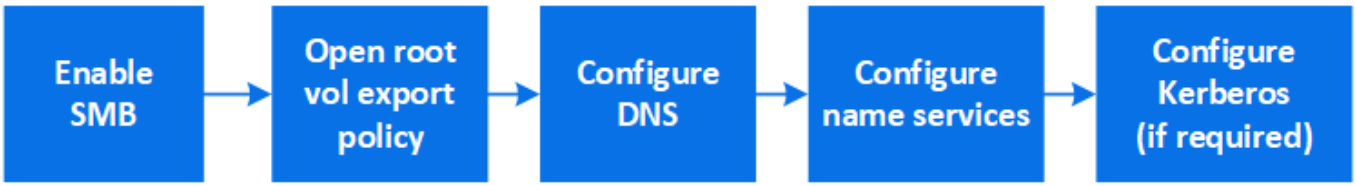
1. Enable NFS on a storage VM.
   a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable NFS**.
      - Confirm the default language.
      - Add network interfaces.
      - Update storage VM administrator account information (optional).
   b. For existing storage VMs: 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

Create or modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables a new or existing storage VM for the SMB protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



Steps

1. Enable SMB on a storage VM.
   a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS**.
      - Enter the following information:
        - Administrator name and password
        - Server name
        - Active directory domain
      - Confirm the Organizational Unit.
      - Confirm the DNS values.
      - Confirm the default language.
      - Add network interfaces.
      - Update storage VM administrator account information (optional).
   b. For existing storage VMs:: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **SMB**.
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
      - 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.

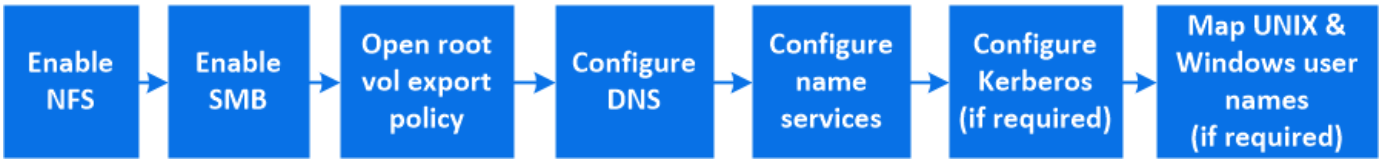
- Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
- If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of 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

Create or modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

This procedure enables a new or existing storage VM to serve both NFS and SMB protocols. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



Steps

1. Enable NFS and SMB on a storage VM.
   a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS** and **Enable NFS**.
      - Enter the following information:
        - Administrator name and password
        - Server name
        - Active directory domain
      - Confirm the Organizational Unit.
      - Confirm the DNS values.
      - Confirm the default language.
      - Add network interfaces.
      - Update storage VM administrator account information (optional).
   b. For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, and then click **Settings**. Complete the following sub-steps if NFS or SMB is not already enabled.
      - Click ⚙ under **NFS**.
      - Click ⚙ under **SMB**.

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 = NFS 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. 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.
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 ✎ under **Name Services Switch**.
5. Configure Kerberos if required: click → in the Kerberos tile and then click **Add**.
6. 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.

Configure NFS with the CLI

NFS configuration overview with the CLI

You can use ONTAP 9 CLI commands to configure NFS client access to files contained in a new volume or qtree in a new or existing storage virtual machine (SVM).

Use these procedures if you want to configure access to a volume or qtree in the following way:

- You want to use any version of NFS currently supported by ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2, or NFSv4.1 with pNFS.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

  To use System Manager to configure NAS multiprotocol access, see Provision NAS storage for both Windows and Linux using both NFS and SMB.

- You want to use best practices, not explore every available option.

  Details about command syntax are available from CLI help and ONTAP man pages.

- UNIX file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

If you want details about the range of ONTAP NFS protocol capabilities, consult the NFS reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Linux servers using NFS
System Manager Classic (available with ONTAP 9.7 and earlier	NFS configuration overview

NFS configuration workflow

Configuring NFS involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal—configuring NFS access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for NFS access.

Preparation

Assess physical storage requirements

Before provisioning NFS storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

Steps

1. Display available space in existing aggregates:

   ```
   storage aggregate show
   ```

   If there is an aggregate with sufficient space, record its name in the worksheet.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

Related information

ONTAP concepts

Assess networking requirements

Before providing NFS storage to clients, you must verify that networking is correctly configured to meet the NFS provisioning requirements.

What you'll need

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

Steps

1. Display the available physical and virtual ports:

   `network port show`

   - When possible, you should use the port with the highest speed for the data network.
   - All components in the data network must have the same MTU setting for best performance.

2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: +

   `network subnet show`

   Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

3. Display available IPspaces:

   `network ipspace show`

   You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster:

   `network options ipv6 show`

   If required, you can enable IPv6 by using the `network options ipv6 modify` command.

Decide where to provision new NFS storage capacity

Before you create a new NFS volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has NFS enabled but not configured, complete the steps in both "Configuring NFS access to an SVM" and "Adding NFS storage to an NFS-enabled SVM".

  Configure NFS access to an SVM

  Add NFS storage to an NFS-enabled SVM

  You might choose to create a new SVM if one of the following is true:

  - You are enabling NFS on a cluster for the first time.
  - You have existing SVMs in a cluster in which you do not want to enable NFS support.
  - You have one or more NFS-enabled SVMs in a cluster, and you want another NFS server in an isolated namespace (multi-tenancy scenario).
    You should also choose this option to provision storage on an existing SVM that has NFS enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

  After enabling NFS on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for NFS access, complete the steps in "Adding NFS storage to an NFS-enabled SVM".

  Adding NFS storage to an NFS-enabled SVM

Worksheet for gathering NFS configuration information

The NFS configuration worksheet enables you to collect the required information to set up NFS access for clients.

You should complete one or both sections of the worksheet depending on the decision you made about where to provision storage:

- If you are configuring NFS access to an SVM, you should complete both sections.

  Configuring NFS access to an SVM

  Adding storage capacity to an NFS-enabled SVM

- If you are adding storage capacity to an NFS-enabled SVM, you should complete only the second section.

  Adding storage capacity to an NFS-enabled SVM

See the command man pages for details about the parameters.

Configure NFS access to an SVM

Parameters for creating an SVM

You supply these values with the `vserver create` command if you are creating a new SVM.

Field	Description	Your value
`-vserver`	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for new NFS storage capacity.	
`-rootvolume`	A unique name you supply for the SVM root volume.	
`-rootvolume-security-style`	Use the UNIX security style for the SVM.	`unix`
`-language`	Use the default language setting in this workflow.	`C.UTF-8`
`ipspace`	IPspaces are distinct IP address spaces in which (storage virtual machines (SVMs)) reside.	

Parameters for creating an NFS server

You supply these values with the `vserver nfs create` command when you create a new NFS server and specify supported NFS versions.

If you are enabling NFSv4 or later, you should use LDAP for improved security.

Field	Description	Your value
`-v3`, `-v4.0`, `-v4.1`, `-v4.1-pnfs`	Enable NFS versions as needed. v4.2 is also supported in ONTAP 9.8 and later when `v4.1` is enabled.	
`-v4-id-domain`	ID mapping domain name.	
`-v4-numeric-ids`	Support for numeric owner IDs (enabled or disabled).	

Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs.

If you are using Kerberos, you should enable Kerberos on multiple LIFs.

Field	Description	Your value
`-lif`	A name you supply for the new LIF.	
`-role`	Use the data LIF role in this workflow.	`data`
`-data-protocol`	Use only the NFS protocol in this workflow.	`nfs`
`-home-node`	The node to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-home-port`	The port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.	

`-address`	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
`-netmask`	The network mask and gateway for the LIF.	
`-subnet`	A pool of IP addresses. Used instead of `-address` and `-netmask` to assign addresses and netmasks automatically.	
`-firewall-policy`	Use the default data firewall policy in this workflow.	`data`

Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS.

Field	Description	Your value
`-domains`	Up to five DNS domain names.	
`-name-servers`	Up to three IP addresses for each DNS name server.	

Name service information

Parameters for creating local users

You supply these values if you are creating local users by using the `vserver services name-service unix-user create` command. If you are configuring local users by loading a file containing UNIX users from a uniform resource identifier (URI), you do not need to specify these values manually.

	User name (`-user`)	**User ID** (`-id`)	**Group ID** (`-primary-gid`)	**Full name** (`-full-name`)
Example	johnm	123	100	John Miller
1				
2				
3				
…				

n				

Parameters for creating local groups

You supply these values if you are creating local groups by using the `vserver services name-service unix-group create` command. If you are configuring local groups by loading a file containing UNIX groups from a URI, you do not need to specify these values manually.

	Group name (`-name`)	**Group ID (`-id`)**
Example	Engineering	100
1		
2		
3		
…		
n		

Parameters for NIS

You supply these values with the `vserver services name-service nis-domain create` command.

Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

Field	**Description**	**Your value**
`-domain`	The NIS domain that the SVM will use for name lookups.	
`-active`	The active NIS domain server.	`true` or `false`
`-servers`	ONTAP 9.0, 9.1: One or more IP addresses of NIS servers used by the NIS domain configuration.	
`-nis-servers`	ONTAP 9.2: A comma-separated list of IP addresses and hostnames for the NIS servers used by the domain configuration.	

Parameters for LDAP

You supply these values with the `vserver services name-service ldap client create` command.

You will also need a self-signed root CA certificate `.pem` file.

Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

Field	Description	Your value
`-vserver`	The name of the SVM for which you want to create an LDAP client configuration.	
`-client-config`	The name you assign for the new LDAP client configuration.	
`-servers`	ONTAP 9.0, 9.1: One or more LDAP servers by IP address in a comma-separated list.	
`-ldap-servers`	ONTAP 9.2: A comma-separated list of IP addresses and hostnames for the LDAP servers.	
`-query-timeout`	Use the default `3` seconds for this workflow.	`3`
`-min-bind-level`	The minimum bind authentication level. The default is `anonymous`. Must be set to `sasl` if signing and sealing is configured.	
`-preferred-ad-servers`	One or more preferred Active Directory servers by IP address in a comma-delimited list.	
`-ad-domain`	The Active Directory domain.	
`-schema`	The schema template to use. You can use a default or custom schema.	
`-port`	Use the default LDAP server port `389` for this workflow.	`389`
`-bind-dn`	The Bind user distinguished name.	

Field	Description	Your value
`-base-dn`	The base distinguished name. The default is `""` (root).	
`-base-scope`	Use the default base search scope `subnet` for this workflow.	`subnet`
`-session-security`	Enables LDAP signing or signing and sealing. The default is `none`.	
`-use-start-tls`	Enables LDAP over TLS. The default is `false`.	

Parameters for Kerberos authentication

You supply these values with the `vserver nfs kerberos realm create` command. Some of the values will differ depending on whether you use Microsoft Active Directory as a Key Distribution Center (KDC) server, or MIT or other UNIX KDC server.

Field	Description	Your value
`-vserver`	The SVM that will communicate with the KDC.	
`-realm`	The Kerberos realm.	
`-clock-skew`	Permitted clock skew between clients and servers.	
`-kdc-ip`	KDC IP address.	
`-kdc-port`	KDC port number.	
`-adserver-name`	Microsoft KDC only: AD server name.	
`-adserver-ip`	Microsoft KDC only: AD server IP address.	
`-adminserver-ip`	UNIX KDC only: Admin server IP address.	
`-adminserver-port`	UNIX KDC only: Admin server port number.	

`-passwordserver-ip`	UNIX KDC only: Password server IP address.	
`-passwordserver-port`	UNIX KDC only: Password server port.	
`-kdc-vendor`	KDC vendor.	{ `Microsoft` | `Other` }
`-comment`	Any desired comments.	

You supply these values with the `vserver nfs kerberos interface enable` command.

Field	Description	Your value
`-vserver`	The name of the SVM for which you want to create a Kerberos configuration.	
`-lif`	The data LIF on which you will enable Kerberos. You can enable Kerberos on multiple LIFs.	
`-spn`	The Service Principle Name (SPN)	
`-permitted-enc-types`	The permitted encryption types for Kerberos over NFS; `aes-256` is recommended, depending on client capabilities.	
`-admin-username`	The KDC administrator credentials to retrieve the SPN secret key directly from the KDC. A password is required	
`-keytab-uri`	The keytab file from the KDC containing the SPN key if you do not have KDC administrator credentials.	
`-ou`	The organizational unit (OU) under which the Microsoft Active Directory server account will be created when you enable Kerberos using a realm for Microsoft KDC.	

Adding storage capacity to an NFS-enabled SVM

Parameters for creating export policies and rules

You supply these values with the `vserver export-policy create` command.

Field	Description	Your value
`-vserver`	The name of the SVM that will host the new volume.	
`-policyname`	A name you supply for a new export policy.	

You supply these values for each rule with the `vserver export-policy rule create` command.

Field	Description	Your value
`-clientmatch`	Client match specification.	
`-ruleindex`	Position of export rule in the list of rules.	
`-protocol`	Use NFS in this workflow.	`nfs`
`-rorule`	Authentication method for read-only access.	
`-rwrule`	Authentication method for read-write access.	
`-superuser`	Authentication method for superuser access.	
`-anon`	User ID to which anonymous users are mapped.	

You must create one or more rules for each export policy.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Examples	0.0.0.0/0,@rootaccess_netgroup	any	krb5	sys	65534
1					
2					
3					
…					

n					

Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a qtree.

Field	Description	Your value
`-vserver`	The name of a new or existing SVM that will host the new volume.	
`-volume`	A unique descriptive name you supply for the new volume.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for the new NFS volume.	
`-size`	An integer you supply for the size of the new volume.	
`-user`	Name or ID of the user that is set as the owner of the volume's root.	
`-group`	Name or ID of the group that is set as the owner of the volume's root.	
`--security-style`	Use the UNIX security style for this workflow.	`unix`
`-junction-path`	Location under root (/) where the new volume is to be mounted.	
`-export-policy`	If you are planning to use an existing export policy, you can enter its name when you create the volume.	

Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume.

Field	Description	Your value
`-vserver`	The name of the SVM on which the volume containing the qtree resides.	

`-volume`	The name of the volume that will contain the new qtree.	
`-qtree`	A unique descriptive name you supply for the new qtree, 64 characters or less.	
`-qtree-path`	The qtree path argument in the format `/vol/volume_name/qtree_name\>` can be specified instead of specifying volume and qtree as separate arguments.	
`-unix-permissions`	Optional: The UNIX permissions for the qtree.	
`-export-policy`	If you are planning to use an existing export policy, you can enter its name when you create the qtree.	

Configure NFS access to an SVM

Create an SVM

If you do not already have at least one SVM in a cluster to provide data access to NFS clients, you must create one.

Steps

1. Create an SVM:

   ```
   vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
   ipspace_name
   ```

   - Use the UNIX setting for the `-rootvolume-security-style` option.
   - Use the default C.UTF-8 `-language` option.
   - The `ipspace` setting is optional.

2. Verify the configuration and status of the newly created SVM:

   ```
   vserver show -vserver vserver_name
   ```

   The `Allowed Protocols` field must include NFS. You can edit this list later.

   The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Verify that the NFS protocol is enabled on the SVM

Before you can configure and use NFS on SVMs, you must verify that the protocol is enabled.

About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.

> You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

Steps

1. Check which protocols are currently enabled and disabled for the SVM:

   `vserver show -vserver vserver_name -protocols`

   You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:
   - To enable the NFS protocol:

     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - To disable a protocol:

     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Confirm that the enabled and disabled protocols were updated correctly:

   `vserver show -vserver vserver_name -protocols`

Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

The following command allows access over NFS by adding `nfs` to the list of enabled protocols on the SVM named vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Open the export policy of the SVM root volume

The default export policy of the SVM root volume must include a rule to allow all clients open access through NFS. Without such a rule, all NFS clients are denied access to the

SVM and its volumes.

About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that access is open to all NFS clients in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

Steps

1. If you are using an existing SVM, check the default root volume export policy:

   ```
   vserver export-policy rule show
   ```

   The command output should be similar to the following:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   If the SVM will only contain volumes secured by Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` or `krb5i`. For example:

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Verify rule creation by using the `vserver export-policy rule show` command.

Result

Any NFS client can now access any volume or qtree created on the SVM.

Create an NFS server

After verifying that NFS is licensed on your cluster, you can use the `vserver nfs create` command to create an NFS server on the SVM and specify the NFS versions it supports.

What you'll need

The SVM must have been configured to allow the NFS protocol.

About this task

The SVM can be configured to support one or more versions of NFS. If you are supporting NFSv4 or later:

- The NFSv4 user ID mapping domain name must be the same on the NFSv4 server and target clients.

  It does not necessarily need to be the same as an LDAP or NIS domain name as long as the NFSv4 server and clients are using the same name.

- Target clients must support the NFSv4 numeric ID setting.
- For security reasons, you should use LDAP for name services in NFSv4 deployments.

Steps

1. Verify that NFS is licensed on your cluster:

   ```
   system license show -package nfs
   ```

   If it is not, contact your sales representative.

2. Create an NFS server:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   You can choose to enable any combination of NFS versions. If you want to support pNFS, you must enable both `-v4.1` and `-v4.1-pnfs` options.

   If you enable v4 or later, you should also be sure that the following options are set correctly:

   - `-v4-id-domain`

     This optional parameter specifies the domain portion of the string form of user and group names as defined by the NFSv4 protocol. By default, ONTAP uses the NIS domain if one is set; if not, the DNS domain is used. You must supply a value that matches the domain name used by target clients.

   - `-v4-numeric-ids`

     This optional parameter specifies whether the support for numeric string identifiers in NFSv4 owner attributes is enabled. The default setting is enabled but you should verify that the target clients support it.

   You can enable additional NFS features later by using the `vserver nfs modify` command.

3. Verify that NFS is running:

```
vserver nfs status -vserver vserver_name
```

4. Verify that NFS is configured as desired:

```
vserver nfs show -vserver vserver_name
```

Examples

The following command creates an NFS server on the SVM named vs1 with NFSv3 and NFSv4.0 enabled:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

The following commands verify the status and configuration values of the new NFS server named vs1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                 General NFS Access: true
                              NFS v3: enabled
                            NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

What you'll need

- The underlying physical or logical network port must have been configured to the administrative `up` status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you are using Kerberos authentication, enable Kerberos on multiple LIFs.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM

Steps

1. Create a LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol nfs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

Option	Description
ONTAP 9.5 and earlier	`network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data-protocol nfs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall -policy data -auto-revert {true|false}`

ONTAP 9.6 and later	`network interface create -vserver vserver_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}`

- The `-role` parameter is not required when creating a LIF using a service policy (beginning withONTAP 9.6).
- The `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.

  The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

  You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` man page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default `data` as the LIF role.

  You can create and add a custom firewall policy later if desired.

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

2. Verify that the LIF was created successfully by using the `network interface show` command.
3. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`

IPv6 address	`network ping6`

4. If you are using Kerberos, repeat Steps 1 through 3 to create additional LIFs.

   Kerberos must be enabled separately on each of these LIFs.

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

The following command shows how to create a NAS data LIF that is assigned with the `default-data-files` service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Enable DNS for host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are

resolved using external DNS servers.

What you'll need

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

About this task

The *Network Management Guide* contains information about configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   The following command enables external DNS server servers on the SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   Beginning with ONTAP 9.2, the `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command.

   The following command displays the DNS configurations for all SVMs in the cluster:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

   The `vserver services name-service dns check` command is available beginning with ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure name services

Configure name services overview

Depending on the configuration of your storage system, ONTAP needs to be able to look up host, user, group, or netgroup information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external name services to obtain this information.

You should use a name service such as NIS or LDAP to facilitate name lookups during client authentication. It is best to use LDAP whenever possible for greater security, especially when deploying NFSv4 or later. You should also configure local users and groups in case external name servers are not available.

Name service information must be kept synchronized on all sources.

Configure the name service switch table

You must configure the name service switch table correctly to enable ONTAP to consult local or external name services to retrieve host, user, group, netgroup, or name mapping information.

What you'll need

You must have decided which name services you want to use for host, user, group, netgroup, or name mapping as applicable to your environment.

If you plan to use netgroups, all IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

About this task

Do not include information sources that are not being used. For example, if NIS is not being used in your environment, do not specify the `-sources nis` option.

Steps

1. Add the necessary entries to the name service switch table:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Verify that the name service switch table contains the expected entries in the desired order:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   If you want to make any corrections, you must use the `vserver services name-service ns-switch modify` or `vserver services name-service ns-switch delete` commands.

Example

The following example creates a new entry in the name service switch table for the SVM vs1 to use the local netgroup file and an external NIS server to look up netgroup information in that order:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

After you finish

- You must configure the name services you have specified for the SVM to provide data access.
- If you delete any name service for the SVM, you must remove it from the name service switch table as well.

  The client access to the storage system might not work as expected, if you fail to delete the name service from the name service switch table.

Configure local UNIX users and groups

Configure local UNIX users and groups overview

You can use local UNIX users and groups on the SVM for authentication and name mappings. You can create UNIX users and groups manually, or you can load a file containing UNIX users or groups from a uniform resource identifier (URI).

There is a default maximum limit of 32,768 local UNIX user groups and group members combined in the cluster. The cluster administrator can modify this limit.

Create a local UNIX user

You can use the `vserver services name-service unix-user create` command to create local UNIX users. A local UNIX user is a UNIX user you create on the

SVM as a UNIX name services option to be used in the processing of name mappings.

Step

1. Create a local UNIX user:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* specifies the user name. The length of the user name must be 64 characters or fewer.

   `-id` *`integer`* specifies the user ID that you assign.

   `-primary-gid` *`integer`* specifies the primary group ID. This adds the user to the primary group. After creating the user, you can manually add the user to any desired additional group.

Example

The following command creates a local UNIX user named johnm (full name "John Miller") on the SVM named vs1. The user has the ID 123 and the primary group ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Load local UNIX users from a URI

As an alternative to manually creating individual local UNIX users in SVMs, you can simplify the task by loading a list of local UNIX users into SVMs from a uniform resource identifier (URI) (`vserver services name-service unix-user load-from-uri`).

Steps

1. Create a file containing the list of local UNIX users you want to load.

   The file must contain user information in the UNIX `/etc/passwd` format:

   `user_name: password: user_ID: group_ID: full_name`

   The command discards the value of the *`password`* field and the values of the fields after the *`full_name`* field (*`home_directory`* and *`shell`*).

   The maximum supported file size is 2.5 MB.

2. Verify that the list does not contain any duplicate information.

   If the list contains duplicate entries, loading the list fails with an error message.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX users into SVMs from the URI:

   `vserver services name-service unix-user load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite {true|false}` specifies whether to overwrite entries. The default is `false`.

Example

The following command loads a list of local UNIX users from the URI `ftp://ftp.example.com/passwd` into the SVM named vs1. Existing users on the SVM are not overwritten by information from the URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Create a local UNIX group

You can use the `vserver services name-service unix-group create` command to create UNIX groups that are local to the SVM. Local UNIX groups are used with local UNIX users.

Step

1. Create a local UNIX group:

   `vserver services name-service unix-group create -vserver` *vserver_name* `-name` *group_name* `-id` *integer*

   `-name` *group_name* specifies the group name. The length of the group name must be 64 characters or fewer.

   `-id` *integer* specifies the group ID that you assign.

Example

The following command creates a local group named eng on the SVM named vs1. The group has the ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Add a user to a local UNIX group

You can use the `vserver services name-service unix-group adduser` command to add a user to a supplemental UNIX group that is local to the SVM.

Step

1. Add a user to a local UNIX group:

`vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name`

`-name group_name` specifies the name of the UNIX group to add the user to in addition to the user's primary group.

Example

The following command adds a user named max to a local UNIX group named eng on the SVM named vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Load local UNIX groups from a URI

As an alternative to manually creating individual local UNIX groups, you can load a list of local UNIX groups into SVMs from a uniform resource identifier (URI) by using the `vserver services name-service unix-group load-from-uri` command.

Steps

1. Create a file containing the list of local UNIX groups you want to load.

   The file must contain group information in the UNIX `/etc/group` format:

   group_name: password: group_ID: comma_separated_list_of_users

   The command discards the value of the *password* field.

   The maximum supported file size is 1 MB.

   The maximum length of each line in the group file is 32,768 characters.

2. Verify that the list does not contain any duplicate information.

   The list must not contain duplicate entries, or else loading the list fails. If there are entries already present in the SVM, you must either set the `-overwrite` parameter to `true` to overwrite all existing entries with the new file, or ensure that the new file does not contain any entries that duplicate existing entries.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

   The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX groups into the SVM from the URI:

   `vserver services name-service unix-group load-from-uri -vserver vserver_name -uri {ftp|http|ftps|https}://uri -overwrite {true|false}`

`-overwrite` {`true`|`false`} specifies whether to overwrite entries. The default is `false`. If you specify this parameter as `true`, ONTAP replaces the entire existing local UNIX group database of the specified SVM with the entries from the file you are loading.

Example

The following command loads a list of local UNIX groups from the URI `ftp://ftp.example.com/group` into the SVM named vs1. Existing groups on the SVM are not overwritten by information from the URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Work with netgroups

Working with netgroups overview

You can use netgroups for user authentication and to match clients in export policy rules. You can provide access to netgroups from external name servers (LDAP or NIS), or you can load netgroups from a uniform resource identifier (URI) into SVMs using the `vserver services name-service netgroup load` command.

What you'll need

Before working with netgroups, you must ensure the following conditions are met:

- All hosts in netgroups, regardless of source (NIS, LDAP, or local files), must have both forward (A) and reverse (PTR) DNS records to provide consistent forward and reverse DNS lookups.

  In addition, if an IP address of a client has multiple PTR records, all of those host names must be members of the netgroup and have corresponding A records.

- The names of all hosts in netgroups, regardless of their source (NIS, LDAP, or local files), must be correctly spelled and use the correct case. Case inconsistencies in host names used in netgroups can lead to unexpected behavior, such as failed export checks.
- All IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

  For example, 2011:hu9:0:0:0:0:3:1 must be shortened to 2011:hu9::3:1.

About this task

When you work with netgroups, you can perform the following operations:

- You can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.
- You can use the `vserver services name-service getxxbyyy netgrp` command to check whether a client is part of a netgroup.

  The underlying service for doing the lookup is selected based on the configured name service switch order.

Load netgroups into SVMs

One of the methods you can use to match clients in export policy rules is by using hosts listed in netgroups. You can load netgroups from a uniform resource identifier (URI) into SVMs as an alternative to using netgroups stored in external name servers (`vserver services name-service netgroup load`).

What you'll need

Netgroup files must meet the following requirements before being loaded into an SVM:

- The file must use the same proper netgroup text file format that is used to populate NIS.

  ONTAP checks the netgroup text file format before loading it. If the file contains errors, it will not be loaded and a message is displayed indicating the corrections you have to perform in the file. After correcting the errors, you can reload the netgroup file into the specified SVM.

- Any alphabetic characters in host names in the netgroup file should be lowercase.
- The maximum supported file size is 5 MB.
- The maximum supported level for nesting netgroups is 1000.
- Only primary DNS host names can be used when defining host names in the netgroup file.

  To avoid export access issues, host names should not be defined using DNS CNAME or round robin records.

- The user and domain portions of triples in the netgroup file should be kept empty because ONTAP does not support them.

  Only the host/IP part is supported.

About this task

ONTAP supports netgroup-by-host searches for the local netgroup file. After you load the netgroup file, ONTAP automatically creates a netgroup.byhost map to enable netgroup-by-host searches. This can significantly speed up local netgroup searches when processing export policy rules to evaluate client access.

Step

1. Load netgroups into SVMs from a URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Loading the netgroup file and building the netgroup.byhost map can take several minutes.

   If you want to update the netgroups, you can edit the file and load the updated netgroup file into the SVM.

Example

The following command loads netgroup definitions into the SVM named vs1 from the HTTP URL `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verify the status of netgroup definitions

After loading netgroups into the SVM, you can use the `vserver services name-service netgroup status` command to verify the status of netgroup definitions. This enables you to determine whether netgroup definitions are consistent on all of the nodes that back the SVM.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Verify the status of netgroup definitions:

   ```
   vserver services name-service netgroup status
   ```

   You can display additional information in a more detailed view.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

After the privilege level is set, the following command displays netgroup status for all SVMs:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Create an NIS domain configuration

If a Network Information Service (NIS) is used in your environment for name services, you must create an NIS domain configuration for the SVM by using the `vserver services name-service nis-domain create` command.

What you'll need

All configured NIS servers must be available and reachable before you configure the NIS domain on the SVM.

If you plan to use NIS for directory searches, the maps in your NIS servers cannot have more than 1,024 characters for each entry. Do not specify the NIS server that does not comply with this limit. Otherwise, client access dependent on NIS entries might fail.

About this task

You can create multiple NIS domains. However, you can only use one that is set to `active`.

If your NIS database contains a `netgroup.byhost` map, ONTAP can use it for quicker searches. The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues. Beginning with ONTAP 9.7, NIS `netgroup.byhost` entries can be cached using the `vserver services name-service nis-domain netgroup-database` commands.

Using NIS for host name resolution is not supported.

Steps

1. Create an NIS domain configuration:

```
vserver services name-service nis-domain create -vserver vs1 -domain
domain_name -active true -servers IP_addresses
```

You can specify up to 10 NIS servers.

> Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

2. Verify that the domain is created:

```
vserver services name-service nis-domain show
```

Example

The following command creates and makes an active NIS domain configuration for an NIS domain called nisdomain on the SVM named vs1 with an NIS server at IP address 192.0.2.180:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

Use LDAP

Overview of using LDAP

If LDAP is used in your environment for name services, you need to work with your LDAP administrator to determine requirements and appropriate storage system configurations, then enable the SVM as an LDAP client.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with name servers, use the `-try-channel-binding` parameter with the `ldap client modify` command.

For more information, see
2020 LDAP channel binding and LDAP signing requirements for Windows.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:
  - The domain name of the LDAP server must match the entry on the LDAP client.
  - The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
    - CRYPT (all types) and SHA-1 (SHA, SSHA).
    - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
  - If the LDAP server requires session security measures, you must configure them in the LDAP client.

    The following session security options are available:

        - LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
        - START TLS
        - LDAPS (LDAP over TLS or SSL)
    - To enable signed and sealed LDAP queries, the following services must be configured:
        - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
        - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
        - Kerberos servers must have SRV records present on the DNS server.
    - To enable START TLS or LDAPS, the following points should be considered.
        - It is a NetApp best practice to use Start TLS rather than LDAPS.
        - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
        - A certificate server must already be configured in the domain.
    - To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
        - Both domains should be configured with one of the following trust relationships:
            - Two-way
            - One-way, where the primary trusts the referral domain
            - Parent-child
        - DNS must be configured to resolve all referred server names.
        - Domain passwords should be same to authenticate when --bind-as-cifs-server set to true.

The following configurations are not supported with LDAP referral chasing.

- For all ONTAP versions:
    - LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
    - LDAP signing and sealing (the `-session-security` option)
    - Encrypted TLS connections (the `-use-start-tls` option)
    - Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

  In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

Create a new LDAP client schema

If the LDAP schema in your environment differs from the ONTAP defaults, you must

create a new LDAP client schema for ONTAP before creating the LDAP client configuration.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

If you need to use a non-default LDAP schema, you must create it before creating the LDAP client configuration. Consult with your LDAP administrator before creating a new schema.

The default LDAP schemas provided by ONTAP cannot be modified. To create a new schema, you create a copy and then modify the copy accordingly.

Steps

1. Display the existing LDAP client schema templates to identify the one you want to copy:

   ```
   vserver services name-service ldap client schema show
   ```

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

3. Make a copy of an existing LDAP client schema:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modify the new schema and customize it for your environment:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Install the self-signed root CA certificate on the SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

About this task

When LDAP over TLS is enabled, the ONTAP LDAP client on the SVM does not support revoked certificates in ONTAP 9.0 and 9.1.

Beginning with ONTAP 9.2, all applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

Steps

1. Install the self-signed root CA certificate:
   a. Begin the certificate installation:

      `security certificate install -vserver vserver_name -type server-ca`

      The console output displays the following message:

      `Please enter Certificate: Press <Enter> when done`

   b. Open the certificate `.pem` file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
   c. Verify that the certificate is displayed correctly.
   d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed:

   `security certificate show -vserver vserver_name`

Create an LDAP client configuration

If you want ONTAP to access the external LDAP servers in your environment, you must first set up an LDAP client on the storage system.

What you'll need

One of the first three servers in the AD-domain resolved list must be up and serving data. Otherwise, this task fails.

There are multiple servers, out of which more than two servers are down at any point of time.

Steps

1. Consult with your LDAP administrator to determine the appropriate configuration values for the `vserver services name-service ldap client create` command:
   a. Specify a domain-based or an address-based connection to LDAP servers.

      The `-ad-domain` and `-servers` options are mutually exclusive.

      - Use the `-ad-domain` option to enable LDAP server discovery in the Active Directory domain.

        You can use the `-preferred-ad-servers` option to specify one or more preferred Active Directory servers by IP address in a comma-delimited list. After the client is created, you can modify this list by using the `vserver services name-service ldap client modify` command.

      - Use the `-servers` option to specify one or more LDAP servers (AD or UNIX) by IP address in a comma-delimited list.

The `-servers` option is deprecated in ONTAP 9.2. Beginning with ONTAP 9.2, the `-ldap-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address for the LDAP server.

b. Specify a default or custom LDAP schema.

Most LDAP servers can use the default read-only schemas that are provided by ONTAP. It is best to use those default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema (they are read-only), and then modifying the copy.

Default schemas:

- MS-AD-BIS

  Based on RFC-2307bis, this is the preferred LDAP schema for most standard Windows 2012 and later LDAP deployments.

- `AD-IDMU`

  Based on Active Directory Identity Management for UNIX, this schema is appropriate for most Windows 2008, Windows 2012, and later AD servers.

- `AD-SFU`

  Based on Active Directory Services for UNIX, this schema is appropriate for most Windows 2003 and earlier AD servers.

- `RFC-2307`

  Based on RFC-2307 (*An Approach for Using LDAP as a Network Information Service*), this schema is appropriate for most UNIX AD servers.

c. Select bind values.

- `-min-bind-level {anonymous|simple|sasl}` specifies the minimum bind authentication level.

  The default value is **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* specifies the bind user.

  For Active Directory servers, you must specify the user in the account (DOMAIN\user) or principal (user@domain.com) form. Otherwise, you must specify the user in distinguished name (CN=user,DC=domain,DC=com) form.

- `-bind-password` *`password`* specifies the bind password.

d. Select session security options, if required.

You can enable either LDAP signing and sealing or LDAP over TLS if required by the LDAP server.

- `--session-security {none|sign|seal}`

  You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

You should also set `-min-bind-level {sasl}` unless you want the bind authentication to fall back to **`anonymous`** or **`simple`** if the signing and sealing bind fails.

- `-use-start-tls {true|false}`

  If set to **`true`** and the LDAP server supports it, the LDAP client uses an encrypted TLS connection to the server. The default value is **`false`**. You must install a self-signed root CA certificate of the LDAP server to use this option.

  > If the SVM has a SMB server added to a domain and the LDAP server is one of the domain controllers of the home-domain of the SMB server, then you can modify the `-session-security-for-ad-ldap` option by using the `vserver cifs security modify` command.

e. Select port, query, and base values.

The default values are recommended, but you must verify with your LDAP administrator that they are appropriate for your environment.

- `-port` *`port`* specifies the LDAP server port.

  The default value is `389`.

  If you plan to use Start TLS to secure the LDAP connection, you must use the default port 389. Start TLS begins as a plaintext connection over the LDAP default port 389, and that connection is then upgraded to TLS. If you change the port, Start TLS fails.

- `-query-timeout` *`integer`* specifies the query timeout in seconds.

  The allowed range is from 1 through 10 seconds. The default value is `3` seconds.

- `-base-dn` *`LDAP_DN`* specifies the base DN.

  Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled). The default value is `""` (root).

- `-base-scope {base|onelevel|subtree}` specifies the base search scope.

  The default value is `subtree`.

- `-referral-enabled {true|false}` specifies whether LDAP referral chasing is enabled.

  Beginning with ONTAP 9.5, this allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is returned by the primary LDAP server indicating that the desired records are present on referred LDAP servers. The default value is **`false`**.

  To search for records present in the referred LDAP servers, the base-dn of the referred records must be added to the base-dn as part of LDAP client configuration.

2. Create an LDAP client configuration on the SVM:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain
```

```
-preferred-ad-servers preferred_ad_server_list -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

You must provide the SVM name when creating an LDAP client configuration.

3. Verify that the LDAP client configuration is created successfully:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Examples

The following command creates a new LDAP client configuration named ldap1 for the SVM vs1 to work with an Active Directory server for LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 –ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

The following command creates a new LDAP client configuration named ldap1 for the SVM vs1 to work with an Active Directory server for LDAP on which signing and sealing is required:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 –ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

The following command creates a new LDAP client configuration named ldap1 for the SVM vs1 to work with an Active Directory server for LDAP where LDAP referral chasing is required:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 –ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

The following command modifies the LDAP client configuration named ldap1 for the SVM vs1 by specifying the base DN:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

The following command modifies the LDAP client configuration named ldap1 for the SVM vs1 by enabling referral chasing:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associate the LDAP client configuration with SVMs

To enable LDAP on an SVM, you must use the `vserver services name-service ldap create` command to associate an LDAP client configuration with the SVM.

What you'll need

- An LDAP domain must already exist within the network and must be accessible to the cluster that the SVM is located on.
- An LDAP client configuration must exist on the SVM.

Steps

1. Enable LDAP on the SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   Beginning with ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

   The following command enables LDAP on the "vs1"SVM and configures it to use the "ldap1" LDAP client configuration:

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

The name service check command is available beginning with ONTAP 9.2.

Verify LDAP sources in the name service switch table

You must verify that LDAP sources for name services are listed correctly in the name service switch table for the SVM.

Steps

1. Display the current name service switch table contents:

   `vserver services name-service ns-switch show -vserver svm_name`

   The following command shows the results for the SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

   `namemap` specifies the sources to search for name mapping information and in what order. In a UNIX-only environment, this entry is not necessary. Name mapping is only required in a mixed environment using both UNIX and Windows.

2. Update the `ns-switch` entry as appropriate:

If you want to update the ns-switch entry for…	Enter the command…
User information	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

If you want to update the ns-switch entry for…	Enter the command…
Group information	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Netgroup information	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Use Kerberos with NFS for strong security

Overview of using Kerberos with NFS for strong security

If Kerberos is used in your environment for strong authentication, you need to work with your Kerberos administrator to determine requirements and appropriate storage system configurations, and then enable the SVM as a Kerberos client.

Your environment should meet the following guidelines:

- Your site deployment should follow best practices for Kerberos server and client configuration before you configure Kerberos for ONTAP.
- If possible, use NFSv4 or later if Kerberos authentication is required.

  NFSv3 can be used with Kerberos. However, the full security benefits of Kerberos are only realized in ONTAP deployments of NFSv4 or later.

- To promote redundant server access, Kerberos should be enabled on several data LIFs on multiple nodes in the cluster using the same SPN.
- When Kerberos is enabled on the SVM, one of the following security methods must be specified in export rules for volumes or qtrees depending on your NFS client configuration.
  - `krb5` (Kerberos v5 protocol)
  - `krb5i` (Kerberos v5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos v5 protocol with privacy service)

In addition to the Kerberos server and clients, the following external services must be configured for ONTAP to support Kerberos:

- Directory service

  You should use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS. Do not use NIS, whose requests are sent in clear text and are hence not secure.

- NTP

  You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

  Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

Verify permissions for Kerberos configuration

Kerberos requires that certain UNIX permissions be set for the SVM root volume and for local users and groups.

Steps

1. Display the relevant permissions on the SVM root volume:

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   The root volume of the SVM must have the following configuration:

Name…	Setting…
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

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

2. Display the local UNIX users:

   `vserver services name-service unix-user show -vserver vserver_name`

   The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase. The first component of the NFS client user SPN is used as the user. The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.
root	0	0	Required for mounting.

If these values are not shown, you can use the `vserver services name-service unix-user modify` command to update them.

3. Display the local UNIX groups:

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

   If these values are not shown, you can use the `vserver services name-service unix-group modify` command to update them.

Create an NFS Kerberos realm configuration

If you want ONTAP to access external Kerberos servers in your environment, you must first configure the SVM to use an existing Kerberos realm. To do so, you need to gather configuration values for the Kerberos KDC server, and then use the `vserver nfs kerberos realm create` command to create the Kerberos realm configuration on an SVM.

What you'll need

The cluster administrator should have configured NTP on the storage system, client, and KDC server to avoid authentication issues. Time differences between a client and server (clock skew) are a common cause of authentication failures.

Steps

1. Consult with your Kerberos administrator to determine the appropriate configuration values to supply with the `vserver nfs kerberos realm create` command.
2. Create a Kerberos realm configuration on the SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name {AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Verify that the Kerberos realm configuration was created successfully:

   `vserver nfs kerberos realm show`

Examples

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses a Microsoft Active Directory server as the KDC server. The Kerberos realm is AUTH.EXAMPLE.COM. The Active Directory server is named ad-1 and its IP address is 10.10.8.14. The permitted clock skew is 300 seconds (the default). The IP address of the KDC server is 10.10.8.14, and its port number is 88 (the default). "Microsoft Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses an MIT KDC. The Kerberos realm is SECURITY.EXAMPLE.COM. The permitted clock skew is 300 seconds. The IP address of the KDC server is 10.10.9.1, and its port number is 88. The KDC vendor is Other to indicate a UNIX vendor. The IP address of the administrative server is 10.10.9.1, and its port number is 749 (the default). The IP address of the password server is 10.10.9.1, and its port number is 464 (the default). "UNIX Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configure NFS Kerberos permitted encryption types

By default, ONTAP supports the following encryption types for NFS Kerberos: DES, 3DES, AES-128, and AES-256. You can configure the permitted encryption types for each SVM to suit the security requirements for your particular environment by using the `vserver nfs modify` command with the `-permitted-enc-types` parameter.

About this task

For greatest client compatibility, ONTAP supports both weak DES and strong AES encryption by default. This means, for example, that if you want to increase security and your environment supports it, you can use this procedure to disable DES and 3DES and require clients to use only AES encryption.

You should use the strongest encryption available. For ONTAP, that is AES-256. You should confirm with your KDC administrator that this encryption level is supported in your environment.

- Enabling or disabling AES entirely (both AES-128 and AES-256) on SVMs is disruptive because it destroys the original DES principal/keytab file, thereby requiring that the Kerberos configuration be disabled on all LIFs for the SVM.

  Before making this change, you should verify that NFS clients do not rely on AES encryption on the SVM.

- Enabling or disabling DES or 3DES does not require any changes to the Kerberos configuration on LIFs.

Step

1. Enable or disable the permitted encryption type you want:

If you want to enable or disable…	Follow these steps…
DES or 3DES	a. Configure the NFS Kerberos permitted encryption types of the SVM: `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separate multiple encryption types with a comma. b. Verify that the change was successful: `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

If you want to enable or disable…	Follow these steps…

AES-128 or AES-256	a. Identify on which SVM and LIF Kerberos is enabled:
	
	`vserver nfs kerberos interface show`
	
	b. Disable Kerberos on all LIFs on the SVM whose NFS Kerberos permitted encryption type you want to modify:
	
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. Configure the NFS Kerberos permitted encryption types of the SVM:
	
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	Separate multiple encryption types with a comma.
	
	d. Verify that the change was successful:
	
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. Reenable Kerberos on all LIFs on the SVM:
	
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. Verify that Kerberos is enabled on all LIFs:
	
	`vserver nfs kerberos interface show`

Enable Kerberos on a data LIF

You can use the `vserver nfs kerberos interface enable` command to enable Kerberos on a data LIF. This enables the SVM to use Kerberos security services for NFS.

About this task

If you are using an Active Directory KDC, the first 15 characters of any SPNs used must be unique across SVMs within a realm or domain.

Steps

1. Create the NFS Kerberos configuration:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
```

logical_interface -spn *service_principal_name*

ONTAP requires the secret key for the SPN from the KDC to enable the Kerberos interface.

For Microsoft KDCs, the KDC is contacted and a user name and password prompt are issued at the CLI to obtain the secret key. If you need to create the SPN in a different OU of the Kerberos realm, you can specify the optional `-ou` parameter.

For non-Microsoft KDCs, the secret key can be obtained using one of two methods:

If you…	You must also include the following parameter with the command…
Have the KDC administrator credentials to retrieve the key directly from the KDC	`-admin-username` *kdc_admin_username*
Do not have the KDC administrator credentials but have a keytab file from the KDC containing the key	`-keytab-uri` {ftp|http}://*uri*

2. Verify that Kerberos was enabled on the LIF:

   `vserver nfs kerberos-config show`

3. Repeat steps 1 and 2 to enable Kerberos on multiple LIFs.

Example

The following command creates and verifies an NFS Kerberos configuration for the SVM named vs1 on the logical interface ves03-d1, with the SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM in the OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Add storage capacity to an NFS-enabled SVM

Add storage capacity to an NFS-enabled SVM overview

To add storage capacity to an NFS-enabled SVM, you must create a volume or qtree to provide a storage container, and create or modify an export policy for that container. You can then verify NFS client access from the cluster and test access from client systems.

What you'll need

- NFS must be completely set up on the SVM.
- The default export policy of the SVM root volume must contain a rule that permits access to all clients.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to a Kerberos configuration must be complete.

Create an export policy

Before creating export rules, you must create an export policy to hold them. You can use the `vserver export-policy create` command to create an export policy.

Steps

1. Create an export policy:

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   The policy name can be up to 256 characters long.

2. Verify that the export policy was created:

   `vserver export-policy show -policyname` *`policy_name`*

Example

The following commands create and verify the creation of an export policy named exp1 on the SVM named vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Add a rule to an export policy

Without rules, the export policy cannot provide client access to data. To create a new export rule, you must identify clients and select a client match format, select the access and security types, specify an anonymous user ID mapping, select a rule index number, and select the access protocol. You can then use the `vserver export-policy rule create` command to add the new rule to an export policy.

What you'll need

- The export policy you want to add the export rules to must already exist.
- DNS must be correctly configured on the data SVM and DNS servers must have correct entries for NFS clients.

  This is because ONTAP performs DNS lookups using the DNS configuration of the data SVM for certain client match formats, and failures in export policy rule matching can prevent client data access.

- If you are authenticating with Kerberos, you must have determined which of the following security methods is used on your NFS clients:
  - `krb5` (Kerberos V5 protocol)
  - `krb5i` (Kerberos V5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos V5 protocol with privacy service)

About this task

It is not necessary to create a new rule if an existing rule in an export policy covers your client match and access requirements.

If you are authenticating with Kerberos and if all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5`, `krb5i`, or `krb5p`.

Steps

1. Identify the clients and the client match format for the new rule.

   The `-clientmatch` option specifies the clients to which the rule applies. Single or multiple client match values can be specified; specifications of multiple values must be separated by commas. You can specify the match in any of the following formats:

Client match format	Example
Domain name preceded by the "." character	`.example.com` or `.example.com,.example.net,...`
Host name	`host1` or `host1,host2, ...`
IPv4 address	`10.1.12.24` or `10.1.12.24,10.1.12.25, ...`
IPv4 address with a subnet mask expressed as a number of bits	`10.1.12.10/4` or `10.1.12.10/4,10.1.12.11/4,...`
IPv4 address with a network mask	`10.1.16.0/255.255.255.0` or `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
IPv6 address in dotted format	`::1.2.3.4` or `::1.2.3.4,::1.2.3.5,...`

Client match format	Example
IPv6 address with a subnet mask expressed as a number of bits	`ff::00/32` or `ff::00/32,ff::01/32,...`
A single netgroup with the netgroup name preceded by the @ character	`@netgroup1` or `@netgroup1,@netgroup2,...`

You can also combine types of client definitions; for example, `.example.com,@netgroup1`.

When specifying IP addresses, note the following:

- Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed.

  Entries in this format are interpreted as a text string and treated as a host name.

- When specifying individual IP addresses in export rules for granular management of client access, do not specify IP addresses that are dynamically (for example, DHCP) or temporarily (for example, IPv6) assigned.

  Otherwise, the client loses access when its IP address changes.

- Entering an IPv6 address with a network mask, such as ff::12/ff::00, is not allowed.

2. Select the access and security types for client matches.

   You can specify one or more of the following access modes to clients that authenticate with the specified security types:

   - `-rorule` (read-only access)
   - `-rwrule` (read-write access)
   - `-superuser` (root access)

   > A client can only get read-write access for a specific security type if the export rule allows read-only access for that security type as well. If the read-only parameter is more restrictive for a security type than the read-write parameter, the client might not get read-write access. The same is true for superuser access.

   You can specify a comma-separated list of multiple security types for a rule. If you specify the security type as `any` or `never`, do not specify any other security types. Choose from the following valid security types:

When security type is set to…	A matching client can access the exported data…
`any`	Always, regardless of incoming security type.

When security type is set to…	A matching client can access the exported data…
`none`	If listed alone, clients with any security type are granted access as anonymous. If listed with other security types, clients with a specified security type are granted access and clients with any other security type are granted access as anonymous.
`never`	Never, regardless of incoming security type.
`krb5`	If it is authenticated by Kerberos 5. Authentication only: The header of each request and response is signed.
`krb5i`	If it is authenticated by Kerberos 5i. Authentication and integrity: The header and body of each request and response is signed.
`krb5p`	If it is authenticated by Kerberos 5p. Authentication, integrity, and privacy: The header and body of each request and response is signed, and the NFS data payload is encrypted.
`ntlm`	If it is authenticated by CIFS NTLM.
`sys`	If it is authenticated by NFS AUTH_SYS.

The recommended security type is `sys`, or if Kerberos is used, `krb5`, `krb5i`, or `krb5p`.

If you are using Kerberos with NFSv3, the export policy rule must allow `-rorule` and `-rwrule` access to `sys` in addition to `krb5`. This is because of the need to allow Network Lock Manager (NLM) access to the export.

3. Specify an anonymous user ID mapping.

   The `-anon` option specifies a UNIX user ID or user name that is mapped to client requests that arrive with a user ID of 0 (zero), which is typically associated with the user name root. The default value is `65534`. NFS clients typically associate user ID 65534 with the user name nobody (also known as *root squashing*). In ONTAP, this user ID is associated with the user pcuser. To disable access by any client with a user ID of 0, specify a value of `65535`.

4. Select the rule index order.

   The `-ruleindex` option specifies the index number for the rule. Rules are evaluated according to their order in the list of index numbers; rules with lower index numbers are evaluated first. For example, the rule with index number 1 is evaluated before the rule with index number 2.

If you are adding…	Then…
The first rule to an export policy	Enter `1`.
Additional rules to an export policy	a. Display existing rules in the policy: `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Select an index number for the new rule depending on the order it should be evaluated.

5. Select the applicable NFS access value: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` matches any version, `nfs3` and `nfs4` match only those specific versions.

6. Create the export rule and add it to an existing export policy:

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {nfs|nfs3|nfs4} -clientmatch { text |` *`"text,text,…"`* `} -rorule` *`security_type`* `-rwrule` *`security_type`* `-superuser` *`security_type`* `-anon` *`user_ID`*

7. Display the rules for the export policy to verify that the new rule is present:

   `vserver export-policy rule show -policyname` *`policy_name`*

   The command displays a summary for that export policy, including a list of rules applied to that policy. ONTAP assigns each rule a rule index number. After you know the rule index number, you can use it to display detailed information about the specified export rule.

8. Verify that the rules applied to the export policy are configured correctly:

   `vserver export-policy rule show -policyname` *`policy_name`* `-vserver` *`vserver_name`* `-ruleindex` *`integer`*

Examples

The following commands create and verify the creation of an export rule on the SVM named vs1 in an export policy named rs1. The rule has the index number 1. The rule matches any client in the domain eng.company.com and the netgroup @netgroup1. The rule enables all NFS access. It enables read-only and read-write access to users that authenticated with AUTH_SYS. Clients with the UNIX user ID 0 (zero) are anonymized unless authenticated with Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon 65534
-superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                           RO Access Rule: sys
                           RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                 Superuser Security Types: krb5
             Honor SetUID Bits in SETATTR: true
                Allow Creation of Devices: true
```

The following commands create and verify the creation of an export rule on the SVM named vs2 in an export policy named expol2. The rule has the index number 21. The rule matches clients to members of the netgroup dev_netgroup_main. The rule enables all NFS access. It enables read-only access for users that authenticated with AUTH_SYS and requires Kerberos authentication for read-write and root access. Clients with the UNIX user ID 0 (zero) are denied root access unless authenticated with Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Create a volume or qtree storage container

Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

What you'll need

The SVM security style must be UNIX, and NFS should be set up and running.

About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

Steps

1. Create the volume with a junction point:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user
   ```

user_name_or_number -group *group_name_or_number* -junction-path *junction_path* [-policy *export_policy_name*]

The choices for `-junction-path` are the following:

- Directly under root, for example, */new_vol*

  You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, */existing_dir/new_vol*

  You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, */new_dir/new_vol*, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

+
If you plan to use an existing export policy, you can specify it when you create the volume. You can also add an export policy later with the `volume modify` command.

2. Verify that the volume was created with the desired junction point:

   `volume show -vserver` *vserver_name* `-volume` *volume_name* `-junction`

Examples

The following command creates a new volume named users1 on the SVM vs1.example.com and the aggregate aggr1. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type volume (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

The following command creates a new volume named "home4" on the SVM "vs1.example.com" and the aggregate "aggr1". The directory `/eng/` already exists in the namespace for the vs1 SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Create a qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

What you'll need

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be UNIX, and NFS should be set up and running.

Steps

1. Create the qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/`*`volume_name/_qtree_name`*.

   By default, qtrees inherit the export policies of their parent volume, but they can be configured to use their own. If you plan to use an existing export policy, you can specify it when you create the qtree. You can also add an export policy later with the `volume qtree modify` command.

2. Verify that the qtree was created with the desired junction path:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Example

The following example creates a qtree named qt01 located on SVM vs1.example.com that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Secure NFS access using export policies

Secure NFS access using export policies

You can use export policies to restrict NFS access to volumes or qtrees to clients that match specific parameters. When provisioning new storage, you can use an existing policy and rules, add rules to an existing policy, or create a new policy and rules. You can also check the configuration of export policies

Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy.The commands only validate export configuration for host names, netgroups, and anonymous users.

Manage the processing order of export rules

You can use the `vserver export-policy rule setindex` command to manually set an existing export rule's index number. This enables you to specify the precedence by which ONTAP applies export rules to client requests.

About this task

If the new index number is already in use, the command inserts the rule at the specified spot and reorders the list accordingly.

Step

1. Modify the index number of a specified export rule:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname
policy_name -ruleindex integer -newruleindex integer
```

Example

The following command changes the index number of an export rule at index number 3 to index number 2 in an export policy named rs1 on the SVM named vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Assign an export policy to a volume

Each volume contained in the SVM must be associated with an export policy that contains export rules for clients to access data in the volume.

About this task

You can associate an export policy to a volume when you create the volume or at any time after you create the volume. You can associate one export policy to the volume, although one policy can be associated to many volumes.

Steps

1. If an export policy was not specified when the volume was created, assign an export policy to the volume:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Verify that the policy was assigned to the volume:

   ```
   volume show -volume volume_name -fields policy
   ```

Example

The following commands assign the export policy nfs_policy to the volume vol1 on the SVM vs1 and verify the assignment:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Assign an export policy to a qtree

Instead of exporting an entire volume, you can also export a specific qtree on a volume to make it directly accessible to clients. You can export a qtree by assigning an export policy to it. You can assign the export policy either when you create a new qtree or by modifying an existing qtree.

What you'll need

The export policy must exist.

About this task

By default, qtrees inherit the parent export policy of the containing volume if not otherwise specified at the time of creation.

You can associate an export policy to a qtree when you create the qtree or at any time after you create the qtree. You can associate one export policy to the qtree, although one policy can be associated with many qtrees.

Steps

1. If an export policy was not specified when the qtree was created, assign an export policy to the qtree:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Verify that the policy was assigned to the qtree:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Example

The following commands assign the export policy nfs_policy to the qtree qt1 on the SVM vs1 and verify the assignment:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verify NFS client access from the cluster

You can give select clients access to the share by setting UNIX file permissions on a UNIX administration host. You can check client access by using the `vserver export-policy check-access` command, adjusting the export rules as necessary.

Steps

1. On the cluster, check client access to exports by using the `vserver export-policy check-access` command.

   The following command checks read/write access for an NFSv3 client with the IP address 1.2.3.4 to the volume home2. The command output shows that the volume uses the export policy `exp-home-dir` and that access is denied.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                        Policy    Policy     Rule
Path                    Policy          Owner     Owner Type Index  Access
----------------------- --------------- --------- ---------- ------
----------
/                       default         vs1_root  volume          1 read
/eng                    default         vs1_root  volume          1 read
/eng/home2              exp-home-dir    home2     volume          1 denied

3 entries were displayed.
```

2. Examine the output to determine whether the export policy works as intended and the client access behaves as expected.

   Specifically, you should verify which export policy is used by the volume or qtree and the type of access the client has as a result.

3. If necessary, reconfigure the export policy rules.

Test NFS access from client systems

After you verify NFS access to the new storage object, you should test the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM. You should then repeat the process as a non-root user on a client system.

What you'll need

- 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. On the cluster, verify the IP address of the LIF that is hosting the new volume:

   ```
   network interface show –vserver svm_name
   ```

2. Log in as the root user to the administration host client system.
3. Change the directory to the mount folder:

   ```
   cd /mnt/
   ```

4. Create and mount a new folder using the IP address of the SVM:
   a. Create a new folder:

      ```
      mkdir /mnt/folder
      ```

   b. Mount the new volume at this new directory:

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. Change the directory to the new folder:

```
cd 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 hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Create a new file, verify that it exists, and write text to it:

a. Create a test file:

```
touch filename
```

b. Verify that the file exists.:

```
ls -l filename
```

c. Enter:

```
cat > filename
```

Type some text, and then press Ctrl+D to write text to the test file.

d. Display the content of the test file.

```
cat filename
```

e. Remove the test file:

```
rm filename
```

f. Return to the parent directory:

```
cd ..
```

```
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 ..
```

6. As root, set any desired UNIX ownership and permissions on the mounted volume.
7. On a UNIX client system identified in your export rules, log in as one of the authorized users who now has access to the new volume, and repeat the procedures in steps 3 to 5 to verify that you can mount the volume and create a file.

Where to find additional information

After you have successfully tested NFS client access, you can perform additional NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of storage virtual machine (SVM).

NFS configuration

You can further configure NFS access using the following information and technical reports:

- NFS management

  Describes how to configure and manage file access using NFS.

- NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

  Serves as an NFSv3 and NFSv4 operational guide, and provides an overview of the ONTAP operating system with a focus on NFSv4.

- NetApp Technical Report 4073: Secure Unified Authentication

  Explains how to configure ONTAP for use with UNIX-based Kerberos version 5 (krb5) servers for NFS storage authentication and Windows Server Active Directory (AD) as the KDC and Lightweight Directory Access Protocol (LDAP) identity provider.

- NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

  Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

Networking configuration

You can further configure networking features and name services using the following informati and technical reports:

- NFS management

  Describes how to configure and manage ONTAP networking.

- NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations

  Describes the implementation of ONTAP network configurations, and provides common network deployment scenarios and best practice recommendations.

- NetApp Technical Report 4668: Name Services Best Practices Guide

Explains how to configure LDAP, NIS, DNS, and local file configuration for authentication purposes.

SAN protocol configuration

If you want to provide or modify SAN access to the new SVM, you can use the FC or iSCSI configuration information, which is available for multiple host operating systems.

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

  Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

How ONTAP exports differ from 7-Mode exports

How ONTAP exports differ from 7-Mode exports

If you are unfamiliar with how ONTAP implements NFS exports, you can compare 7-Mode and ONTAP export configuration tools, as well as sample 7-Mode `/etc/exports` files with clustered policies and rules.

In ONTAP there is no `/etc/exports` file and no `exportfs` command. Instead, you must define an export policy. Export policies enable you to control client access in much the same way as you did in 7-Mode, but give you additional functionality such as the ability to reuse the same export policy for multiple volumes.

Related information

NFS management

NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

Comparison of exports in 7-Mode and ONTAP

Exports in ONTAP are defined and used differently than they are in 7-Mode environments.

Areas of difference	7-Mode	ONTAP
How exports are defined	Exports are defined in the `/etc/exports` file.	Exports are defined by creating an export policy within an SVM. An SVM can include more than one export policy.

Scope of export	• Exports apply to a specified file path or qtree. • You must create a separate entry in `/etc/exports` for each file path or qtree. • Exports are persistent only if they are defined in the `/etc/exports` file.	• Export policies apply to an entire volume, including all of the file paths and qtrees contained in the volume. • Export policies can be applied to more than one volume if you want. • All export policies are persistent across system restarts.
Fencing (specifying different access for specific clients to the same resources)	To provide specific clients different access to a single exported resource, you have to list each client and its permitted access in the `/etc/exports` file.	Export policies are composed of a number of individual export rules. Each export rule defines specific access permissions for a resource and lists the clients that have those permissions. To specify different access for specific clients, you have to create an export rule for each specific set of access permissions, list the clients that have those permissions, and then add the rules to the export policy.
Name aliasing	When you define an export, you can choose to make the name of the export different from the name of the file path. You should use the `-actual` parameter when defining such an export in the `/etc/exports` file.	You can choose to make the name of the exported volume different from the actual volume name. To do this, you must mount the volume with a custom junction path name within the SVM namespace. By default, volumes are mounted with their volume name. To customize a volume's junction path name you need to unmount it, rename it, and then remount it.

Examples of ONTAP export policies

You can review example export policies to better understand how export policies work in ONTAP.

Sample ONTAP implementation of a 7-Mode export

The following example shows a 7-Mode export as it appears in the `/etc/export` file:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

To reproduce this export as a clustered export policy, you have to create an export policy with three export rules, and then assign the export policy to the volume vol1.

