



Manage SMB servers

ONTAP 9

NetApp
April 24, 2024

Table of Contents

- Manage SMB servers 1
 - Modify SMB servers 1
 - Use options to customize SMB servers 2
 - Manage SMB server security settings 10
 - Configure SMB Multichannel for performance and redundancy 42
 - Configure default Windows user to UNIX user mappings on the SMB server 44
 - Display information about what types of users are connected over SMB sessions 47
 - Command options to limit excessive Windows client resource consumption 48
 - Improve client performance with traditional and lease oplocks 49
 - Apply Group Policy Objects to SMB servers 56
 - Commands for managing SMB servers computer account passwords 75
 - Manage domain controller connections 76
 - Use null sessions to access storage in non-Kerberos environments 80
 - Manage NetBIOS aliases for SMB servers 82
 - Manage miscellaneous SMB server tasks 86
 - Use IPv6 for SMB access and SMB services 92

Manage SMB servers

Modify SMB servers

You can move a SMB server from a workgroup to an Active Directory domain, from a workgroup to another workgroup, or from an Active Directory domain to a workgroup by using the `vserver cifs modify` command.

About this task

You can also modify other attributes of the SMB server, such as the SMB server name and administrative status. See the man page for details.

Choices

- Move the SMB server from a workgroup to an Active Directory domain:

- a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Move the SMB server from the workgroup to an Active Directory domain: `vserver 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` container within the `example.com` domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

- Move the SMB server from a workgroup to another workgroup:

- a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modify the workgroup for the SMB server: `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Move the SMB server from an Active Directory domain to a workgroup:

- a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Move the SMB server from the Active Directory domain to a workgroup: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



To enter workgroup mode, all domain-based features must be disabled and their configuration removed automatically by the system, including continuously-available shares, shadow copies, and AES. However, domain-configured share ACLs such as "EXAMPLE.COM\userName" will not work properly, but cannot be removed by ONTAP. Remove these share ACLs as soon as possible using external tools after the command completes. If AES is enabled, you may be asked to supply the name and password of a Windows account with sufficient privileges to disable it in the "EXAMPLE.COM" domain.

- Modify other attributes by using the appropriate parameter of the `vserver cifs modify` command.

Use options to customize SMB servers

Available SMB server options

It is useful to know what options are available when considering how to customize the SMB server. Although some options are for general use on the SMB server, several are used to enable and configure specific SMB functionality. SMB server options are controlled with the `vserver cifs options modify` option.

The following list specifies the SMB server options that are available at the admin privilege level:

- **Configuring the SMB session timeout value**

Configuring this option enables you to specify the number of seconds of idle time before an SMB session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.

- **Configuring the default UNIX user**

Configuring this option enables you to specify the default UNIX user that the SMB server uses. ONTAP automatically creates a default user named "pcuser" (with a UID of 65534), creates a group named "pcuser" (with a GID of 65534), and adds the default user to the "pcuser" group. When you create a SMB server, ONTAP automatically configures "pcuser" as the default UNIX user.

- **Configuring the guest UNIX user**

Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the SMB

server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the SMB server.

- **Enabling or disabling read grant execution for mode bits**

Enabling or disabling this option enables you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

- **Enabling or disabling the ability to delete read-only files from NFS clients**

Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics does not allow the deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is `disabled`, which results in NTFS delete semantics.

- **Configuring Windows Internet Name Service server addresses**

Configuring this option enables you to specify a list of Windows Internet Name Service (WINS) server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the SMB server options that are available at the advanced privilege level:

- **Granting UNIX group permissions to CIFS users**

Configuring this option determines whether the incoming CIFS user who is not the owner of the file can be granted the group permission. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `true`, then the group permission is granted for the file. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `false`, then the normal UNIX rules are applicable to grant the file permission. This parameter is applicable to UNIX security-style files that have permission set as `mode bits` and is not applicable to files with the NTFS or NFSv4 security mode. The default setting is `false`.

- **Enabling or disabling SMB 1.0**

SMB 1.0 is disabled by default on an SVM for which a SMB server is created in ONTAP 9.3.



Beginning ONTAP 9.3, SMB 1.0 is disabled by default for new SMB servers created in ONTAP 9.3. You should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

- **Enabling or disabling SMB 2.x**

SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, ONTAP also automatically disables SMB 3.X.

SMB 2.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.0**

SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions that support SMB 3.0.

SMB 3.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.1**

Windows 10 is the only Windows version that supports SMB 3.1.

SMB 3.1 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling ODX copy offload**

ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

- **Enabling or disabling the direct-copy mechanism for ODX copy offload**

The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

- **Enabling or disabling automatic node referrals**

With automatic node referrals, the SMB server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share.

- **Enabling or disabling export policies for SMB**

This option is disabled by default.

- **Enabling or disabling using junction points as reparse points**

If this option is enabled, the SMB server exposes junction points to SMB clients as reparse points. This option is valid only for SMB 2.x or SMB 3.0 connections. This option is enabled by default.

This option is supported only on SVMs. The option is enabled by default on SVMs

- **Configuring the number of maximum simultaneous operations per TCP connection**

The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**

This option is enabled by default.

- **Enabling or disabling local Windows users authentication**

This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**

ONTAP uses the shadow copy functionality to perform remote backups of data stored using the Hyper-V over SMB solution.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Configuring the shadow copy directory depth**

Configuring this option enables you to define the maximum depth of directories on which to create shadow copies when using the shadow copy functionality.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Enabling or disabling multidomain search capabilities for name mapping**

If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (*) in the domain portion of the Windows user name (for example, *\\joe), ONTAP searches for the specified user in all of the domains with bidirectional trusts to the home domain. The home domain is the domain that contains the SMB server's computer account.

As an alternative to searching all of the bidirectionally trusted domains, you can configure a list of preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred list is used to perform multidomain name mapping searches.

The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**

Configuring this option enables you to configure the file system sector size in bytes that ONTAP reports to SMB clients. There are two valid values for this option: 4096 and 512. The default value is 4096. You might need to set this value to 512 if the Windows application supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control**

Enabling this option enables you to secure objects on the SMB server by using Dynamic Access Control (DAC), including using auditing to stage central access policies and using Group Policy Objects to implement central access policies. The option is disabled by default.

This option is supported only on SVMs.

- **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**

Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to anonymous users. By default, there are no access restrictions for anonymous users.

- **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**

Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

- **Enabling or disabling the SMB fake open functionality**

Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how ONTAP makes open and close requests when querying for attribute information on files and directories. By default, the SMB fake open functionality is enabled. This option is useful only for connections that are made with SMB 2.x or later.

- **Enabling or disabling the UNIX extensions**

Enabling this option enables UNIX extensions on a SMB server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled.

If you have UNIX-based SMB clients, such as Mac OSX clients, in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the SMB server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

- **Enabling or disabling support for short name searches**

Enabling this option allows the SMB server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is `false`.

- **Enabling or disabling support for automatic advertisement of DFS capabilities**

Enabling or disabling this option determines whether SMB servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that connect to shares. ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the SMB server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the SMB server advertises DFS capabilities only when the clients connect to shares where symbolic link access is enabled.

- **Configuring the maximum number of SMB credits**

Beginning with ONTAP 9.4, configuring the `-max-credits` option allows you to limit the number of credits to be granted on an SMB connection when clients and server are running SMB version 2 or later. The default value is 128.

- **Enabling or disabling support for SMB Multichannel**

Enabling the `-is-multichannel-enabled` option in ONTAP 9.4 and later releases allows the SMB server to establish multiple connections for a single SMB session when appropriate NICs are deployed on the cluster and its clients. Doing so improves throughput and fault tolerance. The default value for this parameter is `false`.

When SMB Multichannel is enabled, you can also specify the following parameters:

- The maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.
- The maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

Configuring SMB server options

You can configure SMB server options at any time after you have created a SMB server on a storage virtual machine (SVM).

Step

1. Perform the desired action:

If you want to configure SMB server options...	Enter the command...
At admin-privilege level	<code>vserver cifs options modify -vserver vserver_name options</code>
At advanced-privilege level	<p>a. <code>set -privilege advanced</code></p> <p>b. <code>vserver cifs options modify -vserver vserver_name options</code></p> <p>c. <code>set -privilege admin</code></p>

For more information about configuring SMB server options, see the man page for the `vserver cifs options modify` command.

Configure the grant UNIX group permission to SMB users

You can configure this option to grant group permissions to access files or directories even if the incoming SMB user is not the owner of the file.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the grant UNIX group permission as appropriate:

If you want to	Enter the command
Enable the access to the files or directories to get group permissions even if the user is not the owner of the file	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Disable the access to the files or directories to get group permissions even if the user is not the owner of the file	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. Verify that the option is set to the desired value: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Return to the admin privilege level: `set -privilege admin`

Configure access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the *null user*) can access certain information on the network. You can use a SMB server option to configure access restrictions for the anonymous user.

About this task

The `-restrict-anonymous` SMB server option corresponds to the `RestrictAnonymous` registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:

Value	Description
no-restriction (default)	Specifies no access restrictions for anonymous users.
no-enumeration	Specifies that only enumeration is restricted for anonymous users.
no-access	Specifies that access is restricted for anonymous users.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the restrict anonymous setting: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level: `set -privilege admin`

Related information

[Available SMB server options](#)

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

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

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the **Security** tab in the Windows Properties box.

You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where ONTAP must preserve UNIX permissions during save operations.
- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.

Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients.

The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.

- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes.

If ONTAP reports the volume as FAT, the application does not try to change an ACL.

Related information

[Configuring security styles on FlexVol volumes](#)

[Configuring security styles on qtrees](#)

Enable or disable the presentation of NTFS ACLs for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

About this task

If you enable this option, ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the UNIX NTFS ACL option setting: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level: `set -privilege admin`

How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX

permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Manage SMB server security settings

How ONTAP handles SMB client authentication

Before users can create SMB connections to access data contained on the SVM, they must be authenticated by the domain to which the SMB server belongs. The SMB server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

Kerberos authentication

ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is the primary authentication service for Active Directory. The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients who want to establish a session with another computer, such as the SMB server, contact a KDC directly to obtain their session credentials.

NTLM authentication

NTLM client authentication is done using a challenge response protocol based on shared knowledge of a user-specific secret based on a password.

If a user creates an SMB connection using a local Windows user account, authentication is done locally by the SMB server using NTLMv2.

Guidelines for SMB server security settings in an SVM disaster recovery configuration

Before creating an SVM that is configured as a disaster recovery destination where the identity is not preserved (the `-identity-preserve` option is set to `false` in the SnapMirror configuration), you should know about how SMB server security settings are managed on the destination SVM.

- Non-default SMB server security settings are not replicated to the destination.

When you create a SMB server on the destination SVM, all SMB server security settings are set to default values. When the SVM disaster recovery destination is initialized, updated, or resynced, the SMB server security settings on the source are not replicated to the destination.

- You must manually configure non-default SMB server security settings.

If you have non-default SMB server security settings configured on the source SVM, you must manually configure these same settings on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Display information about SMB server security settings

You can display information about SMB server security settings on your storage virtual machines (SVMs). You can use this information to verify that the security settings are correct.

About this task

A displayed security setting can be the default value for that object or a non-default value that is configured either by using the ONTAP CLI or by using Active Directory group policy objects (GPOs).

Do not use the `vserver cifs security show` command for SMB servers in workgroup mode, because some of the options are not valid.

Step

1. Perform one of the following actions:

If you want display information about...	Enter the command...
All security settings on a specified SVM	<pre>vserver cifs security show -vserver vserver_name</pre>

If you want display information about...	Enter the command...
A specific security setting or settings on the SVM	<code>vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]</code> You can enter <code>-fields ?</code> 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

Enable or disable required password complexity for local SMB users

Required password complexity provides enhanced security for local SMB users on your storage virtual machines (SVMs). The required password complexity feature is enabled by default. You can disable it and reenable it at any time.

Before you begin

Local users, local groups, and local user authentication must be enabled on the CIFS server.



About this task

You must not use the `vserver cifs security modify` command for a CIFS server in workgroup mode because some of the options are not valid.

Steps

1. Perform one of the following actions:

If you want required password complexity for local SMB users to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required true</code>
Disabled	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity-required false</code>

2. Verify the security setting for required password complexity: `vserver cifs security show -vserver vserver_name`

Example

The following example shows that required password complexity is enabled for local SMB users for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

Related information

[Displaying information about CIFS server security settings](#)

Modify the CIFS server Kerberos security settings

You can modify certain CIFS server Kerberos security settings, including the maximum allowed Kerberos clock skew time, the Kerberos ticket lifetime, and the maximum number of ticket renewal days.

About this task

Modifying CIFS server Kerberos settings by using the `vserver cifs security modify` command modifies the settings only on the single storage virtual machine (SVM) that you specify with the `-vserver` parameter. You can centrally manage Kerberos security settings for all SVMs on the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

Steps

- 1. Perform one or more of the following actions:

If you want to...	Enter...
Specify the maximum allowed Kerberos clock skew time in minutes (9.13.1 and later) or seconds (9.12.1 or earlier).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>The default setting is 5 minutes.</p>
Specify the Kerberos ticket lifetime in hours.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>The default setting is 10 hours.</p>
Specify the maximum number of ticket renewal days.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>The default setting is 7 days.</p>
Specify the timeout for sockets on KDCs after which all KDCs are marked as unreachable.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>The default setting is 3 seconds.</p>

- 2. Verify the Kerberos security settings:

```
vserver cifs security show -vserver vserver_name
```


Example

The following example makes the following changes to Kerberos security: “Kerberos Clock Skew” is set to 3 minutes and “Kerberos Ticket Age” is set to 8 hours for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:                3 minutes
                Kerberos Ticket Age:                  8 hours
                Kerberos Renewal Age:                  7 days
                Kerberos KDC Timeout:                  3 seconds
                Is Signing Required:                    false
    Is Password Complexity Required:                    true
    Use start_tls For AD LDAP connection:                false
                Is AES Encryption Enabled:              false
                LM Compatibility Level: lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:              false
```

Related information

[Displaying information about CIFS server security settings](#)

[Supported GPOs](#)

[Applying Group Policy Objects to CIFS servers](#)

Set the SMB server minimum authentication security level

You can set the SMB server minimum security level, also known as the *LMCompatibilityLevel*, on your SMB server to meet your business security requirements for SMB client access. The minimum security level is the minimum level of the security tokens that the SMB server accepts from SMB clients.



About this task

- SMB servers in workgroup mode support only NTLM authentication. Kerberos authentication is not supported.
- LMCompatibilityLevel applies only to SMB client authentication, not admin authentication.

You can set the minimum authentication security level to one of four supported security levels.

Value	Description
lm-ntlm-ntlmv2-krb (default)	The storage virtual machine (SVM) accepts LM, NTLM, NTLMv2, and Kerberos authentication security.
ntlm-ntlmv2-krb	The SVM accepts NTLM, NTLMv2, and Kerberos authentication security. The SVM denies LM authentication.
ntlmv2-krb	The SVM accepts NTLMv2 and Kerberos authentication security. The SVM denies LM and NTLM authentication.
krb	The SVM accepts Kerberos authentication security only. The SVM denies LM, NTLM, and NTLMv2 authentication.

Steps

1. Set the minimum authentication security level: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verify that the authentication security level is set to the desired level: `vserver cifs security show -vserver vserver_name`

Related information

[Enabling or disabling AES encryption for Kerberos-based communication](#)

Configure strong security for Kerberos-based communication by using AES encryption

For strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. By default, when you create a SMB server on the SVM, 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 [enable and disable encryption types 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

[Modifying the CIFS server Kerberos security settings](#)

Enable or disable AES encryption for Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you 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	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

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::> vsriver cifs security modify -vsriver 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::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  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	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Disabled	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Verify that AES encryption is enabled or disabled as desired:

```
vsriver cifs security show
-vsriver vsriver_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
```

Use SMB signing to enhance network security

Use SMB signing to enhance network security overview

SMB signing helps to ensure that network traffic between the SMB server and the client is not compromised; it does this by preventing replay attacks. By default, ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the SMB server to require SMB signing.

How SMB signing policies affect communication with a CIFS server

In addition to the CIFS server SMB signing security settings, two SMB signing policies on Windows clients control the digital signing of communications between clients and the CIFS server. You can configure the setting that meets your business requirements.

Client SMB policies are controlled through Windows local security policy settings, which are configured by using the Microsoft Management Console (MMC) or Active Directory GPOs. For more information about client SMB signing and security issues, see the Microsoft Windows documentation.

Here are descriptions of the two SMB signing policies on Microsoft clients:

- Microsoft network client: Digitally sign communications (if server agrees)

This setting controls whether the client’s SMB signing capability is enabled. It is enabled by default. When this setting is disabled on the client, the client communications with the CIFS server depends on the SMB signing setting on the CIFS server.

- Microsoft network client: Digitally sign communications (always)

This setting controls whether the client requires SMB signing to communicate with a server. It is disabled by default. When this setting is disabled on the client, SMB signing behavior is based on the policy setting for Microsoft network client: Digitally sign communications (if server agrees) and the setting on the CIFS server.



If your environment includes Windows clients configured to require SMB signing, you must enable SMB signing on the CIFS server. If you do not, the CIFS server cannot serve data to these systems.

The effective results of client and CIFS server SMB signing settings depends on whether the SMB sessions uses SMB 1.0 or SMB 2.x and later.

The following table summarizes the effective SMB signing behavior if the session uses SMB 1.0:

Client	ONTAP—signing not required	ONTAP—signing required
Signing disabled and not required	Not signed	Signed
Signing enabled and not required	Not signed	Signed
Signing disabled and required	Signed	Signed
Signing enabled and required	Signed	Signed



Older Windows SMB 1 clients and some non-Windows SMB 1 clients might fail to connect if signing is disabled on the client but required on the CIFS server.

The following table summarizes the effective SMB signing behavior if the session uses SMB 2.x or SMB 3.0:



For SMB 2.x and SMB 3.0 clients, SMB signing is always enabled. It cannot be disabled.

Client	ONTAP—signing not required	ONTAP—signing required
Signing not required	Not signed	Signed
Signing required	Signed	Signed

The following table summarizes the default Microsoft client and server SMB signing behavior:

Protocol	Hash algorithm	Can enable/disable	Can require/not require	Client default	Server default	DC default
SMB 1.0	MD5	Yes	Yes	Enabled (not required)	Disabled (not required)	Required
SMB 2.x	HMAC SHA-256	No	Yes	Not required	Not required	Required
SMB 3.0	AES-CMAC.	No	Yes	Not required	Not required	Required



Microsoft no longer recommends using Digitally sign communications (if client agrees) or Digitally sign communications (if server agrees) Group Policy settings. Microsoft also no longer recommends using the EnableSecuritySignature registry settings. These options only affect the SMB 1 behavior and can be replaced by the Digitally sign communications (always) Group Policy setting or the RequireSecuritySignature registry setting. You can also get more information from the Microsoft Blog <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx> [The Basics of SMB Signing (covering both SMB1 and SMB2)]

Performance impact of SMB signing

When SMB sessions use SMB signing, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM containing the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in signed SMB traffic. SMB signing offload is enabled by default when SMB signing is enabled.

Enhanced SMB signing performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance

impact of SMB signing can vary widely; you can verify it only through testing in your network environment.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

Recommendations for configuring SMB signing

You can configure SMB signing behavior between SMB clients and the CIFS server to meet your security requirements. The settings you choose when configuring SMB signing on your CIFS server are dependent on what your security requirements are.

You can configure SMB signing on either the client or the CIFS server. Consider the following recommendations when configuring SMB signing:

If...	Recommendation...
You want to increase the security of the communication between the client and the server	Make SMB signing required at the client by enabling the <code>Require Option (Sign always)</code> security setting on the client.
You want all SMB traffic to a certain storage virtual machine (SVM) signed	Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.

See Microsoft documentation for more information on configuring Windows client security settings.

Guidelines for SMB signing when multiple data LIFS are configured

If you enable or disable required SMB signing on the SMB server, you should be aware of the guidelines for multiple data LIFS configurations for an SVM.

When you configure a SMB server, there might be multiple data LIFs configured. If so, the DNS server contains multiple A record entries for the CIFS server, all using the same SMB server host name, but each with a unique IP address. For example, a SMB server that has two data LIFs configured might have the following DNS A record entries:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

The normal behavior is that upon changing the required SMB signing setting, only new connections from clients are affected by the change in the SMB signing setting. However, there is an exception to this behavior. There is a case where a client has an existing connection to a share, and the client creates a new connection to the same share after the setting is changed, while maintaining the original connection. In this case, both the new and the existing SMB connection adopt the new SMB signing requirements.

Consider the following example:

- 1. Client1 connects to a share without required SMB signing using the path `o:\.`

2. The storage administrator modifies the SMB server configuration to require SMB signing.
3. Client1 connects to the same share with required SMB signing using the path `s:\` (while maintaining the connection using the path `o:\`).
4. The result is that SMB signing is used when accessing data over both the `o:\` and `s:\` drives.

Enable or disable required SMB signing for incoming SMB traffic

You can enforce the requirement for clients to sign SMB messages by enabling required SMB signing. If enabled, ONTAP accepts SMB messages only if they have valid signatures. If you want to permit SMB signing, but not require it, you can disable required SMB signing.

About this task

By default, required SMB signing is disabled. You can enable or disable required SMB signing at any time.



SMB signing is not disabled by default under the following circumstances:

1. Required SMB signing is enabled, and the cluster is reverted to a version of ONTAP that does not support SMB signing.
2. The cluster is subsequently upgraded to a version of ONTAP that supports SMB signing.

Under these circumstances, the SMB signing configuration that was originally configured on a supported version of ONTAP is retained through reversion and subsequent upgrade.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value that you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB signing security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB signing security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled required SMB signing on the source SVM, you must manually enable required SMB signing on the destination SVM.

Steps

1. Perform one of the following actions:

If you want required SMB signing to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Disabled	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

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.

Determine whether SMB sessions are signed

You can display information about connected SMB sessions on the CIFS server. You can use this information to determine whether SMB sessions are signed. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

Steps

1. Perform one of the following actions:

If you want display information about...	Enter the command...
All signed sessions on a specified storage virtual machine (SVM)	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>
Details for a signed session with a specific session ID on the SVM	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

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
ID        ID        Workstation    Windows User    Open    Idle
-----
3151272279 1        10.1.1.1      DOMAIN\joe      2       23s
```

The following command displays detailed session information, including whether the session is signed, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Related information

[Monitoring SMB signed session statistics](#)

Monitor SMB signed session statistics

You can monitor SMB sessions statistics and determine which established sessions are signed and which are not.

About this task

The `statistics` command at the advanced privilege level provides the `signed_sessions` counter that you can use to monitor the number of signed SMB sessions. The `signed_sessions` counter is available with the following statistics objects:

- `cifs` enables you to monitor SMB signing for all SMB sessions.
- `smb1` enables you to monitor SMB signing for SMB 1.0 sessions.
- `smb2` enables you to monitor SMB signing for SMB 2.x and SMB 3.0 sessions.

SMB 3.0 statistics are included in the output for the `smb2` object.

If you want to compare the number of signed session to the total number of sessions, you can compare output for the `signed_sessions` counter with the output for the `established_sessions` counter.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Start a data collection:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id  
sample_ID [-node node_name]
```

If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB signing statistics:

If you want to view information for...	Enter...
Signed sessions	<code>show -sample-id sample_ID -counter signed_sessions node_name [-node node_name]</code>
Signed sessions and established sessions	<code>show -sample-id sample_ID -counter signed_sessions established_sessions n ode_name [-node node_name]</code>

If you want to display information for only a single node, specify the optional `-node` parameter.

5. Return to the admin privilege level:

```
set -privilege admin
```

Examples

The following example shows how you can monitor SMB 2.x and SMB 3.0 signing statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

The following command stops the data collection for the sample:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

The following command shows signed SMB sessions and established SMB sessions by node from the sample:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

The following command shows signed SMB sessions for node2 from the sample:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

The following command moves back to the admin privilege level:

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

Related information

[Determining whether SMB sessions are signed](#)

[Performance monitoring and management overview](#)

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

SMB encryption overview

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on SMB servers. You can also configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create 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.

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
False	False	No encryption is enabled.

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

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

Performance impact of SMB encryption

When SMB sessions use SMB encryption, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM that contains the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in encrypted SMB traffic. SMB encryption offload is enabled by default when SMB encryption is enabled.

Enhanced SMB encryption performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB encryption can vary widely; you can verify it only through testing in your network environment.

SMB encryption is disabled by default on the SMB server. You should enable SMB encryption only on those SMB shares or SMB servers that require encryption. With SMB encryption, ONTAP performs additional processing of decrypting the requests and encrypting the responses for every request. SMB encryption should therefore be enabled only when necessary.

Enable or disable required SMB encryption for incoming SMB traffic

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

About this task

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

Steps

- 1. Perform one of the following actions:

If you want required SMB encryption for incoming SMB traffic on the CIFS server to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -is-smb-encryption -required true</code>
Disabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -is-smb-encryption -required false</code>

- 2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

The `is-smb-encryption-required` field displays `true` if required SMB encryption is enabled on the CIFS server and `false` if it is disabled.

Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on SVM `vs1`:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption -required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-encryption-required
vserver  is-smb-encryption-required
-----  -
vs1      true
```

Determine whether clients are connected using encrypted SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

About this task

SMB clients sessions can have one of three encryption levels:

- `unencrypted`

The SMB session is not encrypted. Neither storage virtual machine (SVM)-level or share-level encryption is configured.

- `partially-encrypted`

Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- `encrypted`

The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

Steps

1. Perform one of the following actions:

If you want display information about...	Enter the command...
Sessions with a specified encryption setting for sessions on a specified SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> {unencrypted partially-encrypted encrypted} -instance</code>
The encryption setting for a specific session ID on a specified SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 2:

```

cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted

```

Monitor SMB encryption statistics

You can monitor SMB encryption statistics and determine which established sessions and share connections are encrypted and which are not.

About this task

The `statistics` command at the advanced privilege level provides the following counters, which you can use to monitor the number of encrypted SMB sessions and share connections:

Counter name	Descriptions
<code>encrypted_sessions</code>	Gives the number of encrypted SMB 3.0 sessions
<code>encrypted_share_connections</code>	Gives the number of encrypted shares on which a tree connect has happened
<code>rejected_unencrypted_sessions</code>	Gives the number of session setups rejected due to a lack of client encryption capability
<code>rejected_unencrypted_shares</code>	Gives the number of share mappings rejected due to a lack of client encryption capability

These counters are available with the following statistics objects:

- `cifs` enables you to monitor SMB encryption for all SMB 3.0 sessions.

SMB 3.0 statistics are included in the output for the `cifs` object. If you want to compare the number of encrypted sessions to the total number of sessions, you can compare output for the `encrypted_sessions` counter with the output for the `established_sessions` counter.

If you want to compare the number of encrypted share connections to the total number of share connections, you can compare output for the `encrypted_share_connections` counter with the output for the `connected_shares` counter.

- `rejected_unencrypted_sessions` provides the number of times an attempt has been made to establish an SMB session that requires encryption from a client that does not support SMB encryption.
- `rejected_unencrypted_shares` provides the number of times an attempt has been made to connect to an SMB share that requires encryption from a client that does not support SMB encryption.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop the data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Start a data collection:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB encryption statistics:

If you want to view information for...	Enter...
Encrypted sessions	<code>show -sample-id <i>sample_ID</i> -counter encrypted_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted sessions and established sessions	<code>show -sample-id <i>sample_ID</i> -counter encrypted_sessions established_sessions <i>node_name</i> [-node <i>node_name</i>]</code>

If you want to view information for...	Enter...
Encrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted share connections and connected shares	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections connected_shares <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted sessions	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share <i>node_name</i> [-node <i>node_name</i>]</code>

If you want to display information only for a single node, specify the optional `-node` parameter.

