NetApp

Manage SMB with the CLI

ONTAP 9

NetApp
February 12, 2026

Table of Contents

Manage SMB with the CLI

Learn about ONTAP SMB

ONTAP file access features are available for the SMB protocol. You can enable a CIFS server, create shares, and enable Microsoft services.

> (i) *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.

SMB server support

Learn about ONTAP SMB server support

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.

Related information

Network management

Modify servers

System administration

Supported ONTAP SMB versions and functionality

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. All SMB versions are supported. 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 SMB servers, and can be enabled or disabled as needed. SMB 1.0 can be enabled or disabled as needed.

> **ⓘ** Default settings for SMB 1.0 and 2.0 connections to domain controllers also depend on the ONTAP version. Learn more about `vserver cifs security modify` in the ONTAP command reference. 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:	
		3.0	3.1.1
Legacy SMB 1.0 functionality		X	X
Durable handles		X	X
Compounded operations		X	X
Asynchronous operations		X	X
Increased read and write buffer sizes		X	X
Increased scalability		X	X
SMB signing	X	X	X
Alternate Data Stream (ADS) file format	X	X	X
Large MTU (enabled by default beginning with ONTAP 9.7)	X	X	X
Lease oplocks		X	X
Continuously available shares	X	X	X
Persistent handles		X	X
Witness		X	X
SMB encryption: AES-128-CCM	X	X	X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:	
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
SMB encryption: AES-128-GCM	X		X

Related information

Learn about using ONTAP signing to enhance network security

Set the server minimum authentication security level

Configuring required SMB encryption on SMB servers for data transfers over SMB

NetApp Interoperability

Unsupported Windows features in ONTAP SMB

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 ONTAP SMB SVMs

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
```

Vserver	Database	Enabled	Source 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>,…
```

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

> (i) The field `-nis-servers` replaced the field `-servers`. This field can take either a hostname or an IP address for the NIS server.

e. Verify that the NIS name service is properly configured: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver        Domain              Server
-------------  ------------------- ---------------
vs1            example.com         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.

Learn about ONTAP SMB name service switch configuration

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`
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 ONTAP 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. Learn more about `vserver cifs modify` in the ONTAP command reference.

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 ONTAP 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.

  (i) 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.

Configure ONTAP 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`

Learn more about `vserver cifs options modify` and configuring SMB server options in the ONTAP command reference.

Configure the grant UNIX group permission to ONTAP 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`

If you want to	Enter the command
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 ONTAP SMB 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 server options](#)

Manage how file security is presented to SMB clients for UNIX security-style data

Learn about presenting ONTAP file security to SMB clients for UNIX security-style data

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

- Configure security styles on FlexVol volumes
- Configure security styles on qtrees

Configure the presentation of NTFS ACLs to ONTAP SMB clients 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`

Learn about preserving UNIX permissions for ONTAP SMB FlexVol volumes

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.

Learn about managing UNIX permissions using the Windows Security tab for ONTAP SMB servers

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

Learn about handling ONTAP 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.

Learn about SMB server security settings for ONTAP 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 ONTAP 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`
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

Display information about GPO configurations

Configure ONTAP 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

Do 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

- Display information about server security settings
- Learn about local users and groups
- Requirements for local user passwords
- Change local user account passwords

Modify the ONTAP SMB 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 (9.13.1 and later) or seconds (9.12.1 or earlier).	`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

Display information about server security settings

Supported GPOs

Applying Group Policy Objects to CIFS servers

Set the ONTAP 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.

Value	Description
`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

Configure AES encryption for Kerberos-based communication

Configure strong ONTAP SMB security for Kerberos-based communication 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, Advanced Encryption Standard (AES) encryption is disabled. You must enable it to take advantage of the strong security provided by 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:

- AES 256
- AES 128
- DES
- RC4-HMAC

If you want to use the highest security encryption type for Kerberos communication, you should enable AES encryption for Kerberos communication on the SVM.

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.

Beginning with ONTAP 9.12.1, you can specify which encryption types to advertise to the Active Directory (AD)

KDC. You can use the `-advertised-enc-types` option to enable recommended encryption types, and you can use it to disable weaker encryption types. Learn how to Configure AES encryption for Kerberos-based communication.

> ⓘ 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.

Related information

Modify the server security settings

Configure AES encryption for ONTAP SMB Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you should use AES-256 and AES-128 encryption on the SMB server. Beginning with ONTAP 9.13.1, AES encryption is enabled by default. 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.

Whether AES encryption is enabled by default and whether you have the option to specify encryption types depends on your ONTAP version.

ONTAP version	AES encryption is enabled …	You can specify encryption types?
9.13.1 and later	By default	Yes
9.12.1	Manually	Yes
9.11.1 and earlier	Manually	No

Beginning with ONTAP 9.12.1, AES encryption is enabled and disabled using the `-advertised-enc-types` option, which allows you to specify the encryption types advertised to the AD KDC. The default setting is `rc4` and `des`, but when an AES type is specified, AES encryption is enabled. You can also use the option to explicitly disable the weaker RC4 and DES encryption types. In ONTAP 9.11.1 and earlier, you must use the `-is-aes-encryption-enabled` option to enable and disable AES encryption, and encryption types cannot be specified.

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.

Example 1. Steps

ONTAP 9.12.1 and later

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 -advertised -enc-types aes-128,aes-256`
Disabled	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

Note: The `-is-aes-encryption-enabled` option is deprecated in ONTAP 9.12.1 and might be removed in a later release.

2. Verify that AES encryption is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Examples

The following example enables the AES encryption types for the SMB server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver   advertised-enc-types
-------   --------------------
vs1       aes-128,aes-256
```

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 -advertised-enc
-types aes-128,aes-256

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 advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 and earlier

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.

Examples

The following example enables the AES encryption types for the SMB 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 CIFS
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
```

Related information

Domain user fails to log in cluster with Domain-Tunnel

Use SMB signing to enhance network security

Learn about using ONTAP SMB signing to enhance network security

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.

Learn how signing policies affect communication with ONTAP SMB servers

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

> (i) 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)]

Learn about the performance impact of ONTAP 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 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.

ONTAP SMB signing configuration recommendations

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.

Learn about ONTAP SMB signing configuration for multiple data LIFS

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.

