Clustered Data ONTAP® 8.2

File Access Management Guide for CIFS

Contents

Understanding SMB file access with Data ONTAP

There are certain SMB file access concepts you should understand before you configure a CIFS server and then configure SMB shares to let SMB clients access files on your cluster.

How namespaces and volume junctions affect SMB access on SVMs with FlexVol volumes

You must understand what namespaces and volume junctions are and how they work to correctly configure SMB access on Storage Virtual Machines (SVMs) in your storage environment.

Related concepts

What namespaces in SVMs with FlexVol volumes are

A namespace is a logical grouping of volumes that are joined together at junction points to create a single, logical file system that derives from the Storage Virtual Machine (SVM) root volume. Each SVM has a namespace.

CIFS and NFS servers on a data SVM can store and access data across the namespace. Each client can access the entire namespace by mounting an export or accessing a single SMB share at the top of the namespace.

Alternatively, SVM administrators can create exports at each volume junction so that clients can create mount points at intermediate locations in the namespace, or they can create SMB shares that point to any directory path in the namespace.

Volumes can be added at any time by mounting them to any location in the namespace. Clients can immediately access the newly added volume, provided that the volume junction is under the point at which they are accessing the namespace and provided that they have sufficient permissions.

Volume junction usage rules

Volume junctions are a way to join individual volumes together into a single, logical namespace to enable data access to NAS clients. Understanding how volume junctions are formed helps you to interpret and apply the usage rules.

When NAS clients access data by traversing a junction, the junction appears to be an ordinary directory. A junction is formed when a volume is mounted to a mount point below the root and is used to create a file-system tree. The top of a file-system tree is always the root volume, which is represented by a slash (/). A junction leads from a directory in one volume to the root directory of another volume.

- Although specifying a junction point is optional when a volume is created, data in the volume cannot be exported (NFS) and a share cannot be created (CIFS) until the volume is mounted to a junction point in the namespace.
- A volume that was not mounted during volume creation can be mounted post-creation.
- New volumes can be added to the namespace at any time by mounting them to a junction point.
- Mounted volumes can be unmounted; however, unmounting a volume disrupts NAS client access to all data in the volume and to all volumes mounted at child junction points beneath the unmounted volume.
- Junction points can be created directly below a parent volume junction, or they can be created on a directory within a volume.

  For example, a path to a volume junction for a volume named "vol3" might be `/vol1/vol2/vol3`, or it might be `/vol1/dir2/vol3`, or even `/dir1/dir2/vol3`.

How volume junctions are used in SMB and NFS namespaces

You can mount volumes at junction points anywhere within the namespace to create a single, logical namespace. If you specify a junction point when the volume is created, the volume is automatically mounted at the time the volume is created and is available for NAS access. You can create SMB shares and NFS exports on the mounted volume.

If you do not specify a junction point, the volume is online but is not mounted for NAS file access. You must mount a volume to a junction point before it can be used for NAS file access.

What the typical NAS namespace architectures are

All Storage Virtual Machine (SVM) name spaces derive from the root volume; however, there are several typical NAS namespace architectures that you can use as you create your SVM name space. You can choose the namespace architecture that matches your business and workflow needs.

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

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

Namespace with single branched tree

An architecture with a single branched tree has a single insertion point to the root of the SVM namespace. The single insertion point can be either a junctioned volume or a directory beneath the root. All other volumes are mounted at junction points beneath the single insertion point (which can be a volume or a directory).
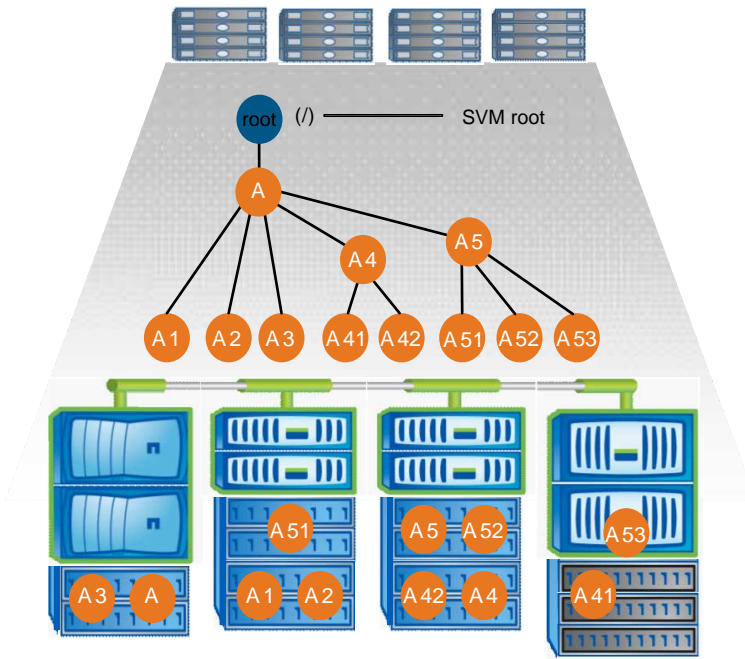
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where all volumes are junctioned below the single insertion point, which is a directory named "data":

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

Namespace with multiple branched trees

An architecture with multiple branched trees has multiple insertion points to the root of the SVM namespace. The insertion points can be either junctioned volumes or directories beneath the root. All other volumes are mounted at junction points beneath the insertion points (which can be volumes or directories).
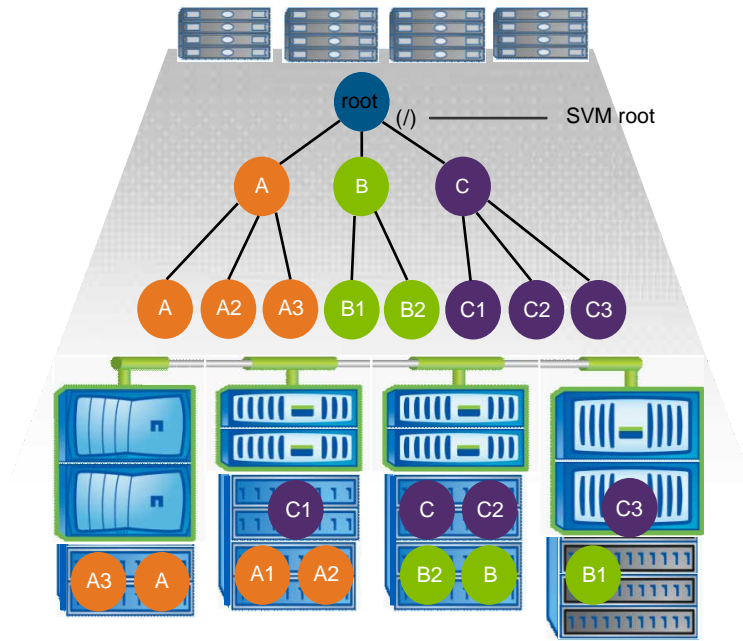
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are three insertion points to the root volume of the SVM. Two insertion points are directories named "data" and "projects". One insertion point is a junctioned volume named "audit":

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

Namespace with multiple stand-alone volumes

In an architecture with stand-alone volumes, every volume has an insertion point to the root of the SVM namespace; however, the volume is not junctioned below another volume. Each volume has a unique path, and is either junctioned directly below the root or is junctioned under a directory below the root.
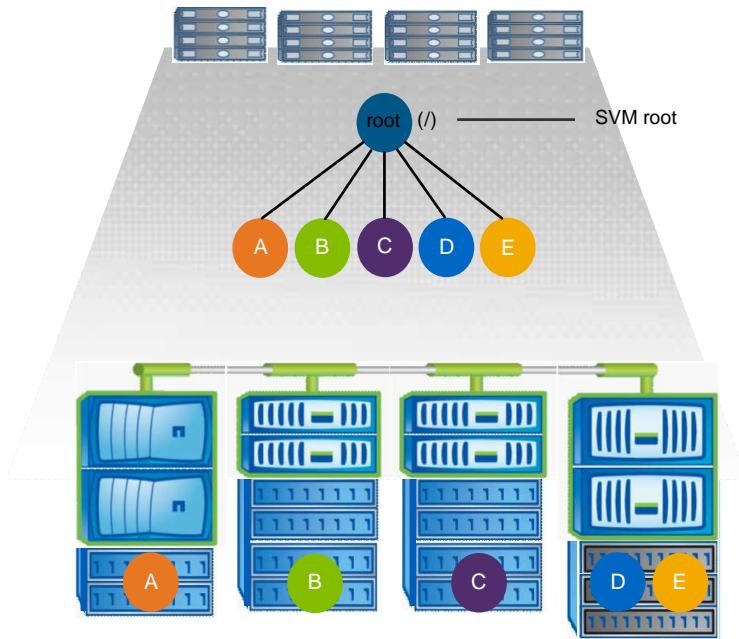
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are five insertion points to the root volume of the SVM, with each insertion point representing a path to one volume.

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

LIF configuration requirements for file access management

To properly manage file access control, Data ONTAP must communicate with external services such as NIS, LDAP, and Active Directory servers. The Storage Virtual Machine (SVM) LIFs must be properly configured to allow these communications.

The communication with external services usually happens over the data LIF of the SVM. Therefore, you must ensure that the SVM has a data LIF properly configured to reach all required external services on each node.

In addition, in some situations, communication over the data LIF might fail or must be made on a node that does not host data LIFs for the SVM. In this case, the storage system attempts to use node-management and cluster-management LIFs instead. If your environment allows this, you should also ensure that the node-management and cluster-management LIFs in the cluster can reach these external services as well.

For more information about LIF configuration, see the *Clustered Data ONTAP Network Management Guide*.

Related concepts

Setting up the CIFS server on page 41

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367

How security styles affect data access

Each volume and qtree on the storage system has a security style. The security style determines what type of permissions are used for data on volumes when authorizing users. You must understand what the different security styles are, when and where they are set, how they impact permissions, how they differ between volume types, and more.

Related tasks

Configuring security styles on SVM root volumes on page 109
Configuring security styles on FlexVol volumes on page 110
Configuring security styles on qtrees on page 110

What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions Data ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of Data ONTAP. However, Data ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
UNIX	NFS	NFSv3 mode bits	UNIX	NFS and SMB
		NFSv4.x ACLs	UNIX	
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.x ACLs	UNIX	
		NTFS ACLs	NTFS	
Unified (only for Infinite Volumes)	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.1 ACLs	UNIX	
		NTFS ACLs	NTFS	

For more information about the unified security style, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

Note: Data ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Note: Infinite Volumes always use the unified security style. You cannot configure or change the security style of an Infinite Volume.

How to decide on what security style to use on SVMs with FlexVol volumes

To help you decide what security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if...
UNIX	- The file system is managed by a UNIX administrator. - The majority of users are NFS clients. - An application accessing the data uses a UNIX user as the service account.
NTFS	- The file system is managed by a Windows administrator. - The majority of users are SMB clients. - An application accessing the data uses a Windows user as the service account.
Mixed	The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or qtree, it inherits its security style.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing Storage Virtual Machine (SVM).
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

Infinite Volumes cannot inherit security styles. All files and directories in Infinite Volumes always use the unified security style. The security style of an Infinite Volume and the files and directories it contains cannot be changed.

How authentication provides SMB access security

Authentication is the process of verifying the identity of an entity. Before users can create SMB connections to access data contained on the Storage Virtual Machine (SVM), they must be authenticated by the domain to which the CIFS server belongs.

The CIFS server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

Related concepts

Using local users and groups for authentication and authorization on page 156

How file and share permissions are used to secure SMB access on page 24

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23

Related tasks

Modifying the CIFS server Kerberos security settings on page 62

Kerberos authentication

Data ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is a protocol designed to provide strong authentication within a client/server environment. The basis of the protocol is a shared secret key cryptology system that provides secure authentication in a networked environment.

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

KDC Resource SID Compression feature

The Key Distribution Center (KDC) can use the Resource SID Compression feature when Active Directory servers are hosted on Windows Server 2012.

Microsoft introduced an enhancement to its Kerberos implementation for Windows Server 2012 that was later called KDC Resource SID Compression, in which the KDC automatically compresses the group security identifiers (SIDs) in the resource domain. This compression can reduce the size of the service ticket and reduce application authentication failures caused by large ticket sizes. To compress resource SIDs, the KDC stores the SID of the resource domain of which the target resource is a member. The KDC inserts only the RID portion of each resource SID into the ResourceGroupIds portion of the authentication data.

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

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes

User mapping between a Windows user and a UNIX user is a fundamental part of multiprotocol access. Multiprotocol access over SMB depends on user mapping between a user's Windows identity and UNIX identity to evaluate the user's rights to perform file and folder operations within volumes and qtrees.

Data ONTAP always maps the user's Windows identity to the user's UNIX identity during the authentication process. The information about the mapped UNIX user and the UNIX user's groups are saved with the Windows user's credential. Hence, a user credential also contains its mapped UNIX credential.

Data ONTAP maps user names. It does not map groups. However, because group membership is critically important when determining file access, as part of the mapping process the mapped UNIX user's group membership is retrieved and cached along with the user mapping information.

Related concepts

Related tasks

How name mapping works

Data ONTAP goes through a number of steps when attempting to map user names. They include checking the local name mapping database and LDAP, trying the user name, and using the default user if configured.

When Data ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which

order is determined by the `-nm-switch` parameter of the Storage Virtual Machine (SVM) configuration.

- For Windows to UNIX mapping

  If no mapping is found, Data ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and it cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

  If no mapping is found, Data ONTAP tries to find a Windows account that matches the UNIX name in the CIFS domain. If this does not work, it uses the default CIFS user, provided that it is configured. If the default CIFS user is not configured and it cannot obtain a mapping this way either, mapping fails and an error is returned.

How file and share permissions are used to secure SMB access

Authorization is the process of determining what an authenticated entity can do. Authorization includes share permissions as well as file permissions. Authorization as it relates to file access determines what an entity can do to files and folders contained on the Storage Virtual Machine (SVM).

Share permissions and file permissions are both evaluated to determine effective permissions that determine what file and folder access requests a user is authorized to perform.

- Share permissions control what a user can do over an SMB connection.
- File permissions control what a user can do on the files and folders to which the permissions are applied.

  File permissions are effective regardless of whether SMB or NFS is used to access the data.

Related concepts

How Data ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, Data 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. Data ONTAP does not set any NTFS ACLs using the constructed ACL.

How to manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in UNIX or mixed security-style qtrees or volumes on Storage Virtual Machines (SVMs) with FlexVol volumes, 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 UNIX security-style volume or qtree. This is also true for a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  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 the listed entries and then 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 UNIX security objects and adding 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.

Role export policies play with SMB access

Export policies for SMB access are optional starting with Data ONTAP 8.2, and they are disabled by default. Export policies for SMB can be enabled if desired to provide a third layer of SMB access control, along with share and file permissions.

Related concepts

Securing SMB access using export policies on page 148

Very large CIFS configuration changes might take some time to finish

When you enter CLI commands on the storage system, they are typically executed instantaneously. However, when the CLI command results in a large CIFS configuration change, it might take a while for the configuration change to finish after you entered the CLI command and received confirmation that it was successful.

The larger the change and the more objects are affected, the longer it can take to complete. Examples for this delay are creating several thousand new shares or modifying several thousand share ACLs. The following command areas are affected by this delay:

- Servers
- Home directories
- Shares
- Share ACLs
- Superusers
- Symlink path mapping
- Server security

If you make such very large configuration changes, allow time for the changes to finish.

Configuring and managing Active Directory computer accounts for SVMs (no CIFS license)

You can create and manage an Active Directory (AD) computer account for a Storage Virtual Machine (SVM, formerly known as Vserver) even if you do not have CIFS licensed on any of the cluster nodes. You can also configure and manage preferred domain controllers for the AD computer account.

How to choose whether to create a CIFS server or an Active Directory computer account

You can configure your Storage Virtual Machine (SVM) with a CIFS server that is a member of an Active Directory domain, or if you do not have CIFS licensed, you can create a computer account for your SVM on an Active Directory domain. You need to understand how the configurations differ and how to choose whether you should create a CIFS server or an Active Directory computer account on your SVM.

You can only have one Active Directory account per SVM. Therefore, you must make a choice about whether to create a CIFS server or an Active Directory computer account.

- If you currently have an Active Directory computer account configured on the SVM and you subsequently license CIFS on the cluster and want to create a full-function CIFS server on the SVM, you must first delete the Active Directory computer account.
- If you currently have a CIFS server on the SVM and you subsequently do not need a full CIFS server on the SVM and want to configure an Active Directory computer account instead, you must first delete the CIFS server.

CIFS server

You should choose to create a CIFS server if the following is true:

- You have CIFS licensed on the cluster.
  The CIFS license can be on one or more nodes.
- You want to offer file services and other value-add CIFS functionality, such as home directories or symlink access to SMB clients.

Active Directory computer account

You should choose to create an Active Directory machine account if the following is true:

- You do not have CIFS licensed on the cluster.

- You want to create an Active Directory computer account for the SVM and use it for purposes other than file services or value-add CIFS functionality.

  For example, you might want to use an Active Directory account as the service account for applications accessing data over the iSCSI or FC protocols.

Related concepts

Managing Active Directory computer accounts on page 28
Setting up the CIFS server on page 41

Managing Active Directory computer accounts

You can manage Active Directory computer accounts by creating, displaying information about, or deleting the computer account, changing the domain to which the computer account belongs, and changing or resetting the computer account password.

Related concepts

How to choose whether to create a CIFS server or an Active Directory computer account on page 27
Setting up CIFS servers on SVMs with FlexVol volumes on page 40

Creating Active Directory computer accounts for SVMs

You can create an Active Directory computer account for your Storage Virtual Machine (SVM) if you want the SVM to have a computer account in the domain, but do not want to license CIFS or do not need to configure SMB file access or CIFS value-add functionality.

Before you begin

- The cluster time must be synchronized to within five minutes of the time on the Active Directory domain controllers for the domain to which you want to associate the SVM computer account.

  The recommendation is to configure cluster NTP services to use the same NTP servers for time synchronization as the Active Directory domain uses or to use the Active Directory domain controllers as the cluster time servers.
- You must have sufficient permissions to add a computer account to the OU (organizational unit) in the domain to which you want to associate the SVM computer account.
- DNS must be configured on the SVM, and the DNS servers must either be set to the Active Directory-integrated DNS for the domain to which you want to associate the computer account, or the DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

About this task

You must keep the following in mind when creating the Active Directory computer account:

- The Active Directory computer account name can be up to 15 characters in length.
  Characters that are not allowed include the following: @ # * ( ) = + [ ] | ; : " , < > \ / and ?
- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default is to add the Active Directory computer account to the CN=Computer object.
  You can choose to add the computer account to a different OU by using the optional `-ou` option.
  When specifying the OU, you do not specify the domain portion of the distinguished name, you
  only specify the OU or CN portion of the distinguished name. Data ONTAP appends the value
  provided for the required `-domain` parameter onto the value provided for `-ou` parameter to
  produce the Active Directory distinguished name, which is used when creating the Active
  Directory computer account object.

Steps

1. Create the Active Directory computer account:

   vserver active-directory create -vserver *vserver_name* -account-name
   ***NetBIOS_account_name* -domain *FQDN* [-ou *organizational_unit*]**

2. Verify that the Active Directory computer account has been created in the desired OU by using
   the `vserver active-directory show` command.

   Example

   The following command creates the Active Directory computer account named vs1 for SVM
   vs1 in the myexample.com domain. The computer account is placed in the
   OU=eng,DC=myexample,DC=com container.

   ```
   cluster1::> vserver active-directory create -vserver vs1 -account-name vs1 -
   domain myexample.com -ou OU=eng

   In order to create an Active Directory machine account, you must supply the
   name and password of a Windows account with sufficient privileges to add
   computers to the "OU=eng" container within the "myexample.com" domain.

   Enter the user name: Admin_user

   Enter the password:

   cluster1::> vserver active-directory show

                   Account      Domain/Workgroup
    Vserver        Name         Name
    -------------- -----------  ----------------
    vs1            VS1          MYEXAMPLE
   ```

Changing the Active Directory domain to which the SVM computer account is associated

You can change the Active Directory domain to which the Storage Virtual Machine (SVM) computer
account is associated. This can be useful if you want to use an account from another domain for an

application's service account or if you are migrating SVM resources used by applications to another domain.

Before you begin

- The time set on the cluster nodes must match to within five minutes of the time set on the Active Directory domain controllers for the domain to which you want to associate the SVM computer account.

  The recommendation is to configure cluster NTP services to use the same NTP servers for time synchronization as the new Active Directory domain uses or to use the Active Directory domain controllers of the new domain as the cluster time servers.
- You must have sufficient permissions to add a computer account to the OU (organizational unit) in the new domain to which you want to associate the SVM computer account.
- The DNS servers for the SVM must either be set to the Active Directory-integrated DNS for the new domain to which you want to associate the SVM computer account, or the DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

About this task

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- When changing the domain to which the Active Directory computer account is associated, the computer account in the new domain is placed in the CN=Computers container.

  You cannot specify where to place the computer account when changing the domain. If you want the location of the computer account to be in a container other than CN=Computers container, you must delete the Active Directory account and re-create it by using the `vserver active-directory create` command.

Steps

1. Change the domain of the Active Directory computer account:

   `vserver active-directory modify -vserver vserver_name -domain FQDN`

2. Verify that the Active Directory computer account has been created in the CN=Computer by using the `vserver active-directory show` command.

   > **Example**
   >
   > The following command changes the domain for the Active Directory computer account named vs1 for SVM vs1 to the example.com domain. The computer account is placed in the CN=Computers container.
   >
   > ```
   > cluster1::> vserver active-directory modify -vserver vs1 -domain example.com
   >
   > In order to create an Active Directory machine account, you must supply the
   > name and password of a Windows account with sufficient privileges to add
   > computers to the "CN=Computers" container within the "example.com" domain.
   >
   > Enter the user name: Admin_user
   > ```

```
Enter the password:

cluster1::> vserver active-directory show

                Account      Domain/Workgroup
 Vserver        Name         Name
 -------------- -----------  ----------------
 vs1            VS1          EXAMPLE
```

Displaying information about Active Directory computer accounts for SVMs

You can display information about Active Directory computer accounts for Storage Virtual Machines (SVMs), including the SVM computer account name, the name of the domain to which the computer account is associated, and the organizational unit where the computer account is located.

Step

1. Display information about Active Directory computer accounts for SVMs by using the vserver active-directory show command.

   You can customize the view by specifying optional parameters. See the man page for the command for details.

   Examples

   The following command displays information about all Active Directory accounts for SVMs on the cluster:

   ```
   cluster1::> vserver active-directory show

                   Account      Domain/Workgroup
    Vserver        Name         Name
    -------------- -----------  ----------------
    vs1            CIFSSERVER1  EXAMPLE
    vs2            CIFSSERVER2  EXAMPLE2
   ```

   The following command displays detailed information about all Active Directory accounts for SVMs on the cluster:

   ```
   cluster1::> vserver active-directory show -instance

                                         Vserver: vs1
             Active Directory account NetBIOS Name: CIFSSERVER1
                   NetBIOS Domain/Workgroup Name: EXAMPLE
                     Fully Qualified Domain Name: EXAMPLE.COM
                             Organizational Unit: CN=Computers

                                         Vserver: vs2
             Active Directory account NetBIOS Name: CIFSSERVER2
                   NetBIOS Domain/Workgroup Name: EXAMPLE
   ```

```
                              Fully Qualified Domain Name: EXAMPLE2.COM
                                       Organizational Unit: CN=Computers
```

Deleting Active Directory computer accounts for SVMs

If you no longer want a Storage Virtual Machine (SVM) to have a computer account in an Active Directory domain or if you want to configure a CIFS server on the SVM instead of an Active Directory computer account, you can delete the computer account.

Before you begin

You must have sufficient permissions to delete a computer account from the OU (organizational unit) in the Active Directory domain that contains the SVM computer account.

About this task

The SVM can have either an Active Directory computer account or a CIFS server, but it cannot have both. If you currently have an Active Directory computer account on your SVM and want to create a CIFS server on that SVM, you must first delete the Active Directory computer account before you can create the CIFS server.

Steps

1. Delete the Active Directory computer account:

   vserver active-directory delete -vserver *vserver_name*

   You are asked to enter the user name and password of a user with sufficient permission to delete the computer account from the OU where the computer account is located.

2. Verify that the computer account is deleted:

   vserver active-directory show

Example

The following command deletes the Active Directory computer account on SVM vs2:

```
cluster1::> vserver active-directory show

              Account      Domain/Workgroup
 Vserver      Name         Name
 -------------- ----------- ----------------
 vs1          VS1          EXAMPLE
 vs2          VS2          MYEXAMPLE

cluster1::> vserver active-directory delete -vserver vs2

In order to delete an Active Directory machine account, you must supply the
name and password of a Windows account with sufficient privileges to remove
computers from the "example.com" domain.
```

```
Enter the user name: Admin_user

Enter the password:

cluster1::> vserver active-directory show

              Account     Domain/Workgroup
 Vserver      Name        Name
 ------------- ----------- ----------------
 vs1          VS1         EXAMPLE
```

Changing or resetting Active Directory computer account passwords for SVMs

You can change the password for the Active Directory computer account for good security practices, or reset it if the password is lost.

Step

1. Perform one of the following actions:

If you...	Use the command...
Know the password and want to change it	**vserver active-directory password-change -vserver vserver_name**
Do not know the password and want to reset it	**vserver active-directory password-reset -vserver vserver_name**
	A password reset might be required if the password stored along with the machine account in the Active Directory domain is changed or reset by something other than by the Storage Virtual Machine (SVM). The operation requires the credentials for a user with permission to reset the password in the organizational unit (OU) that contains the computer account.