Rule	Element	Value
Rule 1	`-clientmatch` (client specification)	`@readonly_netgroup`
	`-ruleindex`(position of export rule in the list of rules)	`1`
	`-protocol`	`nfs`
	`-rorule`(allow read-only access)	`sys` (client authenticated with AUTH_SYS)
	`-rwrule`(allow read-write access)	`never`
	`-superuser`(allow superuser access)	`none`(root *squashed* to anon)
Rule 2	`-clientmatch`	`@rootaccess_netgroup`
	`-ruleindex`	`2`
	`-protocol`	`nfs`
	`-rorule`	`sys`
	`-rwrule`	`sys`
	`-superuser`	`sys`

Rule	Element	Value
Rule 3	-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2
	-ruleindex	3
	-protocol	nfs
	-rorule	sys
	-rwrule	sys
	-superuser	none

1. Create an export policy called exp_vol1:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Create three rules with the following parameters to the base command:
   - Base command:

     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```

   - Rule parameters:

     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none

     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     -rwrule sys -superuser sys

     -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
     -protocol nfs -rorule sys -rwrule sys -superuser none
     ```

3. Assign the policy to the volume vol1:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Sample consolidation of 7-Mode exports

The following example shows a 7-Mode `/etc/export` file that includes one line for each of 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP, one of two policies is needed for each qtree: one with a rule including `-clientmatch host1519s`, or one with a rule including `-clientmatch host2057s`.

1. Create two export policies called exp_vol1q1 and exp_vol1q2:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Create a rule for each policy:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Apply the policies to the qtrees:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [next 4 qtrees…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [next 4 qtrees…]

If you need to add additional qtrees for those hosts later, you would use the same export policies.

Manage NFS with the CLI

NFS reference overview

ONTAP includes file access features available for the NFS protocol. You can enable an NFS server and export volumes or qtrees.

You perform these procedure under the following circumstances:

- You want to understand the range of ONTAP NFS protocol capabilities.
- You want to perform less common configuration and maintenance tasks, not basic NFS configuration.

- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

Understand NAS file access

Namespaces and junction points

Namespaces and junction points overview

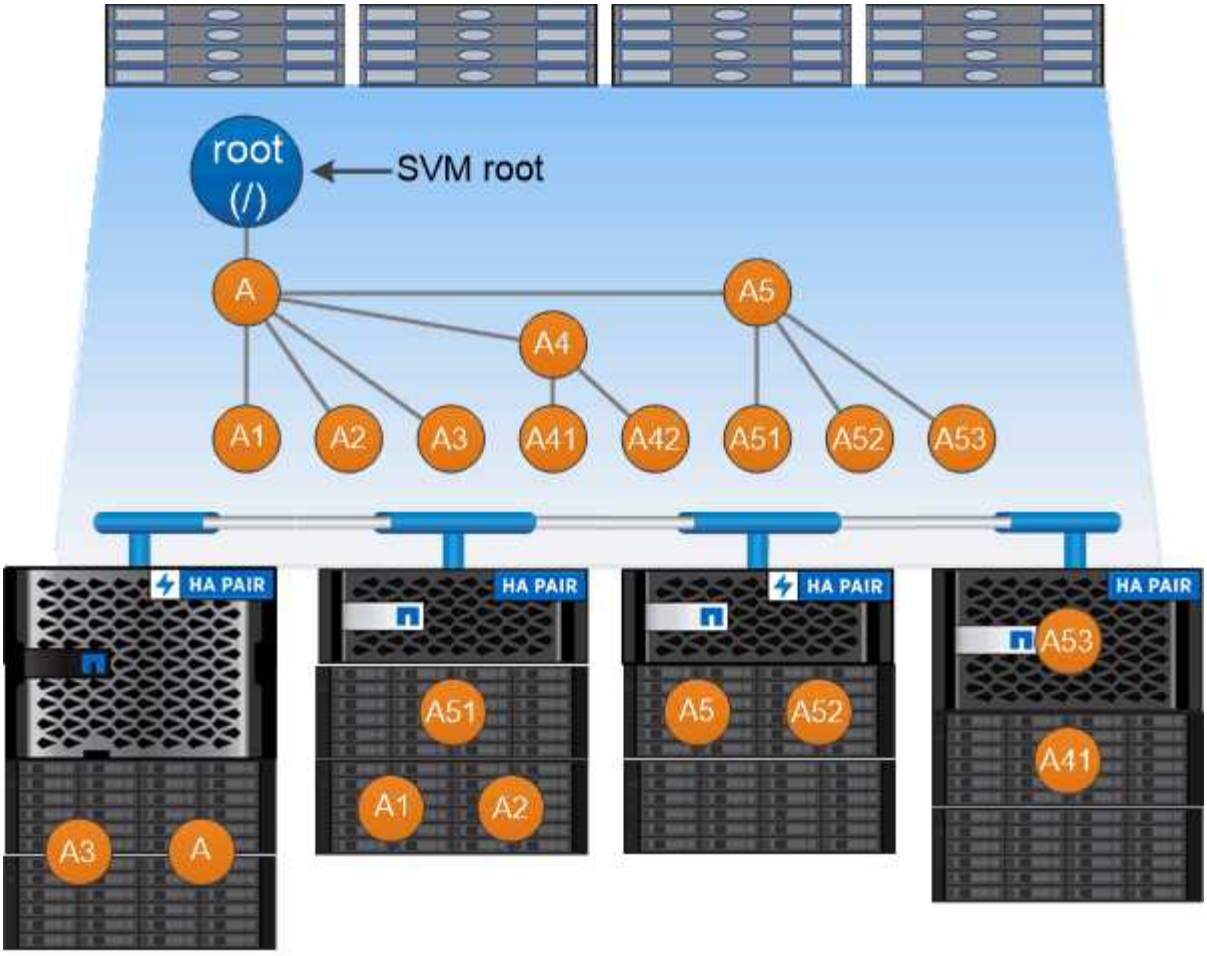
A NAS *namespace* is a logical grouping of volumes joined together at *junction points* to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the cluster.

Rather than mounting every volume containing a file of interest, NAS clients mount an NFS *export* or access an SMB *share.* The export or share represents the entire namespace or an intermediate location within the namespace. The client accesses only the volumes mounted below its access point.

You can add volumes to the namespace as needed. You can create junction points directly below a parent volume junction or on a directory within a volume. A path to a volume junction for a volume named “vol3” might be `/vol1/vol2/vol3`, or `/vol1/dir2/vol3`, or even `/dir1/dir2/vol3`. The path is called the *junction path.*

Every SVM has a unique namespace. The SVM root volume is the entry point to the namespace hierarchy.

To ensure that data remains available in the event of a node outage or failover, you should create a *load-sharing mirror* copy for the SVM root volume.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Example

The following example creates a volume named “home4” located on SVM vs1 that has a junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

What the typical NAS namespace architectures are

There are several typical NAS namespace architectures that you can use as you create your SVM name space. You can choose the namespace architecture that matches your business and workflow needs.

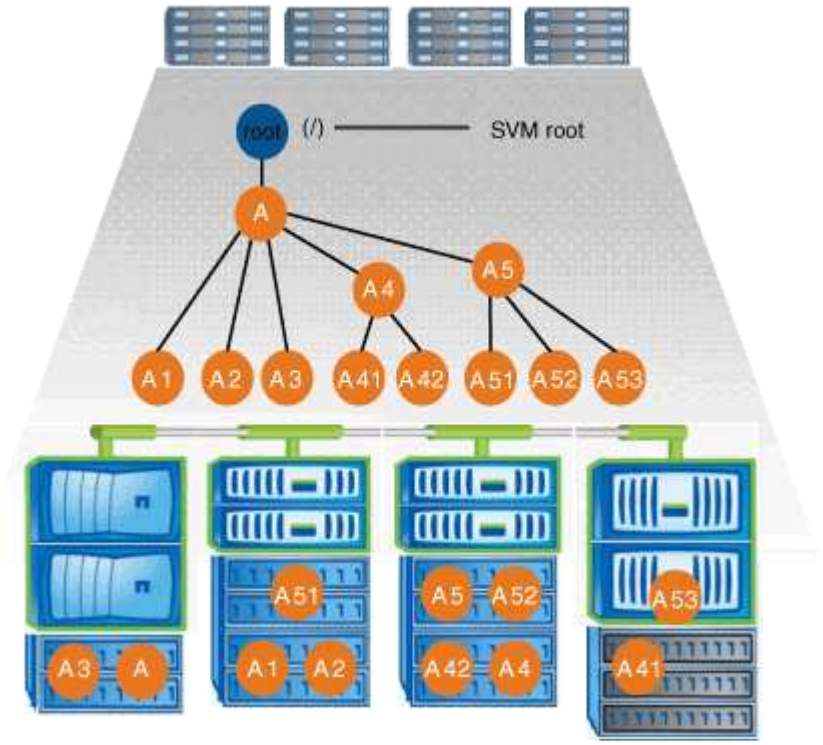
The top of the namespace is always the root volume, which is represented by a slash (/). The namespace architecture under the root falls into three basic categories:

- A single branched tree, with only a single junction to the root of the namespace

- Multiple branched trees, with multiple junction points to the root of the namespace
- Multiple stand-alone volumes, each with a separate junction point to the root of the name space

Namespace with single branched tree

An architecture with a single branched tree has a single insertion point to the root of the SVM namespace. The single insertion point can be either a junctioned volume or a directory beneath the root. All other volumes are mounted at junction points beneath the single insertion point (which can be a volume or a directory).

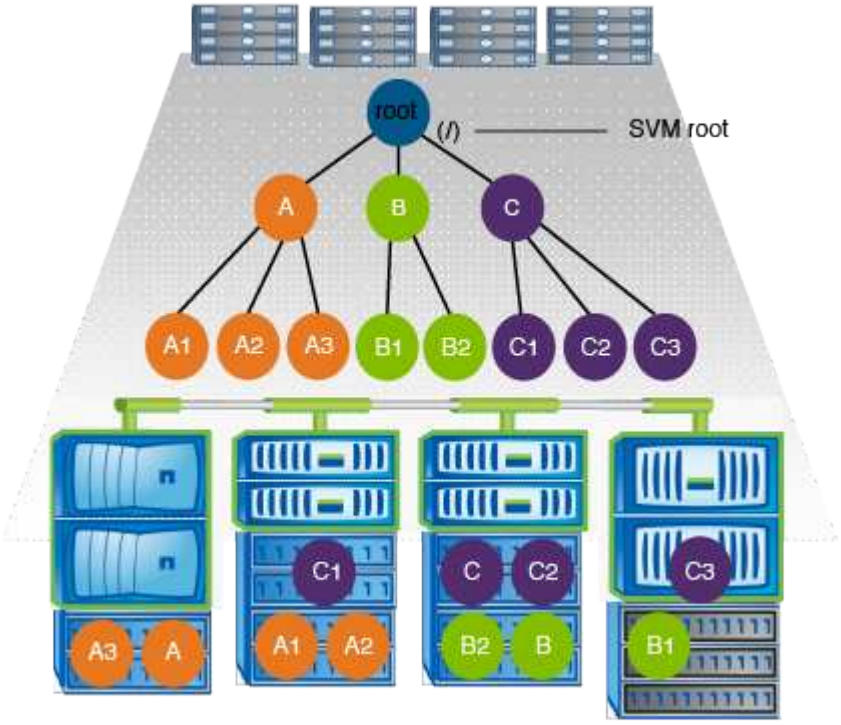


For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where all volumes are junctioned below the single insertion point, which is a directory named “data”:

```
                 Junction                        Junction
Vserver Volume   Active   Junction Path          Path Source
------- -------- -------- --------------------   -----------
vs1     corp1    true     /data/dir1/corp1       RW_volume
vs1     corp2    true     /data/dir1/corp2       RW_volume
vs1     data1    true     /data/data1            RW_volume
vs1     eng1     true     /data/data1/eng1       RW_volume
vs1     eng2     true     /data/data1/eng2       RW_volume
vs1     sales    true     /data/data1/sales      RW_volume
vs1     vol1     true     /data/vol1             RW_volume
vs1     vol2     true     /data/vol2             RW_volume
vs1     vol3     true     /data/vol3             RW_volume
vs1     vs1_root -        /                      -
```

Namespace with multiple branched trees

An architecture with multiple branched trees has multiple insertion points to the root of the SVM namespace. The insertion points can be either junctioned volumes or directories beneath the root. All other volumes are mounted at junction points beneath the insertion points (which can be volumes or directories).



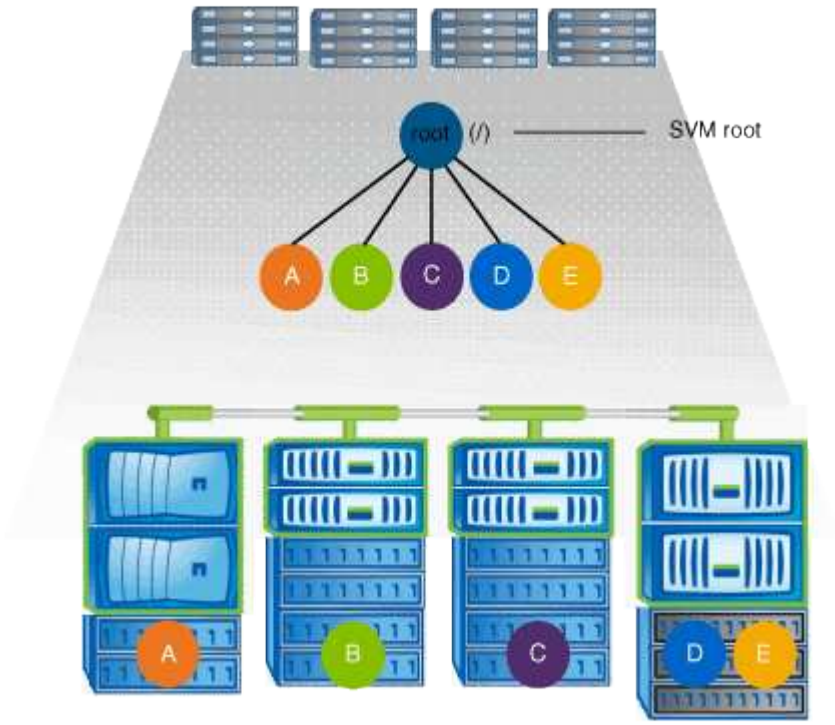
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are three insertion points to the root volume of the SVM. Two insertion points are directories named “data” and “projects”. One insertion point is a junctioned volume named “audit”:

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Namespace with multiple stand-alone volumes

In an architecture with stand-alone volumes, every volume has an insertion point to the root of the SVM namespace; however, the volume is not junctioned below another volume. Each volume has a unique path,

and is either junctioned directly below the root or is junctioned under a directory below the root.



For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are five insertion points to the root volume of the SVM, with each insertion point representing a path to one volume.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

How ONTAP controls access to files

How ONTAP controls access to files overview

ONTAP controls access to files according to the authentication-based and file-based restrictions that you specify.

When a client connects to the storage system to access files, ONTAP has to perform two tasks:

- Authentication

  ONTAP has to authenticate the client by verifying the identity with a trusted source. In addition, the

authentication type of the client is one method that can be used to determine whether a client can access data when configuring export policies (optional for CIFS).

- Authorization

  ONTAP has to authorize the user by comparing the user's credentials with the permissions configured on the file or directory and determining what type of access, if any, to provide.

To properly manage file access control, ONTAP must communicate with external services such as NIS, LDAP, and Active Directory servers. Configuring a storage system for file access using CIFS or NFS requires setting up the appropriate services depending on your environment in ONTAP.

Authentication-based restrictions

With authentication-based restrictions, you can specify which client machines and which users can connect to the storage virtual machine (SVM).

ONTAP supports Kerberos authentication from both UNIX and Windows servers.

File-based restrictions

ONTAP evaluates three levels of security to determine whether an entity is authorized to perform a requested action on files and directories residing on an SVM. Access is determined by the effective permissions after evaluation of the three security levels.

Any storage object can contain up to three types of security layers:

- Export (NFS) and share (SMB) security

  Export and share security applies to client access to a given NFS export or SMB share. Users with administrative privileges can manage export and share-level security from SMB and NFS clients.

- Storage-Level Access Guard file and directory security

  Storage-Level Access Guard security applies to SMB and NFS client access to SVM volumes. Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map to a Windows user on the SVM that owns the volume.

  > If you view the security settings on a file or directory from an NFS or SMB client, you will not see Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

- NTFS, UNIX, and NFSv4 native file-level security

  Native file-level security exists on the file or directory that represents the storage object. You can set file-level security from a client. File permissions are effective regardless of whether SMB or NFS is used to access the data.

How ONTAP handles NFS client authentication

How ONTAP handles NFS client authentication overview

NFS clients must be properly authenticated before they can access data on the SVM. ONTAP authenticates the clients by checking their UNIX credentials against the name services that you configure.

When an NFS client connects to the SVM, ONTAP obtains the UNIX credentials for the user by checking different name services, depending on the name services configuration of the SVM. ONTAP can check credentials for local UNIX accounts, NIS domains, and LDAP domains. At least one of them must be configured so that ONTAP can successfully authenticate the user. You can specify multiple name services and the order in which ONTAP searches them.

In a pure NFS environment with UNIX volume security styles, this configuration is sufficient to authenticate and provide the proper file access for a user connecting from an NFS client.

If you are using mixed, NTFS, or unified volume security styles, ONTAP must obtain a SMB user name for the UNIX user for authentication with a Windows domain controller. This can happen either by mapping individual users using local UNIX accounts or LDAP domains, or by using a default SMB user instead. You can specify which name services ONTAP searches in which order, or specify a default SMB user.

How ONTAP uses name services

ONTAP uses name services to obtain information about users and clients. ONTAP uses this information to authenticate users accessing data on or administering the storage system, and to map user credentials in a mixed environment.

When you configure the storage system, you must specify what name services you want ONTAP to use for obtaining user credentials for authentication. ONTAP supports the following name services:

- Local users (file)
- External NIS domains (NIS)
- External LDAP domains (LDAP)

You use the `vserver services name-service ns-switch` command family to configure SVMs with the sources to search for network information and the order in which to search them. These commands provide the equivalent functionality of the `/etc/nsswitch.conf` file on UNIX systems.

When an NFS client connects to the SVM, ONTAP checks the specified name services to obtain the UNIX credentials for the user. If name services are configured correctly and ONTAP can obtain the UNIX credentials, ONTAP successfully authenticates the user.

In an environment with mixed security styles, ONTAP might have to map user credentials. You must configure name services appropriately for your environment to allow ONTAP to properly map user credentials.

ONTAP also uses name services for authenticating SVM administrator accounts. You must keep this in mind when configuring or modifying the name service switch to avoid accidentally disabling authentication for SVM administrator accounts. For more information about SVM administration users, see xref:./nfs-admin/../authentication/index.html[Administrator authentication and RBAC.

How ONTAP grants SMB file access from NFS clients

ONTAP uses Windows NT File System (NTFS) security semantics to determine whether a UNIX user, on an NFS client, has access to a file with NTFS permissions.

ONTAP does this by converting the user's UNIX User ID (UID) into a SMB credential, and then using the SMB credential to verify that the user has access rights to the file. A SMB credential consists of a primary Security Identifier (SID), usually the user's Windows user name, and one or more group SIDs that correspond to Windows groups of which the user is a member.

The time ONTAP takes converting the UNIX UID into a SMB credential can be from tens of milliseconds to hundreds of milliseconds because the process involves contacting a domain controller. ONTAP maps the UID to the SMB credential and enters the mapping in a credential cache to reduce the verification time caused by the conversion.

How the NFS credential cache works

When an NFS user requests access to NFS exports on the storage system, ONTAP must retrieve the user credentials either from external name servers or from local files to authenticate the user. ONTAP then stores these credentials in an internal credential cache for later reference. Understanding how the NFS credential caches works enables you to handle potential performance and access issues.

Without the credential cache, ONTAP would have to query name services every time an NFS user requested access. On a busy storage system that is accessed by many users, this can quickly lead to serious performance problems, causing unwanted delays or even denials to NFS client access.

With the credential cache, ONTAP retrieves the user credentials and then stores them for a predetermined amount of time for quick and easy access should the NFS client send another request. This method offers the following advantages:

- It eases the load on the storage system by handling fewer requests to external name servers (such as NIS or LDAP).
- It eases the load on external name servers by sending fewer requests to them.
- It speeds up user access by eliminating the wait time for obtaining credentials from external sources before the user can be authenticated.

ONTAP stores both positive and negative credentials in the credential cache. Positive credentials means that the user was authenticated and granted access. Negative credentials means that the user was not authenticated and was denied access.

By default, ONTAP stores positive credentials for 24 hours; that is, after initially authenticating a user, ONTAP uses the cached credentials for any access requests by that user for 24 hours. If the user requests access after 24 hours, the cycle starts over: ONTAP discards the cached credentials and obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous 24 hours, ONTAP caches the updated credentials for use for the next 24 hours.

By default, ONTAP stores negative credentials for two hours; that is, after initially denying access to a user, ONTAP continues to deny any access requests by that user for two hours. If the user requests access after 2 hours, the cycle starts over: ONTAP obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous two hours, ONTAP caches the updated credentials for use for the next two hours.

Create and manage data volumes in NAS namespaces

Create data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

What you'll need

The aggregate in which you want to create the volume must already exist.

> The following characters cannot be used in the junction path: * # " > < | ? \
>
> In addition, the junction path length cannot be more than 255 characters.

Steps

1. Create the volume with a junction point:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed} -junction-path junction_path
   ```

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   The junction path is case insensitive; `/ENG` is the same as `/eng`. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is `/ENG`, the path of a SMB share must start with `/ENG`, not `/eng`.

   There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created with the desired junction point:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Example

The following example creates a volume named "home4" located on SVM vs1 that has a junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Create data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

What you'll need

The aggregate in which you want to create the volume must already exist.

Steps

1. Create the volume without a junction point by using the following command:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Example

The following example creates a volume named "sales" located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Mount or unmount existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount and offline a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume's namespace, are inaccessible to NAS clients.

> To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must offline the volume, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article:
>
> NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP

When you unmount and offline a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

If you want to…	Enter the commands…
Mount a volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`
Unmount a volume	`volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name`

2. Verify that the volume is in the desired mount state:

```
volume show -vserver vserver_name -volume volume_name -fields state,junction-
path,junction-active
```

Examples

The following example mounts a volume named “sales” located on SVM vs1 to the junction point `/sales`:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

The following example unmounts and offlines a volume named “data” located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Display volume mount and junction point information

You can display information about mounted volumes for storage virtual machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

Step

1. Perform the desired action:

If you want to display…	Enter the command…

Summary information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -junction`
Detailed information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Specific information about mounted and unmounted volumes on the SVM	a. If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?` b. Display the desired information by using the `-fields` parameter: `volume show -vserver vserver_name -fields fieldname,…`

Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configure security styles

How security styles affect data access

What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
Unix	NFS	NFSv3 mode bits	Unix	NFS and SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.ACLs		
		NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		
		NTFS ACLs	NTFS	

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see FlexGroup volumes management overview.

Beginning with ONTAP 9.2, the `show-effective-permissions` parameter to the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission.

ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Decide which security style to use on SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to

ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if…
UNIX	• The file system is managed by a UNIX administrator. • The majority of users are NFS clients. • An application accessing the data uses a UNIX user as the service account.
NTFS	• The file system is managed by a Windows administrator. • The majority of users are SMB clients. • An application accessing the data uses a Windows user as the service account.
Mixed	• The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Configure security styles on SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

   The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created:

   `vserver show -vserver` *`vserver_name`*

Configure security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If the FlexVol volume…	Use the command…
Does not yet exist	`volume create` and include the `-security-style` parameter to specify the security style.

Already exists	`volume modify` and include the `-security-style` parameter to specify the security style.

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

Configure security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:

If the qtree…	Use the command…
Does not exist yet	`volume qtree create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume qtree modify` and include the `-security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree` *`qtree_name`* `-instance`

Set up file access using NFS

Set up file access using NFS overview

You must complete a number of steps to allow clients access to files on storage virtual machines (SVMs) using NFS. There are some additional steps that are optional depending on the current configuration of your environment.

For clients to be able to access files on SVMs using NFS, you must complete the following tasks:

1. Enable the NFS protocol on the SVM.

   You must configure the SVM to allow data access from clients over NFS.

2. Create an NFS server on the SVM.

   An NFS server is a logical entity on the SVM that enables the SVM to serve files over NFS. You must create the NFS server and specify the NFS protocol versions you want to allow.

3. Configure export policies on the SVM.

   You must configure export policies to make volumes and qtrees available to clients.

4. Configure the NFS server with the appropriate security and other settings depending on the network and storage environment.

   This step might include configuring Kerberos, LDAP, NIS, name mappings, and local users.

Secure NFS access using export policies

How export policies control client access to volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the storage virtual machine (SVM) for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running ONTAP.

Default export policy for SVMs

Each SVM has a default export policy that contains no rules. An export policy with rules must exist before clients can access data on the SVM. Each FlexVol volume contained in the SVM must be associated with an export policy.

When you create an SVM, the storage system automatically creates a default export policy called `default` for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM. Alternatively, you can create a custom export policy with rules. You can modify and

rename the default export policy, but you cannot delete the default export policy.

When you create a FlexVol volume in its containing SVM, the storage system creates the volume and associates the volume with the default export policy for the root volume of the SVM. By default, each volume created in the SVM is associated with the default export policy for the root volume. You can use the default export policy for all volumes contained in the SVM, or you can create a unique export policy for each volume. You can associate multiple volumes with the same export policy.

How export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.

  The maximum size for the `-clientmatch` field is 4096 characters.

- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.

> Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy.
>
> The commands only validate export configuration for host names, netgroups, and anonymous users.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

Manage clients with an unlisted security type

When a client presents itself with a security type that is not listed in an access parameter of an export rule, you have the choice of either denying access to the client or mapping it to the anonymous user ID instead by using the option `none` in the access parameter.

A client might present itself with a security type that is not listed in an access parameter because it was authenticated with a different security type or was not authenticated at all (security type AUTH_NONE). By default, the client is automatically denied access to that level. However, you can add the option `none` to the access parameter. As a result, clients with an unlisted security style are mapped to the anonymous user ID instead. The `-anon` parameter determines what user ID is assigned to those clients. The user ID specified for the `-anon` parameter must be a valid user that is configured with permissions you deem appropriate for the anonymous user.

Valid values for the `-anon` parameter range from `0` to `65535`.

User ID assigned to `-anon`	Resulting handling of client access requests
`0 - 65533`	The client access request is mapped to the anonymous user ID and gets access depending on the permissions configured for this user.
`65534`	The client access request is mapped to the user nobody and gets access depending on the permissions configured for this user. This is the default.
`65535`	The access request from any client is denied when mapped to this ID and the client presents itself with security type AUTH_NONE. The access request from clients with user ID 0 is denied when mapped to this ID and the client presents itself with any other security type.

When using the option `none`, it is important to remember that the read-only parameter is processed first. Consider the following guidelines when configuring export rules for clients with unlisted security types:

Read-only includes `none`	Read-write includes `none`	Resulting access for clients with unlisted security types
No	No	Denied
No	Yes	Denied because read-only is processed first
Yes	No	Read-only as anonymous
Yes	Yes	Read-write as anonymous

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access to any security type, but in this case only applies to clients already filtered by the read-only rule.

Therefore, clients #1 and #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-write access with its own user ID.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access only as the anonymous user.

Therefore, client #1 and client #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-only access with its own user ID but is denied read-write access.

How security types determine client access levels

The security type that the client authenticated with plays a special role in export rules. You must understand how the security type determines the levels of access the client gets to a volume or qtree.

The three possible access levels are as follows:

1. Read-only
2. Read-write
3. Superuser (for clients with user ID 0)

Because the access level by security type is evaluated in this order, you must observe the following rules when

constructing access level parameters in export rules:

For a client to get access level…	These access parameters must match the client's security type…
Normal user read-only	Read-only (`-rorule`)
Normal user read-write	Read-only (`-rorule`) and read-write (`-rwrule`)
Superuser read-only	Read-only (`-rorule`) and `-superuser`
Superuser read-write	Read-only (`-rorule`) and read-write (`-rwrule`) and `-superuser`

The following are valid security types for each of these three access parameters:

- `any`
- `none`
- `never`

  This security type is not valid for use with the `-superuser` parameter.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

When matching a client's security type against each of the three access parameters, there are three possible outcomes:

If the client's security type…	Then the client…
Matches the one specified in the access parameter.	Gets access for that level with its own user ID.
Does not match the one specified, but the access parameter includes the option `none`.	Gets access for that level but as the anonymous user with the user ID specified by the `-anon` parameter.
Does not match the one specified and the access parameter does not include the option `none`.	Does not get any access for that level.This does not apply to the `-superuser` parameter because it always includes `none` even when not specified.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, has user ID 0, sends an access request using the NFSv3 protocol, and did not authenticate (AUTH_NONE).

The client access protocol and IP address matches all three clients. The read-only parameter allows read-only access to all clients regardless of security type. The read-write parameter allows read-write access to clients with their own user ID that authenticated with AUTH_SYS or Kerberos v5. The superuser parameter allows superuser access to clients with user ID 0 that authenticated with Kerberos v5.

Therefore, client #1 gets superuser read-write access because it matches all three access parameters. Client #2 gets read-write access but not superuser access. Client #3 gets read-only access but not superuser access.

Manage superuser access requests

When you configure export policies, you need to consider what you want to happen if the storage system receives a client access request with user ID 0, meaning as a superuser, and set up your export rules accordingly.

In the UNIX world, a user with the user ID 0 is known as the superuser, typically called root, who has unlimited access rights on a system. Using superuser privileges can be dangerous for several reasons, including breach of system and data security.

By default, ONTAP maps clients presenting with user ID 0 to the anonymous user. However, you can specify the `-superuser` parameter in export rules to determine how to handle clients presenting with user ID 0 depending on their security type. The following are valid options for the `-superuser` parameter:

- `any`
- `none`

  This is the default setting if you do not specify the `-superuser` parameter.

- `krb5`
- `ntlm`
- `sys`

There are two different ways how clients presenting with user ID 0 are handled, depending on the `-superuser` parameter configuration:

If the `-superuser` parameter and the client's security type…	Then the client…
Match	Gets superuser access with user ID 0.
Do not match	Gets access as the anonymous user with the user ID specified by the `-anon` parameter and its assigned permissions. This is regardless of whether the read-only or read-write parameter specifies the option `none`.

If a client presents with user ID 0 to access a volume with NTFS security style and the `-superuser` parameter is set to `none`, ONTAP uses the name mapping for the anonymous user to obtain the proper credentials.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 has the IP address 10.1.16.207, has user ID 746, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate.

Client #2 does not get superuser access. Instead, it gets mapped to anonymous because the `-superuser` parameter is not specified. This means it defaults to `none` and automatically maps user ID 0 to anonymous. Client #2 also only gets read-only access because its security type did not match the read-write parameter.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

The export rule allows superuser access for clients with user ID 0. Client #1 gets superuser access because it matches the user ID and security type for the read-only and `-superuser` parameters. Client #2 does not get read-write or superuser access because its security type does not match the read-write parameter or the `-superuser` parameter. Instead, client #2 is mapped to the anonymous user, which in this case has the user ID 0.

How ONTAP uses export policy caches

To improve system performance, ONTAP uses local caches to store information such as host names and netgroups. This enables ONTAP to process export policy rules more quickly than retrieving the information from external sources. Understanding what the caches are and what they do can help you troubleshoot client access issues.

You configure export policies to control client access to NFS exports. Each export policy contains rules, and each rule contains parameters to match the rule to clients requesting access. Some of these parameters require ONTAP to contact an external source, such as DNS or NIS servers, to resolve objects such as domain names, host names, or netgroups.

These communications with external sources take a small amount of time. To increase performance, ONTAP reduces the amount of time it takes to resolve export policy rule objects by storing information locally on each node in several caches.

Cache name	Type of information stored
Access	Mappings of clients to corresponding export policies
Name	Mappings of UNIX user names to corresponding UNIX user IDs
ID	Mappings of UNIX user IDs to corresponding UNIX user IDs and extended UNIX group IDs
Host	Mappings of host names to corresponding IP addresses
Netgroup	Mappings of netgroups to corresponding IP addresses of members
Showmount	List of exported directories from SVM namespace

If you change information on the external name servers in your environment after ONTAP retrieved and stored it locally, the caches might now contain outdated information. Although ONTAP refreshes caches automatically after certain time periods, different caches have different expiration and refresh times and algorithms.

Another possible reason for caches to contain outdated information is when ONTAP attempts to refresh cached information but encounters a failure when attempting to communicate with name servers. If this happens, ONTAP continues to use the information currently stored in the local caches to prevent client disruption.

As a result, client access requests that are supposed to succeed might fail, and client access requests that are supposed to fail might succeed. You can view and manually flush some of the export policy caches when troubleshooting such client access issues.

How the access cache works

ONTAP uses an access cache to store the results of export policy rule evaluation for client access operations to a volume or qtree. This results in performance improvements because the information can be retrieved much faster from the access cache than going through the export policy rule evaluation process every time a client sends an I/O request.

Whenever an NFS client sends an I/O request to access data on a volume or qtree, ONTAP must evaluate each I/O request to determine whether to grant or deny the I/O request. This evaluation involves checking every export policy rule of the export policy associated with the volume or qtree. If the path to the volume or qtree involves crossing one or more junction points, this might require performing this check for multiple export policies along the path.

Note that this evaluation occurs for every I/O request sent from an NFS client, such as read, write, list, copy and other operations; not just for initial mount requests.

After ONTAP has identified the applicable export policy rules and decided whether to allow or deny the request, ONTAP then creates an entry in the access cache to store this information.

When an NFS client sends an I/O request, ONTAP notes the IP address of the client, the ID of the SVM, and the export policy associated with the target volume or qtree, and first checks the access cache for a matching entry. If a matching entry exists in the access cache, ONTAP uses the stored information to allow or deny the I/O request. If a matching entry does not exist, ONTAP then goes through the normal process of evaluating all applicable policy rules as explained above.

Access cache entries that are not actively used are not refreshed. This reduces unnecessary and wasteful communication with external name serves.

Retrieving the information from the access cache is much faster than going through the entire export policy rule evaluation process for every I/O request. Therefore, using the access cache greatly improves performance by reducing the overhead of client access checks.

How access cache parameters work

Several parameters control the refresh periods for entries in the access cache. Understanding how these parameters work enables you to modify them to tune the access cache and balance performance with how recent the stored information is.

The access cache stores entries consisting of one or more export rules that apply to clients attempting to access volumes or qtrees. These entries are stored for a certain amount of time before they are refreshed. The

refresh time is determined by access cache parameters and depends on the type of access cache entry.

You can specify access cache parameters for individual SVMs. This allows the parameters to differ according to SVM access requirements. Access cache entries that are not actively used are not refreshed, which reduces unnecessary and wasteful communication with external name serves.

Access cache entry type	Description	Refresh period in seconds
Positive entries	Access cache entries that have not resulted in access denial to clients.	Minimum: 300 Maximum: 86,400 Default: 3,600
Negative entries	Access cache entries that have resulted in access denial to clients.	Minimum: 60 Maximum: 86,400 Default: 3,600

Example

An NFS client attempts to access a volume on a cluster. ONTAP matches the client to an export policy rule and determines that the client gets access based on the export policy rule configuration. ONTAP stores the export policy rule in the access cache as a positive entry. By default, ONTAP keeps the positive entry in the access cache for one hour (3,600 seconds), and then automatically refreshes the entry to keep the information current.

To prevent the access cache from filling up unnecessarily, there is an additional parameter to clear existing access cache entries that have not been used for a certain time period to decide client access. This `-harvest-timeout` parameter has an allowed range of 60 through 2,592,000 seconds and a default setting of 86,400 seconds.

Remove an export policy from a qtree

If you decide you do not want a specific export policy assigned to a qtree any longer, you can remove the export policy by modifying the qtree to inherit the export policy of the containing volume instead. You can do this by using the `volume qtree modify` command with the `-export-policy` parameter and an empty name string ("").

Steps

1. To remove an export policy from a qtree, enter the following command:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Verify that the qtree was modified accordingly:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Validate qtree IDs for qtree file operations

ONTAP can perform an optional additional validation of qtree IDs. This validation ensures

that client file operation requests use a valid qtree ID and that clients can only move files within the same qtree. You can enable or disable this validation by modifying the `-validate-qtree-export` parameter. This parameter is enabled by default.

About this task

This parameter is only effective when you have assigned an export policy directly to one or more qtrees on the storage virtual machine (SVM).

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want qtree ID validation to be…	Enter the following command…
Enabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Disabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Export policy restrictions and nested junctions for FlexVol volumes

If you configured export policies to set a less restrictive policy on a nested junction but a more restrictive policy on a higher level junction, access to the lower level junction might fail.

You should ensure that higher level junctions have less restrictive export policies than lower level junctions.

Using Kerberos with NFS for strong security

ONTAP support for Kerberos

Kerberos provides strong secure authentication for client/server applications. Authentication provides verification of user and process identities to a server. In the ONTAP environment, Kerberos provides authentication between storage virtual machines (SVMs) and NFS clients.

In ONTAP 9, the following Kerberos functionality is supported:

- Kerberos 5 authentication with integrity checking (krb5i)

Krb5i uses checksums to verify the integrity of each NFS message transferred between client and server. This is useful both for security reasons (for example, to ensure that data has not been tampered with) and for data integrity reasons (for example, to prevent data corruption when using NFS over unreliable networks).

- Kerberos 5 authentication with privacy checking (krb5p)

  Krb5p uses checksums to encrypt all the traffic between client and the server. This is more secure and also incurs more load.

- 128-bit and 256-bit AES encryption

  Advanced Encryption Standard (AES) is an encryption algorithm for securing electronic data. ONTAP now supports AES with 128-bit keys (AES-128) and AES with 256-bit keys (AES-256) encryption for Kerberos for stronger security.

- SVM-level Kerberos realm configurations

  SVM administrators can now create Kerberos realm configurations at the SVM level. This means that SVM administrators no longer have to rely on the cluster administrator for Kerberos realm configuration and can create individual Kerberos realm configurations in a multi-tenancy environment.

Requirements for configuring Kerberos with NFS

Before you configure Kerberos with NFS on your system, you must verify that certain items in your network and storage environment are properly configured.

> The steps to configure your environment depend on what version and type of client operating system, domain controller, Kerberos, DNS, etc., that you are using. Documenting all these variables is beyond the scope of this document. For more information, see the respective documentation for each component.
>
> For a detailed example of how to set up ONTAP and Kerberos 5 with NFSv3 and NFSv4 in an environment using Windows Server 2008 R2 Active Directory and Linux hosts, see technical report 4073.

The following items should be configured first:

Network environment requirements

- Kerberos

  You must have a working Kerberos setup with a key distribution center (KDC), such as Windows Active Directory based Kerberos or MIT Kerberos.

  NFS servers must use `nfs` as the primary component of their machine principal.

- Directory service

  You must use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS.

- NTP

You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

  Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

- User accounts

  Each client must have a user account in the Kerberos realm. NFS servers must use “nfs” as the primary component of their machine principal.

NFS client requirements

- NFS

  Each client must be properly configured to communicate over the network using NFSv3 or NFSv4.

  Clients must support RFC1964 and RFC2203.

- Kerberos

  Each client must be properly configured to use Kerberos authentication, including the following details:

  - Encryption for TGS communication is enabled.

    AES-256 for strongest security.

  - The most secure encryption type for TGT communication is enabled.
  - The Kerberos realm and domain are configured correctly.
  - GSS is enabled.

    When using machine credentials:

  - Do not run `gssd` with the `-n` parameter.
  - Do not run `kinit` as the root user.

- Each client must use the most recent and updated operating system version.

  This provides the best compatibility and reliability for AES encryption with Kerberos.

- DNS

  Each client must be properly configured to use DNS for correct name resolution.

- NTP

  Each client must be synchronizing with the NTP server.

- Host and domain information

  Each client’s `/etc/hosts` and `/etc/resolv.conf` files must contain the correct host name and DNS information, respectively.

- Keytab files

  Each client must have a keytab file from the KDC. The realm must be in uppercase letters. The encryption type must be AES-256 for strongest security.

- Optional: For best performance, clients benefit from having at least two network interfaces: one for communicating with the local area network and one for communicating with the storage network.

Storage system requirements

- NFS license

  The storage system must have a valid NFS license installed.

- CIFS license

  The CIFS license is optional. It is only required for checking Windows credentials when using multiprotocol name mapping. It is not required in a strict UNIX-only environment.

- SVM

  You must have at least one SVM configured on the system.

- DNS on the SVM

  You must have configured DNS on each SVM.

- NFS server

  You must have configured NFS on the SVM.

- AES encryption

  For strongest security, you must configure the NFS server to allow only AES-256 encryption for Kerberos.

- SMB server

  If you are running a multiprotocol environment, you must have configured SMB on the SVM. The SMB server is required for multiprotocol name mapping.

- Volumes

  You must have a root volume and at least one data volume configured for use by the SVM.

- Root volume

  The root volume of the SVM must have the following configuration:

Name	Setting
Security style	UNIX
UID	root or ID 0

Name	Setting
GID	root or ID 0
UNIX permissions	777

In contrast to the root volume, data volumes can have either security style.

- UNIX groups

  The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0
pcuser	65534 (created automatically by ONTAP when you create the SVM)

- UNIX users

  The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase The first component of the NFS client user SPN is used as the user.
pcuser	65534	65534	Required for NFS and CIFS multiprotocol use Created and added to the pcuser group automatically by ONTAP when you create the SVM.
root	0	0	Required for mounting

  The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.

- Export policies and rules

  You must have configured export policies with the necessary export rules for the root and data volumes and qtrees. If all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` , `krb5i`, or `krb5p`.

- Kerberos-UNIX name mapping

  If you want the user identified by the NFS client user SPN to have root permissions, you must create a name mapping to root.

Related information

NetApp Technical Report 4073: Secure Unified Authentication

NetApp Interoperability Matrix Tool

System administration

Logical storage management

Specify the user ID domain for NFSv4

To specify the user ID domain, you can set the `-v4-id-domain` option.

About this task

By default, ONTAP uses the NIS domain for NFSv4 user ID mapping, if one is set. If an NIS domain is not set, the DNS domain is used. You might need to set the user ID domain if, for example, you have multiple user ID domains. The domain name must match the domain configuration on the domain controller. It is not required for NFSv3.

Step

1. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configure name services

How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns

Database type	Defines name service sources for…	Valid sources are…
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

Example

The following example displays the name service switch configuration for the SVM svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

To look up IP addresses for hosts, ONTAP first consults local source files. If the query does not return any results, DNS servers are checked next.

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

Related information

NetApp Technical Report 4668: Name Services Best Practices Guide

Use LDAP

LDAP Overview

An LDAP (Lightweight Directory Access Protocol) server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your storage system to look up user information in your existing LDAP database.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:

- The domain name of the LDAP server must match the entry on the LDAP client.
- The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
  - CRYPT (all types) and SHA-1 (SHA, SSHA).
  - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
- If the LDAP server requires session security measures, you must configure them in the LDAP client.

  The following session security options are available:

  - LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
  - START TLS
  - LDAPS (LDAP over TLS or SSL)
- To enable signed and sealed LDAP queries, the following services must be configured:
  - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
  - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
  - Kerberos servers must have SRV records present on the DNS server.
- To enable START TLS or LDAPS, the following points should be considered.
  - It is a NetApp best practice to use Start TLS rather than LDAPS.
  - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
  - A certificate server must already be configured in the domain.
- To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
  - Both domains should be configured with one of the following trust relationships:
    - Two-way
    - One-way, where the primary trusts the referral domain
    - Parent-child
  - DNS must be configured to resolve all referred server names.
  - Domain passwords should be same to authenticate when `--bind-as-cifs-server` set to true.

The following configurations are not supported with LDAP referral chasing.

- For all ONTAP versions:
- LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
- LDAP signing and sealing (the `-session-security` option)
- Encrypted TLS connections (the `-use-start-tls` option)
- Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- Beginning with ONTAP 9.11.1, you can use LDAP fast bind for nsswitch authentication.

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

  In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the NFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`. test

LDAP signing and sealing on SMB traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

LDAPS concepts

You must understand certain terms and concepts about how ONTAP secures LDAP communication. ONTAP can use START TLS or LDAPS for setting up authenticated sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

Terminology

There are certain terms that you should understand about how ONTAP uses LDAPS to secure LDAP communication.

- **LDAP**

  (Lightweight Directory Access Protocol) A protocol for accessing and managing information directories. LDAP is used as an information directory for storing objects such as users, groups, and netgroups. LDAP also provides directory services that manage these objects and fulfill LDAP requests from LDAP clients.

- **SSL**

  (Secure Sockets Layer) A protocol developed for sending information securely over the Internet. It has been deprecated in favor of TLS. SSL is not supported in ONTAP 9.0-9.4.

- **TLS**

  (Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL.

- **LDAPS (LDAP over SSL or TLS)**

A protocol that uses TLS or SSL to secure communication between LDAP clients and LDAP servers. The terms *LDAP over SSL* and *LDAP over TLS* are sometimes used interchangeably; TLS is supported by ONTAP 9 and later, SSL is supported by ONTAP 9.5 and later.

  - In ONTAP 9.5-9.8, LDAPS can only be enabled on port 636. To do so, use the `-use-ldaps-for-ad-ldap` parameter with the `vserver cifs security modify` command.
  - Beginning with ONTAP 9.9.1, LDAPS can be enabled on any port, although port 636 remains the default. To do so, set the `-ldaps-enabled` parameter to `true` and specify the desired `-port` parameter. For more information, see the `vserver services name-service ldap client create` man page

  It is a NetApp best practice to use Start TLS rather than LDAPS.

- **Start TLS**

  (Also known as *start_tls*, *STARTTLS*, and *StartTLS*) A mechanism to provide secure communication by using the TLS protocols.

  ONTAP uses STARTTLS for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. The LDAP server must be configured to allow connections over LDAP port 389; otherwise, LDAP TLS connections from the SVM to the LDAP server fail.

How ONTAP uses LDAPS

ONTAP supports TLS server authentication, which enables the SVM LDAP client to confirm the LDAP server's identity during the bind operation. TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.

LDAP supports STARTTLS to encrypt communications using TLS. STARTTLS begins as a plaintext connection over the standard LDAP port (389), and that connection is then upgraded to TLS.

ONTAP supports the following:

- LDAPS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAPS for LDAP traffic for name mapping and other UNIX information

  Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping and other UNIX information, such as users, groups, and netgroups.

- Self-signed root CA certificates

  When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

By default, LDAPS is disabled.

Enable LDAP RFC2307bis support

If you want to use LDAP and require the additional capability to use nested group

memberships, you can configure ONTAP to enable LDAP RFC2307bis support.

What you'll need

You must have created a copy of one of the default LDAP client schemas that you want to use.

About this task

In LDAP client schemas, group objects use the memberUid attribute. This attribute can contain multiple values and lists the names of the users that belong to that group. In RFC2307bis enabled LDAP client schemas, group objects use the uniqueMember attribute. This attribute can contain the full distinguished name (DN) of another object in the LDAP directory. This enables you to use nested groups because groups can have other groups as members.

The user should not be a member of more than 256 groups including nested groups. ONTAP ignores any groups over the 256 group limit.

By default, RFC2307bis support is disabled.

RFC2307bis support is enabled automatically in ONTAP when an LDAP client is created with the MS-AD-BIS schema.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Modify the copied RFC2307 LDAP client schema to enable RFC2307bis support:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modify the schema to match the object class supported in the LDAP server:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modify the schema to match the attribute name supported in the LDAP server:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Configuration options for LDAP directory searches

You can optimize LDAP directory searches, including user, group, and netgroup information, by configuring the ONTAP LDAP client to connect to LDAP servers in the most appropriate way for your environment. You need to understand when the default LDAP base and scope search values suffice and which parameters to specify when

custom values are more appropriate.

LDAP client search options for user, group, and netgroup information can help avoid failed LDAP queries, and therefore failed client access to storage systems. They also help ensure that the searches are as efficient as possible to avoid client performance issues.

Default base and scope search values

The LDAP base is the default base DN that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base DN. This option is appropriate when your LDAP directory is relatively small and all relevant entries are located in the same DN.

If you do not specify a custom base DN, the default is `root`. This means that each query searches the entire directory. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

The LDAP base scope is the default search scope that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base scope. It determines whether the LDAP query searches only the named entry, entries one level below the DN, or the entire subtree below the DN.

If you do not specify a custom base scope, the default is `subtree`. This means that each query searches the entire subtree below the DN. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

Custom base and scope search values

Optionally, you can specify separate base and scope values for user, group, and netgroup searches. Limiting the search base and scope of queries this way can significantly improve performance because it limits the search to a smaller subsection of the LDAP directory.

If you specify custom base and scope values, they override the general default search base and scope for user, group, and netgroup searches. The parameters to specify custom base and scope values are available at the advanced privilege level.

LDAP client parameter…	Specifies custom…
`-base-dn`	Base DN for all LDAP searchesMultiple values can be entered if needed (for example, if LDAP referral chasing is enabled in ONTAP 9.5 and later releases).
`-base-scope`	Base scope for all LDAP searches
`-user-dn`	Base DNs for all LDAP user searchesThis parameter also applies to user name-mapping searches.
`-user-scope`	Base scope for all LDAP user searches This parameter also applies to user name-mapping searches.
`-group-dn`	Base DNs for all LDAP group searches

`-group-scope`	Base scope for all LDAP group searches
`-netgroup-dn`	Base DNs for all LDAP netgroup searches
`-netgroup-scope`	Base scope for all LDAP netgroup searches

Multiple custom base DN values

If your LDAP directory structure is more complex, it might be necessary for you to specify multiple base DNs to search multiple parts of your LDAP directory for certain information. You can specify multiple DNs for the user, group, and netgroup DN parameters by separating them with a semicolon (;) and enclosing the entire DN search list with double quotes ("). If a DN contains a semicolon, you must add an escape character (\) immediately before the semicolon in the DN.

Note that the scope applies to the entire list of DNs specified for the corresponding parameter. For example, if you specify a list of three different user DNs and subtree for the user scope, then LDAP user searches search the entire subtree for each of the three specified DNs.

Beginning with ONTAP 9.5, you can also specify LDAP *referral chasing*, which allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is not returned by the primary LDAP server. The client uses that referral data to retrieve the target object from the server described in the referral data. To search for objects present in the referred LDAP servers, the base-dn of the referred objects can be added to the base-dn as part of LDAP client configuration. However, referred objects are only looked up when referral chasing is enabled (using the `-referral-enabled true` option) during LDAP client creation or modification.

Improve performance of LDAP directory netgroup-by-host searches

If your LDAP environment is configured to allow netgroup-by-host searches, you can configure ONTAP to take advantage of this and perform netgroup-by-host searches. This can significantly speed up netgroup searches and reduce possible NFS client access issues due to latency during netgroup searches.

What you'll need

Your LDAP directory must contain a `netgroup.byhost` map.

Your DNS servers should contain both forward (A) and reverse (PTR) lookup records for NFS clients.

When you specify IPv6 addresses in netgroups, you must always shorten and compress each address as specified in RFC 5952.

About this task

NIS servers store netgroup information in three separate maps called `netgroup`, `netgroup.byuser`, and `netgroup.byhost`. The purpose of the `netgroup.byuser` and `netgroup.byhost` maps is to speed up netgroup searches. ONTAP can perform netgroup-by-host searches on NIS servers for improved mount response times.

By default, LDAP directories do not have such a `netgroup.byhost` map like NIS servers. It is possible, though, with the help of third-party tools, to import a NIS `netgroup.byhost` map into LDAP directories to enable fast netgroup-by-host searches. If you have configured your LDAP environment to allow netgroup-by-

host searches, you can configure the ONTAP LDAP client with the `netgroup.byhost` map name, DN, and search scope for faster netgroup-by-host searches.

Receiving the results for netgroup-by-host searches faster enables ONTAP to process export rules faster when NFS clients request access to exports. This reduces the chance of delayed access due to netgroup search latency issues.

Steps

1. Obtain the exact full distinguished name of the NIS `netgroup.byhost` map you imported into your LDAP directory.

   The map DN can vary depending on the third-party tool you used for import. For best performance, you should specify the exact map DN.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enable netgroup-by-host searches in the LDAP client configuration of the storage virtual machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client -config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true`|`false`} enables or disables netgroup-by-host search for LDAP directories. The default is `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` specifies the distinguished name of the `netgroup.byhost` map in the LDAP directory. It overrides the base DN for netgroup-by-host searches. If you do not specify this parameter, ONTAP uses the base DN instead.

   `-netgroup-byhost-scope` {`base`|`onelevel`|`subtree`} specifies the search scope for netgroup-by-host searches. If you do not specify this parameter, the default is `subtree`.

   If the LDAP client configuration does not exist yet, you can enable netgroup-by-host searches by specifying these parameters when creating a new LDAP client configuration using the `vserver services name-service ldap client create` command.

   > Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

4. Return to the admin privilege level: `set -privilege admin`

Example

The following command modifies the existing LDAP client configuration named “ldap_corp” to enable netgroup-by-host searches using the `netgroup.byhost` map named “nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com” and the default search scope `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

After you finish

The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues.

Related information

IETF RFC 5952: A Recommendation for IPv6 Address Text Representation

Use LDAP fast bind for nsswitch authentication

Beginning with ONTAP 9.11.1, you can take advantage of LDAP *fast bind* functionality (also known as *concurrent bind*) for faster and simpler client authentication requests. To use this functionality, the LDAP server must support fast bind functionality.

About this task

Without fast bind, ONTAP uses LDAP simple bind to authenticate admin users with the LDAP server. With this authentication method, ONTAP sends a user or group name to the LDAP server, receives the stored hash password, and compares the server hash code with the hash passcode generated locally from the user password. If they are identical, ONTAP grants login permission.

With fast bind functionality, ONTAP sends only user credentials (user name and password) to the LDAP server through a secure connection. The LDAP server then validates these credentials and instructs ONTAP to grant login permissions.

One advantage of fast bind is that there is no need for ONTAP to support every new hashing algorithm supported by LDAP servers, because password hashing is performed by the LDAP server.

Learn about using fast bind.

You can use existing LDAP client configurations for LDAP fast bind. However, it is strongly recommended that the LDAP client be configured for TLS or LDAPs; otherwise, the password is sent over the wire in plain text.

To enable LDAP fast bind in an ONTAP environment, you must satisfy these requirements:

- ONTAP admin users must be configured on an LDAP server that supports fast bind.
- The ONTAP SVM must be configured for LDAP in the name services switch (nsswitch) database.
- ONTAP admin user and group accounts must be configured for nsswitch authentication using fast bind.

Steps

1. Confirm with your LDAP administrator that LDAP fast bind is supported on the LDAP server.
2. Ensure that ONTAP admin user credentials are configured on the LDAP server.
3. Verify that the admin or data SVM is configured correctly for LDAP fast bind.
   a. To confirm that the LDAP fast bind server is listed in the LDAP client configuration, enter:

      ```
      vserver services name-service ldap client show
      ```

      Learn about LDAP client configuration.

   b. To confirm that `ldap` is one of the configured sources for the nsswitch `passwd` database, enter:

      ```
      vserver services name-service ns-switch show
      ```

      Learn about nsswitch configuration.

4. Ensure that admin users are authenticating with nsswitch and that LDAP fast bind authentication is enabled in their accounts.
   - For existing users, enter `security login modify` and verify the following parameter settings:

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

   - For new admin users, see Enable LDAP or NIS account access.

Display LDAP statistics

Beginning with ONTAP 9.2, you can display LDAP statistics for storage virtual machines (SVMs) on a storage system to monitor the performance and diagnose issues.

What you'll need

- You must have configured an LDAP client on the SVM.
- You must have identified LDAP objects from which you can view data.

Step

1. View the performance data for counter objects:

   `statistics show`

Examples

The following example shows the performance data for object `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                              Value
-------------------------------- --------------------------------
instance_name                        vserverName:LDAP (NIS & Name
                                     Mapping):GetUserInfoFromName:
                                     1.1.1.1
last_modified_time                   1460610787
node_name                            nodeName
num_not_found_responses              1
num_request_failures                 1
num_requests_sent                    1
num_responses_received               1
num_successful_responses             0
num_timeouts                         0
operation                            GetUserInfoFromName
process_name                         secd
request_latency                      52131us
```

Configure name mappings

Configure name mappings overview

ONTAP uses name mapping to map SMB identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to SMB identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a SMB client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use SMB access or NTFS security style on volumes.
- You configure the default user to be used instead.

  In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID.

How name mapping works

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

  If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

  If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default SMB user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

  Even if name mappings for machine accounts are defined, the mappings are ignored.

Multidomain searches for UNIX user to Windows user name mappings

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the SMB server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the SMB server on the SVM belongs.

- *Bidirectional trust*

  With bidirectional trusts, both domains trust each other. If the SMB server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

- *Outbound trust*

  With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

  A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

- *Inbound trust*

  With an inbound trust, the other domain trusts the SMB server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

  A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

How wildcards (*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user "root" is mapped to the user named "administrator". All trusted domains are searched in order until the first matching user named "administrator" is found.
*	**	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found. The pattern ** is only valid for name mapping from UNIX to Windows, not the other way around.

How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by ONTAP
- Use the preferred trusted domain list that you compile

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

Name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

Create a name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

Step

1. Create a name mapping:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string `" "` (the space character). See the `vserver name-mapping create` man page for details.

When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

Examples

The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes “$” as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john$ops to UNIX user john_ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure the default user

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Configure the default UNIX user	`vserver cifs options modify -default-unix-user user_name`
Configure the default Windows user	`vserver nfs modify -default-win-user user_name`

Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

See the man page for each command for more information.

Enable access for Windows NFS clients

ONTAP supports file access from Windows NFSv3 clients. This means that clients running Windows operating systems with NFSv3 support can now access files on NFSv3 exports on the cluster. To successfully use this functionality, you must properly configure the storage virtual machine (SVM) and be aware of certain requirements and limitations.

What you'll need

NFSv3 must be enabled on the SVM.

About this task

By default, Windows NFSv3 client support is disabled.

Windows NFSv3 clients do not support the network status monitor (NSM) protocol. As a result, Windows NFSv3 client sessions might experience disruptions during storage failover and volume move operations.

Steps

1. Enable Windows NFSv3 client support:

```
vserver nfs modify -vserver vserver_name -v3-ms-dos-client enabled
```

2. On all SVMs that support Windows NFSv3 clients, disable the `-enable-ejukebox` and `-v3 -connection-drop` parameters: `vserver nfs modify -vserver vserver_name -enable -ejukebox false -v3-connection-drop disabled`

   Windows NFSv3 clients can now mount exports on the storage system.

3. Ensure that each Windows NFSv3 client uses hard mounts by specifying the `-o mtype=hard` option.

   This is required to ensure reliable mounts.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Enable the display of NFS exports on NFS clients

NFS clients can use the `showmount -e` command to see a list of exports available from an ONTAP NFS server. This can help users identify the file system they want to mount.

Beginning with ONTAP 9.2, ONTAP allows NFS clients to view the export list by default. In earlier releases, the `showmount` option of the `vserver nfs modify` command must be enabled explicitly. For viewing the export list, NFSv3 should be enabled on the SVM.

Example

The following command shows the showmount feature on the SVM named vs1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

The following command executed on an NFS client displays the list of exports on an NFS server with the IP address 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Manage file access using NFS

Enable or disable NFSv3

You can enable or disable NFSv3 by modifying the `-v3` option. This allows file access for clients using the NFSv3 protocol. By default, NFSv3 is enabled.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Disable NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Enable or disable NFSv4.0

You can enable or disable NFSv4.0 by modifying the `-v4.0` option. This allows file access for clients using the NFSv4.0 protocol. In ONTAP 9.9.1, NFSv4.0 is enabled by default; in earlier releases, it is disabled by default.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Enable NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Disable NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Enable or disable NFSv4.1

You can enable or disable NFSv4.1 by modifying the `-v4.1` option. This allows file access for clients using the NFSv4.1 protocol. In ONTAP 9.9.1, NFSv4.1 is enabled by default; in earlier releases, it is disabled by default.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Enable NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Disable NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Enable or disable pNFS

pNFS improves performance by allowing NFS clients to perform read/write operations on

storage devices directly and in parallel, bypassing the NFS server as a potential bottleneck. To enable or disable pNFS (parallel NFS), you can modify the `-v4.1-pnfs` option.

If the ONTAP release is…	The pNFS default is…
9.8 or later	disabled
9.7 or earlier	enabled

What you'll need

NFSv4.1 support is required to be able to use pNFS.

If you want to enable pNFS, you must first disable NFS referrals. They cannot both be enabled at the same time.

If you use pNFS with Kerberos on SVMs, you must enable Kerberos on every LIF on the SVM.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Disable pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Control NFS access over TCP and UDP

You can enable or disable NFS access to storage virtual machines (SVMs) over TCP and UDP by modifying the `-tcp` and `-udp` parameters, respectively. This enables you to control whether NFS clients can access data over TCP or UDP in your environment.

About this task

These parameters only apply to NFS. They do not affect auxiliary protocols. For example, if NFS over TCP is disabled, mount operations over TCP still succeed. To completely block TCP or UDP traffic, you can use export policy rules.

> You must turn off the SnapDiff RPC Server before you disable TCP for NFS to avoid a command failed error. You can disable TCP by using the command `vserver snapdiff-rpc-server off -vserver vserver name`.

Step

1. Perform one of the following actions:

If you want NFS access to be…	Enter the command…

Enabled over TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Disabled over TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Enabled over UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Disabled over UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Control NFS requests from nonreserved ports

You can reject NFS mount requests from nonreserved ports by enabling the `-mount -rootonly` option. To reject all NFS requests from nonreserved ports, you can enable the `-nfs-rootonly` option.

About this task

By default, the option `-mount-rootonly` is `enabled`.

By default, the option `-nfs-rootonly` is `disabled`.