Configure ONTAP 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
```

> ⓘ Changes to the encryption settings take effect for new connections. Existing connections are unaffected.

Related information

- snapmirror create

Determine whether ONTAP 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 ONTAP 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.

   Learn more about `statistics start` in the ONTAP command reference.

3. Use the `statistics stop` command to stop collecting data for the sample.

   Learn more about `statistics stop` in the ONTAP command reference.

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.

Learn more about `statistics show` in the ONTAP command reference.

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

-
-

Configure required SMB encryption on SMB servers for data transfers over SMB

Learn about ONTAP SMB encryption

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 an 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:

- An SMB server security option that enables the functionality on the SVM
- An 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.
False	False	No encryption is enabled.

SMB clients that do not support encryption cannot connect to an SMB server or share that requires encryption.

Changes to the encryption settings take effect for new connections. Existing connections are unaffected.

Learn about the performance impact of ONTAP 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 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 ONTAP SMB encryption for incoming 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
```

Related information

- snapmirror create

Determine whether clients are connected using encrypted ONTAP 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 ONTAP 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.

   Learn more about `statistics start` in the ONTAP command reference.

3. Use the `statistics stop` command to stop collecting data for the sample.

   Learn more about `statistics stop` in the ONTAP command reference.

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`*`]`

If you want to view information for…	Enter…

Encrypted sessions and established sessions	`show -sample-id` *`sample_ID`* `-counter`
	`encrypted_sessions|established_session`
	`s|`*`node_name`* `[-node` *`node_name`*`]`

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_nam`*
	`e [-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.

Learn more about `statistics show` in the ONTAP command reference.

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

- Determine which statistics, objects, and counters are available on servers

- Performance monitoring and management overview

Secure LDAP session communication

Learn about ONTAP SMB LDAP signing and sealing

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 ONTAP SMB servers

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`

   > (i) 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 self-signed root CA certificates for ONTAP SMB SVMs

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 self-signed root CA certificates on the ONTAP SMB 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

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`

Related information

- security certificate install
- security certificate show

Enable LDAP over TLS on the ONTAP SMB 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:

- Learn about LDAP for ONTAP NFS SVMs
- 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`

> (i) 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 ONTAP 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
```

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 ONTAP SMB 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 ONTAP SMB 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 administrator groups to the ONTAP SMB 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, 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.

If you want to…	Then…
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 ONTAP 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
```

ONTAP 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

Learn more about `vserver cifs options modify` in the [ONTAP command reference](#).

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

Learn about improving ONTAP SMB client performance with traditional and lease oplocks

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.

Learn about writing ONTAP SMB 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 ONTAP 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,...]` (i) 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.

If you want to…	Then…
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

Enable or disable oplocks on existing SMB shares

Monitor oplock status

ONTAP commands for enabling or disabling oplocks on SMB 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

Monitor oplock status

Enable or disable oplocks on existing ONTAP 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` (i) 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.
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` (i) 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

- Enable or disable oplocks when creating SMB shares
- Monitor oplock status
- Add or remove share properties on existing shares

Monitor ONTAP SMB 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

Learn more about `vserver oplocks show` in the ONTAP command reference.

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

Enable or disable oplocks when creating SMB shares

Enable or disable oplocks on existing SMB shares

Commands for enabling or disabling oplocks on SMB volumes and qtrees

Apply Group Policy Objects to SMB servers

Learn about applying Group Policy Objects to ONTAP SMB servers

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

- [Learn about file access security for servers](#)
- [SMB and NFS auditing and security tracing](#)

Learn about supported ONTAP SMB 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.

> **(i)** 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.

    > **(i)** 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.

  > **(i)** 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

- [Enable or disable GPO support on servers](#)
- [Learn about file access security for servers](#)
- [SMB and NFS auditing and security tracing](#)
- [Modify the server security settings](#)
- [Learn about using BranchCache to cache share content at a branch office](#)
- [Learn about using ONTAP signing to enhance network security](#)
- [Learn about configuring bypass traverse checking](#)
- [Configure access restrictions for anonymous users](#)

ONTAP SMB server requirements for GPOs

To use Group Policy Objects (GPOs) with your SMB server, your system must meet several requirements.

- SMB must be licensed on the cluster. The SMB license is included with [ONTAP One](#). If you don't have ONTAP One and the license is not installed, contact your sales representative.
- 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 ONTAP SMB servers

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

Learn about supported GPOs

Server requirements for GPOs

Learn about updating GPOs on SMB servers

Manually update GPO settings on SMB servers

Display information about GPO configurations

How GPOs are updated on the SMB server

Learn about updating GPOs on ONTAP SMB servers

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.

Manually update GPO settings on ONTAP SMB servers

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`

Display information about ONTAP SMB 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`

If you want to display information about all Group Policy configurations…	Enter the command…
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

Display information about ONTAP SMB 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`

If you want to display information about all restricted group GPOs…	Enter the command…
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 GPO configurations

Display information about ONTAP SMB 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

- Learn about file access security for servers
- Display information about GPO configurations
- Display information about central access policy rules

Display information about ONTAP SMB 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

- Learn about file access security for servers
- Display information about GPO configurations
- Display information about central access policies

ONTAP commands for managing SMB server 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 the domain account password when ONTAP is synchronized with AD services	`vserver cifs domain password change`
Reset the domain account password when ONTAP is not synchronized with AD services	`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`

Learn more about `vserver cifs domain password` in the [ONTAP command reference](#).

Manage domain controller connections

Display information about ONTAP SMB 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

- [Reset and rediscover servers](#)
- [Stop or start servers](#)

Reset and rediscover ONTAP SMB 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

- Display information about discovered servers
- Stop or start servers

Manage ONTAP SMB 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 can be defined to use this mode with LIFs that are not assigned to a site in sites-and-services.

- 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.

Before you begin

You must be at the advanced privilege level.

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 ONTAP SMB 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

ONTAP commands for managing preferred SMB 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`

Learn more about `vserver cifs domain preferred-dc` in the ONTAP command reference.

Related information

Add preferred domain controllers

Enable encrypted connections to ONTAP SMB 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 ONTAP SMB null sessions to access storage in non-Kerberos environments

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.

Learn how ONTAP SMB storage systems provide 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). Learn more about `vserver cifs options modify` and `vserver cifs options show` and the `-restrict-anonymous` option in the ONTAP command reference.