-vserver is the name of the SVM associated with the Active Directory account whose domain password you want to change or reset.

Managing domain controller connections for Active Directory computer accounts

You can manage domain controller connections for Active Directory computer accounts by displaying information about discovered Active Directory servers, resetting and rediscovering the Active Directory servers, configuring a list of preferred domain controllers, and displaying the list of preferred domain controllers.

Displaying information about discovered Active Directory servers for SVMs

You can display information related to discovered LDAP servers and domain controllers for the domain to which the Storage Virtual Machine (SVM) computer account is associated.

About this task

The `vserver active-directory discovered-servers show` command is an alias of the `vserver cifs domain discovered-servers show` command. You can use either command to display information about discovered Active Directory servers on your SVM.

Step

1. To display all or a subset of the information related to discovered servers, enter the following command:

   `vserver active-directory discovered-servers show`

   By default, the command displays the following information about discovered servers:

   - Node name
   - SVM name
   - Active Directory domain name
   - Server type
   - Preference
   - Domain controller name
   - Domain controller address
   - Status

   You can customize the view by specifying optional parameters. See the man page for the command for details.

   Example

   The following command shows discovered servers for SVM vs1:

   ```
   cluster1::> vserver active-directory discovered-servers show -vserver vs1

   Node: node1
   Vserver: vs1

   Domain Name    Type      Preference DC-Name         DC-Address       Status
   ------------- --------- ---------- --------------- ---------------- -------
   ""             NIS       preferred  192.168.10.222  192.168.10.222  OK
   example.com    MS-LDAP   adequate   DC-1            192.168.192.24  OK
   example.com    MS-LDAP   adequate   DC-2            192.168.192.25  OK
   example.com    MS-DC     adequate   DC-1            192.168.192.24  OK
   example.com    MS-DC     adequate   DC-2            192.168.192.25  OK
   ```

Resetting and rediscovering Active Directory servers

Resetting and rediscovering Active Directory servers on your Storage Virtual Machine (SVM) enables the SVM to discard stored information about LDAP servers and domain controllers. After discarding server information, the SVM reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

About this task

The `vserver active-directory discovered-servers reset-servers` command is an alias of the `vserver cifs domain discovered-servers reset-servers` command. You can use either command to reset and rediscover Active Directory servers on your SVM.

Steps

1. Enter the following command:

   `vserver active-directory discovered-servers reset-servers -vserver vserver_name`

2. Display information about the newly rediscovered servers:

   `vserver active-directory discovered-servers show -vserver vserver_name`

Example

The following command resets and rediscovers servers for SVM vs1:

```
cluster1::> vserver active-directory discovered-servers reset-servers -
vserver vs1

cluster1::> vserver active-directory discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type      Preference DC-Name     DC-Address   Status
--------------  --------  ---------- ----------- -----------  -------
""              NIS       preferred  1.1.3.4     1.1.3.4      OK
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
```

Adding or removing preferred domain controllers

Data ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers on the Storage Virtual Machine (SVM) for the domain in which the Active Directory computer account is configured.

About this task

The `vserver active-directory preferred-dc add` and `vserver active-directory preferred-dc remove` commands are aliases of the `vserver cifs domain preferred-dc add` and `vserver cifs domain preferred-dc remove` commands respectively. You can use either set of commands to manage preferred domain controllers for the Active Directory domain account.

Step

1. Perform one of the following actions:

If you want to...	Use the command...
Add preferred domain controllers	`vserver active-directory preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...`
Remove preferred domain controllers	`vserver active-directory preferred-dc remove -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...`

`-vserver vserver_name` specifies the SVM name.

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

`-preferred-dc IP_address`, ... specifies one or more IP addresses of the preferred domain controllers to add or remove, as a comma-delimited list. When adding preferred domain controllers, the order of the comma-delimited list indicates order of preference.

Examples

The following command adds domain controller IP addresses 10.1.1.10 and 10.1.1.20 to the list of preferred domain controllers that SVM vs1 uses to manage external access to the example.com domain. The example.com domain contains the SVM Active Directory account.

```
cluster1::> vserver active-directory preferred-dc add -vserver vs1 -domain
example.com -preferred-dc 10.1.1.10,10.1.1.20
```

The following command removes the domain controller IP address 10.1.1.20 from the list of preferred domain controllers that Storage Virtual Machine (SVM) vs1 uses to manage external access to the example.com domain.

```
cluster1::> vserver active-directory preferred-dc remove -vserver vs1 -
domain example.com -preferred-dc 10.1.1.20
```

Displaying information about preferred domain controllers

You can display information about the list of preferred domain controllers for the domain to which the Active Directory computer account for the Storage Virtual Machine (SVM) is associated. This can be helpful when you want to know which domain controllers are contacted preferentially.

About this task

The vserver active-directory preferred-dc show command is an alias of the vserver cifs domain preferred-dc show command. You can use either command to display information about preferred domain controllers for the Active Directory domain account.

Step

1. To display all or a subset of the information related to discovered preferred domain controllers, enter the following command:

   vserver active-directory preferred-dc show

   By default, the command displays the following information about preferred domain controllers:

   - SVM name
   - Active Directory domain name
   - List of IP addresses of the preferred domain controllers

   You can customize the view by specifying optional parameters. See the man page for the command for details.

Example

The following command displays all preferred domain controllers for SVM vs1:

```
cluster1::> vserver active-directory preferred-dc show -vserver vs1

Vserver    Domain Name          Preferred Domain Controllers
---------  ------------------   ----------------------------
vs1        example.com          10.1.1.10, 10.1.1.20
```

Configuring and managing CIFS servers

You can configure and manage CIFS servers to let SMB clients access files on your cluster. Each data Storage Virtual Machine (SVM) in the cluster can be bound to exactly one Active Directory domain; however, the data SVMs do not need to be bound to the same domain. Each data SVM can be bound to a unique Active Directory domain.

Supported SMB clients and domain controllers

Before you can use SMB with your Storage Virtual Machine (SVM), you need to know which SMB clients and domain controllers Data ONTAP supports.

For the latest information about which SMB clients and domain controllers Data ONTAP supports, see the Interoperability Matrix at *support.netapp.com/matrix*.

Unsupported Windows features

Before you use CIFS in your network, you need to be aware of certain Windows features that Data ONTAP does not support.

Data ONTAP does not support the following Windows features:

- Encrypted File System (EFS)
- Logging of NT File System (NTFS) events in the change journal
- Microsoft File Replication Service (FRS)
- Microsoft Windows Indexing Service
- Remote storage through Hierarchical Storage Management (HSM)
- Quota management from Windows clients
- Windows quota semantics
- The LMHOSTS file
- NTFS native compression

Where to find information about SMB support on Infinite Volumes

For information about the SMB versions and functionality that Infinite Volumes support, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

How to choose whether to create a CIFS server or an Active Directory computer account

You can configure your Storage Virtual Machine (SVM) with a CIFS server that is a member of an Active Directory domain, or if you do not have CIFS licensed, you can create a computer account for your SVM on an Active Directory domain. You need to understand how the configurations differ and how to choose whether you should create a CIFS server or an Active Directory computer account on your SVM.

You can only have one Active Directory account per SVM. Therefore, you must make a choice about whether to create a CIFS server or an Active Directory computer account.

- If you currently have an Active Directory computer account configured on the SVM and you subsequently license CIFS on the cluster and want to create a full-function CIFS server on the SVM, you must first delete the Active Directory computer account.
- If you currently have a CIFS server on the SVM and you subsequently do not need a full CIFS server on the SVM and want to configure an Active Directory computer account instead, you must first delete the CIFS server.

CIFS server

You should choose to create a CIFS server if the following is true:

- You have CIFS licensed on the cluster.
  The CIFS license can be on one or more nodes.
- You want to offer file services and other value-add CIFS functionality, such as home directories or symlink access to SMB clients.

Active Directory computer account

You should choose to create an Active Directory machine account if the following is true:

- You do not have CIFS licensed on the cluster.
- You want to create an Active Directory computer account for the SVM and use it for purposes other than file services or value-add CIFS functionality.
  For example, you might want to use an Active Directory account as the service account for applications accessing data over the iSCSI or FC protocols.

Related concepts

Setting up CIFS servers on SVMs with FlexVol volumes

You can enable and configure CIFS servers to let SMB clients access files on your cluster. There are a number of tasks to plan and to complete when setting up a CIFS server on a Storage Virtual Machine (SVM) with FlexVol volumes.

For more information about setting up CIFS servers on Storage Virtual Machines (SVMs) with Infinite Volume, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Prerequisites for CIFS server setup

CIFS licensing, time services, and network routing prerequisites must be met before you begin the CIFS server setup process.

- CIFS must be licensed on the cluster.
- Time services must be set up on the cluster.

  The cluster must be synchronized to a reliable time source to ensure that CIFS server creation succeeds. During the CIFS server creation process, Data ONTAP must use Kerberos authentication to authenticate with the domain that you want the CIFS server to join. Kerberos authentication requires, by default, that the time configured on a requesting host match, within five minutes, the time configured on the Kerberos server. If the cluster's time does not match to within five minutes of the time configured on the domain controller, CIFS setup fails.

- Prior to creating the CIFS server, there must be a route to an Active Directory domain controller for the domain to which you want to join the CIFS server.

  If there are no data LIFs present for each Storage Virtual Machine (SVM) and the node management LIFs are on a segment that does not route to the Active Directory server, CIFS setup fails. A route to the Active Directory server can be provided by either of two ways:

  - By configuring the node management LIFs to be on a network segment that can route to an Active Directory domain controller
  - By configuring at least one SVM data LIF on the SVM that can route to the Active Directory domain controller prior to creating the CIFS server

Related concepts

Setting up the CIFS server

Setting up the CIFS server involves completing the CIFS server configuration worksheet, creating the Storage Virtual Machine (SVM) with the proper setting for CIFS access, configuring DNS on the SVM, creating the CIFS server, and, if necessary, setting up UNIX user and group name services.

Before you set up your CIFS server, you must understand the choices you need to make when performing the setup. You should make decisions regarding the SVM, DNS, and CIFS server configurations and record your choices in the planning worksheet prior to creating the configuration. This can help you in successfully creating a CIFS server.

Creating SVMs can only be completed by a cluster administrator.

Steps

1. Completing the CIFS server setup configuration worksheet on page 42
Use this worksheet to record the values that you need during the CIFS server setup process. As part of completing the worksheet, you need to record the information you need to create the Storage Virtual Machine (SVM), configure DNS services, and create the CIFS server.

2. Creating an SVM with FlexVol volumes for the CIFS server (cluster administrators only) on page 46
You must first create a Storage Virtual Machine (SVM) with a configuration that is appropriate for hosting a CIFS server. Before you create the SVM, you must choose the aggregate that holds the root volume.

3. Configuring DNS on the SVM on page 48
You must configure DNS on the Storage Virtual Machine (SVM) before creating the CIFS server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the CIFS server will join.

4. Creating a CIFS server on page 49
A CIFS server is necessary to provide SMB clients with access to the Storage Virtual Machine (SVM). After you set up DNS services on the SVM, you can create a CIFS server.

5. Configuring name services on the SVM on page 51
With SMB access, user mapping to a UNIX user is always performed, even if accessing data in an NTFS security-style volume. If you map Windows users to corresponding UNIX users whose information is stored in NIS or LDAP directory stores, you should configure these name services during CIFS setup.

Related concepts

Prerequisites for CIFS server setup on page 40
Setting up network access for the CIFS server on page 51

Completing the CIFS server setup configuration worksheet

Use this worksheet to record the values that you need during the CIFS server setup process. As part of completing the worksheet, you need to record the information you need to create the Storage Virtual Machine (SVM), configure DNS services, and create the CIFS server.

Information for creating an SVM with FlexVol volumes

Note: For information about creating an SVM with Infinite Volume, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Types of information	Your values
SVM name The name you want to assign to the SVM. The SVM name can contain alphanumeric characters and the following special characters: . - _ However, the name of the SVM should not start with a number or the following special characters: . - The maximum number of characters allowed in an SVM name is 47. You must specify the SVM name.	
Name for SVM root volume You must specify the name you want to assign to the root volume. The root volume's name must start with an alphabetic character (a to z or A to Z) and be 203 or fewer characters in length.	
Name of the aggregate that holds the SVM root volume You must specify an aggregate name. The aggregate must exist.	
Security style for the SVM root volume You must specify a security style for the root volume. Possible values are `ntfs`, `unix`, and `mixed`.	

Types of information	Your values
UNIX user and group name services for the SVM You must specify the sources that are searched for name service information and the order in which they are searched. This parameter provides the functionality of the `/etc/nsswitch.conf` file on UNIX systems. Supported name services for storing local UNIX user and group information are local files, NIS, and LDAP. You can configure one or more of the name services. UNIX name services are important in an SMB environment, even one that provides access using SMB connections only, with no NFS access. This is because during the SMB session setup, Data ONTAP always performs Windows to UNIX user mapping when constructing the SMB credential. You must specify which name services to use. > **Note:** If you do not want to create a Windows to UNIX name mapping scheme, you can choose to automatically map Windows users to the default UNIX user. When you create an SVM, Data ONTAP automatically creates a UNIX user named "pcuser" in the local files and assigns that user as the default UNIX user. You must configure `files` as one of the name services if you want to use the local "pcuser" as the default UNIX user. For more information about configuring name services for UNIX users and groups, see the *Clustered Data ONTAP File Access Management Guide for NFS*.	
User mapping name services for the SVM You can optionally specify the sources (local files or LDAP) that are searched for name mapping information and the order in which they are searched. The default name service for user mapping is local files. If you plan to configure the CIFS server to use the default UNIX user, or if you plan to use local files to store user mapping information, it is not necessary to specify a value for this parameter. You should specify this parameter for the two following scenarios: • Use this parameter if you want to use LDAP for storing user mapping information. • Use this parameter if you want to use both local files and LDAP for storing user mapping information.	

Types of information	Your values
SVM language setting You can optionally specify the default language to use for the SVM and its volumes. If you do not specify a default language, the default SVM language is set to C.UTF-8. The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. **Note:** The language of the SVM with FlexVol volumes can be modified after the SVM is created. For more information about setting the SVM language, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.	
Snapshot policy You can optionally specify the Snapshot policy to apply to the SVM. If you do not specify a Snapshot policy, the default cluster Snapshot policy is applied to the SVM. This policy is enabled by default. By default, the Snapshot policy is inherited by the volumes on the SVM. You can change which Snapshot policy is applied to the SVM at any time. See the Snapshot copy section of the *Clustered Data ONTAP Logical Storage Management Guide* for more information about Snapshot policies.	
Quota policy You can optionally specify the quota policy to apply to the SVM. If you do not specify a quota policy, a blank quota policy named "default" is created and applied to the SVM. By default, the quota policy is inherited by the volumes on the SVM. You can change which quota policy is applied to the SVM at any time. This setting is supported only on SVMs with FlexVol volumes. See the quota section of the *Clustered Data ONTAP Logical Storage Management Guide* for more information about quotas.	

Information for configuring DNS

Types of information	Values
IP addresses of the DNS servers List of IP addresses for the DNS servers that will provide name resolution for the CIFS server. The listed DNS servers must contain the service location DNS records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join. The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. CIFS server creation fails if Data ONTAP cannot obtain the service location records through local DNS queries. The simplest way to ensure that Data ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers. However, you can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers. For information about the Active Directory-integrated SRV records, see the topic *How DNS Support for Active Directory Works*: *Microsoft TechNet: technet.microsoft.com/en-us/library/cc759550(WS.10).aspx* on Microsoft TechNet.	
DNS domain name List of domain names to append to a host name when doing host-to-IP name resolution. List the local domain first, followed by the domain names for which DNS queries are most often made.	

Information for creating a CIFS server on the SVM

Types of information	Values
SVM name The name of the SVM you created to host the CIFS server. You must specify the SVM name.	
CIFS server name The name of the CIFS server. The CIFS server name can be the same as or different from the SVM name. The CIFS server name can be up to 15 characters. Characters that are not allowed include the following characters: @ # * ( ) = + [ ] | ; : " , < > \ / ? You must specify the CIFS server name.	

Types of information	Values
Domain name The FQDN of the Active Directory domain that you want the CIFS server to join. A CIFS server appears as a member Windows server object in the Active Directory store. You must specify the domain name.	
Organizational unit The organizational unit within the Active Directory domain where you want the CIFS server computer object placed. This is an optional setting. By default, the CIFS server computer object storage location is CN=Computers.	

Creating an SVM with FlexVol volumes for the CIFS server (cluster administrators only)

You must first create a Storage Virtual Machine (SVM) with a configuration that is appropriate for hosting a CIFS server. Before you create the SVM, you must choose the aggregate that holds the root volume.

Before you begin

- The aggregate on which you want to create the SVM root volume must exist.
- You must know which security style the root volume will have.

  If you plan to implement a Hyper-V or SQL over SMB solution on this SVM, the recommendation is to use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style volumes.
- You must know which name services to configure.

About this task

This task can only be completed by a cluster administrator.

For information about creating an SVM with Infinite Volume, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume by displaying information about all the aggregates in the cluster except for the ones that are node root aggregates:

   ```
   storage aggregate show -has-mroot false
   ```

   You must choose an aggregate that has at least 1 GB of free space to contain the root volume.

2. Record the name of the aggregate on which you want to create the SVM's root volume.

3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

```
vserver create -language ?
```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume snapshot policy show -vserver vserver_name
```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create the CIFS server:

```
vserver create -vserver vserver_name -aggregate aggregate_name -
rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed}
-ns-switch {nis|file|ldap},... [-nm-switch {file|ldap},...] [-language
language [-snapshot-policy snapshot_policy_name] [-quota-policy
quota_policy_name] -comment comment]
```

-ns-switch specifies which directory stores to use for UNIX user and group information and the order in which they are searched.

-nm-switch specifies which directory store to use for name mapping information and the order in which they are searched.

7. Verify that the SVM configuration is correct by using the vserver cifs show command.

Example

The following command creates the SVM named "vs1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style. Only local files name services is configured for storing UNIX user and group information. Local files are used for name mapping storage.

```
cluster1::> storage aggregate show -has-mroot false

Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ ------------
aggr1     239.0GB   229.8GB    4% online      4 node1  raid_dp,
                                                         normal
aggr2     239.0GB   235.9GB    1% online      2 node2  raid_dp,
                                                         normal
aggr3     478.1GB   465.2GB    3% online      1 node3  raid_dp,
                                                         normal

cluster1::> vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root -ns-
switch file -rootvolume-security-style ntfs -language en_US
[Job 72] Job succeeded:              Vserver creation completed

cluster1::> vserver show -vserver vs1

                            Vserver: vs1
                       Vserver Type: data
                       Vserver UUID: 11111111-1111-1111-1111-111111111111
                        Root Volume: vs1_root
```

```
                                    Aggregate: aggr3
                         Name Service Switch: file
                         Name Mapping Switch: file
                                   NIS Domain: -
                   Root Volume Security Style: ntfs
                                  LDAP Client: -
                                     Language: en_US
                              Snapshot Policy: default
                                      Comment:
                    Antivirus On-Access Policy: default
                                 Quota Policy: default
                    List of Aggregates Assigned: -
   Limit on Maximum Number of Volumes allowed: unlimited
                          Vserver Admin State: running
                            Allowed Protocols: nfs, cifs, ndmp
                         Disallowed Protocols: fcp, iscsi
              Is Vserver with Infinite Volume: false
                             QoS Policy Group: -
```

Related tasks

[*Modifying protocols for SVMs*](#) on page 103

Configuring DNS on the SVM

You must configure DNS on the Storage Virtual Machine (SVM) before creating the CIFS server.
Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain
that the CIFS server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain
LDAP and domain controller servers. If the Storage Virtual Machine (SVM) cannot find the Active
Directory LDAP servers and domain controllers, CIFS server setup fails.

Steps

1. Configure DNS services:

   **vserver services dns create -vserver *vserver_name* -domains *FQDN*[,...] -
   name-servers *IP-address*[,...]**

   The domain path is constructed from the values in the -domains parameter.

2. Verify that the DNS configuration is correct and that the service is enabled by using the vserver
   services dns show command.

Example

The following example configures the DNS service on Storage Virtual Machine (SVM) vs1:

```
cluster1::> vserver services dns create -vserver vs1 -domains
iepubs.local,example.com -name-servers 10.1.1.50,10.1.1.51

cluster1::> vserver services dns show -vserver vs1
                                                Name
```

```
Vserver   State      Domains                       Servers
--------  ---------  ----------------------------  -------------
vs1       enabled    iepubs.local, example.com     10.1.1.50,
                                                    10.1.1.51
```

Creating a CIFS server

A CIFS server is necessary to provide SMB clients with access to the Storage Virtual Machine
(SVM). After you set up DNS services on the SVM, you can create a CIFS server.

Before you begin

- The node management LIFs must be on a network segment that can route to the Active Directory
  domain controller of the domain to which you want to join the CIFS server.
  Alternatively, at least one SVM data LIF must exist on the SVM that can route to the Active
  Directory domain controller. If there are no data LIFs present for the SVM and the node
  management LIFs are on a segment that does not route to the Active Directory server, CIFS setup
  fails.
- The cluster time must be synchronized to within five minutes of the Active Directory domain
  controller's time.
  The recommendation is to configure cluster NTP services to use the same NTP servers for time
  synchronization as the Active Directory domain uses.

About this task

You must keep the following in mind when creating the CIFS server:

- The CIFS server name can be up to 15 characters in length.
  The following characters are not allowed: @ # * ( ) = + [ ] | ; : " , < > \ / ?
- You must use the FQDN when specifying the domain.
- The default is to add the CIFS server machine account to the Active Directory CN=Computer
  object.
  You can choose to add the CIFS server to a different organizational unit (OU) by using the -ou
  option. When specifying the OU, you do not specify the domain portion of the distinguished
  name, you only specify the OU or CN portion of the distinguished name. Data ONTAP appends
  the value provided for the required -domain parameter onto the value provided for the -ou
  parameter to produce the Active Directory distinguished name, which is used when joining the
  Active Directory domain.
- The initial administrative status of the CIFS server is up.

Steps

1. Create the CIFS server on the data SVM:

   vserver cifs create -vserver *vserver_name* -domain *FQDN* [-ou
   ***organizational_unit*]**

2. Verify the CIFS server configuration by using the vserver cifs show command.

Examples

The following command creates a CIFS server named "CIFS1" on SVM vs1 and joins the CIFS server to the example.com domain. The CIFS server computer object is placed in the default CN=Computer container:

```
cluster1::> vserver cifs create -vserver vs1 -name CIFS1 -domain example.com

cluster1::> vserver cifs show -vserver vs1
            Server    Status     Domain/Workgroup Authentication
Vserver     Name      Admin      Name             Style
----------- --------- ---------- ---------------- --------------
vs1         CIFS1     up         EXAMPLE          domain
```

The following command creates a CIFS server named "CIFS1" on SVM vs1 in the example.com domain. The machine account is created in the OU=eng,OU=corp,DC=example,DC=com container.