These options do not apply to the NULL procedure.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Allow NFS mount requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Reject NFS mount requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Allow all NFS requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Reject all NFS requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Handle NFS access to NTFS volumes or qtrees for unknown UNIX users

If ONTAP cannot identify UNIX users attempting to connect to volumes or qtrees with NTFS security style, it therefore cannot explicitly map the user to a Windows user. You can configure ONTAP to either deny access to such users for stricter security or map them to a default Windows user to ensure a minimum level of access for all users.

What you'll need

A default Windows user must be configured if you want to enable this option.

About this task

If a UNIX user tries to access volumes or qtrees with NTFS security style, the UNIX user must first be mapped to a Windows user so that ONTAP can properly evaluate the NTFS permissions. However, if ONTAP cannot look up the name of the UNIX user in the configured user information name service sources, it cannot explicitly map the UNIX user to a specific Windows user. You can decide how to handle such unknown UNIX users in the following ways:

- Deny access to unknown UNIX users.

  This enforces stricter security by requiring explicit mapping for all UNIX users to gain access to NTFS volumes or qtrees.

- Map unknown UNIX users to a default Windows user.

  This provides less security but more convenience by ensuring that all users get a minimum level of access to NTFS volumes or qtrees through a default Windows user.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want the default Windows user for unknown UNIX users…	Enter the command…
Enabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Disabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Considerations for clients that mount NFS exports using a nonreserved port

The `-mount-rootonly` option must be disabled on a storage system that must support clients that mount NFS exports using a nonreserved port even when the user is logged in as root. Such clients include Hummingbird clients and Solaris NFS/IPv6 clients.

If the `-mount-rootonly` option is enabled, ONTAP does not allow NFS clients that use nonreserved ports, meaning ports with numbers higher than 1,023, to mount NFS exports.

Perform stricter access checking for netgroups by verifying domains

By default, ONTAP performs an additional verification when evaluating client access for a netgroup. The additional check ensures that the client's domain matches the domain configuration of the storage virtual machine (SVM). Otherwise, ONTAP denies client access.

About this task

When ONTAP evaluates export policy rules for client access and an export policy rule contains a netgroup, ONTAP must determine whether a client's IP address belongs to the netgroup. For this purpose, ONTAP converts the client's IP address to a host name using DNS and obtains a fully qualified domain name (FQDN).

If the netgroup file only lists a short name for the host and the short name for the host exists in multiple domains, it is possible for a client from a different domain to obtain access without this check.

To prevent this, ONTAP compares the domain that was returned from DNS for the host against the list of DNS domain names configured for the SVM. If it matches, access is allowed. If it does not match, access is denied.

This verification is enabled by default. You can manage it by modifying the `-netgroup-dns-domain -search` parameter, which is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

If you want domain verification for netgroups to be…	Enter…
Enabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Disabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Set the privilege level to admin:

   ```
   set -privilege admin
   ```

Modify ports used for NFSv3 services

The NFS server on the storage system uses services such as mount daemon and Network Lock Manager to communicate with NFS clients over specific default network ports. In most NFS environments the default ports work correctly and do not require modification, but if you want to use different NFS network ports in your NFSv3 environment, you can do so.

What you'll need

Changing NFS ports on the storage system requires that all NFS clients reconnect to the system, so you should communicate this information to your users in advance of making the change.

About this task

You can set the ports used by the NFS mount daemon, Network Lock Manager, Network Status Monitor, and NFS quota daemon services for each storage virtual machine (SVM). The port number change affects NFS clients accessing data over both TCP and UDP.

Ports for NFSv4 and NFSv4.1 cannot be changed.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Disable access to NFS:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Set the NFS port for the specific NFS service:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS port parameter	Description	Default port
`-mountd-port`	NFS mount daemon	635
`-nlm-port`	Network Lock Manager	4045
`-nsm-port`	Network Status Monitor	4046
`-rquotad-port`	NFS quota daemon	4049

   Besides the default port, the allowed range of port numbers is 1024 through 65535. Each NFS service must use a unique port.

4. Enable access to NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use the `network connections listening show` command to verify the port number changes.
6. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following commands set the NFS Mount Daemon port to 1113 on the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Commands for managing NFS servers

There are specific ONTAP commands for managing NFS servers.

If you want to…	Use this command…
Create an NFS server	`vserver nfs create`
Display NFS servers	`vserver nfs show`
Modify an NFS server	`vserver nfs modify`
Delete an NFS server	`vserver nfs delete`

Hide the `.snapshot` directory listing under NFSv3 mount points Explicit access to the `.snapshot` directory will still be allowed even if the option is enabled.	`vserver nfs` commands with the `-v3-hide-snapshot` option enabled

See the man page for each command for more information.

Troubleshoot name service issues

When clients experience access failures due to name service issues, you can use the `vserver services name-service getxxbyyy` command family to manually perform various name service lookups and examine the details and results of the lookup to help with troubleshooting.

About this task

- For each command, you can specify the following:
  - Name of the node or storage virtual machine (SVM) to perform the lookup on.

    This enables you to test name service lookups for a specific node or SVM to narrow the search for a potential name service configuration issue.
  - Whether to show the source used for the lookup.

    This enables you to check whether the correct source was used.
- ONTAP selects the service for performing the lookup based on the configured name service switch order.
- These commands are available at the advanced privilege level.

Steps

1. Perform one of the following actions:

To retrieve the…	Use the command…
IP address of a host name	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (IPv4 addresses only)
Members of a group by group ID	`vserver services name-service getxxbyyy getgrbygid`
Members of a group by group name	`vserver services name-service getxxbyyy getgrbyname`

List of groups a user belongs to	`vserver services name-service getxxbyyy getgrlist`
Host name of an IP address	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (IPv4 addresses only)
User information by user name	`vserver services name-service getxxbyyy getpwbyname` You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`.
User information by user ID	`vserver services name-service getxxbyyy getpwbyuid` You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`.
Netgroup membership of a client	`vserver services name-service getxxbyyy netgrp`
Netgroup membership of a client using netgroup-by-host search	`vserver services name-service getxxbyyy netgrpbyhost`

The following example shows a DNS lookup test for the SVM vs1 by attempting to obtain the IP address for the host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

The following example shows a NIS lookup test for the SVM vs1 by attempting to retrieve user information for a user with the UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

The following example shows an LDAP lookup test for the SVM vs1 by attempting to retrieve user information for a user with the name ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

The following example shows a netgroup lookup test for the SVM vs1 by attempting to find out whether the client dnshost0 is a member of the netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analyze the results of the test you performed and take the necessary action.

If the…	Check the…
Host name or IP address lookup failed or yielded incorrect results	DNS configuration
Lookup queried an incorrect source	Name service switch configuration

User or group lookup failed or yielded incorrect results	Name service switch configuration Source configuration (local files, NIS domain, LDAP client) Network configuration (for example, LIFs and routes)
Host name lookup failed or timed out, and the DNS server does not resolve DNS short names (for example, host1)	DNS configuration for top-level domain (TLD) queries. You can disable TLD queries using the `-is-tld -query-enabled false` option to the `vserver services name-service dns modify` command.

Related information

NetApp Technical Report 4668: Name Services Best Practices Guide

Verify name service connections

Beginning with ONTAP 9.2, you can check DNS and LDAP name servers to verify that they are connected to ONTAP. These commands are available at the admin privilege level.

About this task

You can check for a valid DNS or LDAP name service configuration on an as-needed basis using the name service configuration checker. This validation check can be initiated at the command line or in System Manager.

For DNS configurations, all servers are tested and need to be working for the configuration to be considered valid. For LDAP configurations, as long as any server is up, the configuration is valid. The name service commands apply the configuration checker unless the `skip-config-validation` field is true (the default is false).

Step

1. Use the appropriate command to check a name service configuration. The UI displays the status of the configured servers.

To check…	Use this command…
DNS configuration status	`vserver services name-service dns check`
LDAP configuration status	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

Configuration validation is successful if at least one of the configured servers (name-servers/ldap-servers) is reachable and providing the service. A warning is shown if some of the servers are not reachable.

Commands for managing name service switch entries

You can manage name service switch entries by creating, displaying, modifying, and deleting them.

If you want to…	Use this command…
Create a name service switch entry	`vserver services name-service ns-switch create`
Display name service switch entries	`vserver services name-service ns-switch show`
Modify a name service switch entry	`vserver services name-service ns-switch modify`
Delete a name service switch entry	`vserver services name-service ns-switch delete`

See the man page for each command for more information.

Related information

NetApp Technical Report 4668: Name Services Best Practices Guide

Commands for managing name service cache

You can manage name service cache by modifying the time to live (TTL) value. The TTL value determines how long name service information is persistent in cache.

If you want to modify the TTL value for…	Use this command…
Unix users	`vserver services name-service cache unix-user settings`
Unix groups	`vserver services name-service cache unix-group settings`
Unix netgroups	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Group membership	`vserver services name-service cache group-membership settings`

Related information

ONTAP 9 Commands

Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

See the man page for each command for more information.

Commands for managing local UNIX users

There are specific ONTAP commands for managing local UNIX users.

If you want to…	Use this command…
Create a local UNIX user	`vserver services name-service unix-user create`
Load local UNIX users from a URI	`vserver services name-service unix-user load-from-uri`
Display local UNIX users	`vserver services name-service unix-user show`
Modify a local UNIX user	`vserver services name-service unix-user modify`
Delete a local UNIX user	`vserver services name-service unix-user delete`

See the man page for each command for more information.

Commands for managing local UNIX groups

There are specific ONTAP commands for managing local UNIX groups.

If you want to…	Use this command…
Create a local UNIX group	`vserver services name-service unix-group create`
Add a user to a local UNIX group	`vserver services name-service unix-group adduser`
Load local UNIX groups from a URI	`vserver services name-service unix-group load-from-uri`
Display local UNIX groups	`vserver services name-service unix-group show`
Modify a local UNIX group	`vserver services name-service unix-group modify`
Delete a user from a local UNIX group	`vserver services name-service unix-group deluser`
Delete a local UNIX group	`vserver services name-service unix-group delete`

See the man page for each command for more information.

Limits for local UNIX users, groups, and group members

ONTAP introduced limits for the maximum number of UNIX users and groups in the cluster, and commands to manage these limits. These limits can help avoid performance issues by preventing administrators from creating too many local UNIX users and groups in the cluster.

There is a limit for the combined number of local UNIX user groups and group members. There is a separate limit for local UNIX users. The limits are cluster-wide. Each of these new limits is set to a default value that you can modify up to a preassigned hard limit.

Database	Default limit	Hard limit
Local UNIX users	32,768	65,536
Local UNIX groups and group members	32,768	65,536

Manage limits for local UNIX users and groups

There are specific ONTAP commands for managing limits for local UNIX users and groups. Cluster administrators can use these commands to troubleshoot performance issues in the cluster believed to be related to excessive numbers of local UNIX users and groups.

About this task

These commands are available to the cluster administrator at the advanced privilege level.

Step

1. Perform one of the following actions:

If you want to…	Use the command…
Display information about local UNIX user limits	`vserver services unix-user max-limit show`
Display information about local UNIX group limits	`vserver services unix-group max-limit show`
Modify local UNIX user limits	`vserver services unix-user max-limit modify`
Modify local UNIX group limits	`vserver services unix-group max-limit modify`

See the man page for each command for more information.

Commands for managing local netgroups

You can manage local netgroups by loading them from a URI, verifying their status across nodes, displaying them, and deleting them.

If you want to…	Use the command…
Load netgroups from a URI	`vserver services name-service netgroup load`
Verify the status of netgroups across nodes	`vserver services name-service netgroup status` Available at the advanced privilege level and higher.
Display local netgroups	`vserver services name-service netgroup file show`
Delete a local netgroup	`vserver services name-service netgroup file delete`

See the man page for each command for more information.

Commands for managing NIS domain configurations

There are specific ONTAP commands for managing NIS domain configurations.

If you want to…	Use this command…
Create a NIS domain configuration	`vserver services name-service nis-domain create`
Display NIS domain configurations	`vserver services name-service nis-domain show`
Display binding status of a NIS domain configuration	`vserver services name-service nis-domain show-bound`
Display NIS statistics	`vserver services name-service nis-domain show-statistics` Available at the advanced privilege level and higher.
Clear NIS statistics	`vserver services name-service nis-domain clear-statistics` Available at the advanced privilege level and higher.
Modify a NIS domain configuration	`vserver services name-service nis-domain modify`
Delete a NIS domain configuration	`vserver services name-service nis-domain delete`
Enable caching for netgroup-by-host searches	`vserver services name-service nis-domain netgroup-database config modify` Available at the advanced privilege level and higher.

See the man page for each command for more information.

Commands for managing LDAP client configurations

There are specific ONTAP commands for managing LDAP client configurations.

> SVM administrators cannot modify or delete LDAP client configurations that were created by cluster administrators.

If you want to…	Use this command…
Create an LDAP client configuration	`vserver services name-service ldap client create`
Display LDAP client configurations	`vserver services name-service ldap client show`
Modify an LDAP client configuration	`vserver services name-service ldap client modify`
Change the LDAP client BIND password	`vserver services name-service ldap client modify-bind-password`
Delete an LDAP client configuration	`vserver services name-service ldap client delete`

See the man page for each command for more information.

Commands for managing LDAP configurations

There are specific ONTAP commands for managing LDAP configurations.

If you want to…	Use this command…
Create an LDAP configuration	`vserver services name-service ldap create`
Display LDAP configurations	`vserver services name-service ldap show`
Modify an LDAP configuration	`vserver services name-service ldap modify`
Delete an LDAP configuration	`vserver services name-service ldap delete`

See the man page for each command for more information.

Commands for managing LDAP client schema templates

There are specific ONTAP commands for managing LDAP client schema templates.

> SVM administrators cannot modify or delete LDAP client schemas that were created by cluster administrators.

If you want to…	Use this command…

Copy an existing LDAP schema template	`vserver services name-service ldap client schema copy` Available at the advanced privilege level and higher.
Display LDAP schema templates	`vserver services name-service ldap client schema show`
Modify an LDAP schema template	`vserver services name-service ldap client schema modify` Available at the advanced privilege level and higher.
Delete an LDAP schema template	`vserver services name-service ldap client schema delete` Available at the advanced privilege level and higher.

See the man page for each command for more information.

Commands for managing NFS Kerberos interface configurations

There are specific ONTAP commands for managing NFS Kerberos interface configurations.

If you want to…	Use this command…
Enable NFS Kerberos on a LIF	`vserver nfs kerberos interface enable`
Display NFS Kerberos interface configurations	`vserver nfs kerberos interface show`
Modify an NFS Kerberos interface configuration	`vserver nfs kerberos interface modify`
Disable NFS Kerberos on a LIF	`vserver nfs kerberos interface disable`

See the man page for each command for more information.

Commands for managing NFS Kerberos realm configurations

There are specific ONTAP commands for managing NFS Kerberos realm configurations.

If you want to…	Use this command…
Create an NFS Kerberos realm configuration	`vserver nfs kerberos realm create`
Display NFS Kerberos realm configurations	`vserver nfs kerberos realm show`

If you want to…	Use this command…
Modify an NFS Kerberos realm configuration	`vserver nfs kerberos realm modify`
Delete an NFS Kerberos realm configuration	`vserver nfs kerberos realm delete`

See the man page for each command for more information.

Commands for managing export policies

There are specific ONTAP commands for managing export policies.

If you want to…	Use this command…
Display information about export policies	`vserver export-policy show`
Rename an export policy	`vserver export-policy rename`
Copy an export policy	`vserver export-policy copy`
Delete an export policy	`vserver export-policy delete`

See the man page for each command for more information.

Commands for managing export rules

There are specific ONTAP commands for managing export rules.

If you want to…	Use this command…
Create an export rule	`vserver export-policy rule create`
Display information about export rules	`vserver export-policy rule show`
Modify an export rule	`vserver export-policy rule modify`
Delete an export rule	`vserver export-policy rule delete`

If you have configured multiple identical export rules matching different clients, be sure to keep them in sync when managing export rules.

See the man page for each command for more information.

Configure the NFS credential cache

Reasons for modifying the NFS credential cache time-to-live

ONTAP uses a credential cache to store information needed for user authentication for NFS export access to provide faster access and improve performance. You can configure how long information is stored in the credential cache to customize it for your environment.

There are several scenarios when modifying the NFS credential cache time-to-live (TTL) can help resolve issues. You should understand what these scenarios are as well as the consequences of making these modifications.

Reasons

Consider changing the default TTL under the following circumstances:

Issue	Remedial action
The name servers in your environment are experiencing performance degradation due to a high load of requests from ONTAP.	Increase the TTL for cached positive and negative credentials to reduce the number of requests from ONTAP to name servers.
The name server administrator made changes to allow access to NFS users that were previously denied.	Decrease the TTL for cached negative credentials to reduce the time NFS users have to wait for ONTAP to request fresh credentials from external name servers so they can get access.
The name server administrator made changes to deny access to NFS users that were previously allowed.	Reduce the TTL for cached positive credentials to reduce the time before ONTAP requests fresh credentials from external name servers so the NFS users are now denied access.

Consequences

You can modify the length of time individually for caching positive and negative credentials. However, you should be aware of both the advantages and disadvantages of doing so.

If you…	The advantage is…	The disadvantage is…
Increase the positive credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to deny access to NFS users that previously were allowed access but are not anymore.
Decrease the positive credential cache time	It takes less time to deny access to NFS users that previously were allowed access but are not anymore.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.

If you…	The advantage is…	The disadvantage is…
Increase the negative credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to grant access to NFS users that previously were not allowed access but are now.
Decrease the negative credential cache time	It takes less time to grant access to NFS users that previously were not allowed access but are now.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.

Configure the time-to-live for cached NFS user credentials

You can configure the length of time that ONTAP stores credentials for NFS users in its internal cache (time-to-live, or TTL) by modifying the NFS server of the storage virtual machine (SVM). This enables you to alleviate certain issues related to high load on name servers or changes in credentials affecting NFS user access.

About this task

These parameters are available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

If you want to modify the TTL for cached…	Use the command…
Positive credentials	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` The TTL is measured in milliseconds. The default is 24 hours (86,400,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).
Negative credentials	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` The TTL is measured in milliseconds. The default is 2 hours (7,200,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).

3. Return to the admin privilege level:

```
set -privilege admin
```

Manage export policy caches

Flush export policy caches

ONTAP uses several export policy caches to store information related to export policies for faster access. Flushing export policy caches manually (`vserver export-policy cache flush`) removes potentially outdated information and forces ONTAP to retrieve current information from the appropriate external resources. This can help resolve a variety of issues related to client access to NFS exports.

About this task

Export policy cache information might be outdated due to the following reasons:

- A recent change to export policy rules
- A recent change to host name records in name servers
- A recent change to netgroup entries in name servers
- Recovering from a network outage that prevented netgroups from being fully loaded

Steps

1. If you do not have name service cache enabled, perform one of the following actions in advance privilege mode:

If you want to flush…	Enter the command…
All export policy caches (except for showmount)	`vserver export-policy cache flush -vserver vserver_name`
The export policy rules access cache	`vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache.
The host name cache	`vserver export-policy cache flush -vserver vserver_name -cache host`
The netgroup cache	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. If name service cache is enabled, perform one of the following actions:

If you want to flush…	Enter the command…
The export policy rules access cache	`vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache.
The host name cache	`vserver services name-service cache hosts forward-lookup delete-all`
The netgroup cache	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Display the export policy netgroup queue and cache

ONTAP uses the netgroup queue when importing and resolving netgroups and it uses the netgroup cache to store the resulting information. When troubleshooting export policy netgroup related issues, you can use the `vserver export-policy netgroup queue show` and `vserver export-policy netgroup cache show` commands to display the status of the netgroup queue and the contents of the netgroup cache.

Step

1. Perform one of the following actions:

To display the export policy netgroup…	Enter the command…
Queue	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

See the man page for each command for more information.

Check whether a client IP address is a member of a netgroup

When troubleshooting NFS client access issues related to netgroups, you can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.

About this task

Checking netgroup membership enables you to determine whether ONTAP is aware that a client is or is not member of a netgroup. It also lets you know whether the ONTAP netgroup cache is in a transient state while refreshing netgroup information. This information can help you understand why a client might be unexpectedly granted or denied access.

Step

1. Check the netgroup membership of a client IP address: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   The command can return the following results:

   - The client is a member of the netgroup.

     This was confirmed through a reverse lookup scan or a netgroup-by-host search.

   - The client is a member of the netgroup.

     It was found in the ONTAP netgroup cache.

   - The client is not a member of the netgroup.
   - The membership of the client cannot yet be determined because ONTAP is currently refreshing the netgroup cache.

     Until this is done, membership cannot be explicitly ruled in or out. Use the `vserver export-policy netgroup queue show` command to monitor the loading of the netgroup and retry the check after it is finished.

Example

The following example checks whether a client with the IP address 172.17.16.72 is a member of the netgroup mercury on the SVM vs1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimize access cache performance

You can configure several parameters to optimize the access cache and find the right balance between performance and how current the information stored in the access cache is.

About this task

When you configure the access cache refresh periods, keep the following in mind:

- Higher values mean entries stay longer in the access cache.

  The advantage is better performance because ONTAP spends less resources on refreshing access cache entries. The disadvantage is that if export policy rules change and access cache entries become stale as a result, it takes longer to update them. As a result, clients that should get access might get denied, and clients that should get denied might get access.

- Lower values mean ONTAP refreshes access cache entries more often.

  The advantage is that entries are more current and clients are more likely to be correctly granted or denied access. The disadvantage is a decrease in performance because ONTAP spends more resources refreshing access cache entries.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

To modify the…	Enter…
Refresh period for positive entries	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Refresh period for negative entries	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Timeout period for old entries	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verify the new parameter settings:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Manage file locks

About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

How ONTAP treats read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

> Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How ONTAP differs from Windows on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the

SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply Windows Access Control List (ACL) security settings that prevent users or applications from renaming critical directories.

Learn more about How to prevent directories from being renamed while clients are accessing them.

Display information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. See the man page for the command for more information.

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------ ----------- --------- -----------
-------
vol1    /vol1/file1              lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                        delegation  -
               Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
```

```
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Breaking locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

   The man page for the command contains detailed information.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

3. Perform one of the following actions:

If you want to break a lock by specifying…	Enter the command…
The SVM name, volume name, LIF name, and file path	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
The lock ID	`vserver locks break -lockid UUID`

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

How FPolicy first-read and first-write filters work with NFS

NFS clients experience high response time during high traffic of read/write requests when the FPolicy is enabled using an external FPolicy server with read/write operations as monitored events. For NFS clients, the use of first-read and first-write filters in the FPolicy reduces the number of FPolicy notifications and improves performance.

In NFS, the client does I/O on a file by fetching its handle. This handle might remain valid across reboots of the server and the client. Therefore, the client is free to cache the handle and send requests on it without retrieving handles again. In a regular session, lots of reads/write requests are sent to the file server. If notifications are generated for all these requests, it might result in the following issues:

- A larger load due to additional notification processing, and higher response time.
- A large number of notifications being sent to the FPolicy server even though the server unaffected by all of the notifications.

After receiving the first read/write request from a client for a particular file, a cache entry is created and the read/write count is incremented. This request is marked as the first-read/write operation, and an FPolicy event is generated. Before you plan and create your FPolicy filters for an NFS client, you should understand the basics of how FPolicy filters work.

- First-read: Filters the client read requests for first-read.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file -session-io-grouping-duration` settings determine the first-read request for which FPolicy is processed.

- First-write: Filters the client write requests for first-write.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file -session-io-grouping-duration` settings determine the first-write request for which FPolicy processed.

The following options are added in NFS servers database.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modify the NFSv4.1 server implementation ID

The NFSv4.1 protocol includes a server implementation ID that documents the server domain, name, and date. You can modify the server implementation ID default values. Changing the default values can be useful, for example, when gathering usage statistics or troubleshooting interoperability issues. For more information, see RFC 5661.

About this task

The default values for the three options are as follows:

Option	Option name	Default value
NFSv4.1 Implementation ID Domain	`-v4.1-implementation -domain`	netapp.com
NFSv4.1 Implementation ID Name	`-v4.1-implementation-name`	Cluster version name
NFSv4.1 Implementation ID Date	`-v4.1-implementation-date`	Cluster version date

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to modify the NFSv4.1 implementation ID…	Enter the command…
Domain	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Manage NFSv4 ACLs

Benefits of enabling NFSv4 ACLs

There are many benefits to enabling NFSv4 ACLs.

The benefits of enabling NFSv4 ACLs include the following:

- Finer-grained control of user access for files and directories
- Better NFS security
- Improved interoperability with CIFS
- Removal of the NFS limitation of 16 groups per user

How NFSv4 ACLs work

A client using NFSv4 ACLs can set and view ACLs on files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, the new file or subdirectory inherits all ACL Entries (ACEs) in the ACL that have been tagged with the appropriate inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions, and whether the parent directory has an ACL:

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

  A parent ACL is inherited even if `-v4.0-acl` is set to `off`.

- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a non-inheritable ACL, the new object is created only with mode bits.

If the `-chown-mode` parameter has been set to `restricted` with commands in the `vserver nfs` or `vserver export-policy rule` families, file ownership can be changed by the superuser only, even if the on-disk permissions set with NFSv4 ACLs allow a non-root user to change the file ownership. For more information, see the relevant man pages.

Enable or disable modification of NFSv4 ACLs

When ONTAP receives a `chmod` command for a file or directory with an ACL, by default the ACL is retained and modified to reflect the mode bit change. You can disable the `-v4-acl-preserve` parameter to change the behavior if you want the ACL to be dropped instead.

About this task

When using unified security style, this parameter also specifies whether NTFS file permissions are preserved or dropped when a client sends a chmod, chgroup, or chown command for a file or directory.

The default for this parameter is enabled.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the following command…

Enable retention and modification of existing NFSv4 ACLs (default)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Disable retention and drop NFSv4 ACLs when changing mode bits	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Return to the admin privilege level:

```
set -privilege admin
```

How ONTAP uses NFSv4 ACLs to determine whether it can delete a file

To determine whether it can delete a file, ONTAP uses a combination of the file's DELETE bit, and the containing directory's DELETE_CHILD bit. For more information, see the NFS 4.1 RFC 5661.

Enable or disable NFSv4 ACLs

To enable or disable NFSv4 ACLs, you can modify the `-v4.0-acl` and `-v4.1-acl` options. These options are disabled by default.

About this task

The `-v4.0-acl` or `-v4.1-acl` option controls the setting and viewing of NFSv4 ACLs; it does not control enforcement of these ACLs for access checking.

Step

1. Perform one of the following actions:

If you want to…	Then…
Enable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Disable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Enable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

Disable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modify the maximum ACE limit for NFSv4 ACLs

You can modify the maximum number of allowed ACEs for each NFSv4 ACL by modifying the parameter `-v4-acl-max-aces`. By default, the limit is set to 400 ACEs for each ACL. Increasing this limit can help ensure successful migration of data with ACLs containing over 400 ACEs to storage systems running ONTAP.

About this task

Increasing this limit might impact performance for clients accessing files with NFSv4 ACLs.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Modify the maximum ACE limit for NFSv4 ACLs:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   The valid range of

   `max_ace_limit` is `192` to `1024`.

3. Return to the admin privilege level:

   `set -privilege admin`

Manage NFSv4 file delegations

Enable or disable NFSv4 read file delegations

To enable or disable NFSv4 read file delegations, you can modify the `-v4.0-read-delegation`or `-v4.1-read-delegation` option. By enabling read file delegations, you can eliminate much of the message overhead associated with the opening and closing of files.

About this task

By default, read file delegations are disabled.

The disadvantage of enabling read file delegations is that the server and its clients must recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

Step

1. Perform one of the following actions:

If you want to…	Then…
Enable NFSv4 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Enable NFSv4.1 read file delegations	Enter the following command: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Disable NFSv4 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Disable NFSv4.1 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

Enable or disable NFSv4 write file delegations

To enable or disable write file delegations, you can modify the `-v4.0-write -delegation`or `-v4.1-write-delegation` option. By enabling write file delegations, you can eliminate much of the message overhead associated with file and record locking in addition to opening and closing of files.

About this task

By default, write file delegations are disabled.

The disadvantage of enabling write file delegations is that the server and its clients must perform additional tasks to recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

Step

1. Perform one of the following actions:

If you want to…	Then…
Enable NFSv4 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`

If you want to…	Then…
Enable NFSv4.1 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Disable NFSv4 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Disable NFSv4.1 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

Configure NFSv4 file and record locking

About NFSv4 file and record locking

For NFSv4 clients, ONTAP supports the NFSv4 file-locking mechanism, maintaining the state of all file locks under a lease-based model.

NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

Specify the NFSv4 locking lease period

To specify the NFSv4 locking lease period (that is, the time period in which ONTAP irrevocably grants a lock to a client), you can modify the `-v4-lease-seconds` option. Shorter lease periods speed up server recovery while longer lease periods are beneficial for servers handling a very large amount of clients.

About this task

By default, this option is set to `30`. The minimum value for this option is `10`. The maximum value for this option is the locking grace period, which you can set with the `locking.lease_seconds` option.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Specify the NFSv4 locking grace period

To specify the NFSv4 locking grace period (that is, the time period in which clients attempt to reclaim their locking state from ONTAP during server recovery), you can modify the `-v4-grace-seconds` option.

About this task

By default, this option is set to `45`.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

How NFSv4 referrals work

When you enable NFSv4 referrals, ONTAP provides “intra-SVM” referrals to NFSv4 clients. Intra-SVM referral is when a cluster node receiving the NFSv4 request refers the NFSv4 client to another logical interface (LIF) on the storage virtual machine (SVM).

The NFSv4 client should access the path that received the referral at the target LIF from that point onward. The original cluster node provides such a referral when it determines that there exists a LIF in the SVM that is resident on the cluster node on which the data volume resides, thereby enabling the clients faster access to the data and avoiding extra cluster communication.

Enable or disable NFSv4 referrals

You can enable NFSv4 referrals on storage virtual machines (SVMs) by enabling the options `-v4-fsid-change` and `-v4.0-referrals`or `-v4.1-referrals`. Enabling NFSV4 referrals can result in faster data access for NFSv4 clients that support this feature.

What you’ll need

If you want to enable NFS referrals, you must first disable parallel NFS. You cannot enable both at the same time.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the command…
Enable NFSv4 referrals	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Disable NFSv4 referrals	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Enable NFSv4.1 referrals	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Disable NFSv4.1 referrals	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Display NFS statistics

You can display NFS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the NFS objects from which you can view data.

   ```
   statistics catalog object show -object nfs*
   ```

2. Use the `statistics start` and optional `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Example: Monitoring NFSv3 performance

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

Related information

Performance monitoring setup

Display DNS statistics

You can display DNS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the DNS objects from which you can view data.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Monitoring DNS statistics

The following examples show performance data for DNS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

The following command displays data from the sample by specifying counters that display the number of DNS queries sent versus the number of DNS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that display the number of times a specific error was received for a DNS query on the particular server:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Related information

Performance monitoring setup

Display NIS statistics

You can display NIS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the NIS objects from which you can view data.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Monitoring NIS statistics

The following examples display performance data for NIS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

The following command displays data from the sample by specifying counters that show the number of NIS queries sent versus the number of NIS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that show the number of times a specific error was received for a NIS query on the particular server:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                          YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

Related information

Performance monitoring setup

Support for VMware vStorage over NFS

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features in an NFS environment.

Supported features

The following features are supported:

- Copy offload

  Enables an ESXi host to copy virtual machines or virtual machine disks (VMDKs) directly between the source and destination data store location without involving the host. This conserves ESXi host CPU cycles and network bandwidth. Copy offload preserves space efficiency if the source volume is sparse.

- Space reservation

  Guarantees storage space for a VMDK file by reserving space for it.

Limitations

VMware vStorage over NFS has the following limitations:

- Copy offload operations can fail in the following scenarios:
  - While running wafliron on the source or destination volume because it temporarily takes the volume offline
  - While moving either the source or destination volume
  - While moving either the source or destination LIF
  - While performing takeover or giveback operations
  - While performing switchover or switchback operations
- Server-side copy can fail due to file handle format differences in the following scenario:

  You attempt to copy data from SVMs that have currently or had previously exported qtrees to SVMs that have never had exported qtrees. To work around this limitation, you can export at least one qtree on the destination SVM.

Related information

What VAAI offloaded operations are supported by Data ONTAP?

Enable or disable VMware vStorage over NFS

You can enable or disable support for VMware vStorage over NFS on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

About this task

By default, support for VMware vStorage over NFS is disabled.

Steps

1. Display the current vStorage support status for SVMs:

```
vserver nfs show -vserver vserver_name -instance
```

2. Perform one of the following actions:

If you want to…	Enter the following command…
Enable VMware vStorage support	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Disable VMware vStorage support	`vserver nfs modify -vserver vserver_name -vstorage disabled`

After you finish

You must install the NFS Plug-in for VMware VAAI before you can use this functionality. For more information, see *Installing the NetApp NFS Plug-in for VMware VAAI*.

Related information

NetApp Documentation: NetApp NFS Plug-in for VMware VAAI

Enable or disable rquota support

ONTAP supports the remote quota protocol version 1 (rquota v1). The rquota protocol enables NFS clients to obtain quota information for users from a remote machine. You can enable rquota on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

About this task

By default, rquota is disabled.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Enable rquota support for SVMs	`vserver nfs modify -vserver vserver_name -rquota enable`
Disable rquota support for SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

For more information about quotas, see Logical storage management.

NFSv3 and NFSv4 performance improvement by modifying the TCP transfer size

You can improve the performance of NFSv3 and NFSv4 clients connecting to storage systems over a high-latency network by modifying the TCP maximum transfer size.

When clients access storage systems over a high-latency network, such as a wide area network (WAN) or

metro area network (MAN) with a latency over 10 milliseconds, you might be able to improve the connection performance by modifying the TCP maximum transfer size. Clients accessing storage systems in a low-latency network, such as a local area network (LAN), can expect little to no benefit from modifying these parameters. If the throughput improvement does not outweigh the latency impact, you should not use these parameters.

To determine whether your storage environment would benefit from modifying these parameters, you should first conduct a comprehensive performance evaluation of a poorly performing NFS client. Review whether the low performance is because of excessive round trip latency and small request on the client. Under these conditions, the client and server cannot fully use the available bandwidth because they spend the majority of their duty cycles waiting for small requests and responses to be transmitted over the connection.

By increasing the NFSv3 and NFSv4 request size, the client and server can use the available bandwidth more effectively to move more data per unit time; therefore, increasing the overall efficiency of the connection.

Keep in mind that the configuration between the storage system and the client might vary. The storage system and the client supports maximum size of 1 MB for transfer operations. However, if you configure the storage system to support 1 MB maximum transfer size but the client only supports 64 KB, then the mount transfer size is limited to 64 KB or less.

Before modifying these parameters, you must be aware that it results in additional memory consumption on the storage system for the period of time necessary to assemble and transmit a large response. The more high-latency connections to the storage system, the higher the additional memory consumption. Storage systems with high memory capacity might experience very little effect from this change. Storage systems with low memory capacity might experience noticeable performance degradation.

The successful use of these parameter relies on the ability to retrieve data from multiple nodes of a cluster. The inherent latency of the cluster network might increase the overall latency of the response. Overall latency tends to increase when using these parameters. As a result, latency sensitive workloads might show negative impact.

Modify the NFSv3 and NFSv4 TCP maximum transfer size

You can modify the `-tcp-max-xfer-size` option to configure maximum transfer sizes for all TCP connections using the NFSv3 and NFSv4.x protocols.

About this task

You can modify these options individually for each storage virtual machine (SVM).

Beginning with ONTAP 9, the `v3-tcp-max-read-size` and `v3-tcp-max-write-size` options are obsolete. You must use the `-tcp-max-xfer-size` option instead.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the command…
Modify the NFSv3 or NFSv4 TCP maximum transfer size	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Range	Default
`-tcp-max-xfer-size`	8192 to 1048576 bytes	65536 bytes

The maximum transfer size that you enter must be a multiple of 4 KB (4096 bytes). Requests that are not properly aligned negatively affect performance.

3. Use the `vserver nfs show -fields tcp-max-xfer-size` command to verify the changes.
4. If any clients use static mounts, unmount and remount for the new parameter size to take effect.

Example

The following command sets the NFSv3 and NFSv4.x TCP maximum transfer size to 1048576 bytes on the SVM named vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure the number of group IDs allowed for NFS users

By default, ONTAP supports up to 32 group IDs when handling NFS user credentials using Kerberos (RPCSEC_GSS) authentication. When using AUTH_SYS authentication, the default maximum number of group IDs is 16, as defined in RFC 5531. You can increase the maximum up to 1,024 if you have users who are members of more than the default number of groups.

About this task

If a user has more than the default number of group IDs in their credentials, the remaining group IDs are truncated and the user might receive errors when attempting to access files from the storage system. You should set the maximum number of groups, per SVM, to a number that represents the maximum groups in your environment.

The following table shows the two parameters of the `vserver nfs modify` command that determine the maximum number of group IDs in three sample configurations:

Parameters	Settings	Resulting group IDs limit

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	These are the default settings.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Some older NFS clients might not be compatible with AUTH_SYS extended groups.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

If you want to set the maximum number of allowed auxiliary groups…	Enter the command…
Only for RPCSEC_GSS and leave AUTH_SYS set to the default value of 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
For both RPCSEC_GSS and AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verify the `-extended-groups-limit` value and verify whether AUTH_SYS is using extended groups: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following example enables extended groups for AUTH_SYS authentication and sets the maximum number of extended groups to 512 for both AUTH_SYS and RPCSEC_GSS authentication. These changes are made only for clients who access the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Control root user access to NTFS security-style data

You can configure ONTAP to allow NFS clients access to NTFS security-style data and NTFS clients to access NFS security-style data. When using NTFS security style on an NFS data store, you must decide how to treat access by the root user and configure the storage virtual machine (SVM) accordingly.

About this task

When a root user accesses NTFS security-style data, you have two options:

- Map the root user to a Windows user like any other NFS user and manage access according to NTFS ACLs.
- Ignore NTFS ACLs and provide full access to root.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

If you want the root user to…	Enter the command…
Be mapped to a Windows user	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Bypass the NT ACL check	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   By default, this parameter is disabled.

If this parameter is enabled but there is no name mapping for the root user, ONTAP uses a default SMB administrator credential for auditing.

3. Return to the admin privilege level:

```
set -privilege admin
```

Appendix: Supported NFS versions and clients

Appendix: Supported NFS versions and clients

Before you can use NFS in your network, you need to know which NFS versions and clients ONTAP supports.

This table notes when major and minor NFS protocol versions are supported by default in ONTAP. Support by default does not indicate that this is the earliest version of ONTAP supporting that NFS protocol.

Version	Enabled by default
NFSv3	Yes
NFSv4.0	Yes, beginning with ONTAP 9.9.1
NFSv4.1	Yes, beginning with ONTAP 9.9.1
NFSv4.2	Yes, beginning with ONTAP 9.9.1
pNFS	No

For the latest information about which NFS clients ONTAP supports, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

NFSv4.0 functionality supported by ONTAP

ONTAP supports all the mandatory functionality in NFSv4.0 except the SPKM3 and LIPKEY security mechanisms.

The following NFSV4 functionality is supported:

- **COMPOUND**

  Allows a client to request multiple file operations in a single remote procedure call (RPC) request.

- **File delegation**

  Allows the server to delegate file control to some types of clients for read and write access.

- **Pseudo-fs**

  Used by NFSv4 servers to determine mount points on the storage system. There is no mount protocol in

NFSv4.

- **Locking**

  Lease-based. There are no separate Network Lock Manager (NLM) or Network Status Monitor (NSM) protocols in NFSv4.

For more information about the NFSv4.0 protocol, see RFC 3530.

Limitations of ONTAP support for NFSv4

You should be aware of several limitations of ONTAP support for NFSv4.

- The delegation feature is not supported by every client type.
- In ONTAP 9.4 and earlier releases, names with non-ASCII characters on volumes other than UTF8 volumes are rejected by the storage system.

  In ONTAP 9.5 and later releases, volumes created with the utf8mb4 language setting and mounted using NFS v4 are no longer subject to this restriction.

- All file handles are persistent; the server does not give volatile file handles.
- Migration and replication are not supported.
- NFSv4 clients are not supported with read-only load-sharing mirrors.

  ONTAP routes NFSv4 clients to the source of the load-sharing mirror for direct read and write access.

- Named attributes are not supported.
- All recommended attributes are supported, except for the following:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

  Although it does not support the `quota*` attributes, ONTAP does support user and group quotas through the RQUOTA side band protocol.

ONTAP support for NFSv4.1

Beginning with ONTAP 9.8, nconnect functionality is available by default when NFSv4.1 is enabled.

Earlier NFS client implementations use only a single TCP connection with a mount. In ONTAP, a single TCP connection can become a bottleneck with increasing IOPS. However, an nconnect-enabled client can have multiple TCP connections (up to 16) associated with a single NFS mount. Such an NFS client multiplexes file operations onto multiple TCP connections in a round-robin fashion and thus obtains higher throughput from the available network bandwidth. Nconnect is recommended for NFSv3 and NFSv4.1 mounts only.

See your NFS client documentation to confirm whether nconnect is supported in your client version.

NFSv4.1 is enabled by default in ONTAP 9.9.1 and later. In earlier releases, you can enable it by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM).

ONTAP does not support NFSv4.1 directory and file level delegations.

ONTAP support for NFSv4.2

Beginning with ONTAP 9.8, the NFSv4.2 protocol is supported to allow access for NFSv4.2 clients.

NFSv4.2 is enabled by default in ONTAP 9.9.1 and later. In ONTAP 9.8, you can enable v4.2 by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM). Enabling NFSv4.1 also enables clients to use the NFSv4.1 features while mounted as v4.2.

The following NFSv4.2 optional features are supported:

- Beginning with ONTAP 9.9.1, Mandatory Access Control (MAC) labelled NFS is supported when NFSv4.2 is enabled.
- Additional NFSv4.2 optional features will be added in a later ONTAP release.

Enable NFS v4.2 security labels

Beginning with ONTAP 9.9.1, NFS security labels can be enabled. They are disabled by default.

With NFS v4.2 security labels, ONTAP NFS servers are Mandatory Access Control (MAC) aware, storing and retrieving sec_label attributes sent by clients.

For more information, see RFC7240

> NFS v4.2 security labels are not currently supported for NDMP dump operations. If security labels are encountered on files or directories, the dump fails.

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Enable security labels:

   ```
   vserver nfs modify -vserver svm_name -v4.2-seclabel enabled
   ```

ONTAP support for parallel NFS

ONTAP supports parallel NFS (pNFS). The pNFS protocol offers performance

improvements by giving clients direct access to the data of a set of files distributed across multiple nodes of a cluster. It helps clients locate the optimal path to a volume.

Use of hard mounts

When troubleshooting mounting problems, you need to be sure that you are using the correct mount type. NFS supports two mount types: soft mounts and hard mounts. You should use only hard mounts for reliability reasons.

You should not use soft mounts, especially when there is a possibility of frequent NFS timeouts. Race conditions can occur as a result of these timeouts, which can lead to data corruption.

Appendix: NFS and SMB file and directory naming dependencies

Appendix: NFS and SMB file and directory naming dependencies

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and qtree names, depending on the ONTAP release.

Characters a file or directory name can use

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

Case-sensitivity of file and directory names in a multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.

- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
  - On SMB clients, you see `testdir` and `TESTDI~1`.
  - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

    In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `text.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
  - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
  - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.

If you have enabled or modified character mapping using the Vserver CIFS character-mapping commands, a normally case-insensitive Windows lookup becomes case-sensitive.

How ONTAP creates file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

  If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.
- In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

How ONTAP handles multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary

characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

- You must create a new volume in one of the following ways:
- Setting the volume `-language` option explicitly:

  ```
  volume create -language utf8mb4 {…}
  ```

- Inheriting the volume `-language` option from an SVM that has been created with or modified for the option:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- You cannot modify existing volumes for utf8mb4 support; you must create a new utf8mb4-ready volume, and then migrate the data using client-based copy tools.

  You can update SVMs for utf8mb4 support, but existing volumes retain their original language codes.

  LUN names with 4-byte UTF-8 characters are not currently supported.

- Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

  In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

- When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

  To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Unicode characters are allowed in qtree names.

- You can use either the `volume qtree` command family or System Manager to set or modify qtree names.
- qtree names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.

In releases before ONTAP 9.5, the junction-path of the qtree's parent volume can contain qtree and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in qtree names, provided that the qtree is in a volume enabled for utf8mb4.

Configure character mapping for SMB file name translation on volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

  You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

  For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named "a-b" would have its request mapped to the NFS name of "a:b" (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.
- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

Step

1. Configure character mapping:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

   The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

   - Source mapping

     The following table shows the permissible Unicode character set for source mapping:

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C	\	Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark
0x3C	<	Less than
0x3E	>	Greater than
0x7C	|	Vertical line
0xB1	±	Plus-minus sign

   - Target mapping

     You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000…U+F8FF.

Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to…	Use this command…
Create new file character mappings	`vserver cifs character-mapping create`
Display information about file character mappings	`vserver cifs character-mapping show`
Modify existing file character mappings	`vserver cifs character-mapping modify`
Delete file character mappings	`vserver cifs character-mapping delete`

For more information, see the man page for each command.

Manage NFS over RDMA

NFS over RDMA

NFS over RDMA utilizes RDMA adapters, allowing data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead.

NFS over RDMA configurations are designed for customers with latency sensitive or high-bandwidth workloads such as machine learning and analytics. NVIDIA has extended NFS over RDMA to enable GPU Direct Storage (GDS). GDS further accelerates GPU-enabled workloads by bypassing the CPU and main memory altogether, using RDMA to transfer data between the storage system and GPU memory directly.

NFS over RDMA is supported beginning with ONTAP 9.10.1. NFS over RDMA configurations are only supported for the NFSv4.0 protocol when used with the Mellanox CX-5 or CX-6 adapter, which provides support for RDMA using version 2 of the RoCE protocol. GDS is only supported using NVIDIA Tesla- and Ampere-family GPUs with Mellanox NIC cards and MOFED software. NFS over RDMA support is limited to node-local traffic only. Standard FlexVols or FlexGroups where all constituents are on the same node are supported and must be accessed from a LIF on the same node. NFS mount sizes higher than 64k result in

unstable performance with NFS over RDMA configurations.

Requirements

- Storages systems must be running ONTAP 9.10.1.
  - You can configure NFS over RDMA with System Manager beginning with ONTAP 9.12.1. In ONTAP 9.10.1 and 9.11.1, you need to use the CLI to configure NFS over RDMA.
- Both nodes in the HA pair must be the same version.
- Storage system controllers must have RDMA support (currently A400, A700, and A800).
- Storage appliance configured with RDMA-supported hardware (e.g. Mellanox CX-5 or CX-6).
- Data LIFs must be configured to support RDMA.
- Clients must be using Mellanox RDMA-capable NIC cards and Mellanox OFED (MOFED) network software.

Next Steps

- Configure NICs for NFS over RDMA
- Configure LIFs for NFS over RDMA
- NFS settings for NFS over RDMA

Further reading

- RDMA
- RFC 7530: NFS Version 4 Protocol
- RFC 8166: Remote Direct Memory Access Transport for Remote Procedure Call Version 1
- RFC 8167: Bidirectional Remote Procedure Call on RPC-over-RDMA Transports
- RFC 8267: NFS Upper-Layer Binding to RPC-over-RDMA version 1

Configure NICs for NFS over RDMA

NFS over RDMA requires NIC configuration for both the client system and storage platform.

Storage platform configuration

An X1148 RDMA adapter needs to be installed on the server. If you are using an HA configuration, you must have a corresponding X1148 adapter on the failover partner so RDMA service can continue during failover. The NIC must be ROCE capable.

Beginning with ONTAP 9.10.1, you can view a list of RDMA offload protocols with the command:
`network port show -rdma-protocols roce`

Client system configuration

Clients must be using Mellanox RDMA-capable NIC cards (e.g. X1148) and Mellanox OFED network software. Consult Mellanox documentation for supported models and versions. Although the client and server can be directly connected, the use of switches is recommended due to improved failover performance with a switch.

The client, server, and any switches, and all ports on switches must be configured using Jumbo frames. Also ensure that priority flow-control is in effect on any switches.

Once this configuration is confirmed, you can mount the NFS.

System Manager

You must be using ONTAP 9.12.1 or later to configure network interfaces with NFS over RDMA using System Manager.

Steps

1. Check if RDMA is supported. Navigate to **Network > Ethernet Ports** and select the appropriate node in the group view. When you expand the node, look at the **RDMA protocols** field for a given port: the value **RoCE** denotes RDMA is supported; a dash (**-**) indicates it is not supported.
2. To add a VLAN, select **+ VLAN**. Select the appropriate node. In the **Port** dropdown menu, the available ports will display the text **RoCE Enabled** if they support RDMA; no text will be displayed if they do not support RDMA.
3. Follow the workflow in Enable NAS storage for Linux servers using NFS to configure a new NFS server.

   When adding network interfaces, you will have the option to select **Use RoCE ports**. Select this option for any network interfaces that you want to use NFS over RDMA.

CLI

1. Check if RDMA access is enabled on the NFS server with the command:

   ```
   vserver nfs show-vserver SVM_name
   ```

   By default, `-rdma` should be enabled. If it is not, enable RDMA access on the NFS server:

   ```
   vserver nfs modify -vserver SVM_name -rdma enabled
   ```

2. Mount the client via NFSv4.0 over RDMA:
   a. The input for the proto parameter depends on the server IP protocol version. If it is IPv4, use `proto=rdma`. If it is IPv6, use `proto=rdma6`.
   b. Specify the NFS target port as `port=20049` instead of the standard port 2049:

      ```
      mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address
      :/volume_path mount_point
      ```

3. **OPTIONAL**: If you need to unmount the client, run the command `unmount mount_path`

More information

- Create an NFS server
- Enable NAS storage for Linux servers using NFS

Configure LIFs for NFS over RDMA

To utilize NFS over RDMA, you must configure your LIFs (network interface) to be RDMA compatible. Both the LIF and its failover pair must be capable of supporting RDMA.

Create a new LIF

System Manager

You must be using ONTAP 9.12.1 or later to create a network interface for NFS over RDMA with System Manager.

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select + Add .
3. When you select **NFS,SMB/CIFS,S3**, you will have the option to **Use RoCE ports**. Select the checkbox for **Use RoCE ports**.
4. Select the storage VM and home node. Assign a name. Enter the IP address and subnet mask.
5. Once you enter the IP address and subnet mask, System Manager will filter the list of broadcast domains to those that have RoCE capable ports. Select a broadcast domain. You can optionally add a gateway.
6. Select **Save**.

CLI

Steps

1. Create a LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - The service policy must be either default-data-files or a custom policy that includes the data-nfs network interface service.
   - The `-rdma-protocols` parameter accepts a list, which is by default empty. When `roce` is added as a value, the LIF can only be configured on ports supporting RoCE offload, affecting bot LIF migration and failover.

Modify a LIF

System Manager

You must be using ONTAP 9.12.1 or later to create a network interface for NFS over RDMA with System Manager.

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **> Edit** beside the network interface you want to change.
3. Check **Use RoCE Ports** to enable NFS over RDMA or uncheck the box to disable it. If the network interface is on a RoCE capable port, you will see a checkbox next to **Use RoCE ports**.
4. Modify the other settings as needed.
5. Select **Save** to confirm your changes.

CLI

1. You can check the status of your LIFs with the `network interface show` command. The service policy must include the data-nfs network interface service. The `-rdma-protocols` list should include `roce`. If either of these conditions are untrue, modify the LIF.
2. To modify the LIF, run:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

Modifying a LIF to require a particular offload protocol when the LIF is not currently assigned to a port that supports that protocol will produce an error.

Migrate a LIF

ONTAP also allows you to migrate network interfaces (LIFs) to utilize NFS over RDMA. When performing this migration, you must ensure the destination port is RoCE capable. Beginning in ONTAP 9.12.1, you can complete this procedure in System Manager. When selecting a destination port for the network interface, System Manager will designate whether ports are RoCE capable.

You can only migrate a LIF to an NFS over RDMA configuration if:

- It is an NFS RDMA network interface (LIF) hosted on a RoCE capable port.
- It is an NFS TCP network interface (LIF) hosted on a RoCE capable port.
- It is an NFS TCP network interface (LIF) hosted on a non-RoCE capable port.

For more information about migrating a network interface, refer to Migrate a LIF.

More Information

- Create a LIF
- Create a LIF
- Modify a LIF
- Migrate a LIF

Modify the NFS configuration

In most cases, you will not need to modify the configuration of the NFS-enabled storage VM for NFS over RDMA.

If you are, however, dealing with issues related to Mellanox chips and LIF migration, you should increase the NFSv4 locking grace period. By default, the grace period is set to 45 seconds. Beginning with ONTAP 9.10.1, the grace period has a maximum value of 180 (seconds).

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

For more information about this task, see Specifying the NFSv4 locking grace period.

Configure SMB with the CLI

SMB configuration overview with the CLI

You can use ONTAP 9 CLI commands to configure SMB client access to files contained in a new volume or qtree in a new or existing SVM.

SMB (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

Use these procedures if you want to configure SMB access to a volume or qtree in the following way:

- You want to use SMB version 2 or later.
- You want to serve SMB clients only, not NFS clients (not a multiprotocol configuration).
- NTFS file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

  Cluster administrator privileges are required to create SVMs and LIFs. SVM administrator privileges are sufficient for other SMB configuration tasks.

- You want to use the CLI, not System Manager or an automated scripting tool.

  To use System Manager to configure NAS multiprotocol access, see Provision NAS storage for both Windows and Linux using both NFS and SMB.

- You want to use best practices, not explore every available option.

  Details about command syntax are available from CLI help and ONTAP man pages.

If you want details about the range of ONTAP SMB protocol capabilities, consult the SMB reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Windows servers using SMB
System Manager Classic (available with ONTAP 9.7 and earlier)	SMB configuration overview

SMB configuration workflow

Configuring SMB involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal; configuring SMB access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for SMB access.

Preparation

Assess physical storage requirements

Before provisioning SMB storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

Steps

1. Display available space in existing aggregates: `storage aggregate show`

   If there is an aggregate with sufficient space, record its name in the worksheet.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

Assess networking requirements

Before providing SMB storage to clients, you must verify that networking is correctly configured to meet the SMB provisioning requirements.

Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

Steps

1. Display the available physical and virtual ports: `network port show`
   - When possible, you should use the port with the highest speed for the data network.
   - All components in the data network must have the same MTU setting for best performance.
2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: `network subnet show`

   Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

3. Display available IPspaces: `network ipspace show`

   You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster: `network options ipv6 show`

   If required, you can enable IPv6 by using the `network options ipv6 modify` command.

Decide where to provision new SMB storage capacity

Before you create a new SMB volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has SMB enabled but not configured, complete the steps in both “Configuring SMB access to an SVM” and “Adding storage capacity to an SMB-enabled SVM”.

  Configuring SMB access to an SVM

  Configuring SMB client access to shared storage

  You might choose to create a new SVM if one of the following is true:

  - You are enabling SMB on a cluster for the first time.
  - You have existing SVMs in a cluster in which you do not want to enable SMB support.
  - You have one or more SMB-enabled SVMs in a cluster, and you want one of the following connections:
    - To a different Active Directory forest or workgroup.
    - To an SMB server in an isolated namespace (multi-tenancy scenario).
      You should also choose this option to provision storage on an existing SVM that has SMB enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

  After enabling SMB on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for SMB access, complete the steps in “Adding storage capacity to an SMB-enabled SVM”.

  Configuring SMB client access to shared storage

Worksheet for gathering SMB configuration information

The SMB configuration worksheet enables you to collect the required information to set up SMB access for clients.

You should complete one or both sections of the worksheet, depending on the decision you made about where to provision storage:

- If you are configuring SMB access to an SVM, you should complete both sections.

Configuring SMB access to an SVM

Configuring SMB client access to shared storage

- If you are adding storage capacity to an SMB-enabled SVM, you should complete only the second section.

  Configuring SMB client access to shared storage

The command man pages contain details about the parameters.

Configuring SMB access to an SVM

Parameters for creating an SVM

You supply these values with the `vserver create` command if you are creating a new SVM.

Field	Description	Your value
`-vserver`	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for new SMB storage capacity.	
`-rootvolume`	A unique name you supply for the SVM root volume.	
`-rootvolume-security-style`	Use the NTFS security style for the SVM.	`ntfs`
`-language`	Use the default language setting in this workflow.	`C.UTF-8`
`ipspace`	Optional: IPspaces are distinct IP address spaces in which SVMs reside.	

Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs.

Field	Description	Your value
`-lif`	A name you supply for the new LIF.	

Field	Description	Your value
`-role`	Use the data LIF role in this workflow.	`data`
`-data-protocol`	Use only the SMB protocol in this workflow.	`cifs`
`-home-node`	The node to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-home-port`	The port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-address`	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
`-netmask`	The network mask and gateway for the LIF.	
`-subnet`	A pool of IP addresses. Used instead of `-address` and `-netmask` to assign addresses and netmasks automatically.	
`-firewall-policy`	Use the default data firewall policy in this workflow.	`data`
`-auto-revert`	Optional: Specifies whether a data LIF is automatically reverted to its home node on startup or under other circumstances. The default setting is `false`.	

Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS.

Field	Description	Your value
`-domains`	Up to five DNS domain names.	

Field	Description	Your value
`-name-servers`	Up to three IP addresses for each DNS name server.	

Setting up an SMB server in an Active Directory domain

Parameters for time service configuration

You supply these values with the `cluster time-service ntp server create` command when you are configuring time services.

Field	Description	Your value
`-server`	The host name or IP address of the NTP server for the Active Directory domain.	

Parameters for creating an SMB server in an Active Directory domain

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify domain information.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	
`-domain`	The fully qualified domain name (FQDN) of the Active Directory domain to associate with the SMB server.	
`-ou`	Optional: The organizational unit within the Active Directory domain to associate with the SMB server. By default, this parameter is set to CN=Computers.	
`-netbios-aliases`	Optional: A list of NetBIOS aliases, which are alternate names to the SMB server name.	
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Parameters for creating an SMB server in a workgroup

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify supported SMB versions.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	
`-workgroup`	The name of the workgroup (up to 15 characters).	
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Parameters for creating local users

You supply these values when you create local users by using the `vserver cifs users-and-groups local-user create` command. They are required for SMB servers in workgroups and optional in AD domains.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local user.	
`-user-name`	The name of the local user (up to 20 characters).	
`-full-name`	Optional: The user's full name. If the full name contains a space, enclose the full name within double quotation marks.	
`-description`	Optional: A description for the local user. If the description contains a space, enclose the parameter in quotation marks.	

Field	Description	Your value
`-is-account-disabled`	Optional: Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.	

Parameters for creating local groups

You supply these values when you create local groups by using the `vserver cifs users-and-groups local-group create` command. They are optional for SMB servers in AD domains and workgroups.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local group.	
`-group-name`	The name of the local group (up to 256 characters).	
`-description`	Optional: A description for the local group. If the description contains a space, enclose the parameter in quotation marks.	

Adding storage capacity to an SMB-enabled SVM

Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a qtree.

Field	Description	Your value
`-vserver`	The name of a new or existing SVM that will host the new volume.	
`-volume`	A unique descriptive name you supply for the new volume.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for the new SMB volume.	
`-size`	An integer you supply for the size of the new volume.	
`-security-style`	Use the NTFS security style for this workflow.	`ntfs`

Field	Description	Your value
`-junction-path`	Location under root (/) where the new volume is to be mounted.	

Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume.

Field	Description	Your value
`-vserver`	The name of the SVM on which the volume containing the qtree resides.	
`-volume`	The name of the volume that will contain the new qtree.	
`-qtree`	A unique descriptive name you supply for the new qtree, 64 characters or less.	
`-qtree-path`	The qtree path argument in the format `/vol/volume_name/qtree_name\>` can be specified instead of specifying volume and qtree as separate arguments.	

Parameters for creating SMB shares

You supply these values with the `vserver cifs share create` command.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB share.	
`-share-name`	The name of the SMB share that you want to create (up to 256 characters).	
`-path`	The name of the path to the SMB share (up to 256 characters). This path must exist in a volume before creating the share.	

Field	Description	Your value
`-share-properties`	Optional: A list of share properties. The default settings are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.	
`-comment`	Optional: A text comment for the server (up to 256 characters). Windows clients can see this SMB share description when browsing on the network.	

Parameters for creating SMB share access control lists (ACLs)

You supply these values with the `vserver cifs share access-control create` command.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB ACL.	
`-share`	The name of the SMB share on which to create.	
`-user-group-type`	The type of the user or group to add to the share's ACL. The default type is `windows`	`windows`
`-user-or-group`	The user or group to add to the share's ACL. If you specify the user name, you must include the user's domain using the "domain\username" format.	
`-permission`	Specifies the permissions for the user or group.	`[ No_access | Read | Change | Full_Control ]`

Configure SMB access to an SVM

Configure SMB access to an SVM

If you do not already have an SVM configured for SMB client access, you must either create and configure a new SVM or configure an existing SVM. Configuring SMB involves opening SVM root volume access, creating an SMB server, creating a LIF, enabling host-name resolution, configuring name services, and if desired, enabling Kerberos security.

Create an SVM

If you do not already have at least one SVM in a cluster to provide data access to SMB clients, you must create one.

Steps

1. Create an SVM: `vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - Use the NTFS setting for the `-rootvolume-security-style` option.
   - Use the default C.UTF-8 `-language` option.
   - The `ipspace` setting is optional.
2. Verify the configuration and status of the newly created SVM: `vserver show -vserver vserver_name`

   The `Allowed Protocols` field must include CIFS. You can edit this list later.

   The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

Verify that the SMB protocol is enabled on the SVM

Before you can configure and use SMB on SVMs, you must verify that the protocol is enabled.

About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.