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

Configure access restrictions for anonymous users

Grant null users access to ONTAP SMB 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

Learn about managing NetBIOS aliases for ONTAP SMB servers

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

[Display information about NetBIOS over TCP connections](#)

Add NetBIOS alias lists to ONTAP SMB servers

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

- [Remove NetBIOS aliases from the list for SMB servers](#)
- [Display the NetBIOS aliases list for SMB servers](#)

Remove NetBIOS aliases from the list for ONTAP SMB servers

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 NetBIOS aliases list for ONTAP SMB 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`

If you want to display information about…	Enter…
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
```

Learn more about `vserver cifs show` in the ONTAP command reference.

Related information

- Add NetBIOS alias lists to servers
- Commands for managing servers

Determine whether ONTAP 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`
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 ONTAP SMB servers

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 cifs 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

- Display information about discovered servers
- Reset and rediscover servers

Move ONTAP SMB 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 before moving ONTAP SMB servers

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 ONTAP SMB SVMs to Active Directory domains

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`. Learn more about `up` in the ONTAP command reference.
- 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`

Learn more about `vserver cifs modify` in the [ONTAP command reference](). If you need to reconfigure DNS for the new domain, learn more about `vserver dns modify` in the [ONTAP command reference]().

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 ONTAP SMB 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.

> (i) 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.
```

ONTAP 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`

Learn more about `vserver cifs` in the [ONTAP command reference](#).

Related information

[What happens to local users and groups when deleting SMB servers](#)

Enable the ONTAP SMB 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

Learn about the ONTAP SMB requirements for 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. The SMB license is included with ONTAP One. If
you don't have ONTAP One and the license is not installed, contact your sales representative.

SMB protocol version requirements

- For SVMs, ONTAP supports IPv6 on all versions of the SMB protocol.

> (i) NetBIOS name service (NBNS) over IPv6 is not supported.

Learn about support for IPv6 with ONTAP 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 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.

ⓘ | 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

Learn how ONTAP SMB 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.

> (i) 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.

> (i) NIS name services are used for storing and managing UNIX user, group, netgroup, and host name objects.

Related information

- Enable IPv6 for servers
- Monitor and display information about IPv6 sessions

Enable IPv6 for ONTAP SMB servers

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`

   IPv6 is enabled. IPv6 data LIFs for SMB access can be configured.

Related information

- Monitor and display information about IPv6 sessions
- Visualize the network using System Manager
- Enabling IPv6 on the cluster
- network options ipv6 modify

Learn about disabling IPv6 for ONTAP SMB servers

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.

Related information

- Visualize the ONTAP network using System Manager

Monitor and display information about IPv6 ONTAP 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

Learn about ONTAP SMB security styles and their effects

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.

The `show-effective-permissions` parameter with 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. Learn more about `vserver security file-directory show-effective-permissions` in the ONTAP command reference.

> (i) 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.

Related information

- ONTAP command reference

Learn about where and when to set ONTAP SMB 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 SMB security styles to use on ONTAP 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.

Learn about ONTAP SMB security style inheritance

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.

Learn about preserving UNIX permissions for ONTAP SMB FlexVol volumes

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.

Learn about managing UNIX permissions using the Windows Security tab for ONTAP SMB servers

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 SMB security styles on ONTAP 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 SMB security styles on ONTAP 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 SMB security styles on ONTAP 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

Learn about creating and managing ONTAP SMB data volumes in NAS namespaces

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 ONTAP SMB 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.

> (i) 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. Learn more about `volume create` in the ONTAP command reference.

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 ONTAP SMB 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. Learn more about `volume create` in the [ONTAP command reference](#).

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 ONTAP SMB 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 take a volume offline, 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.

(i) To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must take the volume offline, 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 take a volume offline, 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 *svm_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 take offline 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 ONTAP SMB 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

Learn about ONTAP SMB name mappings configuration

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.

Learn about ONTAP SMB name mapping

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.

Learn about ONTAP SMB 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. (i) 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.

Learn about ONTAP SMB 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 ONTAP SMB 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). Learn more about `vserver name-mapping create` in the ONTAP command reference.

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 ONTAP SMB 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`

ONTAP commands for managing SMB 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`

Learn more about `vserver name-mapping` in the ONTAP command reference.

Configure multidomain name-mapping searches

Enable or disable ONTAP SMB 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 server options

Reset and rediscover trusted ONTAP SMB 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

Display information about discovered trusted domains

Display information about discovered trusted ONTAP SMB 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

Reset and rediscover trusted domains

Add, remove, or replace trusted ONTAP SMB domains in preferred 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

Display information about the preferred trusted domain list

Display information about the preferred trusted ONTAP SMB 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

Add, remove, or replace trusted domains in preferred lists

Create and configure SMB shares

Learn about creating and configuring ONTAP SMB shares

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

- Learn about local users and groups
- SMB configuration for Microsoft Hyper-V and SQL Server
- Configure character mapping for file name translation on volumes

Learn about the default administrative ONTAP SMB shares

When you create a CIFS server on your storage virtual machine (SVM), 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:

> (i) Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

- ipc$
- admin$ (ONTAP 9.7 and earlier only)
- 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 (ONTAP 9.7 and earlier only)

  > (i) Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

  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

Configure advanced file permissions using the Windows Security tab

Learn about ONTAP 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.

- For ONTAP 9.7 and earlier, the admin$, ipc$, and c$ administrative shares are automatically created on every CIFS server and are reserved share names. Beginning with ONTAP 9.8, the admin$ share is no longer automatically created.

- 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:

  ```
  ** [ ] " / \ : ; | < > , ? * =
  ```

Learn about ONTAP SMB 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

Learn about using ONTAP SMB share properties

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 snapshots can be viewed and traversed by clients.