```
cluster1::> vserver cifs create -vserver vs1 –cifs-server CIFS1 -domain
example.com –ou OU=eng,OU=corp
```

The following command creates a CIFS server named "CIFS2" on SVM vs1 in the example.com domain. The storage administrator wants to create the machine account in the OU=eng,OU=corp,DC=example,DC=com container; however the distinguished name is mistakenly used for the value of the -ou parameter. Doing so results in an error, because the SVM interprets the container location as OU=eng,OU=corp,DC=example,DC=com,DC=example,DC=com instead of OU=eng,OU=corp,DC=example,DC=com.

If the distinguished name is mistakenly used for the value of the -ou parameter, the command fails with the error message shown in the example:

```
cluster1::> vserver cifs create -vserver vs1 –cifs-server CIFS2 -domain
example.com –ou OU=eng,OU=corp,DC=example,DC=com

Error: command failed: Failed to create CIFS server CIFS2. Reason: SecD
Error: ou not found
```

Related concepts

Related tasks

Configuring name services on the SVM

With SMB access, user mapping to a UNIX user is always performed, even if accessing data in an
NTFS security-style volume. If you map Windows users to corresponding UNIX users whose
information is stored in NIS or LDAP directory stores, you should configure these name services
during CIFS setup.

About this task

You can configure the CIFS server to map all Windows users to the default UNIX user. In this case,
configuring NIS or LDAP UNIX user and group name services is optional for SMB access.

Steps

1. If UNIX users and group information is managed by NIS name services, configure NIS name
   services by using the information located in the *Clustered Data ONTAP File Access Management
   Guide for NFS*.

2. If UNIX users and group information is managed by LDAP name services, configure LDAP
   name services by using the information located in the *Clustered Data ONTAP File Access
   Management Guide for NFS*.

Setting up network access for the CIFS server

Before clients can access data stored on the CIFS server over SMB shares, you must complete the
network setup configuration worksheet, create data LIFs, configure default gateways, and add any
needed routing groups and static routes.

Before you set up network access for the CIFS server, you must understand the choices you need to
make when performing the setup. You should make decisions regarding data LIF configurations,
routing groups, default gateways, and static routes, and record your choices in the planning
worksheet prior to creating the configuration. This can help you in successfully enabling network
access to resources on the CIFS server.

Creating data LIFs, routing groups, and static routes can only be completed by a cluster
administrator.

Steps

1. [Completing the network setup worksheet](#) on page 52
   You should record the values that you need to set up the network for a CIFS server. As part of completing the network setup worksheet, you need to enter information about the CIFS server data LIFs. You also need to record information about the default gateways, and optionally, for custom routing groups and static routes.

2. [Creating data LIFs (cluster administrators only)](#) on page 55
   Before you can provide SMB access to the CIFS server, you must create data LIFs.

3. [Creating default gateways, static routes, and routing groups (cluster administrators only)](#) on page 57
   After you create data LIFs on the Storage Virtual Machine (SVM), you configure the default gateways by adding the default routes to the CIFS server's routing groups. You can also add additional static routes to the routing groups.

Related concepts

[Prerequisites for CIFS server setup](#) on page 40
[Setting up the CIFS server](#) on page 41

Completing the network setup worksheet

You should record the values that you need to set up the network for a CIFS server. As part of completing the network setup worksheet, you need to enter information about the CIFS server data LIFs. You also need to record information about the default gateways, and optionally, for custom routing groups and static routes.

Information for creating LIFs on the Storage Virtual Machine (SVM)

Types of information	Values
Data LIF names The name to give to the logical network interfaces that clients use when accessing data from the CIFS server. You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports. To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes. You can provide descriptive names for the interfaces. For example, you can name the data LIFs according to the node assigned as their home node. For example, you can name a LIF whose home node is node1 " lif1", a LIF whose home node is node2 "lif2", and so on.	

Types of information	Values
Protocols allowed on the data LIFs Protocols that can use the data LIFs (CIFS, NFS, FlexCache, iSCSI, FC, and none). This is an optional setting. By default, CIFS, NFS, and FlexCache are allowed. **Note:** Protocols that can use the LIF cannot be modified after the LIF is created. If you might want to allow other protocols on the data LIF at a future time, you should configure the LIF to allow those protocols during LIF creation.	
Data LIF home node The home node is the node to which the logical interface returns when the LIF is reverted to its home port. Record a home node for each data LIF.	
Data LIF home port The home port is the port to which the logical interface returns when the LIF is reverted to its home port. Record a home port for each data LIF.	
Data LIF IP addresses You can configure SVM data LIFs that are on different subnets. The recommendation is to have at least two data LIFs per subnet so that there is no single point of failure for data access through a subnet. Record an IP address for each data LIF.	
Data LIF network mask There might be more than one netmask, depending on whether data LIF IP addresses are configured for more than one subnet.	
Optional custom routing groups Data ONTAP automatically creates a routing group that is appropriate for the netmask that the cluster administrator provided when creating the data LIF. If an appropriate routing group exists, Data ONTAP assigns the existing routing group to the LIF. You can optionally create your own custom routing group.	
Data LIF default gateway IP address There might be more than one default gateway, depending on whether data LIF IP addresses are configured for more than one subnet.	

Types of information	Values
Optional static routes for the data LIF You can configure optional static routes for the routing groups assigned to the data LIFs.	

Information for DNS entries on the DNS server for the data LIFs

After you configure your data LIFs, the DNS administrator must create DNS "A" and "PTR" records for the IP addresses assigned to the data LIFs. To load balance client connections to the assigned data IP addresses, you must create multiple "A" records that all point to the same host name. DNS load balances connections that are made using the host name to the assigned IP addresses in a round-robin fashion.

> **Note:** If you assigned the CIFS server a name that is different from the SVM name, you must create DNS entries that point to the CIFS server name instead of the SVM name. Clients must use the CIFS server name when connecting to SMB shares, not the SVM name.

> For example, if you create a CIFS server named "CIFS1" in the EXAMPLE.LOCAL domain that is hosted on the SVM named vs1 and assign the IP addresses 10.1.1.1, 10.1.1.2, 10.1.1.3, and 10.1.1.4 to the four data LIFs, your DNS "A" record entries are as follows:

> ```
> 10.1.1.1 A CIFS1.EXAMPLE.COM CIFS1
> 10.1.1.2 A CIFS.EXAMPLE.COM CIFS1
> 10.1.1.3 A CIFS1.EXAMPLE.COM CIFS1
> 10.1.1.4 A CIFS1.EXAMPLE.COM CIFS1
> ```

> If an NFS server is also configured on the SVM where clients access data over NFS using the same data LIFs and the CIFS server name is different than the SVM name, you must consider what DNS name you want to use to access data over NFS.

> You can choose to use the same DNS name that you are using to access data over SMB (the CIFS server name), or you can access data over NFS by using a different host name. If you use another host name when accessing data over NFS, you must also create a set of "A" and "PTR" records that point to that host name. This host name can be the same as the SVM name, or you can use another host name you have chosen specifically for NFS access. If you record the chosen host name in DNS, NFS clients can use this name when mounting an export.

There is an alternative method for creating the data LIF DNS records and managing DNS load balancing for the CIFS server. Data ONTAP supports onboard SVM DNS load balancing using DNS delegation. To learn more about SVM DNS load balancing, see the section about balancing network loads in the *Clustered Data ONTAP Network Management Guide* and the knowledge base article *How to set up DNS load balancing in Cluster-Mode* at *support.netapp.com*.

Types of information	Values
DNS A and PTR records for the CIFS server You need to create "A" and "PTR" records for IP addresses assigned to the data LIFs. The host name for these records is the CIFS server name.	
Optional: DNS A and PTR record for a hostname you want to use to provide access using protocols other than SMB You need an additional set of "A" and "PTR" records for the data LIFs if the SVM provides access to NFS clients or to FlexCache and the host name you want to use for NFS and FlexCache access is different than the CIFS server name.	

Creating data LIFs (cluster administrators only)

Before you can provide SMB access to the CIFS server, you must create data LIFs.

Before you begin

You must have the list of IP addresses to assign to the data LIFs.

About this task

- You can associate data LIFs with ports that are assigned the data role.
- You can configure Storage Virtual Machine (SVM) data LIFs that are on different subnets.
- To use host names to connect to the CIFS server data ports, you must create DNS A and PTR record entries that assign the IP addresses to the FQDN of the CIFS server.
- You should not configure data LIFs that carry CIFS traffic to automatically revert to their home nodes.

This task can only be completed by a cluster administrator.

Steps

1. Determine what data ports are available:

   network port show -role data

2. For each node that contains aggregates on which you plan to create data volumes, create a data LIF:

   network interface create -vserver *vserver_name* **-lif** *lif_name* **-role data -home-node** *node_name* **-home-port** *port* **-address -netmask-length** *integer*

   There are a number of optional parameters that you might want to use to customize the configuration. For example, you can designate which failover policy to use or create a custom failover group.

For more information about using optional parameters, see the *Clustered Data ONTAP Network Management Guide*.

After the command executes, the following message is displayed:

```
Info: Your interface was created successfully; the routing group
<routing_group_name> was created
```

An associated routing group is automatically created when you create the first data LIF in an IP subnet. A routing group is a container for SVM routes, including the default route.

3. Record the name of the routing group.

   You need the name of the routing group when you create the default route and other static routes for the SVM.

4. Verify that the LIF network configuration is correct by using the `network interface show` command.

   You can create customized data LIF solutions using VLANs or interface groups (a logical grouping of interface ports).

   For more information, see the man pages for the `network port ifgrp` and `network port vlan` command families. For more information about configuring network solutions, see the *Clustered Data ONTAP Network Management Guide*.

5. Create the DNS `A` and `PTR` records for the data LIF IP addresses assigned to the CIFS server.

6. If necessary, create DNS `A` and `PTR` records for the data LIF IP addresses that resolve to the host name that you want to use to access data over NFS or FlexCache.

   You need to perform this step if you do not want to use the CIFS server name as the host name when accessing data over protocols other than SMB. The host name that you use for this step is commonly the SVM name, but it is not a requirement to do so.

Example

The following example creates data LIFs on node1 and node2, the two nodes that contain the aggregates that will host data volumes for SVM vs1. The CIFS server name is also named "vs1" and is a member of the IEPUB.LOCAL domain. A default route is added to the routing group that was automatically created during LIF creation. The following DNS `A` records and the corresponding `PTR` records are added to the DNS server:

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

```
cluster1::> network port show -role data -node node1
                                 Auto-Negot  Duplex      Speed (Mbps)
Node   Port   Role         Link  MTU Admin/Oper Admin/Oper Admin/Oper
------ ------ ------------ ---- ----- ---------- ---------- ------------
node1
       a0a    data         down 1500  true/-     auto/-      auto/-
       e0c    data         up   1500  true/true  full/full   auto/1000
       e0d    data         up   1500  true/true  full/full   auto/1000
       e1b    data         up   1500  true/true  full/full   auto/1000
       e1c    data         down 1500  true/true  full/half   auto/10
       e1d    data         down 1500  true/true  full/half   auto/10
```

```
cluster1::> network port show -role data -node node2
                                      Auto-Negot  Duplex     Speed (Mbps)
Node   Port   Role         Link  MTU  Admin/Oper  Admin/Oper Admin/Oper
------ ------ ------------ ---- ----- ----------- ---------- ------------
node2
       e0c    data         up   1500  true/true   full/full   auto/1000
       e0d    data         up   1500  true/true   full/full   auto/1000
       e1b    data         up   1500  true/true   full/full   auto/1000
       e1c    data         down 1500  true/true   full/half   auto/10
       e1d    data         down 1500  true/true   full/half   auto/10

cluster1::> network interface create -vserver vs1 -lif lif1 -role data -home-node
node1 -home-port e1b -address 10.1.1.128 -netmask-length 24

Info: Your interface was created successfully; the routing group d10.1.1.0/24 was
created

cluster1::> network interface create -vserver vs1 -lif lif2 -role data -home-node
node2 -home-port e1b -address 10.1.1.129 -netmask-length 24

cluster1::> network interface show -vserver vs1
         Logical    Status     Network          Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node      Port    Home
-------- ---------- ---------- --------------- --------- ------- ----
vs1
         lif1       up/up      10.1.1.128/24    node1     e1b     true
         lif2       up/up      10.1.1.129/24    node2     e1b     true
```

Creating default gateways, static routes, and routing groups (cluster administrators only)

After you create data LIFs on the Storage Virtual Machine (SVM), you configure the default gateways by adding the default routes to the CIFS server's routing groups. You can also add additional static routes to the routing groups.

Before you begin

You must know the IP address of the default gateway for any default routes that you create.

About this task

Data ONTAP automatically creates an associated routing group on the SVM when you create the first data LIF in an IP subnet. A routing group is a container for static routes, including the default route. A routing group scope is bound by the SVM. Routing groups are not shared across SVMs.

You can configure SVM data LIFs that are on different subnets and that have different gateways. If you have SVM data LIFs that are on different subnets, Data ONTAP creates routing groups for each subnet. If you want the SVM to have a default routes to each gateway, you must add the default routes to the appropriate routing groups. You can also add other static routes to the configured routing groups.

Note: Under some circumstances, you might not want a default route configured for one or more of the data LIF subnets on the SVM. For example, you might want to permit file access to clients only on particular subnets or permit access only to particular servers. In this case, you must add the necessary static routes to the appropriate routing group before the SVM can provide NAS access to external NAS hosts.

For more information about the following commands, see the man pages and the *Clustered Data ONTAP Network Management Guide*.

This task can only be completed by a cluster administrator.

Steps

1. Identify the name of the routing groups on the SVM to which the data LIFs are associated:

   network routing-groups show -vserver *vserver_name*

2. Create any custom routing groups that you want configured by using the `network routing-groups create` command.

3. For each routing group on the SVM for which you want a default route configured, create a default route:

   network routing-groups route create -vserver *vserver_name* -routing-group *routing_group_name* -destination 0.0.0.0/0 -gateway *gateway_IP_address*

4. Add any custom static routes to the routing groups by using the `network routing-groups route create` command.

5. Verify that the route configuration is correct by using the `network routing-groups route show` command.

Example

The following commands add a default route to the routing group that was automatically created during data LIF creation for SVM vs1:

```
cluster1::> network routing-groups show -vserver vs1
          Routing
Vserver   Group     Subnet        Role          Metric
--------- --------- ------------- ------------- -------
vs1
          d10.1.1.0/24
                    10.1.1.0/24   data              20

cluster1::> network routing-groups route create -vserver vs1 -routing-group
d10.1.1.0/24 -destination 0.0.0.0/0 -gateway  10.1.1.1

cluster1::> network routing-groups route show -vserver vs1
          Routing
Vserver   Group         Destination   Gateway     Metric
--------- ------------- ------------- ----------- ------
vs1       d10.1.1.0/24  0.0.0.0/0     10.1.1.1    20
```

Managing CIFS servers

After you set up a CIFS server, you can perform management tasks. For example, you can configure CIFS server options, manage CIFS server security settings, configure SMB and SMB signing,

configure LDAP over SSL/TLS, manage oplocks, configure IPv6 SMB access, apply GPOs to CIFS servers, manage domain controller connections, and manage the CIFS server service.

Related concepts

Related tasks

Using options to customize CIFS servers

You can use options to customize CIFS servers, for example, to configure the default UNIX user. At the advanced privilege level, you can also enable or disable local Windows users and groups and local Windows user authentication, automatic node referrals and remote copy offload, export policies for SMB access, and other options.

Available CIFS server options

It is useful to know what CIFS server options are available when considering how to customize the CIFS server. Some options are for general use on the CIFS server. A number of the options are used to enable and configure specific CIFS functionality.

The following list specifies the CIFS server options available at admin-privilege level:

* Default UNIX user
  Starting with Data ONTAP 8.2 and later releases, this option has a default value. The value is set to `pcuser`.

> **Note:** Starting with Data ONTAP 8.2 and later releases, Data ONTAP automatically creates the default user named "pcuser" (with a UID of 65534), the group named "pcuser" (with a GID of 65534), and adds the default user to the "pcuser" group. When you create a CIFS server, Data ONTAP automatically configures "pcuser" as the default UNIX user.

- Read grants execute for mode bits
  You can use this option 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.
- WINS server addresses
  There is no default value.
- Default UNIX group
  There is no default value. This option is supported only on SVMs with Infinite Volume.

The following list specifies the CIFS server options available at advanced-privilege level:

- Enabling or disabling SMB 2.x
  SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, Data ONTAP also automatically disables SMB 3.0.
  This option is supported only on SVMs with FlexVol volumes. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.
- 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 to support SMB 3.0.
  This option is supported only on SVMs with FlexVol volumes. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.
- Enabling or disabling ODX copy offload
  This option is enabled by default. ODX copy offload is used automatically by Windows clients that support it.
- Enabling or disabling automatic node referrals
  This option is disabled by default. With automatic node referrals, the CIFS server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share. This option must be disabled on Hyper-V over SMB configurations.
- Enabling or disabling export policies for SMB
  The default is to disable export policies for SMB.
- Enabling or disabling using junction points as reparse points
  This option is only valid for SMB 2.x or SMB 3.0 connections.
  This option is supported only on SVMs with FlexVol volumes. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.
- 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

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

  This option is supported only on SVMs with FlexVol volumes, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.
- Configuring the shadow copy directory depth

  This option is used with the shadow copy functionality and defines the maximum depth of directories on which to create shadow copies.

  This option is supported only on SVMs with FlexVol volumes, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs with FlexVol volumes, and disabled by default on SVMs with Infinite Volume.
- Enabling or disabling multidomain search capabilities for name mapping

  This option is used to enable or disable the multidomain name mapping search capability. 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, Data ONTAP searches for the specified user in all domains with bidirectional trusts to the home domain. The home domain is the domain that contains the CIFS server's computer account.

  As an alternative to searching all bidirectionally trusted domains, a list of preferred trusted domains can be configured. 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

  This option is used to configure the file system sector size in bytes that Data 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.

For more information about configuring CIFS server options, see the man pages.

Related concepts

Related tasks

Configuring CIFS server options

You can configure CIFS server options at any time after you have created a CIFS server on a Storage Virtual Machine (SVM)

Step

1. Perform the desired action:

If you want to configure CIFS server options...	Enter the command...
At admin-privilege level	`vserver cifs options modify -vserver vserver_name options`
At advanced-privilege level	a. `set -privilege advanced` b. `vserver cifs options modify -vserver vserver_name options` c. `set -privilege admin`

`options` is a list of one or more CIFS server options.

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

Managing CIFS server security settings

You can manage the CIFS server security settings by modifying the Kerberos security settings, enabling or disabling required SMB signing for incoming SMB traffic, enabling or disabling LDAP over SSL/TLS, requiring or not requiring password complexity for local users, and displaying information about current CIFS server security settings.

Modifying the CIFS server Kerberos security settings

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

About this task

Modifying CIFS server Kerberos settings by using the vserver cifs security modify command modifies the settings only on the single Storage Virtual Machine (SVM) that you specify with the -vserver parameter. You can centrally manage Kerberos security settings for all SVMs on

the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

Steps

1. Perform one or more of the following actions:

If you want to...	Enter...
Specify the maximum allowed Kerberos clock skew time in minutes	**vserver cifs security modify -vserver** *vserver_name* **-kerberos-clock-skew** *integer_in_minutes* **Note:** The default setting is five minutes.
Specify the Kerberos ticket lifetime in hours	**vserver cifs security modify -vserver** *vserver_name* **-kerberos-ticket-age** *integer_in_hours* **Note:** The default setting is ten hours.
Specify the maximum number of ticket renewal days	**vserver cifs security modify -vserver** *vserver_name* **-kerberos-renew-age** *integer_in_days* **Note:** The default setting is seven days.

2. Verify the Kerberos security settings:

   vserver cifs security show -vserver *vserver_name*

   Example

   The following example makes the following changes to Kerberos security. The Kerberos clock skew is set to three minutes and the Kerberos ticket lifetime is set to eight 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
               Is Signing Required:                   false
               Is Password Complexity Required:       true
               Use start-tls For AD LDAP Connections: false
   ```

Related concepts

Kerberos authentication on page 22

Related tasks

Enabling or disabling 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, Data 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.

Note: SMB signing is not disabled by default under the following circumstance:

1. Required SMB signing is enabled and the cluster is reverted to a version of Data ONTAP that does not support SMB signing.

2. The cluster is subsequently upgraded to a version of Data ONTAP that supports SMB signing. Under these circumstances, the SMB signing configuration originally configured on a supported version of Data ONTAP is retained through reversion and subsequent upgrade.

Steps

1. Perform one of the following actions:

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

2. Verify that required SMB signing is enabled or disabled by determining if the value in the Is Signing Required field in the output from 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 Storage Virtual Machine (SVM, formerly known as Vserver) 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
```

Related concepts

Using SMB signing to enhance network security on page 74
Performance impact of SMB signing on page 75
Recommendations for configuring SMB signing on page 76

Related tasks

Displaying information about CIFS server security settings on page 67
Monitoring SMB signed session statistics on page 78

Requiring password complexity for local users

To provide enhanced security for local users on your Storage Virtual Machines (SVMs), you can enforce password complexity requirement for local SMB users. Required password complexity is enabled by default; you can enable or disable required password complexity at any time.

Before you begin

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

Steps

1. Perform one of the following actions:

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

2. Verify the security setting for required password complexity:

vserver cifs security show -vserver *vserver_name*

Example

The following example enables required password complexity for local SMB users for Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

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

cluster1::> vserver cifs security show -vserver vs1

          Vserver: vs1

          Kerberos Clock Skew:                 5 minutes
          Kerberos Ticket Age:                 10 hours
          Kerberos Renewal Age:                7 days
          Is Signing Required:                 false
          Is Password Complexity Required:     true
          Use start-tls For AD LDAP Connections: false
```

Related concepts

Using local users and groups for authentication and authorization on page 156
Requirements for local user passwords on page 162

Related tasks

Displaying information about CIFS server security settings on page 67
Changing local user account passwords on page 170

Enabling LDAP over SSL/TLS on the CIFS server

Before your CIFS server can use secure LDAP communication when binding to Active Directory LDAP, you must modify the CIFS server security settings to enable LDAP over SSL/TLS for Active Directory LDAP communication.

Steps

1. Configure the CIFS server security setting that allows secure LDAP communication with Active Directory LDAP:

   vserver cifs security modify -vserver *vserver_name* -use-start-tls-for-ad-ldap true

2. Verify that the LDAP over SSL/TLS security setting is set to `true`:

   vserver cifs security show -vserver *vserver_name*

After you finish

Install the self-signed root CA certificate that you exported from the Certificate Service certificate store on the Storage Virtual Machine (SVM).

Related concepts

LDAP over SSL/TLS concepts on page 80

Related tasks

Configuring LDAP over SSL/TLS on page 82

Displaying information about CIFS server security settings

You can display information about CIFS 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 configured either by using the Data ONTAP CLI or by using Active Directory group policy objects (GPOs).

Step

1. Perform one of the following actions:

If you want display information about...	Enter the command...
All security settings on a specified SVM	**vserver cifs security show -vserver vserver_name**
A specific security setting or settings on the SVM	**vserver cifs security show -vserver vserver_name -fields [fieldname,...]**

Examples

The following example display 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
          Is Signing Required:                   false
          Is Password Complexity Required:       true
          Use start-tls For AD LDAP Connections: false
```

The following example displays 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 concepts

Configuring SMB on your CIFS server

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. You can configure and manage SMB on the CIFS server associated with your Storage Virtual Machine (SVM).

Supported SMB versions

Data ONTAP supports several versions of the Server Message Block (SMB) protocol on your CIFS server on the data SVM. Data ONTAP support for SMB for SVMs with FlexVol volumes and SVMs with Infinite Volumes differ. You need to be aware of which versions are supported for each type of Storage Virtual Machine (SVM).

Data ONTAP supports the following SMB versions for SVMs with FlexVol volumes and SVMs with Infinite Volumes:

SMB version	Supported on SVMs with FlexVol volumes?	Supported on SVMs with Infinite Volumes?
SMB 1.0	Yes	Yes
SMB 2.0	Yes	No
SMB 2.1	Yes	No
SMB 3.0	Yes	No

Supported SMB 1.0 functionality

The CIFS (SMB 1.0) protocol was introduced by Microsoft for Windows clients. Data ONTAP supports the SMB 1.0 protocol on all versions of clustered Data ONTAP and on Storage Virtual Machines (SVMs) with FlexVol volumes and SVMs with Infinite Volumes.

Over the years, Microsoft has extended the original SMB 1.0 protocol with enhancements to security, file, and disk-management features. Legacy Windows clients (pre-Windows XP) or non-Windows clients that support only SMB 1.0 can access data on the SVM using SMB 1.0.

Supported SMB 2.0 functionality

Clustered Data ONTAP 8.1 and later supports the SMB 2.0 protocol on Storage Virtual Machines (SVMs) with FlexVol volumes. SMB 2.0 is a major redesign of the SMB protocol that provides

performance enhancements and added resiliency against network interruptions through the use of durable handles.

SMB 2.0 is enabled automatically when you create a CIFS server.

Data ONTAP supports the following SMB 2.0 functionality:

- Durable handles

  Enables clients to transparently reconnect to disconnected SMB sessions after short network outages. For example, LIF failovers, LIF moves, and LIF migrations are transparent and nondisruptive for SMB 2.0 connections.

- Compounded operations

  Provides a method for combining multiple SMB messages into a single network transmission request for submission to the underlying transport.

- Asynchronous operations

  Certain SMB commands from the clients can take a longer time for the server to process. For these commands, the CIFS server can send responses asynchronously.

- Increased read and write buffer sizes

  Allows for better throughput across faster networks, even those with high latency.

- Increased scalability

  SMB 2.0 has increased limits for number of SMB sessions, open share connections, and open file connections.

- Increased SMB signing security

  Support for stronger data integrity protection through the use of the HMAC-SHA256 hash algorithm.

Data ONTAP does not support the following SMB 2.0 functionality:

- Symbolic links
- Credit system for flow control

If SMB 2.0 is disabled on the CIFS server, communication between the SMB 2.0 client and the CIFS server falls back to the SMB 1.0 protocol (assuming that the SMB 2.0 client includes the SMB 1.0 dialect in its negotiate request).

For more information, see Technical Report TR-3740 or the SMB 2.0 protocol specification.

Related information

Technical Report: SMB 2—Next-Generation CIFS Protocol in Data ONTAP: media.netapp.com/ documents/tr-3740.pdf

Supported SMB 2.1 functionality

The SMB 2.1 protocol provides several enhancements to the SMB 2.0 protocol. Data ONTAP 8.1 and later supports SMB 2.1 on Storage Virtual Machines (SVMs) with FlexVol volumes. Support for SMB 2.1 is enabled automatically when you enable the SMB 2.0 protocol on the CIFS server.

SMB 2.0 and SMB 2.1 are enabled automatically when you create a CIFS server. SMB 2.0 and SMB 2.1 are always enabled or disabled together. You cannot enable or disable SMB 2.0 and SMB 2.1 separately.

Data ONTAP supports the following SMB 2.1 functionality:

- Lease oplocks
  Data ONTAP uses SMB 2.1 lease oplocks, which is a new client oplock leasing model that provides advantages over traditional oplocks. Lease oplocks offer more flexibility and levels in controlling the client caching. This results in significant performance improvement in high-latency and erratic networks.
- BranchCache version 1
  BranchCache is a feature that delivers WAN bandwidth optimization and improved file access performance using client-side caching at remote offices. SMB 2.1 has the functional extensions needed to manage content hashes, which are used by BranchCache-enabled CIFS servers to provide clients with information about cached content.

Data ONTAP does not support the following SMB 2.1 functionality:

- Large MTU
- Resilient handles

For more information, see Technical Report TR-3740 or the SMB 2.1 protocol specification.

Related information

[Technical Report: SMB 2—Next-Generation CIFS Protocol in Data ONTAP: media.netapp.com/documents/tr-3740.pdf](media.netapp.com/documents/tr-3740.pdf)

Supported SMB 3.0 functionality

Clustered Data ONTAP 8.2 and later supports the SMB 3.0 protocol on Storage Virtual Machines (SVMs) with FlexVol volumes. SMB 3.0 provides important enhancements, including enhancements that facilitate transparent failover and giveback and other nondisruptive operations.

Support for SMB 3.0 is enabled automatically when you create a CIFS server.

Data ONTAP supports the following SMB 3.0 functionality:

- Continuously available share property
  A new share property that, along with persistent handles, allows SMB clients that are connected to shares that are configured to use the continuously available share property to transparently reconnect to a CIFS server following disruptive events such as failover and giveback operations.
- Persistent handles

Enables clients to transparently reconnect to disconnected SMB sessions after certain disruptive events. A persistent handle is preserved after a disconnection. Persistent handles block other file opens while waiting for a reconnection. Along with the continuously available share property, persistent handles provide support for certain nondisruptive operations.

- Remote VSS for SMB shares

  Remote VSS (Volume Shadow Copy Service) for SMB provides the functionality that allows VSS-enabled backup services to create application-consistent volume shadow copies of VSS-aware applications that access data stored over SMB 3.0 shares.

- Witness

  Enables a CIFS server providing SMB shares to Hyper-V and SQL application servers to promptly notify the application servers about network failures.

- ODX copy offload

  ODX enables data transfers within or between ODX-enabled storage servers without transferring the data through the Windows client.

- BranchCache version 2

  Provides enhanced functionality, including smaller, variable-sized content segments, which increases the reuse of existing cached content.

Data ONTAP does not support the following SMB 3.0 functionality:

- SMB Multichannel
- SMB Direct
- SMB Directory Leasing
- SMB Encryption

For more information, see the SMB 3.0 protocol specification.

Related concepts

Related tasks

Enabling or disabling SMB 2.x

SMB 2.x is enabled by default for CIFS servers on Storage Virtual Machine (SVM) with FlexVol volumes. This allows clients to connect to the CIFS server using SMB 2.x. You can enable or disable SMB 2.x at any time by using a CIFS server option.

About this task

The `-smb2-enabled` option enables SMB 2.0 and SMB 2.1.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want SMB 2.x to be...	Enter the command...
Enabled	**`vserver cifs options modify -vserver vserver_name -smb2-enabled true`**
Disabled	**`vserver cifs options modify -vserver vserver_name -smb2-enabled false`**

3. Return to the admin privilege level:

   `set -privilege admin`

   #### Example

   The following example enables SMB 2.x on SVM vs1:

   ```
   cluster1::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by technical support personnel.
   Do you wish to continue? (y or n): y

   cluster1::*> vserver cifs options modify -vserver vs1 -smb2-enabled true

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

Related concepts

Enabling or disabling SMB 3.0

SMB 3.0 is enabled by default for CIFS servers on Storage Virtual Machines (SVMs) with FlexVol volumes. This allows clients that support SMB 3.0 to connect to the CIFS server using SMB 3.0. You can enable or disable SMB 3.0 at any time by using a CIFS server option.