> You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

Steps

1. Check which protocols are currently enabled and disabled for the SVM: `vserver show -vserver vserver_name -protocols`

   You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:
   - To enable the SMB protocol: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - To disable a protocol: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirm that the enabled and disabled protocols were updated correctly: `vserver show -vserver vserver_name -protocols`

Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

The following command allows access over SMB by adding `cifs` to the list of enabled protocols on the SVM named vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Open the export policy of the SVM root volume

The default export policy of the SVM root volume must include a rule to allow all clients open access through SMB. Without such a rule, all SMB clients are denied access to the SVM and its volumes.

About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that all SMB access is open in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

Steps

1. If you are using an existing SVM, check the default root volume export policy: `vserver export-policy rule show`

   The command output should be similar to the following:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verify rule creation by using the `vserver export-policy rule show` command.

Results

Any SMB client can now access any volume or qtree created on the SVM.

Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each

node by using the `network interface capacity details show` command (at the advanced privilege level).

- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM

Steps

1. Create a LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

   ONTAP 9.5 and earlier

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

   ONTAP 9.6 and later

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-service-policy` *`service_policy_name`* `-home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall-policy data -auto-revert {true|false}`

   - The `-role` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).
   - The `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.

     The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).

   - `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` man page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default `data` as the LIF role.

  You can create and add a custom firewall policy later if desired.

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

2. Verify that the LIF was created successfully:

   `network interface show`

3. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

The following command shows how to create a NAS data LIF that is assigned with the `default-data-files` service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Enable DNS for host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

About this task

The *Network Management Guide* contains information about configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   The following command enables external DNS server servers on the SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   Beginning with ONTAP 9.2, the `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command. ``

   The following command displays the DNS configurations for all SVMs in the cluster:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

   The `vserver services name-service dns check` command is available beginning with ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Set up an SMB server in an Active Directory domain

Configure time services

Before creating an SMB server in an Active Domain controller, you must ensure that the cluster time and the time on the domain controllers of the domain to which the SMB server will belong matches to within five minutes.

About this task

You should configure cluster NTP services to use the same NTP servers for time synchronization that the Active Directory domain uses.

Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

Steps

1. Configure time services by using the `cluster time-service ntp server create` command.
   - To configure time services without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_ip_address`
   - To configure time services with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`

2. Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this…	Use this command…
Configure an NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`
Configure an NTP server with symmetric authentication	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Enable symmetric authentication for an existing NTP serverAn existing NTP server can be modified to enable authentication by adding the required key-id.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure a server with a key ID not configured on the NTP server.	`cluster time-service ntp server create -server server_name -key-id key_id` The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.

To do this…	Use this command…
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -authentication disabled`

Create an SMB server in an Active Directory domain

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the Active Directory (AD) domain to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM and to an AD domain controller of the domain to which you want to join the SMB server.

Any user who is authorized to create machine accounts in the AD domain to which you are joining the SMB server can create the SMB server on the SVM. This can include users from other domains.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

About this task

When creating an SMB server in an Activity Directory domain:

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default setting is to add the SMB server machine account to the Active Directory CN=Computer object.
- You can choose to add the SMB server to a different organizational unit (OU) by using the `-ou` option.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the SMB server.

  Configuring NetBIOS aliases for an SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original servers' names.

The `vserver cifs` man pages contain additional optional parameters and naming requirements.

Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller (DC). Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default.

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted. ONTAP requires encryption for domain controller communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3. .

SMB management contains more information about SMB server configuration options.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   If it is not, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in an AD domain: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   When joining a domain, this command might take several minutes to finish.

   The following command creates the SMB server “smb_server01” in the domain “example.com”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   The following command creates the SMB server “smb_server02” in the domain “mydomain.com” and authenticates the ONTAP administrator with a keytab file:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In this example, the command output shows that an SMB server named “SMB_SERVER01” was created on SVM vs1.example.com, and was joined to the “example.com” domain.

   ```
   cluster1::> vserver cifs show -vserver vs1

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                              Authentication Style: domain
                 CIFS Server Administrative Status: up
                           CIFS Server Description: -
                           List of NetBIOS Aliases: -
   ```

4. If desired, enable encrypted communication with the domain controller (ONTAP 9.8 and later): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Examples

The following command creates a SMB server named “smb_server02” on SVM vs2.example.com in the “example.com” domain. The machine account is created in the “OU=eng,OU=corp,DC=example,DC=com” container. The SMB server is assigned a NetBIOS alias.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

The following command enables a user from a different domain, in this case an administrator of a trusted domain, to create a SMB server named “smb_server03” on SVM vs3.example.com. The `-domain` option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the SMB server. The `username` option specifies the administrator of the trusted domain.

- Home domain: example.com
- Trusted domain: trust.lab.com
- Username for the trusted domain: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Create keytab files for SMB authentication

Beginning with ONTAP 9.7, ONTAP supports SVM authentication with Active Directory (AD) servers using keytab files. AD administrators generate a keytab file and make it available to ONTAP administrators as a uniform resource identifier (URI), which is supplied when `vserver cifs` commands require Kerberos authentication with the AD domain.

AD administrators can create the keytab files using the standard Windows Server `ktpass` command. The command should be run on the primary domain where authentication is required. The `ktpass` command can be used to generate keytab files only for primary domain users; keys generated using trusted-domain users are not supported.

Keytab files are generated for specific ONTAP admin users. As long as the admin user's password does not change, the keys generated for the specific encryption type and domain will not change. Therefore, a new keytab file is required whenever the admin user's password is changed.

The following encryption types are supported:

- AES256-SHA1
- DES-CBC-MD5

  ONTAP does not support DES-CBC-CRC encryption type.

- RC4-HMAC

AES256 is the highest encryption type and should be used if enabled on the ONTAP system.

Keytab files can be generated by specifying either the admin password or by using a randomly-generated password. However, at any given time only one password option can be used, because a private key specific to the admin user is needed at the AD server for decrypting the keys inside the keytab file. Any change in the private key for a specific admin will invalidate the keytab file.

Set up an SMB server in a workgroup

Set up an SMB server in a workgroup overview

Setting up an SMB server as a member in a workgroup consists of creating the SMB server, and then creating local users and groups.

You can configure an SMB server in a workgroup when the Microsoft Active Directory domain infrastructure is not available.

An SMB server in workgroup mode supports only NTLM authentication and does not support Kerberos authentication.

Create an SMB server in a workgroup

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the workgroup to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM.

About this task

SMB servers in workgroup mode do not support the following SMB features:

- SMB3 Witness protocol
- SMB3 CA shares
- SQL over SMB
- Folder Redirection
- Roaming Profiles

- Group Policy Object (GPO)
- Volume Snapshot Service (VSS)

The `vserver cifs` man pages contain additional optional configuration parameters and naming requirements.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   If it is not, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in a workgroup: `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

   The following command creates the SMB server “smb_server01” in the workgroup “workgroup01”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In the following example, the command output shows that a SMB server named “smb_server01” was created on SVM vs1.example.com in the workgroup “workgroup01”:

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                     NetBIOS Domain/Workgroup Name: workgroup01
                       Fully Qualified Domain Name: -
                               Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                    Workgroup Name: workgroup01
                               Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

After you finish

For a CIFS server in a workgroup, you must create local users, and optionally local groups, on the SVM.

Related information

SMB management

Create local user accounts

You can create a local user account that can be used to authorize access to data contained in the SVM over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

About this task

Local user functionality is enabled by default when the SVM is created.

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account.

The `vserver cifs users-and-groups local-user` man pages contain details about optional parameters and naming requirements.

Steps

1. Create the local user: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   The following optional parameters might be useful:

   - `-full-name`

     The users's full name.

   - `-description`

     A description for the local user.

   - `-is-account-disabled {true|false}`

     Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.

   The command prompts for the local user's password.

2. Enter a password for the local user, and then confirm the password.
3. Verify that the user was successfully created: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Example

The following example creates a local user "SMB_SERVER01\sue", with a full name "Sue Chang", associated with SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Create local groups

You can create local groups that can be used for authorizing access to data associated with the SVM over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

About this task

Local group functionality is enabled by default when the SVM is created.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can specify a group name with or without the local domain name, and you can optionally specify a description for the local group. You cannot add a local group to another local group.

The `vserver cifs users-and-groups local-group` man pages contain details about optional parameters and naming requirements.

Steps

1. Create the local group: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   The following optional parameter might be useful:

   - `-description`

     A description for the local group.

2. Verify that the group was successfully created: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Example

The following example creates a local group “SMB_SERVER01\engineering” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

After you finish

You must add members to the new group.

Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group, or if you want users to have privileges associated with that group.

About this task

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- To remove a member from a local group, ONTAP must be able to resolve their name to a SID.

Steps

1. Add a member to or remove a member from a group.
   - Add a member: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     You can specify a comma-delimited list of local users, domain users, or domain groups to add to the

specified local group.

- Remove a member: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

Examples

The following example adds a local user “SMB_SERVER01\sue” to the local group “SMB_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

The following example removes the local users “SMB_SERVER01\sue” and “SMB_SERVER01\james” from the local group “SMB_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verify enabled SMB versions

Your ONTAP 9 release determines which SMB versions are enabled by default for connections with clients and domain controllers. You should verify that the SMB server supports the clients and functionality required in your environment.

About this task

For connections with both clients and domain controllers, you should enable SMB 2.0 and later whenever possible. For security reasons, you should avoid using SMB 1.0, and you should disable it if you have verified that it is not required in your environment.

In ONTAP 9, SMB versions 2.0 and later are enabled by default for client connections, but the version of SMB 1.0 enabled by default depends on your ONTAP release.

- Beginning with ONTAP 9.1 P8, SMB 1.0 can be disabled on SVMs.

  The `-smb1-enabled` option to the `vserver cifs options modify` command enables or disables SMB 1.0.

- Beginning with ONTAP 9.3, it is disabled by default on new SVMs.

If your SMB server is in an Active Directory (AD) domain, you can enable SMB 2.0 to connect to a domain controller (DC) beginning with ONTAP 9.1. Doing so is necessary if you have disabled SMB 1.0 on DCs. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default for DC connections.

If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server.

SMB management contains details about supported SMB versions and functionality.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Verify which SMB versions are enabled: `vserver cifs options show`

   You can scroll down the list to view the SMB versions enabled for client connections, and if you are configuring an SMB server in an AD domain, for AD domain connections.

3. Enable or disable the SMB protocol for client connections as required:

   - To enable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version true`
   - To disable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version false`
     Possible values for `smb_version`:
   - `-smb1-enabled`
   - `-smb2-enabled`
   - `-smb3-enabled`
   - `-smb31-enabled`
     The following command enables SMB 3.1 on SVM vs1.example.com:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
-enabled true
```

4. If your SMB server is in an Active Directory domain, enable or disable the SMB protocol for DC connections as required:

   - To enable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true`
   - To disable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false`

5. Return to the admin privilege level: `set -privilege admin`

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you

must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. 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 LIF.
3. 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 LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Configure SMB client access to shared storage

Configure SMB client access to shared storage

To provide SMB client access to shared storage on an SVM, you must create a volume or qtree to provide a storage container, and then create or modify a share for that container. You can then configure share and file permissions, and test access from client systems.

Before you begin

- SMB must be completely set up on the SVM.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to an Active Directory domain or workgroup configuration must be complete.

Create a volume or qtree storage container

Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

Before you begin

The SVM security style must be NTFS, and SMB should be set up and running.

About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

Steps

1. Create the volume with a junction point: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path]`

The choices for `-junction-path` are the following:

- Directly under root, for example, `/new_vol`

  You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, `/existing_dir/new_vol`

  You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point: `volume show -vserver vserver_name -volume volume_name -junction`

Examples

The following command creates a new volume named users1 on the SVM vs1.example.com and the aggregate aggr1. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type volume (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- -------  -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

The following command creates a new volume named “home4” on the SVM"`vs1.example.com`" and the aggregate “aggr1”. The directory `/eng/` already exists in the namespace for the vs1 SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Create a qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

Before you begin

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be NTFS, and SMB should be set up and running.

Steps

1. Create the qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/volume_name/_qtree_name`.

2. Verify that the qtree was created with the desired junction path: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Example

The following example creates a qtree named qt01 located on SVM vs1.example.com that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Requirements and considerations for creating an SMB share

Before creating an SMB share, you must understand requirements for share paths and share properties, particularly for home directories.

Creating an SMB share entails specifying a directory path structure (using the `-path` option in the `vserver cifs share create` command) that clients will access. The directory path corresponds to the junction path for a volume or qtree that you created in the SVM namespace. The directory path and corresponding junction path must exist before creating your share.

Share paths have the following requirements:

- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be put in quotes (for example, `"/new volume/mount here"`).
- If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial “\\” in the UNC path), then the **Security** tab in the Windows Properties box is unavailable.

  This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

Share property defaults can be changed:

- The default initial properties for all shares are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.
- It is optional to specify share properties when you create a share.

However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all of the share properties that you want to apply to the share using a comma-delimited list.

- To designate a home directory share, use the `homedirectory` property.

  This feature enables you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the SVM).

  > You cannot add or remove this property after creating the share.

Home directory shares have the following requirements:

- Before creating SMB home directories, you must add at least one home directory search path by using the `vserver cifs home-directory search-path add` command.
- Home directory shares specified by the value of `homedirectory` on the `-share-properties` parameter must include the `%w` (Windows user name) dynamic variable in the share name.

  The share name can additionally contain the `%d` (domain name) dynamic variable (for example, `%d/%w`) or a static portion in the share name (for example, `home1_%w`).

- If the share is used by administrators or users to connect to other users' home directories (using options to the `vserver cifs home-directory modify` command), the dynamic share name pattern must be preceded by a tilde (`~`).

SMB management and `vserver cifs share` man pages have additional information.

Create an SMB share

You must create an SMB share before you can share data from an SMB server with SMB clients. When you create a share, you can set share properties, such as designating the share as a home directory. You can also customize the share by configuring optional settings.

Before you begin

The directory path for the volume or qtree must exist in the SVM namespace before creating the share.

About this task

When you create a share, the default share ACL (default share permissions) is `Everyone / Full Control`. After testing access to the share, you should remove the default share ACL and replace it with a more secure alternative.

Steps

1. If necessary, create the directory path structure for the share.

   The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

2. Create an SMB share associated with the specified SVM: `vserver cifs share create -vserver`

```
vserver_name -share-name share_name -path path [-share-properties
share_properties,...] [other_attributes] [-comment text]
```

3. Verify that the share was created:`vserver cifs share show -share-name share_name`

Examples

The following command creates an SMB share named “SHARE1” on SVM `vs1.example.com`. Its directory path is `/users`, and it is created with default properties.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

   b. On the newly created drive, create a test file, and then delete the file.

   You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

Before you begin

You must have decided which users or groups will be given access to the share.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

Steps

1. Delete the default share ACL:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a…	Enter the command…
Windows user	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Windows group	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the "`vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

The following commands give `Change` permission to the local Windows group named “Tiger Team” and `Full_Control` permission to the local Windows user named “Sue Chang” for the “datavol5” share on the "`vs1`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configure NTFS file permissions in a share

To enable file access to the users or groups who have access to a share, you must configure NTFS file permissions on files and directories in that share from a Windows client.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

SMB management and your Windows documentation contain information about how to set standard and advanced NTFS permissions.

Steps

1. Log in to a Windows client as an administrator.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the SMB server name containing the share that contains the data to which you want to apply permissions and the name of the share.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\SHARE1`.

      You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Select the file or directory for which you want to set NTFS file permissions.
5. Right-click the file or directory, and then select **Properties**.
6. Select the **Security** tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

7. Click **Edit**.

   The Permissions for <Object> box opens.

8. Perform the desired actions:

If you want to….	Do the following…
Set standard NTFS permissions for a new user or group	a. Click **Add**. The Select User, Computers, Service Accounts, or Groups window opens. b. In the **Enter the object names to select** box, type the name of the user or group on which you want to add NTFS permission. c. Click **OK**.

If you want to….	Do the following…
Change or remove standard NTFS permissions from a user or group	In the **Group or user names** box, select the user or group that you want to change or remove.

9. Perform the desired actions:

If you want to…	Do the following
Set standard NTFS permissions for a new or existing user or group	In the **Permissions for <Object>** box, select the **Allow** or **Deny** boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click **Remove**.

If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

10. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

Verify user access

You should test that the users you configured can access the SMB share and the files it contains.

Steps

1. On a Windows client, log in as one of the users who now has access to the share.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the share name you will provide to users.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\share1`.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.
4. Create a test file, verify that it exists, write text to it, and then remove the test file.

Manage SMB with the CLI

SMB reference overview

ONTAP file access features are available for the SMB protocol. You can enable a CIFS server, create shares, and enable Microsoft services.

> *SMB* (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP SMB protocol capabilities.
- You want to perform less common configuration and maintenance tasks, not basic SMB configuration.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

SMB server support

SMB server support overview

You can enable and configure SMB servers on storage virtual machines (SVMs) to let SMB clients access files on your cluster.

- Each data SVM in the cluster can be bound to exactly one Active Directory domain.
- Data SVMs do not need to be bound to the same domain.
- Multiple SVMs can be bound to the same domain.

You must configure the SVMs and LIFs that you are using to serve data before you can create an SMB server. If your data network is not flat, you might also need to configure IPspaces, broadcast domains, and subnets. The *Network Management Guide* contains details.

Related information

Network management

Modify SMB servers

System administration

Supported SMB versions and functionality

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. In ONTAP 9, all SMB versions are supported; however, default SMB 1.0 support depends on your ONTAP version. You should verify that the ONTAP SMB server supports the clients and functionality required in your environment.

The latest information about which SMB clients and domain controllers ONTAP supports is available in the *Interoperability Matrix Tool*.

SMB 2.0 and later versions are enabled by default for ONTAP 9 SMB servers, and can be enabled or disabled as needed. The following table shows SMB 1.0 support and default configuration.

SMB 1.0 functionality:	In these ONTAP 9 releases:			
	9.0	9.1	9.2	9.3 and later
Is enabled by default	Yes	Yes	Yes	No
Can be enabled or disabled	No	Yes*9.1 P8 or later required.	Yes	Yes

Default settings for SMB 1.0 and 2.0 connections to domain controllers also depend on the ONTAP version. More information is available in the `vserver cifs security modify` man page. For environments with existing CIFS servers running SMB 1.0, you should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

The following table shows which SMB features are supported in each SMB version. Some SMB features are enabled by default and some require additional configuration.

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:				
		1.0	2.0	2.1	3.0	3.1.1
Legacy SMB 1.0 functionality		X	X	X	X	X
Durable handles			X	X	X	X
Compounded operations			X	X	X	X
Asynchronous operations			X	X	X	X
Increased read and write buffer sizes			X	X	X	X
Increased scalability			X	X	X	X
SMB signing	X	X	X	X	X	X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:				
Alternate Data Stream (ADS) file format	X	X	X	X	X	X
Large MTU (enabled by default beginning with ONTAP 9.7)	X			X	X	X
Lease oplocks				X	X	X
Continuously available shares	X				X	X
Persistent handles					X	X
Witness					X	X
SMB encryption: AES-128-CCM	X				X	X
Scale out (required by CA shares)					X	X
Transparent failover					X	X
SMB Multichannel (beginning with ONTAP 9.4)	X				X	X
Preauthentication integrity						X
Cluster client failover v.2 (CCFv2)						X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:				
SMB encryption: AES-128-GCM (beginning with ONTAP 9.1)	X					X

Related information

Using SMB signing to enhance network security

Setting the SMB server minimum authentication security level

Configuring required SMB encryption on SMB servers for data transfers over SMB

NetApp Technical Report 4543: SMB Protocol Best Practices

NetApp Interoperability

Unsupported Windows features

Before you use CIFS in your network, you need to be aware of certain Windows features that ONTAP does not support.

ONTAP does not support the following Windows features:

- Encrypted File System (EFS)
- Logging of NT File System (NTFS) events in the change journal
- Microsoft File Replication Service (FRS)
- Microsoft Windows Indexing Service
- Remote storage through Hierarchical Storage Management (HSM)
- Quota management from Windows clients
- Windows quota semantics
- The LMHOSTS file
- NTFS native compression

Configure NIS or LDAP name services on the SVM

With SMB access, user mapping to a UNIX user is always performed, even when accessing data in an NTFS security-style volume. If you map Windows users to corresponding UNIX users whose information is stored in NIS or LDAP directory stores, or if you use LDAP for name mapping, you should configure these name services during SMB setup.

Before you begin

You must have customized your name services database configuration to match your name service infrastructure.

About this task

SVMs use the name services ns-switch databases to determine the order in which to look up the sources for a given name service database. The ns-switch source can be any combination of “files”, “nis”, or “ldap”. For the groups database, ONTAP attempts to get the group memberships from all configured sources and then uses the consolidated group membership information for access checks. If one of these sources is unavailable at the time of obtaining UNIX group information, ONTAP cannot get the complete UNIX credentials and subsequent access checks might fail. Therefore, you must always check that all ns-switch sources are configured for the group database in the ns-switch settings.

The default is to have the SMB server map all Windows users to the default UNIX user that is stored in the local `passwd` database. If you want to use the default configuration, configuring NIS or LDAP UNIX user and group name services or LDAP user mapping is optional for SMB access.

Steps

1. If UNIX user, group, and netgroup information is managed by NIS name services, configure NIS name services:
   a. Determine the current ordering of name services by using the `vserver services name-service ns-switch show` command.

      In this example, the three databases (`group`, `passwd`, and `netgroup`) that can use `nis` as a name service source are using only `files` as a source.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                  Source
      Vserver         Database       Enabled      Order
      --------------- ------------   ---------    ---------
      vs1             hosts          true         dns,
                                                  files
      vs1             group          true         files
      vs1             passwd         true         files
      vs1             netgroup       true         files
      vs1             namemap        true         files
      ```

      You must add the `nis` source to the `group` and `passwd` databases, and optionally to the `netgroup` database.

   b. Adjust the name service ns-switch database ordering as desired by using the `vserver services name-service ns-switch modify` command.

      For best performance, you should not add a name service to a name service database unless you plan on configuring that name service on the SVM.

      If you modify the configuration for more than one name service database, you must run the command separately for each name service database that you want to modify.

      In this example, `nis` and `files` are configured as sources for the `group` and `passwd` databases, in

that order. The rest of the name service databases are unchanged.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. Verify that the ordering of name services is correct by using the `vserver services name-service ns-switch show` command.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. Create the NIS name service configuration:
`vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,… -active true+`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```

> Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

e. Verify that the NIS name service is properly configured and active: `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   10.0.0.60
```

2. If UNIX user, group, and netgroup information or name mapping is managed by LDAP name services, configure LDAP name services by using the information located NFS management.

How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`

Specify source type…	To look up information in…	Managed by the command families…
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

Example

The following example displays the name service switch configuration for the SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

Manage SMB servers

Modify SMB servers

You can move a SMB server from a workgroup to an Active Directory domain, from a workgroup to another workgroup, or from an Active Directory domain to a workgroup by using the `vserver cifs modify` command.

About this task

You can also modify other attributes of the SMB server, such as the SMB server name and administrative status. See the man page for details.

Choices

- Move the SMB server from a workgroup to an Active Directory domain:
  a. Set the administrative status of the SMB server to `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Move the SMB server from the workgroup to an Active Directory domain: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

  In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou=`*`example`* `ou` container within the *`example`*.com domain.

  Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

- Move the SMB server from a workgroup to another workgroup:
  a. Set the administrative status of the SMB server to `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. Modify the workgroup for the SMB server: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Move the SMB server from an Active Directory domain to a workgroup:
  a. Set the administrative status of the SMB server to `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Move the SMB server from the Active Directory domain to a workgroup: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> To enter workgroup mode, all domain-based features must be disabled and their configuration removed automatically by the system, including continuously-available shares, shadow copies, and AES. However, domain-configured share ACLs such as "EXAMPLE.COM\userName" will not work properly, but cannot be removed by ONTAP. Remove these share ACLs as soon as possible using external tools after the command completes. If AES is enabled, you may be asked to supply the name and password of a Windows account with sufficient privileges to disable it in the "EXAMPLE.COM" domain.

- Modify other attributes by using the appropriate parameter of the `vserver cifs modify` command.

Use options to customize SMB servers

Available SMB server options

It is useful to know what options are available when considering how to customize the SMB server. Although some options are for general use on the SMB server, several are used to enable and configure specific SMB functionality. SMB server options are controlled with the `vserver cifs options modify` option.

The following list specifies the SMB server options that are available at the admin privilege level:

- **Configuring the SMB session timeout value**

  Configuring this option enables you to specify the number of seconds of idle time before an SMB session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.

- **Configuring the default UNIX user**

  Configuring this option enables you to specify the default UNIX user that the SMB server uses. ONTAP automatically creates a default user named “pcuser” (with a UID of 65534), creates a group named “pcuser” (with a GID of 65534), and adds the default user to the “pcuser” group. When you create a SMB server, ONTAP automatically configures “pcuser” as the default UNIX user.

- **Configuring the guest UNIX user**

  Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the SMB server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the SMB server.

- **Enabling or disabling read grant execution for mode bits**

  Enabling or disabling this option enables you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

- **Enabling or disabling the ability to delete read-only files from NFS clients**

  Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics does not allow the deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is `disabled`, which results in NTFS delete semantics.

- **Configuring Windows Internet Name Service server addresses**

  Configuring this option enables you to specify a list of Windows Internet Name Service (WINS) server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the SMB server options that are available at the advanced privilege level:

- **Granting UNIX group permissions to CIFS users**

  Configuring this option determines whether the incoming CIFS user who is not the owner of the file can be granted the group permission. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `true`, then the group permission is granted for the file. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `false`, then the normal UNIX rules are applicable to grant the file permission. This parameter is applicable to UNIX security-style files that have permission set as `mode bits` and is not applicable to files with the NTFS or NFSv4 security mode. The default setting is `false`.

- **Enabling or disabling SMB 1.0**

  SMB 1.0 is disabled by default on an SVM for which a SMB server is created in ONTAP 9.3.

  Beginning ONTAP 9.3, SMB 1.0 is disabled by default for new SMB servers created in ONTAP 9.3. You should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

- **Enabling or disabling SMB 2.x**

  SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, ONTAP also automatically disables SMB 3.X.

  SMB 2.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.0**

  SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions that support SMB 3.0.

  SMB 3.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.1**

  Windows 10 is the only Windows version that supports SMB 3.1.

  SMB 3.1 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling ODX copy offload**

  ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

- **Enabling or disabling the direct-copy mechanism for ODX copy offload**

  The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

- **Enabling or disabling automatic node referrals**

  With automatic node referrals, the SMB server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share.

- **Enabling or disabling export policies for SMB**

  This option is disabled by default.

- **Enabling or disabling using junction points as reparse points**

  If this option is enabled, the SMB server exposes junction points to SMB clients as reparse points. This option is valid only for SMB 2.x or SMB 3.0 connections. This option is enabled by default.

  This option is supported only on SVMs. The option is enabled by default on SVMs

- **Configuring the number of maximum simultaneous operations per TCP connection**

  The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**

  This option is enabled by default.

- **Enabling or disabling local Windows users authentication**

  This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**

  ONTAP uses the shadow copy functionality to perform remote backups of data stored using the Hyper-V over SMB solution.

  This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Configuring the shadow copy directory depth**

  Configuring this option enables you to define the maximum depth of directories on which to create shadow

copies when using the shadow copy functionality.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Enabling or disabling multidomain search capabilities for name mapping**

  If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (*) in the domain portion of the Windows user name (for example, *\joe), ONTAP searches for the specified user in all of the domains with bidirectional trusts to the home domain. The home domain is the domain that contains the SMB server's computer account.

  As an alternative to searching all of the bidirectionally trusted domains, you can configure a list of preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred list is used to perform multidomain name mapping searches.

  The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**

  Configuring this option enables you to configure the file system sector size in bytes that ONTAP reports to SMB clients. There are two valid values for this option: `4096` and `512`. The default value is `4096`. You might need to set this value to `512` if the Windows application supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control**

  Enabling this option enables you to secure objects on the SMB server by using Dynamic Access Control (DAC), including using auditing to stage central access policies and using Group Policy Objects to implement central access policies. The option is disabled by default.

  This option is supported only on SVMs.

- **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**

  Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to anonymous users. By default, there are no access restrictions for anonymous users.

- **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**

  Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

- **Enabling or disabling the SMB fake open functionality**

  Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how ONTAP makes open and close requests when querying for attribute information on files and directories. By default, the SMB fake open functionality is enabled. This option is useful only for connections that are made with SMB 2.x or later.

- **Enabling or disabling the UNIX extensions**

Enabling this option enables UNIX extensions on a SMB server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled.

If you have UNIX-based SMB clients, such as Mac OSX clients, in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the SMB server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

- **Enabling or disabling support for short name searches**

  Enabling this option allows the SMB server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is `false`.

- **Enabling or disabling support for automatic advertisement of DFS capabilities**

  Enabling or disabling this option determines whether SMB servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that connect to shares. ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the SMB server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the SMB server advertises DFS capabilities only when the clients connect to shares where symbolic link access is enabled.

- **Configuring the maximum number of SMB credits**

  Beginning with ONTAP 9.4, configuring the `-max-credits` option allows you to limit the number of credits to be granted on an SMB connection when clients and server are running SMB version 2 or later. The default value is 128.

- **Enabling or disabling support for SMB Multichannel**

  Enabling the `-is-multichannel-enabled` option in ONTAP 9.4 and later releases allows the SMB server to establish multiple connections for a single SMB session when appropriate NICs are deployed on the cluster and its clients. Doing so improves throughput and fault tolerance. The default value for this parameter is `false`.

  When SMB Multichannel is enabled, you can also specify the following parameters:

  - The maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.
  - The maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

Configuring SMB server options

You can configure SMB server options at any time after you have created a SMB server on a storage virtual machine (SVM).

Step

1. Perform the desired action:

If you want to configure SMB server options…	Enter the command…
At admin-privilege level	`vserver cifs options modify -vserver` *`vserver_name options`*
At advanced-privilege level	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

For more information about configuring SMB server options, see the man page for the `vserver cifs options modify` command.

Configure the grant UNIX group permission to SMB users

You can configure this option to grant group permissions to access files or directories even if the incoming SMB user is not the owner of the file.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the grant UNIX group permission as appropriate:

If you want to	Enter the command
Enable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Disable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Verify that the option is set to the desired value: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Return to the admin privilege level: `set -privilege admin`

Configure access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the *null user*) can access certain information on the network. You can use a SMB server option to configure access restrictions for the anonymous user.

About this task

The `–restrict-anonymous` SMB server option corresponds to the `RestrictAnonymous` registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the

network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:

Value	Description
`no-restriction` (default)	Specifies no access restrictions for anonymous users.
`no-enumeration`	Specifies that only enumeration is restricted for anonymous users.
`no-access`	Specifies that access is restricted for anonymous users.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the restrict anonymous setting: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

Related information

Available SMB server options

Manage how file security is presented to SMB clients for UNIX security-style data

Manage how file security is presented to SMB clients for UNIX security-style data overview

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the **Security** tab in the Windows Properties box.

  You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where ONTAP must preserve UNIX permissions during save operations.
- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.

Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients.

  The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.

- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes.

  If ONTAP reports the volume as FAT, the application does not try to change an ACL.

Related information

Configuring security styles on FlexVol volumes

Configuring security styles on qtrees

Enable or disable the presentation of NTFS ACLs for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

About this task

If you enable this option, ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the UNIX NTFS ACL option setting: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same

UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Manage SMB server security settings

How ONTAP handles SMB client authentication

Before users can create SMB connections to access data contained on the SVM, they must be authenticated by the domain to which the SMB server belongs. The SMB server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

Kerberos authentication

ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is the primary authentication service for Active Directory. The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients who want to establish a session with another computer, such the SMB server, contact a KDC directly to obtain their session credentials.

NTLM authentication

NTLM client authentication is done using a challenge response protocol based on shared knowledge of a user-specific secret based on a password.

If a user creates an SMB connection using a local Windows user account, authentication is done locally by the SMB server using NTLMv2.

Guidelines for SMB server security settings in an SVM disaster recovery configuration

Before creating an SVM that is configured as a disaster recovery destination where the identity is not preserved (the `-identity-preserve` option is set to `false` in the SnapMirror configuration), you should know about how SMB server security settings are managed on the destination SVM.

- Non-default SMB server security settings are not replicated to the destination.

  When you create a SMB server on the destination SVM, all SMB server security settings are set to default values. When the SVM disaster recovery destination is initialized, updated, or resynced, the SMB server security settings on the source are not replicated to the destination.

- You must manually configure non-default SMB server security settings.

  If you have non-default SMB server security settings configured on the source SVM, you must manually configure these same settings on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Display information about SMB server security settings

You can display information about SMB server security settings on your storage virtual machines (SVMs). You can use this information to verify that the security settings are correct.

About this task

A displayed security setting can be the default value for that object or a non-default value that is configured either by using the ONTAP CLI or by using Active Directory group policy objects (GPOs).

Do not use the `vserver cifs security show` command for SMB servers in workgroup mode, because some of the options are not valid.

Step

1. Perform one of the following actions:

If you want display information about…	Enter the command…
All security settings on a specified SVM	`vserver cifs security show -vserver` *`vserver_name`*

If you want display information about…	Enter the command…
A specific security setting or settings on the SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` You can enter `-fields ?` to determine what fields you can use.

Example

The following example shows all security settings for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
              Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:        false
                        LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:        false
                       Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Note that the settings displayed depend on the running ONTAP version.

The following example shows the Kerberos clock skew for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Related information

Displaying information about GPO configurations

Enable or disable required password complexity for local SMB users

Required password complexity provides enhanced security for local SMB users on your storage virtual machines (SVMs). The required password complexity feature is enabled by default. You can disable it and reenable it at any time.

Before you begin

Local users, local groups, and local user authentication must be enabled on the CIFS server.

About this task

You must not use the `vserver cifs security modify` command for a CIFS server in workgroup mode because some of the options are not valid.

Steps

1. Perform one of the following actions:

If you want required password complexity for local SMB users to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Disabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Verify the security setting for required password complexity: `vserver cifs security show -vserver` *`vserver_name`*

Example

The following example shows that required password complexity is enabled for local SMB users for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Related information

Displaying information about CIFS server security settings

Using local users and groups for authentication and authorization

Requirements for local user passwords

Changing local user account passwords

Modify the CIFS server Kerberos security settings

You can modify certain CIFS server Kerberos security settings, including the maximum allowed Kerberos clock skew time, the Kerberos ticket lifetime, and the maximum number of ticket renewal days.

About this task

Modifying CIFS server Kerberos settings by using the `vserver cifs security modify` command modifies the settings only on the single storage virtual machine (SVM) that you specify with the `-vserver` parameter. You can centrally manage Kerberos security settings for all SVMs on the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

Steps

1. Perform one or more of the following actions:

If you want to…	Enter…
Specify the maximum allowed Kerberos clock skew time in minutes.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* The default setting is 5 minutes.
Specify the Kerberos ticket lifetime in hours.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` The default setting is 10 hours.
Specify the maximum number of ticket renewal days.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* The default setting is 7 days.
Specify the timeout for sockets on KDCs after which all KDCs are marked as unreachable.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* The default setting is 3 seconds.

2. Verify the Kerberos security settings:

   `vserver cifs security show -vserver` *`vserver_name`*

Example

The following example makes the following changes to Kerberos security: “Kerberos Clock Skew” is set to 3 minutes and “Kerberos Ticket Age” is set to 8 hours for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
        Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
             Is AES Encryption Enabled:                 false
                LM Compatibility Level:  lm-ntlm-ntlmv2-krb
            Is SMB Encryption Required:                 false
```

Related information

Displaying information about CIFS server security settings

Supported GPOs

Applying Group Policy Objects to CIFS servers

Set the SMB server minimum authentication security level

You can set the SMB server minimum security level, also known as the *LMCompatibilityLevel*, on your SMB server to meet your business security requirements for SMB client access. The minimum security level is the minimum level of the security tokens that the SMB server accepts from SMB clients.

About this task

- SMB servers in workgroup mode support only NTLM authentication. Kerberos authentication is not supported.
- LMCompatibilityLevel applies only to SMB client authentication, not admin authentication.

You can set the minimum authentication security level to one of four supported security levels.

Value	Description
`lm-ntlm-ntlmv2-krb` (default)	The storage virtual machine (SVM) accepts LM, NTLM, NTLMv2, and Kerberos authentication security.
`ntlm-ntlmv2-krb`	The SVM accepts NTLM, NTLMv2, and Kerberos authentication security. The SVM denies LM authentication.
`ntlmv2-krb`	The SVM accepts NTLMv2 and Kerberos authentication security. The SVM denies LM and NTLM authentication.
`krb`	The SVM accepts Kerberos authentication security only. The SVM denies LM, NTLM, and NTLMv2 authentication.

Steps

1. Set the minimum authentication security level: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verify that the authentication security level is set to the desired level: `vserver cifs security show -vserver vserver_name`

Related information

Enabling or disabling AES encryption for Kerberos-based communication

Configure strong security for Kerberos-based communication by using AES encryption

For strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. By default, when you create a SMB server on the SVM, AES encryption is disabled. You must enable it to take advantage of the strong security provided by Advanced Encryption Standard (AES) encryption.

Kerberos-related communication for SMB is used during SMB server creation on the SVM, as well as during the SMB session setup phase. The SMB server supports the following encryption types for Kerberos communication:

- RC4-HMAC
- DES
- AES 128
- AES 256

If you want to use the highest security encryption type for Kerberos communication, you should enable AES encryption for Kerberos communication on the SVM.

Intel AES New Instructions (Intel AES NI) is available in SMB 3.0, improving on the AES algorithm and accelerating data encryption with supported processor families.Beginning with SMB 3.1.1, AES-128-GCM replaces AES-128-CCM as the hash algorithm used by SMB encryption.

When the SMB server is created, the domain controller creates a computer machine account in Active Directory. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account. Subsequently, a particular encryption type is selected for encrypting the service ticket that the client presents to the server during authentication.

Related information

Modifying the CIFS server Kerberos security settings

Enable or disable AES encryption for Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. If you do not want the SMB server to select the AES encryption types for Kerberos-based communication with the Active Directory (AD) KDC, you can disable AES encryption. By default, AES encryption is disabled.

About this task

To enhance security, the storage virtual machine (SVM) changes its machine account password in the AD each time the AES security option is modified. Changing the password might require administrative AD credentials for the organizational unit (OU) that contains the machine account.

If an SVM is configured as a disaster recovery destination where the identity is not preserved (the `-identity -preserve` option is set to `false` in the SnapMirror configuration), the non-default SMB server security settings are not replicated to the destination. If you have enabled AES encryption on the source SVM, you must manually enable it on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Steps

1. Perform one of the following actions:

If you want the AES encryption types for Kerberos communication to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver vserver_name -is-aes-encryption -enabled true`
Disabled	`vserver cifs security modify -vserver vserver_name -is-aes-encryption -enabled false`

2. Verify that AES encryption is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   The `is-aes-encryption-enabled` field displays `true` if AES encryption is enabled and `false` if it is

disabled.

Example

The following example enables the AES encryption types for the CIFS server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes-encryption
-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled
vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

The following example enables the AES encryption types for the SMB server on SVM vs2. The administrator is prompted to enter the administrative AD credentials for the OU containing the SMB server.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes-encryption
-enabled true

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:


cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled
vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Use SMB signing to enhance network security

Use SMB signing to enhance network security overview

SMB signing helps to ensure that network traffic between the SMB server and the client is not compromised; it does this by preventing replay attacks. By default, ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the SMB server to require SMB signing.

How SMB signing policies affect communication with a CIFS server

In addition to the CIFS server SMB signing security settings, two SMB signing policies on Windows clients control the digital signing of communications between clients and the CIFS server. You can configure the setting that meets your business requirements.

Client SMB policies are controlled through Windows local security policy settings, which are configured by using the Microsoft Management Console (MMC) or Active Directory GPOs. For more information about client SMB signing and security issues, see the Microsoft Windows documentation.

Here are descriptions of the two SMB signing policies on Microsoft clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  This setting controls whether the client's SMB signing capability is enabled. It is enabled by default. When this setting is disabled on the client, the client communications with the CIFS server depends on the SMB signing setting on the CIFS server.

- `Microsoft network client: Digitally sign communications (always)`

  This setting controls whether the client requires SMB signing to communicate with a server. It is disabled by default. When this setting is disabled on the client, SMB signing behavior is based on the policy setting for `Microsoft network client: Digitally sign communications (if server agrees)` and the setting on the CIFS server.

> If your environment includes Windows clients configured to require SMB signing, you must enable SMB signing on the CIFS server. If you do not, the CIFS server cannot serve data to these systems.

The effective results of client and CIFS server SMB signing settings depends on whether the SMB sessions uses SMB 1.0 or SMB 2.x and later.

The following table summarizes the effective SMB signing behavior if the session uses SMB 1.0:

Client	ONTAP—signing not required	ONTAP—signing required
Signing disabled and not required	Not signed	Signed
Signing enabled and not required	Not signed	Signed
Signing disabled and required	Signed	Signed
Signing enabled and required	Signed	Signed

> Older Windows SMB 1 clients and some non-Windows SMB 1 clients might fail to connect if signing is disabled on the client but required on the CIFS server.

The following table summarizes the effective SMB signing behavior if the session uses SMB 2.x or SMB 3.0:

> For SMB 2.x and SMB 3.0 clients, SMB signing is always enabled. It cannot be disabled.

Client	ONTAP—signing not required	ONTAP—signing required
Signing not required	Not signed	Signed
Signing required	Signed	Signed

The following table summarizes the default Microsoft client and server SMB signing behavior:

Protocol	Hash algorithm	Can enable/disable	Can require/not require	Client default	Server default	DC default
SMB 1.0	MD5	Yes	Yes	Enabled (not required)	Disabled (not required)	Required
SMB 2.x	HMAC SHA-256	No	Yes	Not required	Not required	Required
SMB 3.0	AES-CMAC.	No	Yes	Not required	Not required	Required

Microsoft no longer recommends using `Digitally sign communications (if client agrees)` or `Digitally sign communications (if server agrees)` Group Policy settings. Microsoft also no longer recommends using the `EnableSecuritySignature` registry settings. These options only affect the SMB 1 behavior and can be replaced by the `Digitally sign communications (always)` Group Policy setting or the `RequireSecuritySignature` registry setting. You can also get more information from the Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Basics of SMB Signing (covering both SMB1 and SMB2)]

Performance impact of SMB signing

When SMB sessions use SMB signing, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM containing the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in signed SMB traffic. SMB signing offload is enabled by default when SMB signing is enabled.

Enhanced SMB signing performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 (supported with Windows 10 and Windows Server 2016), which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance

impact of SMB signing can vary widely; you can verify it only through testing in your network environment.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

Recommendations for configuring SMB signing

You can configure SMB signing behavior between SMB clients and the CIFS server to meet your security requirements. The settings you choose when configuring SMB signing on your CIFS server are dependent on what your security requirements are.

You can configure SMB signing on either the client or the CIFS server. Consider the following recommendations when configuring SMB signing:

If…	Recommendation…
You want to increase the security of the communication between the client and the server	Make SMB signing required at the client by enabling the `Require Option (Sign always)` security setting on the client.
You want all SMB traffic to a certain storage virtual machine (SVM) signed	Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.

See Microsoft documentation for more information on configuring Windows client security settings.

Guidelines for SMB signing when multiple data LIFS are configured

If you enable or disable required SMB signing on the SMB server, you should be aware of the guidelines for multiple data LIFS configurations for an SVM.

When you configure a SMB server, there might be multiple data LIFs configured. If so, the DNS server contains multiple `A` record entries for the CIFS server, all using the same SMB server host name, but each with a unique IP address. For example, a SMB server that has two data LIFs configured might have the following DNS `A` record entries:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

The normal behavior is that upon changing the required SMB signing setting, only new connections from clients are affected by the change in the SMB signing setting. However, there is an exception to this behavior. There is a case where a client has an existing connection to a share, and the client creates a new connection to the same share after the setting is changed, while maintaining the original connection. In this case, both the new and the existing SMB connection adopt the new SMB signing requirements.

Consider the following example:

1. Client1 connects to a share without required SMB signing using the path `O:\`.

2. The storage administrator modifies the SMB server configuration to require SMB signing.
3. Client1 connects to the same share with required SMB signing using the path `S:\` (while maintaining the connection using the path `O:\`).
4. The result is that SMB signing is used when accessing data over both the `O:\` and `S:\` drives.

Enable or disable required SMB signing for incoming SMB traffic

You can enforce the requirement for clients to sign SMB messages by enabling required SMB signing. If enabled, ONTAP accepts SMB messages only if they have valid signatures. If you want to permit SMB signing, but not require it, you can disable required SMB signing.

About this task

By default, required SMB signing is disabled. You can enable or disable required SMB signing at any time.

SMB signing is not disabled by default under the following circumstances:

1. Required SMB signing is enabled, and the cluster is reverted to a version of ONTAP that does not support SMB signing.
2. The cluster is subsequently upgraded to a version of ONTAP that supports SMB signing.

   Under these circumstances, the SMB signing configuration that was originally configured on a supported version of ONTAP is retained through reversion and subsequent upgrade.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value that you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB signing security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB signing security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled required SMB signing on the source SVM, you must manually enable required SMB signing on the destination SVM.

Steps

1. Perform one of the following actions:

If you want required SMB signing to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Disabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verify that required SMB signing is enabled or disabled by determining whether the value in the `Is Signing Required` field in the output of the following command is set to the desired value: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Example

The following example enables required SMB signing for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

Determine whether SMB sessions are signed

You can display information about connected SMB sessions on the CIFS server. You can use this information to determine whether SMB sessions are signed. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

Steps

1. Perform one of the following actions:

If you want display information about…	Enter the command…
All signed sessions on a specified storage virtual machine (SVM)	`vserver cifs session show -vserver vserver_name -is-session-signed true`
Details for a signed session with a specific session ID on the SVM	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

Examples

The following command displays session information about signed sessions on SVM vs1. The default summary output does not display the “Is Session Signed” output field:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

The following command displays detailed session information, including whether the session is signed, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Related information

Monitoring SMB signed session statistics

Monitor SMB signed session statistics

You can monitor SMB sessions statistics and determine which established sessions are signed and which are not.

About this task

The `statistics` command at the advanced privilege level provides the `signed_sessions` counter that you can use to monitor the number of signed SMB sessions. The `signed_sessions` counter is available with the following statistics objects:

- `cifs` enables you to monitor SMB signing for all SMB sessions.
- `smb1` enables you to monitor SMB signing for SMB 1.0 sessions.
- `smb2` enables you to monitor SMB signing for SMB 2.x and SMB 3.0 sessions.

  SMB 3.0 statistics are included in the output for the `smb2` object.

If you want to compare the number of signed session to the total number of sessions, you can compare output for the `signed_sessions` counter with the output for the `established_sessions` counter.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:
   `set -privilege advanced`
2. Start a data collection:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

   You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.
3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB signing statistics:

If you want to view information for…	Enter…
Signed sessions	`show -sample-id sample_ID -counter signed_sessions|`*`node_name`* `[-node` *`node_name`*`]`
Signed sessions and established sessions	`show -sample-id` *`sample_ID`* `-counter signed_sessions|established_sessions|`*`node_name`* `[-node node_name]`

   If you want to display information for only a single node, specify the optional `-node` parameter.
5. Return to the admin privilege level:
   `set -privilege admin`

Examples

The following example shows how you can monitor SMB 2.x and SMB 3.0 signing statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

The following command stops the data collection for the sample:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

The following command shows signed SMB sessions and established SMB sessions by node from the sample:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

The following command shows signed SMB sessions for node2 from the sample:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

The following command moves back to the admin privilege level:

```
cluster1::*> set -privilege admin
```

Related information

Determining whether SMB sessions are signed

Performance monitoring and management overview

Configure required SMB encryption on SMB servers for data transfers over SMB

SMB encryption overview

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on SMB servers. You can also configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create a SMB server on the storage virtual machine (SVM), SMB encryption is disabled. You must enable it to take advantage of the enhanced security provided by SMB encryption.

To create an encrypted SMB session, the SMB client must support SMB encryption. Windows clients beginning with Windows Server 2012 and Windows 8 support SMB encryption.

SMB encryption on the SVM is controlled through two settings:

- A SMB server security option that enables the functionality on the SVM
- A SMB share property that configures the SMB encryption setting on a share-by-share basis

You can decide whether to require encryption for access to all data on the SVM or to require SMB encryption to access data only in selected shares. SVM-level settings supersede share-level settings.

The effective SMB encryption configuration depends on the combination of the two settings and is described in the following table:

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
True	False	Server-level encryption is enabled for all of the shares in the SVM. With this configuration, encryption happens for the entire SMB session.
True	True	Server-level encryption is enabled for all of the shares in the SVM irrespective of share-level encryption. With this configuration, encryption happens for the entire SMB session.
False	True	Share-level encryption is enabled for the specific shares. With this configuration, encryption happens from the tree connect.

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
False	False	No encryption is enabled.

SMB clients that do not support encryption cannot connect to a SMB server or share that requires encryption.

Performance impact of SMB encryption

When SMB sessions use SMB encryption, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM that contains the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in encrypted SMB traffic. SMB encryption offload is enabled by default when SMB encryption is enabled.

Enhanced SMB encryption performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 (supported with Windows 10 and Windows Server 2016), which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB encryption can vary widely; you can verify it only through testing in your network environment.

SMB encryption is disabled by default on the SMB server. You should enable SMB encryption only on those SMB shares or SMB servers that require encryption. With SMB encryption, ONTAP performs additional processing of decrypting the requests and encrypting the responses for every request. SMB encryption should therefore be enabled only when necessary.

Enable or disable required SMB encryption for incoming SMB traffic

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

About this task

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

Steps

1. Perform one of the following actions:

If you want required SMB encryption for incoming SMB traffic on the CIFS server to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Disabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   The `is-smb-encryption-required` field displays `true` if required SMB encryption is enabled on the CIFS server and `false` if it is disabled.

Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Determine whether clients are connected using encrypted SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

About this task

SMB clients sessions can have one of three encryption levels:

- `unencrypted`

  The SMB session is not encrypted. Neither storage virtual machine (SVM)-level or share-level encryption is configured.

- `partially-encrypted`

  Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- `encrypted`

  The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

Steps

1. Perform one of the following actions:

If you want display information about…	Enter the command…
Sessions with a specified encryption setting for sessions on a specified SVM	`vserver cifs session show -vserver` *`vserver_name`* `{unencrypted|partially-encrypted|encrypted} -instance`
The encryption setting for a specific session ID on a specified SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Monitor SMB encryption statistics

You can monitor SMB encryption statistics and determine which established sessions and share connections are encrypted and which are not.

About this task

The `statistics` command at the advanced privilege level provides the following counters, which you can use to monitor the number of encrypted SMB sessions and share connections:

Counter name	Descriptions
`encrypted_sessions`	Gives the number of encrypted SMB 3.0 sessions
`encrypted_share_connections`	Gives the number of encrypted shares on which a tree connect has happened
`rejected_unencrypted_sessions`	Gives the number of session setups rejected due to a lack of client encryption capability
`rejected_unencrypted_shares`	Gives the number of share mappings rejected due to a lack of client encryption capability

These counters are available with the following statistics objects:

- `cifs` enables you to monitor SMB encryption for all SMB 3.0 sessions.

  SMB 3.0 statistics are included in the output for the `cifs` object. If you want to compare the number of encrypted sessions to the total number of sessions, you can compare output for the `encrypted_sessions` counter with the output for the `established_sessions` counter.

  If you want to compare the number of encrypted share connections to the total number of share connections, you can compare output for the `encrypted_share_connections` counter with the output for the `connected_shares` counter.

- `rejected_unencrypted_sessions` provides the number of times an attempt has been made to establish an SMB session that requires encryption from a client that does not support SMB encryption.
- `rejected_unencrypted_shares` provides the number of times an attempt has been made to connect to an SMB share that requires encryption from a client that does not support SMB encryption.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop the data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:
   `set -privilege advanced`
2. Start a data collection:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

   You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB encryption statistics:

If you want to view information for…	Enter…
Encrypted sessions	`show -sample-id` *`sample_ID`* `-counter encrypted_sessions|`*`node_name`* `[-node` *`node_name`*`]`
Encrypted sessions and established sessions	`show -sample-id` *`sample_ID`* `-counter encrypted_sessions|established_sessions|`*`node_name`* `[-node` *`node_name`*`]`

If you want to view information for…	Enter…
Encrypted share connections	`show -sample-id sample_ID -counter encrypted_share_connections|node_name [-node node_name]`
Encrypted share connections and connected shares	`show -sample-id sample_ID -counter encrypted_share_connections|connected_shares|node_name [-node node_name]`
Rejected unencrypted sessions	`show -sample-id sample_ID -counter rejected_unencrypted_sessions|node_name [-node node_name]`
Rejected unencrypted share connections	`show -sample-id sample_ID -counter rejected_unencrypted_share|node_name [-node node_name]`

If you want to display information only for a single node, specify the optional `-node` parameter.

5. Return to the admin privilege level:
`set -privilege admin`

Examples

The following example shows how you can monitor SMB 3.0 encryption statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

The following command stops data collection for that sample:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

The following command shows encrypted SMB sessions and established SMB sessions by the node from the sample:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

The following command shows the number of rejected unencrypted SMB sessions by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

The following command shows the number of connected SMB shares and encrypted SMB shares by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

The following command shows the number of rejected unencrypted SMB share connections by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Related information

Determining which statistics objects and counters are available

Performance monitoring and management overview

Secure LDAP session communication

LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the CIFS

server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`.

LDAP signing and sealing on CIFS traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

Enable LDAP signing and sealing on the CIFS server

Before your CIFS server can use signing and sealing for secure communication with an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP signing and sealing.

Before you begin

You must consult with your AD server administrator to determine the appropriate security configuration values.

Steps

1. Configure the CIFS server security setting that enables signed and sealed traffic with Active Directory LDAP servers: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

2. Verify that the LDAP signing and sealing security setting is set correctly: `vserver cifs security show -vserver` *`vserver_name`*

> If the SVM uses the same LDAP server for querying name-mapping or other UNIX information, such as users, groups, and netgroups, then you must enable the corresponding setting with the `-session-security` option of the `vserver services name-service ldap client modify` command.

Configure LDAP over TLS

Export a copy of the self-signed root CA certificate

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by ONTAP to install the certificate on the storage virtual machine (SVM).

Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library.

Microsoft TechNet Library: technet.microsoft.com

Step

1. Obtain a root CA certificate of the domain controller that is in the `.pem` text format.

   Microsoft TechNet Library: technet.microsoft.com

After you finish

Install the certificate on the SVM.

Related information

Microsoft TechNet Library

Install the self-signed root CA certificate on the SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

About this task

When LDAP over TLS is enabled, the ONTAP LDAP client on the SVM does not support revoked certificates in ONTAP 9.0 and 9.1.

Beginning with ONTAP 9.2, all applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

Steps

1. Install the self-signed root CA certificate:
   a. Begin the certificate installation: `security certificate install -vserver vserver_name -type server-ca`

      The console output displays the following message: `Please enter Certificate: Press <Enter> when done`

   b. Open the certificate `.pem` file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
   c. Verify that the certificate is displayed correctly.
   d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed: `security certificate show -vserver *vserver_name*`

Enable LDAP over TLS on the server

Before your SMB server can use TLS for secure communication with an Active Directory LDAP server, you must modify the SMB server security settings to enable LDAP over TLS.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory (AD) and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with AD servers, use the `-try-channel-binding-for-ad-ldap` parameter with the

`vserver cifs security modify` command.

To learn more, see:

- LDAP overview
- 2020 LDAP channel binding and LDAP signing requirements for Windows.

Steps

1. Configure the SMB server security setting that allows secure LDAP communication with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -use-start-tls -for-ad-ldap true`
2. Verify that the LDAP over TLS security setting is set to `true`: `vserver cifs security show -vserver vserver_name`

> If the SVM uses the same LDAP server for querying name-mapping or other UNIX information (such as users, groups, and netgroups), then you must also modify the `-use -start-tls` option by using the `vserver services name-service ldap client modify` command.

Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance.

Before you begin

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

  The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

  The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- **`-max-connections-per-session`**

  The maximum number of connections allowed per Multichannel session. The default is 32 connections.

  If you want to enable more connections than the default, you must make comparable adjustments to the

client configuration, which also has a default of 32 connections.

- **-max-lifs-per-session**

  The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable SMB Multichannel on the SMB server: `vserver cifs options modify -vserver` *`vserver_name`* `-is-multichannel-enabled true`
3. Verify that ONTAP is reporting SMB Multichannel sessions: `vserver cifs session show` *`options`*
4. Return to the admin privilege level: `set -privilege admin`

Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
                Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Configure default Windows user to UNIX user mappings on the SMB server

Configure the default UNIX user

You can configure the default UNIX user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure the default UNIX user.

About this task

By default, the name of the default UNIX user is “pcuser”, which means that, by default, user mapping to the default UNIX user is enabled. You can specify another name to use as the default UNIX user. The name that you specify must exist in the name service databases configured for the storage virtual machine (SVM). If this option is set to a null string, no one can access the CIFS server as a UNIX default user. That is, each user must have an account in the password database before they can access the CIFS server.

For a user to connect to the CIFS server using the default UNIX user account, the user must meet the following prerequisites:

- The user is authenticated.
- The user is in the CIFS server’s local Windows user database, in the CIFS server’s home domain, or in a trusted domain (if multidomain name mapping searches is enabled on the CIFS server).
- The user name is not explicitly mapped to a null string.

Steps

1. Configure the default UNIX user:

If you want to …	Enter …
Use the default UNIX user “pcuser”	`vserver cifs options modify -default -unix-user pcuser`
Use another UNIX user account as the default user	`vserver cifs options modify -default -unix-user user_name`
Disable the default UNIX user	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verify that the default UNIX user is configured correctly: `vserver cifs options show -vserver vserver_name`

   In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure the guest UNIX user

Configuring the guest UNIX user option means that users who log in from untrusted domains are mapped to the guest UNIX user and can connect to the CIFS server. Alternatively, if you want authentication of users from untrusted domains to fail, you should not configure the guest UNIX user. The default is to not allow users from untrusted domains to connect to the CIFS server (the guest UNIX account is not configured).

About this task

You should keep the following in mind when configuring the guest UNIX account:

- If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database and this option is enabled, the CIFS server considers the user as a

guest user and maps the user to the specified UNIX user.

- If this option is set to a null string, the guest UNIX user is disabled.
- You must create a UNIX user to use as the guest UNIX user in one of the storage virtual machine (SVM) name service databases.
- A user logged in as a guest user is automatically is a member of the BUILTIN\guests group on the CIFS server.
- The 'homedirs-public' option applies only to authenticated users. A user logged in as a guest user does not have a home directory and cannot access other users' home directories.

Steps

1. Perform one of the following actions:

If you want to…	Enter…
Configure the guest UNIX user	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Disable the guest UNIX user	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verify that the guest UNIX user is configured correctly: `vserver cifs options show -vserver` *`vserver_name`*

   In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Map the administrators group to root

If you have only CIFS clients in your environment and your storage virtual machine (SVM) was set up as a multiprotocol storage system, you must have at least one Windows account that has root privilege for accessing files on the SVM; otherwise, you cannot manage the SVM because you do not have sufficient user rights.

About this task

If your storage system was set up as NTFS-only, however, the `/etc` directory has a file-level ACL that enables the administrators group to access the ONTAP configuration files.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the CIFS server option that maps the administrators group to root as appropriate:

If you want to…	Then…
Map the administrator group members to root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` All accounts in the administrators group are considered root, even if you do not have an `/etc/usermap.cfg` entry mapping the accounts to root. If you create a file using an account that belongs to the administrators group, the file is owned by root when you view the file from a UNIX client.
Disable mapping the administrators group members to root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Accounts in the administrators group no longer map to root. You can only explicitly map a single user to root.

3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

Display information about what types of users are connected over SMB sessions

You can display information about what type of users are connected over SMB sessions. This can help you ensure that only the appropriate type of user is connecting over SMB sessions on the storage virtual machine (SVM).

About this task

The following types of users can connect over SMB sessions:

- `local-user`

  Authenticated as a local CIFS user

- `domain-user`

  Authenticated as a domain user (either from the CIFS server's home domain or a trusted domain)

- `guest-user`

  Authenticated as a guest user

- `anonymous-user`

  Authenticated as an anonymous or null user

Steps

1. Determine what type of user is connected over an SMB session: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

If you want to display user type information for established sessions…	Enter the following command…
For all sessions with a specified user type	`vserver cifs session show -vserver vserver_name -user-type {local-user|domain-user|guest-user|anonymous-user}`
For a specific user	`vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Examples

The following command displays session information on the user type for sessions on SVM vs1 established by user "` iepubs\user1`":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Command options to limit excessive Windows client resource consumption

Options to the `vserver cifs options modify` command enable you to control resource consumption for Windows clients. This can be helpful if any clients are outside normal bounds of resource consumption, for example, if there are unusually high numbers of files open, sessions open, or change notify requests.

The following options to the `vserver cifs options modify` command have been added to control Windows client resource consumption. If the maximum value for any of these options is exceeded, the request is denied and an EMS message is sent. An EMS warning message is also sent when 80 percent of the configured limit for these options is reached.

- `-max-opens-same-file-per-tree`

  Maximum number of opens on the same file per CIFS tree

- `-max-same-user-sessions-per-connection`

  Maximum number of sessions opened by the same user per connection

- `-max-same-tree-connect-per-session`

  Maximum number of tree connects on the same share per session

- `-max-watches-set-per-tree`

  Maximum number of watches (also known as *change notifies*) established per tree

See the man pages for the default limits and to display the current configuration.

Beginning with ONTAP 9.4, servers running SMB version 2 or later can limit the number of outstanding requests (*SMB credits*) that the client can send to the server on a SMB connection. The management of SMB credits is initiated by the client and controlled by the server.

The maximum number of outstanding requests that can be granted on an SMB connection is controlled by the `-max-credits` option. The default value for this option is 128.

Improve client performance with traditional and lease oplocks

Improve client performance with traditional and lease oplocks overview

Traditional oplocks (opportunistic locks) and lease oplocks enable an SMB client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic.

Lease oplocks are an enhanced form of oplocks available with the SMB 2.1 protocol and later. Lease oplocks allow a client to obtain and preserve client caching state across multiple SMB opens originating from itself.

Oplocks can be controlled in two ways:

- By a share property, using the `vserver cifs share create` command when the share is created, or the `vserver share properties` command after creation.
- By a qtree property, using the `volume qtree create` command when the qtree is created, or the `volume qtree oplock` commands after creation.

Write cache data-loss considerations when using oplocks

Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must invalidate cached data and flush writes and locks. The client must then relinquish the oplock and access to the file. If there is a network failure during this flush, cached write data might be lost.

- Data-loss possibilities

  Any application that has write-cached data can lose that data under the following set of circumstances:

  - The connection is made using SMB 1.0.
  - It has an exclusive oplock on the file.
  - It is told to either break that oplock or close the file.
  - During the process of flushing the write cache, the network or target system generates an error.
- Error handling and write completion

  The cache itself does not have any error handling—the applications do. When the application makes a write to the cache, the write is always completed. If the cache, in turn, makes a write to the target system over a network, it must assume that the write is completed because if it does not, the data is lost.

Enable or disable oplocks when creating SMB shares

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. Oplocks are enabled on SMB shares residing on storage virtual machines (SVMs). In some circumstances, you might want to disable oplocks. You can enable or disable oplocks on a share-by-share basis.

About this task

If oplocks are enabled on the volume containing a share but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over the volume oplock setting. Disabling oplocks on the share disables both opportunistic and lease oplocks.

You can specify other share properties in addition to specifying the oplock share property by using a comma-delimited list. You can also specify other share parameters.

Steps

1. Perform the applicable action:

If you want to…	Then…
Enable oplocks on a share during share creation	Enter the following command: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` If you want the share to have only the default share properties, which are `oplocks`, `browsable`, and `changenotify` enabled, you do not have to specify the `-share-properties` parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the `-share-properties` parameter with the list of share properties to use for that share.
Disable oplocks on a share during share creation	Enter the following command: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the `oplocks` property.

Related information

Enabling or disabling oplocks on existing SMB shares

Monitoring oplock status

Commands for enabling or disabling oplocks on volumes and qtrees

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. You need to know the commands for enabling or disabling oplocks on volumes or qtrees. You also must know when you can enable or disable oplocks on volumes and qtrees.

- Oplocks are enabled on volumes by default.
- You cannot disable oplocks when you create a volume.
- You can enable or disable oplocks on existing volumes for SVMs at any time.

- You can enable oplocks on qtrees for SVMs.

  The oplock mode setting is a property of qtree ID 0, the default qtree that all volumes have. If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume, which is enabled by default. However, if you do specify an oplock setting on the new qtree, it takes precedence over the oplock setting on the volume.

If you want to…	Use this command…
Enable oplocks on volumes or qtrees	`volume qtree oplocks` with the `-oplock-mode` parameter set to `enable`
Disable oplocks on volumes or qtrees	`volume qtree oplocks` with the `-oplock-mode` parameter set to `disable`

Related information

Monitoring oplock status

Enable or disable oplocks on existing SMB shares

Oplocks are enabled on SMB shares on storage virtual machines (SVMs) by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenable oplocks.

About this task

If oplocks are enabled on the volume containing a share, but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over enabling oplocks on the volume. Disabling oplocks on the share, disables both opportunistic and lease oplocks. You can enable or disable oplocks on existing shares at any time.

Step

1. Perform the applicable action:

If you want to…	Then…
Enable oplocks on a share by modifying an existing share	Enter the following command: `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` ⓘ You can specify additional share properties to add by using a comma-delimited list. Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.

If you want to…	Then…
Disable oplocks on a share by modifying an existing share	Enter the following command: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` You can specify additional share properties to remove by using a comma-delimited list. Share properties that you remove are deleted from the existing list of share properties; however, previously configured share properties that you do not remove remain in effect.

Examples

The following command enables oplocks for the share named “Engineering” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

The following command disables oplocks for the share named “Engineering” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Related information

Enabling or disabling oplocks when creating SMB shares

Monitoring oplock status

Adding or removing share properties on an existing SMB share

Monitor oplock status

You can monitor and display information about oplock status. You can use this information to determine which files have oplocks, what the oplock level and oplock state level are, and whether oplock leasing is used. You can also determine information about locks that you might need to break manually.

About this task

You can display information about all oplocks in summary form or in a detailed list form. You can also use optional parameters to display information about a smaller subset of existing locks. For example, you can specify that the output return only locks with the specified client IP address or with the specified path.

You can display the following information about traditional and lease oplocks:

- SVM, node, volume, and LIF on which the oplock is established
- Lock UUID
- IP address of the client with the oplock
- Path at which the oplock is established
- Lock protocol (SMB) and type (oplock)
- Lock state
- Oplock level
- Connection state and SMB expiration time
- Open Group ID if a lease oplock is granted

See the `vserver oplocks show` man page for a detailed description of each parameter.

Steps

1. Display oplock status by using the `vserver locks show` command.

Examples

The following command displays default information about all locks. The oplock on the displayed file is granted with a `read-batch` oplock level:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

The following example displays more detailed information about the lock on a file with the path `/data2/data2_2/intro.pptx`. A lease oplock is granted on the file with a `batch` oplock level to a client with an IP address of `10.3.1.3`:

> When displaying detailed information, the command provides separate output for oplock and sharelock information. This example only shows the output from the oplock section.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Related information

Enabling or disabling oplocks when creating SMB shares

Enabling or disabling oplocks on existing SMB shares

Commands for enabling or disabling oplocks on volumes and qtrees

Apply Group Policy Objects to SMB servers

Apply Group Policy Objects to SMB servers overview

Your SMB server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all storage virtual machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your SMB server, ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your SMB server, the Active Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

Related information

Securing file access by using Dynamic Access Control (DAC)

SMB and NFS auditing and security tracing

Supported GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled storage virtual machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs:

- Advanced audit policy configuration settings:

  Object access: Central Access Policy staging

  Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:

  - Do not audit
  - Audit only success events
  - Audit only failure events
  - Audit both success and failure events

  > If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

  Set by using the `Audit Central Access Policy Staging` setting in the `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:

  - Group Policy refresh interval for CIFS-enabled SVM

    Set by using the `Registry` GPO.

  - Group Policy refresh random offset

    Set by using the `Registry` GPO.

- Hash publication for BranchCache

  The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:

  - Per-share
  - All-shares
  - Disabled
    Set by using the `Registry` GPO.

- Hash version support for BranchCache

  The following three hash version settings are supported:

  - BranchCache version 1
  - BranchCache version 2
  - BranchCache versions 1 and 2
    Set by using the `Registry` GPO.

> To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings

  - Audit policy and event log

    - Audit logon events

      Specifies the type of logon events to be audited, including the following settings:

      - Do not audit
      - Audit only success events
      - Audit on failure events
      - Audit both success and failure events
        Set by using the `Audit logon events` setting in the `Local Policies/Audit Policy` GPO.

        > If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

    - Audit object access

      Specifies the type of object access to be audited, including the following settings:

      - Do not audit
      - Audit only success events
      - Audit on failure events
      - Audit both success and failure events

Set by using the `Audit object access` setting in the `Local Policies/Audit Policy` GPO.

> If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Log retention method

  Specifies the audit log retention method, including the following settings:

  - Overwrite the event log when size of the log file exceeds the maximum log size
  - Do not overwrite the event log (clear log manually)
    Set by using the `Retention method for security log` setting in the `Event Log` GPO.

- Maximum log size

  Specifies the maximum size of the audit log.

  Set by using the `Maximum security log size` setting in the `Event Log` GPO.

> To use audit policy and event log GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

◦ File system security

Specifies a list of files or directories on which file security is applied through a GPO.

Set by using the `File System` GPO.

> The volume path to which the file system security GPO is configured must exist within the SVM.

◦ Kerberos policy

- Maximum clock skew

  Specifies maximum tolerance in minutes for computer clock synchronization.

  Set by using the `Maximum tolerance for computer clock synchronization` setting in the `Account Policies/Kerberos Policy` GPO.

- Maximum ticket age

  Specifies maximum lifetime in hours for user ticket.

  Set by using the `Maximum lifetime for user ticket` setting in the `Account Policies/Kerberos Policy` GPO.

- Maximum ticket renew age

  Specifies maximum lifetime in days for user ticket renewal.

Set by using the `Maximum lifetime for user ticket renewal` setting in the `Account Policies/Kerberos Policy` GPO.

- User rights assignment (privilege rights)
  - Take ownership

    Specifies the list of users and groups that have the right to take ownership of any securable object.

    Set by using the `Take ownership of files or other objects` setting in the `Local Policies/User Rights Assignment` GPO.

  - Security privilege

    Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.

    Set by using the `Manage auditing and security log` setting in the `Local Policies/User Rights Assignment` GPO.

  - Change notify privilege (bypass traverse checking)

    Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.

    The same privilege is required for users to receive notifications of changes to files and directories. Set by using the `Bypass traverse checking` setting in the `Local Policies/User Rights Assignment` GPO.

- Registry values
  - Signing required setting

    Specifies whether required SMB signing is enabled or disabled.

    Set by using the `Microsoft network server: Digitally sign communications (always)` setting in the `Security Options` GPO.

- Restrict anonymous

  Specifies what the restrictions for anonymous users are and includes the following three GPO settings:

  - No enumeration of Security Account Manager (SAM) accounts:

    This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

    Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts` setting in the `Local Policies/Security Options` GPO.

  - No enumeration of SAM accounts and shares

    This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` setting in the `Local Policies/Security Options` GPO.

- Restrict anonymous access to shares and named pipes

  This security setting restricts anonymous access to shares and pipes. This option is displayed as `no-access` in ONTAP if it is enabled.

  Set by using the `Network access: Restrict anonymous access to Named Pipes and Shares` setting in the `Local Policies/Security Options` GPO.

When displaying information about defined and applied group policies, the `Resultant restriction for anonymous user` output field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- `no-access`

  The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is enabled.

- `no-enumeration`

  The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Either the `Network access: Do not allow anonymous enumeration of SAM accounts` or the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs is enabled.

- `no-restriction`

  The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Both the `Network access: Do not allow anonymous enumeration of SAM accounts` and `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs are disabled.
    - Restricted Groups

      You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.

      Set by using the `Restricted Groups` GPO.

- Central access policy settings

  Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

Related information

Enabling or disabling GPO support on a CIFS server

Securing file access by using Dynamic Access Control (DAC)

SMB and NFS auditing and security tracing

Modifying the CIFS server Kerberos security settings

Using BranchCache to cache SMB share content at a branch office

Using SMB signing to enhance network security

Configuring bypass traverse checking

Configuring access restrictions for anonymous users

Requirements for using GPOs with your SMB server

To use Group Policy Objects (GPOs) with your SMB server, your system must meet several requirements.

- SMB must be licensed on the cluster.
- A SMB server must be configured and joined to a Windows Active Directory domain.
- The SMB server admin status must be on.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the SMB server computer object.
- GPO support must be enabled on the SMB server.

Enable or disable GPO support on a CIFS server

You can enable or disable Group Policy Object (GPO) support on a CIFS server. If you enable GPO support on a CIFS server, the applicable GPOs that are defined on the group policy—the policy that is applied to the organizational unit (OU) that contains the CIFS server computer object—are applied to the CIFS server.

About this task

GPOs cannot be enabled on CIFS servers in workgroup mode.

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable GPOs	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Disable GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Verify that GPO support is in the desired state: `vserver cifs group-policy show -vserver +vserver_name_`

   Group Policy Status for CIFS servers in workgroup mode is displayed as “disabled”.

Example

The following example enables GPO support on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Related information

Supported GPOs

Requirements for using GPOs with your CIFS server

How GPOs are updated on the CIFS server

Manually updating GPO settings on the CIFS server

Displaying information about GPO configurations

How GPOs are updated on the SMB server

How GPOs are updated on the CIFS server overview

By default, ONTAP retrieves and applies Group Policy Object (GPO) changes every 90 minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before ONTAP automatically updates them, you can trigger a manual update on a CIFS server with an ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes.

  This interval is configurable and can be set using the `Refresh interval` and `Random offset` GPO settings.

  ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active

Directory are higher than those on the CIFS server, ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

- Security Settings GPOs are refreshed every 16 hours.

  ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.

  > The 16-hour default value cannot be changed in the current ONTAP version. It is a Windows client default setting.

- All GPOs can be updated manually with an ONTAP command.

  This command simulates the Windows `gpupdate.exe`/force` command.

Related information

Manually updating GPO settings on the CIFS server

What to do if GPO updates are failing

Under some circumstances, Group Policy Object (GPO) updates from Windows 2012 domain controllers might fail, which leads to nothing being visible under the `Central Access Policy Settings` section of the output for the `vserver cifs group-policy show-defined` command. You should know how to correct this issue if it occurs.

Underlying cause	Remedy
When ONTAP attempts to connect to the Windows 2012 domain controller to perform the GPO update, the connection might fail with the error `error 0xc00000bd (NT STATUS_DUPLICATE_NAME).` This error occurs when the server name used to make the connection is different from the NetBIOS name of the CIFS server. There are various reasons this might occur, including the use of aliases. Additionally, ONTAP pads the NetBIOS name used when connecting to the domain controller to make the name length equal to 15 characters. This can make it appear that the CIFS server name and the NetBIOS name are different.	1. Disable NetBIOS name checking on the Windows server by adding the following registry key with the value set to `1`: `"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\DisableStrictNameChecking"` To learn more about this registry key, contact Microsoft Support. Microsoft Support 2. Reboot the domain controller.

Manually updating GPO settings on the CIFS server

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

Step

1. Perform the appropriate action:

If you want to update…	Enter the command…
Changed GPO settings	`vserver cifs group-policy update -vserver vserver_name`
All GPO settings	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Related information

How GPOs are updated on the CIFS server

Display information about GPO configurations

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

About this task

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFs server.

Steps

1. Display information about GPO configurations by performing one of the following actions:

If you want to display information about all Group Policy configurations…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Applied to a CIFS-enabled storage virtual machine (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
```

```
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache : version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
```

```
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
```

```
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
```

```
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Related information

Enabling or disabling GPO support on a CIFS server

Display detailed information about restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

About this task

By default, the following information is displayed:

- Group policy name
- Group policy version

- Link

  Specifies the level in which the group policy is configured. Possible output values include the following:

  - `Local` when the group policy is configured in ONTAP
  - `Site` when the group policy is configured at the site level in the domain controller
  - `Domain` when the group policy is configured at the domain level in the domain controller
  - `OrganizationalUnit` when the group policy is configured at the Organizational Unit (OU) level in the domain controller
  - `RSOP` for the resultant set of policies derived from all the group policies defined at various levels
- Restricted group name
- The users and groups who belong to and who do not belong to the restricted group
- The list of groups to which the restricted group is added

  A group can be a member of groups other than the groups listed here.

Step

1. Display information about all restricted group GPOs by performing one of the following actions:

If you want to display information about all restricted group GPOs…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Applied to a CIFS server	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Example

The following example displays information about restricted group GPOs defined in the Active Directory domain to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

The following example displays information about restricted groups GPOs applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

Related information

Display information about central access policies

You can display detailed information about the central access policies that are defined in Active Directory. You can also display information about the central access policies that are applied to the CIFS server through group policy objects (GPOs).

About this task

By default, the following information is displayed:

- SVM name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

CIFS servers in workgroup mode are not displayed because they do not support GPOs.

Step

1. Display information about central access policies by performing one of the following actions:

If you want to display information about all central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Applied to a CIFS server	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Example

The following example displays information for all the central access policies that are defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

The following example displays information for all the central access policies that are applied to the storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                  SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Related information

Securing file access by using Dynamic Access Control (DAC)

Displaying information about GPO configurations

Displaying information about central access policy rules

Display information about central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

Table 1. Step

If you want to display information about all central access policy rules associated with central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Applied to a CIFS server	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Example

The following example displays information for all central access policy rules associated with central access policies defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

The following example displays information for all central access policy rules associated with central access policies applied to storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Related information

Securing file access by using Dynamic Access Control (DAC)

Displaying information about GPO configurations

Displaying information about central access policies

Commands for managing SMB servers computer account passwords

You need to know the commands for changing, resetting, and disabling passwords, and for configuring automatic update schedules. You can also configure a schedule on the SMB server to update it automatically.

If you want to…	Use this command…
Change or reset the domain account password and you know the password	`vserver cifs domain password change`
Reset the domain account password and you do not know the password	`vserver cifs domain password reset`
Configure SMB servers for automatic computer account password changes	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Disable automatic computer account password changes on SMB servers	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

See the man page for each command for more information.

Manage domain controller connections

Display information about discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

Step

1. To display information related to discovered servers, enter the following command: `vserver cifs domain discovered-servers show`

Example

The following example shows discovered servers for SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Related information

Resetting and rediscovering servers

Stopping or starting the CIFS server

Reset and rediscover servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

Steps

1. Enter the following command: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Display information about the newly rediscovered servers: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Example

The following example resets and rediscovers servers for storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Related information

Displaying information about discovered servers

Stopping or starting the CIFS server

Manage domain controller discovery

Beginning with ONTAP 9.3, you can modify the default process by which domain controllers (DCs) are discovered. This enables you to limit discovery to your site or to a pool of preferred DCs, which can lead to performance improvements depending on the environment.

About this task

By default, the dynamic discovery process discovers all available DCs, including any preferred DCs, all DCs in the local site, and all remote DCs. This configuration can lead to latency in authentication and accessing shares in certain environments. If you have already determined the pool of DCs that you want to use, or if the remote DCs are inadequate or inaccessible, you can change the discovery method.

In ONTAP 9.3 and later releases, the `discovery-mode` parameter of the `cifs domain discovered-servers` command enables you to select one of the following discovery options:

- All DCs in the domain are discovered.
- Only DCs in the local site are discovered.

  The `default-site` parameter for the SMB server must be defined to use this mode.

- Server discovery is not performed, the SMB server configuration depends only on preferred DCs.

  To use this mode, you must first define the preferred DCs for the SMB server.

Step

1. Specify the desired discovery option: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

Options for the `mode` parameter:

- `all`

  Discover all available DCs (default).

- `site`

  Limit DC discovery to your site.

- `none`

  Use only preferred DCs and not perform discovery.

Add preferred domain controllers

ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

Step

1. To add to the list of preferred domain controllers, enter the following command:
   `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* specifies the storage virtual machine (SVM) name.

   `-domain` *`domain_name`* specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.

   `-preferred-dc` *`IP_address`*`,…` specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the SMB server on SVM vs1 uses to manage external access to the cifs.lab.example.com domain.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Related information

Commands for managing preferred domain controllers

Commands for managing preferred domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

If you want to…	Use this command…
Add a preferred domain controller	`vserver cifs domain preferred-dc add`
Display preferred domain controllers	`vserver cifs domain preferred-dc show`
Remove a preferred domain controller	`vserver cifs domain preferred-dc remove`

See the man page for each command for more information.

Related information

Adding preferred domain controllers

Enable SMB2 connections to domain controllers

Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller. Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB2 is enabled by default.

About this task

The `smb2-enabled-for-dc-connections` command option enables the system default for the release of ONTAP you are using. The system default for ONTAP 9.1 is enabled for SMB 1.0 and disabled for SMB 2.0. The system default for ONTAP 9.2 is enabled for SMB 1.0 and enabled for SMB 2.0. If the domain controller cannot negotiate SMB 2.0 initially, it uses SMB 1.0.

SMB 1.0 can be disabled from ONTAP to a domain controller. In ONTAP 9.1, if SMB 1.0 has been disabled, SMB 2.0 must be enabled in order to communicate with a domain controller.

Learn more about:

- Verifying enabled SMB versions.
- Supported SMB versions and functionality.

> If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server.

Steps

1. Before changing SMB security settings, verify which SMB versions are enabled: `vserver cifs security show`
2. Scroll down the list to see the SMB versions.
3. Perform the appropriate command, using the `smb2-enabled-for-dc-connections` option.

If you want SMB2 to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true`
Disabled	`vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false`

Enable encrypted connections to domain controllers

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted.

About this task

ONTAP requires encryption for domain controller (DC) communications when the `-encryption-required -for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3.

When encrypted DC communications are required, the `-smb2-enabled-for-dc-connections` option is ignored, because ONTAP only negotiates SMB3 connections. If a DC doesn't support SMB3 and encryption, ONTAP will not connect with it.

Step

1. Enable encrypted communication with the DC: `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Use null sessions to access storage in non-Kerberos environments

Use null sessions to access storage in non-Kerberos environments overview

Null session access provides permissions for network resources, such as storage system data, and to client-based services running under the local system. A null session occurs when a client process uses the "system" account to access a network resource. Null session configuration is specific to non-Kerberos authentication.

How the storage system provides null session access

Because null session shares do not require authentication, clients that require null session access must have their IP addresses mapped on the storage system.

By default, unmapped null session clients can access certain ONTAP system services, such as share enumeration, but they are restricted from accessing any storage system data.

ONTAP supports Windows RestrictAnonymous registry setting values with the `-restrict-anonymous` option. This enables you to control the extent to which unmapped null users can view or access system resources. For example, you can disable share enumeration and access to the IPC$ share (the hidden named pipe share). The `vserver cifs options modify` and `vserver cifs options show` man pages provide more information about the `-restrict-anonymous` option.

Unless otherwise configured, a client running a local process that requests storage system access through a null session is a member only of nonrestrictive groups, such as “everyone”. To limit null session access to selected storage system resources, you might want to create a group to which all null session clients belong; creating this group enables you to restrict storage system access and to set storage system resource permissions that apply specifically to null session clients.

ONTAP provides a mapping syntax in the `vserver name-mapping` command set to specify the IP address of clients allowed access to storage system resources using a null user session. After you create a group for null users, you can specify access restrictions for storage system resources and resource permissions that apply only to null sessions. Null user is identified as anonymous logon. Null users do not have access to any home directory.

Any null user accessing the storage system from a mapped IP address is granted mapped user permissions. Consider appropriate precautions to prevent unauthorized access to storage systems mapped with null users. For maximum protection, place the storage system and all clients requiring null user storage system access on a separate network, to eliminate the possibility of IP address “spoofing”.

Related information

Configuring access restrictions for anonymous users

Grant null users access to file system shares

You can allow access to your storage system resources by null session clients by assigning a group to be used by null session clients and recording the IP addresses of null session clients to add to the storage system’s list of clients allowed to access data using null sessions.

Steps

1. Use the `vserver name-mapping create` command to map the null user to any valid windows user, with an IP qualifier.

   The following command maps the null user to user1 with a valid host name google.com:

   ```
   vserver name-mapping create –direction win-unix  -position 1 –pattern
   “ANONYMOUS LOGON” –replacement user1 – hostname google.com
   ```

   The following command maps the null user to user1 with a valid IP address 10.238.2.54/32:

   ```
   vserver name-mapping create –direction win-unix  -position 2 –pattern
   “ANONYMOUS LOGON” –replacement user1 –address 10.238.2.54/32
   ```

2. Use the `vserver name-mapping show` command to confirm the name mapping.

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1        -                10.72.40.83/32      Pattern: anonymous logon
                                           Replacement: user1
```

3. Use the `vserver cifs options modify –win-name-for-null-user` command to assign Windows membership to the null user.

   This option is applicable only when there is a valid name mapping for the null user.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Use the `vserver cifs options show` command to confirm the mapping of the null user to the Windows user or group.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Manage NetBIOS aliases for SMB servers

Manage NetBIOS aliases for SMB servers overview

NetBIOS aliases are alternative names for your SMB server that SMB clients can use when connecting to the SMB server. Configuring NetBIOS aliases for a SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original file servers' names.

You can specify a list of NetBIOS aliases when you create the SMB server or at any time after you create the SMB server. You can add or remove NetBIOS aliases from the list at any time. You can connect to the SMB server using any of the names in the NetBIOS alias list.

Related information

Displaying information about NetBIOS over TCP connections

Add a list of NetBIOS aliases to the SMB server

If you want SMB clients to connect to the SMB server by using an alias, you can create a list of NetBIOS aliases, or you can add NetBIOS aliases to an existing list of NetBIOS aliases.

About this task

- The NetBIOS alias name can be 15 up to characters in length.
- You can configure up to 200 NetBIOS aliases on the SMB server.
- The following characters are not allowed:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Steps

1. Add the NetBIOS aliases:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - You can specify one or more NetBIOS aliases by using a comma-delimited list.
   - The specified NetBIOS aliases are added to the existing list.
   - A new list of NetBIOS aliases is created if the list is currently empty.
2. Verify that the NetBIOS aliases were added correctly: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

Related information

Removing NetBIOS aliases from the NetBIOS alias list

Displaying the list of NetBIOS aliases on CIFS servers

Remove NetBIOS aliases from the NetBIOS alias list

If you do not need specific NetBIOS aliases for a CIFS server, you can remove those NetBIOS aliases from the list. You can also remove all NetBIOS aliases from the list.

About this task

You can remove more than one NetBIOS alias by using a comma-delimited list. You can remove all of the NetBIOS aliases on a CIFS server by specifying – as the value for the `-netbios-aliases` parameter.

Steps

1. Perform one of the following actions:

If you want to remove…	Enter…
Specific NetBIOS aliases from the list	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
All NetBIOS aliases from the list	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verify that the specified NetBIOS aliases were removed: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Display the list of NetBIOS aliases on CIFS servers

You can display the list of NetBIOS aliases. This can be useful when you want to determine the list of names over which SMB clients can make connections to the CIFS server.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter…
A CIFS server's NetBIOS aliases	`vserver cifs show -display-netbios -aliases`
The list of NetBIOS aliases as part of the detailed CIFS server information	`vserver cifs show -instance`

The following example displays information about a CIFS server's NetBIOS aliases:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example displays the list of NetBIOS aliases as part of the detailed CIFS server information:

`vserver cifs show -instance`

```
                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

See the man page for the commands for more information.

Related information

Adding a list of NetBIOS aliases to the CIFS server

Commands for managing CIFS servers

Determine whether SMB clients are connected using NetBIOS aliases

You can determine whether SMB clients are connected using NetBIOS aliases, and if so, which NetBIOS alias is used to make the connection. This can be useful when troubleshooting connection issues.

About this task

You must use the `-instance` parameter to display the NetBIOS alias (if any) associated with an SMB connection. If the CIFS server name or an IP address is used to make the SMB connection, the output for the `NetBIOS Name` field is - (hyphen).

Step

1. Perform the desired action:

If you want to display NetBIOS information for…	Enter…
SMB connections	`vserver cifs session show -instance`

If you want to display NetBIOS information for…	Enter…
Connections using a specified NetBIOS alias:	`vserver cifs session show -instance -netbios-name` *netbios_name*

The following example displays information about the NetBIOS alias used to make the SMB connection with session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                Open Shares: 2
                 Open Files: 2
                 Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Manage miscellaneous SMB server tasks

Stop or start the CIFS server

You can stop the CIFS server on a SVM, which can be useful when performing tasks while users are not accessing data over SMB shares. You can restart SMB access by starting the CIFS server. By stopping the CIFS server, you can also modify the protocols allowed on the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Stop the CIFS server	`vserver cifs stop -vserver` *`vserver_name`* `[-foreground {true|false}]`
Start the CIFS server	`vserver cifs start -vserver` *`vserver_name`* `[-foreground {true|false}]`

`-foreground` specifies whether the command should execute in the foreground or background. If you do not enter this parameter, it is set to `true`, and the command is executed in the foreground.

2. Verify that the CIFS server administrative status is correct by using the `vserver cifs show` command.

Example

The following commands start the CIFS server on SVM vs1:

```
cluster1::> vserver start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Related information

Displaying information about discovered servers

Resetting and rediscovering servers

Move CIFS servers to different OUs

The CIFS server create-process uses the default organizational unit (OU) CN=Computers during setup unless you specify a different OU. You can move CIFS servers to different OUs after setup.

Steps

1. On the Windows server, open the **Active Directory Users and Computers** tree.
2. Locate the Active Directory object for the storage virtual machine (SVM).
3. Right-click the object and select **Move**.
4. Select the OU that you want to associate with the SVM

Results

The SVM object is placed in the selected OU.

Modify the dynamic DNS domain on the SVM before moving the SMB server

If you want the Active Directory-integrated DNS server to dynamically register the SMB server's DNS records in DNS when you move the SMB server to another domain, you must modify dynamic DNS (DDNS) on the storage virtual machine (SVM) before moving the SMB server.

Before you begin

DNS name services must be modified on the SVM to use the DNS domain that contains the service location records for the new domain that will contain the SMB server computer account. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers.

About this task

Although DDNS (if configured on the SVM) automatically adds the DNS records for data LIFs to the new domain, the DNS records for the original domain are not automatically deleted from the original DNS server. You must delete them manually.

To complete your DDNS modifications before moving the SMB server, see the following topic:

Configure dynamic DNS services

Join a SVM to an Active Directory domain

You can join a storage virtual machine (SVM) to an Active Directory domain without deleting the existing SMB server by modifying the domain using the `vserver cifs modify` command. You can rejoin the current domain or join a new one.

Before you begin

- The SVM must already have a DNS configuration.
- The DNS configuration for the SVM must be able to serve the target domain.

  The DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

About this task

- The administrative status of the CIFS server must be set to "down" to proceed with Active Directory domain modification.
- If the command completes successfully, the administrative status is automatically set to "up".
- When joining a domain, this command might take several minutes to complete.

Steps

1. Join the SVM to the CIFS server domain: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   For more information, see the man page for the `vserver cifs modify` command. If you need to reconfigure DNS for the new domain, see the man page for the `vserver dns modify` command.

In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou= example ou` container within the *example*.com domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

2. Verify that the CIFS server is in the desired Active Directory domain: `vserver cifs show`

Example

In the following example, the SMB server “CIFSSERVER1” on SVM vs1 joins the example.com domain using keytab authentication:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Display information about NetBIOS over TCP connections

You can display information about NetBIOS over TCP (NBT) connections. This can be useful when troubleshooting NetBIOS-related issues.

Step

1. Use the `vserver cifs nbtstat` command to display information about NetBIOS over TCP connections.

   NetBIOS name service (NBNS) over IPv6 is not supported.

Example

The following example shows the NetBIOS name service information displayed for “cluster1”:

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Commands for managing SMB servers

You need to know the commands for creating, displaying, modifying, stopping, starting, and deleting SMB servers. There are also commands to reset and rediscover servers, change or reset machine account passwords, schedule changes for machine account passwords, and add or remove NetBIOS aliases.

If you want to…	Use this command…
Create an SMB server	`vserver cifs create`
Display information about an SMB server	`vserver cifs show`
Modify an SMB server	`vserver cifs modify`
Move an SMB server to another domain	`vserver cifs modify`

Stop an SMB server	`vserver cifs stop`
Start an SMB server	`vserver cifs start`
Delete an SMB server	`vserver cifs delete`
Reset and rediscover servers for the SMB server	`vserver cifs domain discovered-servers reset-servers`
Change the SMB server's machine account password	`vserver cifs domain password change`
Reset the SMB server's machine account password	`vserver cifs domain password change`
Schedule automatic password changes for the SMB server's machine account	`vserver cifs domain password schedule modify`
Add NetBIOS aliases for the SMB server	`vserver cifs add-netbios-aliases`
Remove NetBIOS aliases for the SMB server	`vserver cifs remove-netbios-aliases`

See the man page for each command for more information.

Related information

What happens to local users and groups when deleting SMB servers

Enable the NetBios name service

Beginning with ONTAP 9, the NetBios name service (NBNS, sometimes called Windows Internet Name Service or WINS) is disabled by default. Previously, CIFS-enabled storage virtual machines (SVMs) sent name registration broadcasts regardless of whether WINS was enabled on a network. To limit such broadcasts to configurations where NBNS is required, you must enable NBNS explicitly for new CIFS servers.

Before you begin

- If you are already using NBNS and you upgrade to ONTAP 9, it is not necessary to complete this task. NBNS will continue to work as before.
- NBNS is enabled over UDP (port 137).
- NBNS over IPv6 is not supported.

Steps

1. Set the privilege level to advanced.

```
set -privilege advanced
```

2. Enable NBNS on a CIFS server.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Return to the admin privilege level.

```
set -privilege admin
```

Use IPv6 for SMB access and SMB services

Requirements for using IPv6

Before you can use IPv6 on your SMB server, you need to know which versions of ONTAP and SMB support it and what the license requirements are.

ONTAP license requirements

No special license is required for IPv6 when SMB is licensed.

SMB protocol version requirements

- For SVMs, ONTAP supports IPv6 on all versions of the SMB protocol.

NetBIOS name service (NBNS) over IPv6 is not supported.

Support for IPv6 with SMB access and CIFS services

If you want to use IPv6 on your CIFS server, you need to be aware of how ONTAP supports IPv6 for SMB access and network communication for CIFS services.

Windows client and server support

ONTAP provides support for Windows servers and clients that support IPv6. The following describes Microsoft Windows client and server IPv6 support:

- Windows XP and Windows 2003 support IPv6 for SMB file sharing.

  These versions provide limited support for IPv6.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 and later support IPv6 for both SMB file sharing and Active Directory services, including DNS, LDAP, CLDAP, and Kerberos services.

  If IPv6 addresses are configured, Windows 7 and Windows Server 2008 and later releases use IPv6 by default for Active Directory services. Both NTLM and Kerberos authentication over IPv6 connections are supported.

  All Windows clients supported by ONTAP can connect to SMB shares by using IPv6 addresses.

For the latest information about which Windows clients ONTAP supports, see the Interoperability Matrix.

Interoperability Matrix

NT domains are not supported for IPv6.

Additional CIFS services support

In addition to IPv6 support for SMB file shares and Active Directory services, ONTAP provides IPv6 support for the following:

- Client-side services, including offline folders, roaming profiles, folder redirection, and Previous Versions
- Server-side services, including Dynamic home directories (Home Directory feature), symlinks and Widelinks, BranchCache, ODX copy offload, automatic node referrals, and Previous Versions
- File access management services, including the use of Windows local users and groups for access control and rights management, setting file permissions and audit policies using the CLI, security tracing, file locks management, and monitoring SMB activity
- NAS multiprotocol auditing
- FPolicy
- Continuously available shares, Witness protocol, and Remote VSS (used with Hyper-V over SMB configurations)

Name service and authentication service support

Communication with the following name services are supported with IPv6:

- Domain controllers
- DNS servers
- LDAP servers
- KDC servers
- NIS servers

How CIFS servers use IPv6 to connect to external servers

To create a configuration that meets your requirements, you must be aware of how CIFS servers use IPv6 when making connections to external servers.

- Source address selection

  If an attempt is made to connect to an external server, the source address selected must be of the same type as the destination address. For example, if connecting to an IPv6 address, the storage virtual machine (SVM) hosting the CIFS server must have a data LIF or management LIF that has an IPv6 address to use as the source address. Similarly, if connecting to an IPv4 address, the SVM must have a data LIF or management LIF that has an IPv4 address to use as the source address.

- For servers dynamically discovered using DNS, server discovery is performed as follows:
  - If IPv6 is disabled on the cluster, only IPv4 servers addresses are discovered.
  - If IPv6 is enabled on the cluster, both IPv4 and IPv6 server addresses are discovered. Either type might be used depending upon the suitability of the server to which the address belongs and the

availability of IPv6 or IPv4 data or management LIFs.
Dynamic server discovery is used for discovering Domain Controllers and their associated services, such as LSA, NETLOGON, Kerberos, and LDAP.

- DNS server connectivity

  Whether the SVM uses IPv6 when connecting to a DNS server depends on the DNS name services configuration. If DNS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the DNS name services configuration can use IPv4 addresses so that connections to DNS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring DNS name services.

- LDAP server connectivity

  Whether the SVM uses IPv6 when connecting to an LDAP server depends on the LDAP client configuration. If the LDAP client is configured to use IPv6 addresses, connections are made by using IPv6. If desired, the LDAP client configuration can use IPv4 addresses so that connections to LDAP servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring the LDAP client configuration.

  > The LDAP client configuration is used when configuring LDAP for UNIX user, group, and netgroup name services.

- NIS server connectivity

  Whether the SVM uses IPv6 when connecting to a NIS server depends on the NIS name services configuration. If NIS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the NIS name services configuration can use IPv4 addresses so that connections to NIS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring NIS name services.

  > NIS name services are used for storing and managing UNIX user, group, netgroup, and host name objects.

Related information

Enabling IPv6 for SMB (cluster administrators only)

Monitoring and displaying information about IPv6 SMB sessions

Enable IPv6 for SMB (cluster administrators only)

IPv6 networks are not enabled during cluster setup. A cluster administrator must enable IPv6 after cluster setup is complete to use IPv6 for SMB. When the cluster administrator enables IPv6, it is enabled for the entire cluster.

Step

1. Enable IPv6: `network options ipv6 modify -enabled true`

   For more information about enabling IPv6 on the cluster and configuring IPv6 LIFs, see the *Network Management Guide*.

   IPv6 is enabled. IPv6 data LIFs for SMB access can be configured.

Related information

Monitoring and displaying information about IPv6 SMB sessions

Network management

Disable IPv6 for SMB

Even though IPv6 is enabled on the cluster using a network option, you cannot disable IPv6 for SMB by using the same command. Instead, ONTAP disables IPv6 when the cluster administrator disables the last IPv6-enabled interface on the cluster. You should communicate with the cluster administrator about management of your IPv6 enabled interfaces.

For more information about disabling IPv6 on the cluster, see the *Network Management Guide*.

Related information

Network management

Monitor and display information about IPv6 SMB sessions

You can monitor and display information about SMB sessions that are connected using IPv6 networks. This information is useful in determining which clients are connecting using IPv6 as well as other useful information about IPv6 SMB sessions.

Step

1. Perform the desired action:

If you want to determine whether…	Enter the command…
SMB sessions to a storage virtual machine (SVM) are connected using IPv6	`vserver cifs session show -vserver vserver_name -instance`
IPv6 is used for SMB sessions through a specified LIF address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` `LIF_IP_address` is the data LIF's IPv6 address.

Set up file access using SMB

Configure security styles

How security styles affect data access

What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your

purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
UNIX	NFS	NFSv3 mode bits	UNIX	NFS and SMB
		NFSv4.x ACLs	UNIX	
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.x ACLs	UNIX	
NTFS ACLs	NTFS	Unified	NFS or SMB	
NFSv3 mode bits	UNIX			
NFSv4.1 ACLs	UNIX	NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		NTFS ACLs

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see FlexGroup volumes management overview.

Beginning with ONTAP 9.2, the `show-effective-permissions` parameter to the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission.

ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

2021-12-09, BURT 1443623

Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Decide which security style to use on SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if…
UNIX	• The file system is managed by a UNIX administrator. • The majority of users are NFS clients. • An application accessing the data uses a UNIX user as the service account.
NTFS	• The file system is managed by a Windows administrator. • The majority of users are SMB clients. • An application accessing the data uses a Windows user as the service account.
Mixed	The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Configure security styles on SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

   The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created: `vserver show -vserver vserver_name`

Configure security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If the FlexVol volume…	Use the command…
Does not yet exist	`volume create` and include the `-security -style` parameter to specify the security style.
Already exists	`volume modify` and include the `-security -style` parameter to specify the security style.

   The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

   If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

   For more information about the `volume create` or `volume modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

   ```
   volume show -volume volume_name -instance
   ```

Configure security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:

If the qtree…	Use the command…
Does not exist yet	`volume qtree create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume qtree modify` and include the `-security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree qtree_name -instance`

Create and manage data volumes in NAS namespaces

Create and manage data volumes in NAS namespaces overview

To manage file access in a NAS environment, you must manage data volumes and junction points on your storage virtual machine (SVM). This includes planning your namespace architecture, creating volumes with or without junction points, mounting or unmounting volumes, and displaying information about data volumes and NFS server or CIFS server namespaces.

Create data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

Before you begin

The aggregate in which you want to create the volume must already exist.

> The following characters cannot be used in the junction path: * # " > < | ? \
>
> In addition, the junction path length cannot be more than 255 characters.

Steps

1. Create the volume with a junction point: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the

volume name.

Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

The junction path is case insensitive; `/ENG` is the same as `/eng`. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is `/ENG`, the path of a CIFS share must start with `/ENG`, not `/eng`.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created with the desired junction point: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Example

The following example creates a volume named "home4" located on SVM vs1 that has a junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Create data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

Before you begin

The aggregate in which you want to create the volume must already exist.

Steps

1. Create the volume without a junction point by using the following command: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize

difficult-to-troubleshoot file-access issues.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point: `volume show -vserver vserver_name -volume volume_name -junction`

Example

The following example creates a volume named “sales” located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Mount or unmount existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount and offline a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume’s namespace, are inaccessible to NAS clients.

> To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must offline the volume, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article:https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/NFSv3_clients_still_have_access_to_a_volume_after_being_removed_from_the_namespace_in_ONTAP[NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP]

When you unmount and offline a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

If you want to…	Enter the commands…
Mount a volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`
Unmount a volume	`volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name`

2. Verify that the volume is in the desired mount state: `volume show -vserver vserver_name -volume volume_name -fields state,junction-path,junction-active`

Examples

The following example mounts a volume named “sales” located on SVM vs1 to the junction point `/sales`:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

The following example unmounts and offlines a volume named “data” located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Display volume mount and junction point information

You can display information about mounted volumes for storage virtual machines (SVMs)

and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

Steps

1. Perform the desired action:

If you want to display…	Enter the command…
Summary information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -junction`
Detailed information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Specific information about mounted and unmounted volumes on the SVM	a. If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?` b. Display the desired information by using the `-fields` parameter: volume show -vserver vserver_name -fields fieldname,…

Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configure name mappings

Configure name mappings overview

ONTAP uses name mapping to map CIFS identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to CIFS identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a CIFS client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use CIFS access or NTFS security style on volumes.
- You configure the default user to be used instead.

  In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID.

How name mapping works

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

  If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

  If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default CIFS user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

  Even if name mappings for machine accounts are defined, the mappings are ignored.

Multidomain searches for UNIX user to Windows user name mappings

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the CIFS server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the CIFS server on the SVM belongs.

- *Bidirectional trust*

  With bidirectional trusts, both domains trust each other. If the CIFS server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

  UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

- *Outbound trust*

  With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

  A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

- *Inbound trust*

  With an inbound trust, the other domain trusts the CIFS server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

  A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

How wildcards (*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user "root" is mapped to the user named "administrator". All trusted domains are searched in order until the first matching user named "administrator" is found.
*	**	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found. The pattern ** is only valid for name mapping from UNIX to Windows, not the other way around.

How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by ONTAP
- Use the preferred trusted domain list that you compile

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

Name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

Create a name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

Step

1. Create a name mapping: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string `" "` (the space character). See the `vserver name-mapping create` man page for details.

   When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

Examples

The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes “$” as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john$ops to UNIX user john_ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure the default user

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

Steps

1. Perform one of the following actions:

If you want to…	Enter the following command…
Configure the default UNIX user	`vserver cifs options modify -default -unix-user` *user_name*
Configure the default Windows user	`vserver nfs modify -default-win-user` *user_name*

Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

See the man page for each command for more information.

Configure multidomain name-mapping searches

Enable or disable multidomain name mapping searches

With multidomain name mapping searches, you can use a wild card (*) in the domain portion of a Windows name when configuring UNIX user to Windows user name mapping. Using a wild card (*) in the domain portion of the name enables ONTAP to search all domains that have a bidirectional trust with the domain that contains the CIFS server's computer account.

About this task

As an alternative to searching all bidirectionally trusted domains, you can configure a list of preferred trusted domains. When a list of preferred trusted domains is configured, ONTAP uses the preferred trusted domain list instead of the discovered bidirectionally trusted domains to perform multidomain name mapping searches.

- Multidomain name mapping searches are enabled by default.
- This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want multidomain name mapping searches to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Related information

Available SMB server options

Reset and rediscover trusted domains

You can force the rediscovery of all the trusted domains. This can be useful when the trusted domain servers are not responding appropriately or the trust relationships have changed. Only domains with a bidirectional trust with the home domain, which is the domain containing the CIFS server's computer account, are discovered.

Step

1. Reset and rediscover trusted domains by using the `vserver cifs domain trusts rediscover` command.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Related information

Displaying information about discovered trusted domains

Display information about discovered trusted domains

You can display information about the discovered trusted domains for the CIFS server's home domain, which is the domain containing the CIFS server's computer account. This can be useful when you want to know which trusted domains are discovered and how they are ordered within the discovered trusted-domain list.

About this task

Only the domains with bidirectional trusts with the home domain are discovered. Since the home domain's domain controller (DC) returns the list of trusted domains in an order determined by the DC, the order of the domains within the list cannot be predicted. By displaying the list of trusted domains, you can determine the search order for multidomain name mapping searches.

The displayed trusted domain information is grouped by node and storage virtual machine (SVM).

Step

1. Display information about discovered trusted domains by using the `vserver cifs domain trusts show` command.

   `vserver cifs domain trusts show -vserver vs1`

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Related information

Resetting and rediscovering trusted domains

Add, remove, or replace trusted domains in preferred trusted domain lists

You can add or remove trusted domains from the preferred trusted domain list for the SMB server or you can modify the current list. If you configure a preferred trusted domain list, this list is used instead of the discovered bidirectional trusted domains when performing multidomain name mapping searches.

About this task

- If you are adding trusted domains to an existing list, the new list is merged with the existing list with the new entries placed at the end. The trusted domains are searched in the order they appear in the trusted domain list.
- If you are removing trusted domains from the existing list and do not specify a list, the entire trusted domain list for the specified storage virtual machine (SVM) is removed.
- If you modify the existing list of trusted domains, the new list overwrites the existing list.

> You should enter only bidirectionally trusted domains in the preferred trusted domain list. Even though you can enter outbound or inbound trust domains into the preferred domain list, they are not used when performing multidomain name mapping searches. ONTAP skips the entry for the unidirectional domain and moves on to the next bidirectional trusted domain in the list.

Step

1. Perform one of the following actions:

If you want to do the following with the list of preferred trusted domains…	Use the command…
Add trusted domains to the list	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Remove trusted domains from the list	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modify the existing list	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Examples

The following command adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred trusted domain list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command removes two trusted domains from the list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command modifies the trusted domain list used by SVM vs1. The new list replaces the original list:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Related information

Displaying information about the preferred trusted domain list

Display information about the preferred trusted domain list

You can display information about which trusted domains are in the preferred trusted domain list and the order in which they are searched if multidomain name mapping searches are enabled. You can configure a preferred trusted domain list as an alternative

to using the automatically discovered trusted domain list.

Steps

1. Perform one of the following actions:

If you want to display information about the following…	Use the command…
All preferred trusted domains in the cluster grouped by storage virtual machine (SVM)	`vserver cifs domain name-mapping-search show`
All preferred trusted domains for a specified SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

The following command displays information about all preferred trusted domains on the cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ---------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Related information

Adding, removing, or replacing trusted domains in preferred trusted domain lists

Create and configure SMB shares

Create and configure SMB shares overview

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the storage virtual machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you recreate the CIFS server on the SVM, you must re-create the SMB shares.

Related information

Manage file access using SMB

SMB configuration for Microsoft Hyper-V and SQL Server

Configure character mapping for SMB file name translation on volumes

What the default administrative shares are

When you create a CIFS server on your storage virtual machine (SVM), three default administrative shares are automatically created. You should understand what those default shares are and how they are used.

ONTAP creates the following default administrative shares when you create the CIFS server:

- ipc$
- admin$
- c$

Because shares that end with the $ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

How the ipc$ and admin$ default shares are used

The ipc$ and admin$ shares are used by ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

- ipc$ share

  The ipc$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc$ share is used during remote administration of a computer and when viewing a computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc$ share. You also cannot rename or delete the ipc$ share.

- admin$ share

  The admin$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin$ share. You also cannot rename or delete the admin$ share.

How the c$ default share is used

The c$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c$ share:

- The path for this share is always the path to the SVM root volume and cannot be modified.
- The default ACL for the c$ share is Administrator / Full Control.

  This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.

- You can change the c$ share's ACL.
- You can change the c$ share settings and share properties.
- You cannot delete the c$ share.
- The SVM administrator can access the rest of the SVM namespace from the mapped c$ share by crossing the namespace junctions.

- The c$ share can be accessed by using the Microsoft Management Console.

Related information

Configuring advanced NTFS file permissions using the Windows Security tab

SMB share naming requirements

You should keep the ONTAP share naming requirements in mind when creating SMB shares on your SMB server.

Share naming conventions for ONTAP are the same as for Windows and include the following requirements:

- The name of each share must be unique for the SMB server.
- Share names are not case-sensitive.
- The maximum share name length is 80 characters.
- Unicode share names are supported.
- Share names ending with the $ character are hidden shares.
- The ADMIN$, IPC$, and c$ administrative shares are automatically created on every CIFS server and are reserved share names.
- You cannot use the share name ONTAP_ADMIN$ when creating a share.
- Share names containing spaces are supported:
  - You cannot use a space as the first character or as the last character in a share name.
  - You must enclose share names containing a space in quotation marks.

  Single quotation marks are considered part of the share name and cannot be used in place of quotation marks.

- The following special characters are supported when you name SMB shares:

  ! @ # $ % & ' _ - . ~ ( ) { }

- The following special characters are not supported when you name SMB shares:

  " / \ : ; | < > , ? * =

Directory case-sensitivity requirements when creating shares in a multiprotocol environment

If you create shares in an SVM where the 8.3 naming scheme is used to distinguish between directory names where there are only case differences between the names, you must use the 8.3 name in the share path to ensure that the client connects to the desired directory path.

In the following example, two directories named “testdir” and “TESTDIR” were created on a Linux client. The junction path of the volume containing the directories is `/home`. The first output is from a Linux client and the second output is from an SMB client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

When you create a share to the second directory, you must use the 8.3 name in the share path. In this example, the share path to the first directory is `/home/testdir` and the share path to the second directory is `/home/TESTDI~1`.

Use SMB share properties

Use SMB share properties overview

You can customize the properties of SMB shares.

The available share properties are as follows:

Share properties	Description
`oplocks`	This property specifies that the share uses opportunistic locks, also known as client-side caching.
`browsable`	This property allows Windows clients to browse the share.
`showsnapshot`	This property specifies that Snapshot copies can be viewed and traversed by clients.
`changenotify`	This property specifies that the share supports Change Notify requests. For shares on an SVM, this is a default initial property.
`attributecache`	This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.

Share properties	Description
`continuously-available`	This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
`branchcache`	This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify “per-share” as the operating mode in the CIFS BranchCache configuration.
`access-based-enumeration`	This property specifies that *Access Based Enumeration* (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user’s access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
`namespace-caching`	This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1 clients do not cache directory enumeration results. Because SMB 2 and SMB 3 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1 client connections.
`encrypt-data`	This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.

Add or remove share properties on an existing SMB share

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

Before you begin

The share whose properties you want to modify must exist.

About this task

Guidelines for adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect.

Newly added properties are appended to the existing list of share properties.

- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the `vserver cifs share properties add` command.

  You can use the `vserver cifs share properties remove` command to remove share properties.

Guidelines for removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.

Steps

1. Enter the appropriate command:

If you want to…	Enter the command…
Add share properties	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remove share properties	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verify the share property settings: `vserver cifs share show -vserver vserver_name -share -name share_name`

Examples

The following command adds the `showsnapshot` share property to a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