Share properties	Description
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.
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 existing ONTAP SMB shares

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 shares

Optimize ONTAP 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

Create shares with the force-group share setting

Create ONTAP SMB shares 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 user access with the force-group share setting

View information about ONTAP 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>
```

ONTAP 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`

Learn more about `vserver cifs` in the ONTAP command reference.

Secure file access by using SMB share ACLs

Learn about managing ONTAP 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.

By default, the share-level ACL gives full control to the standard group named Everyone. Full control in the

ACL means that all users in the domain and all trusted domains have full access to the share. You can control the level of access for a share-level ACL by using the Microsoft Management Console (MMC) on a Windows client or the ONTAP command line. Create share access control lists.

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 ONTAP 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>`

If you want to configure ACLs by using a…	Enter the command…
Windows group	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\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 "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 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
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 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      Tiger Team          windows    Change
vs1              datavol5      Sue Chang           windows    Full_Control
```

ONTAP 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 for ONTAP SMB SVMs

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

- Create NTFS security descriptors on servers
- Display information about file security on NTFS security-style volumes
- Display information about file security on mixed security-style volumes
- Display information about file security on UNIX security-style volumes

ONTAP commands for SMB NTFS file permissions

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.

Steps

1. Create an NTFS security descriptor.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. Add DACLs to the NTFS security descriptor.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Create a file/directory security policy.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

Learn about UNIX file permissions providing access control when accessing files over ONTAP SMB servers

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)

Learn about DAC file access security for ONTAP SMB servers

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

- Learn about supported GPOs
- Learn about applying Group Policy Objects to SMB servers
- Enable or disable GPO support on servers
- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules
- Configure central access policies to secure data on servers
- Display information about security for servers
- SMB and NFS auditing and security tracing

Supported DAC functionality for ONTAP SMB servers

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 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.

Functionality	Comments
Conditional expressions to file access checks	When modifying the security parameters of a file, users can 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.

Learn about using DAC and central access policies with ONTAP SMB 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 DAC for ONTAP SMB servers

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.

You can find information about how to configure Dynamic Access Control on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Dynamic Access Control Scenario Overview

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

Configure central access policies to secure data on servers

Manage ACLs containing DAC ACEs when DAC is disabled on ONTAP SMB servers

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 ONTAP SMB 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 find information about how to configure central access policies on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Central Access Policy Scenario

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

- Learn about applying Group Policy Objects to SMB servers
- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules
- Enable or disable DAC for servers

Display information about DAC security for ONTAP SMB servers

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`

If you want to display information…	Enter the following command…
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

- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules

Revert considerations for DAC on ONTAP SMB servers

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.

Secure SMB access using export policies

Learn about using export policies with ONTAP SMB access

If export policies for SMB access are enabled on the SMB 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 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)

Learn about configuring and managing export policies.

Learn about ONTAP SMB export rules

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 ONTAP 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 ONTAP 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.

> ⓘ Enabling export policies for CIFS/SMB in an NFS-enabled SVM allows a Linux client to use the `showmount -e` command on the SVM to view the junction paths of all SMB volumes with associated export policy rules.

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

Learn about secure ONTAP SMB 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

Configuration workflow for Storage-Level Access Guard on ONTAP SMB servers

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.

```
Create a security descriptor.
        │
        ▼
Optional: Remove unwanted default DACL
              entries.
        │
        ▼
Add new DACL entries to the security descriptor.
        │
        ▼
Add new SACL entries to the security descriptor.
        │
        ▼
Verify that DACL and SACL entries are correct.
        │
        ▼
Create a security policy.
        │
        ▼
Add a task to the security policy with the access-
control type set to SLAG and with the NTFS
security descriptor created above.
        │
        ▼
Apply the security policy.
        │
        ▼
Verify that the applied SLAG security settings are
                  correct.
```

Related information

[Configure Storage-Level Access Guard on servers](#)

Configure Storage-Level Access Guard on ONTAP SMB servers

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

- Commands for managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard
- Configuration workflow for Storage-Level Access Guard on servers
- Display information about Storage-Level Access Guard on servers
- Remove Storage-Level Access Guard on servers

Effective SLAG matrix on ONTAP SMB servers

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**	**Qtree SLAG in an AFS**	**Qtree SLAG in a snapshot**
Volume access in an Access File System (AFS)	YES	NO	N/A	N/A
Volume access in a snapshot	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 a snapshot (when SLAG is present in the qtree AFS)	NO	NO	YES	NO
Qtree access in a snapshot (when SLAG is not present in the qtree AFS)	YES	NO	NO	NO

Display information about Storage-Level Access Guard on ONTAP SMB servers

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 on ONTAP SMB servers

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

Learn about local ONTAP SMB users and groups

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 ONTAP SMB 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

- [Learn about local user authentication](#)
- [List of supported privileges](#)

Learn about local ONTAP SMB user authentication

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

Enable or disable local user authentication on servers

Learn about ONTAP SMB user access tokens

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.

Learn about using SnapMirror on ONTAP SMB 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.

Learn the effects of deleting ONTAP SMB servers on users and groups

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.

Learn how to use Microsoft Management Console with local ONTAP SMB 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.

Learn about reverting ONTAP SMB clusters

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 ONTAP SMB 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 auditing This includes viewing, dumping, and clearing the security log.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators,` `BUILTIN\Backup Operators,` `BUILTIN\Power Users,` `BUILTIN\Users, Everyone`	Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

Related information

- Learn about assigning privileges
- Learn about configuring bypass traverse checking

Learn about assigning ONTAP SMB 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

- Add privileges to local or domain users or groups
- Remove privileges from local or domain users or groups
- Reset privileges for local or domain users and groups
- Learn about configuring bypass traverse checking

Learn about BUILTIN groups and local administrator accounts on ONTAP SMB servers

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 ONTAP SMB 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:

    ```
    ~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
    ```

Related information

- Configure password complexity for local users
- Display information about server security settings
- Change local user account passwords

Predefined BUILTIN groups and default ONTAP SMB 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

• Learn about BUILTIN groups and local administrator accounts on servers

- List of supported privileges

- Learn about configuring bypass traverse checking

Enable or disable local users and groups functionality

Learn about local ONTAP SMB users and groups functionality

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 on ONTAP SMB servers

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`
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 on servers
- Enable or disable local user accounts

Enable or disable local user authentication on ONTAP SMB servers

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

- Learn about local user authentication
- Enable or disable local users and groups on servers

Manage local user accounts

Modify local ONTAP SMB 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.
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}`

If you want to…	Enter the command…
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 ONTAP SMB 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`
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 ONTAP SMB 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

Configure password complexity for local users

Display information about server security settings

Display information about ONTAP SMB 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. Learn more about `vserver cifs` in the ONTAP command reference.