About this task

This option must be enabled if you want to configure continuously available shares.

ODX copy offload requires that SMB 3.0 be enabled. If ODX copy offload is enabled and you disable SMB 3.0, Data ONTAP automatically disables ODX copy offload. Similarly, if you enable ODX copy offload, Data ONTAP will automatically enable SMB 3.0 if it is not already enabled.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want SMB 3.0 to be...	Enter the command...
Enabled	`vserver cifs options modify -vserver vserver_name -smb3-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -smb3-enabled false`

3. Return to the admin privilege level:

```
set -privilege admin
```

> **Example**
>
> The following commands enable SMB 3.0 on SVM vs1:
>
> ```
> cluster1::> set -privilege advanced
> Warning: These advanced commands are potentially dangerous; use them
> only when directed to do so by technical support personnel.
> Do you wish to continue? (y or n): y
>
> cluster1::*> vserver cifs options modify -vserver vs1 -smb3-enabled true
>
> cluster1::*> set -privilege admin
> ```

Related concepts

Supported SMB 3.0 functionality on page 70

Using SMB signing to enhance network security

SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised; it does this by preventing replay attacks. By default, Data ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the CIFS 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 communicates normally with the CIFS server without SMB signing, regardless of 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.

  Note: 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	Data ONTAP—signing not required	Data 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

Client	Data ONTAP—signing not required	Data ONTAP—signing required
Signing enabled and required	Signed	Signed

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

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

Client	Data ONTAP—signing not required	Data 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

Performance impact of SMB signing

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

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

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

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

Recommendations for configuring SMB signing

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

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

If...	Recommendation...
You want to increase the security of the communication between the client and the server	Make SMB signing required at the client by enabling the `Require Option (Sign always)` security setting on the client.
You want all SMB traffic to a certain Storage Virtual Machine (SVM) signed	Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.

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

Related tasks

Considerations when multiple data LIFS are configured

If you enable or disable required SMB signing on the CIFS sever, there are certain considerations you should keep in mind when you have multiple data LIFS configured for a Storage Virtual Machine (SVM).

When you configure a CIFS 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 CIFS server host name, but each with a unique IP address. For example, a CIFS 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 CIFS 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.

Enabling or disabling 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, Data 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.

Note: SMB signing is not disabled by default under the following circumstance:

1. Required SMB signing is enabled and the cluster is reverted to a version of Data ONTAP that does not support SMB signing.

2. The cluster is subsequently upgraded to a version of Data ONTAP that supports SMB signing. Under these circumstances, the SMB signing configuration originally configured on a supported version of Data ONTAP is retained through reversion and subsequent upgrade.

Steps

1. Perform one of the following actions:

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

2. Verify that required SMB signing is enabled or disabled by determining if the value in the Is Signing Required field in the output from 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 Storage Virtual Machine (SVM, formerly known as Vserver) 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
```

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

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

> **Note:** 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.

For more information about using the `statistics` command, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. 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.

2. Optional: Use the `statistics stop` command to stop collecting data for the sample.

3. View SMB signing statistics:

If you want to view information for...	Enter this command...
Signed sessions	**show -sample-id** *sample_ID* **-counter signed_sessions|node_name [-node** *node_name***]**
Signed sessions and established sessions	**show -sample-id** *sample_ID* **-counter signed_sessions|established_sessions|node_name [-node** *node_name***]**

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

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 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
```

Related tasks

Using LDAP over SSL/TLS to secure communication

You can use LDAP over SSL/TLS to secure communication between the Storage Virtual Machine
(SVM) LDAP client and the LDAP server. This allows LDAP to encrypt all traffic to and from the
LDAP server.

LDAP over SSL/TLS concepts

You must understand certain terms and concepts about how Data ONTAP uses SSL/TLS to secure
LDAP communication. Data ONTAP can use LDAP over SSL/TLS for setting up authenticated
sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

Terminology

There are certain terms that you should understand about how Data ONTAP uses LDAP over SSL to
secure LDAP communication.

LDAP   (Lightweight Directory Access Protocol) A set of protocols for accessing and
            managing information directories. LDAP is used as information directory for storing
            objects such as users, groups, and netgroups. LDAP also provides directory services
            that manage these objects and fulfill LDAP requests from LDAP clients.

SSL (Secure Sockets Layer) A secure protocol developed for sending information securely over the Internet. SSL is used to provide either server or mutual (server and client) authentication. SSL provides encryption only. If a method to ensure data integrity is needed, it must be provided by the application using SSL.

TLS (Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL.

LDAP over SSL/TLS (Also known as *LDAPS*) A protocol that uses SSL or TLS to secure communication between LDAP clients and LDAP servers. The terms *SSL* and *TLS* are often used interchangeably unless referring to a specific version of the protocol.

Start TLS (Also known as *start_tls*, *STARTTLS*, and *StartTLS*) A mechanism to provide secure communication by using the TLS/SSL protocols.

How Data ONTAP uses LDAP over SSL/TLS

By default, LDAP communications between client and server applications are not encrypted. This means that it is possible to use a network monitoring device or software and view the communications between LDAP client and server computers. This is especially problematic when an LDAP simple bind is used because the credentials (user name and password) used to bind the LDAP client to the LDAP server are passed over the network unencrypted.

The SSL and TLS protocols run above TCP/IP and below higher-level protocols, such as LDAP. They use TCP/IP on behalf of the higher-level protocols, and in the process, permit an SSL-enabled server to authenticate itself to an SSL-enabled client and permit both machines to establish an encrypted connection. These capabilities address fundamental security concerns about communication over the Internet and other TCP/IP networks. Data ONTAP uses the START TLS method to set up the secured connection.

Data ONTAP supports SSL server authentication, which enables the Storage Virtual Machine (SVM) LDAP client to confirm the LDAP server's identity during the bind operation. SSL/TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.

This version of Data ONTAP supports the following:

- LDAP over SSL/TLS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAP over SSL/TLS for LDAP traffic for name mapping
  Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping.
- Self-signed root CA certificates
  When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

Data ONTAP does not support signing (integrity protection) and sealing (encryption) of the data.

The default is not to enable LDAP over SSL/TLS.

Configuring LDAP over SSL/TLS

To configure LDAP over SSL/TLS, you must enable LDAP over SSL/TLS on the Storage Virtual Machine (SVM), export a copy of the self-signed root CA certificate, and, using the exported file, install the self-signed root CA certificate on the SVM.

Steps

1. Enabling LDAP over SSL/TLS on the CIFS server on page 82
   Before your CIFS server can use secure LDAP communication when binding to Active Directory LDAP, you must modify the CIFS server security settings to enable LDAP over SSL/TLS for Active Directory LDAP communication.

2. Exporting a copy of the self-signed root CA certificate on page 83
   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 Data ONTAP to install the certificate on the Storage Virtual Machine (SVM).

3. Installing the self-signed root CA certificate on the SVM on page 83
   Before you can use secure LDAP authentication when binding to LDAP servers, you must install the self-signed root CA certificate on the Storage Virtual Machine (SVM).

Enabling LDAP over SSL/TLS on the CIFS server

Before your CIFS server can use secure LDAP communication when binding to Active Directory LDAP, you must modify the CIFS server security settings to enable LDAP over SSL/TLS for Active Directory LDAP communication.

Steps

1. Configure the CIFS server security setting that allows secure LDAP communication with Active Directory LDAP:

   vserver cifs security modify -vserver *vserver_name* -use-start-tls-for-ad-ldap true

2. Verify that the LDAP over SSL/TLS security setting is set to `true`:

   vserver cifs security show -vserver *vserver_name*

After you finish

Install the self-signed root CA certificate that you exported from the Certificate Service certificate store on the Storage Virtual Machine (SVM).

Exporting 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 Data 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: technet.microsoft.com*.

Step

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

   For more information, consult the *Microsoft TechNet Library: technet.microsoft.com*.

After you finish

Install the certificate on the SVM.

Installing the self-signed root CA certificate on the SVM

Before you can use secure LDAP authentication when binding to LDAP servers, you must install the self-signed root CA certificate on the Storage Virtual Machine (SVM).

Steps

1. Install the self-signed root CA certificate:

   a) Enter the following command to 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 paste the certificate on the console.

   c) Verify that the certificate is displayed after the console prompt.

   d) To complete the installation, press **Enter**.

2. Verify that the certificate is installed:

   `security certificate show -vserver vserver_name`

Improving client performance with traditional and lease oplocks

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

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

Lease oplocks are not supported on Storage Virtual Machines (SVMs) with Infinite Volumes.

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.

Enabling or disabling 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) with FlexVol volumes by default. 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.

Step

1. Perform the applicable action:

If you want to...	Then...
Enable oplocks on a share during share creation	Enter the following command: **vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path_to_share* -share-properties [oplocks,...]** **Note:** If you want the share to have only the default share properties, which are oplocks, browsable, and changenotify enabled, you do not have to specify the -share-properties parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the -share-properties parameter with the list of share properties to use for that share.
Disable oplocks on a share during share creation	Enter the following command: **vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path_to_share* -share-properties [*other_share_property*,...]** **Note:** When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the oplocks property.

Related tasks

Enabling or disabling oplocks on existing SMB shares

Oplocks are enabled on SMB shares on Storage Virtual Machines (SVMs) with FlexVol volumes by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenable oplocks.

About this task

If oplocks are enabled on the volume containing a share, but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over

enabling oplocks on the volume. Disabling oplocks on the share, disables both opportunistic and lease oplocks. You can enable or disable oplocks on existing shares at any time.

Step

1. Perform the applicable action:

If you want to...	Then...
Enable oplocks on a share by modifying an existing share	Enter the following command: **vserver share properties add -vserver** *vserver_name* **-share-name** *share_name* **-share-properties oplocks** > **Note:** You can specify additional share properties to add by using a comma-delimited list. Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.
Disable oplocks on a share by modifying an existing share	Enter the following command: **vserver share properties remove -vserver** *vserver_name* **-share-name** *share_name* **-share-properties oplocks** > **Note:** You can specify additional share properties to remove by using a comma-delimited list. Share properties that you remove are deleted from the existing list of share properties; however, previously configured share properties that you do not remove remain in effect.

Examples

The following command enables oplocks for the share named "Engineering" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

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

cluster1::> vserver cifs share properties show
Vserver          Share           Properties
---------------- --------------- ----------------
vs1              Engineering     oplocks
                                 browsable
                                 changenotify
                                 showsnapshot
```

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

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

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

```
Vserver          Share           Properties
---------------- --------------- -----------------
vs1              Engineering     browsable
                                 changenotify
                                 showsnapshot
```

Related tasks

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 with FlexVol volumes at any time.
- You cannot disable oplocks on volumes for SVMs with Infinite Volume.
- You can enable oplocks on qtrees for SVMs with FlexVol volumes.
  If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume. However, if you do specify an oplock setting on the qtree, it takes precedence over the oplock setting on the volume.

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

Related tasks

Monitoring 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

  A lock can be in one of the following states:

Lock state	Description
granted	The lock is established.
revoking	The server is currently coordinating with the client to change the state of the lock.
revoked	The lock is undergoing revocation to be downgraded or released.
adjusted	The lock is undergoing revocation to be replaced by a lock equal to or weaker than the current lock.
subsumed	The lock is one of a set of locks that will replace a lock that is being revoked.
waiting	The lock is waiting to be granted because it conflicts with another lock.
denied	The lock has been denied.
timeout	The lock was waiting and has now timed out.
gone	The lock is about to be released.
unused	The lock is allocated but has not been processed into any state.

* Oplock level

  A lock can have the following oplock levels:

Oplock level	Description
`batch`	Permits the client to cache all operations on the file.
`exclusive`	Permits the client to cache reads and writes on the file.
`read-batch`	Permits the client to cache reads and opens on the file.
`level2`	Permits the client to cache reads on the file.
`null`	Disallows the client from caching any operations on the file.

- Connection state and SMB expiration time
- Open Group ID if a lease oplock is granted

Step

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`:

Note: 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:
78a90c59d45ae2l1998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Related tasks

Related references

Using IPv6 for SMB access and CIFS services

Starting with Data ONTAP 8.2, SMB clients can access files on your Storage Virtual Machine (SVM) over an IPv6 network and can use IPv6 for CIFS service communications.

After you enable IPv6 on the cluster and properly configure data LIFs, IPv6 works immediately. You do not have configure any settings on the SVM and you do not have to enable any CIFS server options.

Requirements for using IPv6

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

Data ONTAP version and license requirements

- Data ONTAP 8.2 and later supports IPv6.
  Commands used to configure CIFS servers, SMB access, and CIFS services and features that support IPv6 can use either IPv4 or IPv6 addresses whenever an IP address is a supported command parameter. Similarly, commands supported with IPv6 that display information about IP addresses display both IPv4 and IPv6 addresses.
- No special license is required for IPv6; however, CIFS must be licensed, and a CIFS server must exist on the Storage Virtual Machine (SVM) to user IPv6 with SMB access and CIFS services.

SMB protocol version requirements

- For SVMs with FlexVol volumes, Data ONTAP supports IPv6 on all versions of the SMB protocol.
- For SVMs with Infinite Volume, Data ONTAP supports IPv6 on SMB 1.0.
  This is because SMB 2.x and SMB 3.0 are not supported on SVMs with Infinite Volume.

  Note: 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 Data ONTAP supports IPv6 for SMB access and network communication for CIFS services.

Windows client and server support

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

- Windows XP and Windows 2003 support IPv6 for SMB file sharing.
  These versions provide limited support for IPv6.
- Windows Vista, 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 Data ONTAP can connect to SMB shares by using IPv6 addresses.

For the latest information about which Windows clients Data ONTAP supports, see the Interoperability Matrix at *support.netapp.com/matrix*.

  Note: NT domains are not supported for IPv6.

Additional CIFS services support

In addition to IPv6 support for SMB file shares and Active Directory services, Data 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.

> **Note:** 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.

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

Related tasks

Enabling 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 *Clustered Data ONTAP Network Management Guide*.

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

Related tasks

How to 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, Data 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 *Clustered Data ONTAP Network Management Guide*.

Monitoring and displaying information about IPv6 SMB sessions

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

Step

1. Perform the desired action:

If you want to determine whether...	Enter the command...
SMB sessions to a Storage Virtual Machine (SVM) are connected using IPv6	`vserver cifs session show -vserver vserver_name -instance`
IPv6 is used for SMB sessions through a specified LIF address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` `LIF_IP_address` is the data LIF's IPv6 address.

Applying Group Policy Objects to CIFS servers

Your CIFS 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 CIFS server, Data ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your CIFS 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

Supported GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled Storage Virtual Machines (SVMs), the SVM can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs with FlexVol volumes:

- Registry settings:

  - Group Policy refresh interval for CIFS-enabled SVM
  - Group Policy refresh random offset
  - Hash publication for BranchCache

The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The three supported operating modes are per-share, all shares, and disabled.

- Hash version support for BranchCache

    The three supported settings are support for BranchCache version 1, support for BranchCache version 2, and support for both versions 1 and 2.

- Kerberos security settings:

    - Maximum clock skew
    - Maximum ticket age
    - Maximum ticket renew age

The following GPOs are currently supported on SVMs with Infinite Volume:

- Registry settings:

    - Group Policy refresh interval for CIFS-enabled SVM
    - Group Policy refresh random offset

- Kerberos security settings:

    - Maximum clock skew
    - Maximum ticket age
    - Maximum ticket renew age

Related concepts

Kerberos authentication on page 22
Using BranchCache to cache SMB share content at a branch office on page 298

Related tasks

Enabling or disabling GPO support on a CIFS server on page 95
Modifying the CIFS server Kerberos security settings on page 62

Requirements for using GPOs with your CIFS server

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

- CIFS must be licensed on the cluster.
- A CIFS server must be configured and joined to a Windows Active Directory domain.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the CIFS server computer object.
- GPO support must be enabled on the CIFS server.

Enabling or disabling GPO support on a CIFS server

You can enable or disable Group Policy Object (GPO) support on the CIFS server. If you enable GPO support on the CIFS server, applicable GPOs that are defined on the group policy (in this case,

the policy applied to the OU containing the CIFS server computer object) are applied to the CIFS server.

Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable GPOs	**vserver cifs group-policy modify -vserver _vserver_name_ -status enabled**
Disable GPOs	**vserver cifs group-policy modify -vserver _vserver_name_ -status disabled**

2. Verify that GPO support is in the desired state by using the following command:

   vserver cifs group-policy show -vserver _vserver_name_

Example

The following example enables GPO support on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

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

cluster1::> vserver cifs group-policy show -vserver vs1
Virtual Server    GPO Status
--------------    ----------
vs1               enabled
```

Related concepts

Supported GPOs on page 94
Requirements for using GPOs with your CIFS server on page 95

Related tasks

Displaying information about GPO configurations on page 98

How GPOs are updated on the CIFS server

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

- All GPOs are verified and updated as needed every 90 minutes.
  By default, Data 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, Data 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.
Data ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.

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

• All GPOs can be updated manually with a Data ONTAP command.
This command simulates the Windows gpupdate.exe /force command.

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 force a GPO update.

Steps

1. Update GPO settings manually by entering the following command:
   vserver cifs group-policy update -vserver *vserver_name*

2. Verify that the update succeeded by entering the following command:
   vserver cifs group-policy show-applied -vserver *vserver_name*

Example

The following example updates the GPOs on an SVM with FlexVol volumes named vs1:

```
cluster1::> vserver cifs group-policy update -vserver vs1

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

Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7

    GPO Name: Resultant Set of Policy
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
```

```
    Security Settings:
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
```

Displaying 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.

Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display information about all Group Policy configurations defined in Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Display information about all Group Policy configurations applied to a CIFS server	`vserver cifs group-policy show-applied -vserver vserver_name`

Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM with FlexVol volumes named vs1 belongs and the GPO configurations applied to SVM vs1:

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

Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache : all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
```

```
      GPO Name: Resultant Set of Policy
         Status: disabled
   Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
   Security Settings:
      Kerberos:
         Max Clock Skew: 5
         Max Ticket Age: 10
         Max Renew Age:  7

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

Vserver: vs1
-----------------------------
   GPO Name: Default Domain Policy
      Level: Domain
      Status: enabled
   Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
   Security Settings:
      Kerberos:
         Max Clock Skew: 5
         Max Ticket Age: 10
         Max Renew Age:  7

   GPO Name: Resultant Set of Policy
   Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
   Security Settings:
      Kerberos:
         Max Clock Skew: 5
         Max Ticket Age: 10
         Max Renew Age:  7
```

Related tasks

Managing domain controller connections

You can manage domain controller connections by displaying information about currently discovered LDAP and domain controller servers, resetting and rediscovering LDAP and domain controller servers, managing the preferred domain controller list, and displaying information about currently configured preferred domain controllers.

Displaying 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 tasks

Resetting and rediscovering 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 tasks

Adding preferred domain controllers

Data 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 CIFS 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 references

Commands for managing preferred domain controllers on page 102

Commands for managing preferred domain controllers

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

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

See the man page for each command for more information.

Related tasks

Adding preferred domain controllers on page 101

Managing miscellaneous CIFS server tasks

You can terminate or restart SMB access to CIFS servers, change or reset the domain account password, move the CIFS server to a different OU, change the CIFS server's domain, display information about NetBIOS over TCP connections, modify or display information about CIFS servers, or delete CIFS servers.

You can also configure the default UNIX user.

Configuring 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 user.

Step

1. Configure the default UNIX user:

   vserver cifs options modify -default-unix-user *user_name*

Related concepts

Creating name mappings on page 115

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23

Modifying protocols for SVMs

Before you can configure and use NFS or SMB on Storage Virtual Machines (SVMs), you must enable the protocol. This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the vserver modify command.

Steps

1. Check which protocols are currently enabled for the SVM by entering the following command:

   vserver show -vserver *vserver_name* -fields allowed-protocols

2. Modify the list of enabled protocols for the SVM by entering the following command:

   vserver modify vserver *vserver_name* -allowed-protocols *protocol_name[,protocol_name,...]*

   You must enter the complete list of protocols you want to be enabled on the SVM, including the protocols that are already enabled. Any protocol not specified with the command is automatically disabled and moved to the disallowed protocol list.

   You can also use the SVM setup wizard to modify protocols for the SVM by using the vserver setup command.

   See the man page for each command for more information.

3. Confirm that the allowed protocol list was updated correctly by entering the following command:

   vserver show -vserver *vserver_name* -fields allowed-protocols

   ### Examples

   The following command displays which protocols are currently enabled on the SVM named vs1.

```
vs1::> vserver show -vserver vs1 -fields allowed-protocols
vserver allowed-protocols
------- -----------------
vs1     nfs
```

The following command allows access over SMB by adding `cifs` to the list of enabled protocols on the SVM named vs1.

```
vs1::> vserver modify -vserver vs1 -allowed-protocols nfs,cifs
```

Stopping or starting the CIFS server

You can stop the CIFS server on an 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).

About this task

Note: If you stop the CIFS server, established SMB sessions are terminated and their open files are closed. Workstations with cached data will not be able to save those changes, which could result in data loss.

Steps

1. Perform one of the following actions:

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

   `-foreground` specifies whether the command should execute in the foreground or background. If you do not enter this parameter, it is set to `true`, and the command is executed in the foreground.

2. Verify that the CIFS server administrative status is correct by using the `vserver cifs show` command.

Example

The following commands start the CIFS server on SVM vs1:

```
cluster1::> vserver start -vserver vs1
```

```
cluster1::> vserver cifs show -vserver vs1

                                      Vserver: vs1
                    CIFS Server NetBIOS Name: VS1
                NetBIOS Domain/Workgroup Name: DOMAIN
                   Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                          Authentication Style: domain
              CIFS Server Administrative Status: up
```

Related tasks

[Displaying information about discovered servers](#) on page 100
[Resetting and rediscovering servers](#) on page 100

Changing or resetting the domain account password

The CIFS server on your Storage Virtual Machine (SVM) has an Active Directory domain account.
You can change the password for this account for good security practices, or reset it if the password
is lost.

Step

1. Perform one of the following actions:

If you...	Use the command...
Know the password and want to change it	`vserver cifs password-change`
Do not know the password and want to reset it	`vserver cifs password-reset`

See the man page for each command for more information.

Moving 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

Result

The SVM object is placed in the selected OU.

Related concepts

Joining an SVM to an active directory domain

You can join a Storage Virtual Machine (SVM) to an active directory domain without deleting the existing CIFS server by modifying the domain using the vserver cifs modify command.

Before you begin

- To create a CIFS server, the SVM must already have a DNS configuration.
- Before joining the SVM to a new domain, you should ensure that the same DNS configuration for the SVM can serve the target domain.

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

Step

1. Join the SVM to the CIFS server domain by entering the following command:

   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.

Example

In the following example, the CIFS server "CIFSSERVER1" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1 joins the example2.com domain.