The following command removes the `browsable` share property from a share named “share2” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path      Properties   Comment    ACL
---------  ------   --------  ----------   --------   -----------
vs1        share2   /share2   oplocks      -          Everyone / Full
Control
                              changenotify
```

Related information

Commands for managing SMB shares

Optimize SMB user access with the force-group share setting

When you create a share from the ONTAP command line to data with UNIX effective security, you can specify that all files created by SMB users in that share belong to the same group, known as the *force-group*, which must be a predefined group in the UNIX group database. Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups.

Specifying a force-group is meaningful only if the share is in a UNIX or mixed qtree. There is no need to set a force-group for shares in an NTFS volume or qtree because access to files in these shares is determined by Windows permissions, not UNIX GIDs.

If a force-group has been specified for a share, the following becomes true of the share:

- SMB users in the force-group who access this share are temporarily changed to the GID of the force-group.

  This GID enables them to access files in this share that are not accessible normally with their primary GID or UID.

- All files in this share created by SMB users belong to the same force-group, regardless of the primary GID of the file owner.

When SMB users try to access a file created by NFS, the SMB users' primary GIDs determine access rights.

The force-group does not affect how NFS users access files in this share. A file created by NFS acquires the GID from the file owner. Determination of access permissions is based on the UID and primary GID of the NFS user who is trying to access the file.

Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups. For example, if you want to create a share to store the company's web pages and give write access to users in the Engineering and Marketing departments, you can create a share and give write access to a force-group named "webgroup1". Because of the force-group, all files created by SMB users in this share are owned by the "webgroup1" group. In addition, users are automatically assigned the GID of the "webgroup1" group when accessing the share. As a result, all the users can write to this share without you needing to manage the access rights of the users in the Engineering and Marketing departments.

Related information

Creating an SMB share with the force-group share setting

Create an SMB share with the force-group share setting

You can create an SMB share with the force-group share setting if you want SMB users that access data on volumes or qtrees with UNIX file security to be regarded by ONTAP as belonging to the same UNIX group.

Step

1. Create the SMB share: `vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name`

   If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial "`\\`" in the UNC path), then the **Security** tab in the Windows Properties box is unavailable. This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

   If you want to remove the force-group after the share is created, you can modify the share at any time and specify an empty string ("") as the value for the `-force-group-for-create` parameter. If you remove the force-group by modifying the share, all existing connections to this share continue to have the previously set force-group as the primary GID.

Example

The following command creates a "webpages" share that is accessible on the web in the `/corp/companyinfo` directory in which all files that SMB users create are assigned to the webgroup1 group:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Related information

Optimize SMB user access with the force-group share setting

View information about SMB shares using the MMC

You can view information about SMB shares on your SVM and perform some management tasks using the Microsoft Management Console (MMC). Before you can view the shares, you need to connect the MMC to the SVM.

About this task

You can perform the following tasks on shares contained within SVMs using the MMC:

- View shares
- View active sessions
- View open files
- Enumerate the list of sessions, files and tree connections in the system
- Close open files in the system
- Close open sessions
- Create/manage shares

The views displayed by the preceding capabilities are node specific and not cluster specific. Therefore, when you use the MMC to connect to the SMB server host name (that is, cifs01.domain.local), you are routed, based on how you have set up DNS, to a single LIF within your cluster.

The following functions are not supported in MMC for ONTAP:

- Creating new local users/groups
- Managing/viewing existing local users/groups
- Viewing events or performance logs
- Storage
- Services and applications

In instances where the operation is not supported, you might experience `remote procedure call failed` errors.

FAQ: Using Windows MMC with ONTAP

Steps

1. To open Computer Management MMC on any Windows server, in the **Control Panel**, select **Administrative Tools** > **Computer Management**.
2. Select **Action** > **Connect to another computer**.

   The Select Computer dialog box appears.
3. Type the name of the storage system or click **Browse** to locate the storage system.
4. Click **OK**.

   The MMC connects to the SVM.
5. In the navigation pane, click **Shared Folders** > **Shares**.

   A list of shares on the SVM is displayed in the right display pane.
6. To display the share properties for a share, double-click the share to open the **Properties** dialog box.
7. If you cannot connect to the storage system using MMC, you can add the user to the BUILTIN\Administrators group or BUILTIN\Power Users group by using one of the following commands on the storage system:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Commands for managing SMB shares

You use the `vserver cifs share` and `vserver cifs share properties`

commands to manage SMB shares.

If you want to…	Use this command…
Create an SMB share	`vserver cifs share create`
Display SMB shares	`vserver cifs share show`
Modify an SMB share	`vserver cifs share modify`
Delete an SMB share	`vserver cifs share delete`
Add share properties to an existing share	`vserver cifs share properties add`
Remove share properties from an existing share	`vserver cifs share properties remove`
Display information about share properties	`vserver cifs share properties show`

See the man page for each command for more information.

Secure file access by using SMB share ACLs

Guidelines for managing SMB share-level ACLs

You can change share-level ACLs to give users more or less access rights to the share. You can configure share-level ACLs by using either Windows users and groups or UNIX users and groups.

After you create a share, by default, the share-level ACL gives read access to the standard group named Everyone. Read access in the ACL means that all users in the domain and all trusted domains have read-only access to the share.

You can change a share-level ACL by using the Microsoft Management Console (MMC) on a Windows client or the ONTAP command line.

The following guidelines apply when you use the MMC:

- The user and group names specified must be Windows names.
- You can specify only Windows permissions.

The following guidelines apply when you use the ONTAP command line:

- The user and group names specified can be Windows names or UNIX names.

  If a user and group type is not specified when creating or modifying ACLs, the default type is Windows users and groups.

- You can specify only Windows permissions.

Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names or UNIX user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

Steps

1. Delete the default share ACL:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a…	Enter the command…
Windows user	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission` *`access_right`*
Windows group	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission` *`access_right`*
UNIX user	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-user`* `-user-or-group` *`UNIX_user_name`* `-permission access_right`
UNIX group	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-group`* `-user-or-group` *`UNIX_group_name`* `-permission access_right`

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the "`vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

The following command gives `Read` permission to the “engineering” UNIX group for the “eng” share on the "`vs2.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group  eng
-permission Read

cluster1::> vserver cifs share access-control show
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

The following commands give `Change` permission to the local Windows group named “Tiger Team” and `Full_Control` permission to the local Windows user named “Sue Chang” for the “datavol5” share on the "`vs1`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Commands for managing SMB share access control lists

You need to know the commands for managing SMB access control lists (ACLs), which includes creating, displaying, modifying, and deleting them.

If you want to…	Use this command…
Create a new ACL	`vserver cifs share access-control create`
Display ACLs	`vserver cifs share access-control show`
Modify an ACL	`vserver cifs share access-control modify`
Delete an ACL	`vserver cifs share access-control delete`

Secure file access by using file permissions

Configure advanced NTFS file permissions using the Windows Security tab

You can configure standard NTFS file permissions on files and folders by using the **Windows Security** tab in the Windows Properties window.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

      If your CIFS server name is “CIFS_SERVER” and your share is named “share1”, you should type `\\CIFS_SERVER\share1`.

      You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.
4. Right-click the file or directory, and then select **Properties**.
5. Select the **Security** tab.

   The **Security** tab displays the list of users and groups for which NTFS permission are set. The **Permissions for** box displays a list of Allow and Deny permissions in effect for each user or group selected.

6. Click **Advanced**.

   The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click **Change Permissions**.

   The Permissions window opens.

8. Perform the desired actions:

If you want to…	Do the following…
Set up advanced NTFS permissions for a new user or group	a. Click **Add**. b. In the **Enter the object name to select** box, type the name of the user or group that you want to add. c. Click **OK**.
Change advanced NTFS permissions from a user or group	a. In the **Permissions entries:** box, select the user or group whose advanced permissions you want to change. b. Click **Edit**.
Remove advanced NTFS permissions for a user or group	a. In the **Permissions entries:** box, select the user or group that you want to remove. b. Click **Remove**. c. Skip to Step 13.

If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for <Object> box opens.

9. In the **Apply to** box, select how you want to apply this NTFS file permission entry.

   If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

    - To allow the specified access, select the **Allow** box.
    - To not allow the specified access, select the **Deny** box.
      You can set permissions on the following advanced rights:
    - **Full control**

      If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).

    - **Traverse folder / execute file**
    - **List folder / read data**
    - **Read attributes**
    - **Read extended attributes**
    - **Create files / write data**
    - **Create folders / append data**
    - **Write attributes**
    - **Write extended attributes**
    - **Delete subfolders and files**

- **Delete**
- **Read permissions**
- **Change permissions**
- **Take ownership**

> If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

11. If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.
12. Click **OK**.
13. After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:
    - Select the **Include inheritable permissions from this object's parent** box.

      This is the default.

    - Select the **Replace all child object permissions with inheritable permissions from this object** box.

      This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.

      > Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.

    - Select both boxes.
    - Select neither box.
14. Click **OK** to close the **Permissions** box.
15. Click **OK** to close the **Advanced Security settings for <Object>** box.

    For more information about how to set advanced NTFS permissions, see your Windows documentation.

Related information

Configure and apply file security on NTFS files and folders using the CLI

Displaying information about file security on NTFS security-style volumes

Displaying information about file security on mixed security-style volumes

Displaying information about file security on UNIX security-style volumes

Configure NTFS file permissions using the ONTAP CLI

You can configure NTFS file permissions on files and directories using the ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

How UNIX file permissions provide access control when accessing files over SMB

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions

  Configuring export permissions for SMB access is optional.

- Share permissions
- File permissions

  The following types of file permissions might be applied to the data on which the user wants to perform an action:

  - NTFS
  - UNIX NFSv4 ACLs
  - UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.

> Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

Secure file access by using Dynamic Access Control (DAC)

Secure file access by using Dynamic Access Control (DAC) overview

You can secure access by using Dynamic Access Control and by creating central access policies in Active Directory and applying them to files and folders on SVMs through applied Group Policy Objects (GPOs). You can configure auditing to use central access

policy staging events to see the effects of changes to central access policies before you apply them.

Additions to CIFS credentials

Before Dynamic Access Control, a CIFS credential included a security principal's (the user's) identity and Windows group membership. With Dynamic Access Control, three more types of information are added to the credential—device identity, device claims, and user claims:

- Device identity

  The analog of the user's identity information, except it is the identity and group membership of the device that the user is logging in from.

- Device claims

  Assertions about a device security principal. For example, a device claim might be that it is a member of a specific OU.

- User claims

  Assertions about a user security principal. For example, a user claim might be that their AD account is a member of a specific OU.

Central access policies

Central access policies for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

Central access policy staging with advanced auditing

Central access policies can be "staged", in which case they are evaluated in a "what-if" manner during file access checks. The results of what would have happened if the policy was in effect and how that differs from what is currently configured are logged as an audit event. In this way, administrators can use audit event logs to study the impact of an access policy change before actually putting the policy in play. After evaluating the impact of an access policy change, the policy can be deployed via GPOs to the desired SVMs.

Related information

Supported GPOs

Applying Group Policy Objects to CIFS servers

Enabling or disabling GPO support on a CIFS server

Displaying information about GPO configurations

Displaying information about central access policies

Displaying information about central access policy rules

Configuring central access policies to secure data on CIFS servers

Displaying information about Dynamic Access Control security

SMB and NFS auditing and security tracing

Supported Dynamic Access Control functionality

If you want to use Dynamic Access Control (DAC) on your CIFS server, you need to understand how ONTAP supports Dynamic Access Control functionality in Active Directory environments.

Supported for Dynamic Access Control

ONTAP supports the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Claims into the file system	Claims are simple name and value pairs that state some truth about a user. User credentials now contain claim information, and security descriptors on files can perform access checks that include claims checks. This gives administrators a finer level of control over who can access files.
Conditional expressions to file access checks	When modifying the security parameters of a file, users can now add arbitrarily complex conditional expressions to the file's security descriptor. The conditional expression can include checks for claims.
Central control of file access via central access policies	Central access policies are a kind of ACL stored in Active Directory that can be tagged to a file. Access to the file is only granted if the access checks of both the security descriptor on disk and the tagged central access policy allows access.This gives administrators the ability to control access to files from a central location (AD) without having to modify the security descriptor on disk.
Central access policy staging	Adds the ability to try out security changes without affecting actual file access, by "staging" a change to the central access policies, and seeing the effect of the change in an audit report.
Support for displaying information about central access policy security by using the ONTAP CLI	Extends the `vserver security file-directory show` command to display information about applied central access policies.
Security tracing that includes central access policies	Extends the `vserver security trace` command family to display results that include information about applied central access policies.

Unsupported for Dynamic Access Control

ONTAP does not support the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Automatic classification of NTFS file system objects	This is an extension to the Windows File Classification Infrastructure that is not supported in ONTAP.
Advanced auditing other than central access policy staging	Only central access policy staging is supported for advanced auditing.

Considerations when using Dynamic Access Control and central access policies with CIFS servers

There are certain considerations you must keep in mind when using Dynamic Access Control (DAC) and central access policies to secure files and folders on CIFS servers.

NFS access can be denied to root if policy rule applies to domain\administrator user

Under certain circumstances, NFS access to root might be denied when central access policy security is applied to the data that the root user is attempting to access. The issue occurs when the central access policy contains a rule that is applied to the domain\administrator and the root account is mapped to the domain\administrator account.

Instead of applying a rule to the domain\administrator user, you should apply the rule to a group with administrative privileges, such as the domain\administrators group. In this way, you can map root to the domain\administrator account without root being impacted by this issue.

CIFS server's BUILTIN\Administrators group has access to resources when the applied central access policy is not found in Active Directory

It is possible that resources contained within the CIFS server have central access policies applied to them, but when the CIFS server uses the central access policy's SID to attempt to retrieve information from Active Directory, the SID does not match any existing central access policy SIDs in Active Directory. Under these circumstances, the CIFS server applies the local default recovery policy for that resource.

The local default recovery policy allows the CIFS server's BUILTIN\Administrators group access to that resource.

Enable or disable Dynamic Access Control overview

The option that enables you to use Dynamic Access Control (DAC) to secure objects on your CIFS server is disabled by default. You must enable the option if you want to use Dynamic Access Control on your CIFS server. If you later decide that you do not want to use Dynamic Access Control to secure objects stored on the CIFS server, you can disable the option.

About this task

Once Dynamic Access Control is enabled, the file system can contain ACLs with Dynamic Access Control-related entries. If Dynamic Access Control is disabled, the current Dynamic Access Control entries will be

ignored, and new ones will not be allowed.

This option is available only at the advanced privilege level.

Step

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want Dynamic Access Control to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Disabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Return to the administrator privilege level: `set -privilege admin`

Related information

Configuring central access policies to secure data on CIFS servers

Manage ACLs that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled

If you have resources that have ACLs applied with Dynamic Access Control ACEs and you disable Dynamic Access Control on the storage virtual machine (SVM), you must remove the Dynamic Access Control ACEs before you can manage the non-Dynamic Access Control ACEs on that resource.

About this task

After Dynamic Access Control is disabled, you cannot remove existing non-Dynamic Access Control ACEs or add new non-Dynamic Access Control ACEs until you have removed the existing Dynamic Access Control ACEs.

You can use whichever tool you normally use to manage ACLs to perform these steps.

Steps

1. Determine what Dynamic Access Control ACEs are applied to the resource.
2. Remove the Dynamic Access Control ACEs from the resource.
3. Add or remove non-Dynamic Access Control ACEs as desired from the resource.

Configure central access policies to secure data on CIFS servers

There are several steps that you must take to secure access to data on the CIFS server using central access policies, including enabling Dynamic Access Control (DAC) on the CIFS server, configuring central access policies in Active Directory, applying the central access policies to Active Directory containers with GPOs, and enabling GPOs on the CIFS server.

Before you begin

- The Active Directory must be configured to use central access policies.
- You must have sufficient access on the Active Directory domain controllers to create central access policies and to create and apply GPOs to the containers that contain the CIFS servers.
- You must have sufficient administrative access on the storage virtual machine (SVM) to execute the necessary commands.

About this task

Central access policies are defined and applied to group policy objects (GPOs) on Active Directory. You can consult the Microsoft TechNet Library for instructions about configuring central access policies and GPOs.

Microsoft TechNet Library

Steps

1. Enable Dynamic Access Control on the SVM if it is not already enabled by using the `vserver cifs options modify` command.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Enable group policy objects (GPOs) on the CIFS server if they are not already enabled by using the `vserver cifs group-policy modify` command.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Create central access rules and central access policies on Active Directory.
4. Create a group policy object (GPO) to deploy the central access policies on Active Directory.
5. Apply the GPO to the container where the CIFS server computer account is located.
6. Manually update the GPOs applied to the CIFS server by using the `vserver cifs group-policy update` command.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Verify that the GPO central access policy is applied to the resources on the CIFS server by using the `vserver cifs group-policy show-applied` command.

   The following example shows that the Default Domain Policy has two central access policies that are applied to the CIFS server:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
   ```

```
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
```

```
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Related information

Displaying information about GPO configurations

Displaying information about central access policies

Displaying information about central access policy rules

Enabling or disabling Dynamic Access Control

Display information about Dynamic Access Control security

You can display information about Dynamic Access Control (DAC) security on NTFS volumes and on data with NTFS effective security on mixed security-style volumes. This includes information about conditional ACEs, resource ACEs, and central access policy ACEs. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Where output is displayed with group and user SIDs	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
About file and directory security for files and directories where the hexadecimal bit mask is translated to textual format	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Examples

The following example displays Dynamic Access Control security information about the path `/vol1` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
               File Inode Number: 112
                  Security Style: mixed
                 Effective Style: ntfs
                  DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                       POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                       ALLOW-Everyone-0x1f01ff-OI|CI
                                       ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Related information

Displaying information about GPO configurations

Displaying information about central access policies

Displaying information about central access policy rules

Revert considerations for Dynamic Access Control

You should be aware of what happens when reverting to a version of ONTAP that does not support Dynamic Access Control (DAC) and what you must do before and after reverting.

If you want to revert the cluster to a version of ONTAP that does not support Dynamic Access Control and Dynamic Access Control is enabled on one or more the storage virtual machines (SVMs), you must do the following before reverting:

- You must disable Dynamic Access Control on all SVMs that have it enabled on the cluster.
- You must modify any auditing configurations on the cluster that contain the `cap-staging` event type to use only the `file-op` event type.

You must understand and act on some important revert considerations for files and folders with Dynamic Access Control ACEs:

- If the cluster is reverted, existing Dynamic Access Control ACEs are not removed; however, they will be ignored in file access checks.
- Since Dynamic Access Control ACEs are ignored after reversion, access to files will change on files with Dynamic Access Control ACEs.

  This could allow users to access files they previously could not, or not be able to access files that they previously could.

- You should apply non-Dynamic Access Control ACEs to the affected files to restore their previous level of security.

  This can be done either before reverting or immediately after reversion completes.

> Since Dynamic Access Control ACEs are ignored after reversion, it is not required that you remove them when applying non-Dynamic Access Control ACEs to the affected files. However, if desired, you can manually remove them.

Where to find additional information about configuring and using Dynamic Access Control and central access policies

Additional resources are available to help you configure and use Dynamic Access Control and central access policies.

You can find information about how to configure Dynamic Access Control and central access policies on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Dynamic Access Control Scenario Overview

Microsoft TechNet: Central Access Policy Scenario

The following references can help you configure the SMB server to use and support Dynamic Access Control and central access policies:

- **Using GPOs on the SMB server**

  Applying Group Policy Objects to SMB servers

- **Configuring NAS auditing on the SMB server**

  SMB and NFS auditing and security tracing

Secure SMB access using export policies

How export policies are used with SMB access

If export policies for SMB access are enabled on the CIFS server, export policies are used when controlling access to SVM volumes by SMB clients. To access data, you can create an export policy that allows SMB access and then associate the policy with the volumes containing SMB shares.

An export policy has one or more rules applied to it that specifies which clients are allowed access to the data and what authentication protocols are supported for read-only and read-write access. You can configure export policies to allow access over SMB to all clients, a subnet of clients, or a specific client and to allow authentication using Kerberos authentication, NTLM authentication, or both Kerberos and NTLM authentication when determining read-only and read-write access to data.

After processing all export rules applied to the export policy, ONTAP can determine whether the client is granted access and what level of access is granted. Export rules apply to client machines, not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions. You associate exactly one export policy with each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

- Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
- Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

You associate exactly one export policy to each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

- Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
- Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

Each SVM has at least one export policy called “default”, which contains no rules. You cannot delete this export policy, but you can rename or modify it. Each volume on the SVM by default is associated with the default export policy. If export policies for SMB access is disabled on the SVM, the “default” export policy has no effect on SMB access.

You can configure rules that provide access to both NFS and SMB hosts and associate that rule with an export policy, which can then be associated with the volume that contains data to which both NFS and SMB hosts need access. Alternatively, if there are some volumes where only SMB clients require access, you can configure an export policy with rules that only allow access using the SMB protocol and that uses only Kerberos or NTLM (or both) for authentication for read-only and write access. The export policy is then associated to the volumes where only SMB access is desired.

If export policies for SMB is enabled and a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the volume’s export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied. This is true even if the share and file permissions would otherwise permit access. This means that you must configure your export policy to minimally allow the following on volumes containing SMB shares:

- Allow access to all clients or the appropriate subset of clients
- Allow access over SMB
- Allow appropriate read-only and write access by using Kerberos or NTLM authentication (or both)

For information about configuring and managing export policies, see NFS management.

How export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.

  The maximum size for the `-clientmatch` field is 4096 characters.

- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

Examples of export policy rules that restrict or allow access over SMB

The examples show how to create export policy rules that restrict or allow access over SMB on an SVM that has export policies for SMB access enabled.

Export policies for SMB access are disabled by default. You need to configure export policy rules that restrict or allow access over SMB only if you have enabled export policies for SMB access.

Export rule for SMB access only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: cifs1
- Index number: 1
- Client match: Matches only clients on the 192.168.1.0/24 network
- Protocol: Only enables SMB access
- Read-only access: To clients using NTLM or Kerberos authentication
- Read-write access: To clients using Kerberos authentication

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Export rule for SMB and NFS access

The following command creates an export rule on the SVM named"` vs1`" that has the following configuration:

- Policy name: cifsnfs1
- Index number: 2
- Client match: Matches all clients
- Protocol: SMB and NFS access
- Read-only access: To all clients
- Read-write access: To clients using Kerberos (NFS and SMB) or NTLM authentication (SMB)
- Mapping for UNIX user ID 0 (zero): Mapped to user ID 65534 (which typically maps to the user name nobody)
- Suid and sgid access: Allows

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Export rule for SMB access using NTLM only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: ntlm1
- Index number: 1
- Client match: Matches all clients
- Protocol: Only enables SMB access
- Read-only access: Only to clients using NTLM
- Read-write access: Only to clients using NTLM

> If you configure the read-only option or the read-write option for NTLM-only access, you must use IP address-based entries in the client match option. Otherwise, you receive `access denied` errors. This is because ONTAP uses Kerberos Service Principal Names (SPN) when using a host name to check on the client’s access rights. NTLM authentication does not support SPN names.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Enable or disable export policies for SMB access

You can enable or disable export policies for SMB access on storage virtual machines (SVMs). Using export policies to control SMB access to resources is optional.

Before you begin

The following are the requirements for enabling export policies for SMB:

- The client must have a “PTR” record in DNS before you create the export rules for that client.
- An additional set of “A” and “PTR” records for host names is required if the SVM provides access to NFS clients and the host name you want to use for NFS access is different from the CIFS server name.

About this task

When setting up a new CIFS server on your SVM, the use of export policies for SMB access is disabled by default. You can enable export policies for SMB access if you want to control access based on authentication protocol or on client IP addresses or host names. You can enable or disable export policies for SMB access at any time.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable export policies:
   - Enable export policies: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - Disable export policies: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables the use of export policies to control SMB client access to resources on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Secure file access by using Storage-Level Access Guard

Secure file access by using Storage-Level Access Guard

In addition to securing access by using native file-level and export and share security, you can configure Storage-Level Access Guard, a third layer of security applied by ONTAP at the volume level. Storage-Level Access Guard applies to access from all NAS protocols to the storage object to which it is applied.

Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map

to a Windows user on the SVM that owns the volume.

Storage-Level Access Guard behavior

- Storage-Level Access Guard applies to all the files or all the directories in a storage object.

  Because all files or directories in a volume are subject to Storage-Level Access Guard settings, inheritance through propagation is not required.

- You can configure Storage-Level Access Guard to apply to files only, to directories only, or to both files and directories within a volume.
  - File and directory security

    Applies to every directory and file within the storage object. This is the default setting.

  - File security

    Applies to every file within the storage object. Applying this security does not affect access to, or auditing of, directories.

  - Directory security

    Applies to every directory within the storage object. Applying this security does not affect access to, or auditing of, files.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

- If you view the security settings on a file or directory from an NFS or SMB client, you do not see the Storage-Level Access Guard security.

  It's applied at the storage object level and stored in the metadata used to determine the effective permissions.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

  It is designed to be modified by storage administrators only.

- You can apply Storage-Level Access Guard to volumes with NTFS or mixed security style.
- You can apply Storage-Level Access Guard to volumes with UNIX security style as long as the SVM containing the volume has a CIFS server configured.
- When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated to volumes mounted under it.
- The Storage-Level Access Guard security descriptor is replicated with SnapMirror data replication and with SVM replication.
- There is special dispensation for virus scanners.

  Exceptional access is allowed to these servers to screen files and directories, even if Storage-Level Access Guard denies access to the object.

- FPolicy notifications are not sent if access is denied because of Storage-Level Access Guard.

Order of access checks

Access to a file or directory is determined by the combined effect of the export or share permissions, the Storage-Level Access Guard permissions set on volumes, and the native file permissions applied to files and/or directories. All levels of security are evaluated to determine what the effective permissions a file or directory has. The security access checks are performed in the following order:

1. SMB share or NFS export-level permissions
2. Storage-Level Access Guard
3. NTFS file/folder access control lists (ACLs), NFSv4 ACLs, or UNIX mode bits

Use cases for using Storage-Level Access Guard

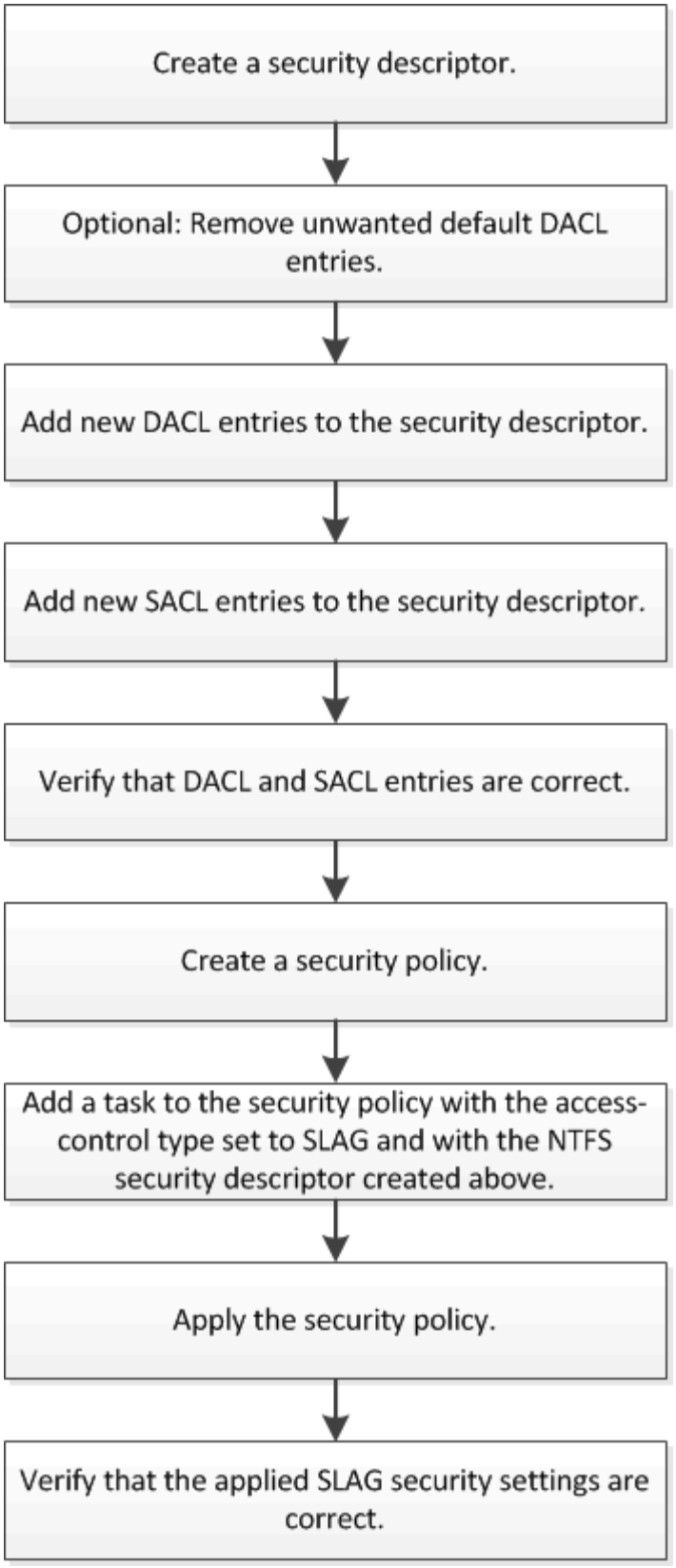
Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. There are certain use cases where the ability to control access at the storage level is beneficial.

Typical use cases for this feature include the following scenarios:

- Intellectual property protection by auditing and controlling all users' access at the storage level
- Storage for financial services companies, including banking and trading groups
- Government services with separate file storage for individual departments
- Universities protecting all student files

Workflow to configure Storage-Level Access Guard

The workflow to configure Storage-Level Access Guard (SLAG) uses the same ONTAP CLI commands that you use to configure NTFS file permissions and auditing policies. Instead of configuring file and directory access on a designated target, you configure SLAG on the designated storage virtual machine (SVM) volume.



Related information

Configuring Storage-Level Access Guard

Configure Storage-Level Access Guard

There are a number of steps you need to follow to configure Storage-Level Access Guard on a volume or qtree. Storage-Level Access Guard provides a level of access security that is set at the storage level. It provides security that applies to all accesses from all NAS protocols to the storage object to which it has been applied.

Steps

1. Create a security descriptor by using the `vserver security file-directory ntfs create` command.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   A security descriptor is created with the following four default DACL access control entries (ACEs):

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   If you do not want to use the default entries when configuring Storage-Level Access Guard, you can remove them prior to creating and adding your own ACEs to the security descriptor.

2. Remove any of the default DACL ACEs from the security descriptor that you do not want configured with Storage-Level Access Guard security:

   a. Remove any unwanted DACL ACEs by using the `vserver security file-directory ntfs`

`dacl remove` command.

In this example, three default DACL ACEs are removed from the security descriptor: BUILTIN\Administrators, BUILTIN\Users, and CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. Verify that the DACL ACEs you do not want to use for Storage-Level Access Guard security are removed from the security descriptor by using the `vserver security file-directory ntfs dacl show` command.

In this example, the output from the command verifies that three default DACL ACEs have been removed from the security descriptor, leaving only the NT AUTHORITY\SYSTEM default DACL ACE entry:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-
folders, files
```

3. Add one or more DACL entries to a security descriptor by using the `vserver security file-directory ntfs dacl add` command.

In this example, two DACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Add one or more SACL entries to a security descriptor by using the `vserver security file-directory ntfs sacl add` command.

In this example, two SACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
```

```
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verify that the DACL and SACL ACEs are configured correctly by using the `vserver security file-directory ntfs dacl show` and `vserver security file-directory ntfs sacl show` commands, respectively.

   In this example, the following command displays information about DACL entries for security descriptor “sd1”:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In this example, the following command displays information about SACL entries for security descriptor “sd1”:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   files
   ```

6. Create a security policy by using the `vserver security file-directory policy create` command.

   The following example creates a policy named “policy1”:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Verify that the policy is correctly configured by using the `vserver security file-directory policy show` command.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Add a task with an associated security descriptor to the security policy by using the `vserver security file-directory policy-task add` command with the `-access-control` parameter set to `slag`.

   Even though a policy can contain more than one Storage-Level Access Guard task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

   In this example, a task is added to the policy named “policy1”, which is assigned to security descriptor “sd1”. It is assigned to the `/datavol1` path with the access control type set to “slag”.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Verify that the task is configured correctly by using the `vserver security file-directory policy task show` command.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
      -----  -----------  ---------------  --------  ----------
   ---------------
      1      /datavol1    slag             ntfs      propagate  sd1
   ```

10. Apply the Storage-Level Access Guard security policy by using the `vserver security file-directory apply` command.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    The job to apply the security policy is scheduled.

11. Verify that the applied Storage-Level Access Guard security settings are correct by using the `vserver security file-directory show` command.

    In this example, the output from the command shows that Storage-Level Access Guard security has been applied to the NTFS volume `/datavol1`. Even though the default DACL allowing Full Control to Everyone remains, Storage-Level Access Guard security restricts (and audits) access to the groups defined in the Storage-Level Access Guard settings.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Related information

Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI

Workflow to configure Storage-Level Access Guard

Displaying information about Storage-Level Access Guard

Removing Storage-Level Access Guard

Effective SLAG matrix

You can configure SLAG on a volume or a qtree or both. The SLAG matrix defines on which volume or qtree is the SLAG configuration applicable under various scenarios listed in the table.

	Volume SLAG in an AFS	Volume SLAG in a Snapshot copy	Qtree SLAG in an AFS	Qtree SLAG in a Snapshot copy
Volume access in an Access File System (AFS)	YES	NO	N/A	N/A
Volume access in a Snapshot copy	YES	NO	N/A	N/A
Qtree access in an AFS (when SLAG is present in the qtree)	NO	NO	YES	NO
Qtree access in an AFS (when SLAG is not present in qtree)	YES	NO	NO	NO
Qtree access in Snapshot copy (when SLAG is present in the qtree AFS)	NO	NO	YES	NO
Qtree access in Snapshot copy (when SLAG is not present in the qtree AFS)	YES	NO	NO	NO

Display information about Storage-Level Access Guard

Storage-Level Access Guard is a third layer of security applied on a volume or qtree. Storage-Level Access Guard settings cannot be viewed by using the Windows Properties window. You must use the ONTAP CLI to view information about Storage-Level Access Guard security, which you can use to validate your configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the volume or qtree whose Storage-Level Access Guard security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display Storage-Level Access Guard security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
With expanded detail	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Examples

The following example displays Storage-Level Access Guard security information for the NTFS security-style volume with the path `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

The following example displays the Storage-Level Access Guard information about the mixed security-style volume at the path `/datavol5` in SVM vs1. The top level of this volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Remove Storage-Level Access Guard

You can remove Storage-Level Access Guard on a volume or qtree if you no longer want set access security at the storage level. Removing Storage-Level Access Guard does not modify or remove regular NTFS file and directory security.

Steps

1. Verify that the volume or qtree has Storage-Level Access Guard configured by using the `vserver security file-directory show` command.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Remove Storage-Level Access Guard by using the `vserver security file-directory remove-slag` command.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Verify that Storage-Level Access Guard has been removed from the volume or qtree by using the `vserver security file-directory show` command.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Manage file access using SMB

Use local users and groups for authentication and authorization

How ONTAP uses local users and groups

Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

- **Local user**

  A user account with a unique security identifier (SID) that has visibility only on the storage virtual machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

  User accounts have several uses:

  - Used to grant *User Rights Management* privileges to a user.
  - Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local group**

  A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of

members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant *User Rights Management* privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local domain**

  A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

- **Security identifier (SID)**

  A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **NTLM authentication**

  A Microsoft Windows security method used to authenticate users on a CIFS server.

- **Cluster replicated database (RDB)**

  A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

Reasons for creating local users and local groups

There are several reasons for creating local users and local groups on your storage virtual machine (SVM). For example, you can access an SMB server by using a local user account if the domain controllers (DCs) are unavailable, you might want to use local groups to assign privileges, or your SMB server is in a workgroup.

You can create one or more local user accounts for the following reasons:

- Your SMB server is in a workgroup, and domain users are not available.

  Local users are required in workgroup configurations.

- You want the ability to authenticate and log in to the SMB server if the domain controllers are unavailable.

  Local users can authenticate with the SMB server by using NTLM authentication when the domain controller is down, or when network problems prevent your SMB server from contacting the domain controller.

- You want to assign *User Rights Management* privileges to a local user.

  User Rights Management is the ability for an SMB server administrator to control what rights the users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account, or by making the user a member of a local group that has those privileges.

You can create one or more local groups for the following reasons:

- Your SMB server is in a workgroup, and domain groups are not available.

  Local groups are not required in workgroup configurations, but they can be useful for managing access privileges for local workgroup users.

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.

  Some built-in user groups have predefined privileges. To assign a customized set of privileges, you can create a local group and assign the necessary privileges to that group. You can then add local users, domain users, and domain groups to the local group.

Related information

How local user authentication works

List of supported privileges

How local user authentication works

Before a local user can access data on a CIFS server, the user must create an authenticated session.

Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and NTLMv2 are supported.

ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server's local domain name (the CIFS server name):

- The domain portion matches

  Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.

- The domain portion does not match

  ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed.

  For example, if the user exists in Active Directory but the password is invalid or expired, ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain names do not match. For example, if a matching domain account exists but it is disabled, ONTAP uses the corresponding local account on the CIFS server for authentication.

- The domain portion is not specified

  ONTAP first attempts authentication as a local user. If authentication as a local user fails, then ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.

After local or domain user authentication is completed successfully, ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

Related information

Enabling or disabling local user authentication

How user access tokens are constructed

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user's group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

- Local user login

  Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.

- Domain user login

  When a domain user logs in, ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user's domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is `Domain Users` (RID 513). You cannot change the default.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.

There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

Guidelines for using SnapMirror on SVMs that contain local groups

You should be aware of the guidelines when you configure SnapMirror on volumes owned by SVMs that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

What happens to local users and groups when deleting CIFS servers

The default set of local users and groups is created when a CIFS server is created, and they are associated with the storage virtual machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.

The CIFS server administrative status does not affect visibility of local users or groups.

How you can use Microsoft Management Console with local users and groups

You can view information about local users and groups from the Microsoft Management Console. With this release of ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

Guidelines for reverting

If you plan to revert the cluster to an ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user rights, you must be aware of certain considerations.

- Due to security reasons, information about configured local users, groups, and privileges are not deleted when ONTAP is reverted to a version that does not support local users and groups functionality.
- Upon a revert to a prior major version of ONTAP, ONTAP does not use local users and groups during authentication and credential creation.
- Local users and groups are not removed from file and folder ACLs.
- File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

  To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

What local privileges are

List of supported privileges

ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the storage virtual machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
SeTcbPrivilege	None	Act as part of the operating system
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Back up files and directories, overriding any ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restore files and directories, overriding any ACLs Set any valid user or group SID as the file owner
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Take ownership of files or other objects
SeSecurityPrivilege	BUILTIN\Administrators	Manage auditingThis includes viewing, dumping, and clearing the security log.
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	Bypass traverse checkingUsers with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

Related information

Managing local privileges

Configuring bypass traverse checking

Assign privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

- You can assign a set of privileges to a group that you create.

  You then add a user to the group that has the privileges that you want that user to have.

- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

Related information

Adding privileges to local or domain users or groups

Removing privileges from local or domain users or groups

Resetting privileges for local or domain users and groups

Configuring bypass traverse checking

Guidelines for using BUILTIN groups and the local administrator account

There are certain guidelines you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.

  After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.

- There is no local Guest account.

Related information

Predefined BUILTIN groups and default privileges

Requirements for local user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy*.

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters:

    ~ ! @ # $ % ^ & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

Related information

Enabling or disabling required password complexity for local SMB users

Displaying information about CIFS server security settings

Changing local user account passwords

Predefined BUILTIN groups and default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
`BUILTIN\Administrators`RID 544 When first created, the local `Administrator` account, with a RID of 500, is automatically made a member of this group. When the storage virtual machine (SVM) is joined to a domain, the `domain\Domain Admins` group is added to the group. If the SVM leaves the domain, the `domain\Domain Admins` group is removed from the group.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 When first created, this group does not have any members. Members of this group have the following characteristics: • Can create and manage local users and groups. • Cannot add themselves or any other object to the `BUILTIN\Administrators` group.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 When first created, this group does not have any members (besides the implied `Authenticated Users` special group). When the SVM is joined to a domain, the `domain\Domain Users` group is added to this group. If the SVM leaves the domain, the `domain\Domain Users` group is removed from this group.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.	`SeChangeNotifyPrivilege`

Related information

Guidelines for using BUILTIN groups and the local administrator account

List of supported privileges

Configuring bypass traverse checking

Enable or disable local users and groups functionality

Enable or disable local users and groups functionality overview

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, ONTAP disables local user and group functionality if any node in the cluster is reverted to an ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of ONTAP that supports it.

Related information

Modify local user accounts

Modify local groups

Add privileges to local or domain users or groups

Enable or disable local users and groups

You can enable or disable local users and groups for SMB access on storage virtual machines (SVMs). Local users and groups functionality is enabled by default.

About this task

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local users and groups to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`

If you want local users and groups to be…	Enter the command…
Disabled	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local users and groups functionality on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Related information

Enable or disable local user authentication

Enable or disable local user accounts

Enable or disable local user authentication

You can enable or disable local user authentication for SMB access on storage virtual machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

Before you begin

Local users and groups functionality must be enabled on the CIFS server.

About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local authentication to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local user authentication on SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Related information

How local user authentication works

Enabling or disabling local users and groups

Manage local user accounts

Modify local user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

If you want to…	Enter the command…
Modify the local user's full name	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text` If the full name contains a space, then it must be enclosed within double quotation marks.

If you want to…	Enter the command…
Modify the local user's description	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` If the description contains a space, then it must be enclosed within double quotation marks.
Enable or disable the local user account	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account-disabled {true|false}`
Rename the local user account	`vserver cifs users-and-groups local-user rename -vserver` *`vserver_name`* `-user-name` *`user_name`* `-new-user-name` *`new_user_name`* When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name.

Example

The following example renames the local user "CIFS_SERVER\sue" to "CIFS_SERVER\sue_new" on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Enable or disable local user accounts

You enable a local user account if you want the user to be able to access data contained in the storage virtual machine (SVM) over an SMB connection. You can also disable a local user account if you do not want that user to access SVM data over SMB.

About this task

You enable a local user by modifying the user account.

Step

1. Perform the appropriate action:

If you want to…	Enter the command…
Enable the user account	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account-disabled false`

If you want to…	Enter the command…
Disable the user account	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

Change local user account passwords

You can change a local user's account password. This can be useful if the user's password is compromised or if the user has forgotten the password.

Step

1. Change the password by performing the appropriate action: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Example

The following example sets the password for the local user "CIFS_SERVER\sue" associated with storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Related information

Enabling or disabling required password complexity for local SMB users

Displaying information about CIFS server security settings

Display information about local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user's settings, and also to troubleshoot authentication or file access issues.

About this task

Information about a user's password is never displayed.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Display information about all users on the storage virtual machine (SVM)	`vserver cifs users-and-groups local-user show -vserver vserver_name`
Display detailed account information for a user	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

There are other optional parameters that you can choose when you run the command. See the man page for more information.

Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

Display information about group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

About this task

You can customize the command to display only the information that you want to see.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Display local user membership information for a specified local user	`vserver cifs users-and-groups local-user show-membership -user-name user_name`
Display local user membership information for the local group of which this local user is a member	`vserver cifs users-and-groups local-user show-membership -membership group_name`

If you want to…	Enter the command…
Display user membership information for local users that are associated with a specified storage virtual machine (SVM)	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
Display detailed information for all local users on a specified SVM	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

Example

The following example displays the membership information for all local users on SVM vs1; user “CIFS_SERVER\Administrator” is a member of the “BUILTIN\Administrators” group, and “CIFS_SERVER\sue” is a member of “CIFS_SERVER\g1” group:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ------------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Delete local user accounts

You can delete local user accounts from your storage virtual machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

About this task

Keep the following in mind when deleting local users:

- The file system is not altered.

  Windows Security Descriptors on files and directories that refer to this user are not adjusted.

- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

Steps

1. Determine the name of the local user account that you want to delete: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*
2. Delete the local user: `vserver cifs users-and-groups local-user delete -vserver` *vserver_name* `-user-name` *username_name*
3. Verify that the user account is deleted: `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

Example

The following example deletes the local user “CIFS_SERVER\sue” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Manage local groups

Modify local groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

If you want to…	Use the command…
Modify the local group description	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` If the description contains a space, then it must be enclosed within double quotation marks.
Rename the local group	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Examples

The following example renames the local group “CIFS_SERVER\engineering” to “CIFS_SERVER\engineering_new”:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

The following example modifies the description of the local group “CIFS_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Display information about local groups

You can display a list of all local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

Step

1. Perform one of the following actions:

If you want information about…	Enter the command…
All local groups on the cluster	`vserver cifs users-and-groups local-group show`
All local groups on the SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following example displays information about all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

About this task

Guidelines for adding members to a local group:

- You cannot add users to the special *Everyone* group.
- The local group must exist before you can add a user to it.
- The user must exist before you can add the user to a local group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

Guidelines for removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- The group from which you want to remove a member must exist.
- ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

Step

1. Add or remove a member in a group.

If you want to…	Then use the command…
Add a member to a group	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.
Remove a member from a group	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

The following example adds a local user “SMB_SERVER\sue” and a domain group “AD_DOM\dom_eng” to the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

The following example removes the local users “SMB_SERVER\sue” and “SMB_SERVER\james” from the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Related information

Displaying information about members of local groups

Display information about members of local groups

You can display a list of all members of local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter the command…
Members of all local groups on the cluster	`vserver cifs users-and-groups local-group show-members`
Members of all local groups on the SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Example

The following example displays information about members of all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- --------------------------- ----------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

Delete a local group

You can delete a local group from the storage virtual machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

About this task

Keep the following in mind when deleting local groups:

- The file system is not altered.

  Windows Security Descriptors on files and directories that refer to this group are not adjusted.

- If the group does not exist, an error is returned.
- The special *Everyone* group cannot be deleted.
- Built-in groups such as *BUILTIN\Administrators BUILTIN\Users* cannot be deleted.

Steps

1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Delete the local group: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verify that the group is deleted: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Example

The following example deletes the local group “CIFS_SERVER\sales” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Update domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

About this task

You must specify the name of the storage virtual machine (SVM) on which you want to update domain names.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform the appropriate action:

If you want to update domain users and groups and…	Use this command…
Display domain users and groups that successfully updated and that failed to update	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

If you want to update domain users and groups and…	Use this command…
Display domain users and groups that successfully updated	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Display only the domain users and groups that fail to update	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suppress all status information about updates	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example updates the names of domain users and groups associated with storage virtual machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Manage local privileges

Add privileges to local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

Before you begin

The local or domain user or group to which privileges will be added must already exist.

About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

  The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Add one or more privileges to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verify that the desired privileges are applied to the object: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Example

The following example adds the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” to the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Remove privileges from local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges

that users and groups have.

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

  The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Remove one or more privileges from a local or domain user or group: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verify that the desired privileges have been removed from the object: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Example

The following example removes the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” from the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Reset privileges for local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

Steps

1. Reset the privileges on a local or domain user or group: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verify that the privileges are reset on the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Examples

The following example resets the privileges on the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have privileges associated with their accounts:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group “BUILTIN\Administrators”, effectively removing the privilege entry:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Display information about privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or groups. This information helps you determine whether the desired user rights

are applied.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter this command…
Custom privileges for all domain and local users and groups on the storage virtual machine (SVM)	`vserver cifs users-and-groups privilege show -vserver vserver_name`
Custom privileges for a specific domain or local user and group on the SVM	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

   There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------  --------------------   ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configure bypass traverse checking

Configure bypass traverse checking overview

Bypass traverse checking is a user right (also known as a *privilege*) that determines whether a user can traverse all the directories in the path to a file even if the user does not have permissions on the traversed directory. You should understand what happens when allowing or disallowing bypass traverse checking, and how to configure bypass traverse checking for users on storage virtual machines (SVMs).

What happens when allowing or disallowing bypass traverse checking

- If allowed, when a user attempts to access a file, ONTAP does not check the traverse permission for the intermediate directories when determining whether to grant or deny access to the file.
- If disallowed, ONTAP checks the traverse (execute) permission for all directories in the path to the file.

  If any of the intermediate directories do not have the “X” (traverse permission), ONTAP denies access to the file.

Configure bypass traverse checking

You can configure bypass traverse checking by using the ONTAP CLI or by configuring Active Directory group policies with this user right.

The `SeChangeNotifyPrivilege` privilege controls whether users are allowed to bypass traverse checking.

- Adding it to local SMB users or groups on the SVM or to domain users or groups allows bypass traverse checking.
- Removing it from local SMB users or groups on the SVM or from domain users or groups disallows bypass traverse checking.

By default, the following BUILTIN groups on the SVM have the right to bypass traverse checking:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

If you do not want to allow members of one of these groups to bypass traverse checking, you must remove this privilege from the group.

You must keep the following in mind when configuring bypass traverse checking for local SMB users and groups on the SVM by using the CLI:

- If you want to allow members of a custom local or domain group to bypass traverse checking, you must add the `SeChangeNotifyPrivilege` privilege to that group.
- If you want to allow an individual local or domain user to bypass traverse checking and that user is not a member of a group with that privilege, you can add the `SeChangeNotifyPrivilege` privilege to that user account.
- You can disable bypass traverse checking for local or domain users or groups by removing the `SeChangeNotifyPrivilege` privilege at any time.

To disable bypass travers checking for specified local or domain users or groups, you must also remove the `SeChangeNotifyPrivilege` privilege from the `Everyone` group.

Related information

Allow users or groups to bypass directory traverse checking

Disallow users or groups from bypassing directory traverse checking

Configure character mapping for SMB file name translation on volumes

Create SMB share access control lists

Secure file access by using Storage-Level Access Guard

List of supported privileges

Allow users or groups to bypass directory traverse checking

If you want a user to be able traverse all the directories in the path to a file even if the user does not have permissions on a traversed directory, you can add the `SeChangeNotifyPrivilege` privilege to local SMB users or groups on storage virtual machines (SVMs). By default, users are able to bypass directory traverse checking.

Before you begin

- A SMB server must be exist on the SVM.
- The local users and groups SMB server option must be enabled.
- The local or domain user or group to which the `SeChangeNotifyPrivilege` privilege will be added must already exist.

About this task

When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Enable bypass traverse checking by adding the `SeChangeNotifyPrivilege` privilege to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

2. Verify that the specified user or group has bypass traverse checking enabled: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Example

The following command enables users that belong to the “EXAMPLE\eng” group to bypass directory traverse checking by adding the `SeChangeNotifyPrivilege` privilege to the group:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege
```

Related information

Disallowing users or groups from bypassing directory traverse checking

Disallow users or groups from bypassing directory traverse checking

If you do not want a user to traverse all the directories in the path to a file because the user does not have permissions on the traversed directory, you can remove the

`SeChangeNotifyPrivilege` privilege from local SMB users or groups on storage virtual machines (SVMs).

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Disallow bypass traverse checking: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   The command removes the `SeChangeNotifyPrivilege` privilege from the local or domain user or group that you specify with the value for the `-user-or-group-name name` parameter.

2. Verify that the specified user or group has bypass traverse checking disabled: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Example

The following command disallows users that belong to the “EXAMPLE\eng” group from bypassing directory traverse checking:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng          -
```

Related information

Allowing users or groups to bypass directory traverse checking

Display information about file security and audit policies

Display information about file security and audit policies overview

You can display information about file security on files and directories contained within volumes on storage virtual machines (SVMs). You can display information about audit

policies on FlexVol volumes. If configured, you can display information about Storage-Level Access Guard and Dynamic Access Control security settings on FlexVol volumes.

Displaying information about file security

You can display information about file security applied to data contained within volumes and qtrees (for FlexVol volumes) with the following security styles:

- NTFS
- UNIX
- Mixed

Displaying information about audit policies

You can display information about audit policies for auditing access events on FlexVol volumes over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

Displaying information about Storage-Level Access Guard (SLAG) security

Storage-Level Access Guard security can be applied on FlexVol volumes and qtree objects with the following security styles:

- NTFS
- Mixed
- UNIX (if a CIFS server is configured on the SVM that contains the volume)

Displaying information about Dynamic Access Control (DAC) security

Dynamic Access Control security can be applied on an object within a FlexVol volume with the following security styles:

- NTFS
- Mixed (if the object has NTFS effective security)

Related information

Securing file access by using Storage-Level Access Guard

Displaying information about Storage-Level Access Guard

Display information about file security on NTFS security-style volumes

You can display information about file and directory security on NTFS security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Because NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights, UNIX-related output fields contain display-only UNIX file permission information.
- ACL output is displayed for file and folders with NTFS security.
- Because Storage-Level Access Guard security can be configured on the volume root or qtree, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file ACLs and Storage-Level Access Guard ACLs.
- The output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
With expanded detail	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Examples

The following example displays the security information about the path `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

The following example displays the security information with expanded masks about the path `/data/engineering` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
```

```
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Related information

Displaying information about file security on mixed security-style volumes

Displaying information about file security on UNIX security-style volumes

Display information about file security on mixed security-style volumes

You can display information about file and directory security on mixed security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Mixed security-style volumes and qtrees can contain some files and folders that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

  This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both UNIX file permissions and Storage-Level Access Guard ACLs.
- If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the security information about the path `/projects` in SVM vs1 in expanded-mask form. This mixed security-style path has UNIX effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

The following example displays the security information about the path `/data` in SVM vs1. This mixed security-style path has an NTFS effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

The following example displays the security information about the volume at the path `/datavol5` in SVM vs1. The top level of this mixed security-style volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Related information

Displaying information about file security on NTFS security-style volumes

Displaying information about file security on UNIX security-style volumes

Display information about file security on UNIX security-style volumes

You can display information about file and directory security on UNIX security-style volumes, including what the security styles and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use

the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or directory security information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.
- ACL output is displayed only for file and folders with NFSv4 security.

  This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output does not apply in the case of NFSv4 security descriptors.

  They are only meaningful for NTFS security descriptors.

- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
With expanded detail	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Examples

The following example displays the security information about the path `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

The following example displays the security information about the path `/home` in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                        Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Related information

Displaying information about file security on NTFS security-style volumes

Displaying information about file security on mixed security-style volumes

Display information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

  NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
As a detailed list	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the audit policy information for the path `/corp` in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Display information about NFSv4 audit policies on FlexVol volumes using the CLI

You can display information about NFSv4 audit policies on FlexVol volumes using the ONTAP CLI, including what the security styles and effective security styles are, what

permissions are applied, and information about system access control lists (SACLs). You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the files or directories whose audit information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only NFSv4 SACLs for audit policies.
- Files and directories in a mixed security-style volume that are of UNIX security style can have NFSv4 audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NFSv4 SACLs.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular NFSv4 file and directory SACLs and Storage-Level Access Guard NTFS SACLs.
- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Steps

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the security information about the path `/lab` in SVM vs1. This UNIX security-style path has an NFSv4 SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Ways to display information about file security and audit policies

You can use the wildcard character (*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (**) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories. If you want to display information of a particular file or directory named as "**", then you need to provide the complete path inside double quotes ("``").

Example

The following command with the wildcard character displays the information about all files and directories below the path `/1/` of SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

The following command displays the information of a file named as "*" under the path `/vol1/a` of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI

Manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI overview

You can manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on storage virtual machines (SVMs) by using the CLI.

You can manage NTFS file security and audit policies from SMB clients or by using the CLI. However, using the CLI to configure file security and audit policies removes the need to use a remote client to manage file security. Using the CLI can significantly reduce the time it takes to apply security on many files and folders using a single command.

You can configure Storage-Level Access Guard, which is another layer of security applied by ONTAP to SVM volumes. Storage-Level Access Guard applies to accesses from all NAS protocols to the storage object to which Storage-Level Access Guard is applied.

Storage-Level Access Guard can be configured and managed only from the ONTAP CLI. You cannot manage Storage-Level Access Guard settings from SMB clients. Moreover, if you view the security settings on a file or directory from an NFS or SMB client, you will not see the Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. Therefore, Storage-Level Access Guard provides an extra layer of security for data access that is independently set and managed by the storage administrator.

Even though only NTFS access permissions are supported for Storage-Level Access Guard, ONTAP can perform security checks for access over NFS to data on volumes where Storage-Level Access Guard is applied if the UNIX user maps to a Windows user on the SVM that owns the volume.

NTFS security-style volumes

All files and folders contained within NTFS security-style volumes and qtrees have NTFS effective security. You can use the `vserver security file-directory` command family to implement the following types of security on NTFS security-style volumes:

- File permissions and audit policies to files and folders contained in the volume
- Storage-Level Access Guard security on volumes

Mixed security-style volumes

Mixed security-style volumes and qtrees can contain some files and folders that have UNIX effective security and use UNIX file permissions, either mode bits or NFSv4.x ACLs and NFSv4.x audit policies, and some files and folders that have NTFS effective security and use NTFS file permissions and audit policies. You can use the `vserver security file-directory` command family to apply the following types of security to mixed security-style data:

- File permissions and audit policies to files and folders with NTFS effective security-style in the mixed volume or qtree
- Storage-Level Access Guard to volumes with either NTFS and UNIX effective security-style

UNIX security-style volumes

UNIX security-style volumes and qtrees contain files and folders that have UNIX effective security (either mode bits or NFSv4.x ACLs). You must keep the following in mind if you want to use the `vserver security file-directory` command family to implement security on UNIX security-style volumes:

- The `vserver security file-directory` command family cannot be used to manage UNIX file security and audit policies on UNIX security-style volumes and qtrees.
- You can use the `vserver security file-directory` command family to configure Storage-Level Access Guard on UNIX security-style volumes, provided the SVM with the target volume contains a CIFS server.

Related information

Display information about file security and audit policies

Configure and apply file security on NTFS files and folders using the CLI

Configure and apply audit policies to NTFS files and folders using the CLI

Secure file access by using Storage-Level Access Guard

Use cases for using the CLI to set file and folder security

Because you can apply and manage file and folder security locally without involvement from a remote client, you can significantly reduce the time it takes to set bulk security on a large number of files or folders.

You can benefit from using the CLI to set file and folder security in the following use cases:

- Storage of files in large enterprise environments, such as file storage in home directories
- Migration of data
- Change of Windows domain
- Standardization of file security and audit policies across NTFS file systems

Limits when using the CLI to set file and folder security

You need to be aware of certain limits when using the CLI to set file and folder security.

- The `vserver security file-directory` command family does not support setting NFSv4 ACLs.

  You can only apply NTFS security descriptors to NTFS files and folders.

How security descriptors are used to apply file and folder security

Security descriptors contain the access control lists that determine what actions a user can perform on files and folders, and what is audited when a user accesses files and folders.

- **Permissions**

  Permissions are allowed or denied by an object's owner and determine what actions an object (users, groups, or computer objects) can perform on specified files or folders.

- **Security descriptors**

  Security descriptors are data structures that contain security information that define permissions associated with a file or folder.

- **Access control lists (ACLs)**

  Access control lists are the lists contained within a security descriptor that contain information on what actions users, groups, or computer objects can perform on the file or folder to which the security descriptor is applied. The security descriptor can contain the following two types of ACLs:

  - Discretionary access control lists (DACLs)
  - System access control lists (SACLs)

- **Discretionary access control lists (DACLs)**

  DACLs contain the list of SIDS for the users, groups, and computer objects who are allowed or denied access to perform actions on files or folders. DACLs contain zero or more access control entries (ACEs).

- **System access control lists (SACLs)**

  SACLs contain the list of SIDS for the users, groups, and computer objects for which successful or failed auditing events are logged. SACLs contain zero or more access control entries (ACEs).

- **Access Control Entries (ACEs)**

  ACEs are individual entries in either DACLs or SACLs:

- A DACL access control entry specifies the access rights that are allowed or denied for particular users, groups, or computer objects.
- A SACL access control entry specifies the success or failure events to log when auditing specified actions performed by particular users, groups, or computer objects.

- **Permission inheritance**

  Permission inheritance describes how permissions defined in security descriptors are propagated to an object from a parent object. Only inheritable permissions are inherited by child objects. When setting permissions on the parent object, you can decide whether folders, sub-folders, and files can inherit them with “Apply to `this-folder`, `sub-folders`, and `files`”.

Related information

Configure and apply file security on NTFS files and folders using the CLI

SMB and NFS auditing and security tracing

Configuring and applying audit policies to NTFS files and folders using the CLI

Guidelines for applying file-directory policies that use local users or groups on the SVM disaster recovery destination

There are certain guidelines that you must keep in mind before applying file-directory policies on the storage virtual machine (SVM) disaster recovery destination in an ID discard configuration if your file-directory policy configuration uses local users or groups in either the security descriptor or the DACL or SACL entries.

You can configure a disaster recovery configuration for an SVM where the source SVM on the source cluster replicates the data and configuration from the source SVM to a destination SVM on a destination cluster.

You can set up one of two types of SVM disaster recovery:

- Identity preserved

  With this configuration, the identity of the SVM and the CIFS server is preserved.

- Identity discarded

  With this configuration, the identity of the SVM and the CIFS server is not preserved. In this scenario, the name of the SVM and the CIFS server on the destination SVM is different from the SVM and the CIFS server name on the source SVM.

Guidelines for identity discarded configurations

In an identity discarded configuration, for an SVM source that contains local user, group, and privilege configurations, the name of the local domain (local CIFS server name) must be changed to match the CIFS server name on the SVM destination. For example, if the source SVM name is “vs1” and CIFS server name is “CIFS1”, and the destination SVM name is “vs1_dst” and the CIFS server name is “CIFS1_DST”, then the local domain name for a local user named “CIFS1\user1” is automatically changed to “CIFS1_DST\user1” on the destination SVM:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Even though local user and group names are automatically changed in the local user and group databases, local users or group names are not automatically changed in file-directory policy configurations (policies configured on the CLI using the `vserver security file-directory` command family).

For example, for “vs1”, if you have configured a DACL entry where the `-account` parameter is set to “CIFS1\user1”, the setting is not automatically changed on the destination SVM to reflect the destination’s CIFS server name.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

You must use the `vserver security file-directory modify` commands to manually change the CIFS server name to the destination CIFS server name.

File-directory policy configuration components that contain account parameters

There are three file-directory policy configuration components that can use parameter settings that can contain local users or groups:

- Security descriptor

  You can optionally specify the owner of the security descriptor and the primary group of the owner of the security descriptor. If the security descriptor uses a local user or group for the owner and primary group entries, you must modify the security descriptor to use the destination SVM in the account name. You can use the `vserver security file-directory ntfs modify` command to make any necessary changes to the account names.

- DACL entries

  Each DACL entry must be associated with an account. You must modify any DACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing DACL entries, you must remove any DACL entries with local users or groups from the security descriptors, create new DACL entries with the corrected destination account names, and associate these new DACL entries with the appropriate security descriptors.

- SACL entries

  Each SACL entry must be associated with an account. You must modify any SACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing SACL entries, you must remove any SACL entries with local users or groups from the security descriptors, create new SACL entries with the corrected destination account names, and associate these new SACL entries with the appropriate security descriptors.

You must make any necessary changes to local users or groups used in the file-directory policy configuration before applying the policy; otherwise, the apply job fails.

Configure and apply file security on NTFS files and folders using the CLI

Create an NTFS security descriptor

Creating an NTFS security descriptor (file security policy) is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within storage virtual machines (SVMs). You can associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

Add NTFS DACL access control entries to the NTFS security descriptor

Adding DACL (discretionary access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

About this task

You can add one or more ACEs to the security descriptor's DACL.

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

You can optionally customize DACL entries by specifying what rights you want to allow or deny for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)

If you do not specify rights for the DACL entry, the default is to set the rights to `Full Control`.

You can optionally customize DACL entries by specifying how to apply inheritance.

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

Steps

1. Add a DACL entry to a security descriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   `vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny -account domain\joe -rights full-control -apply-to this-folder -vserver vs1`

2. Verify that the DACL entry is correct: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   `vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

   ```
                    Vserver: vs1
   Security Descriptor Name: sd1
                Allow or Deny: deny
            Account Name or SID: DOMAIN\joe
                  Access Rights: full-control
     Advanced Access Rights: -
                       Apply To: this-folder
                  Access Rights: full-control
   ```

Create security policies

Creating a file security policy for SVMs is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each SVM (containing NTFS security-style volumes or mixed security-style volumes).

Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verify the security policy: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Add a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

  Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.

  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

When adding tasks to security policies, you must specify the following four required parameters:

- SVM name
- Policy name

- Path
- Security descriptor to associate with the path

You can customize the security descriptor configuration by using the following optional parameters:

- Security type
- Propagation mode
- Index position
- Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Apply security policies

Applying a file security policy to SVMs is the last step in creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   The policy apply job is scheduled and the Job ID is returned.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitor the security policy job

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verify the applied file security

You can verify the file security settings to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired settings.

About this task

You must supply the name of the SVM that contains the data and the path to the file and folders on which you want to verify security settings. You can use the optional `-expand-mask` parameter to display detailed information about the security settings.

Step

1. Display file and folder security settings: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
```

```
                        Group:BUILTIN\Administrators
                        DACL - ACEs
                          ALLOW-Everyone-0x1f01ff
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...0 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
```

```
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configure and apply audit policies to NTFS files and folders using the CLI overview

There are several steps you must perform to apply audit policies to NTFS files and folders when using the ONTAP CLI. First, you create an NTFS security descriptor and add SACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a storage virtual machine (SVM).

About this task

After applying the security policy, you can monitor the security policy job and then verify the settings for the applied audit policy.

When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

Related information

Securing file access by using Storage-Level Access Guard

Limits when using the CLI to set file and folder security

How security descriptors are used to apply file and folder security

SMB and NFS auditing and security tracing

Configure and apply file security on NTFS files and folders using the CLI

Create an NTFS security descriptor

Creating an NTFS security descriptor audit policy is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within SVMs. You will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

Steps

1. If you want to use the advanced parameters, set the privilege level to advanced: `set -privilege advanced`
2. Create a security descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verify that the security descriptor configuration is correct: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                          Security Descriptor Name: sd1
                    Owner of the Security Descriptor: DOMAIN\joe
   ```

4. If you are in the advanced privilege level, return to the admin privilege level: `set -privilege admin`

Add NTFS SACL access control entries to the NTFS security descriptor

Adding SACL (system access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in SVMs. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

About this task

You can add one or more ACEs to the security descriptor's SACL.

If the security descriptor contains a SACL that has existing ACEs, the command adds the new ACE to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new ACE to it.

You can configure SACL entries by specifying what rights you want to audit for success or failure events for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)

If you do not specify rights for the SACL entry, the default setting is `Full Control`.

You can optionally customize SACL entries by specifying how to apply inheritance with the `apply to` parameter. If you do not specify this parameter, the default is to apply this SACL entry to this folder, subfolders,

and files.

Steps

1. Add a SACL entry to a security descriptor: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   `vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1`

2. Verify that the SACL entry is correct: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   `vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                                 Vserver: vs1
                    Security Descriptor Name: sd1
         Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
```

Create security policies

Creating an audit policy for storage virtual machines (SVMs) is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each storage virtual machine (SVM) (containing NTFS security-style volumes or mixed security-style volumes).

Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verify the security policy: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Add a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

  Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.

  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

You can customize the security descriptor configuration by using the following optional parameters:

- Security type
- Propagation mode

- Index position
- Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Apply security policies

Applying an audit policy to SVMsis the last step in creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

The policy apply job is scheduled and the Job ID is returned.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitor the security policy job

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Verify the applied audit policy

You can verify the audit policy to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired audit security settings.

About this task

You use the `vserver security file-directory show` command to display audit policy information. You must supply the name of the SVM that contains the data and the path to the data whose file or folder audit policy information you want to display.

Step

1. Display audit policy settings: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Example

The following command displays the audit policy information applied to the path “/corp” in SVM vs1. The path has both a SUCCESS and a SUCCESS/FAIL SACL entry applied to it:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerations when managing security policy jobs

If a security policy job exists, under certain circumstances, you cannot modify that security policy or the tasks assigned to that policy. You should understand under what conditions you can or cannot modify security policies so that any attempts that you make to modify the policy are successful. Modifications to the policy include adding, removing, or modifying tasks assigned to the policy and deleting or modifying the policy.

You cannot modify a security policy or a task assigned to that policy if a job exists for that policy and that job is in the following states:

- The job is running or in progress.
- The job is paused.
- The job is resumed and is in the running state.
- If the job is waiting to failover to another node.

Under the following circumstances, if a job exists for a security policy, you can successfully modify that security policy or a task assigned to that policy:

- The policy job is stopped.

- The policy job has successfully finished.

Commands for managing NTFS security descriptors

There are specific ONTAP commands for managing security descriptors. You can create, modify, delete, and display information about security descriptors.

If you want to…	Use this command…
Create NTFS security descriptors	`vserver security file-directory ntfs create`
Modify existing NTFS security descriptors	`vserver security file-directory ntfs modify`
Display information about existing NTFS security descriptors	`vserver security file-directory ntfs show`
Delete NTFS security descriptors	`vserver security file-directory ntfs delete`

See the man pages for the `vserver security file-directory ntfs` commands for more information.

Commands for managing NTFS DACL access control entries

There are specific ONTAP commands for managing DACL access control entries (ACEs). You can add ACEs to NTFS DACLs at any time. You can also manage existing NTFS DACLs by modifying, deleting, and displaying information about ACEs in DACLs.

If you want to…	Use this command…
Create ACEs and add them to NTFS DACLs	`vserver security file-directory ntfs dacl add`
Modify existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl modify`
Display information about existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl show`
Remove existing ACEs from NTFS DACLs	`vserver security file-directory ntfs dacl remove`

See the man pages for the `vserver security file-directory ntfs dacl` commands for more information.

Commands for managing NTFS SACL access control entries

There are specific ONTAP commands for managing SACL access control entries (ACEs). You can add ACEs to NTFS SACLs at any time. You can also manage existing NTFS SACLs by modifying, deleting, and displaying information about ACEs in SACLs.

If you want to…	Use this command…
Create ACEs and add them to NTFS SACLs	`vserver security file-directory ntfs sacl add`
Modify existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl modify`
Display information about existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl show`
Remove existing ACEs from NTFS SACLs	`vserver security file-directory ntfs sacl remove`

See the man pages for the `vserver security file-directory ntfs sacl` commands for more information.

Commands for managing security policies

There are specific ONTAP commands for managing security policies. You can display information about policies and you can delete policies. You cannot modify a security policy.

If you want to…	Use this command…
Create security policies	`vserver security file-directory policy create`
Display information about security policies	`vserver security file-directory policy show`
Delete security policies	`vserver security file-directory policy delete`

See the man pages for the `vserver security file-directory policy` commands for more information.

Commands for managing security policy tasks

There are ONTAP commands for adding, modifying, removing, and displaying information about security policy tasks.

If you want to…	Use this command…
Add security policy tasks	`vserver security file-directory policy task add`
Modify security policy tasks	`vserver security file-directory policy task modify`
Display information about security policy tasks	`vserver security file-directory policy task show`
Remove security policy tasks	`vserver security file-directory policy task remove`

See the man pages for the `vserver security file-directory policy task` commands for more information.

Commands for managing security policy jobs

There are ONTAP commands for pausing, resuming, stopping, and displaying information about security policy jobs.

If you want to…	Use this command…
Pause security policy jobs	`vserver security file-directory job pause -vserver vserver_name -id integer`
Resume security policy jobs	`vserver security file-directory job resume -vserver vserver_name -id integer`
Display information about security policy jobs	`vserver security file-directory job show -vserver vserver_name` You can determine the job ID of a job using this command.
Stop security policy jobs	`vserver security file-directory job stop -vserver vserver_name -id integer`

See the man pages for the `vserver security file-directory job` commands for more information.

Configure the metadata cache for SMB shares

How SMB metadata caching works

Metadata caching enables file attribute caching on SMB 1.0 clients to provide faster access to file and folder attributes. You can enable or disable attribute caching on a per-share basis. You can also configure the time-to-live for cached entries if metadata caching is enabled. Configuring metadata caching is not necessary if clients are

connecting to shares over SMB 2.x or SMB 3.0.

When enabled, the SMB metadata cache stores path and file attribute data for a limited amount of time. This can improve SMB performance for SMB 1.0 clients with common workloads.