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 ONTAP SMB 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`
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 ONTAP SMB 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 ONTAP SMB 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 ONTAP SMB 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. Learn more about `vserver cifs` in the [ONTAP command reference](#).

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 ONTAP SMB 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

Display information about members of local groups

Display ONTAP SMB 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 local ONTAP SMB groups

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 ONTAP SMB 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`
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 ONTAP SMB 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 ONTAP SMB 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 ONTAP SMB 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 ONTAP SMB 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. Learn more about `vserver cifs users-and-groups privilege show` in the ONTAP command reference.

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

Learn about configuring ONTAP SMB bypass traverse checking

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.

> (i) 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 file name translation on volumes
- Create share access control lists
- Secure file access by using Storage-Level Access Guard
- List of supported privileges
- Add privileges to local or domain users or groups

Allow users or groups to bypass ONTAP SMB 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

Disallow users or groups from bypassing directory traverse checking

Disallow users or groups from bypassing ONTAP SMB 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

Allow users or groups to bypass directory traverse checking

Display information about file security and audit policies

Learn about viewing ONTAP SMB file security and audit policies

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

- Learn about secure file access by using Storage-Level Access Guard
- Display information about Storage-Level Access Guard on servers

Display information about ONTAP SMB 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

- Display information about file security on mixed security-style volumes
- Display information about file security on UNIX security-style volumes

Display information about ONTAP SMB 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

- Display information about file security on NTFS security-style volumes
- Display information about file security on UNIX security-style volumes

Display information about ONTAP SMB 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

ONTAP commands to display information about NTFS audit policies on SMB FlexVol volumes

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
```

ONTAP commands to display information about NFSv4 audit policies on SMB FlexVol volumes

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
```

Learn how to display ONTAP SMB file security and audit policies information

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

ONTAP commands for managing SMB NTFS file security, NTFS audit policies, and Storage-Level Access Guard

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

- Learn about viewing file security and audit policies
- Create NTFS security descriptors on servers
- Commands to configure and apply audit policies to files and folders
- Learn about secure file access by using Storage-Level Access Guard

ONTAP commands to set SMB 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

Learn about the limits when using ONTAP commands to set SMB 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.

Use security descriptors to apply ONTAP SMB 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

- SMB and NFS auditing and security tracing
- Commands to configure and apply audit policies to files and folders

Learn about applying file-directory policies that use local SMB users or groups on the ONTAP 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 NTFS security descriptors on ONTAP SMB servers

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. Learn more in the ONTAP command reference.

Add NTFS DACL access control entries to NTFS security descriptors on ONTAP SMB servers

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)

> (i) 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. Learn more about the commands described in this procedure in the ONTAP command reference.

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
   ```

Learn more about `vserver security file-directory ntfs dacl` in the ONTAP command reference.

Create ONTAP SMB 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 tasks to the ONTAP SMB 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. Learn more about the commands described in this procedure in the ONTAP command reference.

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
   ```

Learn more about `vserver security file-directory policy task` in the ONTAP command reference.

Apply ONTAP SMB 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).

> ⓘ When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. When a security policy and its associated DACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

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 ONTAP SMB security policy jobs

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
   ```

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

ONTAP commands to configure and apply SMB audit policies to NTFS files and folders

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

- Learn about secure file access by using Storage-Level Access Guard
- Learn about the limits when using commands to set SMB file and folder security
- Use security descriptors to apply file and folder security
- SMB and NFS auditing and security tracing
- Create NTFS security descriptors on servers

Create NTFS security descriptors on ONTAP SMB servers

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

Object	Access type	Access rights	Where to apply the permissions
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. Learn more about the commands described in this procedure in the ONTAP command reference.

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 NTFS security descriptors on ONTAP SMB servers

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 ONTAP SMB 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 tasks to the ONTAP SMB 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. Learn more about the commands described in this procedure in the ONTAP command reference.

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
   ```

Learn more about `vserver security file-directory policy task` in the [ONTAP command reference](#).

Apply ONTAP SMB security policies

Applying an audit 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).

> ⓘ When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. When a security policy and its associated DACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

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 ONTAP SMB security policy jobs