```
cluster1::> vserver cifs modify -vserver vs1 -domain example2.com -
status-admin down

cluster1::> vserver cifs show -vserver vs1

          Server       Domain/Workgroup
Vserver   Name         Name                 Authentication Style
--------- -----------  ----------------     --------------------
vs1       CIFSSERVER1  example2             domain
```

Related concepts

Displaying 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.

   Note: 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 CIFS servers

You need to know the commands for creating, displaying, modifying, and deleting CIFS servers.

If you want to...	Use this command...
Create a CIFS server	`vserver cifs create`

If you want to...	Use this command...
Display information about a CIFS server	`vserver cifs show`
Modify a CIFS server or move a CIFS server to another domain	`vserver cifs modify`
Delete a CIFS server	`vserver cifs delete`

See the man page for each command for more information.

Related concepts

Setting up the CIFS server on page 41

What happens to local users and groups when deleting CIFS servers on page 160

Setting up file access using SMB

You must complete a number of steps to allow clients to access files using SMB on the CIFS-enabled Storage Virtual Machine (SVM).

Configuring security styles

You configure security styles on FlexVol volumes and qtrees to determine the type of permissions Data ONTAP uses to control access and what client type can modify these permissions.

For information about the security style of Infinite Volumes, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

Related concepts

Configuring security styles on SVM root volumes

You configure the Storage Virtual Machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Perform one of the following actions:

Create the SVM with the...	Specify the security style by...
`vserver setup` command	Entering the desired root volume security style when prompted by the CLI wizard.
`vserver create` command	Including the `-rootvolume-security-style` parameter with the desired security style.

The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

For more information about the `vserver setup` or `vserver create` commands, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

2. To display the configuration, including the security style of the SVM you created, enter the following command:

```
vserver show -vserver vserver_name
```

Configuring security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the Storage Virtual Machine (SVM).

Steps

1. Perform one of the following actions:

If the FlexVol volume...	Use the command...
Does not yet exist	`volume create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume modify` and include the `-security-style` parameter to specify the security style.

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see the *Clustered Data ONTAP Logical Storage Management Guide*.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

Configuring security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:

If the qtree...	Use the command...
Does not exist yet	`volume qtree create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume qtree modify` and include the `-security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`. You cannot use `unified` security style because it only applies to Infinite Volumes.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see the *Clustered Data ONTAP Logical Storage Management Guide*.

2. To display the configuration, including the security style of the qtree you created, enter the following command:
   `volume qtree show -qtree qtree_name -instance`

Creating and managing data volumes in NAS namespaces

To manage file access in a NAS environment, you must manage data volumes and junction points on your Storage Virtual Machine (SVM) with FlexVol volumes. This includes planning your namespace architecture, creating volumes with or without junction points, mounting or unmounting volumes, and displaying information about data volumes and NFS server or CIFS server namespaces.

Related concepts

Creating data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

Before you begin

The aggregate in which you want to create the volume must already exist.

Steps

1. Create the volume with a junction point:
   `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs| unix|mixed} -junction-path junction_path`

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.

   Specifying a volume security style is optional. If you do not specify a security style, Data ONTAP creates the volume with the same security style that is applied to the root volume of the Storage Virtual Machine (SVM). However, the root volume's security style might not be the

security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

The junction path is case insensitive; /ENG is the same as /eng. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is /ENG, the path of a CIFS share must start with /ENG, not /eng.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

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

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

---

Example

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

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

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

Creating data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

Before you begin

The aggregate in which you want to create the volume must already exist.

Steps

1. Create the volume without a junction point by using the following command:

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

   Specifying a volume security style is optional. If you do not specify a security style, Data ONTAP creates the volume with the same security style that is applied to the root volume of the Storage Virtual Machine (SVM). However, the root volume's security style might not be the

security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point:

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

Example

The following example creates a volume named "sales" located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3 -size
20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                        Junction                    Junction
Vserver     Volume      Active     Junction Path    Path Source
---------   ----------  --------   --------------   -----------
vs1         data        true       /data            RW_volume
vs1         home4       true       /eng/home        RW_volume
vs1         vs1_root    -          /                -
vs1         sales       -          -                -
```

Mounting or unmounting existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the Storage Virtual Machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume's namespace, are inaccessible to NAS clients. When you unmount a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

If you want to...	Enter the command...
Mount a volume	`volume mount -vserver `*`vserver_name`*` -volume `*`volume_name`*` -junction-path `*`junction_path`*
Unmount a volume	`volume unmount -vserver `*`vserver_name`*` -volume `*`volume_name`*

2. Verify that the volume is in the desired mount state:

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

Examples

The following example mounts a volume named "sales" located on SVM vs1 to the junction point /sales:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver    Volume     Active   Junction Path    Path Source
---------  ---------- -------- ---------------  -----------
vs1        data       true     /data            RW_volume
vs1        home4      true     /eng/home        RW_volume
vs1        vs1_root   -        /                -
vs1        sales      true     /sales           RW_volume
```

The following example unmounts a volume named "data" located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver    Volume     Active   Junction Path    Path Source
---------  ---------- -------- ---------------  -----------
vs1        data       -        -                -
vs1        home4      true     /eng/home        RW_volume
vs1        vs1_root   -        /                -
vs1        sales      true     /sales           RW_volume
```

Displaying volume mount and junction point information

You can display information about mounted volumes for Storage Virtual Machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

Step

1. Perform the desired action:

If you want to display...	Enter the command...
Summary information about mounted and unmounted volumes on the SVM	`volume show -vserver `*`vserver_name`*` -junction`
Detailed information about mounted and unmounted volumes on the SVM	`volume show -vserver `*`vserver_name`*` -volume `*`volume_name`*` -instance`
Specific information about mounted and unmounted volumes on the SVM	**a.** If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?` **b.** Display the desired information by using the `-fields` parameter: `volume show -vserver `*`vserver_name`*` -fields `*`fieldname,...`*

Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                         Junction                 Junction
Vserver     Volume      Active    Junction Path   Path Source
---------   ----------  --------  --------------- -----------
vs1         data        true      /data           RW_volume
vs1         home4       true      /eng/home       RW_volume
vs1         vs1_root    -         /               -
vs1         sales       true      /sales          RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields vserver,volume,aggregate,size,state,type,security-
style,junction-path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path junction-parent node
------- ------   --------- ---- ------ ---- -------------- ------------- --------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -               node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2        vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1   data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2   data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images       vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs         vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -               node3
```

Creating name mappings

Data ONTAP uses name mapping to map Windows identities to UNIX identities when accessing data contained on a Storage Virtual Machine (SVM) using SMB connections. It needs this

information to obtain user credentials and provide proper file access regardless of whether the data is of NTFS security style, UNIX security style, or unified security style.

Name mapping is usually required due to allow multiprotocol access over SMB and NFS to the same files, regardless of the effective security style applied to the requested files.

You do not have to configure Windows identity to UNIX identity name mapping if you configure the default UNIX identity to be used instead.

Related concepts

Related tasks

Name mapping conversion rules

A Data ONTAP system keeps a set of conversion rules for each Storage Virtual Machine (SVM). Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX sed program.

It is possible to allow NFS access to volumes with NTFS security style for users in a different domain from the one that the storage system belongs to, provided that the proper name mapping rule exists.

If a user matches a rule to map to a user in a different domain, the domain must be trusted. To ensure successful mapping to users in other domains for both SMB and NFS access, there must be a bidirectional trust relationship between the domains.

If a user matches a rule but the user cannot authenticate in the other domain because it is untrusted, the mapping fails.

The SVM automatically discovers all bidirectional trusted domains, which are used for multi-domain user mapping searches. Alternatively, you can configure a list of preferred trusted domains that are used for name mapping searches instead of the list of automatically discovered trusted domains.

Regular expressions are not case-sensitive when mapping from Windows to UNIX. However, they are case-sensitive for Kerberos-to-UNIX and UNIX-to-Windows mappings.

As an example, the following rule converts the Windows user named "jones" in the domain named "ENG" into the UNIX user named "jones".

Pattern	Replacement
ENG\\jones	jones

Note that the backslash is a special character in regular expressions and must be escaped with another backslash.

The caret (^), underscore (_), and ampersand (&) characters can be used as prefixes for digits in replacement patterns. These characters specify uppercase, lowercase, and initial-case transformations, respectively. For instance:

- If the initial pattern is (.+) and the replacement pattern is \1, then the string jOe is mapped to jOe (no change).
- If the initial pattern is (.+) and the replacement pattern is _1, then the string jOe is mapped to joe.
- If the initial pattern is (.+) and the replacement pattern is \^1, then the string jOe is mapped to JOE.
- If the initial pattern is (.+) and the replacement pattern is \&1, then the string jOe is mapped to Joe.

If the character following a backslash-underscore (_), backslash-caret (\^), or backslash-ampersand (\&) sequence is not a digit, then the character following the backslash is used verbatim.

The following example converts any Windows user in the domain named "ENG" into a UNIX user with the same name in NIS.

Pattern	Replacement
ENG\\(.+)	\1

The double backslash (\\) matches a single backslash. The parentheses denote a subexpression but do not match any characters themselves. The period matches any single character. The asterisk matches zero or more of the previous expression. In this example, you are matching ENG\ followed by one or more of any character. In the replacement, \1 refers to whatever the first subexpression matched. Assuming the Windows user ENG\jones, the replacement evaluates to jones; that is, the portion of the name following ENG\.

> **Note:** If you are using the CLI, you must delimit all regular expressions with double quotation marks ("). For instance, to enter the regular expression (.+) in the CLI, type "(.+)" at the command prompt. Quotation marks are not required in the Web UI.

For further information about regular expressions, see your UNIX system administration documentation, the online UNIX documentation for sed or regex, or *Mastering Regular Expressions*, published by O'Reilly and Associates.

Creating a name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

About this task

For each Storage Virtual Machine (SVM), Data ONTAP supports up to 1,024 name mappings for each direction.

Step

1. To create a name mapping, enter the following command:

    `vserver name-mapping create -vserver vserver_name -direction {krb-unix|`
    `win-unix|unix-win} -position integer -pattern text -replacement text`

    `-vserver vserver_name` specifies the SVM name.

    `-direction {krb-unix|win-unix|unix-win}` specifies the mapping direction.

    `-position integer` specifies the desired position in the priority list of a new mapping.

    `-pattern text` specifies the pattern to be matched, up to 256 characters in length.

    `-replacement text` specifies the replacement pattern, up to 256 characters in length.

    When Windows-to-UNIX mappings are created, any CIFS clients that have open connections to the Data ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

    Examples

    The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\John.

    ```
    vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
    -position 1 -pattern johnd -replacement "ENG\\John"
    ```

    The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. The mapping maps every CIFS user in the domain ENG to users in the NIS domain associated with the SVM.

    ```
    vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
    -position 1 -pattern "ENG\\(.+)"
    -replacement "\1"
    ```

Commands for managing name mappings

There are specific Data ONTAP commands for managing name mappings.

If you want to...	Use this command...
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`

See the man page for each command for more information.

Configuring multidomain name-mapping searches

You can configure Storage Virtual Machines (SVMs) to perform multidomain name-mapping searches. This enables Data ONTAP to search every bidirectional trusted domain to find a match when performing UNIX user to Windows user name mapping.

Related concepts

Related tasks

Multidomain searches for UNIX user to Windows user name mappings

Data ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used

instead of the discovered trusted domain list and is searched in order until a matching result is returned.

How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with Data ONTAP. Active Directory trust relationships with the CIFS server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the CIFS server on the Storage Virtual Machine (SVM) belongs.

- *Bidirectional trust*
  With bidirectional trusts, both domains trust each other. If the CIFS server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.
  UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.
- *Outbound trust*
  With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.
  A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.
- *Inbound trust*
  With an inbound trust, the other domain trusts the CIFS server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.
  A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

How wildcards (*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user "root" is mapped to the user named "administrator". All trusted domains are searched in order until the first matching user named "administrator" is found.
*	**	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found.

How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by Data ONTAP

  - The advantage to this method is that there is no management overhead and that the list is made of trusted domains that Data ONTAP has determined are valid.
  - The disadvantage is that you cannot choose the order that the trusted domains are searched.
- Use the preferred trusted domain list that you compile

  - The advantage to this method is that you can configure the list of trusted domains in the order that you want them searched.
  - The disadvantage is that there is more management overhead and that the list might become outdated, with some listed domains not being valid, bidirectionally trusted domains.

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.

  The search ends as soon as the Windows user is found. If the same Windows user name exists in two different trusted domains, then the user belonging to the domain listed first in the preferred trusted-domain list is returned. If the Windows user is not found in any domains in the preferred list, an error is returned.

  If you want the home domain to be included in the search, it must be included in the preferred trusted domain list.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.

  The search ends as soon as the Windows user is found. If the same Windows user name exists in two different trusted domains, the user belonging to the domain listed first in the automatically discovered trusted-domain list is returned. You cannot control the order of the trusted domains in the automatically discovered list. If the Windows user is not found in any of the discovered trusted domains, the user is then looked up in the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

Related concepts

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23
Name mapping conversion rules on page 116
Creating name mappings on page 115

Related tasks

Resetting and rediscovering trusted domains on page 122
Displaying information about discovered trusted domains on page 123

Enabling or disabling multidomain name mapping searches

With multidomain name mapping searches, you can use a wild card (*) in the domain portion of a
Windows name when configuring UNIX user to Windows user name mapping. Using a wild card (*)
in the domain portion of the name enables Data ONTAP to search all domains that have a
bidirectional trust with the domain that contains the CIFS server's computer account.

About this task

As an alternative to searching all bidirectionally trusted domains, you can configure a list of
preferred trusted domains. When a list of preferred trusted domains is configured, Data ONTAP uses
the preferred trusted domain list instead of the discovered bidirectionally trusted domains to perform
multidomain name mapping searches.

- Multidomain name mapping searches are enabled by default.
- This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

   set -privilege advanced

2. Perform one of the following actions:

If you want multidomain name mapping searches to be...	Enter the command...
Enabled	**vserver cifs options modify -vserver** *vserver_name* **-is-trusted-domain-enum-search-enabled true**
Disabled	**vserver cifs options modify -vserver** *vserver_name* **-is-trusted-domain-enum-search-enabled false**

3. Return to the admin privilege level:

   set -privilege admin

Related references

Available CIFS server options on page 59

Resetting and rediscovering trusted domains

You can force the rediscovery of all the trusted domains. This can be useful when the trusted domain
servers are not responding appropriately or the trust relationships have changed. Only domains with a

bidirectional trust with the home domain, which is the domain containing the CIFS server's computer account, are discovered.

Step

1. Reset and rediscover trusted domains by using the `vserver cifs domain trusts rediscover` command.

   Example

   `vserver cifs domain trusts rediscover -vserver vs1`

Related tasks

Displaying information about discovered trusted domains

You can display information about the discovered trusted domains for the CIFS server's home domain, which is the domain containing the CIFS server's computer account. This can be useful when you want to know which trusted domains are discovered and how they are ordered within the discovered trusted-domain list.

About this task

Only the domains with bidirectional trusts with the home domain are discovered. Since the home domain's domain controller (DC) returns the list of trusted domains in an order determined by the DC, the order of the domains within the list cannot be predicted. By displaying the list of trusted domains, you can determine the search order for multidomain name mapping searches.

The displayed trusted domain information is grouped by node and Storage Virtual Machine (SVM).

Step

1. Display information about discovered trusted domains by using the `vserver cifs domain trusts show` command.

   Example

   `vserver cifs domain trusts show -vserver vs1`

   ```
      Node: node1
   Vserver: vs1

   Home Domain          Trusted Domain
   -------------------- ----------------------------------
   EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

      Node: node2
   ```

```
Vserver: vs1

Home Domain            Trusted Domain
---------------------  ----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM
```

Related tasks

Adding, removing, or replacing trusted domains in preferred trusted domain lists

You can add or remove trusted domains from the preferred trusted domain list for the CIFS server or you can modify the current list. If you configure a preferred trusted domain list, this list is used instead of the discovered bidirectional trusted domains when performing multidomain name mapping searches.

About this task

- If you are adding trusted domains to an existing list, the new list is merged with the existing list with the new entries placed at the end. The trusted domains are searched in the order they appear in the trusted domain list.
- If you are removing trusted domains from the existing list and do not specify a list, the entire trusted domain list for the specified Storage Virtual Machine (SVM) is removed.
- If you modify the existing list of trusted domains, the new list overwrites the existing list.

Note: You should enter only bidirectionally trusted domains in the preferred trusted domain list. Even though you can enter outbound or inbound trust domains into the preferred domain list, they are not used when performing multidomain name mapping searches. Data ONTAP skips the entry for the unidirectional domain and moves on to the next bidirectional trusted domain in the list.

Step

1. Perform one of the following actions:

If you want to do the following with the list of preferred trusted domains...	Use the command...
Add trusted domains to the list	`vserver cifs domain name-mapping-search add -vserver vserver_name -trusted-domains FQDN, ...`
Remove trusted domains from the list	`vserver cifs domain name-mapping-search remove -vserver vserver_name [-trusted-domains FQDN, ...]`

If you want to do the following with the list of preferred trusted domains...	Use the command...
Modify the existing list	`vserver cifs domain name-mapping-search modify -vserver vserver_name -trusted-domains FQDN, ...`

`-vserver vserver_name` specifies the SVM name.

`-trusted-domain FQDN` specifies a comma-delimited list of fully-qualified domain names of the trusted domains for the home domain. The home domain is the domain which contains the computer account for the CIFS server.

Examples

The following command adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred trusted domain list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1 -
trusted-domains cifs1.example.com, cifs2.example.com
```

The following command removes two trusted domains from the list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1 -
trusted-domains cifs1.example.com, cifs2.example.com
```

The following command modifies the trusted domain list used by SVM vs1. The new list replaces the original list:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1 -
trusted-domains cifs3.example.com
```

Related tasks

Displaying information about the preferred trusted domain list

You can display information about which trusted domains are in the preferred trusted domain list and the order in which they are searched if multidomain name mapping searches are enabled. You can configure a preferred trusted domain list as an alternative to using the automatically discovered trusted domain list.

Step

1. Perform one of the following actions:

If you want to display information about the following...	Use the command...
All preferred trusted domains in the cluster grouped by Storage Virtual Machine (SVM)	`vserver cifs domain name-mapping-search show`
All preferred trusted domains for a specified SVM	`vserver cifs domain name-mapping-search show -vserver vserver_name`

Examples

The following command displays information about all preferred trusted domains on the cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Related tasks

Adding, removing, or replacing trusted domains in preferred trusted domain lists on page 124

Creating and configuring SMB shares

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, Data ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the Storage Virtual Machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you re-create the CIFS server on the SVM, you must re-create the SMB shares.

Related concepts

How file and share permissions are used to secure SMB access on page 24

Managing file access using SMB on page 156

Configuring Data ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions on page 341

What the default administrative shares are

When you create a CIFS server on your Storage Virtual Machine (SVM), three default administrative shares are automatically created. You should understand what those default shares are and how they are used.

Data ONTAP creates the following default administrative shares when you create the CIFS server:

- ipc$
- admin$
- c$

Because shares that end with the $ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

How the ipc$ and admin$ default shares are used

The ipc$ and admin$ shares are used by Data ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

- ipc$ share

  The ipc$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc$ share is used during remote administration of a computer and when viewing a computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc$ share. You also cannot rename or delete the ipc$ share.
- admin$ share

  The admin$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin$ share. You also cannot rename or delete the admin$ share.

How the c$ default share is used

The c$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c$ share:

- The path for this share is always the path to the SVM root volume and cannot be modified.
- The default ACL for the c$ share is Administrator / Full Control.

  This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.
- You can change the c$ share's ACL.
- You can change the c$ share settings and share properties.
- You cannot delete the c$ share.
- Data ONTAP 8.2.1 and later releases in the 8.2 release family support c$ as a default administrative share that is automatically created during SVM creation.

- If you are upgrading from a version of Data ONTAP that does not support automatic creation of the c$ administrative share and a CIFS server already exists on the SVM, the c$ share is not automatically created upon upgrade.

  In this case, the administrator must manually create the c$ share.

- If you revert or downgrade to a version of Data ONTAP that does not support the c$ share and a CIFS server already exists on the SVM, the c$ administrative share is not automatically deleted.

  The c$ administrative share continues to exist and can be used to administer and manage files and folders in the SVM root volume.

- The SVM administrator can access the rest of the SVM namespace from the mapped c$ share by crossing the namespace junctions.

- The c$ share can be accessed by using the Microsoft Management Console.

Related tasks

Share naming considerations

You should keep Data ONTAP share naming considerations in mind when creating SMB shares on your CIFS server.

Share naming conventions for Data ONTAP are the same as for Windows and include the following requirements:

- The name of each share must be unique for the CIFS server.
- Share names are not case-sensitive.
- The maximum share name length is 80 characters.
- Unicode share names are supported.
- Share names ending with the $ character are hidden shares.
- The ADMIN$, IPC$, and c$ administrative shares are automatically created on every CIFS server and are reserved share names.
- You cannot use the share name ONTAP_ADMIN$ when creating a share.
- Share names containing spaces are supported:

  - You cannot use a space as the first character or as the last character in a share name.
  - You must enclose share names containing a space in quotation marks.

    Note: Single quotation marks are considered part of the share name and cannot be used in place of quotation marks.

- The following special characters are supported when you name SMB shares:
  ! @ # $ % & ' _ - . ~ ( ) { }
- The following special characters are not supported when you name SMB shares:
  + [ ] " / \ : ; | < > , ? * =

Related concepts

Related tasks

Non-Unicode clients not supported

Clustered Data ONTAP only supports Unicode clients when accessing data using CIFS.

> **Note:** Because of a limitation, older Macintosh clients running versions Tiger (Mac OS X 10.4.11) and Leopard (Mac OS X 10.5.8) do not fully support Unicode in SMB requests; therefore, they are not supported with Data ONTAP 8.2 or later. To use Macintosh clients when mounting shares with SMB, they must be upgraded to Snow Leopard (Mac OS X 10.6) or later.

Elimination of execute permission requirements on share paths

For versions of Data ONTAP earlier than 8.1.2, if the root of the name space and any contained path components, including junction points, does not allow execute access for a user accessing a folder through an SMB share, access might be denied. Starting with Data ONTAP 8.1.2 and later releases, this restriction is eliminated.

Data ONTAP supports a unified namespace for NAS. A NAS namespace consists of the root of the Storage Virtual Machine (SVM) namespace and FlexVol volumes that are joined together with junctions that present as a hierarchy of subdirectories below the root. This namespace hierarchy presents to the clients as a single SMB share. In essence, junctions stitch together volumes to create a single large file structure.

SMB clients can access the namespace by mapping to the root of the namespace, thus providing access to all the volumes beneath it through the data LIFs on the SVM. Alternatively, clients can also access contained flexible volumes by mounting or mapping at the volume junction points or by mapping using a path to a directory within the namespace, which provides alternative routes to access data contained within the junctioned volumes.

In versions earlier than Data ONTAP 8.1.2, SMB access issues might occur where the root of the namespace or any component in the path to the folder being accessed has an effective UNIX security style (a UNIX security-style volume or a mixed security-style volume with a UNIX effective security). Access issues can occur because of the requirement that the mapped UNIX user must have execute permissions on the namespace root and on any path component that is of UNIX security style (either through the owner, group, or other mode bits or through NFSv4 ACLs). This is a requirement, irrespective of the share location within the namespace hierarchy. This requirement does not apply if all volumes including the root of the namespace and all LS mirrors are of NTFS security style.

For example, consider the path `/unix1/dir1/dir2/ntfs1/`, in which `unix1` is a UNIX security-style volume, `ntfs1` is an NTFS security-style volume, and `dir1` and `dir2` are regular directories. In versions of Data ONTAP earlier than 8.1.2, a user must have execute permissions on `unix1`, `dir1`, and `dir2` to map a share that points to the path.

Starting with Data ONTAP 8.1.2 and later, this restriction is eliminated. Execute permissions are not required for the mapped UNIX user to access data over SMB shares. This is true regardless of security style for the namespace root, any directory component within the path, or any junctioned volumes.

Be aware that after upgrading to Data ONTAP 8.1.2 or later from a version of Data ONTAP earlier than 8.1.2, effective access permissions might change as a result of eliminating this requirement. If you are using the execute permission requirement as a way to restrict SMB access, you might need to adjust your share or file permissions to apply the desired access restrictions.

Information you need when creating SMB shares

You should be aware of what information you need before creating SMB shares. There are certain required parameters that you must supply when you create SMB shares and certain choices about share parameters and share properties that you must make.

When you create a share, you must provide all of the following information:

- The name of the Storage Virtual Machine (SVM) on which to create the share
- The complete path in a volume to the SMB share, beginning with the junction path to the volume
  The SMB share path is case sensitive.
- The name of the share entered by users when they connect to the share

When you create a share, you can optionally specify a description for the share. The share description appears in the **Comment** field when you browse the shares on the network.

You can specify the following optional share parameters:

- Whether support for symlinks and widelinks in the share is allowed
- Whether a custom UNIX umask is configured for new files configured on the share
- Whether a custom UNIX umask is configured for new directories configured on the share
- Whether a custom attribute cache lifetime is configured for the attribute cache
  This share setting is useful only if the attribute cache share property is set.
- Whether to configure offline files, and if so, which offline file setting to specify
- Whether operations trigger virus scans on the share, and if so, which operations trigger the scan
  For more information about configuring an antivirus solution, see the *Clustered Data ONTAP Antivirus Configuration Guide*.

You can specify the following optional share properties:

- Whether the share is a home directory share
- Whether the share supports opportunistic locks
- Whether the share is browsable
- Whether the share shows Snapshot copies
- Whether the share supports change notification
- Whether metadata caching is enabled for the share
- Whether the share is a continuously available share
- Whether the share allows clients to request BranchCache hashes on the files within the share

- Whether the share supports access-based enumeration

Related concepts

Share naming considerations on page 128

Related tasks

Creating an SMB share on a CIFS server on page 131

Creating an SMB share on a CIFS server

You must create an SMB share before you can share data on a CIFS server with SMB clients. When you create a share, you can customize the share by configuring optional settings, such as specifying how symlinks are presented to clients. You can also set share properties when creating the share.