For certain tasks, SMB creates a significant amount of traffic that can include multiple identical queries for path and file metadata. You can reduce the number of redundant queries and improve performance for SMB 1.0 clients by using SMB metadata caching to fetch information from the cache instead.

While unlikely, it is possible that the metadata cache might serve stale information to SMB 1.0 clients. If your environment cannot afford this risk, you should not enable this feature.

Enable the SMB metadata cache

You can improve SMB performance for SMB 1.0 clients by enabling the SMB metadata cache. By default, SMB metadata caching is disabled.

Step

1. Perform the desired action:

If you want to…	Enter the command…
Enable SMB metadata caching when you create a share	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
Enable SMB metadata caching on an existing share	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Related information

Configuring the lifetime of SMB metadata cache entries

Adding or removing share properties on an existing SMB share

Configure the lifetime of SMB metadata cache entries

You can configure the lifetime of SMB metadata cache entries to optimize the SMB metadata cache performance in your environment. The default is 10 seconds.

Before you begin

You must have enabled the SMB metadata cache feature. If SMB metadata caching is not enabled, the SMB cache TTL setting is not used.

Step

1. Perform the desired action:

If you want to configure the lifetime of SMB metadata cache entries when you…	Enter the command…
Create a share	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modify an existing share	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

You can specify additional share configuration options and properties when you create or modify shares. See the man pages for more information.

Manage file locks

About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

How ONTAP treats read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How ONTAP differs from Windows on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

Display information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. See the man page for the command for more information.

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
```

```
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Break locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

The man page for the command contains detailed information.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Perform one of the following actions:

If you want to break a lock by specifying…	Enter the command…
The SVM name, volume name, LIF name, and file path	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
The lock ID	`vserver locks break -lockid UUID`

4. Return to the admin privilege level: `set -privilege admin`

Monitor SMB activity

Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display SMB session information…	Enter the following command…
For all sessions on the SVM in summary form	`vserver cifs session show -vserver vserver_name`

If you want to display SMB session information…	Enter the following command…
On a specified connection ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
From a specified workstation IP address	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
On a specified LIF IP address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
On a specified node	`vserver cifs session show -vserver vserver_name -node {node_name|local}`
From a specified Windows user	`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`
With a specified authentication mechanism	`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1|NTLMv2|Kerberos|Anonymous}`
With a specified protocol version	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1|SMB2|SMB2_1|SMB3|SMB3_1}` Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to `SMB3` or later.

If you want to display SMB session information…	Enter the following command…
With a specified level of continuously available protection	`vserver cifs session show -vserver vserver_name -continuously-available {No|Yes|Partial}` If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
With a specified SMB signing session status	`vserver cifs session show -vserver vserver_name -is-session-signed {true|false}`

Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                  Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
          Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Related information

Displaying information about open SMB files

Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can display information about a file's continuously available protection level, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously-available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

  You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

  You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	`vserver cifs session file show -vserver vserver_name`
On a specified node	`vserver cifs session file show -vserver vserver_name -node {node_name|local}`
On a specified file ID	`vserver cifs session file show -vserver vserver_name -file-id integer`
On a specified SMB connection ID	`vserver cifs session file show -vserver vserver_name -connection-id integer`
On a specified SMB session ID	`vserver cifs session file show -vserver vserver_name -session-id integer`
On the specified hosting aggregate	`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`
On the specified volume	`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`
On the specified SMB share	`vserver cifs session file show -vserver vserver_name -share share_name`

If you want to display open SMB files…	Enter the following command…
On the specified SMB path	`vserver cifs session file show -vserver vserver_name -path path`
With the specified level of continuously available protection	`vserver cifs session file show -vserver vserver_name -continuously -available {No|Yes}` If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	`vserver cifs session file show -vserver vserver_name -reconnected {No|Yes}` If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                 Node: node1
              Vserver: vs1
              File ID: 82
        Connection ID: 104617
           Session ID: 1
            File Type: Regular
            Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
           CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
           Share Mode: rw
          Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Related information

Displaying SMB session information

Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to determine…	Enter…
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show object object_name`
Which counters are available	`statistics catalog counter show object object_name`

See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level: `set -privilege admin`

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:

> This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Related information

Displaying statistics

Display statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

Before you begin

You must have collected data samples by using the `statistics start` and `statistics stop` commands before you can display information about objects.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to display statistics for…	Enter…
All versions of SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x and SMB 3.0	`statistics show -object smb2`
CIFS subsystem of the node	`statistics show -object nblade_cifs`
Multiprotocol audit	`statistics show -object audit_ng`
BranchCache hash service	`statistics show -object hashd`
Dynamic DNS	`statistics show -object ddns_update`

   See the man page for each command for more information.

3. Return to the admin privilege level: `set -privilege admin`

Related information

Determining which statistics objects and counters are available

Monitoring SMB signed session statistics

Displaying BranchCache statistics

Using statistics to monitor automatic node referral activity

SMB configuration for Microsoft Hyper-V and SQL Server

Performance monitoring setup

Deploy SMB client-based services

Use offline files to allow caching of files for offline use

Use offline files to allow caching of files for offline use overview

ONTAP supports the Microsoft Offline Files feature, or *client-side caching*, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

- No caching

  Disables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.

- Manual caching

  Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.

- Automatic document caching

  Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.

- Automatic program caching

  Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM

Using folder redirection to store data on a CIFS server

Using BranchCache to cache SMB share content at a branch office

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Requirements for using offline files

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP releases support offline files.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports offline files on all versions of SMB.

Windows client requirements

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Guidelines for deploying offline files

There are some important guidelines you need to understand when you deploy offline files on home directory shares that have the `showsnapshot` share property set on home directories.

If the `showsnapshot` share property is set on a home directory share that has offline files configured, Windows clients cache all of the Snapshot copies under the `~snapshot` folder in the user's home directory.

Windows clients cache all of the Snapshot copies under the home directory if one of more of the following is true:

- The user makes the home directory available offline from the client.

  The contents of the `~snapshot` folder in the home directory is included and made available offline.

- The user configures folder redirection to redirect a folder such as `My Documents` to the root of a home directory residing on the CIFS server share.

  Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the `~snapshot` folder is included in the cached offline content.

Offline file deployments where the `~snapshot` folder is included in offline files should be avoided. The Snapshot copies in the `~snapshot` folder contain all data on the volume at the point at which ONTAP created the Snapshot copy. Therefore, creating an offline copy of the `~snapshot` folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.

Configure offline files support on SMB shares using the CLI

You can configure offline files support using the ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

About this task

When configuring offline files support, you can choose one of the following four offline files settings:

Setting	Description
`none`	Disallows Windows clients from caching any files on this share.
`manual`	Allows users on Windows clients to manually select files to be cached.
`documents`	Allows Windows clients to cache user documents that are used by the user for offline access.
`programs`	Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

Steps

1. Perform the appropriate action:

If you want to configure offline files on…	Enter the command…
A new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none|manual|documents|programs}`

If you want to configure offline files on…	Enter the command…
An existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none|manual|documents|programs}`

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named “data1” with offline files set to `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

The following command modifies an existing SMB share named “data1” by changing the offline files setting to `manual` and adding values for the file and directory mode creation mask:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Related information

Adding or removing share properties on an existing SMB share

Configure offline files support on SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select **Manage**.
2. On the left panel, select **Computer Management**.
3. Select **Action** > **Connect to another computer**.

   The Select Computer dialog box appears.

4. Type the name of the CIFS server or click **Browse** to locate the CIFS server.

   If the name of CIFS server is the same as the storage virtual machine (SVM) host name, type the SVM name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click **OK**.
6. In the console tree, click **System Tools** > **Shared Folders**.
7. Click **Shares**.
8. In the results pane, right-click the share.
9. Click **Properties**.

   Properties for the share you selected are displayed.

10. In the **General** tab, click **Offline Settings**.

    The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.
12. Click **OK**.

Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM

Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM overview

ONTAP supports storing Windows roaming profiles on a CIFS server associated with the storage virtual machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability

  A user's unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.

- Simplified computer replacement

  Because all of the user's profile information is maintained separately on the network, a user's profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

Related information

Using offline files to allow caching of files for offline use

Using folder redirection to store data on a CIFS server

Requirements for using roaming profiles

Before you can use Microsoft's roaming profiles with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support roaming profiles.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports roaming profiles on all versions of SMB.

Windows client requirements

Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Configure roaming profiles

If you want to automatically make a user's profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server 2012, you can use the Active Directory Administration Center.

Steps

1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows 2012 and later servers).
2. Locate the user for which you want to configure a roaming profile.
3. Right-click the user and click **Properties**.
4. On the **Profile** tab, enter the profile path to the share where you want to store the user's roaming profile, followed by `%username%`.

   For example, a profile path might be the following: `\\vs1.example.com\profiles\%username%`. The first time a user logs in, `%username%` is replaced with the user's name.

   > In the path `\\vs1.example.com\profiles\%username%`, `profiles` is the share name of a share on storage virtual machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click **OK**.

Use folder redirection to store data on a SMB server

Use folder redirection to store data on a SMB server overview

ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

- `Documents`, `Desktop`, and `Start Menu` are examples of folders that you can redirect.
- Users can redirect folders from their Windows client.
- Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
- If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
- Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

Related information

Using offline files to allow caching of files for offline use

Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM

Requirements for using folder redirection

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support Microsoft folder redirection.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Microsoft's folder redirection on all versions of SMB.

Windows client requirements

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Configure folder redirection

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

Steps

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.
2. Click **Properties**.

   Properties for the share you selected are displayed.

3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.

For example, if you want to redirect a folder to the `data` folder in a home directory that is mapped to `Q:\`, specify `Q:\data` as the target.

4. Click **OK**.

   For more information about configuring offline folders, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Access the ~snapshot directory from Windows clients using SMB 2.x

The method that you use to access the `~snapshot` directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the `~snapshot` directory when using SMB 2.x connections to successfully access data stored in Snapshot copies.

The SVM administrator controls whether users on Windows clients can view and access the `~snapshot` directory on a share by enabling or disabling the `showsnapshot` share property using commands from the vserver cifs share properties families.

When the `showsnapshot` share property is disabled, a user on a Windows client using SMB 2.x cannot view the `~snapshot` directory and cannot access Snapshot copies within the `~snapshot` directory, even when manually entering the path to the `~snapshot` directory or to specific Snapshot copies within the directory.

When the `showsnapshot` share property is enabled, a user on a Windows client using SMB 2.x still cannot view the `~snapshot` directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden `~snapshot` directory by manually appending `\~snapshot` to the end of the share path. The hidden `~snapshot` directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden `~snapshot` directory is not accessible from non-junction subdirectories within the share.

Example

With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the “eng” share can access the `~snapshot` directory by manually appending `\~snapshot` to the share path at the root of the share and at every junction point in the path. The hidden `~snapshot` directory is accessible from the following three paths:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recover files and folders using Previous Versions

Recover files and folders using previous versions overview

The ability to use Microsoft Previous Versions is applicable to file systems that support Snapshot copies in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from Snapshot copies from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the Snapshot copies or to restore data from a Snapshot copy without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made Snapshot copies available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in Snapshot copies is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshot copies are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

Requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of ONTAP and SMB, and which Windows clients, support it. You also need to know about the Snapshot copy setting requirement.

ONTAP version requirements

Supports Previous Versions.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Previous Versions on all versions of SMB.

Windows client requirements

Before a user can use Previous Versions to access data in Snapshot copies, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Requirements for Snapshot copy settings

To use Previous Versions to access data in Snapshot copies, an enabled Snapshot policy must be associated to the volume containing the data, clients must be able to access to the Snapshot data, and Snapshot copies must exist.

Use the Previous Versions tab to view and manage Snapshot copy data

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in Snapshot copies without needing to involve the storage virtual machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in Snapshot copies of data stored on the SVM if the administrator has enabled Snapshot copies on the volume containing the share, and if the administrator configures the share to show Snapshot copies.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose Snapshot copies you want to view or manage.
3. Click **Properties**.

   Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

   A list of available Snapshot copies of the selected file or folder is displayed in the Folder versions: box. The listed Snapshot copies are identified by the Snapshot copy name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

If you want to…	Do the following…
View data from that Snapshot copy	Click **Open**.

If you want to…	Do the following…
Create a copy of data from that Snapshot copy	Click **Copy**.

Data in Snapshot copies is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing Snapshot data, close the **Properties** dialog box by clicking **OK**.

   For more information about using the Previous Versions tab to view and manage Snapshot data, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Determine whether Snapshot copies are available for Previous Versions use

You can view Snapshot copies from the Previous Versions tab only if an enabled Snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to Snapshot copies. Determining Snapshot copy availability is helpful when assisting a user with Previous Versions access.

Steps

1. Determine whether the volume on which the share data resides has automatic Snapshot copies enabled and whether clients have access to Snapshot directories: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   The output displays what Snapshot policy is associated with the volume, whether client Snapshot directory access is enabled, and the number of available Snapshot copies.

2. Determine whether the associated Snapshot policy is enabled: `volume snapshot policy show -policy policy-name`
3. List the available Snapshot copies: `volume snapshot show -volume volume_name`

   For more information about configuring and managing Snapshot policies and Snapshot schedules, see Data Protection.

Example

The following example displays information about Snapshot policies associated with the volume named “data1” that contains the shared data and available Snapshot copies on “data1”.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Related information

Creating a Snapshot configuration to enable Previous Versions access

Data protection

Create a Snapshot configuration to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to Snapshot copies is enabled and provided that Snapshot copies exist. If your Snapshot copy configuration does not meet these requirements, you can create a Snapshot copy configuration that does.

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated Snapshot policy, associate a Snapshot policy to the volume and enable it by using the `volume modify` command.

   For more information about using the `volume modify` command, see the man pages.

2. Enable access to the Snapshot copies by using the `volume modify` command to set the `-snap-dir` option to `true`.

   For more information about using the `volume modify` command, see the man pages.

3. Verify that Snapshot policies are enabled and that access to Snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

   For more information about using the `volume show` and `volume snapshot policy show` commands, see the man pages.

   For more information about configuring and managing Snapshot policies and Snapshot schedules, see Data Protection.

Related information

Data protection

Guidelines for restoring directories that contain junctions

There are certain guidelines you should keep in mind when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related information

Creating and managing data volumes in NAS namespaces

Deploy SMB server-based services

Manage home directories

How ONTAP enables dynamic home directories

ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of creating separate shares for each user, you can configure one share with a few home directory parameters to define a user's relationship between an entry point (the share) and the home directory (a directory on the SVM).

A user who is logged in as a guest user does not have a home directory and cannot access other users' home directories. There are four variables that determine how a user is mapped to a directory:

- **Share name**

  This is the name of the share that you create to which the user connects. You must set the home directory property for this share.

  The share name can use the following dynamic names:

  - `%w` (the user's Windows user name)
  - `%d` (the user's Windows domain name)
  - `%u` (the user's mapped UNIX user name)
    To make the share name unique across all home directories, the share name must contain either the `%w` or the `%u` variable. The share name can contain both the `%d` and the `%w` variable (for example, `%d/%w`), or the share name can contain a static portion and a variable portion (for example, home_`%w`).

- **Share path**

  This is the relative path, which is defined by the share and is therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, `home`), dynamic (for example, `%w`), or a combination of the two (for example, `eng/%w`).

- **Search paths**

  This is the set of absolute paths from the root of the SVM that you specify that directs the ONTAP search for home directories. You can specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, ONTAP tries them in the order specified until it finds a valid path.

- **Directory**

  This is the user's home directory that you create for the user. The directory name is usually the user's name. You must create the home directory in one of the directories that are defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home_`%w` - share path: `%w`
- Home directory share name #2: `%w` - share path: `%d/%w`
- Search path #1: `/vol0home/home`
- Search path #2: `/vol1home/home`
- Search path #3: `/vol2home/home`
- Home directory: `/vol1home/home/jsmith`

Scenario 1: The user connects to `\\vs1\home_jsmith`. This matches the first home directory share name and generates the relative path `jsmith`. ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/vol0home/home/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/jsmith` does exist; therefore, search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/vol0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/vol2home/home/acme/jsmith` does not exist; the home directory does not exist; therefore, the connection fails.

Home directory shares

Add a home directory share

If you want to use the SMB home directory feature, you must add at least one share with the home directory property included in the share properties.

About this task

You can create a home directory share at the time you create the share by using the `vserver cifs share create` command, or you can change an existing share into a home directory share at any time by using the `vserver cifs share modify` command.

To create a home directory share, you must include the `homedirectory` value in the `-share-properties` option when you create or modify a share. You can specify the share name and share path using variables that are dynamically expanded when users connect to their home directories. Available variables that you can use in the path are `%w`, `%d`, and `%u`, corresponding to the Windows user name, domain, and mapped UNIX user name, respectively.

Steps

1. Add a home directory share:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name` *`share-name`* specifies the home directory share name.

   In addition to containing one of the required variables, if the share name contains one of the literal strings `%w`, `%u`, or `%d`, you must precede the literal string with a % (percent) character to prevent ONTAP from treating the literal string as a variable (for example, `%%w`).

   - The share name must contain either the `%w` or the `%u` variable.

- The share name can additionally contain the `%d` variable (for example, `%d/%w`) or a static portion in the share name (for example, home1_`%w`).
- If the share is used by administrators to connect to other users' home directories or to permit users to connect to other users' home directories, the dynamic share name pattern must be preceded by a tilde (~).

  The `vserver cifs home-directory modify` is used to enable this access by setting the `-is -home-dirs-access-for-admin-enabled` option to `true`) or by setting the advanced option `-is -home-dirs-access-for-public-enabled` to `true`.

`-path path` specifies the relative path to the home directory.

`-share-properties homedirectory[,…]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

1. Verify that you successfully added the home directory share by using the `vserver cifs share show` command.

Example

The following command creates a home directory share named `%w`. The `oplocks`, `browsable`, and `changenotify` share properties are set in addition to setting the `homedirectory` share property.

This example does not display output for all of the shares on the SVM. Output is truncated.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Related information

Adding a home directory search path

Requirements and guidelines for using automatic node referrals

Managing accessibility to users' home directories

Home directory shares require unique user names

Be careful to assign unique user names when creating home directory shares using the `%w` (Windows user name) or `%u` (UNIX user name) variables to generate shares dynamically. The share name is mapped to your user name.

Two problems can occur when a static share's name and a user's name are the same:

- When the user lists the shares on a cluster using the `net view` command, two shares with the same user name are displayed.
- When the user connects to that share name, the user is always connected to the static share and cannot access the home directory share with the same name.

For example, there is a share named "administrator" and you have an "administrator" Windows user name. If you create a home directory share and connect to that share, you get connected to the "administrator" static share, not to your "administrator" home directory share.

You can resolve the issue with duplicate share names by following any of these steps:

- Renaming the static share so that it no longer conflicts with the user's home directory share.
- Giving the user a new user name so that it no longer conflicts with the static share name.
- Creating a CIFS home directory share with a static name such as "home" instead of using the `%w` parameter to avoid conflicts with the share names.

What happens to static home directory share names after upgrading

Home directory share names must contain either the `%w` or the `%u` dynamic variable. You should be aware of what happens to existing static home directory share names after upgrading to a version of ONTAP with the new requirement.

If your home directory configuration contains static share names and you upgrade to ONTAP, the static home directory share names are not changed and are still valid. However, you cannot create any new home directory shares that do not contain either the `%w` or `%u` variable.

Requiring that one of these variables is included in the user's home directory share name ensures that every share name is unique across the home directory configuration. If desired, you can change the static home directory share names to names that contain either the `%w` or `%u` variable.

Add a home directory search path

If you want to use ONTAP SMB home directories, you must add at least one home directory search path.

About this task

You can add a home directory search path by using the `vserver cifs home-directory search-path add` command.

The `vserver cifs home-directory search-path add` command checks the path specified in the `-path` option during command execution. If the specified path does not exist, the command generates a message prompting for whether you want to continue. You choose `y` or `n`. If you choose `y` to continue, ONTAP creates the search path. However, you must create the directory structure before you can use the search path in the home directory configuration. If you choose not to continue, the command fails; the search path is not created. You can then create the path directory structure and rerun the `vserver cifs home-directory search-path add` command.

Steps

1. Add a home directory search path: `vserver cifs home-directory search-path add -vserver`

`vserver -path path`

2. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

Example

The following example adds the path `/home1` to the home directory configuration on SVM vs1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

The following example attempts to add the path `/home2` to the home directory configuration on SVM vs1. The path does not exist. The choice is made to not continue.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Related information

Adding a home directory share

Create a home directory configuration using the %w and %d variables

You can create a home directory configuration using the `%w` and `%d` variables. Users can then connect to their home share using dynamically created shares.

Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name %w` specifies the home directory share name. ONTAP dynamically creates the share name

as each user connects to their home directory. The share name will be of the form *windows_user_name*.

`-path %d/%w` specifies the relative path to the home directory. The relative path is dynamically created as each user connects to their home directory and will be of the form *domain/windows_user_name*.

`-share-properties homedirectory[,…]+` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver-name` specifies the CIFS-enabled SVM on which to add the search path.

   `-path path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

   For example, if you created a qtree with the path of `/vol/vol1/users` and the user name whose directory you want to create is mydomain\user1, you would create a directory with the following path: `/vol/vol1/users/mydomain/user1`.

   If you created a volume named “home1” mounted at `/home1`, you would create a directory with the following path: `/home1/mydomain/user1`.

9. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

   For example, if user mydomain\user1 wants to connect to the directory created in Step 8 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %d/%w.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with NTFS security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from Windows hosts. You can also use this type of configuration when users access their home directories from Windows and UNIX hosts and the file system administrator uses Windows-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Related information

Configuring home directories using the %u variable

Additional home directory configurations

Displaying information about an SMB user's home directory path

Configure home directories using the %u variable

You can create a home directory configuration where you designate the share name using the `%w` variable but you use the `%u` variable to designate the relative path to the home directory share. Users can then connect to their home share using dynamically shares created using their Windows user name without being aware of the actual name or path of the home directory.

Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name %w` specifies the home directory share name. The share name is dynamically created as each user connects to their home directory and is of the form *windows_user_name*.

   > You can also use the `%u` variable for the `-share-name` option. This creates a relative share path that uses the mapped UNIX user name.

   `-path %u` specifies the relative path to the home directory. The relative path is created dynamically as each user connects to their home directory and is of the form *mapped_UNIX_user_name*.

   > The value for this option can contain static elements as well. For example, `eng/%u`.

   `-share-properties homedirectory\[,...\]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.
5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` specifies the CIFS-enabled SVM on which to add the search path.

   `-path path` specifies the absolute directory path to the search path.
7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. If the UNIX user does not exist, create the UNIX user using the `vserver services unix-user create` command.

   > The UNIX user name to which you map the Windows user name must exist before mapping the user.
9. Create a name mapping for the Windows user to the UNIX user using the following command: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

If name mappings already exist that map Windows users to UNIX users, you do not have to perform the mapping step.

The Windows user name is mapped to the corresponding UNIX user name. When the Windows user connects to their home directory share, they connect to a dynamically created home directory with a share name that corresponds to their Windows user name without being aware that the directory name corresponds to the UNIX user name.

10. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

    For example, if you created a qtree with the path of `/vol/vol1/users` and the mapped UNIX user name of the user whose directory you want to create is “unixuser1”, you would create a directory with the following path: `/vol/vol1/users/unixuser1`.

    If you created a volume named “home1” mounted at `/home1`, you would create a directory with the following path: `/home1/unixuser1`.

11. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

    For example, if user mydomain\user1 maps to UNIX user unixuser1 and wants to connect to the directory created in Step 10 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %u.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with UNIX security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from both Windows hosts or Windows and UNIX hosts and the file system administrator uses UNIX-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Related information

Creating a home directory configuration using the %w and %d variables

Additional home directory configurations

Displaying information about an SMB user's home directory path

Additional home directory configurations

You can create additional home directory configurations using the `%w`, `%d`, and `%u` variables, which enables you to customize the home directory configuration to meet your needs.

You can create a number of home directory configurations using a combination of variables and static strings in the share names and search paths. The following table provides some examples illustrating how to create different home directory configurations:

Paths created when `/vol1/user` contains home directories…	**Share command…**
To create a share path `\\vs1\~win_username` that directs the user to `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\win_username` that directs the user to `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\win_username` that directs the user to `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\unix_username` that directs the user to `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Commands for managing search paths

There are specific ONTAP commands for managing search paths for SMB home directory configurations. For example, there are commands for adding, removing, and displaying information about search paths. There is also a command for changing the search path order.

If you want to…	**Use this command…**
Add a search path	`vserver cifs home-directory search-path add`
Display search paths	`vserver cifs home-directory search-path show`

If you want to…	Use this command…
Change the search path order	`vserver cifs home-directory search-path reorder`
Remove a search path	`vserver cifs home-directory search-path remove`

See the man page for each command for more information.

Display information about an SMB user's home directory path

You can display an SMB user's home directory path on the storage virtual machine (SVM), which can be used if you have multiple CIFS home directory paths configured and you want to see which path holds the user's home directory.

Step

1. Display the home directory path by using the `vserver cifs home-directory show-user` command.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

Related information

Managing accessibility to users' home directories

Manage accessibility to users' home directories

By default, a user's home directory can be accessed only by that user. For shares where the dynamic name of the share is preceded with a tilde (~), you can enable or disable access to users' home directories by Windows administrators or by any other user (public access).

Before you begin

Home directory shares on the storage virtual machine (SVM) must be configured with dynamic share names that are preceded with a tilde (~). The following cases illustrate share naming requirements:

Home directory share name	Example of command to connect to the share
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`

Home directory share name	Example of command to connect to the share
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Step

1. Perform the appropriate action:

If you want to enable or disable access to users' home directories to…	Enter the following…
Windows administrators	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` The default is `true`.
Any user (public access)	a. Set the privilege level to advanced: `set -privilege advanced` b. Enable or disable access: `vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs-access -for-public-enabled {true|false}` The default is `false`. c. Return to the admin privilege level: `set -privilege admin`

The following example enables public access to users' home directories:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Related information

Displaying information about an SMB user's home directory path

Configure SMB client access to UNIX symbolic links

How ONTAP enables you to provide SMB client access to UNIX symbolic links

A symbolic link is a file that is created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, the client is redirected to the target file or directory to which the symbolic link refers. ONTAP supports relative and absolute symbolic links, including widelinks (absolute links with targets outside the local file system).

ONTAP provides SMB clients the ability to follow UNIX symbolic links that are configured on the SVM. This feature is optional, and you can configure it on a per-share basis, using the `-symlink-properties` option of the `vserver cifs share create` command, with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

If you enable symbolic links on a share, relative symbolic links work without further configuration.

If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination SMB path. When creating absolute symbolic link mappings, you can specify whether it is a local link or a *widelink*; widelinks can be links to file systems on other storage devices or links to file systems hosted in separate SVMs on the same ONTAP system. When you create a widelink, it must include the information for the client to follow; that is, you create a reparse point for the client to discover the directory junction point. If you create an absolute symbolic link to a file or directory outside of the local share but set the locality to local, ONTAP disallows access to the target.

If a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory to which the widelink refers. ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

- **Reparse points and ONTAP file system services**

  A *reparse point* is an NTFS file system object that can be optionally stored on volumes along with a file. Reparse points provide SMB clients the ability to receive enhanced or extended file system services when working with NTFS style volumes. Reparse points consist of standard tags that identify the type of reparse point, and the content of the reparse point that can be retrieved by SMB clients for further processing by the client. Of the object types available for extended file system functionality, ONTAP implements support for NTFS symbolic links and directory junction points using reparse point tags. SMB clients that cannot understand the contents of a reparse point simply ignore it and don’t provide the extended file system service that the reparse point might enable.

- **Directory junction points and ONTAP support for symbolic links**

  Directory junction points are locations within a file system directory structure that can refer to alternate locations where files are stored, either on a different path (symbolic links) or a separate storage device (widelinks). ONTAP SMB servers expose directory junction points to Windows clients as reparse points, allowing capable clients to obtain reparse point contents from ONTAP when a directory junction point is traversed. They can thereby navigate and connect to different paths or storage devices as though they were part of the same file system.

- **Enabling widelink support using reparse point options**

  The `-is-use-junctions-as-reparse-points-enabled` option is enabled by default in ONTAP 9. Not all SMB clients support widelinks, so the option to enable the information is configurable on a per-protocol version basis, allowing administrators to accommodate both supported and non-supported SMB clients. In ONTAP 9.2 and later releases, you must enable the option `-widelink-as-reparse-point-versions` for each client protocol that accesses the share using widelinks; the default is SMB1. In earlier releases, only widelinks accessed using the default SMB1 were reported, and systems using SMB2 or SMB3 were unable to access the widelinks.

For more information, see the Microsoft NTFS documentation.

Microsoft Documentation: Reparse Points

Limits when configuring UNIX symbolic links for SMB access

You need to be aware of certain limits when configuring UNIX symbolic links for SMB access.

Limit	Description
45	Maximum length of the CIFS server name that you can specify when using an FQDN for the CIFS server name. You can alternatively specify the CIFS server name as a NetBIOS name, which is limited to 15 characters.
80	Maximum length of the share name.
256	Maximum length of the UNIX path that you can specify when creating a symbolic link or when modifying an existing symbolic link's UNIX path.The UNIX path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.
256	Maximum length of the CIFS path that you can specify when creating a symbolic link or when modifying an existing symbolic link's CIFS path.The CIFS path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.

Related information

Creating symbolic link mappings for SMB shares

Control automatic DFS advertisements in ONTAP with a CIFS server option

A CIFS server option controls how DFS capabilities are advertised to SMB clients when connecting to shares. Because ONTAP uses DFS referrals when clients access symbolic links over SMB, you should be aware of what the impact is when disabling or enabling this option.

A CIFS server option determines whether the CIFS servers automatically advertise that they are DFS capable to SMB clients. By default, this option is enabled and the CIFS server always advertises that it is DFS capable to SMB clients (even when connecting to shares where access to symbolic links is disabled). If you want the CIFS server to advertise that it is DFS capable to clients only when they are connecting to shares where access to symbolic links is enabled, you can disable this option.

You should be aware of what happens when this option is disabled:

- The share configurations for symbolic links is unchanged.
- If the share parameter is set to allow symbolic link access (either read-write access or read-only access), the CIFS server advertises DFS capabilities to clients connecting to that share.

  Client connections and access to symbolic links continue without interruption.

- If the share parameter is set to not allow symbolic link access (either by disabling access or if the value for the share parameter is null), the CIFS server does not advertise DFS capabilities to clients connecting to that share.

  Because clients have cached information that the CIFS server is DFS capable and it is no longer advertising that it is, clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. After the option is disabled, you might need to reboot clients that are connected to these shares, thus clearing the cached information.

These changes do not apply to SMB 1.0 connections.

Configure UNIX symbolic link support on SMB shares

You can configure UNIX symbolic link support on SMB shares by specifying a symbolic link share-property setting when you create SMB shares or at any time by modifying existing SMB shares. UNIX symbolic link support is enabled by default. You can also disable UNIX symbolic link support on a share.

About this task

When configuring UNIX symbolic link support for SMB shares, you can choose one of the following settings:

Setting	Description
`enable` (DEPRECATED*)	Specifies that symbolic links are enabled for read-write access.
`read_only` (DEPRECATED*)	Specifies that symlinks are enabled for read-only access. This setting does not apply to widelinks. Widelink access is always read-write.
`hide` (DEPRECATED*)	Specifies that SMB clients are prevented from seeing symlinks.
`no-strict-security`	Specifies that clients follow symlinks outside of share boundaries.
`symlinks`	Specifies that symlinks are enabled locally for read-write access. The DFS advertisements are not generated even if the CIFS option `is-advertise-dfs-enabled` is set to `true`. This is the default setting.

Setting	Description
`symlinks-and-widelinks`	Specifies that both local symlinks and widelinks for read-write access. The DFS advertisements are generated for both local symlink and widelinks even if the CIFS option `is-advertise-dfs-enabled` is set to `false`.
`disable`	Specifies that symlinks and widelinks are disabled. The DFS advertisements are not generated even if the CIFS option `is-advertise-dfs-enabled` is set to `true`.
`""` (null, not set)	Disables symbolic links on the share.
– (not set)	Disables symbolic links on the share.

*The *enable*, *hide*, and *read-only* parameters are deprecated and may be removed in a future release of ONTAP.

Steps

1. Configure or disable symbolic link support:

If it is…	Enter…
A new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable|hide|read-only|""|-|symlinks|symlinks-and-widelinks|disable},...]`
An existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable|hide|read-only|""|-|symlinks|symlinks-and-widelinks|disable},...]`

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named “data1” with the UNIX symbolic link configuration set to `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                   Share Properties: oplocks
                                     browsable
                                     changenotify
                 Symlink Properties: enable
           File Mode Creation Mask: -
      Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Related information

Creating symbolic link mappings for SMB shares

Create symbolic link mappings for SMB shares

You can create mappings of UNIX symbolic links for SMB shares. You can either create a relative symbolic link, which refers to the file or folder relative to its parent folder, or you can create an absolute symbolic link, which refers to the file or folder using an absolute path.

About this task

Widelinks are not accessible from Mac OS X clients if you use SMB 2.x. When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails. However, you can use widelinks with Mac OS X clients if you use SMB 1.

Steps

1. To create symbolic link mappings for SMB shares: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` specifies the storage virtual machine (SVM) name.

`-unix-path path` specifies the UNIX path. The UNIX path must begin with a slash (`/`) and must end with a slash (`/`).

`-share-name share_name` specifies the name of the SMB share to map.

`-cifs-path path` specifies the CIFS path. The CIFS path must begin with a slash (`/`) and must end with a slash (`/`).

`-cifs-server server_name` specifies the CIFS server name. The CIFS server name can be specified as a DNS name (for example, mynetwork.cifs.server.com), IP address, or NetBIOS name. The NetBIOS name can be determined by using the `vserver cifs show` command. If this optional parameter is not specified, the default value is the NetBIOS name of the local CIFS server.

`-locality {local|free|widelink}` specifies whether to create a local link, a free link or a wide symbolic link. A local symbolic link maps to the local SMB share. A free symbolic link can map anywhere on the local SMB server. A wide symbolic link maps to any SMB share on the network. If you do not specify this optional parameter, the default value is `local`.

`-home-directory {true|false}` specifies whether the target share is a home directory. Even though this parameter is optional, you must set this parameter to `true` when the target share is configured as a home directory. The default is `false`.

Example

The following command creates a symbolic link mapping on the SVM named vs1. It has the UNIX path `/src/`, the SMB share name “SOURCE”, the CIFS path `/mycompany/source/`, and the CIFS server IP address 123.123.123.123, and it is a widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Related information

Configuring UNIX symbolic link support on SMB shares

Commands for managing symbolic link mappings

There are specific ONTAP commands for managing symbolic link mappings.

If you want to…	Use this command…
Create a symbolic link mapping	`vserver cifs symlink create`
Display information about symbolic link mappings	`vserver cifs symlink show`
Modify a symbolic link mapping	`vserver cifs symlink modify`
Delete a symbolic link mapping	`vserver cifs symlink delete`

See the man page for each command for more information.

Use BranchCache to cache SMB share content at a branch office

Use BranchCache to cache SMB share content at a branch office overview

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on storage virtual machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

Related information

Using offline files to allow caching of files for offline use

Requirements and guidelines

BranchCache version support

You should be aware of which BranchCache versions ONTAP supports.

ONTAP supports BranchCache 1 and the enhanced BranchCache 2:

- When you configure BranchCache on the SMB server for the storage virtual machine (SVM), you can enable BranchCache 1, BranchCache 2, or all versions.

  By default, all versions are enabled.

- If you enable only BranchCache 2, the remote office Windows client machines must support BranchCache 2.

  Only SMB 3.0 or later clients support BranchCache 2.

For more information about BranchCache versions, see the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Network protocol support requirements

You must be aware of the network protocol requirements for implementing ONTAP BranchCache.

You can implement the ONTAP BranchCache feature over IPv4 and IPv6 networks using SMB 2.1 or later.

All CIFS servers and branch office machines participating in the BranchCache implementation must have the SMB 2.1 or later protocol enabled. SMB 2.1 has protocol extensions that allow a client to participate in a BranchCache environment. This is the minimum SMB protocol version that offers BranchCache support. SMB

2.1 supports version BranchCache version 1.

If you want to use BranchCache version 2, SMB 3.0 is the minimum supported version. All CIFS servers and branch office machines participating in a BranchCache 2 implementation must have SMB 3.0 or later enabled.

If you have remote offices where some of the clients support only SMB 2.1 and some of the clients support SMB 3.0, you can implement a BranchCache configuration on the CIFS server that provides caching support over both BranchCache 1 and BranchCache 2.

Even though the Microsoft BranchCache feature supports using both the HTTP/HTTPS and SMB protocols as file access protocols, ONTAP BranchCache only supports the use of SMB.

ONTAP and Windows hosts version requirements

ONTAP and branch office Windows hosts must meet certain version requirements before you can configure BranchCache.

Before configuring BranchCache, you must ensure that the version of ONTAP on the cluster and participating branch office clients support SMB 2.1 or later and support the BranchCache feature. If you configure Hosted Cache mode, you must also ensure that you use a supported host for the cache server.

BranchCache 1 is supported on the following ONTAP versions and Windows hosts:

- Content server: storage virtual machine (SVM) with ONTAP
- Cache server: Windows Server 2008 R2 or Windows Server 2012 or later
- Peer or client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 or Windows Server 2012 or later

BranchCache 2 is supported on the following ONTAP versions and Windows hosts:

- Content server: SVM with ONTAP
- Cache server: Windows Server 2012 or later
- Peer or client: Windows 8 or Windows Server 2012 or later

For the latest information about which Windows clients support BranchCache, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Reasons ONTAP invalidates BranchCache hashes

Understanding the reasons why ONTAP invalidates hashes can be helpful as you plan your BranchCache configuration. It can help you decide which operating mode you should configure and can help you choose on which shares to enable BranchCache.

ONTAP must manage BranchCache hashes to ensure that hashes are valid. If a hash is not valid, ONTAP invalidates the hash and computes a new hash the next time that content is requested, assuming that BranchCache is still enabled.

ONTAP invalidates hashes for the following reasons:

- The server key is modified.

If the server key is modified, ONTAP invalidates all hashes in the hash store.

- A hash is flushed from the cache because the BranchCache hash store maximum size has been reached.

  This is a tunable parameter and can be modified to meet your business requirements.

- A file is modified either through SMB or NFS access.
- A file for which there are computed hashes is restored using the `snap restore` command.
- A volume that contains SMB shares that are BranchCache-enabled is restored using the `snap restore` command.

Guidelines for choosing the hash store location

When configuring BranchCache, you choose where to store hashes and what size the hash store should be. Understanding the guidelines when choosing the hash store location and size can help you plan your BranchCache configuration on a CIFS-enabled SVM.

- You should locate the hash store on a volume where atime updates are permitted.

  The access time on a hash file is used to keep frequently accessed files in the hash store. If atime updates are disabled, the creation time is used for this purpose. It is preferable to use atime to track frequently used files.

- You cannot store hashes on read-only file systems such as SnapMirror destinations and SnapLock volumes.
- If the maximum size of the hash store is reached, older hashes are flushed to make room for new hashes.

  You can increase the maximum size of the hash store to reduce the amount of hashes that are flushed from the cache.

- If the volume on which you store hashes is unavailable or full, or if there is an issue with intra-cluster communication where the BranchCache service cannot retrieve hash information, BranchCache services are not available.

  The volume might be unavailable because it is offline or because the storage administrator specified a new location for the hash store.

  This does not cause issues with file access. If access to the hash store is impeded, ONTAP returns a Microsoft-defined error to the client, which causes the client to request the file using the normal SMB read request.

Related information

Configure BranchCache on the SMB server

Modify the BranchCache configuration

BranchCache recommendations

Before you configure BranchCache, there are certain recommendations you should keep in mind when deciding on which SMB shares you want to enable BranchCache caching.

You should keep the following recommendations in mind when deciding on which operating mode to use and on which SMB shares to enable BranchCache:

- The benefits of BranchCache are reduced when the data to be remotely cached changes frequently.
- BranchCache services are beneficial for shares containing file content that is reused by multiple remote office clients or by file content that is repeatedly accessed by a single remote user.
- Consider enabling caching for read-only content such as data in Snapshot copies and SnapMirror destinations.

Configure BranchCache

Configure BranchCache overview

You configure BranchCache on your SMB server using ONTAP commands. To implement BranchCache, you must also configure your clients, and optionally your hosted cache servers at the branch offices where you want to cache content.

If you configure BranchCache to enable caching on a share-by-share basis, you must enable BranchCache on the SMB shares for which you want to provide BranchCache caching services.

Requirements for configuring BranchCache

After meeting some prerequisites, you can set up BranchCache.

The following requirements must be met before configuring BranchCache on the CIFS server for your SVM:

- ONTAP must be installed on all nodes in the cluster.
- CIFS must be licensed and a CIFS server must be configured.
- IPv4 or IPv6 network connectivity must be configured.
- For BranchCache 1, SMB 2.1 or later must be enabled.
- For BranchCache 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

Configure BranchCache on the SMB server

You can configure BranchCache to provide BranchCache services on a per-share basis. Alternatively, you can configure BranchCache to automatically enable caching on all SMB shares.

About this task

You can configure BranchCache on SVMs.

- You can create an all-shares BranchCache configuration if want to offer caching services for all content contained within all SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for content contained within selected SMB shares on the CIFS server.

You must specify the following parameters when configuring BranchCache:

Required parameters	Description
SVM name	BranchCache is configured on a per SVM basis. You must specify on which CIFS-enabled SVM you want to configure the BranchCache service.
Path to hash store	BranchCache hashes are stored in regular files on the SVM volume. You must specify the path to an existing directory where you want ONTAP to store the hash data.The BranchCache hash path must be read-writable. Read-only paths, such as Snapshot directories are not allowed. You can store hash data in a volume that contains other data or you can create a separate volume to store hash data. If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination. The hash path can contain blanks and any valid file name characters.

You can optionally specify the following parameters:

Optional parameters	Description
Supported Versions	ONTAP support BranchCache 1 and 2. You can enable version 1, version 2, or both versions. The default is to enable both versions.
Maximum size of hash store	You can specify the size to use for the hash data store. If the hash data exceeds this value, ONTAP deletes older hashes to make room for newer hashes. The default size for the hash store is 1 GB. BranchCache performs more efficiently if hashes are not discarded in an overly aggressive manner. If you determine that hashes are discarded frequently because the hash store is full, you can increase the hash store size by modifying the BranchCache configuration.

Optional parameters	Description
Server key	You can specify a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you do not specify a server key, one is randomly generated when you create the BranchCache configuration. You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.
Operating mode	The default is to enable BranchCache on a per-share basis. • To create a BranchCache configuration where you enable BranchCache on a per-share basis, you can either not specify this optional parameter or you can specify `per-share`. • To automatically enable BranchCache on all shares, you must set the operating mode to `all-shares`.

Steps

1. Enable SMB 2.1 and 3.0 as needed:
   a. Set the privilege level to advanced: `set -privilege advanced`
   b. Check the configured SVM SMB settings to determine whether all needed versions of SMB are enabled: `vserver cifs options show -vserver vserver_name`
   c. If necessary, enable SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      The command enables both SMB 2.0 and SMB 2.1.

   d. If necessary, enable SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. Return to the admin privilege level: `set -privilege admin`
2. Configure BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   The specified hash storage path must exist and must reside on a volume managed by the SVM. The path must also be located on a read-writable volume. The command fails if the path is read-only or does not exist.

   If you want to use the same server key for additional SVM BranchCache configurations, record the value you enter for the server key. The server key does not appear when you display information about the BranchCache configuration.

3. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

Examples

The following commands verify that both SMB 2.1 and 3.0 are enabled and configure BranchCache to automatically enable caching on all SMB shares on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

The following commands verify that both SMB 2.1 and 3.0 are enabled, configure BranchCache to enable caching on a per-share basis on SVM vs1, and verify the BranchCache configuration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related information

Requirements and guidelines: BranchCache version support

Where to find information about configuring BranchCache at the remote office

Create a BranchCache-enabled SMB share

Enable BranchCache on an existing SMB share

Modify the BranchCache configuration

Disable BranchCache on SMB shares overview

Delete the BranchCache configuration on SVMs

Where to find information about configuring BranchCache at the remote office

After configuring BranchCache on the SMB server, you must install and configure BranchCache on client computers and, optionally, on caching servers at your remote office. Microsoft provides instructions for configuring BranchCache at the remote office.

Instructions for configuring branch office clients and, optionally, caching servers to use BranchCache are on

the Microsoft BranchCache web site.

Microsoft BranchCache Docs: What's New

Configure BranchCache-enabled SMB shares

Configure BranchCache-enabled SMB shares overview

After you configure BranchCache on the SMB server and at the branch office, you can enable BranchCache on SMB shares that contain content that you want to allow clients at branch offices to cache.

BranchCache caching can be enabled on all SMB shares on the SMB server or on a share-by-share basis.

- If you enable BranchCache on a share-by-share basis, you can enable BranchCache as you create the share or by modifying existing shares.

  If you enable caching on an existing SMB share, ONTAP begins computing hashes and sending metadata to clients requesting content as soon as you enable BranchCache on that share.

- Any clients that have an existing SMB connection to a share do not get BranchCache support if BranchCache is subsequently enabled on that share.

  ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.

> If BranchCache on a SMB share is subsequently disabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (SMB server).

Create a BranchCache-enabled SMB share

You can enable BranchCache on an SMB share when you create the share by setting the `branchcache` share property.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.

  This is the default setting when you create a share.

- You can also specify additional optional share parameters when you create the BranchCache-enabled share.
- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- Since there are no default share properties applied to the share when you use the `-share-properties` parameter, you must specify all other share properties that you want applied to the share in addition to the

`branchcache` share property by using a comma-delimited list.

- For more information, see the man page for the `vserver cifs share create` command.

Step

1. Create a BranchCache-enabled SMB share:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Verify that the BranchCache share property is set on the SMB share by using the `vserver cifs share show` command.

Example

The following command creates a BranchCache-enabled SMB share named “data” with a path of `/data` on SVM vs1. By default, the offline files setting is set to `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Related information

Disabling BranchCache on a single SMB share

Enable BranchCache on an existing SMB share

You can enable BranchCache on an existing SMB share by adding the `branchcache` share property to the existing list of share properties.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to

manual caching.

If the existing share's offline files setting is not set to manual caching, you must configure it by modifying the share.

- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- When you add the `branchcache` share property to the share, existing share settings and share properties are preserved.

  The BranchCache share property is added to the existing list of share properties. For more information about using the `vserver cifs share properties add` command, see the man pages.

Steps

1. If necessary, configure the offline files share setting for manual caching:
   a. Determine what the offline files share setting is by using the `vserver cifs share show` command.
   b. If the offline files share setting is not set to manual, change it to the required value: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Enable BranchCache on an existing SMB share: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verify that the BranchCache share property is set on the SMB share: `vserver cifs share show -vserver vserver_name -share-name share_name`

Example

The following command enables BranchCache on an existing SMB share named "data2" with a path of `/data2` on SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Related information

Adding or removing share properties on an existing SMB share

Disabling BranchCache on a single SMB share

Manage and monitor the BranchCache configuration

Modify BranchCache configurations

You can modify the configuration of the BranchCache service on SVMs, including changing the hash store directory path, the hash store maximum directory size, the operating mode, and which BranchCache versions are supported. You can also increase the size of the volume that contains the hash store.

Steps

1. Perform the appropriate action:

If you want to…	Enter the following…
Modify the hash store directory size	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB|MB|GB|TB|PB]}`
Increase the size of the volume that contains the hash store	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k|m|g|t]` If the volume containing the hash store fills up, you might be able to increase the size of the volume. You can specify the new volume size as a number followed by a unit designation. Learn more about managing FlexVol volumes

If you want to…	Enter the following…
Modify the hash store directory path	`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true|false}` If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination. The BranchCache hash path can contain blanks and any valid file name characters. If you modify the hash path, `-flush-hashes` is a required parameter that specifies whether you want ONTAP to flush the hashes from the original hash store location. You can set the following values for the `-flush-hashes` parameter: • If you specify `true`, ONTAP deletes the hashes in the original location and creates new hashes in the new location as new requests are made by BranchCache-enabled clients. • If you specify `false`, the hashes are not flushed. In this case, you can choose to reuse the existing hashes later by changing the hash store path back to the original location.
Change the operating mode	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share|all-shares|disable}` You should be aware of the following when modifying the operating mode: • ONTAP advertises BranchCache support for a share when the SMB session is set up. • Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.
Change the BranchCache version support	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable|v2-enable|enable-all}`

2. Verify the configuration changes by using the `vserver cifs branchcache show` command.

Display information about BranchCache configurations

You can display information about BranchCache configurations on storage virtual machines (SVMs), which can be used when verifying a configuration or when determining current settings before modifying a configuration.

Step

1. Perform one of the following actions:

If you want to display…	Enter this command…
Summary information about BranchCache configurations on all SVMs	`vserver cifs branchcache show`
Detailed information about the configuration on a specific SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Example

The following example displays information about the BranchCache configuration on SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Change the BranchCache server key

You can change the BranchCache server key by modifying the BranchCache configuration on the storage virtual machine (SVM) and specifying a different server key.

About this task

You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key.

When you change the server key, you must also flush the hash cache. After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Steps

1. Change the server key by using the following command: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   When configuring a new server key, you must also specify `-flush-hashes` and set the value to `true`.

2. Verify that the BranchCache configuration is correct by using the `vserver cifs branchcache show` command.

Example

The following example sets a new server key that contains spaces and flushes the hash cache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related information

Reasons ONTAP invalidates BranchCache hashes

Pre-compute BranchCache hashes on specified paths

You can configure the BranchCache service to pre-compute hashes for a single file, for a directory, or for all files in a directory structure. This can be helpful if you want to compute hashes on data in a BranchCache-enabled share during off, non-peak hours.

About this task

If you want to collect a data sample before you display hash statistics, you must use the `statistics start` and optional `statistics stop` commands.

- You must specify the storage virtual machine (SVM) and path on which you want to pre-compute hashes.
- You must also specify whether you want hashes computed recursively.
- If you want hashes computed recursively, the BranchCache service traverses the entire directory tree under the specified path, and computes hashes for each eligible object.

Steps

1. Pre-compute hashes as desired:

If you want to pre-compute hashes on…	Enter the command…
A single file or directory	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`

If you want to pre-compute hashes on…	Enter the command…
Recursively on all files in a directory structure	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verify that hashes are being computed by using the `statistics` command:
   a. Display statistics for the `hashd` object on the desired SVM instance: `statistics show -object hashd -instance vserver_name`
   b. Verify that the number of hashes created is increasing by repeating the command.

Examples

The following example creates hashes on the path `/data` and on all contained files and subdirectories on SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Related information

Performance monitoring setup

Flush hashes from the SVM BranchCache hash store

You can flush all cached hashes from the BranchCache hash store on the storage virtual machine (SVM). This can be useful if you have changed the branch office BranchCache configuration. For example, if you recently reconfigured the caching mode from distributed caching to hosted caching mode, you would want to flush the hash store.

About this task

After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Step

1. Flush the hashes from the BranchCache hash store: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Display BranchCache statistics

You can display BranchCache statistics to, among other things, identify how well caching is performing, determine whether your configuration is providing cached content to clients, and determine whether hash files were deleted to make room for more recent hash data.

About this task

The `hashd` statistic object contains counters that provide statistical information about BranchCache hashes. The `cifs` statistic object contains counters that provide statistical information about BranchCache-related activity. You can collect and display information about these objects at the advanced-privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Display the BranchCache-related counters by using the `statistics catalog counter show` command.

   For more information about statistics counters, see the man page for this command.

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
       Counter                     Description
   ```

```
    --------------------------
-------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
```