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

Examples

The following example shows how you can monitor SMB 3.0 encryption statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

The following command stops data collection for that sample:

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

The following command shows encrypted SMB sessions and established SMB sessions by the node from the sample:

```
cluster2::*> statistics show -object cifs -counter  
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

The following command shows the number of rejected unencrypted SMB sessions by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter  
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

The following command shows the number of connected SMB shares and encrypted SMB shares by the node from the sample:


```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

The following command shows the number of rejected unencrypted SMB share connections by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

Related information

[Determining which statistics objects and counters are available](#)

[Performance monitoring and management overview](#)

Secure LDAP session communication

LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session

security on queries to an Active Directory (AD) server. You must configure the CIFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`.

LDAP signing and sealing on CIFS traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

Enable LDAP signing and sealing on the CIFS server

Before your CIFS server can use signing and sealing for secure communication with an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP signing and sealing.

Before you begin

You must consult with your AD server administrator to determine the appropriate security configuration values.

Steps

1. Configure the CIFS server security setting that enables signed and sealed traffic with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -session -security-for-ad-ldap {none|sign|seal}`

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

2. Verify that the LDAP signing and sealing security setting is set correctly: `vserver cifs security show -vserver vserver_name`



If the SVM uses the same LDAP server for querying name-mapping or other UNIX information, such as users, groups, and netgroups, then you must enable the corresponding setting with the `-session-security` option of the `vserver services name-service ldap client modify` command.

Configure LDAP over TLS

Export a copy of the self-signed root CA certificate

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by ONTAP to install the certificate on the storage virtual machine (SVM).

Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library.

Step

1. Obtain a root CA certificate of the domain controller that is in the .pem text format.

Microsoft TechNet Library: technet.microsoft.com

After you finish

Install the certificate on the SVM.

Related information

Microsoft TechNet Library

Install the self-signed root CA certificate on the SVM

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

About this task

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

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

Steps

1. Install the self-signed root CA certificate:
 - a. Begin the certificate installation: `security certificate install -vserver vserver_name -type server-ca`

The console output displays the following message: Please enter Certificate: Press <Enter> when done
 - b. Open the certificate .pem file with a text editor, copy the certificate, including the lines beginning with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----, and then paste the certificate after the command prompt.
 - c. Verify that the certificate is displayed correctly.
 - d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed: `security certificate show -vserver vserver_name`

Enable LDAP over TLS on the server

Before your SMB server can use TLS for secure communication with an Active Directory LDAP server, you must modify the SMB server security settings to enable LDAP over TLS.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory (AD) and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenble LDAP

channel binding with AD servers, use the `-try-channel-binding-for-ad-ldap` parameter with the `vserver cifs security modify` command.

To learn more, see:

- [LDAP overview](#)
- [2020 LDAP channel binding and LDAP signing requirements for Windows](#).

Steps

1. Configure the SMB server security setting that allows secure LDAP communication with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -use-start-tls -for-ad-ldap true`
2. Verify that the LDAP over TLS security setting is set to true: `vserver cifs security show -vserver vserver_name`



If the SVM uses the same LDAP server for querying name-mapping or other UNIX information (such as users, groups, and netgroups), then you must also modify the `-use-start-tls` option by using the `vserver services name-service ldap client modify` command.

Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance.

Before you begin

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- `-max-connections-per-session`

The maximum number of connections allowed per Multichannel session. The default is 32 connections.

If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- **-max-lifs-per-session**

The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable SMB Multichannel on the SMB server: `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. Verify that ONTAP is reporting SMB Multichannel sessions: `vserver cifs session show options`
4. Return to the admin privilege level: `set -privilege admin`

Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s                               Administrator      0
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance
```

```
Vserver: vs1
```

```
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

Configure default Windows user to UNIX user mappings on the SMB server

Configure the default UNIX user

You can configure the default UNIX user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure the default UNIX user.

About this task

By default, the name of the default UNIX user is “pcuser”, which means that, by default, user mapping to the default UNIX user is enabled. You can specify another name to use as the default UNIX user. The name that you specify must exist in the name service databases configured for the storage virtual machine (SVM). If this option is set to a null string, no one can access the CIFS server as a UNIX default user. That is, each user must have an account in the password database before they can access the CIFS server.

For a user to connect to the CIFS server using the default UNIX user account, the user must meet the following prerequisites:

- The user is authenticated.
- The user is in the CIFS server’s local Windows user database, in the CIFS server’s home domain, or in a trusted domain (if multidomain name mapping searches is enabled on the CIFS server).

- The user name is not explicitly mapped to a null string.

Steps

1. Configure the default UNIX user:

If you want to ...	Enter ...
Use the default UNIX user “pcuser”	<code>vserver cifs options modify -default -unix-user pcuser</code>
Use another UNIX user account as the default user	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Disable the default UNIX user	<code>vserver cifs options modify -default -unix-user ""</code>

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verify that the default UNIX user is configured correctly: `vserver cifs options show -vserver vserver_name`

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Configure the guest UNIX user

Configuring the guest UNIX user option means that users who log in from untrusted domains are mapped to the guest UNIX user and can connect to the CIFS server. Alternatively, if you want authentication of users from untrusted domains to fail, you should not configure the guest UNIX user. The default is to not allow users from untrusted domains to connect to the CIFS server (the guest UNIX account is not configured).

About this task

You should keep the following in mind when configuring the guest UNIX account:

- If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database and this option is enabled, the CIFS server considers the user as a guest user and maps the user to the specified UNIX user.
- If this option is set to a null string, the guest UNIX user is disabled.
- You must create a UNIX user to use as the guest UNIX user in one of the storage virtual machine (SVM) name service databases.
- A user logged in as a guest user is automatically is a member of the BUILTIN\guests group on the CIFS server.
- The 'homedirs-public' option applies only to authenticated users. A user logged in as a guest user does not have a home directory and cannot access other users' home directories.

Steps

1. Perform one of the following actions:

If you want to...	Enter...
Configure the guest UNIX user	<code>vserver cifs options modify -guest -unix-user <i>unix_name</i></code>
Disable the guest UNIX user	<code>vserver cifs options modify -guest -unix-user ""</code>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verify that the guest UNIX user is configured correctly: `vserver cifs options show -vserver vserver_name`

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Map the administrators group to root

If you have only CIFS clients in your environment and your storage virtual machine (SVM) was set up as a multiprotocol storage system, you must have at least one Windows

account that has root privilege for accessing files on the SVM; otherwise, you cannot manage the SVM because you do not have sufficient user rights.

About this task

If your storage system was set up as NTFS-only, however, the `/etc` directory has a file-level ACL that enables the administrators group to access the ONTAP configuration files.

Steps

- 1. Set the privilege level to advanced: `set -privilege advanced`
- 2. Configure the CIFS server option that maps the administrators group to root as appropriate:

If you want to...	Then...
Map the administrator group members to root	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> All accounts in the administrators group are considered root, even if you do not have an <code>/etc/usermap.cfg</code> entry mapping the accounts to root. If you create a file using an account that belongs to the administrators group, the file is owned by root when you view the file from a UNIX client.
Disable mapping the administrators group members to root	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Accounts in the administrators group no longer map to root. You can only explicitly map a single user to root.

- 3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
- 4. Return to the admin privilege level: `set -privilege admin`

Display information about what types of users are connected over SMB sessions

You can display information about what type of users are connected over SMB sessions. This can help you ensure that only the appropriate type of user is connecting over SMB sessions on the storage virtual machine (SVM).

About this task

The following types of users can connect over SMB sessions:

- `local-user`

Authenticated as a local CIFS user

- `domain-user`

Authenticated as a domain user (either from the CIFS server's home domain or a trusted domain)

- `guest-user`

Authenticated as a guest user

- `anonymous-user`

Authenticated as an anonymous or null user

Steps

1. Determine what type of user is connected over an SMB session: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

If you want to display user type information for established sessions...	Enter the following command...
For all sessions with a specified user type	<code>vserver cifs session show -vserver vserver_name -user-type {local-user domain-user guest-user anonymous-user}</code>
For a specific user	<code>vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type</code>