Steps

1. If necessary, create the directory path structure for the share.

   You must create the directory path structure specified by the `-path` option in the `vserver cifs share create` command before creating your share. The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

   If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial "\\" in the UNC path), then the **Security** tab in the Windows Properties box is unavailable. This is a Windows client issue rather than a Data ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

2. Create an SMB share on a CIFS server associated with the specified Storage Virtual Machine (SVM) by entering the following command:
   vserver cifs share create -vserver *vserver_name* **-share-name** *share_name*
   -path *path* **[-share-properties** *share_properties***,...] [-symlink-properties**
   {enable|hide|read_only},...] [-file-umask *octal_integer***] [-dir-umask**
   *octal_integer***] [-comment** *text***] [-attribute-cache-ttl [***integer***h]|**
   [*integer***m]|[***integer***s]] [-offline-files {none|manual|documents|programs}]**
   [-vscan-fileop-profile {no-scan|standard|strict|writes-only}]

   `-vserver` *vserver_name* specifies the CIFS-enabled SVM on which to create the share.

   `-share-name` *share_name* specifies the name of the new SMB share.

   `-path` *path* specifies the directory path to the SMB share.

   - This path must exist.
   - A directory path name can be up to 255 characters long.
   - If there is a space in the path name, the entire string must be quoted (for example, "/new volume/mount here").
   - If this is a home directory share as specified by the value of home directory on the `-share-properties` parameter, you can make the share name dynamic by specifying the `%w`

(Windows user name), `%u` (UNIX user name), `%d` (domain name) variables, or any of their combinations as a part of the value of this parameter.

`-share-properties` *share_properties* specifies an optional list of properties for the share.

- The default initial property for all shares on FlexVol volumes are `oplocks`, `changenotify`, and `browsable`.
- It is optional to specify share properties when you create a share.
  However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all the share properties that you want to apply to the share using a comma-delimited list.
- For SVMs with Infinite Volume, the default initial properties are `oplocks` and `browsable`.

The list of share properties can include one or more of the following:

- `homedirectory`
  The Data ONTAP CIFS home directory feature enables you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the SVM).

  Note: This property cannot be added or removed after share creation.

- `oplocks`
  This specifies that the share uses opportunistic locks, also known as *client-side caching*. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled.
  An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named `/dept/finance` contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.

- `browsable`
  This specifies that the share can be browsed by Windows clients.

- `showsnapshot`
  This specifies that Snapshot copies can be viewed and traversed by clients.

- `changenotify`
  This specifies that the share supports *Change Notify* requests. For shares on SVMs with FlexVol volumes, this is a default initial property.
  For shares on SVMs with Infinite Volume, the `changenotify` property is not set by default, and setting it requires the advanced privilege level. When the `changenotify` property is set for a share on SVMs with Infinite Volume, change notifications are not sent for changes to file attributes and time stamps.

- `attributecache`

This specifies that file attribute caching on the SMB share is enabled to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.

- `continuously-available`

  This specifies that SMB 3.0 and later clients that support it are permitted to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for SVMs with Infinite Volume.

- `branchcache`

  This specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is effective only if you specify `per-share` as the operating mode in the CIFS BranchCache configuration. This option is not supported for SVMs with Infinite Volume.

- `access-based-enumeration`

  This specifies that *Access Based Enumeration* is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

`-symlink-properties` *share_symlink_property* specifies how UNIX symbolic links (symlinks) are presented to SMB clients. You can specify one of the following values:

- `enabled`

  This setting specifies that symlinks are enabled for read-write access

- `read_only`

  This setting specifies that symlinks are enabled for read-only access

- `hide`

  This setting specifies that SMB clients are prevented from seeing symlinks

  Note: To disable symlinks, specify the value as "" or "-".

`-file-umask` *octal_integer* specifies the default UNIX umask for new files created on the share. If not specified, the umask defaults to 022.

`-dir-umask` *octal_integer* specifies the default UNIX umask for new directories created on the share. If not specified, the umask defaults to 000.

  Note: Accessing an existing directory or file through multiple SMB shares that have different values for the `-file-umask` and `-dir-umask` parameters returns consistent permissions and access rights. For instance, assume you have a share named "share1" that has a file umask of 000 and a share named "share2" that has a file umask of 022, and that these shares overlap (that is, can access the same directories). If you create a file named \\server\share1\abc, the umask for that file is 000. If you create a file named \\server\share2\123, the umask for that file is 022.

`-comment` *text* specifies a text description of the share. The description can be up to 255 characters long. If there is a space in the description, the entire string must be quoted (for example, "This is engineering's share.").

`-attribute-cache-ttl` *time_interval* specifies the lifetime for the attribute cache share property. Specifying this option is useful only if you specify `attributecache` as a value of the `-share-properties` parameter.

`-offline-files` specifies the caching behavior of Windows clients when accessing data from the share. The value can be one of following:

- `none`
  This setting disallows Windows clients from caching any files on this share.
- `manual`
  This setting allows users on Windows clients to manually select files to be cached.
- `documents`
  This setting allows Windows clients to cache user documents that are used by the user for offline access.
- `programs`
  This setting allows Windows clients to cache programs that are used by the user for offline access. A user can use those files in an offline mode even if the share is available.

`-vscan-filop-profile` specifies which operations trigger virus scans. The value can be one of following:

- `no-scan`
  Virus scans are never triggered for this share.
- `standard`
  Virus scans are triggered by open, close, and rename operations. This is the default profile.
- `strict`
  Virus scans are triggered by open, read, close, and rename operations.
- `writes-only`
  Virus scans are triggered only when a file that has been modified is closed.

For information about configuring an antivirus solution, see the *Clustered Data ONTAP Antivirus Configuration Guide*.

Examples

The following command creates an SMB share named "SHARE1" on Storage Virtual Machine (SVM, formerly known as Vserver) "vs1". Its directory path is /u/eng. Oplocks and browsability are specified on the share, and the UNIX umask is explicitly set as 022 on files and 000 on directories.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name
SHARE1 -path /u/eng -share-properties browsable,oplocks -file-umask
022 -dir-umask 000
```

The following command creates an SMB share named "DOCUMENTS" on the SVM "vs1". The path to the share is /documents. The share uses opportunistic locks (client-side caching),

a notification is generated when a change occurs, and the share allows clients to cache user documents on this share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name
DOCUMENTS -path /documents -share-properties changenotify,oplocks -
offline-files documents
```

Related concepts

What the default administrative shares are on page 127
Share naming considerations on page 128
Information you need when creating SMB shares on page 130
Securing file access by using SMB share ACLs on page 139
Securing file access by using file permissions on page 141

Related tasks

Displaying SMB session information on page 257
Displaying information about open SMB files on page 260
Adding or removing share properties on an existing SMB share on page 135

Adding or removing share properties on an existing SMB share

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

Before you begin

The share whose properties you want to modify must exist.

About this task

You need to keep the following in mind when adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect.
  Newly added properties are appended to the existing list of share properties.
- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the vserver cifs share properties add command.
  You can use the vserver cifs share properties remove command to remove share properties.

You need to keep the following in mind when removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.

The available share properties are as follows:

Share properties	Description
oplocks	This property specifies that the share uses opportunistic locks, also known as client-side caching.
browsable	This property allows Windows clients to browse the share.
showsnapshot	This property specifies that Snapshot copies can be viewed and traversed by clients.
changenotify	This property specifies that the share supports Change Notify requests. For shares on an SVM with FlexVol volumes, this is a default initial property. For shares on an SVM with Infinite Volume, the changenotify property is not set by default, and setting it requires the advanced privilege level. When the changenotify property is set for a share on an SVM with Infinite Volume, change notifications are not sent for changes to file attributes and time stamps.
attributecache	This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.
continuously-available	This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
branchcache	This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration.
access-based-enumeration	This specifies that *Access Based Enumeration* is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

Steps

1. Enter the appropriate command:

If you want to...	Enter the command...
Add share properties	**vserver cifs share properties add -vserver** *vserver_name* **-share-name** *share_name* **-share-properties** *properties,...*
Remove share properties	**vserver cifs share properties remove -vserver** *vserver_name* **-share-name** *share_name* **-share-properties** *properties,...*

- -vserver *vserver_name* specifies the name of the Storage Virtual Machine (SVM) that contains the share whose properties you want to modify.
- -share-name *share_name* is the name of the share whose properties you want to modify.
- -share-properties *properties* is the list of share properties you want to add or remove.

2. Verify the share property settings:

vserver cifs share show -vserver vserver_name -share-name share_name

---

Examples

The following command adds the showsnapshot share property to a share named "share1" on SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver     Share   Path       Properties   Comment    ACL
---------   ------  --------   ----------   --------   -----------
vs1         share1  /share1    oplocks      -          Everyone /
                               browsable               Full
                               changenotify            Control
                               showsnapshot
```

The following command removes the browsable share property from a share named "share2" on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver     Share   Path       Properties   Comment    ACL
---------   ------  --------   ----------   --------   -----------
vs1         share2  /share2    oplocks      -          Everyone /
                               changenotify            Full
                                                       Control
```

Related tasks

Related references

Viewing information about SVM shares using the MMC

You can view information about SMB shares on your Storage Virtual Machine (SVM) using the MMC (Microsoft Management Console). Before you can view the shares, you need to connect the MMC to the SVM.

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select **Manage**.

2. On the left panel, select **Computer Management**.

3. Select **Action > Connect to another computer**.

   The Select Computer dialog box appears.

4. Type the name of the storage system or click **Browse** to locate the storage system.

5. Click **OK**.

   The MMC connects to the SVM.

6. Perform the following:

   a) From the Computer Management page, expand the **System Tools** hierarchy in the left navigation pane.

      An error message displays: `The remote procedure call failed and did not execute(1727).` The right display pane remains blank. This is a known issue in this version of Data ONTAP.

   b) To work around this issue, click **OK** to close the error box, and then click **System Tools** again.

      The **System Tools** hierarchy expands.

7. In the navigation pane, click **Shared Folders > Shares**.

   A list of shares on the SVM is displayed in the right display pane.

8. To display the share properties for a share, double-click the share to open the **Properties** box.

Commands for managing SMB shares

You use the `vserver cifs share` and `vserver cifs share properties` commands to manage SMB shares.

If you want to...	Use this command...
Create an SMB share	`vserver cifs share create`
Display SMB shares	`vserver cifs share show`
Modify an SMB share	`vserver cifs share modify`
Delete an SMB share	`vserver cifs share delete`
Add share properties to an existing share	`vserver cifs share properties add`
Remove share properties from an existing share	`vserver cifs share properties remove`
Display information about share properties	`vserver cifs share properties show`

See the man page for each command for more information.

Securing file access by using SMB share ACLs

You can secure access to files and folders over a network by configuring share access control lists (ACLs) on SMB shares. Share-level ACLs are used in combination with file-level permissions and, optionally, export policies to determine effective access rights.

You can use either domain or local users or groups when configuring ACLs.

Related concepts

Related tasks

How Data ONTAP uses share-level ACLs

A share-level ACL consists of a list of access control entries (ACEs). Each ACE contains a user or group name and a set of permissions that determines user or group access to the share, regardless of the security style of the volume or qtree containing the share.

When an SMB user tries to access a share, Data ONTAP always checks the share-level ACL (access control list) to determine whether access should be granted.

A share-level ACL only restricts access to files in the share; it never grants more access than the file-level ACLs.

Creating SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

Steps

1. Use the `vserver cifs share access-control create` command to create an access control list for an SMB share.

2. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

> The following command gives `Change` permissions to the group named "salesteam" for the share "sales" on the Storage Virtual Machine (SVM) named vs1:
>
> ```
> cluster1::> vserver cifs share access-control create -vserver vs1 -share
> sales -user-or-group salesteam -permission Change
>
> cluster1::> vserver cifs share access-control show
>               Share       User/Group                   Access
> Vserver       Name        Name                         Permission
> -------------- ----------- -------------------------- -----------
> vs1           sales       salesteam                    Change
> ```

Commands for managing SMB share access control lists

You need to know the commands for managing SMB access control lists (ACLs), which includes creating, displaying, modifying, and deleting them.

If you want to...	Use this command...
Create a new ACL	`vserver cifs share access-control create`
Display ACLs	`vserver cifs share access-control show`
Modify an ACL	`vserver cifs share access-control modify`
Delete an ACL	`vserver cifs share access-control delete`

Securing file access by using file permissions

You can secure access by configuring file permissions on files and folders contained within the share through which SMB clients access data. File-level permissions are used in combination with share-level ACLs and, optionally, export policies to determine effective access rights. Files and folders might be secured with NTFS permissions or UNIX permissions.

If files and folders are secured with UNIX file permissions, then the mapped UNIX user and the UNIX user's groups are used to evaluate file permissions.

Related concepts

How file and share permissions are used to secure SMB access on page 24

How security styles affect data access on page 19

How name mapping is used to secure SMB file access on SVMs with FlexVol volumes on page 23

How UNIX file permissions provide access control when accessing files over SMB on page 147

Securing file access by using SMB share ACLs on page 139

Related tasks

Performing security traces on page 236

Configuring standard NTFS file permissions by using the Windows Security tab

You can configure standard NTFS file permissions on files and directories by using the Windows Security tab in the Windows Properties window. This is the same method used when configuring standard file permissions on data residing on a Windows client.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain DACLs for applying file and folder access permissions, security access control lists (SACLs) for file and folder auditing, or both SACLs and DACLs.

You can set standard NTFS file permissions for file and folder access by completing the following steps on a Windows host:

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** box:

   a) Select a **Drive** letter.

   b) In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

   Example

   If your CIFS server name is CIFS_SERVER and your share is named "share1", you would enter \\CIFS_SERVER\share1.

   > **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

   c) Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.

4. Right-click the file or directory, and then select **Properties**.

5. Select the **Security** tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

6. Click **Edit**.

   The Permissions for <Object> box opens.

7. Perform the desired actions:

If you want to....	Do the following...
Set standard NTFS permissions for a new user or group	**a.** Click **Add**. The Select User, Computers, Service Accounts, or Groups window opens. **b.** In the **Enter the object names to select** box, type the name of the user or group on which you want to add NTFS permission. **c.** Click **OK**.
Change or remove standard NTFS permissions from a user or group	In the **Group or user names** box, select the user or group that you want to change or remove.

8. Perform the desired actions:

If you want to...	Do the following
Set standard NTFS permissions for a new or existing user or group	In the **Permissions for <Object>** box, select the **Allow** or **Deny** boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click **Remove**.

Standard permissions are compilations of the more granular advanced access rights. You can set the following types of standard permissions:

- **Full control**
- **Modify**
- **Read & Execute**
- **List folder contents**
- **Read**
- **Write**

> **Note:** If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

9. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

For more information about how to set standard NTFS permissions, see your Windows documentation.

Related concepts

[Displaying information about file security and audit policy on FlexVol volumes](#) on page 186

Related tasks

[Configuring and applying file security on NTFS files and folders using the CLI](#) on page 205
[Displaying information about file security on NTFS security-style FlexVol volumes](#) on page 187
[Displaying information about file security on mixed security-style FlexVol volumes](#) on page 191
[Displaying information about file security on UNIX security-style FlexVol volumes](#) on page 194

Configuring advanced NTFS file permissions using the Windows Security tab

You can configure standard NTFS file permissions on files and folders by using the **Windows Security** tab in the Windows Properties window.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** dialog box:

   a) Select a **Drive** letter.
   b) In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

   Example

   If your CIFS server name is "CIFS_SERVER" and your share is named "share1", you should type \\CIFS_SERVER\share1.

   > **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

   c) Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.

4. Right-click the file or directory, and then select **Properties**.

5. Select the **Security** tab.

   The **Security** tab displays the list of users and groups for which NTFS permission are set. The **Permissions for** box displays a list of Allow and Deny permissions in effect for each user or group selected.

6. Click **Advanced**.

   The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click **Change Permissions**.

   The Permissions window opens.

8. Perform the desired actions:

If you want to...	Do the following...
Set up advanced NTFS permissions for a new user or group	**a.** Click **Add**.
	b. In the **Enter the object name to select** box, type the name of the user or group that you want to add.
	c. Click **OK**.
Change advanced NTFS permissions from a user or group	**a.** In the **Permissions entries:** box, select the user or group whose advanced permissions you want to change.
	b. Click **Edit**.
Remove advanced NTFS permissions for a user or group	**a.** In the **Permissions entries:** box, select the user or group that you want to remove.
	b. Click **Remove**.
	c. Skip to Step 13.

If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for <Object> box opens.

9. In the **Apply to** box, select how you want to apply this NTFS file permission entry.

You can select one of the following:

- **This folder, subfolders and files**
- **This folder and subfolders**
- **This folder only**
- **This folder and files**
- **Subfolders and files only**
- **Subfolders only**
- **Files only**

If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

- To allow the specified access, select the **Allow** box.
- To not allow the specified access, select the **Deny** box.

You can set permissions on the following advanced rights:

- **Full control**
  If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).
- **Traverse folder / execute file**
- **List folder / read data**

- **Read attributes**
- **Read extended attributes**
- **Create files / write data**
- **Create folders / append data**
- **Write attributes**
- **Write extended attributes**
- **Delete subfolders and files**
- **Delete**
- **Read permissions**
- **Change permissions**
- **Take ownership**

> **Note:** If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

11. If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.

12. Click **OK**.

13. After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:

    - Select the **Include inheritable permissions from this object's parent** box.
      This is the default.
    - Select the **Replace all child object permissions with inheritable permissions from this object** box.
      This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.

      > **Note:** Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in Data ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.

    - Select both boxes.
    - Select neither box.

14. Click **OK** to close the **Permissions** box.

15. Click **OK** to close the **Advanced Security settings for <Object>** box.

    For more information about how to set advanced NTFS permissions, see your Windows documentation.

Related tasks

How to configure NTFS file permissions using the Data ONTAP CLI

You can configure NTFS file permissions on files and directories using the Data ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

Related tasks

How UNIX file permissions provide access control when accessing files over SMB

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions
  Configuring export permissions for SMB access is optional in Data ONTAP 8.2 and later releases.
- Share permissions
- File permissions
  The following types of file permissions might be applied to the data on which the user wants to perform an action:

  - NTFS
  - UNIX NFSv4 ACLs
  - UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.

> **Note:** Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

Securing SMB access using export policies

You can optionally use export policies to restrict SMB access to files and folders on Storage Virtual Machine (SVM) volumes. You can use export policies in combination with share-level and file-level permissions to determine effective access rights.

For information about configuring and managing export policies, see the *Clustered Data ONTAP File Access Management Guide for NFS*.

Related concepts

Role export policies play with SMB access on page 26
Creating and configuring SMB shares on page 126
Securing file access by using SMB share ACLs on page 139
Securing file access by using file permissions on page 141

How export policies are used with SMB access

If export policies for SMB access are enabled on the CIFS server, export policies are used when controlling access to Storage Virtual Machine (SVM) volumes or qtrees by SMB clients. To access data, you can create an export policy that allows SMB access and then associate the policy with the volumes or qtrees containing SMB shares.

An export policy has one or more rules applied to it that specifies which clients are allowed access to the data and what authentication protocols are supported for read-only and read-write access. You can configure export policies to allow access over SMB to all clients, a subnet of clients, or a specific client and to allow authentication using Kerberos authentication, NTLM authentication, or both Kerberos and NTLM authentication when determining read-only and read-write access to data.

After processing all export rules applied to the export policy, Data ONTAP can determine whether the client is granted access and what level of access is granted. Export rules apply to client machines, not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions.

You associate exactly one export policy with each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

- Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
- Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

You associate exactly one export policy to each volume or qtree to configure client access to the volume or qtree. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

Each SVM has at least one export policy called "default", which contains no rules. You cannot delete this export policy, but you can rename or modify it. Each volume on the SVM by default is associated with the default export policy. If export policies for SMB access is disabled on the SVM, the "default" export policy has no effect on SMB access.

You can configure rules that provide access to both NFS and SMB hosts and associate that rule with an export policy, which can then be associated with the volume or qtree that contains data to which both NFS and SMB hosts need access. Alternatively, if there are some volumes or qtrees where only SMB clients require access, you can configure an export policy with rules that only allow access using the SMB protocol and that uses only Kerberos or NTLM (or both) for authentication for read-only and write access. The export policy is then associated to the volumes or qtrees where only SMB access is desired.

If export policies for SMB is enabled and a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the volume's export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied. This is true even if the share and file permissions would otherwise permit access. This means that you must configure your export policy to minimally allow the following on volumes or qtrees containing SMB shares:

- Allow access to all clients or the appropriate subset of clients
- Allow access over SMB
- Allow appropriate read-only and write access by using Kerberos or NTLM authentication (or both)

For information about configuring and managing export policies, see the *Clustered Data ONTAP File Access Management Guide for NFS*.

Related concepts

Related tasks

Related references

What happens to existing SMB export policies when upgrading

For releases earlier than Data ONTAP 8.2, SMB export policies are mandatory. Starting with Data ONTAP 8.2, export policies for SMB access are optional and are disabled by default. You need to be aware of what happens when upgrading from releases where export policies are mandatory.

If you upgrade from a version of Data ONTAP where configured export policies were mandatory for SMB access and the cluster contains Storage Virtual Machines (SVMs) with CIFS servers, support for export policies is enabled for those SVMs after the upgrade. You do not need to reconfigure SMB access for existing CIFS servers when upgrading.

If you create a new SVM and CIFS server on the upgraded cluster, export policies for the new CIFS server are disabled by default. You can enable and configure export policies on the new CIFS servers if desired.

Enabling or disabling export policies for SMB access

You can enable or disable export policies for SMB access on Storage Virtual Machines (SVMs). Using export policies to control SMB access to resources is optional for Data ONTAP 8.2 and later.

Before you begin

The following are the requirements for enabling export policies for SMB:

- The client must have a "PTR" record in DNS before you create the export rules for that client.
- An additional set of "A" and "PTR" records for host names is required if the SVM provides access to NFS clients and the host name you want to use for NFS access is different from the CIFS server name.

About this task

Starting with Data ONTAP 8.2, a new option controls whether export policies are enabled for SMB access. When setting up a new CIFS server on your SVM, the usage of export policies for SMB access is disabled by default. You can enable export policies for SMB access if you want to control access based on authentication protocol or on client IP addresses or host names. You can enable or disable export policies for SMB access at any time.

When upgrading a cluster from versions of Data ONTAP earlier than 8.2, this option is automatically enabled on CIFS servers in the cluster that are using export policies to control SMB access. There is no unexpected change to configured access controls when you upgrade to a version of Data ONTAP where export policies for SMB access is optional.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want export policies to be...	Enter the command...
Enabled	**vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled true**
Disabled	**vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false**

3. Return to the admin privilege level:

set -privilege admin

Example

The following example enables the usage of export policies to control SMB client access to resources on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy-
enabled true

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

Related concepts

How export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume or qtree against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.
- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, and the client does not match one or more of them, the rule does not apply.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

Related references

Examples of export policy rules that restrict or allow access over SMB

The examples show how to create export policy rules that restrict or allow access over SMB on a Storage Virtual Machine (SVM) that has export policies for SMB access enabled.

Export policies for SMB access are disabled by default. You need to configure export policy rules that restrict or allow access over SMB only if you have enabled export policies for SMB access.