```
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
    ....Output truncated....
```

3. Collect BranchCache-related statistics by using the `statistics start` and `statistics stop` commands.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. Display the collected BranchCache statistics by using the `statistics show` command.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. Return to the admin privilege level: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Related information

Displaying statistics

Performance monitoring setup

Support for BranchCache Group Policy Objects

ONTAP BranchCache provides support for BranchCache Group Policy Objects (GPOs),

which allow centralized management for certain BranchCache configuration parameters. There are two GPOs used for BranchCache, the Hash Publication for BranchCache GPO and the Hash Version Support for BranchCache GPO.

- **Hash Publication for BranchCache GPO**

  The Hash Publication for BranchCache GPO corresponds to the `-operating-mode` parameter. When GPO updates occur, this value is applied to storage virtual machine (SVM) objects contained within the organizational unit (OU) to which the group policy applies.

- **Hash Version Support for BranchCache GPO**

  The Hash Version Support for BranchCache GPO corresponds to the `-versions` parameter. When GPO updates occur, this value is applied to SVM objects contained within the organizational unit to which the group policy applies.

Related information

Applying Group Policy Objects to CIFS servers

Display information about BranchCache Group Policy Objects

You can display information about the CIFS server's Group Policy Object (GPO) configuration to determine whether BranchCache GPOs are defined for the domain to which the CIFS server belongs and, if so, what the allowed settings are. You can also determine whether BranchCache GPO settings are applied to the CIFS server.

About this task

Even though a GPO setting is defined within the domain to which the CIFS server belongs, it is not necessarily applied to the organizational unit (OU) containing the CIFS-enabled storage virtual machine (SVM). Applied GPO setting are the subset of all defined GPOs that are applied to the CIFS-enabled SVM. BranchCache settings applied through GPOs override settings applied through the CLI.

Steps

1. Display the defined BranchCache GPO setting for the Active Directory domain by using the `vserver cifs group-policy show-defined` command.

   This example does not display all of the available output fields for the command. Output is truncated.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Display the BranchCache GPO setting applied to the CIFS server by using the `vserver cifs group-policy show-applied` command. ``

> This example does not display all of the available output fields for the command. Output is truncated.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Related information

Enabling or disabling GPO support on a CIFS server

Disable BranchCache on SMB shares

Disable BranchCache on SMB shares overview

If you do not want to provide BranchCache caching services on certain SMB shares but you might want to provide caching services on those shares later, you can disable BranchCache on a share-by-share basis. If you have BranchCache configured to offer caching on all shares but you want to temporarily disable all caching services, you can modify the BranchCache configuration to stop automatic caching on all shares.

If BranchCache on an SMB share is subsequently disabled after first being enabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server on the storage virtual machine (SVM)).

Related information

Configuring BranchCache-enabled SMB shares

Disable BranchCache on a single SMB share

If you do not want to offer caching services on certain shares that previously offered cached content, you can disable BranchCache on an existing SMB share.

Step

1. Enter the following command: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   The BranchCache share property is removed. Other applied share properties remain in effect.

Example

The following command disables BranchCache on an existing SMB share named “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Stop automatic caching on all SMB shares

If your BranchCache configuration automatically enables caching on all SMB shares on each storage virtual machine (SVM), you can modify the BranchCache configuration to stop automatically caching content for all SMB shares.

About this task

To stop automatic caching on all SMB shares, you change the BranchCache operating mode to per-share caching.

Steps

1. Configure BranchCache to stop automatic caching on all SMB shares: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

Example

The following command changes the BranchCache configuration on storage virtual machine (SVM, formerly known as Vserver) vs1 to stop automatic caching on all SMB shares:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Disable or enable BranchCache on the SVM

What happens when you disable or reenable BranchCache on the CIFS server

If you previously configured BranchCache but do not want the branch office clients to use cached content, you can disable caching on the CIFS server. You must be aware of what happens when you disable BranchCache.

When you disable BranchCache, ONTAP no longer computes hashes or sends the metadata to the requesting client. However, there is no interruption to file access. Thereafter, when BranchCache-enabled clients request metadata information for content they want to access, ONTAP responds with a Microsoft-defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the storage virtual machine (SVM).

After BranchCache is disabled on the CIFS server, SMB shares do not advertise BranchCache capabilities. To access data on new SMB connections, clients make normal read SMB requests.

You can reenable BranchCache on the CIFS server at any time.

- Because the hash store is not deleted when you disable BranchCache, ONTAP can use the stored hashes when replying to hash requests after you reenable BranchCache, provided that the requested hash is still valid.
- Any clients that have made SMB connections to BranchCache-enabled shares during the time when BranchCache was disabled do not get BranchCache support if BranchCache is subsequently reenabled.

  This is because ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that established sessions to BranchCache-enabled shares while BranchCache was disabled need to disconnect and reconnect to use cached content for this share.

If you do not want to save the hash store after you disable BranchCache on a CIFS server, you can manually delete it. If you reenable BranchCache, you must ensure that the hash store directory exists. After BranchCache is reenabled, BranchCache-enabled shares advertise BranchCache capabilities. ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Disable or enable BranchCache

You can disable BranchCache on the storage virtual machine (SVM) by changing the BranchCache operating mode to `disabled`. You can enable BranchCache at any time by changing the operating mode to either offer BranchCache services per-share or automatically for all shares.

Steps

1. Run the appropriate command:

If you want to…	Then enter the following…
Disable BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Enable BranchCache per share	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Enable BranchCache for all shares	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Verify that the BranchCache operating mode is configured with the desired setting: `vserver cifs branchcache show -vserver vserver_name`

Example

The following example disables BranchCache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Delete the BranchCache configuration on SVMs

What happens when you delete the BranchCache configuration

If you previously configured BranchCache but do not want the storage virtual machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

Delete the BranchCache configuration

The command you use for deleting the BranchCache service on your storage virtual machine (SVM) differs depending on whether you want to delete or keep existing hashes.

Step

1. Run the appropriate command:

If you want to…	Then enter the following…
Delete the BranchCache configuration and delete existing hashes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`

If you want to…	Then enter the following…
Delete the BranchCache configuration but keep existing hashes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Example

The following example deletes the BranchCache configuration on SVM vs1 and deletes all existing hashes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

What happens to BranchCache when reverting

It is important to understand what happens when you revert ONTAP to a release that does not support BranchCache.

- When you revert to a version of ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information.

  Instead, they request the actual content using normal SMB read requests. In response to the request for content, the SMB server sends the actual content that is stored on the storage virtual machine (SVM).

- When a node hosting a hash store is reverted to a release that does not support BranchCache, the storage administrator needs to manually revert the BranchCache configuration using a command that is printed out during the revert.

  This command deletes the BranchCache configuration and hashes.

  After the revert completes, the storage administrator can manually delete the directory that contained the hash store if desired.

Related information

Deleting the BranchCache configuration on SVMs

Improve Microsoft remote copy performance

Improve Microsoft remote copy performance overview

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer.

ONTAP supports ODX for both the SMB and SAN protocols. The source can be either a CIFS server or LUN, and the destination can be either a CIFS server or LUN.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination. In summary, the

client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

For SMB environments, this functionality is only available when both the client and the storage server support SMB 3.0 and the ODX feature. For SAN environments, this functionality is only available when both the client and the storage server support the ODX feature. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used irrespective of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

Related information

Improving client response time by providing SMB automatic node referrals with Auto Location

SMB configuration for Microsoft Hyper-V and SQL Server

How ODX works

ODX copy offload uses a token-based mechanism for reading and writing data within or between ODX-enabled CIFS servers. Instead of routing the data through the host, the CIFS server sends a small token, which represents the data, to the client. The ODX client presents that token to the destination server, which then can transfer the data represented by that token from the source to the destination.

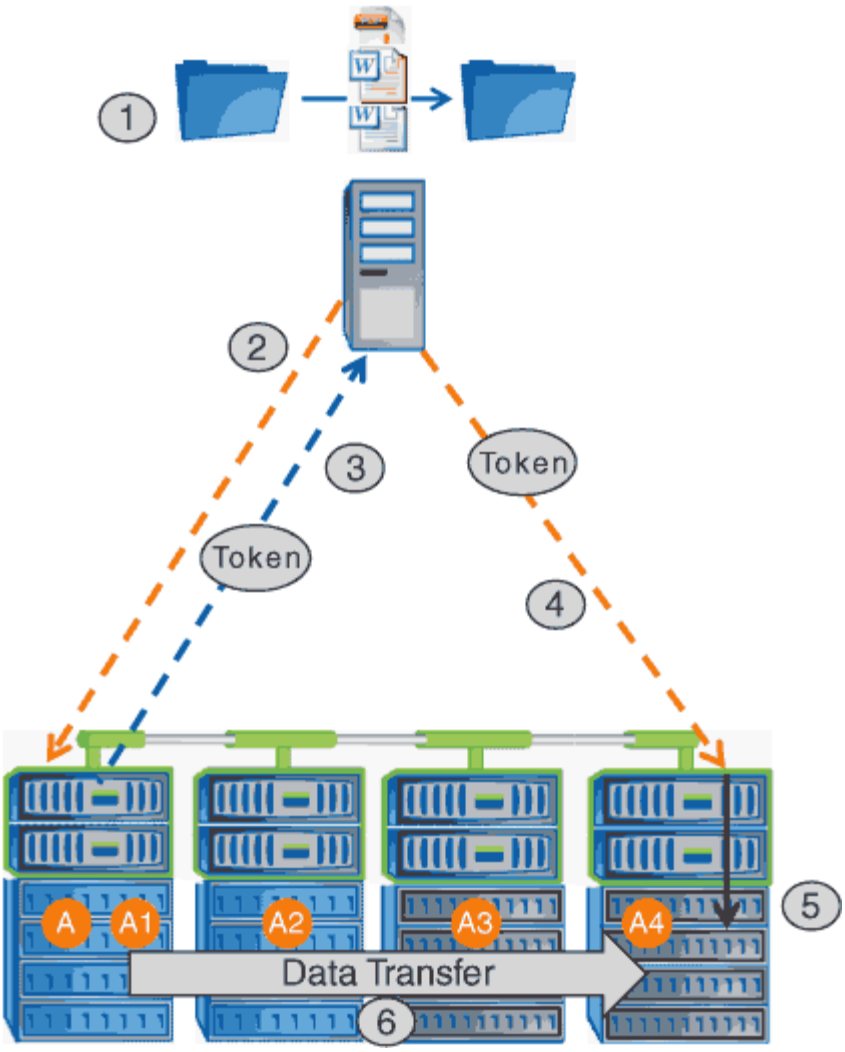
When an ODX client learns that the CIFS server is ODX-capable, it opens the source file and requests a token from the CIFS server. After opening the destination file, the client uses the token to instruct the server to copy the data directly from the source to the destination.

> The source and destination can be on the same storage virtual machine (SVM) or on different SVMs, depending on the scope of the copy operation.

The token serves as a point-in-time representation of the data. As an example, when you copy data between storage locations, a token representing a data segment is returned to the requesting client, which the client copies to the destination, thereby removing the need to copy the underlying data through the client.

ONTAP supports tokens that represent 8 MB of data. ODX copies of greater than 8 MB are performed by using multiple tokens, with each token representing 8 MB of data.

The following figure explains the steps that are involved with an ODX copy operation:



1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.
2. The ODX-capable client automatically translates this transfer request into an ODX request.

   The ODX request that is sent to the CIFS server contains a request for a token.
3. If ODX is enabled on the CIFS server and the connection is over SMB 3.0, the CIFS server generates a token, which is a logical representation of the data on the source.
4. The client receives a token that represents the data and sends it with the write request to the destination CIFS server.

   This is the only data that is copied over the network from the source to the client and then from the client to the destination.
5. The token is delivered to the storage subsystem.
6. The SVM internally performs the copy or move.

   If the file that is copied or moved is larger than 8 MB, multiple tokens are needed to perform the copy. Steps 2 through 6 as performed as needed to complete the copy.

If there is a failure with the ODX offloaded copy, the copy or move operation falls back to traditional reads and writes for the copy or move operation. Similarly, if the destination CIFS server does not support ODX or ODX is disabled, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

Requirements for using ODX

Before you can use ODX for copy offloads with your storage virtual machine (SVM), you need to be aware of certain requirements.

ONTAP version requirements

ONTAP releases support ODX for copy offloads.

SMB version requirements

- ONTAP supports ODX with SMB 3.0 and later.
- SMB 3.0 must be enabled on the CIFS server before ODX can be enabled:
  - Enabling ODX also enables SMB 3.0, if it is not already enabled.
  - Disabling SMB 3.0 also disables ODX.

Windows server and client requirements

Before you can use ODX for copy offloads, the Windows client must support the feature. Support for ODX starts with Windows 2012 Server and Windows 8.

The Interoperability Matrix contains the latest information about supported Windows clients.

NetApp Interoperability Matrix Tool

Volume requirements

- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

  Secondary compression type is not supported.

Guidelines for using ODX

Before you can use ODX for copy offload, you need to be aware of the guidelines. For example, you need to know on which types of volumes you can use ODX and you need to understand the intra-cluster and inter-cluster ODX considerations.

Volume guidelines

- You cannot use ODX for copy offload with the following volume configurations:
  - Source volume size is less than 1.25 GB

The volume size must be 1.25 GB or larger to use ODX.

- Read-only volumes

  ODX is not used for files and folders residing in load-sharing mirrors or in SnapMirror or SnapVault destination volumes.

- If the source volume is not deduplicated

- ODX copies are supported only for intra-cluster copies.

  You cannot use ODX to copy files or folders to a volume in another cluster.

Other guidelines

- In SMB environments, to use ODX for copy offload, the files must be 256 kb or larger.

  Smaller files are transferred using a traditional copy operation.

- ODX copy offload uses deduplication as part of the copy process.

  If you do not want deduplication to occur on SVM volumes when copying or moving data, you should disable ODX copy offload on that SVM.

- The application that performs the data transfer must be written to support ODX.

  Application operations that support ODX include the following:

  - Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing Snapshot copies, and copying files between virtual machines
  - Windows Explorer operations
  - Windows PowerShell copy commands
  - Windows command prompt copy commands

    Robocopy at the Windows command prompt supports ODX.

    The applications must be running on Windows servers or clients that support ODX.

    For more information about supported ODX applications on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Use cases for ODX

You should be aware of the use cases for using ODX on SVMs so that you can determine under what circumstances ODX provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same SVM

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

- Inter-cluster

  The source and destination LUNs are on different volumes that are located on different nodes across clusters. This is only supported for SAN and does not work for CIFS.

There are some additional special use cases:

- With the ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

  You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided that the SMB shares and LUNs are on the same cluster.

- Hyper-V provides some additional use cases for ODX copy offload:

  - You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

    This allows copies from guest operating systems to pass through to the underlying storage.

  - When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
  - ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Enable or disable ODX

You can enable or disable ODX on storage virtual machines (SVMs). The default is to enable support for ODX copy offload if SMB 3.0 is also enabled.

Before you begin

SMB 3.0 must be enabled.

About this task

If you disable SMB 3.0, ONTAP also disables SMB ODX. If you reenable SMB 3.0, you must manually reenable SMB ODX.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want ODX copy offload to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables ODX copy offload on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Related information

Available SMB server options

Improve client response time by providing SMB automatic node referrals with Auto Location

Improve client response time by providing SMB automatic node referrals with Auto Location overview

Auto Location uses SMB automatic node referrals to increase SMB client performance on storage virtual machines (SVMs). Automatic node referrals automatically redirect the requesting client to a LIF on the node SVM that is hosting the volume in which the data resides, which can lead to improved client response times.

When an SMB client connects to an SMB share hosted on the SVM, it might connect using a LIF that is on a node that does not own the requested data. The node to which the client is connected accesses data owned by another node by using the cluster network. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data:

- ONTAP provides this functionality by using Microsoft DFS referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else.

  A node makes a referral when it determines that there is anSVM LIF on the node containing the data.

- Automatic node referrals are supported for IPv4 and IPv6 LIF IP addresses.
- Referrals are made based on the location of the root of the share through which the client is connected.
- The referral occurs during SMB negotiation.

  The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

> If a share spans multiple junction points and some of the junctions are to volumes contained on other nodes, data within the share is spread across multiple nodes. Because ONTAP provides referrals that are local to the root of the share, ONTAP must use the cluster network to retrieve the data contained within these non-local volumes. With this type of namespace architecture, automatic node referrals might not provide significant performance benefits.

If the node hosting the data does not have an available LIF, ONTAP establishes the connection using the LIF chosen by the client. After a file is opened by an SMB client, it continues to access the file through the same referred connection.

If, for any reason, the CIFS server cannot make a referral, there is no disruption to SMB service. The SMB connection is established as if automatic node referrals were not enabled.

Related information

Improving Microsoft remote copy performance

Requirements and guidelines for using automatic node referrals

Before you can use SMB automatic node referrals, also known as *autolocation*, you need to be aware of certain requirements, including which versions of ONTAP support the feature. You also need to know about supported SMB protocol versions and certain other

special guidelines.

ONTAP version and license requirements

- All nodes in the cluster must be running a version of ONTAP that supports automatic node referrals.
- Widelinks must be enabled on a SMB share to use autolocation.
- CIFS must be licensed, and an SMB server must exist on the SVMs.

SMB protocol version requirements

- For SVMs, ONTAP supports automatic node referrals on all versions of SMB.

SMB client requirements

All Microsoft clients supported by ONTAP support SMB automatic node referrals.

The Interoperability Matrix contains the latest information about which Windows clients ONTAP supports.

NetApp Interoperability Matrix Tool

Data LIF requirements

If you want to use a data LIF as a potential referral for SMB clients, you must create data LIFs with both NFS and CIFS enabled.

Automatic node referrals can fail to work if the target node contains data LIFs that are enabled only for the NFS protocol, or enabled only for the SMB protocol.

If this requirement is not met, data access is not affected. The SMB client maps the share using the original LIF that the client used to connect to the SVM.

NTLM authentication requirements when making a referred SMB connection

NTLM authentication must be allowed on the domain containing the CIFS server and on the domains containing clients that want to use automatic node referrals.

When making a referral, the SMB server refers an IP address to the Windows client. Because NTLM authentication is used when making a connection using an IP address, Kerberos authentication is not performed for referred connections.

This happens because the Windows client cannot craft the service principal name used by Kerberos (which is of the form `service/NetBIOS name` and `service/FQDN`), which means that the client cannot request a Kerberos ticket to the service.

Guidelines for using automatic node referrals with the home directory feature

When shares are configured with the home directory share property enabled, there can be one or more home directory search paths configured for a home directory configuration. The search paths can point to volumes contained on each node containing SVM volumes. Clients receive a referral and, if an active, local data LIF is available, connect through a referred LIF that is local to the home user's home directory.

There are guidelines when SMB 1.0 clients access dynamic home directories with automatic node referrals enabled. This is because SMB 1.0 clients require the automatic node referral before they have authenticated, which is before the SMB server has the user's name. However, SMB home directory access works correctly for

SMB 1.0 clients if the following statements are true:

- SMB home directories are configured to use simple names, such as “%w” (Windows user name) or “%u” (mapped UNIX user name), and not domain-name style names, such as "`%d\%w `" (domain-name\user-name).
- When creating home directory shares, the CIFS home directory shares names are configured with variables (“%w” or “%u”), and not with static names, such as “HOME”.

For SMB 2.x and SMB 3.0 clients, there are no special guidelines when accessing home directories using automatic node referrals.

Guidelines for disabling automatic node referrals on CIFS servers with existing referred connections

If you disable automatic node referrals after the option has been enabled, clients currently connected to a referred LIF keep the referred connection. Because ONTAP uses DFS referrals as the mechanism for SMB automatic node referrals, clients can even reconnect to the referred LIF after you disable the option until the client’s cached DFS referral for the referred connection times out. This is true even in the case of a revert to a version of ONTAP that does not support automatic node referrals. Clients continue to use referrals until the DFS referral times out from the client’s cache.

Autolocation uses SMB automatic node referrals to increase SMB client performance by referring clients to the LIF on the node that owns the data volume of an SVM. When an SMB client connects to an SMB share hosted on an SVM, it might connect using a LIF on a node that does not own the requested data and uses cluster interconnect network to retrieve data. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data.

ONTAP provides this functionality by using Microsoft Distributed File System (DFS) referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else. A node makes a referral when it determines that there is an SVM LIF on the node containing the data. Referrals are made based on the location of the root of the share through which the client is connected.

The referral occurs during SMB negotiation. The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

Guidelines for using automatic node referrals with Mac OS clients

Mac OS X clients do not support SMB automatic node referrals, even though the Mac OS supports Microsoft’s Distributed File System (DFS). Windows clients make a DFS referral request before connecting to an SMB share. ONTAP provides a referral to a data LIF found on the same node that hosts the requested data, which leads to improved client response times. Although the Mac OS supports DFS, Mac OS clients do not behave exactly like Windows clients in this area.

Related information

How ONTAP enables dynamic home directories

Network management

NetApp Interoperability Matrix Tool

Support for SMB automatic node referrals

Before you enable SMB automatic node referrals, you should be aware that certain

ONTAP functionality does not support referrals.

- The following types of volumes do not support SMB automatic node referrals:
  - Read-only members of a load-sharing mirror
  - Destination volume of a data-protection mirror
- Node referrals do not move alongside a LIF move.

  If a client is using a referred connection over an SMB 2.x or SMB 3.0 connection and a data LIF moves nondisruptively, the client continues to use the same referred connection, even if the LIF is no longer local to the data.

- Node referrals do not move alongside a volume move.

  If a client is using a referred connection over any SMB connection and a volume move occurs, the client continues to use the same referred connection, even if the volume is no longer located on the same node as the data LIF.

Enable or disable SMB automatic node referrals

You can enable SMB automatic node referrals to increase SMB client access performance. You can disable automatic node referrals if you do not want ONTAP to make referrals to SMB clients.

Before you begin

A CIFS server must be configured and running on the storage virtual machine (SVM).

About this task

The SMB automatic node referrals functionality is disabled by default. You can enable or disable this functionality on each SVM as required.

This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable SMB automatic node referrals as required:

If you want SMB automatic node referrals to be…	Enter the following command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   The option setting takes effect for new SMB sessions. Clients with existing connection can utilize node referral only when their existing cache timeout expires.

3. Switch to the admin privilege level: `set -privilege admin`

Related information

Available SMB server options

Use statistics to monitor automatic node referral activity

To determine how many SMB connections are referred, you can monitor automatic node referral activity by using the `statistics` command. By monitoring referrals you can determine the extent to which automatic referrals are locating connections on nodes that host the shares and whether you should redistribute your data LIFs to provide better local access to shares on the CIFS server.

About this task

The `cifs` object provides several counters at the advanced privilege level that are helpful when monitoring SMB automatic node referrals:

- `node_referral_issued`

  Number of clients that have been issued a referral to the share root's node after the client connected using a LIF hosted by a node different from the share root's node.

- `node_referral_local`

  Number of clients that connected using a LIF hosted by the same node that hosts the share root. Local access generally provides optimal performance.

- `node_referral_not_possible`

  Number of clients that have not been issued a referral to the node hosting the share root after connecting using a LIF hosted by a node different from the share root's node. This is because an active data LIF for the share root's node was not found.

- `node_referral_remote`

  Number of clients that connected using a LIF hosted by a node different from the node that hosts the share root. Remote access might result in degraded performance.

You can monitor automatic node referral statistics on your storage virtual machine (SVM) by collecting and viewing data for a specific time period (a sample). You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

To evaluate and use the information you gather from the `statistics` command, you should understand the distribution of clients in your environments.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. View automatic node referral statistics by using the `statistics` command.

This example views automatic node referral statistics by collecting and viewing data for a sampled time period:

a. Start the collection: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Wait for the desired collection time to elapse.

c. Stop the collection: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

d. View the automatic node referral statistics: `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                 Value
    ------------------------------ ----------------------------
    node_name                                               node1
    node_referral_issued                                        0
    node_referral_local                                         1
    node_referral_not_possible                                  2
    node_referral_remote                                        2
    ...

    node_name                                               node2
    node_referral_issued                                        2
    node_referral_local                                         1
    node_referral_not_possible                                  0
    node_referral_remote                                        2
    ...
```

Output displays counters for all nodes participating in SVM vs1. For clarity, only output fields related to automatic node referral statistics are provided in the example.

3. Return to the admin privilege level: `set -privilege admin`

Related information

Displaying statistics

Performance monitoring setup

Monitor client-side SMB automatic node referral information using a Windows client

To determine what referrals are made from the client's perspective, you can use the Windows `dfsutil.exe` utility.

The Remote Server Administration Tools (RSAT) kit available with Windows 7 and later clients contains the `dfsutil.exe` utility. Using this utility, you can display information about the contents of the referral cache as well as view information about each referral that the client is currently using. You can also use the utility to clear the client's referral cache. For more information, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Provide folder security on shares with access-based enumeration

Provide folder security on shares with access-based enumeration overview

When access-based enumeration (ABE) is enabled on an SMB share, users who do not have permission to access a folder or file contained within the share (whether through individual or group permission restrictions) do not see that shared resource displayed in their environment, although the share itself remains visible.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify files or folders contained within the share. However, they do not allow you to control whether folders or files within the share are visible to users who do not have permission to access them. This could pose problems if the names of these folders or files within the share describe sensitive information, such as the names of customers or products under development.

Access-based enumeration (ABE) extends share properties to include the enumeration of files and folders within the share. ABE therefore enables you to filter the display of files and folders within the share based on user access rights. That is, the share itself would be visible to all users, but files and folders within the share could be displayed to or hidden from designated users. In addition to protecting sensitive information in your workplace, ABE enables you to simplify the display of large directory structures for the benefit of users who do not need access to your full range of content. For example, the share itself would be visible to all users, but files and folders within the share could be displayed or hidden.

Learn about Performance impact when using SMB/CIFS Access Based Enumeration.

Enable or disable access-based enumeration on SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares to allow or prevent users from seeing shared resources that they do not have permission to access.

About this task

By default, ABE is disabled.

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable ABE on a new share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` You can specify additional optional share settings and additional share properties when you create an SMB share. For more information, see the man page for the `vserver cifs share create` command.
Enable ABE on an existing share	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Existing share properties are preserved. The ABE share property is added to the existing list of share properties.
Disable ABE on an existing share	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Other share properties are preserved. Only the ABE share property is removed from the list of share properties.

2. Verify that the share configuration is correct by using the `vserver cifs share show` command.

Examples

The following example creates an ABE SMB share named “sales” with a path of `/sales` on SVM vs1. The share is created with `access-based-enumeration` as a share property:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example adds the `access-based-enumeration` share property to an SMB share named "data2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ---------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Related information

Adding or removing share properties on an existing SMB share

Enable or disable access-based enumeration from a Windows client

You can enable or disable access-based enumeration (ABE) on SMB shares from a Windows client, which allows you to configure this share setting without needing to connect to the CIFS server.

The `abecmd` utility is not available in new versions of Windows Server and Windows clients. It was released as part of Windows Server 2008. Support ended for Windows Server 2008 on January 14, 2020.

Steps

1. From a Windows client that supports ABE, enter the following command: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   For more information about the `abecmd` command, see your Windows client documentation.

NFS and SMB file and directory naming dependencies

NFS and SMB file and directory naming dependencies overview

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and qtree names, depending on the ONTAP release.

Characters a file or directory name can use

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

Case-sensitivity of file and directory names in a multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.

- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
  - On SMB clients, you see `testdir` and `TESTDI~1`.
  - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

    In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `text.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
  - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
  - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.

If you have enabled or modified character mapping using the Vserver CIFS character-mapping commands, a normally case-insensitive Windows lookup becomes case-sensitive.

How ONTAP creates file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

  If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.
- In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

How ONTAP handles multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary

characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

- You must create a new volume in one of the following ways:
- Setting the volume `-language` option explicitly: `volume create -language utf8mb4 {…}`
- Inheriting the volume `-language` option from an SVM that has been created with or modified for the option: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- You cannot modify existing volumes for utf8mb4 support; you must create a new utf8mb4-ready volume, and then migrate the data using client-based copy tools.

  You can update SVMs for utf8mb4 support, but existing volumes retain their original language codes.

  LUN names with 4-byte UTF-8 characters are not currently supported.

- Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

  In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

- When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

  To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Beginning with ONTAP 9, Unicode characters are allowed in qtree names.

- You can use either the `volume qtree` command family or System Manager to set or modify qtree names.
- qtree names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.

  In releases before ONTAP 9.5, the junction-path of the qtree's parent volume can contain qtree and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in qtree names, provided that the qtree is in a volume enabled for utf8mb4.

Configure character mapping for SMB file name translation on volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

  You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

  For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named "a-b" would have its request mapped to the NFS name of "a:b" (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.
- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

Step

1. Configure character mapping: +

`vserver cifs character-mapping create -vserver vserver_name -volume volume_name -mapping mapping_text, … +`

The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C. +

The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

- Source mapping +

The following table shows the permissible Unicode character set for source mapping:

+

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C		Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark
0x3C	<	Less than
0x3E	>	Greater than
0x7C	|	Vertical line
0xB1	±	Plus-minus sign

- Target mapping

  You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000… U+F8FF.

Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Related information

Creating and managing data volumes in NAS namespaces

Commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to…	Use this command…
Create new file character mappings	`vserver cifs character-mapping create`
Display information about file character mappings	`vserver cifs character-mapping show`
Modify existing file character mappings	`vserver cifs character-mapping modify`
Delete file character mappings	`vserver cifs character-mapping delete`

For more information, see the man page for each command.

Related information

Configuring character mapping for SMB file name translation on volumes

Provide S3 client access to NAS data

S3 multiprotocol overview

Beginning with ONTAP 9.12.1, you can enable clients running the S3 protocol to access the same data that are being served to clients that use the NFS and SMB protocols without reformatting. This capability allows NAS data to continue to be served to NAS clients, while presenting object data to S3 clients running S3 applications (such as data mining and artificial intelligence).

S3 multiprotocol functionality addresses two use cases:

1. Access to existing NAS data using S3 clients

If your existing data was created using traditional NAS clients (NFS or SMB) and is located on NAS volumes (FlexVol or FlexGroup volumes), you can now use analytical tools on S3 clients to access this data.

2. Backend storage for modern clients capable of performing I/O using both NAS and S3 protocols

   You can now provide integrated access for applications such Spark and Kafka that can read and write the same data using both NAS and S3 protocols.

How S3 multiprotocol works

ONTAP multiprotocol allows you to present the same data set as a file hierarchy or as objects in a bucket. To do so, ONTAP creates “S3 NAS buckets” that allow S3 clients to create, read, delete, and enumerate files in NAS storage using S3 object requests. This mapping conforms to the NAS security configuration, observing file and directory access permissions as well as writing to the security audit trail as necessary.

This mapping is accomplished by presenting a specified NAS directory hierarchy as an S3 bucket. Each file in the directory hierarchy is represented as an S3 object whose name is relative from the mapped directory downwards, with directory boundaries represented by the slash character ('/').

Normal ONTAP-defined S3 users can access this storage, as governed by the bucket policies defined for the bucket that maps to the NAS directory. For this to be possible, mappings must be defined between the S3 users and SMB/NFS users. The credentials of the SMB/NFS uses will be used for the NAS permissions checking and included in any audit records resulting from these accesses.

When created by SMB or NFS clients, a file is immediately placed in a directory, and therefore visible to clients, before any data is written to it. S3 clients expect different semantics, in which the new object is not visible in the namespace until all its data has been written. This mapping of S3 to NAS storage creates files using S3 semantics, keeping the files invisible externally until the S3 creation command completes.

Data protection for S3 NAS buckets

S3 NAS “buckets” are simply mappings of NAS data for S3 clients, they are not standard S3 buckets. Therefore, there is no need to protect S3 NAS buckets using NetApp S3 SnapMirror functionality. Instead, you can replicate source SVMs containing S3 NAS buckets using a standard SnapMirror data protection relationship with destination SVMs.

Learn about SnapMirror SVM replication.

Auditing for S3 NAS buckets

Because S3 NAS buckets are not conventional S3 buckets, S3 audit cannot be configured to audit access on them. Learn more about S3 audit.

Nonetheless, the NAS files and directories that are mapped in S3 NAS buckets can be audited for access events using conventional ONTAP audit procedures. S3 operations can therefore trigger NAS audit events, with the following exceptions:

- If S3 client access is denied by the S3 policy configuration (group or bucket policy), NAS audit for the event is not initiated. This is because S3 permissions are checked before SVM audit checks can be made.
- If the target file of an S3 Get request is 0 size, 0 content is returned to the Get request and the Read access is not logged.
- If the target file of an S3 Get request is in a folder for which the user has no traverse permission, the access attempt fails and the event is not logged.

Learn about auditing NAS events on SVMs.

S3 and NAS interoperability

ONTAP S3 NAS buckets support standard NAS and S3 functionality except as listed here.

NAS functionality not currently supported by S3 NAS buckets

FabricPool capacity tier

S3 NAS buckets cannot configured as a capacity tier for FabricPool.

S3 functionality not currently supported by S3 NAS buckets

AWS user metadata

- Key-values pairs received as part of S3 user-metadata are not stored on disk along with object data in the current release.
- Request headers with the prefix "x-amz-meta" are ignored.

AWS Tags

- On PUT object and Multipart Initiate requests, headers with the prefix "x-amz-tagging" are ignored.
- Requests to update tags on an existing file (i.e. a Put, Get, and Delete requests with the ?tagging query-string) are rejected with an error.

Versioning

It is not possible to specify versioning in the bucket mapping configuration.

- Requests that include non-null version specifications (the versionId=xyz query-string) receive error responses.
- Requests to affect the versioning state of a bucket are rejected with errors.

Multipart operations

The following operations are not supported:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

NAS data requirements for S3 client access

It is important to understand that there are some inherent incompatibilities when mapping NAS files and directories for S3 access. It might be necessary to adjust NAS file hierarchies before serving them using S3 NAS buckets.

An S3 NAS bucket provides S3 access to a NAS directory by mapping that directory using S3 bucket syntax, and the files in the directory tree are viewed as objects. The object names are the slash-delimited pathnames of the files relative to the directory specified in the S3 bucket configuration.

This mapping imposes some requirements when files and directories are served using S3 NAS buckets:

- S3 names are limited to 1024 bytes, so files with longer pathnames are not accessible using S3.
- File and directory names are limited to 255 characters, so an object name cannot have more than 255 consecutive non-slash (‘/’) characters
- An SMB pathname that is delimited by backslash (‘\’) characters will appear to s3 as an object name containing forward-slash (‘/’) characters instead.
- Some pairs of legal S3 object names cannot coexist in the mapped NAS directory tree. For example, the legal S3 object names “part1/part2” and “part1/part2/part3” map to files that cannot simultaneously exist in the NAS directory tree, as “part1/part2” is a file in the first name and a directory in the other.
  - If “part1/part2” is an existing file, an S3 creation of “part1/part2/part3” will fail.
  - If “part1/part2/part3” is an existing file, an S3 creation or deletion of “part1/part2” will fail.
  - An S3 object creation that matches the name of an existing object replaces the pre-existing object (in unversioned buckets); that holds in NAS but requires an exact match. The examples above will not cause removal of the existing object because while the names collide, they do not match.

While an object store is designed to support a very large number of arbitrary names, a NAS directory structure can experience performance problems if a very large number of names are placed in one directory. In particular, names with no slash (‘/’) characters in them will all be placed into the root directory of the NAS mapping. Applications that make extensive use of names that are not “NAS-friendly” would be better hosted on an actual object store bucket rather than a NAS mapping.

Enable S3 protocol access to NAS data

Enabling S3 protocol access consists of ensuring that a NAS-enabled SVM meets the same requirements as an S3-enabled server, including adding an object store server, and verifying networking and authentication requirements.

For new ONTAP installations, it is recommended that you enable S3 protocol access to an SVM after configuring it to serve NAS data to clients. To learn about NAS protocol configuration, see:

- NFS configuration
- SMB configuration

Before you begin

The following must be configured before enabling the S3 protocol:

- The S3 protocol and the desired NAS protocols – NFS, SMB, or both – are licensed.
- An SVM is configured for the desired NAS protocols.
- NFS and/or SMB servers exist.
- DNS and any other required services are configured.
- NAS data is being exported or shared to client systems.

About this task

A Certificate Authority (CA) certificate is required to enable HTTPS traffic from S3 clients to the S3-enabled SVM. CA certificates from three sources can be used:

- A new ONTAP self-signed certificate on the SVM.
- An existing ONTAP self-signed certificate on the SVM.

- A third-party certificate.

You can use the same data LIFs for the S3/NAS bucket that you use for serving NAS data. If specific IP addresses are required, see Create data LIFs. An S3 service data policy is required to enable S3 data traffic on LIFs; you can modify the SVM's existing service policy to include S3.

When you create the S3 object server, you should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The S3 server FQDN must not begin with a bucket name.

System Manager

1. Enable S3 on a storage VM with NAS protocols configured.
   a. Click **Storage > Storage VMs**, select a NAS-ready storage VM, click Settings, and then click ⚙ under S3.
   b. Select the certificate type. Whether you select system-generated certificate or one of your own, it will be required for client access.
   c. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
   - The secret key will not be displayed again.
   - If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

CLI

1. Verify that the S3 protocol is allowed on the SVM:
   `vserver show -fields allowed-protocols`
2. Record the public key certificate for this SVM.
   If a new ONTAP self-signed certificate is needed, see Create and install a CA certificate on the SVM.
3. Update the service data policy
   a. Display the service data policy for the SVM
      `network interface service-policy show -vserver svm_name`
   b. Add the `data-core` and `data-s3-server services` if they are not present.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Verify that the data LIFs on the SVM meet your requirements:
   `network interface show -vserver svm_name`
5. Create the S3 server:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

You can specify additional options when creating the S3 server or at any time later.

- HTTPS is enabled by default on port 443. You can change the port number with the -secure-listener -port option.
  When HTTPS is enabled, CA certificates are required for proper integration with SSL/TLS.
- HTTP is disabled by default; when enabled, the server listens on port 80. You can enable it with the -is-http-enabled option or change the port number with the -listener-port option.
  When HTTP is enabled, all the request and responses are sent over the network in clear text.

6. Verify that S3 is configured as desired:
   `vserver object-store-server show`

Example
The following command verifies the configuration values of all object storage servers:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
            Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Create S3 NAS bucket

An S3 NAS buckets is a mapping between an S3 bucket name and a NAS path. S3 NAS buckets allow you to provide S3 access to any part of an SVM namespace having existing volumes and directory structure.

Before you begin

- An S3 object server is configured in an SVM containing NAS data.
- The NAS data conforms to the requirements for S3 client access.

About this task

You can configure S3 NAS buckets to specify any set of files and directories within the root directory of the SVM.

You can also set bucket policies that allow or disallow access to NAS data based on any combination of these parameters:

- Files and directories
- User and group permissions
- S3 operations

For example, you might want separate bucket policies that grant read-only data access to a large group of users, and another that allows a limited group to perform operations on a subset of that data.

Because S3 NAS “buckets” are mappings and not S3 buckets, the following properties of standard S3 buckets don’t apply to S3 NAS buckets.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group**
  No volumes or qtree are created when configuring S3 NAS buckets.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud**
  S3 NAS buckets are not protected or mirrored using S3 SnapMirror, but will instead be using regular SnapMirror protection available at volume granularity.

- **versioning-state**
  NAS volumes usually have Snapshot technology available to save different versions. However, versioning is not currently available in S3 NAS buckets.
- **logical-used \ object-count**
  Equivalent statistics are available for NAS volumes through the volume commands.

System Manager

Add a new S3 NAS bucket on an NAS-enabled storage VM.

1. Click **Storage > Buckets**, then click **Add**.
2. Enter a name for the S3 NAS bucket and select the storage VM, do not enter a size, then click **More Options**.
3. Enter a valid path name or click Browse to select from a list of valid path names.
   When you enter a valid pathname, options that are not relevant to S3 NAS configuration are hidden.
4. If you have already mapped S3 users to NAS users and created groups, you can configure their permissions, then click **Save**.
   You must have already mapped S3 users to NAS users before configuring permissions in this step.

Otherwise, click **Save** to complete S3 NAS bucket configuration.

CLI

Create an S3 NAS bucket in an SVM containing NAS filesystems.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Example:

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

Enable S3 client users

To enable S3 client users to access NAS data, you must map S3 user names to corresponding NAS users, then grant them permission to access the NAS data using bucket service polices.

Before you begin

User names for client access – LINUX/UNIX, Windows and S3 client users – must already exist.

About this task

Mapping an S3 user name to a corresponding LINUX/UNIX or Windows user allows authorization checks on the NAS files to be honored when those files are accessed by S3 clients. S3 to NAS mappings are specified by providing an S3 user name *Pattern*, which can be expressed as a single name or a POSIX regular expression, and a LINUX/UNIX or Windows user name *Replacement*.

In case there is no name-mapping present, default name-mapping will be used, where the S3 user name itself will be used as the UNIX user name and Windows user name. You can modify the UNIX and Windows default user name mappings with the `vserver object-store-server modify` command.

Only local name-mapping configuration is supported; LDAP is not supported.

After S3 users are mapped to NAS users, you can grant permissions to users specifying the resources (directories and files) to which they have access and the actions they are allowed or not allowed to perform there.

System Manager

1. Create local name mappings for UNIX or Windows clients (or both).
   a. Click **Storage > Buckets**, then select the S3/NAS-enabled storage VM.
   b. Select **Settings**, then click → in **Name Mapping** (under **Host Users and Groups**).
   c. In the **S3 to Windows** or **S3 to UNIX** tiles (or both), click **Add**, then entered the desired **Pattern** (S3) and **Replacement** (NAS) user names.
2. Create a bucket policy to provide client access.
   a. Click **Storage > Buckets**, click ⋮ next to the desired S3 bucket, then click **Edit**.
   b. Click **Add** and supply the desired values.
      - **Principal** - Provide S3 user names or use the default (all users)
      - **Effect** - Select **Allow** or **Deny/**
      - **Actions** - Enter actions for these users and resources. The set of resource operations that the object store server currently supports for S3 NAS buckets are: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning and ListBucketVersions. Wildcards are accepted for this parameter.
      - **Resources** - Enter folder or file paths in which the actions are allowed or denied, or use the defaults (root directory of the bucket).

CLI

1. Create local name mappings for UNIX or Windows clients (or both).
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - priority number for mapping evaluation; enter 1 or 2.
   - `-pattern` - an S3 user name or a regular expression
   - `-replacement` - a windows or unix user name

   Examples
   ```
   vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
   -replacement win_user_1
   vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
   -replacement unix_user_1
   ```

2. Create a bucket policy to provide client access.
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - specifies whether access is allowed or denied when a user requests an action.
   - `-action <Action>, …` - specifies resource operations that are allowed or denied. The set of resource operations that the object store server currently supports for S3 NAS buckets are: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning and ListBucketVersions. Wildcards are accepted for this parameter.

- `-principal <Objectstore Principal>, …` - validates the user requesting access against the object store server users or groups specified in this parameter.
  - An object store server group is specified by adding a prefix group/ to the group name.
  - `-principal` - (the hyphen character) grants access to all users.
- `-resource <text>, …` - specifies the bucket, folder, or object for which allow/deny permissions are set. Wildcards are accepted for this parameter.
- `[-sid <SID>]` - specifies an optional text comment for the object store server bucket policy statement.

Examples

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

SMB configuration for Microsoft Hyper-V and SQL Server

SMB configuration for Microsoft Hyper-V and SQL Server overview

ONTAP features allow you to enable nondisruptive operations for two Microsoft applications over the SMB protocol: Microsoft Hyper-V and Microsoft SQL Server.

You should use these procedures if you want to implement SMB nondisruptive operations under the following circumstances:

- Basic SMB protocol file access has been configured.
- You want to enable SMB 3.0 or later file shares residing in SVMs to store the following objects:
  - Hyper-V virtual machine files
  - SQL Server system databases

Related information

For additional information about ONTAP technology and interaction with external services, see these Technical Reports (TRs):

NetApp Technical Report 4172: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices

NetApp Technical Report 4369: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP

Configure ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

You can use continuously available SMB 3.0 and later file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in SVMs, while at the same time providing nondisruptive operations (NDOs) for both

planned and unplanned events.

Microsoft Hyper-V over SMB

To create a Hyper-V over SMB solution, you must first configure ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.

The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with Hyper-V over SMB configurations.

  For information about using SnapManager with Hyper-V over SMB configurations, see *SnapManager for Hyper-V Installation and Administration Guide*.

Microsoft SQL Server over SMB

To create a SQL Server over SMB solution, you must first configure ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.

SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server, see the Microsoft web site.
- SnapCenter Plug-in for Microsoft SQL Server is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with SQL Server over SMB configurations.

  For information about using SnapCenter Plug-in for Microsoft SQL Server, see the SnapCenter Plug-in for Microsoft SQL Server document.

Nondisruptive operations for Hyper-V and SQL Server over SMB

What nondisruptive operations for Hyper-V and SQL Server over SMB means

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover
- Upgrade
- Planned aggregate relocation (ARL)
- LIF migration and failover
- Planned volume move

Protocols that enable nondisruptive operations over SMB

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

- SMB 3.0
- Witness

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

- **Continuously available share**

  An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.

- **Node**

  A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the *local node* and the other node is sometimes called the *partner node* or *remote node*. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner's storage.

- **Nondisruptive aggregate relocation**

  The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.

- **Nondisruptive failover**

  See *Takeover*.

- **Nondisruptive LIF migration**

  The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.

- **Nondisruptive operations**

  The ability to perform major ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.

- **Nondisruptive upgrade**

  The ability to upgrade node hardware or software without application interruption.

- **Nondisruptive volume move**

  The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.

- **Persistent handles**

  A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost. However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

  Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

- **SFO giveback**

  Returning aggregates to their home locations when recovering from a takeover event.

- **SFO pair**

  A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.

- **Takeover**

  The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

How SMB 3.0 functionality supports nondisruptive operations over SMB shares

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the `continuously-available` share property and a type of file handle known as a *persistent handle* that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the continuously

available share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the storage virtual machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if a failure causes the Hyper-V application to fail over to another node in the Windows Server cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. “Failover Clustering” is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

What the Witness protocol does to enhance transparent failover

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

- It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
- The shares must use SMB 3.0 with the continuous availability share property set.
- The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the storage virtual machine (SVM) hosting data for the application servers.

> The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner. The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

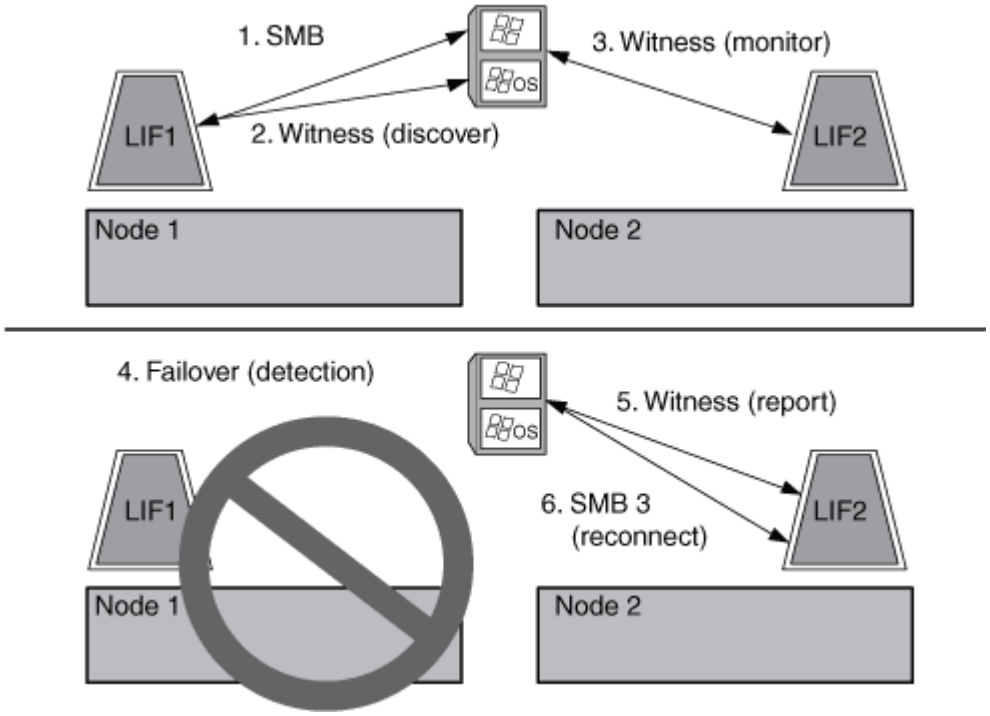
- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

How the Witness protocol works

ONTAP implements the Witness protocol by using a node’s SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.
2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the storage virtual machine (SVM).
3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.
4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.
5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.
6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.



Share-based backups with Remote VSS

Share-based backups with Remote VSS overview

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

- **VSS (Volume Shadow Copy Service)**

  A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

  A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.

- **Shadow copy**

  A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

- **Shadow copy set**

  A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

- **Shadow copy set automatic recovery**

  The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

- **Shadow copy ID**

  A GUID that uniquely identifies a shadow copy.

- **Shadow copy set ID**

  A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

- **SnapManager for Hyper-V**

  The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V

files over SMB shares.

Related information

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

Share-based backups with Remote VSS

Example of a directory structure used by Remote VSS

Remote VSS traverses the directory structure that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is, so that you can successfully create backups of virtual machine files.

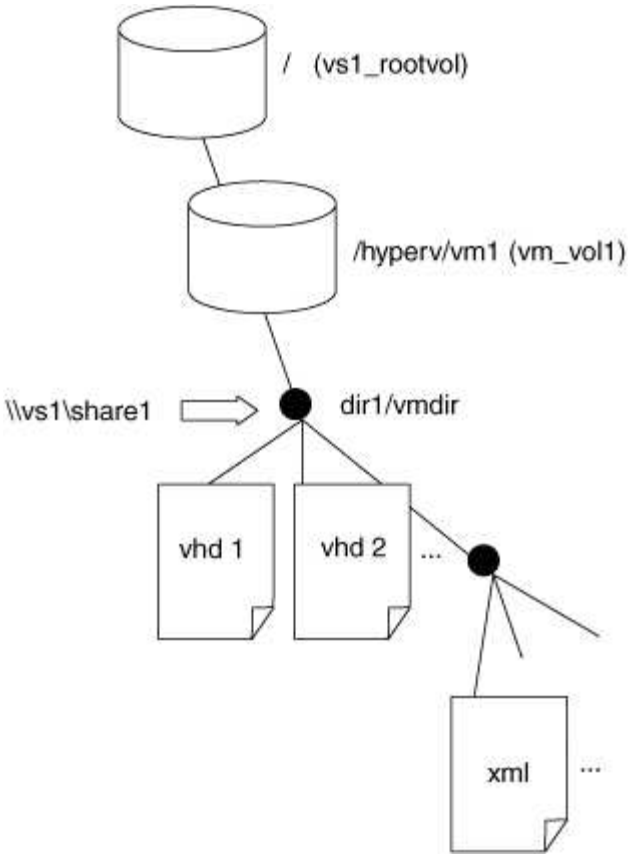
A supported directory structure for the successful creation of shadow copies conforms to the following requirements:

- Only directories and regular files are present within the directory structure that is used to store virtual machine files.

  The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.
- The directory structure that is used to store virtual machine files does not exceed the configured depth of the shadow copy directory.
- The root directory of the share contains only virtual machine files or directories.

In the following illustration, the volume named vm_vol1 is created with a junction point at `/hyperv/vm1` on storage virtual machine (SVM) vs1. Subdirectories to contain the virtual machine files are created under the junction point. The virtual machine files of the Hyper-V server are accessed over share1 that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files that are contained within the directory structure under share1 (up to the configured depth of the shadow copy directory).



How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with ONTAP provides performance optimization when discovering SMB share location.

  ONTAP provides SnapDrive with the name of the volume where the share resides.

- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

  By providing a targeted list of virtual machine files, the shadow copy service does not need to create shadow copies of all the files in the share.

- The storage virtual machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.

  There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation

The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

2. Creating the shadow copy set (if automatic-recovery is used)

   For every share included in the shadow copy set, ONTAP creates a shadow copy and makes the shadow copy writable.

3. Exposing the shadow copy set

   After ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

4. Automatically recovering the shadow copy set

   During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.

   > The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

5. Completing and cleaning up the shadow copy set

   The VSS client notifies ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

This functionality is available on Windows Server 2012 servers. ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same storage virtual machine (SVM)

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

  This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

> To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

- You can use ODX copy offload to export and import SQL Server databases between mapped SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.
- ODX copy offload is used for database exports and imports if the source and destination storage is on the same cluster.

Configuration requirements and considerations

ONTAP and licensing requirements

You need to be aware of certain ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs.

ONTAP version requirements

- Hyper-V over SMB

  ONTAP supports nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.

- SQL Server over SMB

  ONTAP supports nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)

  This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to create point-in-time copies of files that are then used when creating a backup.

  A FlexClone license is optional if you use a backup method that does not use Remote VSS.

Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations).

Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.

  SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.

- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the storage virtual machine (SVM).

  The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple

connections to multiple unique IP addresses.

Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

Beginning with ONTAP 9.4, you can improve throughput and fault tolerance for Hyper-V and SQL server over SMB configurations by enabling SMB Multichannel. To do so, you must have multiple 1G, 10G, or larger NICs deployed on the cluster and clients.

Data LIF requirements

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.

  SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.

- Data LIFs must not be configured to automatically revert.

  After a takeover or giveback event, you should manually revert the data LIFs to their home ports.

- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name.

  The application servers must connect to SMB shares by using the CIFS server name. You must not configure the application servers to make connections by using the LIF IP addresses.

- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

SMB server and volume requirements for Hyper-V over SMB

You need to be aware of certain SMB server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.

- Both Kerberos and NTLM authentication must be allowed in the domain to which the SMB server belongs.

ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.

- Shadow copy functionality must be enabled.

  This functionality is enabled by default.

- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the SMB server local BUILTIN\Administrators or BUILTIN\Backup Operators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- For shadow copy operations to succeed, you must have enough available space on the volume.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

SMB server and volume requirements for SQL Server over SMB

You need to be aware of certain SMB server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

  Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.

- The Windows user account used for installing SQL Server on ONTAP must be assigned the SeSecurityPrivilege privilege.

  This privilege is assigned to the SMB server local BUILTIN\Administrators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.

  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

Share requirements

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.

  In the auto-recovery case, the shadow copy creation fails if a junction is encountered while traversing the

share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files

    The shadow copy creation fails if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.

  - For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).

    The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.
- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

Considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for Hyper-V over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` parameter set to `Yes`.

Continuously available share requirements and considerations for SQL Server over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

Share requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and

imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server operations to succeed, you must have enough available space on the volume.

  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

Share considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for SQL Server over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` share property set.

Remote VSS considerations for Hyper-V over SMB configurations

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

General Remote VSS considerations

- A maximum of 64 shares can be configured per Microsoft application server.

  The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.

- Only one active shadow copy set per CIFS server is allowed.

  A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.

- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.

- In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
- In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

Remote VSS considerations that apply only for shadow copies with automatic recovery

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation.

  This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine file are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

- Amount of available space on the volume must be adequate.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

- No links or non-regular files are allowed within the directory structure on which Remote VSS creates a shadow copy.

  The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy. The clone process does not support them.

- No NFSv4 ACLs are allowed on directories.

  Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

- A maximum of 60 seconds is allowed to create a shadow copy set.

  Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

ODX copy offload requirements for SQL Server and Hyper-V over SMB

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

- SMB 3.0 must be enabled to use ODX copy offload.
- Source volumes must be a minimum of 1.25 GB.

- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

  Secondary compression type is not supported

- To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.

  The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

Recommendations for SQL Server and Hyper-V over SMB configurations

To be sure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

General recommendations

- Separate application server files from general user data.

  If possible, devote an entire storage virtual machine (SVM) and its storage for the application server's data.

- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- For best performance and improved fault tolerance, enable SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as aggregate relocation (ARL) because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use in-guest iSCSI drives when creating clustered virtual machines. Shared `.VHDX` files are not supported for Hyper-V over SMB in ONTAP SMB shares.

Plan the Hyper-V or SQL Server over SMB configuration

Complete the volume configuration worksheet

The worksheet provides an easy way to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all volumes.

- Volume name

- Aggregate name

  You can create volumes on aggregates located on any node in the cluster.

- Size
- Junction path

You should keep the following in mind when creating volumes used to store application server data:

- If the root volume does not have NTFS security style, you must specify the security style as NTFS when you create the volume.

  By default, volumes inherit the security style of the SVM root volume.

- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the Snapshot copy space reserve to `0`.
- The Snapshot policy applied to the volume must be disabled.

  If the SVM Snapshot policy is disabled, then you do not need to specify a Snapshot policy for the volumes. The volumes inherit the Snapshot policy for the SVM. If the Snapshot policy for the SVM is not disabled and is configured to create Snapshot copies, you must specify a Snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage Snapshot copy creation and deletion.

- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named “vol1”, “vol2”, “vol3”, and “vol4”, you can create the namespace shown in the example. You can then create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Types of information	Values
Volume 1: Volume name, aggregate, size, junction path	

Types of information	Values
Volume 2: Volume name, aggregate, size, junction path	
Volume 3: Volume name, aggregate, size, junction path	
Volume 4: Volume name, aggregate, size, junction path	
Volume 5: Volume name, aggregate, size, junction path	
Volume 6: Volume name, aggregate, size, junction path	
Additional volumes: Volume name, aggregate, size, junction path	

Complete the SMB share configuration worksheet

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

Information about SMB shares properties and configuration settings

For each share, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all shares

- Share name
- Path
- Share properties

  You must configure the following two share properties:

  - `oplocks`
  - `continuously-available`

The following share properties must not be set:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`

With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

- Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null [""]).

Information about share paths

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on volumes “vol1”, “vol2”, “vol3”, and “vol4”, you should create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Although you can create shares on the `/data1` and `/data2` paths for administrative management, you must not configure the application servers to use those shares to store data.

Planning worksheet

Types of information	Values
Volume 1: SMB share name and path	
Volume 2: SMB share name and path	
Volume 3: SMB share name and path	
Volume 4: SMB share name and path	
Volume 5: SMB share name and path	

Types of information	Values
Volume 6: SMB share name and path	
Volume 7: SMB share name and path	
Additional volumes: SMB share names and paths	

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB overview

There are several ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you create the ONTAP configuration for nondisruptive operations with Hyper-V and SQL Server over SMB, the following tasks must be completed:

- Time services must be set up on the cluster.
- Networking must be set up for the SVM.
- The SVM must be created.
- Data LIF interfaces must be configured on the SVM.
- DNS must be configured on the SVM.
- Desired names services must be set up for the SVM.
- The SMB server must be created.

Related information

Plan the Hyper-V or SQL Server over SMB configuration

Configuration requirements and considerations

Verify that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

About this task

Kerberos authentication is required when making a continuously available share connection. Part of the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the storage virtual machine (SVM).

Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can be used to restrict access based on authentication method.

Export policies for SMB are optional and are disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication are allowed on a CIFS server by default.

- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and NTLMv2 authentication.

Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2 authentication can be disallowed, either using Security Policy settings or Group Policies.

Steps

1. Perform the following to verify that export policies are disabled on the SVM:
   a. Set the privilege level to advanced:

      set -privilege advanced

   b. Verify that the `-is-exportpolicy-enabled` CIFS server option is set to `false`:

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. Return to the admin privilege level:

      set -privilege admin

2. If export policies for SMB are not disabled, disable them:

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

   For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTMLv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

Verify that domain accounts map to the default UNIX user

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

When you create a storage virtual machine (SVM), ONTAP automatically creates the default user named “pcuser” (with a UID of `65534`) and the group named “pcuser” (with a GID of `65534`), and adds the default user to the “pcuser” group. If you are configuring a Hyper-V over SMB solution on anSVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server’s default UNIX user.

Steps

1. Determine whether there is a default UNIX user:

   `vserver cifs options show -vserver` ***`vserver_name`***

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

   `vserver services unix-user show -vserver` ***`vserver_name`***

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default UNIX user and the default group, and add the default user to the group.

   Generally, the default user is given the user name “pcuser” and must be assigned the UID of `65534`. The default group is generally given the group name “pcuser”. The GID assigned to the group must be `65534`.

   a. Create the default group:
      +

vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534

b. Create the default user and add the default user to the default group:
+
vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534

c. Verify that the default user and default group are configured correctly:
+
vserver services unix-user show -vserver *vserver_name*
+
vserver services unix-group show -vserver *vserver_name* -members

4. If the CIFS server's default user is not configured, perform the following:

   a. Configure the default user:

      vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser**

   b. Verify that the default UNIX user is configured correctly:

      vserver cifs options show -vserver *vserver_name*

5. To verify that the application server's computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the `vserver cifs session show` command.

   For more information about using this command, see the man pages.

Example

The following commands determine that the CIFS server's default user is not set, but determines that the "pcuser" user and "pcuser" group exist. The "pcuser" user is assigned as the CIFS server's default user on SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
```

```
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Verify that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the storage virtual machine (SVM), the security style of the root volume should be set to NTFS.

About this task

- You can specify the root volume security style at the time you create the SVM.
- If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the `volume modify` command.

Steps

1. Determine the current security style of the SVM root volume:

```
volume show -vserver vserver_name -fields vserver,volume,security-style
```

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:

```
volume modify -vserver vserver_name -volume root_volume_name -security-style
ntfs
```

3. Verify that the SVM root volume is set to NTFS security style:

```
volume show -vserver vserver_name -fields vserver,volume,security-style
```

Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verify that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

Steps

1. Verify that the required CIFS server options are enabled on the storage virtual machine (SVM):
   a. Set the privilege level to advanced:

```
set -privilege advanced
```

   b. Enter the following command:

vserver cifs options show -vserver *vserver_name*

The following options should be set to `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Hyper-V only)

2. If any of the options are not set to `true`, perform the following:
   a. Set them to `true` by using the `vserver cifs options modify` command.
   b. Verify that the options are set to `true` by using the `vserver cifs options show` command.
3. Return to the admin privilege level:

set -privilege admin

Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple

connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance for Hyper-V and SQL server over SMB configurations.

What you'll need

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

  The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

  The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- **`-max-connections-per-session`**

  The maximum number of connections allowed per Multichannel session. The default is 32 connections.

  If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- **`-max-lifs-per-session`**

  The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enable SMB Multichannel on the SMB server:

   ```
   vserver cifs options modify -vserver vserver_name -is-multichannel-enabled
   true
   ```

3. Verify that ONTAP is reporting SMB Multichannel sessions:

   ```
   vserver cifs session show options
   ```

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Create NTFS data volumes

You must create NTFS data volumes on the storage virtual machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over SMB application servers. Use the volume configuration worksheet to create your data volumes.

About this task

There are optional parameters that you can use to customize a data volume. For more information about customizing volumes, see the xref:./smb-hyper-v-sql/Logical storage management.

As you create your data volumes, you should not create junction points within a volume that contains the following:

- Hyper-V files for which ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server

> If you inadvertently create a volume that uses mixed or UNIX security style, you cannot change the volume to an NTFS security style volume and then directly use it to create continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V and SQL Server over SMB do not work correctly unless the volumes used in the configuration are created as NTFS security-style volumes.You must either delete the volume and re-create the volume with NTFS security style, or you can map the volume on a Windows host and apply an ACL at the top of the volume and propagate the ACL to all files and folders in the volume.

Steps

1. Create the data volume by entering the appropriate command:

If you want to create a volume in an SVM where the root volume security style is…	Enter the command…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Not NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Verify that the volume configuration is correct:

```
volume show -vserver vserver_name -volume volume_name
```

Create continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and

SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

Steps

1. Display information about the existing data volumes and their junction paths:

   volume show -vserver *vserver_name* -junction

2. Create a continuously available SMB share:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - You can optionally add a comment to the share configuration.
   - By default, the offline files share property is configured on the share and is set to `manual`.
   - ONTAP creates the share with the Windows default share permission of `Everyone` / `Full Control`.

3. Repeat the previous step for all shares in the share configuration worksheet.
4. Verify that your configuration is correct by using the `vserver cifs share show` command.
5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the **Windows Properties** window.

Example

The following commands create a continuously available share named “data2” on storage virtual machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the `-symlink` parameter to `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Add the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require privileges not assigned by default to domain users.

What you’ll need

The domain account used for installing the SQL Server must already exist.

About this task

When adding the privilege to the SQL Server installer’s account, ONTAP might validate the account by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Add the “SeSecurityPrivilege” privilege:

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

The value for the `-user-or-group-name` parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-
group-name account_name
```

Example

The following command adds the “SeSecurityPrivilege” privilege to the SQL Server installer’s account in the EXAMPLE domain for storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configure the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which ONTAP should create shadow copies.

What you’ll need

The VSS shadow copy feature must be enabled.

About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to `0`, ONTAP creates shadow copies for all subdirectories.

> Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Set the VSS shadow copy directory depth to the desired level:

   vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6

3. Return to the admin privilege level:

   set -privilege admin

Manage Hyper-V and SQL Server over SMB configurations

Configure existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the `homedirectory` share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

The following share properties must be configured:

- `continuously-available`
- `oplocks`

The following share properties must not be set. If they are present in the list of current share properties, they need to be removed from the continuously available share:

- `attributecache`
- `branchcache`

Steps

1. Display the current share parameter settings and the current list of configured share properties:

   vserver cifs share show -vserver *vserver_name* -share-name *share_name*

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the

`vserver cifs share properties modify` command.

You can disable symlinks by setting the value of the `-symlink` parameter to `""`.

- You can disable symlinks by setting the value of the `-symlink` parameter to `""`.
- You can set the `-offline-files` parameter to the correct setting by specifying `manual`.

3. Add the `continuously-available` share property, and, if needed, the `oplocks` share property:

   vserver cifs share properties add -vserver *vserver_name* -share-name *share_name* -share-properties continuously-available[,oplock]

   If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

   vserver cifs share properties remove -vserver *vserver_name* -share-name *share_name* -share-properties properties[,…]

   You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

   vserver cifs share show -vserver *vserver_name* -share-name *share_name* -fields symlink-properties,offline-files

6. Verify that the list of configured share properties is correct:

   vserver cifs shares properties show -vserver *vserver_name* -share-name share_name

Examples

The following example shows how to configure an existing share named “share1” on storage virtual machine (SVM) vs1 for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the `-symlink` parameter to "".
- The `-offline-file` parameter is modified and set to `manual`.
- The `continuously-available` share property is added to the share.
- The `oplocks` share property is already in the list of share properties; therefore, it does not need to be added.
- The `attributecache` share property is removed from the share.
- The `browsable` share property is optional for a continuously available share used for NDOs with application servers over SMB and is retained as one of the share properties.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Enable or disable VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

About this task

You can enable or disable VSS shadow copies at any time.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want VSS shadow copies to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following commands enable VSS shadow copies on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Use statistics to monitor Hyper-V and SQL Server over SMB activity

Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash

statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to determine…	Enter…
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show object` *`object_name`*
Which counters are available	`statistics catalog counter show object` *`object_name`*

   See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:

> This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Display SMB statistics

You can display various SMB statistics to monitor performance and diagnose issues.

Steps

1. Use the `statistics start` and optional `statistics stop` commands to collect a data sample.
2. Perform one of the following actions:

If you want to display statistics for…	Enter the following command…
All versions of SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x and SMB 3.0	**`statistics show -object smb2`**
CIFS subsystem of the node	**`statistics show -object nblade_cifs`**

Learn more about the `statistics` commands:

- `statistics show`
- `statistics start`
- `statistics stop`

Verify that the configuration is capable of nondisruptive operations

Use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

Alert ID	Severity	Condition
`HaNotReadyCifsNdo_Alert`	Major	One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.

Alert ID	Severity	Condition
NoStandbyLifCifsNdo_Alert	Minor	The storage virtual machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.

Display nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

Steps

1. Monitor health status by performing the appropriate action:

If you want to display…	Enter the command…
The health status of the system, which reflects the overall status of individual health monitors	**system health status show**
Information about the health status of the CIFS-NDO subsystem	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

If you want to display information about…	Enter the command…
The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status	**system health config show -subsystem CIFS-NDO**
The CIFS-NDO alerts that a health monitor can potentially generate	**system health alert definition show -subsystem CIFS-NDO**
CIFS-NDO health monitor policies, which determine when alerts are raised	**system health policy definition show -monitor node-connect**

Use the `-instance` parameter to display detailed information.

Examples

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

The following output shows detailed information about the configuration and status of the health monitor of the CIFS-NDO subsystem:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verify the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to provide seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.

About this task

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

For proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps

1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:

   vserver cifs shares show -vserver *vserver_name*

2. Verify that the SMB shares are configured for continuous availability:

   vserver cifs shares properties show -vserver *vserver_name*

Examples

The following example displays the share setting for a share named “share1” on storage virtual machine (SVM, formerly known as Vserver) vs1. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the `Symlink Properties` field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                     Vserver: vs1
                       Share: share1
     CIFS Server NetBIOS Name: VS1
                        Path: /data/share1
            Share Properties: oplocks
                              continuously-available
          Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Verify LIF status

Even if you configure storage virtual machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

About this task

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

Steps

1. Display information about configured LIFs for the SVM:

   network interface show -vserver *vserver_name*

   In this example, “lif1” is not located on the home port.

   ```
   network interface show -vserver vs1
   ```

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2      e0d
   false
               lif2         up/up    10.0.0.129/24    node2      e0d
   true
   ```

2. If some of the LIFs are not on their home ports, perform the following steps:
   a. For each LIF, determine what the LIF’s home port is:

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. For each LIF, determine whether the LIF's home port is up:

network port show -node *node_name* -port *port* -fields port,link

`network port show -node node1 -port e0d -fields port,link`

```
node       port link
---------- ---- ----
node1      e0d  up
```

In this example, "lif1" should be migrated back to its home port, `node1:e0d`.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the `up` state, resolve the problem so that these interfaces are up.
4. If needed, revert the LIFs to their home ports:

network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

5. Verify that each node in the cluster has an active LIF for the SVM:

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determine whether SMB sessions are continuously available

Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you to identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display SMB session information…	Enter the following command…
For all sessions on the SVM in summary form	**vserver cifs session show -vserver *vserver_name***
On a specified connection ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
From a specified workstation IP address	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
On a specified LIF IP address	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
On a specified node	**vserver cifs session show -vserver *vserver_name* -node {node_name|local}**

If you want to display SMB session information…	Enter the following command…
From a specified Windows user	**vserver cifs session show -vserver *vserver_name* -windows -user *user_name*** The format for `user_name` is `[domain]\user`.
With a specified authentication mechanism	**vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism** The value for `-auth-mechanism` can be one of the following: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`
With a specified protocol version	**vserver cifs session show -vserver *vserver_name* -protocol -version protocol_version** The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to `SMB3` or later.

If you want to display SMB session information…	Enter the following command…
With a specified level of continuously available protection	**vserver cifs session show -vserver *vserver_name* -continuously-available *continuously_available_protection_level*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` • `Partial` If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
With a specified SMB signing session status	**vserver cifs session show -vserver *vserver_name* -is -session-signed {true|false}**

Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                  Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
             **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can also display information about the continuously available protection level of a file, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously-available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

  You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

  You can use this parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	**vserver cifs session file show -vserver *vserver_name***
On a specified node	**vserver cifs session file show -vserver *vserver_name* -node {node_name|local}**
On a specified file ID	**vserver cifs session file show -vserver *vserver_name* -file-id integer**
On a specified SMB connection ID	**vserver cifs session file show -vserver *vserver_name* -connection-id integer**
On a specified SMB session ID	**vserver cifs session file show -vserver *vserver_name* -session-id integer**
On the specified hosting aggregate	**vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name***
On the specified volume	**vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name***
On the specified SMB share	**vserver cifs session file show -vserver *vserver_name* -share *share_name***
On the specified SMB path	**vserver cifs session file show -vserver *vserver_name* -path *path***

If you want to display open SMB files…	Enter the following command…
With the specified level of continuously available protection	**vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` ⓘ If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	**vserver cifs session file show -vserver *vserver_name* -reconnected *reconnected_state*** The value for `-reconnected` can be one of the following: • `No` • `Yes` ⓘ If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Copyright information

Copyright © 2022 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.