Examples

The following command displays session information on the user type for sessions on SVM vs1 established by user "iepubs\user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node          vserver session-id connection-id lif-address  address
windows-user          user-type
-----
pub1node1 pub1      1          3439441860      10.0.0.1      10.1.1.1
IEPUBS\user1          domain-user
```

Command options to limit excessive Windows client resource consumption

Options to the `vserver cifs options modify` command enable you to control resource consumption for Windows clients. This can be helpful if any clients are outside

normal bounds of resource consumption, for example, if there are unusually high numbers of files open, sessions open, or change notify requests.

The following options to the `vserver cifs options modify` command have been added to control Windows client resource consumption. If the maximum value for any of these options is exceeded, the request is denied and an EMS message is sent. An EMS warning message is also sent when 80 percent of the configured limit for these options is reached.

- `-max-opens-same-file-per-tree`

Maximum number of opens on the same file per CIFS tree

- `-max-same-user-sessions-per-connection`

Maximum number of sessions opened by the same user per connection

- `-max-same-tree-connect-per-session`

Maximum number of tree connects on the same share per session

- `-max-watches-set-per-tree`

Maximum number of watches (also known as *change notifies*) established per tree

See the man pages for the default limits and to display the current configuration.

Beginning with ONTAP 9.4, servers running SMB version 2 or later can limit the number of outstanding requests (*SMB credits*) that the client can send to the server on a SMB connection. The management of SMB credits is initiated by the client and controlled by the server.

The maximum number of outstanding requests that can be granted on an SMB connection is controlled by the `-max-credits` option. The default value for this option is 128.

Improve client performance with traditional and lease oplocks

Improve client performance with traditional and lease oplocks overview

Traditional oplocks (opportunistic locks) and lease oplocks enable an SMB client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic.

Lease oplocks are an enhanced form of oplocks available with the SMB 2.1 protocol and later. Lease oplocks allow a client to obtain and preserve client caching state across multiple SMB opens originating from itself.

Oplocks can be controlled in two ways:

- By a share property, using the `vserver cifs share create` command when the share is created, or the `vserver share properties` command after creation.

- By a qtree property, using the `volume qtree create` command when the qtree is created, or the `volume qtree oplock` commands after creation.

Write cache data-loss considerations when using oplocks

Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must invalidate cached data and flush writes and locks. The client must then relinquish the oplock and access to the file. If there is a network failure during this flush, cached write data might be lost.

- Data-loss possibilities

Any application that has write-cached data can lose that data under the following set of circumstances:

- The connection is made using SMB 1.0.
 - It has an exclusive oplock on the file.
 - It is told to either break that oplock or close the file.
 - During the process of flushing the write cache, the network or target system generates an error.
- Error handling and write completion

The cache itself does not have any error handling—the applications do. When the application makes a write to the cache, the write is always completed. If the cache, in turn, makes a write to the target system over a network, it must assume that the write is completed because if it does not, the data is lost.

Enable or disable oplocks when creating SMB shares

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. Oplocks are enabled on SMB shares residing on storage virtual machines (SVMs). In some circumstances, you might want to disable oplocks. You can enable or disable oplocks on a share-by-share basis.

About this task

If oplocks are enabled on the volume containing a share but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over the volume oplock setting. Disabling oplocks on the share disables both opportunistic and lease oplocks.

You can specify other share properties in addition to specifying the oplock share property by using a comma-delimited list. You can also specify other share parameters.

Steps

1. Perform the applicable action:

If you want to...	Then...
Enable oplocks on a share during share creation	<p data-bbox="841 159 1448 338">Enter the following command: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></p> <div data-bbox="873 373 1456 800">  <p data-bbox="987 384 1448 789">If you want the share to have only the default share properties, which are <code>oplocks</code>, <code>browsable</code>, and <code>changenotify</code> enabled, you do not have to specify the <code>-share-properties</code> parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the <code>-share-properties</code> parameter with the list of share properties to use for that share.</p> </div>
Disable oplocks on a share during share creation	<p data-bbox="841 856 1448 1035">Enter the following command: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></p> <div data-bbox="873 1071 1414 1251">  <p data-bbox="987 1081 1414 1241">When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the <code>oplocks</code> property.</p> </div>

Related information

[Enabling or disabling oplocks on existing SMB shares](#)

[Monitoring oplock status](#)

Commands for enabling or disabling oplocks on volumes and qtrees

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. You need to know the commands for enabling or disabling oplocks on volumes or qtrees. You also must know when you can enable or disable oplocks on volumes and qtrees.

- Oplocks are enabled on volumes by default.
- You cannot disable oplocks when you create a volume.
- You can enable or disable oplocks on existing volumes for SVMs at any time.

- You can enable oplocks on qtrees for SVMs.

The oplock mode setting is a property of qtree ID 0, the default qtree that all volumes have. If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume, which is enabled by default. However, if you do specify an oplock setting on the new qtree, it takes precedence over the oplock setting on the volume.

If you want to...	Use this command...
Enable oplocks on volumes or qtrees	<code>volume qtree oplocks with the -oplock-mode parameter set to enable</code>
Disable oplocks on volumes or qtrees	<code>volume qtree oplocks with the -oplock-mode parameter set to disable</code>

Related information

[Monitoring oplock status](#)

Enable or disable oplocks on existing SMB shares

Oplocks are enabled on SMB shares on storage virtual machines (SVMs) by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenabling 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	<p>Enter the following command: <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>You can specify additional share properties to add by using a comma-delimited list.</p> </div> <p>Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.</p>

If you want to...	Then...
Disable oplocks on a share by modifying an existing share	<p>Enter the following command: <code>vserver cifs share properties remove -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div>  <p>You can specify additional share properties to remove by using a comma-delimited list.</p> </div> <p>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.</p>

Examples

The following command enables oplocks for the share named “Engineering” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

The following command disables oplocks for the share named “Engineering” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	browsable changenotify showsnapshot

Related information

[Enabling or disabling oplocks when creating SMB shares](#)

Monitor oplock status

You can monitor and display information about oplock status. You can use this information to determine which files have oplocks, what the oplock level and oplock state level are, and whether oplock leasing is used. You can also determine information about locks that you might need to break manually.

About this task

You can display information about all oplocks in summary form or in a detailed list form. You can also use optional parameters to display information about a smaller subset of existing locks. For example, you can specify that the output return only locks with the specified client IP address or with the specified path.

You can display the following information about traditional and lease oplocks:

- SVM, node, volume, and LIF on which the oplock is established
- Lock UUID
- IP address of the client with the oplock
- Path at which the oplock is established
- Lock protocol (SMB) and type (oplock)
- Lock state
- Oplock level
- Connection state and SMB expiration time
- Open Group ID if a lease oplock is granted

See the `vserver oplocks show` man page for a detailed description of each parameter.

Steps

1. Display oplock status by using the `vserver locks show` command.

Examples

The following command displays default information about all locks. The oplock on the displayed file is granted with a `read-batch` oplock level:


```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

The following example displays more detailed information about the lock on a file with the path /data2/data2_2/intro.pptx. A lease oplock is granted on the file with a batch oplock level to a client with an IP address of 10.3.1.3:



When displaying detailed information, the command provides separate output for oplock and sharelock information. This example only shows the output from the oplock section.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
  Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Related information

[Enabling or disabling oplocks when creating SMB shares](#)

[Enabling or disabling oplocks on existing SMB shares](#)

[Commands for enabling or disabling oplocks on volumes and qtrees](#)

Apply Group Policy Objects to SMB servers

Apply Group Policy Objects to SMB servers overview

Your SMB server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all storage virtual machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your SMB server, ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your SMB server, the Active

Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

Related information

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[SMB and NFS auditing and security tracing](#)

Supported GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled storage virtual machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs:

- Advanced audit policy configuration settings:

Object access: Central Access Policy staging

Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:

- Do not audit
- Audit only success events
- Audit only failure events
- Audit both success and failure events



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

Set by using the `Audit Central Access Policy Staging` setting in the `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.



To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:
 - Group Policy refresh interval for CIFS-enabled SVM

Set by using the `Registry` GPO.

- Group Policy refresh random offset

Set by using the Registry GPO.

- Hash publication for BranchCache

The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:

- Per-share
- All-shares
- Disabled Set by using the Registry GPO.

- Hash version support for BranchCache

The following three hash version settings are supported:

- BranchCache version 1
- BranchCache version 2
- BranchCache versions 1 and 2 Set by using the Registry GPO.



To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings

- Audit policy and event log

- Audit logon events

Specifies the type of logon events to be audited, including the following settings:

- Do not audit
 - Audit only success events
 - Audit on failure events
 - Audit both success and failure events Set by using the Audit logon events setting in the Local Policies/Audit Policy GPO.



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Audit object access

Specifies the type of object access to be audited, including the following settings:

- Do not audit
 - Audit only success events
 - Audit on failure events
 - Audit both success and failure events Set by using the Audit object access setting in the Local Policies/Audit Policy GPO.



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Log retention method

Specifies the audit log retention method, including the following settings:

- Overwrite the event log when size of the log file exceeds the maximum log size
- Do not overwrite the event log (clear log manually) Set by using the Retention method for security log setting in the Event Log GPO.

- Maximum log size

Specifies the maximum size of the audit log.

Set by using the Maximum security log size setting in the Event Log GPO.



To use audit policy and event log GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- File system security

Specifies a list of files or directories on which file security is applied through a GPO.

Set by using the File System GPO.



The volume path to which the file system security GPO is configured must exist within the SVM.

- Kerberos policy

- Maximum clock skew

Specifies maximum tolerance in minutes for computer clock synchronization.

Set by using the Maximum tolerance for computer clock synchronization setting in the Account Policies/Kerberos Policy GPO.

- Maximum ticket age

Specifies maximum lifetime in hours for user ticket.

Set by using the Maximum lifetime for user ticket setting in the Account Policies/Kerberos Policy GPO.

- Maximum ticket renew age

Specifies maximum lifetime in days for user ticket renewal.

Set by using the Maximum lifetime for user ticket renewal setting in the Account Policies/Kerberos Policy GPO.

- User rights assignment (privilege rights)

- Take ownership

Specifies the list of users and groups that have the right to take ownership of any securable object.

Set by using the `Take ownership of files or other objects` setting in the `Local Policies/User Rights Assignment` GPO.

- Security privilege

Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.

Set by using the `Manage auditing and security log` setting in the `Local Policies/User Rights Assignment` GPO.

- Change notify privilege (bypass traverse checking)

Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.

The same privilege is required for users to receive notifications of changes to files and directories. Set by using the `Bypass traverse checking` setting in the `Local Policies/User Rights Assignment` GPO.

- Registry values

- Signing required setting

Specifies whether required SMB signing is enabled or disabled.

Set by using the `Microsoft network server: Digitally sign communications (always)` setting in the `Security Options` GPO.