Export rule for SMB access only

The following command creates an export rule on the SVM named "vs1" that has the following configuration:

- Policy name: cifs1
- Index number: 1
- Client match: Matches only clients on the 192.168.1.0/24 network
- Protocol: Only enables SMB access
- Read-only access: To clients using NTLM or Kerberos authentication
- Read-write access: To clients using Kerberos authentication

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname cifs1
-ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0 -rorule
krb5,ntlm -rwrule krb5
```

Export rule for SMB and NFS access

The following command creates an export rule on the SVM named" vs1" that has the following configuration:

- Policy name: cifsnfs1
- Index number: 2
- Client match: Matches all clients
- Protocol: SMB and NFS access

- Read-only access: To all clients
- Read-write access: To clients using Kerberos (NFS and SMB) or NTLM authentication (SMB)
- Mapping for UNIX user ID 0 (zero): Mapped to user ID 65534 (which typically maps to the user name nobody)
- Suid and sgid access: Allows

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname cifsnfs1
-ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule
krb5,ntlm -anon 65534 -allow-suid true
```

Export rule for SMB access using NTLM only

The following command creates an export rule on the SVM named "vs1" that has the following configuration:

- Policy name: ntlm1
- Index number: 1
- Client match: Matches all clients
- Protocol: Only enables SMB access
- Read-only access: Only to clients using NTLM
- Read-write access: Only to clients using NTLM

Note: If you configure the read-only option or the read-write option for NTLM-only access, you must use IP address-based entries in the client match option. Otherwise, you receive access denied errors. This is because Data ONTAP uses Kerberos Service Principal Names (SPN) when using a host name to check on the client's access rights. NTLM authentication does not support SPN names.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname ntlm1
-ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm -rwrule ntlm
```

For information about configuring and managing export policies, see the *Clustered Data ONTAP File Access Management Guide for NFS*.

Related concepts

How export rules work on page 151

Considerations when reverting export policies for SMB

For releases earlier than Data ONTAP 8.2, SMB export policies are mandatory. Starting with Data ONTAP 8.2, export policies for SMB access are optional and are disabled by default. There are certain considerations when reverting to a release where export policies are mandatory.

There are two scenarios where export policies for SMB access are a consideration when reverting to a version of Data ONTAP where export policies for SMB are mandatory:

- You have a cluster with an installed version of Data ONTAP where the use of export policies for SMB is optional and export policies are disabled on all Storage Virtual Machines (SVMs).

  In this case, the SVMs and contained volumes do not have export policies that allow SMB access. If you revert to a version of Data ONTAP where export policies are mandatory, export policies are turned on and required for SMB access. This results in denial of access to SMB clients.

  The recommendation is that you configure export policies for SMB on all SVMs before you revert so that there are no hard-to-resolve SMB client access issues after the revert.

- You have a cluster with an installed version of Data ONTAP where the use of export policies for SMB access is optional and export policies for SMB are enabled on some but not all of the SVMs.

  If you revert to a version of Data ONTAP where export policies are mandatory, export policies are turned on and required for SMB access for all SVMs. This results in denial of access to SMB clients on SVMs where export policies were not previously enabled.

  The recommendation is that you configure export policies for SMB on all SVMs before you revert so that there are no hard-to-resolve SMB client access issues after the revert.

Note: If you upgraded from a version of Data ONTAP where export policies are mandatory, export policies for SMB were automatically enabled on existing SVMs. Even if you subsequently disabled export policies for SMB on those existing SVMs, the export policies remain in place. Upon a revert back to a version of Data ONTAP where export policies are mandatory, the existing export policies are used to determine SMB access. However, before reverting, you should create export policies for SMB access on any new SVMs created after the initial upgrade.

Managing file access using SMB

After you create and configure a CIFS server on your Storage Virtual Machine (SVM) and set up file access over SMB shares, there are a number of tasks you might want to perform to manage file access.

Using local users and groups for authentication and authorization

You can create local users and groups on the Storage Virtual Machine (SVM). The CIFS server can use local users for CIFS authentication and can use both local users and groups for authorization when determining both share and file and directory access rights.

Local group members can be local users, domain users and groups, and domain machine accounts.

Local users and groups can also be assigned privileges. Privileges control access to SVM resources and can override the permissions that are set on objects. A user or member of a group that is assigned a privilege is granted the specific rights that the privilege allows.

Note: Privileges do not provide clustered Data ONTAP general administrative capabilities.

Related concepts

How Data ONTAP uses local users and groups

When configuring and using local users and groups, you must understand what they are and how they are used. For example, you can use local users and groups to provide share and file-access security to data residing on the Storage Virtual Machine (SVM). You can also assign user management rights to users through the use of local users and groups.

Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

Local user   A user account with a unique security identifier (SID) that has visibility only on the Storage Virtual Machine (SVM) on which it is created. Local user accounts

have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

User accounts have several uses:

- Used to grant *User Rights Management* privileges to a user.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

Local group
A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant *User Rights Management* privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

Local domain
A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

Security identifier (SID)
A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form: S-1-5-21-3139654847-1303905135-2517279418-123456.

NTLM authentication
A Microsoft Windows security method used to authenticate users on a CIFS server.

Cluster replicated database (RDB)
A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

Reasons for creating local users and groups

There are several reasons for creating local users and groups on your Storage Virtual Machine (SVM). For example, you can access the CIFS server using a local user account if the domain controllers are unavailable, or you may want to use local groups to assign privileges.

You can create one or more local user accounts for the following reasons:

- You want the ability to authenticate and log in to the CIFS server if domain controllers are unavailable.
  Local users can authenticate with the CIFS server using NTLM authentication when the domain controller is down or when network problems prevent your CIFS server from contacting the domain controller.
- You want to assign a local user *User Rights Management* privileges.

User Rights Management is the ability for a CIFS server administrator to control what rights users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account or by making the user a member of a local group that has those privileges.

Note: Although a local user can authenticate locally, the CIFS server is not operating in *Workgroup* mode. *Workgroup* mode is not supported in this version of Data ONTAP. The CIFS server must still be part of an Active Directory domain. The CIFS server is operating as a member server in an Active Directory domain.

You might want to create one or more local groups for the following reasons:

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.
  There are certain built-in user groups with predefined privileges. To assign a customized set of privileges, you can create a local group and assign that group the necessary privileges. You can then add local users, domain users, and domain groups to the local group.

Related concepts

How local user authentication works on page 158
What local privileges are on page 161

How local user authentication works

Before a local user can access data on a CIFS server, the user must create an authenticated session.

Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and NTLMv2 are supported.

Data ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server's local domain name (the CIFS server name):

- The domain portion matches
  Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.
- The domain portion does not match
  Data ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed.
  For example, if the user exists in Active Directory but the password is invalid or expired, Data ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where Data ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain

names do not match. For example, if a matching domain account exists but it is disabled, Data ONTAP uses the corresponding local account on the CIFS server for authentication.

• The domain portion is not specified

Data ONTAP first attempts authentication as a local user. If authentication as a local user fails, then Data ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.

After local or domain user authentication is completed successfully, Data ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

Related tasks

How user access tokens are constructed

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user's group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

• Local user login

Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.

• Domain user login

When a domain user logs in, Data ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. Data ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user's domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is Domain Users (RID 513). This default RID cannot be changed in this version of Data ONTAP.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.

Note: There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

Considerations when using SnapMirror on SVMs that contain local groups

There are certain considerations you should keep in mind if you configure SnapMirror on volumes owned by Storage Virtual Machines (SVMs) that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

What happens to local users and groups when deleting CIFS servers

The default set of local users and groups is created when a CIFS server is created, and they are associated with the Storage Virtual Machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.

> **Note:** The CIFS server administrative status does not affect visibility of local users or groups.

How you can use Microsoft Management Console with local users and groups

You can view information about local users and groups from the Microsoft Management Console. With this release of Data ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

Considerations when reverting

If you plan to revert the cluster to a Data ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user rights, you must be aware of certain considerations.

* Due to security reasons, information about configured local users, groups, and privileges are not deleted when Data ONTAP is reverted to a version that does not support local users and groups functionality.
* Upon a revert to a prior major version of Data ONTAP, Data ONTAP does not use local users and groups during authentication and credential creation.
* Local users and groups are not removed from file and folder ACLs.
* File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

What local privileges are

Privileges are well-known rights that can be granted to local and domain users and groups to perform *User Rights Management* tasks on the CIFS server. You cannot create privileges. You can only add or remove existing privileges.

List of supported privileges

Data ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local groups and add privileges to the groups that you created.

The following table lists the supported privileges on the Storage Virtual Machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
SeTcbPrivilege	None	Act as part of the operating system
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Back up files and directories, overriding an ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restore files and directories, overriding any ACLs
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Take ownership of files or other objects
SeSecurityPrivilege	BUILTIN\Administrators	Manage auditing This includes viewing, dumping, and clearing the security log.

Related concepts

[Managing local privileges](#) on page 182

How to assign privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

• You can assign a set of privileges to a group that you create.

You then add a user to the group that has the privileges that you want that user to have.

- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

Related tasks

Requirements and considerations

Before you create and configure local users and groups on your CIFS server, you need to be aware of certain requirements and considerations.

Considerations when using BUILTIN groups and the local administrator account

There are certain considerations you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you should know that you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.
  After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.
- There is no local Guest account.

Related references

Requirements for local user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy*.

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:

  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters:

~ ! @ # 0 ^ & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

Related tasks

List of BUILTIN groups and their default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups
provided by Data ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
BUILTIN\Administrators RID 544 When first created, the local Administrator account, with a RID of 500, is automatically made a member of this group. When the Storage Virtual Machine (SVM) is joined to a domain, the domain\Domain Admins group is added to the group. If the SVM leaves the domain, the domain \Domain Admins group is removed from the group.	• SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege
BUILTIN\Power Users RID 547 When first created, this group does not have any members. Members of this group: • Can create and manage local users and groups. • Cannot add themselves or any other object to the BUILTIN\Administrators group.	none
BUILTIN\Backup Operators RID 551 When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.	• SeBackupPrivilege • SeRestorePrivilege

Predefined BUILTIN group	Default privileges
BUILTIN\Users RID 545 When first created, this group does not have any members (besides the implied Authenticated Users) special group. When the SVM is joined to a domain, the domain\Domain Users group is added to this group. If the SVM leaves the domain, the domain\Domain Users group is removed from this group.	none
Everyone SID S-1-1-0 This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.	none

Related concepts

Related references

Enabling or disabling local users and groups functionality

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, Data ONTAP disables local user and group functionality if any node in the cluster is reverted to a Data ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of Data ONTAP that supports it.

Related concepts

Enabling or disabling local users and groups

You can enable or disable local users and groups for SMB access on Storage Virtual Machines (SVMs). Local users and groups functionality is enabled by default.

About this task

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.

Steps

1. Set the privilege level to advanced:

`set -privilege advanced`

2. Perform one of the following actions:

If you want local users and groups to be...	Enter the command...
Enabled	**`vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true`**
Disabled	**`vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false`**

3. Return to the admin privilege level:

`set -privilege admin`

Example

The following example enables local users and groups functionality on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and-
groups-enabled true

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

Related tasks

Enabling or disabling local user authentication

You can enable or disable local user authentication for SMB access on Storage Virtual Machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

Before you begin

Local users and groups functionality must be enabled on the CIFS server.

About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want local authentication to be...	Enter the command...
Enabled	**`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true`**
Disabled	**`vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false`**

3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following example enables local user authentication on SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth-
enabled true

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

Related concepts

Related tasks

Managing local user accounts

You can manage local user accounts by creating, modifying, and deleting them, and by displaying information about user accounts and group membership. You can also perform other management tasks, such as enabling, disabling, and renaming user accounts, setting the password for an account, and managing local account password complexity.

Related concepts

Creating local user accounts

You can create a local user account that can be used to authorize access to data contained in the Storage Virtual Machine (SVM) over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

Before you begin

Local users and groups functionality must be enabled.

About this task

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account. The user name must meet the following requirements:

- Must not exceed 20 characters
- Cannot be terminated by a period
- Cannot include commas
- Cannot include any of the following printable characters:

  " / \ [ ] : | < > + = ; ? * @
- Cannot include characters in the ASCII range 1-31, which are non-printable

You can optionally specify the following parameters:

- `-full-name` *user_name* specifies the user's full name.
  If the full name contains a space, it must be enclosed within quotation marks.
- `-description` *text* specifies a description for the local user.
  If the description contains a space, it must be enclosed within quotation marks.

- `-is account-disabled {true|false}` specifies if the user account is enabled or disabled. By default, the user account is enabled.

Steps

1. Create the local user by entering the following command:

   vserver cifs users-and-groups local-user create -vserver *vserver_name* user-name *user_name* optional_parameters

   The command prompts for the local user's password.

2. Enter a password for the local user and confirm the password.

   The password must meet the following requirements:

   - Must be at least six characters in length
   - Must not contain the user account name
   - Must contain characters from at least three of the following four categories:

     - English uppercase characters (A through Z)
     - English lowercase characters (a through z)
     - Base 10 digits (0 through 9)
     - Special characters: ~, !, @, #, 0, ^, &, *, _, -, +, =, `, \, |, (,), [,], :, ;, ", ', <, >, ,, ., ?, /

3. Verify that the user has been successfully created:

   vserver cifs users-and-groups local-user show -vserver *vserver_name*

Example

The following example creates a local user "CIFS_SERVER\sue" associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver vs1 -user-name
CIFS_SERVER\sue

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver   User Name                  Full Name  Description
--------  -------------------------  ---------- -------------
vs1       CIFS_SERVER\Administrator             Built-in administrator account
vs1       CIFS_SERVER\sue
```

Modifying local user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

If you want to...	Enter the command...
Modify the local user's full name	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -full-name text` If the full name contains a space, then it must be enclosed within double quotation marks.
Modify the local user's description	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -description text` If the description contains a space, then it must be enclosed within double quotation marks.
Enable or disable the local user account	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled {true|false}`
Rename the local user account	`vserver cifs users-and-groups local-user rename -vserver vserver_name -user-name user_name -new-user-name new_user_name` The new user name must meet the following criteria: • Must not exceed 20 characters • Cannot be terminated by a period • Cannot include commas • Cannot include any of the following printable characters: `" / \ [ ] :	< > + = ; ? * @` • Cannot include characters in the ASCII range 1-31, which are non-printable When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name.

Example

The following example renames the local user "CIFS_SERVER\sue" to "CIFS_SERVER \sue_new" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Enabling or disabling local user accounts

You enable a local user account if you want the user to be able to access data contained in the
Storage Virtual Machine (SVM) over an SMB connection. You can also disable a local user account
if you do not want that user to access SVM data over SMB.

About this task

You enable a local user by modifying the user account.

Step

1. Perform the appropriate action:

If you want to...	Enter the command...
Enable the user account	**vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account-disabled false**
Disable the user account	**vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is-account-disabled true**

Changing local user account passwords

You can change a local user's account password. This can be useful if the user's password is
compromised or if the user has forgotten the password.

Step

1. Change the password by performing the appropriate action:

   **vserver cifs users-and-groups local-user set-password -vserver
   vserver_name -user-name *user_name***

   The password must meet the following criteria:

   - Must be at least six characters in length
   - Must not contain the user account name
   - Must contain characters from at least three of the following four categories:

     - English uppercase characters (A through Z)
     - English lowercase characters (a through z)
     - Base 10 digits (0 through 9)
     - Special characters:

~ ! @ # 0 ^ & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

Example

The following example sets the password for the local user "CIFS_SERVER\sue" associated with Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user-
name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Related tasks

Displaying information about local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user's settings, and also to troubleshoot authentication or file access issues.

About this task

Information about a user's password is never displayed.

Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display information about all users on the Storage Virtual Machine (SVM)	**vserver cifs users-and-groups local-user show -vserver** *vserver_name*
Display detailed account information for a user	**vserver cifs users-and-groups local-user show -instance -vserver** *vserver_name* **-user-name** *user_name*

There are other optional parameters that you can choose when you run the command. See the man page for more information.

Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver   User Name                    Full Name     Description
--------  --------------------------   ------------  -------------
vs1       CIFS_SERVER\Administrator     James Smith   Built-in administrator account
vs1       CIFS_SERVER\sue               Sue   Jones
```

Displaying information about group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

About this task

You can customize the command to display only the information that you want to see.

Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display local user membership information for a specified local user	**vserver cifs users-and-groups local-user show-membership -user-name** *user_name*
Display local user membership information for the local group of which this local user is a member	**vserver cifs users-and-groups local-user show-membership -membership** *group_name*
Display user membership information for local users that are associated with a specified Storage Virtual Machine (SVM)	**vserver cifs users-and-groups local-user show-membership -vserver** *vserver_name*
Display detailed information for all local users on a specified SVM	**vserver cifs users-and-groups local-user show-membership -instance -vserver** *vserver_name*

Example

The following example displays the membership information for all local users on SVM vs1; user "CIFS_SERVER\Administrator" is a member of the "BUILTIN\Administrators" group, and "CIFS_SERVER\sue" is a member of "CIFS_SERVER\g1" group:

```
cluster1::> vserver cifs users-and-groups local-user show-membership -
vserver vs1
Vserver     User Name                    Membership
---------   --------------------------   -----------------------
```

```
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Deleting local user accounts

You can delete local user accounts from your Storage Virtual Machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

About this task

Keep the following in mind when deleting local users:

- The file system is not altered.
  Windows Security Descriptors on files and directories that refer to this user are not adjusted.
- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

Steps

1. Determine the name of the local user account that you want to delete:

   vserver cifs users-and-groups local-user show -vserver *vserver_name*

2. Delete the local user:

   vserver cifs users-and-groups local-user delete -vserver *vserver_name* -user-name *username_name*

3. Verify that the user account is deleted:

   vserver cifs users-and-groups local-user show -vserver *vserver_name*

Example

The following example deletes the local user "CIFS_SERVER\sue" associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver   User Name                   Full Name      Description
--------  --------------------------  -------------  -------------
vs1       CIFS_SERVER\Administrator   James Smith    Built-in administrator account
vs1       CIFS_SERVER\sue             Sue    Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1 -user-name
CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
--------  --------------------------  -------------  -------------
vs1       CIFS_SERVER\Administrator   James Smith    Built-in administrator account
```

Managing local groups

You can manage local groups by creating or modifying groups, displaying information about groups and group membership, and by deleting unneeded groups. You can also perform other management tasks, such as renaming groups and adding or removing both local and domain users from the local groups.

Related concepts

Creating local groups

You can create local groups that can be used for authorizing access to data associated with the Storage Virtual Machine (SVM) over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

Before you begin

The local users and groups functionality is enabled.

About this task

Keep the following in mind when creating local groups:

* You can specify a group name with or without the local domain name.
  The local domain is the CIFS server name on the SVM. For example, if the CIFS server name is "CIFS_SERVER" and you want to create the "engineering" group, you can specify the group name as "engineering" or "CIFS_SERVER\engineering".
  The following rules apply when using a local domain as part of the group name:

  * You can only specify the local domain name for the SVM to which the group is applied.
    For example, if the local CIFS server name is "CIFS_SERVER", you cannot specify the following local group name: "CORP_SERVER\group1".
  * You cannot use the *BUILTIN* term as a local domain in the group name.
    For example, you cannot create a group named "BUILTIN\group1".
* You cannot specify a group name that already exists.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can optionally specify a description for the local group. The group name must meet the following requirements:

* Must not exceed 256 characters
* Cannot be terminated by a period
* Cannot include commas
* Cannot include any of the following printable characters:

" / \ [ ] : | < > + = ; ? * @

- Cannot include characters in the ASCII range 1-31, which are non-printable

Steps

1. Create the local group by entering the following command:

   vserver cifs users-and-groups local-group create -vserver *vserver_name* -group-name *group_name*

2. Verify that the group is successfully created:

   vserver cifs users-and-groups local-group show -vserver *vserver_name*

Example

The following example creates a local group "CIFS_SERVER\engineering" associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver vs1 -group-name
CIFS_SERVER\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver         Group Name                    Description
-------------- --------------------------- ----------------------------
vs1            BUILTIN\Administrators       Built-in Administrators group
vs1            BUILTIN\Backup Operators     Backup Operators group
vs1            BUILTIN\Power Users          Restricted administrative privileges
vs1            BUILTIN\Users                All users
vs1            CIFS_SERVER\engineering
vs1            CIFS_SERVER\sales
```

Modifying local groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

If you want to...	Use the command...
Modify the local group description	**vserver cifs users-and-groups local-group modify -vserver *vserver_name* -group-name *group_name* -description *text*** If the description contains a space, then it must be enclosed within double quotation marks.

If you want to...	Use the command...

Rename the local group	`vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`
	
	The new group name must meet the following criteria:
	
	• Must not exceed 256 characters
	• Cannot be terminated by a period
	• Cannot include commas
	• Cannot include any of the following printable characters:
	
	    `" / \ [ ] : | < > + = ; ? * @`
	• Cannot include characters in the ASCII range 1-31, which are non-printable

Examples

The following example renames the local group "CIFS_SERVER\engineering" to "CIFS_SERVER\engineering_new":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1 -
group-name CIFS_SERVER\engineering -new-group-name CIFS_SERVER
\engineering_new
```

The following example modifies the description of the local group "CIFS_SERVER\engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1 -
group-name CIFS_SERVER\engineering -description "New Description"
```

Displaying information about local groups

You can display a list of all local groups configured on the cluster or on a specified Storage Virtual Machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

Step

1. Perform one of the following actions:

If you want information about...	Enter the command...
All local groups on the cluster	`vserver cifs users-and-groups local-group show`

If you want information about...	Enter the command...
All local groups on the SVM	`vserver cifs users-and-groups local-group show -vserver vserver_name`

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following example displays information about all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                 Description
--------  -------------------------  ---------------------------
vs1       BUILTIN\Administrators     Built-in Administrators group
vs1       BUILTIN\Backup Operators   Backup Operators group
vs1       BUILTIN\Power Users        Restricted administrative privileges
vs1       BUILTIN\Users              All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales
```

Managing local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

- You cannot add users to the special *Everyone* group.
- The local group must exist before you can add a user to it.
- The user must exist before you can add the user to a local group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- The group from which you want to remove a member must exist.
- Data ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

If you want to...	Use the command...
Add a member to a group	`vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.
Remove a member from a group	`vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

Examples

The following example adds a local user "CIFS_SERVER\sue" and a domain group "AD_DOM\dom_eng" to the local group "CIFS_SERVER\engineering" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1 -group-name CIFS_SERVER\engineering -member-names CIFS_SERVER
\sue,AD_DOMAIN\dom_eng
```

The following example removes the local users "CIFS_SERVER\sue" and "CIFS_SERVER\james" from the local group "CIFS_SERVER\engineering" on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members -
vserver vs1 -group-name CIFS_SERVER\engineering -member-names CIFS_SERVER
\sue,CIFS_SERVER\james
```

Related tasks

Displaying information about members of local groups on page 178

Displaying information about members of local groups

You can display a list of all members of local groups configured on the cluster or on a specified Storage Virtual Machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

Step

1. Perform one of the following actions:

If you want to display information about...	Enter the command...
Members of all local groups on the cluster	`vserver cifs users-and-groups local-group show-members`
Members of all local groups on the SVM	`vserver cifs users-and-groups local-group show-members -vserver vserver_name`

Example

The following example displays information about members of all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members -vserver
vs1
Vserver    Group Name                      Members
---------  ------------------------------  ------------------------
vs1        BUILTIN\Administrators          CIFS_SERVER\Administrator
                                           AD_DOMAIN\Domain Admins
                                           AD_DOMAIN\dom_grp1
           BUILTIN\Users                   AD_DOMAIN\Domain Users
                                           AD_DOMAIN\dom_usr1
           CIFS_SERVER\engineering         CIFS_SERVER\james
```

Deleting a local group

You can delete a local group from the Storage Virtual Machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

About this task

Keep the following in mind when deleting local groups:

- The file system is not altered.
  Windows Security Descriptors on files and directories that refer to this group are not adjusted.
- If the group does not exist, an error is returned.
- The special *Everyone* group cannot be deleted.
- Built-in groups such as *BUILTIN|Administrators BUILTIN|Users* cannot be deleted.

Steps

1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM:

   `vserver cifs users-and-groups local-group show -vserver vserver_name`

2. Delete the local group:

   `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`

3. Verify that the group is deleted:

   vserver cifs users-and-groups local-user show -vserver *vserver_name*

   Example

   The following example deletes the local group "CIFS_SERVER\sales" associated with SVM vs1:

   ```
   cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
   Vserver    Group Name                    Description
   ---------  ----------------------------  --------------------------
   vs1        BUILTIN\Administrators         Built-in Administrators group
   vs1        BUILTIN\Backup Operators       Backup Operators group
   vs1        BUILTIN\Power Users            Restricted administrative privileges
   vs1        BUILTIN\Users                  All users
   vs1        CIFS_SERVER\engineering
   vs1        CIFS_SERVER\sales

   cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1 -group-name
   CIFS_SERVER\sales

   cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
   Vserver    Group Name                    Description
   ---------  ----------------------------  --------------------------
   vs1        BUILTIN\Administrators         Built-in Administrators group
   vs1        BUILTIN\Backup Operators       Backup Operators group
   vs1        BUILTIN\Power Users            Restricted administrative privileges
   vs1        BUILTIN\Users                  All users
   vs1        CIFS_SERVER\engineering
   ```

Updating domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

About this task

You must specify the name of the Storage Virtual Machine (SVM) on which you want to update domain names.

Steps

1. Set the privilege level to advanced:

   set -privilege advanced

2. Perform the appropriate action:

If you want to update domain users and groups and...	Use this command...
Display domain users and groups that successfully updated and that failed to update	**vserver cifs users-and-groups update-names -vserver *vserver_name***

If you want to update domain users and groups and...	Use this command...
Display domain users and groups that successfully updated	`vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only false`
Display only the domain users and groups that fail to update	`vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only true`
Suppress all status information about updates	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress-all-output true`

3. Return to the admin privilege level:

`set -privilege admin`

Example

The following example updates the names of domain users and groups associated with Storage Virtual Machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

    Vserver:          vs1
    SID:              S-1-5-21-123456789-234565432-987654321-12345
    Domain:           EXAMPLE1
    Out-of-date Name: dom_user1
    Updated Name:     dom_user2
    Status:           Successfully updated

    Vserver:          vs1
    SID:              S-1-5-21-123456789-234565432-987654322-23456
    Domain:           EXAMPLE2
    Out-of-date Name: dom_user1
    Updated Name:     dom_user2
    Status:           Successfully updated

    Vserver:          vs1
    SID:              S-1-5-21-123456789-234565432-987654321-123456
    Domain:           EXAMPLE1
    Out-of-date Name: dom_user3
    Updated Name:     dom_user4
    Status:           Successfully updated; also updated SID
"S-1-5-21-123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID
"S-1-5-21-123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID
```

```
"S-1-5-21-123456789-234565432-987654321-123460"
                   to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

Managing local privileges

You can manage local privileges by adding, removing, or resetting privileges for local and domain user accounts and groups. You can also display information about privileges assigned to local and domain user accounts and groups.

Related concepts

Related references

Adding privileges to local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

Before you begin

The local or domain user or group to which privileges will be added must already exist.

About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller.
  The command might fail if Data ONTAP is unable to contact the domain controller.

Steps

1. Add one or more privileges to a local or domain user or group:

vserver cifs users-and-groups privilege add-privilege -vserver
_vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]

The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

`-privileges` _privilege_[,...] is a comma-delimited list of one or more privileges.