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 ONTAP SMB audit policies

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
```

Learn about managing ONTAP SMB 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.

ONTAP commands for managing NTFS security descriptors on SMB servers

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`

Learn more about `vserver security file-directory ntfs` in the ONTAP command reference.

ONTAP commands for managing NTFS DACL access control entries on SMB servers

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`

Learn more about `vserver security file-directory ntfs dacl` in the ONTAP command reference.

ONTAP commands for managing NTFS SACL access control entries on SMB servers

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`

Learn more about `vserver security file-directory ntfs sacl` in the ONTAP command reference.

ONTAP commands for managing SMB 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`

Learn more about `vserver security file-directory policy` in the ONTAP command reference.

ONTAP commands for managing SMB 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`

Learn more about `vserver security file-directory policy task` in the ONTAP command reference.

ONTAP commands for managing SMB 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`

Learn more about `vserver security file-directory job` in the ONTAP command reference.

Configure the metadata cache for SMB shares

Learn about ONTAP SMB metadata caching

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 ONTAP 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

- Configure the lifetime of metadata cache entries
- Add or remove share properties on existing shares

Configure the lifetime of ONTAP 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. Learn more about `vserver cifs share` in the ONTAP command reference.

Manage file locks

Learn about ONTAP SMB 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.
- Unlink
  - For NTFS filesystems, SMB and CIFS delete operations are supported.

    The file will be removed after the last close.

  - NFS unlink operations are not supported.

    It is not supported because NTFS and SMB semantics are required, and the Last Delete-On-Close operation is not supported for NFS.

  - For UNIX filesystems, unlink operation is supported.

    It is supported because NFS and UNIX semantics are required.

- Rename
  - For NTFS filesystems, if the destination file is opened from SMB or CIFS, the destination file can be renamed.
  - NFS rename is not supported.

    It is not supported because NTFS and SMB semantics are required.

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.

Learn about ONTAP SMB 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.

The read-only bit interacts with the ACL and Unix mode bits in the following ways:

When the read-only bit is set on a file:

- No changes are made to the ACL for that file. NFS clients will see the same ACL as before the read-only bit was set.
- Any Unix mode bits that allow write access for the file are ignored.
- Both NFS and SMB clients can read the file, but they cannot modify it.
- ACLs and UNIX mode bits are ignored in favor of the read-only bit. This means that even if the ACL allows write access, the read-only bit prevents modifications.

When the read-only bit is not set on a file:

- ONTAP determines access based on the ACL and UNIX mode bits.
  - If either the ACL or the UNIX mode bits deny write access, then NFS and SMB clients cannot modify the file.
  - If neither the ACL nor UNIX mode bits deny write access, then NFS and SMB clients can modify the file.

> ⓘ 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 in 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 ONTAP SMB 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. Learn more about `vserver locks show` in the ONTAP command reference.

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 ONTAP SMB 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. Learn
more about `vserver locks break` in the ONTAP command reference.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

   Learn more about `vserver locks show` in the ONTAP command reference.

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`

Learn more about the commands described in this procedure in the ONTAP command reference.

Monitor SMB activity

Display ONTAP 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`
On a specified connection ID	`vserver cifs session show -vserver vserver_name -connection-id integer`

If you want to display SMB session information…	Enter the following command…
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}` (i) 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 ONTAP 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. Learn more about `vserver cifs session file show` in the ONTAP command reference.

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

Display session information

Determine which statistics, objects, and counters are available on ONTAP SMB servers

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`

Learn more about `statistics catalog object show`, including which objects and counters are available, in the ONTAP command reference.

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

- Display statistics
- statistics catalog counter show object

- statistics start

Display ONTAP SMB 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.

Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

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`

Learn more about `statistics show` in the ONTAP command reference.

3. Return to the admin privilege level: `set -privilege admin`

Related information

- Determine which statistics, objects, and counters are available on servers
- Monitoring SMB signed session statistics
- Display BranchCache statistics
- Use 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

Learn about using offline files to allow caching of ONTAP SMB files for offline use

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

-
-
-
-

Learn about requirements for using offline ONTAP SMB 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 ONTAP SMB 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 snapshots under the `~snapshot` folder in the user's home directory.

Windows clients cache all of the snapshots 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 snapshots in the `~snapshot` folder contain all data on the volume at the point at which ONTAP created the snapshot. 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.

ONTAP commands to configure offline SMB file support

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}`
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

Add or remove share properties on existing shares

Configure offline files support on ONTAP 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

Learn about using roaming profiles to store ONTAP SMB user profiles centrally

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
- Learn about using offline files to allow caching of files for offline use
- Learn about using folder redirection to store data on servers

Learn about requirements for using roaming ONTAP SMB 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 ONTAP SMB profiles through the Active Directory Users and Computers MMC

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, 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 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

Learn about using folder redirection to store data on ONTAP SMB servers

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

- Learn about 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

Learn about requirements for using ONTAP SMB 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 ONTAP SMB folder redirection using Windows Properties

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/

Learn about accessing the ONTAP ~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 snapshots.

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 snapshots within the `~snapshot` directory, even when manually entering the path to the `~snapshot` directory or to specific snapshots 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

Learn about recovering ONTAP SMB files and folders using previous versions

The ability to use Microsoft Previous Versions is applicable to file systems that support snapshots in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from snapshots from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the snapshots or to restore data from a snapshot without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made snapshots 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 snapshots is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshots 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.

ONTAP SMB 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 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 snapshots, 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 settings

To use Previous Versions to access data in snapshots, an enabled snapshot policy must be associated to the volume containing the data, clients must be able to access to the snapshot data, and snapshots must exist.

View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in snapshots 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 snapshots of data stored on the SVM if the administrator has enabled snapshots on the volume containing the share, and if the administrator configures the share to show snapshots.

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 snapshots 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 snapshots of the selected file or folder is displayed in the Folder versions: box. The listed snapshots are identified by the snapshot 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	Click **Open**.
Create a copy of data from that snapshot	Click **Copy**.

   Data in snapshots 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 ONTAP SMB snapshots are available for Previous Versions use

You can view snapshots 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 snapshots. Determining snapshot 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 snapshots 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 snapshots.

2. Determine whether the associated snapshot policy is enabled: `volume snapshot policy show -policy policy-name`

3. List the available snapshots: `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 snapshots 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

- Create snapshot configurations to enable Previous Versions access
- Data protection

Create ONTAP SMB snapshot configurations to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to snapshots is enabled and provided that snapshots exist. If your snapshot configuration does not meet these requirements, you can create a snapshot 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.

   Learn more about `volume modify` in the [ONTAP command reference](#).

2. Enable access to the snapshots by using the `volume modify` command to set the `-snap-dir` option to `true`.

   Learn more about `volume modify` in the [ONTAP command reference](#).

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.

   Learn more about `volume show` and `volume snapshot policy show` in the [ONTAP command reference](#).

   For more information about configuring and managing snapshot policies and snapshot schedules, see [Data Protection](#).

Related information

[Data protection](#)

Learn about restoring Previous Versions directories that contain ONTAP SMB 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

Learn about enabling dynamic home directories on ONTAP SMB servers

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. Learn more about `vserver cifs home-directory search-path add` in the ONTAP command reference.

- **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 ONTAP SMB home directory shares

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

- Add home directory search paths

- Requirements and guidelines for using automatic node referrals on servers

- Manage accessibility to user home directories

Learn about unique ONTAP SMB user name requirements for home directory shares

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.

Learn about what happens to static ONTAP SMB 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 ONTAP SMB home directory search paths

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

Add home directory shares

Create ONTAP SMB home directory configurations 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

- Configure home directories using the %u variable
- Learn about additional home directory configurations
- Display information about user home directory paths

Configure ONTAP SMB 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*.

   > (i) 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*.

   > (i) 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.

   > (i) 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`

   > (i) 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

- Create home directory configurations using the %w and %d variables
- Learn about additional home directory configurations
- Display information about user home directory paths

Learn about additional ONTAP SMB 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`

ONTAP commands for managing SMB 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`

Learn more about `vserver cifs home-directory search-path` in the ONTAP command reference.

Display information about ONTAP SMB user home directory paths

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

Manage accessibility to user home directories

Manage accessibility to ONTAP SMB user 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

Display information about user home directory paths

Configure SMB client access to UNIX symbolic links

Learn about providing ONTAP 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. The option to enable the information is configurable on a per-protocol version basis because not all SMB clients support widelinks. This allows administrators to accommodate both supported and unsupported SMB clients. You must enable the option `-widelink-as-reparse-point-versions` for each client protocol that accesses the share using widelinks; the default is SMB1.

Related information

- Windows backup applications and Unix-style symlinks

- Microsoft Documentation: Reparse Points

Limits when configuring UNIX symbolic links for ONTAP 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

Create symbolic link mappings for shares

Control automatic DFS advertisements on ONTAP SMB servers

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 ONTAP 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

[Create symbolic link mappings for shares](#)

Create symbolic link mappings for ONTAP 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

Configure UNIX symbolic link support on shares

ONTAP commands for managing SMB 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`

Learn more about `vserver cifs symlink` in the [ONTAP command reference](#).

Windows backup applications and Unix-style symlinks on ONTAP SMB servers

When a backup application running on Windows encounters a Unix-style symbolic link (symlink), the link is followed and the data is backed up. Beginning with ONTAP 9.15.1, you have the option of backing up the symlinks instead of the data. This feature is fully supported with ONTAP FlexGroup volumes and FlexVols.

Overview

Before you change how ONTAP handles symlinks during a Windows backup operation, you should be familiar with the benefits, key concepts, and configuration options.

Benefits

When this feature is disabled or unavailable, each symlink is traversed and the data it links to is backed up. Because of this, unnecessary data can sometimes be backed up and in certain situations the application might end up in a loop. Backing up the symlinks instead avoids these issues. And because the symlink files are very small compared to the data in most cases, the backups take less time to complete. The overall performance of the cluster can also improve because of the reduced IO operations.

Windows server environment

This feature is supported for backup applications running on Windows. You should understand the relevant technical aspects of the environment before using it.

Extended attributes

Windows supports extended attributes (EA) which collectively form additional metadata optionally associated with the files. These attributes are used by various applications, such as the Windows Subsystem for Linux as described at [File Permissions for WSL](#). Applications can request extended attributes for each file when reading data from ONTAP.

The symlinks are returned in the extended attributes when the feature is enabled. Therefore a backup application must provide standard EA support which is used to store the metadata. Some Windows utilities support and preserve the extended attributes. However, if the backup software does not support backing up and restoring the extended attributes, it will not preserve the metadata associated with each file and fail to process the symlinks properly.

Windows configuration

Backup applications running on a Microsoft Windows server can be granted a special privilege allowing them to bypass normal file security. This is typically done by adding the applications to the Backup Operators group. The apps can then back up and restore files as needed as well as perform other related system operations. There are subtle changes to the SMB protocol used by the backup applications which can be detected by ONTAP as the data is read and written.

Requirements

The symlink backup feature has several requirements including:

- Your cluster is running ONTAP 9.15.1 or later.
- A Windows backup application that has been granted special backup privileges.

- The backup application must also support extended attributes and request them during the backup operations.
- The ONTAP symlink backup feature is enabled for the applicable data SVM.

Configuration options

In addition to the ONTAP CLI, you can also manage this feature using the REST API. See What's new with the ONTAP REST API and automation for more information. The configuration determining how ONTAP processes the Unix-style symlinks must be performed separately for each SVM.

Enable the symlink backup feature in ONTAP

A configuration option has been introduced to an existing CLI command with ONTAP 9.15.1. You can use this option to enable or disable Unix-style symlink processing.

Before you begin

Review the basic Requirements. In addition:

- Be able to elevate your CLI privilege to the advanced level.
- Determine the data SVM you want to modify. The SVM `vs1` is used in the example command.

Steps

1. Set the advanced privilege level.