- Restrict anonymous

Specifies what the restrictions for anonymous users are and includes the following three GPO settings:

- No enumeration of Security Account Manager (SAM) accounts:

This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts` setting in the `Local Policies/Security Options` GPO.

- No enumeration of SAM accounts and shares

This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` setting in the `Local Policies/Security Options` GPO.

- Restrict anonymous access to shares and named pipes

This security setting restricts anonymous access to shares and pipes. This option is displayed as `no-access` in ONTAP if it is enabled.

Set by using the `Network access: Restrict anonymous access to Named Pipes and Shares` setting in the `Local Policies/Security Options` GPO.

When displaying information about defined and applied group policies, the `Resultant restriction for anonymous user output` field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- `no-access`

The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is enabled.

- `no-enumeration`

The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:

- The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
- Either the `Network access: Do not allow anonymous enumeration of SAM accounts` or the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs is enabled.

- `no-restriction`

The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:

- The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
- Both the `Network access: Do not allow anonymous enumeration of SAM accounts` and `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs are disabled.

- **Restricted Groups**

You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.

Set by using the `Restricted Groups` GPO.

- **Central access policy settings**

Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

Related information

- [Enabling or disabling GPO support on a CIFS server](#)
- [Securing file access by using Dynamic Access Control \(DAC\)](#)
- [SMB and NFS auditing and security tracing](#)
- [Modifying the CIFS server Kerberos security settings](#)
- [Using BranchCache to cache SMB share content at a branch office](#)
- [Using SMB signing to enhance network security](#)
- [Configuring bypass traverse checking](#)
- [Configuring access restrictions for anonymous users](#)


Requirements for using GPOs with your SMB server

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

- SMB must be licensed on the cluster. 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 a CIFS server

You can enable or disable Group Policy Object (GPO) support on a CIFS server. If you enable GPO support on a CIFS server, the applicable GPOs that are defined on the group policy—the policy that is applied to the organizational unit (OU) that contains the CIFS server computer object—are applied to the CIFS server.



About this task

GPOs cannot be enabled on CIFS servers in workgroup mode.

Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>

If you want to...	Enter the command...
Disable GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. Verify that GPO support is in the desired state: `vserver cifs group-policy show -vserver +vserver_name_`

Group Policy Status for CIFS servers in workgroup mode is displayed as “disabled”.

Example

The following example enables GPO support on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

                Vserver: vs1
Group Policy Status: enabled
```

Related information

[Supported GPOs](#)

[Requirements for using GPOs with your CIFS server](#)

[How GPOs are updated on the CIFS server](#)

[Manually updating GPO settings on the CIFS server](#)

[Displaying information about GPO configurations](#)

How GPOs are updated on the SMB server

How GPOs are updated on the CIFS server overview

By default, ONTAP retrieves and applies Group Policy Object (GPO) changes every 90 minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before ONTAP automatically updates them, you can trigger a manual update on a CIFS server with an ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes.

This interval is configurable and can be set using the `Refresh interval` and `Random offset` GPO settings.

ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active Directory are higher than those on the CIFS server, ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

- Security Settings GPOs are refreshed every 16 hours.

ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.



The 16-hour default value cannot be changed in the current ONTAP version. It is a Windows client default setting.

- All GPOs can be updated manually with an ONTAP command.

This command simulates the Windows `gpupdate.exe /force` command.

Related information

[Manually updating GPO settings on the CIFS server](#)

Manually updating GPO settings on the CIFS server

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

Step

1. Perform the appropriate action:

If you want to update...	Enter the command...
Changed GPO settings	<code>vserver cifs group-policy update -vserver vserver_name</code>
All GPO settings	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

Related information

[How GPOs are updated on the CIFS server](#)

Display information about GPO configurations

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

About this task

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFS server.

Steps

1. Display information about GPO configurations by performing one of the following actions:

If you want to display information about all Group Policy configurations...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Applied to a CIFS-enabled storage virtual machine (SVM)	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

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/dirl
```

```
Kerberos:
```

```
    Max Clock Skew: 5
```

```
    Max Ticket Age: 10
```

```
    Max Renew Age: 7
```

```
Privilege Rights:
```

```
    Take Ownership: usr1, usr2
```

```
    Security Privilege: usr1, usr2
```

```

    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

GPO Name: Resultant Set of Policy
Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age: 7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true

```

```
No enumeration of SAM accounts and shares: false
Restrict anonymous access to shares and named pipes: true
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
      Level: Domain
    Status: enabled
Advanced Audit Settings:
    Object Access:
      Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
      Audit Logon Events: none
      Audit Object Access: success
      Log Retention Method: overwrite-as-needed
      Max Log Size: 16384
    File Security:
      /vol1/home
      /vol1/dir1
    Kerberos:
      Max Clock Skew: 5
      Max Ticket Age: 10
      Max Renew Age: 7
    Privilege Rights:
      Take Ownership: usr1, usr2
      Security Privilege: usr1, usr2
      Change Notify: usr1, usr2
    Registry Values:
```

```
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

    GPO Name: Resultant Set of Policy
    Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age: 7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
```

```
Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

Related information

[Enabling or disabling GPO support on a CIFS server](#)

Display detailed information about restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

About this task

By default, the following information is displayed:

- Group policy name
- Group policy version
- Link

Specifies the level in which the group policy is configured. Possible output values include the following:

- `Local` when the group policy is configured in ONTAP
- `Site` when the group policy is configured at the site level in the domain controller
- `Domain` when the group policy is configured at the domain level in the domain controller
- `OrganizationalUnit` when the group policy is configured at the Organizational Unit (OU) level in the domain controller
- `RSOP` for the resultant set of policies derived from all the group policies defined at various levels
- Restricted group name
- The users and groups who belong to and who do not belong to the restricted group
- The list of groups to which the restricted group is added

A group can be a member of groups other than the groups listed here.

Step

1. Display information about all restricted group GPOs by performing one of the following actions:

If you want to display information about all restricted group GPOs...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Applied to a CIFS server	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

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: gp01
        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: gp01
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

[Displaying information about GPO configurations](#)

Display information about central access policies

You can display detailed information about the central access policies that are defined in Active Directory. You can also display information about the central access policies that are applied to the CIFS server through group policy objects (GPOs).

About this task

By default, the following information is displayed:

- SVM name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules



CIFS servers in workgroup mode are not displayed because they do not support GPOs.

Step

1. Display information about central access policies by performing one of the following actions:

If you want to display information about all central access policies...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
Applied to a CIFS server	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

Example

The following example displays information for all the central access policies that are defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                      SID
-----  -
-----  -
vs1      p1                      S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                      S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                   r2
```

The following example displays information for all the central access policies that are applied to the storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

Vserver	Name	SID
vs1	p1	S-1-17-3386172923-1132988875-3044489393-3993546205
Description: policy #1		
Creation Time: Tue Oct 22 09:34:13 2013		
Modification Time: Wed Oct 23 08:59:15 2013		
Member Rules: r1		
vs1	p2	S-1-17-1885229282-1100162114-134354072-822349040
Description: policy #2		
Creation Time: Tue Oct 22 10:28:20 2013		
Modification Time: Thu Oct 31 10:25:32 2013		
Member Rules: r1		
r2		

Related information

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[Displaying information about GPO configurations](#)

[Displaying information about central access policy rules](#)

Display information about central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions

- Target resources

Table 1. Step

If you want to display information about all central access policy rules associated with central access policies...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Applied to a CIFS server	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

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::> vsserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Related information

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

Commands for managing SMB servers computer account passwords

You need to know the commands for changing, resetting, and disabling passwords, and for configuring automatic update schedules. You can also configure a schedule on the SMB server to update it automatically.

If you want to...	Use this command...
Change or reset the domain account password and you know the password	<code>vsserver cifs domain password change</code>
Reset the domain account password and you do not know the password	<code>vsserver cifs domain password reset</code>
Configure SMB servers for automatic computer account password changes	<code>vsserver cifs domain password schedule modify -vsserver vsserver_name -is -schedule-enabled true</code>

If you want to...	Use this command...
Disable automatic computer account password changes on SMB servers	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</code>

See the man page for each command for more information.

Manage domain controller connections

Display information about discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

Step

1. To display information related to discovered servers, enter the following command: `vserver cifs domain discovered-servers show`

Example

The following example shows discovered servers for SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
```

```
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Related information

[Resetting and rediscovering servers](#)

[Stopping or starting the CIFS server](#)

Reset and rediscover servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

Steps

1. Enter the following command: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Display information about the newly rediscovered servers: `vserver cifs domain discovered-servers show -vserver vserver_name`

Example

The following example resets and rediscovers servers for storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

Related information

[Displaying information about discovered servers](#)

[Stopping or starting the CIFS server](#)

Manage domain controller discovery

Beginning with ONTAP 9.3, you can modify the default process by which domain controllers (DCs) are discovered. This enables you to limit discovery to your site or to a pool of preferred DCs, which can lead to performance improvements depending on the environment.

About this task

By default, the dynamic discovery process discovers all available DCs, including any preferred DCs, all DCs in the local site, and all remote DCs. This configuration can lead to latency in authentication and accessing shares in certain environments. If you have already determined the pool of DCs that you want to use, or if the remote DCs are inadequate or inaccessible, you can change the discovery method.

In ONTAP 9.3 and later releases, the `discovery-mode` parameter of the `cifs domain discovered-servers` command enables you to select one of the following discovery options:

- All DCs in the domain are discovered.
- Only DCs in the local site are discovered.