```
set privilege advanced
```

2. Enable symlink file backup.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Use BranchCache to cache SMB share content at a branch office

Learn about using BranchCache to cache ONTAP SMB share content at a branch office

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

Learn about using offline files to allow caching of files for offline use

Requirements and guidelines

Learn about ONTAP SMB 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/

Learn about ONTAP SMB 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.

Learn about ONTAP SMB 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

Learn about the reasons ONTAP SMB 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.

Learn about choosing the ONTAP SMB 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 servers
- Modify BranchCache configurations on shares

Learn about ONTAP SMB 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 snapshots and SnapMirror destinations.

Configure BranchCache

Learn about ONTAP SMB BranchCache configuration

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 ONTAP SMB 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 SMB server must be configured. The SMB license is included with ONTAP One. If you don't have ONTAP One and the license is not installed, contact your sales representative.
- 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 ONTAP SMB servers

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.
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

- Learn about BranchCache version support
- Learn about configuring BranchCache at the remote office
- Create a BranchCache-enabled SMB share
- Enable BranchCache on existing shares
- Modify BranchCache configurations on shares
- Learn about disabling BranchCache on shares
- Delete the BranchCache configuration on shares

Learn about configuring BranchCache at the remote office in ONTAP SMB

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

Learn about configuring BranchCache-enabled ONTAP SMB shares

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 BranchCache-enabled ONTAP SMB shares

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.

- Learn more about `vserver cifs share create` in the ONTAP command reference.

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

[Disable BranchCache on a single share](#)

Enable BranchCache on existing ONTAP SMB shares

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.
  Learn more about `vserver cifs share properties add` in the ONTAP command reference.

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

- [Add or remove share properties on existing shares](#)
- [Disable BranchCache on a single share](#)

Manage and monitor the BranchCache configuration

Modify BranchCache configurations on ONTAP SMB shares

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 on ONTAP SMB shares

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 ONTAP SMB 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

Learn about the reasons ONTAP invalidates BranchCache hashes

Pre-compute BranchCache hashes on specified ONTAP SMB 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.

  Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

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.

   Learn more about `statistics show` in the ONTAP command reference.

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 ONTAP SMB 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 ONTAP SMB 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.

   ```
   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....
```

Learn more about `statistics catalog counter show` in the [ONTAP command reference](#).

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
```

Learn more about `statistics start` and `statistics stop` in the [ONTAP command reference](#).

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
```

Learn more about `statistics show` in the [ONTAP command reference](#).

5. Return to the admin privilege level: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Related information

- [Display statistics](#)
- [Performance monitoring setup](#)
- [statistics start](#)
- [statistics stop](#)

Learn about ONTAP SMB 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

Learn about applying Group Policy Objects to SMB servers

Display information about ONTAP SMB 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.

   > (i) 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. ``

> (i) 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

- Enable or disable GPO support on servers
- vserver cifs group-policy show-defined
- vserver cifs group-policy show-applied

Disable BranchCache on SMB shares

Learn about disabling BranchCache on ONTAP SMB shares

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

Learn about configuring BranchCache-enabled shares

Disable BranchCache on a single ONTAP 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 ONTAP 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

Learn what happens when you disable or reenable BranchCache on ONTAP SMB servers

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 on ONTAP SMB shares

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

Learn what happens when you delete the BranchCache configuration on ONTAP SMB shares

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 on ONTAP SMB shares

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
```

Learn what happens to ONTAP SMB 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

Delete the BranchCache configuration on shares

Improve Microsoft remote copy performance

Learn about Microsoft remote copy performance improvements on ONTAP SMB servers

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

- Learn about improving client response time by providing automatic node referrals with Auto Location
- SMB configuration for Microsoft Hyper-V and SQL Server

Learn about ODX on ONTAP SMB servers

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.

> (i) 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:
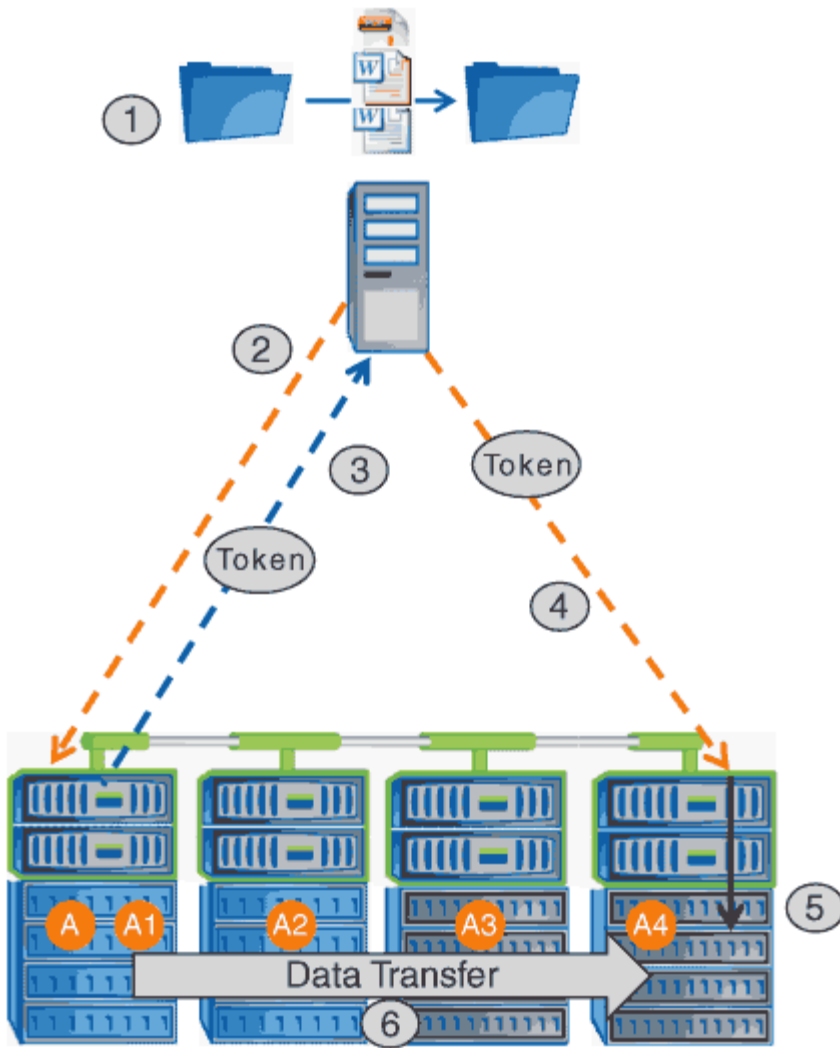
1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.

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 on ONTAP SMB servers

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.

The [NetApp Interoperability Matrix](#)contains the latest information about supported Windows clients.

Volume requirements

- Source volumes must be a minimum of 1.25 GB.
- 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 on ONTAP SMB servers

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 snapshots, 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 on ONTAP SMB servers

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 on ONTAP SMB servers

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 server options

Improve client response time by providing SMB automatic node referrals with Auto Location

Learn about improving client response time by providing ONTAP SMB automatic node referrals with Auto Location

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.

> ℹ️ 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 on ONTAP SMB servers

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. The SMB license is included with ONTAP One. If you don't have ONTAP One and the license is not installed, contact your sales representative.

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

- Learn about enabling dynamic home directories on servers
- Network management
- NetApp Interoperability Matrix Tool

Support for ONTAP 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 ONTAP 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 use node referral only when their existing cache timeout expires.

3. Switch to the admin privilege level: `set -privilege admin`

Related information

Use statistics to monitor ONTAP SMB 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
```

Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

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.

Learn more about `statistics show` in the ONTAP command reference.

3. Return to the admin privilege level: `set -privilege admin`

Related information

- Display statistics
- Performance monitoring setup

Monitor client-side ONTAP 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 ONTAP SMB folder security on shares with access-based enumeration

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 ONTAP 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. Learn more about `vserver cifs share create` in the ONTAP command reference.
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

Add or remove share properties on existing shares

Enable or disable access-based enumeration from a Windows client on ONTAP SMB shares

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

Learn about ONTAP 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.

Learn about valid characters for ONTAP SMB file or directory names

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 ONTAP SMB 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.

Learn about creating ONTAP SMB 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`.

Learn about ONTAP SMB 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 {…}`

- In ONTAP 9.6 and earlier, 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.

  If you are using ONTAP 9.7P1 or later, you can modify existing volumes for utf8mb4 with a support request. For more information, see Can the volume language be changed after creation in ONTAP?.

- Beginning with ONTAP 9.8, you can use the `[-language <Language code>]` parameter to change the volume language from *.UTF-8 to utf8mb4. To change the language of a volume, contact NetApp Support.

> ⓘ   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.

> ℹ️ 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 ONTAP 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

Learn about creating and managing data volumes in namespaces

ONTAP 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`

Learn more about `vserver cifs character-mapping` in the ONTAP command reference.

Related information

Configure character mapping for file name translation on volumes