The `default-site` parameter for the SMB server 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.

Step

1. Specify the desired discovery option: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Options for the `mode` parameter:

- `all`

Discover all available DCs (default).

- `site`

Limit DC discovery to your site.

- `none`

Use only preferred DCs and not perform discovery.

Add preferred domain controllers

ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

Step

1. To add to the list of preferred domain controllers, enter the following command:
`vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...+`

`-vserver vserver_name` specifies the storage virtual machine (SVM) name.

`-domain domain_name` specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.

`-preferred-dc IP_address,...` specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the SMB server on SVM vs1 uses to manage external access to the

cifs.lab.example.com domain.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Related information

[Commands for managing preferred domain controllers](#)

Commands for managing preferred domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

If you want to...	Use this command...
Add a preferred domain controller	<code>vserver cifs domain preferred-dc add</code>
Display preferred domain controllers	<code>vserver cifs domain preferred-dc show</code>
Remove a preferred domain controller	<code>vserver cifs domain preferred-dc remove</code>

See the man page for each command for more information.

Related information

[Adding preferred domain controllers](#)

Enable SMB2 connections to domain controllers

Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller. Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB2 is enabled by default.

About this task

The `smb2-enabled-for-dc-connections` command option enables the system default for the release of ONTAP you are using. The system default for ONTAP 9.1 is enabled for SMB 1.0 and disabled for SMB 2.0. The system default for ONTAP 9.2 is enabled for SMB 1.0 and enabled for SMB 2.0. If the domain controller cannot negotiate SMB 2.0 initially, it uses SMB 1.0.

SMB 1.0 can be disabled from ONTAP to a domain controller. In ONTAP 9.1, if SMB 1.0 has been disabled, SMB 2.0 must be enabled in order to communicate with a domain controller.

Learn more about:

- [Verifying enabled SMB versions.](#)
- [Supported SMB versions and functionality.](#)



If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server.

Steps

1. Before changing SMB security settings, verify which SMB versions are enabled: `vserver cifs security show`
2. Scroll down the list to see the SMB versions.
3. Perform the appropriate command, using the `smb2-enabled-for-dc-connections` option.

If you want SMB2 to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -smb2-enabled-for-dc-connections true</code>
Disabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -smb2-enabled-for-dc-connections false</code>

Enable encrypted connections to domain controllers

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted.

About this task

ONTAP requires encryption for domain controller (DC) communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3.

When encrypted DC communications are required, the `-smb2-enabled-for-dc-connections` option is ignored, because ONTAP only negotiates SMB3 connections. If a DC doesn't support SMB3 and encryption, ONTAP will not connect with it.

Step

1. Enable encrypted communication with the DC: `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Use null sessions to access storage in non-Kerberos environments

Use null sessions to access storage in non-Kerberos environments overview

Null session access provides permissions for network resources, such as storage system data, and to client-based services running under the local system. A null session occurs when a client process uses the “system” account to access a network resource. Null

session configuration is specific to non-Kerberos authentication.

How the storage system provides null session access

Because null session shares do not require authentication, clients that require null session access must have their IP addresses mapped on the storage system.

By default, unmapped null session clients can access certain ONTAP system services, such as share enumeration, but they are restricted from accessing any storage system data.



ONTAP supports Windows RestrictAnonymous registry setting values with the `-restrict-anonymous` option. This enables you to control the extent to which unmapped null users can view or access system resources. For example, you can disable share enumeration and access to the IPC\$ share (the hidden named pipe share). The `vserver cifs options modify` and `vserver cifs options show man` pages provide more information about the `-restrict-anonymous` option.

Unless otherwise configured, a client running a local process that requests storage system access through a null session is a member only of nonrestrictive groups, such as “everyone”. To limit null session access to selected storage system resources, you might want to create a group to which all null session clients belong; creating this group enables you to restrict storage system access and to set storage system resource permissions that apply specifically to null session clients.

ONTAP provides a mapping syntax in the `vserver name-mapping` command set to specify the IP address of clients allowed access to storage system resources using a null user session. After you create a group for null users, you can specify access restrictions for storage system resources and resource permissions that apply only to null sessions. Null user is identified as anonymous logon. Null users do not have access to any home directory.

Any null user accessing the storage system from a mapped IP address is granted mapped user permissions. Consider appropriate precautions to prevent unauthorized access to storage systems mapped with null users. For maximum protection, place the storage system and all clients requiring null user storage system access on a separate network, to eliminate the possibility of IP address “spoofing”.

Related information

[Configuring access restrictions for anonymous users](#)

Grant null users access to file system shares

You can allow access to your storage system resources by null session clients by assigning a group to be used by null session clients and recording the IP addresses of null session clients to add to the storage system’s list of clients allowed to access data using null sessions.

Steps

1. Use the `vserver name-mapping create` command to map the null user to any valid windows user, with an IP qualifier.

The following command maps the null user to user1 with a valid host name google.com:

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

The following command maps the null user to user1 with a valid IP address 10.238.2.54/32:

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Use the `vserver name-mapping show` command to confirm the name mapping.

```
vserver name-mapping show

Vserver:    vs1
Direction:  win-unix
Position Hostname      IP Address/Mask
-----
1          -            10.72.40.83/32      Pattern: anonymous logon
                                     Replacement: user1
```

3. Use the `vserver cifs options modify -win-name-for-null-user` command to assign Windows membership to the null user.

This option is applicable only when there is a valid name mapping for the null user.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Use the `vserver cifs options show` command to confirm the mapping of the null user to the Windows user or group.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Manage NetBIOS aliases for SMB servers

Manage NetBIOS aliases for SMB servers overview

NetBIOS aliases are alternative names for your SMB server that SMB clients can use when connecting to the SMB server. Configuring NetBIOS aliases for a SMB server can

be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original file servers' names.

You can specify a list of NetBIOS aliases when you create the SMB server or at any time after you create the SMB server. You can add or remove NetBIOS aliases from the list at any time. You can connect to the SMB server using any of the names in the NetBIOS alias list.

Related information

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

Add a list of NetBIOS aliases to the SMB server

If you want SMB clients to connect to the SMB server by using an alias, you can create a list of NetBIOS aliases, or you can add NetBIOS aliases to an existing list of NetBIOS aliases.

About this task

- The NetBIOS alias name can be 15 up to characters in length.
- You can configure up to 200 NetBIOS aliases on the SMB server.
- The following characters are not allowed:

@ # * () = + [] | ; : " , < > \ / ?

Steps

1. Add the NetBIOS aliases:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- You can specify one or more NetBIOS aliases by using a comma-delimited list.
- The specified NetBIOS aliases are added to the existing list.
- A new list of NetBIOS aliases is created if the list is currently empty.

2. Verify that the NetBIOS aliases were added correctly: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Related information

[Removing NetBIOS aliases from the NetBIOS alias list](#)

Remove NetBIOS aliases from the NetBIOS alias list

If you do not need specific NetBIOS aliases for a CIFS server, you can remove those NetBIOS aliases from the list. You can also remove all NetBIOS aliases from the list.

About this task

You can remove more than one NetBIOS alias by using a comma-delimited list. You can remove all of the NetBIOS aliases on a CIFS server by specifying `-` as the value for the `-netbios-aliases` parameter.

Steps

1. Perform one of the following actions:

If you want to remove...	Enter...
Specific NetBIOS aliases from the list	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
All NetBIOS aliases from the list	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verify that the specified NetBIOS aliases were removed: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1  
  
Server Name: CIFS_SERVER  
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Display the list of NetBIOS aliases on CIFS servers

You can display the list of NetBIOS aliases. This can be useful when you want to determine the list of names over which SMB clients can make connections to the CIFS server.

Step

1. Perform one of the following actions:

If you want to display information about...	Enter...
A CIFS server's NetBIOS aliases	<code>vserver cifs show -display-netbios -aliases</code>
The list of NetBIOS aliases as part of the detailed CIFS server information	<code>vserver cifs show -instance</code>

The following example displays information about a CIFS server's NetBIOS aliases:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example displays the list of NetBIOS aliases as part of the detailed CIFS server information:

```
vserver cifs show -instance
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

See the man page for the commands for more information.

Related information

[Adding a list of NetBIOS aliases to the CIFS server](#)

[Commands for managing CIFS servers](#)

Determine whether SMB clients are connected using NetBIOS aliases

You can determine whether SMB clients are connected using NetBIOS aliases, and if so, which NetBIOS alias is used to make the connection. This can be useful when troubleshooting connection issues.

About this task

You must use the `-instance` parameter to display the NetBIOS alias (if any) associated with an SMB connection. If the CIFS server name or an IP address is used to make the SMB connection, the output for the NetBIOS Name field is `-` (hyphen).

Step

1. Perform the desired action:

If you want to display NetBIOS information for...	Enter...
SMB connections	<code>vserver cifs session show -instance</code>
Connections using a specified NetBIOS alias:	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

The following example displays information about the NetBIOS alias used to make the SMB connection with session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

Manage miscellaneous SMB server tasks

Stop or start the CIFS server

You can stop the CIFS server on a SVM, which can be useful when performing tasks

while users are not accessing data over SMB shares. You can restart SMB access by starting the CIFS server. By stopping the CIFS server, you can also modify the protocols allowed on the storage virtual machine (SVM).

Steps

- 1. Perform one of the following actions:

If you want to...	Enter the command...
Stop the CIFS server	<code>vserver cifs stop -vserver vserver_name [-foreground {true false}]</code>
Start the CIFS server	<code>vserver cifs start -vserver vserver_name [-foreground {true false}]</code>

`-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

[Displaying information about discovered servers](#)

[Resetting and rediscovering servers](#)

Move CIFS servers to different OUs

The CIFS server create-process uses the default organizational unit (OU) CN=Computers during setup unless you specify a different OU. You can move CIFS servers to different OUs after setup.

Steps

1. On the Windows server, open the **Active Directory Users and Computers** tree.
2. Locate the Active Directory object for the storage virtual machine (SVM).
3. Right-click the object and select **Move**.
4. Select the OU that you want to associate with the SVM

Results

The SVM object is placed in the selected OU.

Modify the dynamic DNS domain on the SVM before moving the SMB server

If you want the Active Directory-integrated DNS server to dynamically register the SMB server's DNS records in DNS when you move the SMB server to another domain, you must modify dynamic DNS (DDNS) on the storage virtual machine (SVM) before moving the SMB server.

Before you begin

DNS name services must be modified on the SVM to use the DNS domain that contains the service location records for the new domain that will contain the SMB server computer account. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers.

About this task

Although DDNS (if configured on the SVM) automatically adds the DNS records for data LIFs to the new domain, the DNS records for the original domain are not automatically deleted from the original DNS server. You must delete them manually.

To complete your DDNS modifications before moving the SMB server, see the following topic:

[Configure dynamic DNS services](#)

Join a SVM to an Active Directory domain

You can join a storage virtual machine (SVM) to an Active Directory domain without deleting the existing SMB server by modifying the domain using the `vserver cifs modify` command. You can rejoin the current domain or join a new one.

Before you begin

- The SVM must already have a DNS configuration.
- The DNS configuration for the SVM must be able to serve the target domain.

The DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

About this task

- The administrative status of the CIFS server must be set to “down” to proceed with Active Directory domain modification.
- If the command completes successfully, the administrative status is automatically set to “up”.
- When joining a domain, this command might take several minutes to complete.

Steps

1. Join the SVM to the CIFS server domain: `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

For more information, see the man page for the `vserver cifs modify` command. If you need to reconfigure DNS for the new domain, see the man page for the `vserver dns modify` command.

In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou= example ou` container within the `example.com` domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

2. Verify that the CIFS server is in the desired Active Directory domain: `vserver cifs show`

Example

In the following example, the SMB server “CIFSSERVER1” on SVM vs1 joins the `example.com` domain using keytab authentication:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status  
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

Display information about NetBIOS over TCP connections

You can display information about NetBIOS over TCP (NBT) connections. This can be useful when troubleshooting NetBIOS-related issues.

Step

1. Use the `vserver cifs nbtstat` command to display information about NetBIOS over TCP connections.



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

Example

The following example shows the NetBIOS name service information displayed for “cluster1”:

```
cluster1::> vserver cifs nbtstat
```

```
Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2  (active  )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State    Time Left  Type
-----
CLUSTER_1     00                wins     57
CLUSTER_1     20                wins     57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2  (active  )
CLUSTER_1     00                wins     58
CLUSTER_1     20                wins     58
4 entries were displayed.
```

Commands for managing SMB servers

You need to know the commands for creating, displaying, modifying, stopping, starting, and deleting SMB servers. There are also commands to reset and rediscover servers, change or reset machine account passwords, schedule changes for machine account passwords, and add or remove NetBIOS aliases.

If you want to...	Use this command...
Create an SMB server	<code>vserver cifs create</code>
Display information about an SMB server	<code>vserver cifs show</code>
Modify an SMB server	<code>vserver cifs modify</code>
Move an SMB server to another domain	<code>vserver cifs modify</code>

Stop an SMB server	<code>vserver cifs stop</code>
Start an SMB server	<code>vserver cifs start</code>
Delete an SMB server	<code>vserver cifs delete</code>
Reset and rediscover servers for the SMB server	<code>vserver cifs domain discovered-servers reset-servers</code>
Change the SMB server's machine account password	<code>vserver cifs domain password change</code>
Reset the SMB server's machine account password	<code>vserver cifs domain password change</code>
Schedule automatic password changes for the SMB server's machine account	<code>vserver cifs domain password schedule modify</code>
Add NetBIOS aliases for the SMB server	<code>vserver cifs add-netbios-aliases</code>
Remove NetBIOS aliases for the SMB server	<code>vserver cifs remove-netbios-aliases</code>

See the man page for each command for more information.

Related information

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

Enable the NetBios name service

Beginning with ONTAP 9, the NetBios name service (NBNS, sometimes called Windows Internet Name Service or WINS) is disabled by default. Previously, CIFS-enabled storage virtual machines (SVMs) sent name registration broadcasts regardless of whether WINS was enabled on a network. To limit such broadcasts to configurations where NBNS is required, you must enable NBNS explicitly for new CIFS servers.

Before you begin

- If you are already using NBNS and you upgrade to ONTAP 9, it is not necessary to complete this task. NBNS will continue to work as before.
- NBNS is enabled over UDP (port 137).
- NBNS over IPv6 is not supported.

Steps

1. Set the privilege level to advanced.

```
set -privilege advanced
```

2. Enable NBNS on a CIFS server.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

3. Return to the admin privilege level.

```
set -privilege admin
```

Use IPv6 for SMB access and SMB services

Requirements for using IPv6

Before you can use IPv6 on your SMB server, you need to know which versions of ONTAP and SMB support it and what the license requirements are.

ONTAP license requirements

No special license is required for IPv6 when SMB is licensed. 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.



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

Support for IPv6 with SMB access and CIFS services

If you want to use IPv6 on your CIFS server, you need to be aware of how ONTAP supports IPv6 for SMB access and network communication for CIFS services.

Windows client and server support

ONTAP provides support for Windows servers and clients that support IPv6. The following describes Microsoft Windows client and server IPv6 support:

- Windows 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

How CIFS servers use IPv6 to connect to external servers

To create a configuration that meets your requirements, you must be aware of how CIFS servers use IPv6 when making connections to external servers.

- Source address selection

If an attempt is made to connect to an external server, the source address selected must be of the same type as the destination address. For example, if connecting to an IPv6 address, the storage virtual machine (SVM) hosting the CIFS server must have a data LIF or management LIF that has an IPv6 address to use as the source address. Similarly, if connecting to an IPv4 address, the SVM must have a data LIF or management LIF that has an IPv4 address to use as the source address.

- For servers dynamically discovered using DNS, server discovery is performed as follows:
 - If IPv6 is disabled on the cluster, only IPv4 servers addresses are discovered.
 - If IPv6 is enabled on the cluster, both IPv4 and IPv6 server addresses are discovered. Either type might be used depending upon the suitability of the server to which the address belongs and the availability of IPv6 or IPv4 data or management LIFs. Dynamic server discovery is used for discovering Domain Controllers and their associated services, such as LSA, NETLOGON, Kerberos, and LDAP.

- DNS server connectivity

Whether the SVM uses IPv6 when connecting to a DNS server depends on the DNS name services configuration. If DNS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the DNS name services configuration can use IPv4 addresses so that connections to DNS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring DNS name services.

- LDAP server connectivity

Whether the SVM uses IPv6 when connecting to an LDAP server depends on the LDAP client configuration. If the LDAP client is configured to use IPv6 addresses, connections are made by using IPv6. If desired, the LDAP client configuration can use IPv4 addresses so that connections to LDAP servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring the LDAP client configuration.



The LDAP client configuration is used when configuring LDAP for UNIX user, group, and netgroup name services.

- NIS server connectivity

Whether the SVM uses IPv6 when connecting to a NIS server depends on the NIS name services configuration. If NIS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the NIS name services configuration can use IPv4 addresses so that connections to NIS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring NIS name services.



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

Related information

[Enabling IPv6 for SMB \(cluster administrators only\)](#)

[Monitoring and displaying information about IPv6 SMB sessions](#)

Enable IPv6 for SMB (cluster administrators only)

IPv6 networks are not enabled during cluster setup. A cluster administrator must enable IPv6 after cluster setup is complete to use IPv6 for SMB. When the cluster administrator enables IPv6, it is enabled for the entire cluster.

Step

1. Enable IPv6: `network options ipv6 modify -enabled true`

For more information about enabling IPv6 on the cluster and configuring IPv6 LIFs, see the *Network Management Guide*.

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

Related information

[Monitoring and displaying information about IPv6 SMB sessions](#)

Disable IPv6 for SMB

Even though IPv6 is enabled on the cluster using a network option, you cannot disable IPv6 for SMB by using the same command. Instead, ONTAP disables IPv6 when the cluster administrator disables the last IPv6-enabled interface on the cluster. You should communicate with the cluster administrator about management of your IPv6 enabled interfaces.

For more information about disabling IPv6 on the cluster, see the *Network Management Guide*.

Related information

[Network management](#)

Monitor and display information about IPv6 SMB sessions

You can monitor and display information about SMB sessions that are connected using IPv6 networks. This information is useful in determining which clients are connecting using IPv6 as well as other useful information about IPv6 SMB sessions.

Step

1. Perform the desired action:

If you want to determine whether...	Enter the command...
SMB sessions to a storage virtual machine (SVM) are connected using IPv6	<pre>vserver cifs session show -vserver vserver_name -instance</pre>
IPv6 is used for SMB sessions through a specified LIF address	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> is the data LIF's IPv6 address.</p>

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.