2. Verify that the desired privileges are applied to the object:

vserver cifs users-and-groups privilege show -vserver _vserver_name_ -user-
or-group-name _name_

Example

The following example adds the privileges "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" to the user "CIFS_SERVER\sue" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
---------  --------------------  --------------
vs1        CIFS_SERVER\sue       SeTcbPrivilege
                                 SeTakeOwnershipPrivilege
```

Removing privileges from local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges that users and groups have.

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, Data ONTAP might validate the domain user or group by contacting the domain controller.
  The command might fail if Data ONTAP is unable to contact the domain controller.

Steps

1. Remove one or more privileges from a local or domain user or group:

   `vserver cifs users-and-groups privilege remove-privilege -vserver`
   `vserver_name -user-or-group-name name -privileges privilege[,...]`

   The value for the `-user-or-group-name` parameter is a local user or group or a domain user or group.

   `-privileges privilege`[,...] is a comma-delimited list of one or more privileges.

2. Verify that the desired privileges have been removed from the object:

   `vserver cifs users-and-groups privilege show -vserver vserver_name -user-`
   `or-group-name name`

Example

The following example removes the privileges "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" from the user "CIFS_SERVER\sue" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
---------  --------------------  --------------
vs1        CIFS_SERVER\sue       SeTcbPrivilege
                                 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege -
vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
---------  --------------------  -------------------
vs1        CIFS_SERVER\sue       -
```

Resetting privileges for local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

Steps

1. Reset the privileges on a local or domain user or group:

> **vserver cifs users-and-groups privilege reset-privilege -vserver**
> ***vserver_name* -user-or-group-name *name***

The value for the `-user-or-group-name` parameter is a local or domain user or group.

2. Verify that the privileges are reset on the object:

> **vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-**
> **or-group-name *name***

Examples

The following example resets the privileges on the user "CIFS_SERVER\sue" on Storage
Virtual Machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have
privileges associated with their accounts:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name     Privileges
---------  --------------------   --------------
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                  SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege -
vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group "BUILTIN\Administrators",
effectively removing the privilege entry:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name       Privileges
---------  -----------------------  -------------------
vs1        BUILTIN\Administrators    SeRestorePrivilege
                                     SeSecurityPrivilege
                                     SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege -
vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Displaying information about privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or
groups. This information helps you determine whether the desired user rights are applied.

Step

1. Perform one of the following actions:

If you want to display information about...	Enter this command...
Custom privileges for all domain and local users and groups on the Storage Virtual Machine (SVM)	**vserver cifs users-and-groups privilege show -vserver vserver_name**
Custom privileges for a specific domain or local user and group on the SVM	**vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name**

There are other optional parameters that you can choose when you run this command. See the man page for more information.

Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------  --------------
vs1       BUILTIN\Administrators SeTakeOwnershipPrivilege
                                 SeRestorePrivilege
vs1       CIFS_SERVER\sue        SeTcbPrivilege
                                 SeTakeOwnershipPrivilege
```

Displaying information about file security and audit policy on FlexVol volumes

You can display information about file security on files and directories on FlexVol volumes. You can also display information about applied audit policies.

You can display information about file security and audit polices applied to data contained within volumes and qtrees with the following security styles:

- NTFS
- UNIX
- Mixed

You can display information about audit policies for auditing access events over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

Related concepts

How security styles affect data access on page 19

Managing NTFS file security and audit policies on SVMs with FlexVol volumes using the CLI on page 203

Related tasks

Performing security traces on page 236

Displaying information about file security on NTFS security-style FlexVol volumes

You can display information about file and directory security on NTFS security-style FlexVol volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the data and the path to the data whose file or directory security information you want to display. If you want to customize the output, you can use the following optional parameters to display information only about file and directory security settings that match the specified parameters:

Optional parameter	Description
`-fields` `fieldsname`,...	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about all entries.
`-volume-name` `volume_name`	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
`-share-name` `share_name`	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.
`-lookup-names` `{true|false}`	- If set to `true`, the command displays information about file and directory security for files and directories where the information about owner and group are stored as names. - If set to `false`, the command displays information about file and directory security for files and directories where the information for owner and group are stored as SIDs.

Optional parameter	Description
`-expand-mask {true|false}`	• If set to `true`, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are store in expanded form. • If set to `false`, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are store in collapsed form. **Note:** By default, if the value of `-expand-mask` is set to `false`, the value displayed for the `Expanded Dos Attributes` output field is "-". You must set the value of this option to `true` if you want to display the expanded DOS attributes.
`-security-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the associated security type of the volume or qtree.
`-effective-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with the specified effective security style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS-effective or UNIX-effective security (but not both).
`-dos-attributes hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos-attr text`	Displays information only for files and directories with the specified extended DOS attributes.
`-user-id unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.

Optional parameter	Description
`-mode-bits` *`octal_permissions`*	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits` *`text`*	Displays information only for files and directories with the specified UNIX mode bits in text form.
`-acls` *`security_acls`*	Displays information only for files and directories with the specified ACLs. You can enter the following information: • Type of ACL, which can be NTFS or NFSv4 For NTFS security-style volumes and qtrees, the ACL type must be NTFS. • Control bits in the security descriptors • Owner, which applies only in the case of NTFS security descriptors • Group, which applies only in the case of NTFS security descriptors • Access Control Entries (ACEs), which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL

Note: UNIX-related output fields contain display-only UNIX file permission information. NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights.

Step

1. Display file and directory security settings:

   vserver security file-directory show -vserver *vserver_name* **-path** *path* *optional_parameters*

Examples

The following example displays the security information about the path `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                          Vserver: vs1
                        File Path: /vol4
                   Security Style: ntfs
                  Effective Style: ntfs
                   DOS Attributes: 10
          DOS Attributes in Text: ----D---
         Expanded Dos Attributes: -
                     Unix User Id: 0
                    Unix Group Id: 0
                   Unix Mode Bits: 777
          Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0x8004
                                   Owner:BUILTIN\Administrators
                                   Group:BUILTIN\Administrators
                                   DACL - ACEs
```

```
                                        ALLOW-Everyone-0x1f01ff
                                        ALLOW-Everyone-0x10000000-OI|CI|IO
```

The following example displays the security information with expanded masks about the
path /data/engineering in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path /data/
engineering -expand-mask true

                 Vserver: vs1
               File Path: /data/engineering
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
      ...0 .... .... .... = Offline
      .... ..0. .... .... = Sparse
      .... .... 0... .... = Normal
      .... .... ..0. .... = Archive
      .... .... ...1 .... = Directory
      .... .... .... .0.. = System
      .... .... .... ..0. = Hidden
      .... .... .... ...0 = Read Only
            Unix User Id: 0
           Unix Group Id: 0
           Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0x8004

                              1... .... .... .... = Self Relative
                              .0.. .... .... .... = RM Control Valid
                              ..0. .... .... .... = SACL Protected
                              ...0 .... .... .... = DACL Protected
                              .... 0... .... .... = SACL Inherited
                              .... .0.. .... .... = DACL Inherited
                              .... ..0. .... .... = SACL Inherit Required
                              .... ...0 .... .... = DACL Inherit Required
                              .... .... ..0. .... = SACL Defaulted
                              .... .... ...0 .... = SACL Present
                              .... .... .... 0... = DACL Defaulted
                              .... .... .... .1.. = DACL Present
                              .... .... .... ..0. = Group Defaulted
                              .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... = Generic Read
                              .0.. .... .... .... .... .... .... .... = Generic Write
                              ..0. .... .... .... .... .... .... .... = Generic Execute
                              ...0 .... .... .... .... .... .... .... = Generic All
                              .... ...0 .... .... .... .... .... .... = System Security
                              .... .... ...1 .... .... .... .... .... = Synchronize
                              .... .... .... 1... .... .... .... .... = Write Owner
                              .... .... .... .1.. .... .... .... .... = Write DAC
                              .... .... .... ..1. .... .... .... .... = Read Control
                              .... .... .... ...1 .... .... .... .... = Delete
                              .... .... .... .... ...1 .... .... .... = Write Attributes
                              .... .... .... .... .... 1... .... .... = Read Attributes
                              .... .... .... .... .... .1.. .... .... = Delete Child
                              .... .... .... .... .... ..1. .... .... = Execute
                              .... .... .... .... .... ...1 .... .... = Write EA
                              .... .... .... .... .... .... 1... .... = Read EA
                              .... .... .... .... .... .... .1.. .... = Append
                              .... .... .... .... .... .... ..1. .... = Write
                              .... .... .... .... .... .... ...1 .... = Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
```

```
                                  0... .... .... .... .... .... .... .... = Generic Read
                                  .0.. .... .... .... .... .... .... .... = Generic Write
                                  ..0. .... .... .... .... .... .... .... = Generic Execute
                                  ...1 .... .... .... .... .... .... .... = Generic All
                                  .... ...0 .... .... .... .... .... .... = System Security
                                  .... .... ...0 .... .... .... .... .... = Synchronize
                                  .... .... .... 0... .... .... .... .... = Write Owner
                                  .... .... .... .0.. .... .... .... .... = Write DAC
                                  .... .... .... ..0. .... .... .... .... = Read Control
                                  .... .... .... ...0 .... .... .... .... = Delete
                                  .... .... .... .... .... ...0 .... .... = Write Attributes
                                  .... .... .... .... .... .... 0... .... = Read Attributes
                                  .... .... .... .... .... .... .0.. .... = Delete Child
                                  .... .... .... .... .... .... ..0. .... = Execute
                                  .... .... .... .... .... .... ...0 .... = Write EA
                                  .... .... .... .... .... .... .... 0... = Read EA
                                  .... .... .... .... .... .... .... .0.. = Append
                                  .... .... .... .... .... .... .... ..0. = Write
                                  .... .... .... .... .... .... .... ...0 = Read
```

Displaying information about file security on mixed security-style FlexVol volumes

You can display information about file and directory security on mixed security-style FlexVol volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the data and the path to the data whose file or directory security information you want to display. If you want to customize the output, you can use the following optional parameters to display information only about file and directory security settings that match the specified parameters:

Optional parameter	Description
-fields fieldsname, ...	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
-instance	Displays detailed information about all entries.
-volume-name volume_name	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
-share-name share_name	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.

Optional parameter	Description
`-lookup-names {true|false}`	If set to `true`, the command displays information about file and directory security for files and directories where the information about owner and group are stored as names. If set to `false`, the command displays information about file and directory security for files and directories where the information for owner and group are stored as SIDs.
`-expand-mask {true|false}`	- If set to `true`, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are store in expanded form. - If set to `false`, the command displays information about file and directory security for files and directories where the hexadecimal bit mask entries are store in collapsed form. **Note:** By default, if the value of `-expand-mask` is set to `false`, the value displayed for the `Expanded Dos Attributes` output field is "-". You must set the value of this option to `true` if you want to display the expanded DOS attributes.
`-security-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the associated security type of the volume or qtree.
`-effective-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with the specified effective security-style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS or UNIX effective security (but not both).
`-dos-attributes hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos-attr text`	Displays information only for files and directories with the specified extended DOS attributes.

Optional parameter	Description
`-user-id` `unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id` `unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.
`-mode-bits` `octal_permissions`	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits` `text`	Displays information only for files and directories with the specified UNIX mode bits in text form.
`-acls` `security_acls`	Displays information only for files and directories with the specified ACLs. You can enter the following information: • Type of ACL, which can be NTFS or NFSv4 For NTFS security-style volumes and qtrees, the ACL type must be NTFS. • Control bits in the security descriptors • Owner, which applies only in the case of NTFS security descriptors • Group, which applies only in the case of NTFS security descriptors • Access Control Entries (ACEs), which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL **Note:** This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

Note: Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

Step

1. Display file and directory security settings:

   ```
   vserver security file-directory show -vserver vserver_name -path path
   optional_parameters
   ```

   > **Examples**
   >
   > The following example displays the security information about the path /projects in SVM vs1 in expanded-mask form. This mixed security-style path has a UNIX-effective security style:
   >
   > ```
   > cluster1::> vserver security file-directory show -vserver vs1 -path /projects -expand-
   > mask true
   > ```

```
                       Vserver: vs1
                     File Path: /projects
                Security Style: mixed
               Effective Style: unix
                DOS Attributes: 10
        DOS Attributes in Text: ----D---
      Expanded Dos Attributes: 0x10
            ...0 .... .... .... = Offline
            .... ..0. .... .... = Sparse
            .... .... 0... .... = Normal
            .... .... ..0. .... = Archive
            .... .... ...1 .... = Directory
            .... .... .... .0.. = System
            .... .... .... ..0. = Hidden
            .... .... .... ...0 = Read Only
                   Unix User Id: 0
                  Unix Group Id: 1
                 Unix Mode Bits: 700
        Unix Mode Bits in Text: rwx------
                          ACLs: -
```

The following example displays the security information about the path `/data` in SVM vs1.
This mixed security-style path has an NTFS-effective security style:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /
data

                              Vserver: vs1
                            File Path: /data
                       Security Style: mixed
                      Effective Style: ntfs
                       DOS Attributes: 10
               DOS Attributes in Text: ----D---
              Expanded Dos Attributes: -
                         Unix User Id: 0
                        Unix Group Id: 0
                       Unix Mode Bits: 777
              Unix Mode Bits in Text: rwxrwxrwx
                                 ACLs: NTFS Security Descriptor
                                       Control:0x8004
                                       Owner:BUILTIN\Administrators
                                       Group:BUILTIN\Administrators
                                       DACL - ACEs
                                         ALLOW-Everyone-0x1f01ff
                                         ALLOW-Everyone-0x10000000-OI|CI|IO
```

Displaying information about file security on UNIX security-style FlexVol volumes

You can display information about file and directory security on UNIX security-style FlexVol
volumes, including what the security styles and effective security styles are, what permissions are
applied, and information about UNIX owners and groups. You can use the results to validate your
security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the data and the path
to the data whose file or directory security information you want to display. If you want to customize

the output, you can use the following optional parameters to display information only about file and directory security that matches the specified parameters:

Optional parameter	Description
-fields *fieldsname*, ...	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
-instance	Displays detailed information about all entries.
-volume-name *volume_name*	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
-share-name *share_name*	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.
-lookup-names {true|false}	Although you can specify a value for the -lookup-names parameter, this parameter does not apply for UNIX security-style volumes. In NFSv4 ACLs, ACE's are displayed in SID format; therefore, lookup name are not stored as a name. The name is stored as SID and that is what is returned even if this value is set to true.
-expand-mask {true|false}	Displays information where the hexadecimal bit mask entry is set to one of the following: • true displays information where the bit mask entries are store in expanded form. • false displays information where the bit mask entries are store in collapsed form.
-security-style {unix|ntfs|mixed|unified}	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the unified value is not valid for this release. This is the associated security type of the volume or qtree.
-effective-style {unix|ntfs|mixed|unified}	Displays information for files and directories with the specified effective security style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the unified value is not valid for this release. This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS or UNIX effective security (but not both).

Optional parameter	Description
`-dos-attributes` `hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr` `text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos-attr` `text`	Displays information only for files and directories with the specified extended DOS attributes.
`-user-id` `unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id` `unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.
`-mode-bits` `octal_permissions`	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits` `text`	Displays information only for files and directories with the specified UNIX mode bits in text form.
`-acls` `system_acls`	Displays information only for files and directories with the specified ACLs. You can enter the following information: • Type of ACL, which can be NTFS or NFSv4 For UNIX security-style volumes and qtrees, the ACL type must be NFSv4. • Control bits in the security descriptors • Owner, which applies only in the case of NTFS security descriptors This does not apply for UNIX security-style volumes and qtrees. • Group, which applies only in the case of NTFS security descriptors This does not apply for UNIX security-style volumes and qtrees. • Access Control Entries (ACEs), which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL **Note:** This field is empty for UNIX-security style files and directories that have only mode bit permissions applied (no NFSv4 ACLs).

Note: UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.

Step

1. Display file and directory security settings:

```
vserver security file-directory show -vserver vserver_name -path path
optional_parameters
```

Examples

The following example displays the security information about the path /home in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                          Vserver: vs1
                        File Path: /home
                   Security Style: unix
                  Effective Style: unix
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 700
           Unix Mode Bits in Text: rwx------
                             ACLs: -
```

The following example displays the security information about the path /home in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home -expand-mask
true

                              Vserver: vs1
                            File Path: /home
                       Security Style: unix
                      Effective Style: unix
                       DOS Attributes: 10
               DOS Attributes in Text: ----D---
              Expanded Dos Attributes: 0x10
                  ...0 .... .... .... = Offline
                  .... ..0. .... .... = Sparse
                  .... .... 0... .... = Normal
                  .... .... ..0. .... = Archive
                  .... .... ...1 .... = Directory
                  .... .... .... .0.. = System
                  .... .... .... ..0. = Hidden
                  .... .... .... ...0 = Read Only
                         Unix User Id: 0
                        Unix Group Id: 1
                       Unix Mode Bits: 700
               Unix Mode Bits in Text: rwx------
                                 ACLs: -
```

Displaying information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective-security styles are, what permissions are applied, and information about

system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the path to the files or directories whose audit information you want to display. If you want to customize the output, you can use the following optional parameters to display information only about file and directory security that matches the specified parameters:

Optional parameter	Description
`-fields` `fieldsname, ...`	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about all entries.
`-volume-name` `volume_name`	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
`-share-name` `share_name`	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.
`-lookup-names` `{true|false}`	Displays information where the information about owner and group is set to one of the following: • `true` displays information where the lookup name is stored as a name. • `false` displays information where the lookup name is stored as a SID.
`-expand-mask` `{true|false}`	Displays information where the hexadecimal bit mask entry is set to one of the following: • `true` displays information where the bit mask entries are store in expanded form. • `false` displays information where the bit mask entries are store in collapsed form.
`-security-style` `{unix|ntfs|mixed|` `unified}`	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the associated security type of the volume or qtree.

Optional parameter	Description
`-effective-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with the specified effective security style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release.
	This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS-effective or UNIX-effective security (but not both).
`-dos-attributes hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos- attr text`	Displays information only for files and directories with the specified extended DOS attributes.
`-user-id unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.
`-mode-bits octal_permissions`	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits text`	Displays information only for files and directories with the specified UNIX mode bits in text form.
`-acls system_acls`	Displays information only for files and directories with the specified ACLs. You can enter the following information: • Type of ACL, which can be NTFS or NFSv4 • Control bits in the security descriptors • Owner, which applies only in the case of NTFS security descriptors. • Group, which applies only in the case of NTFS security descriptors. • Access Control Entries (ACEs) which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL.

Note: NTFS security-style volumes and qtrees use only NTFS system access control lists for audit policies. Mixed security-style volumes and qtrees can contain some files and directories that are of NTFS security style, which can have NTFS audit policies applied to them.

Step

1. Display audit policy settings:

    vserver security file-directory show -vserver *vserver_name* -path *path* *optional_parameters*

    Example

    The following example displays the audit policy information about the path /corp in SVM vs1. This NTFS-security-style path has a NTFS-effective security style. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry:

    vserver security file-directory show -vserver vs1 -path /corp

    ```
            Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
    ```

Displaying information about NFSv4 audit policies on FlexVol volumes using the CLI

You can display information about NFSv4 audit policies on FlexVol volumes using the Data ONTAP CLI, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the path to the files or directories whose audit information you want to display. If you want to customize the output, you can use the following optional parameters to display information only about the audit policies that match the specified parameters:

Optional parameter	Description
`-fields` *fieldsname*, ...	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about all entries.
`-volume-name` *volume_name*	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
`-share-name` *share_name*	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.
`-lookup-names` {true|false}	Displays information where the information about owner and group is set to one of the following: • `true` displays information where the lookup name is stored as a name. • `false` displays information where the lookup name is stored as a SID.
`-expand-mask` {true|false}	Displays information where the hexadecimal bit mask entry is set to one of the following: • `true` displays information where the bit mask entries are store in expanded form. • `false` displays information where the bit mask entries are store in collapsed form.
`-security-style` {unix|ntfs|mixed| unified}	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the associated security type of the volume or qtree.
`-effective-style` {unix|ntfs|mixed| unified}	Displays information for files and directories with the specified effective security style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS or UNIX effective security (but not both). You can apply NFSv4 system access control lists to files and directories with UNIX-effective security style.

Optional parameter	Description
`-dos-attributes` `hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr` `text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos-attr` `text`	Displays information only for files and directories with the specified extended DOS attributes.
`-user-id` `unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id` `unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.
`-mode-bits` `octal_permissions`	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits` `text`	Displays information only for files and directories with the specified UNIX mode bits in text form.

`-acls` `system_acls`	Displays information only for files and directories with the specified ACLs. You can enter the following information:
	
	• Type of ACL, which can be NTFS or NFSv4
	  For UNIX security-style volumes and qtrees, the ACL type must be NFSv4.
	• Control bits in the security descriptors
	• Owner, which applies only in the case of NTFS security descriptors
	  This does not apply for UNIX security-style volumes and qtrees.
	• Group, which applies only in the case of NTFS security descriptors
	  This does not apply for UNIX security-style volumes and qtrees.
	• Access Control Entries (ACEs), which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL
	
	Note: This field is empty for files and directories that are using UNIX security with only mode bit permissions applied (no NFSv4 ACLs).

Note: Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, as well as some files and directories that use NTFS file permissions. Each file or directory can be one of the two security styles, but not both. You can apply NFSv4 audit policies to file and directories with UNIX security style.

Step

1. Display file and directory security settings:

    vserver security file-directory show -vserver *vserver_name* -path *path optional_parameters*

Examples

The following example displays the security information about the path /lab in SVM vs1. This UNIX security-style path has an NFSv4 ACL with a system access control list:

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Managing NTFS file security and audit policies on SVMs with FlexVol volumes using the CLI

You can manage NTFS file security and audit policies on Storage Virtual Machines (SVMs) with FlexVol volumes by using the CLI. This removes the need to use a remote client to manage file security. Using the CLI can significantly reduce the time it takes to apply security on many files and folders using a single command.

You can use the vserver security file-directory command family to implement file security and audit policies on files and folders that have NTFS effective security:

*   All files and folders contained within NTFS security-style volumes and qtrees have NTFS effective security.
*   Mixed security-style volumes and qtrees can contain some files and folders that have UNIX effective security and use UNIX file permissions, either mode bits or NFSv4 ACLs and NFSv4 audit policies, and some files and folders that have NTFS effective security and use NTFS file permissions and audit policies.

    You can use the CLI to apply file permissions and audit policies to files and folders of NTFS and UNIX effective security-style in the mixed volume or qtree.

> **Note:** All files and folders contained within UNIX security-style volumes and qtrees have UNIX effective security. The CLI cannot be used to manage UNIX file security and audit policies on UNIX security-style volumes and qtrees.

Related concepts

Related tasks

Use cases for using the CLI to set file and folder security

Because you can apply and manage file and folder security locally without involvement from a remote client, you can significantly reduce the time it takes to set bulk security on a large number of files or folders.

You can benefit from using the CLI to set file and folder security in the following use cases:

- Storage of files in large enterprise environments, such as file storage in home directories
- Migration of data
- Change of Windows domain
- Standardization of file security and audit policies across NTFS file systems

Limits when using the CLI to set file and folder security

You need to be aware of certain limits when using the CLI to set file and folder security.

- The `vserver security file-directory` command family does not support setting NFSv4 ACLs.
  You can only apply NTFS security descriptors to NTFS files and folders.
- The `vserver security file-directory` command family does not support setting file security (NTFS or NFSv4) on Storage Virtual Machines (SVMs) with Infinite Volume.

How security descriptors are used to apply file and folder security

Security descriptors contain the access control lists that determine what actions a user can perform on files and folders, and what is audited when a user accesses files and folders.

Permissions	Permissions are allowed or denied by an object's owner and determine what actions an object (users, groups, or computer objects) can perform on specified files or folders.
Security descriptors	Security descriptors are data structures that contain security information that define permissions associated with a file or folder.

Access control lists (ACLs)	Access control lists are the lists contained within a security descriptor that contain information on what actions users, groups, or computer objects can perform on the file or folder to which the security descriptor is applied. The security descriptor can contain the following two types of ACLs: • Discretionary access control lists (DACLs) • System access control lists (SACLs)
Discretionary access control lists (DACLs)	DACLs contain the list of SIDS for the users, groups, and computer objects who are allowed or denied access to perform actions on files or folders. DACLs contain zero or more access control entries (ACEs).
System access control lists (SACLs)	SACLs contain the list of SIDS for the users, groups, and computer objects for which successful or failed auditing events are logged. SACLs contain zero or more access control entries (ACEs).
Access Control Entries (ACEs)	ACEs are individual entries in either DACLs or SACLs: • A DACL access control entry specifies the access rights that are allowed or denied for particular users, groups, or computer objects. • A SACL access control entry specifies the success or failure events to log when auditing specified actions performed by particular users, groups, or computer objects.
Permission inheritance	Permission inheritance describes how permissions defined in security descriptors are propagated to an object from a parent object. Only inheritable permissions are inherited by child objects. When setting permissions on the parent object, you can decide whether folders, sub-folders, and files can inherit them with "Apply to `this-folder`, `sub-folders`, and `files`".

Related tasks

Configuring and applying file security on NTFS files and folders using the CLI

There are several steps you must perform to apply NTFS file security when using the Data ONTAP CLI. First, you create an NTFS security descriptor and add DACLs to the security descriptor. Next

you create a security policy and add policy tasks. You then apply the security policy to a Storage Virtual Machine (SVM) with FlexVol volumes.

About this task

After applying the security policy, you can monitor the security policy job and then verify the settings on the applied file security.

Steps

1. Creating an NTFS security descriptor on page 207
   Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machine (SVM, formerly known as Vserver) with FlexVol volumes. Later, you will associate the security descriptor to the file or folder path in a policy task.

2. Adding NTFS DACL access control entries to the NTFS security descriptor on page 209
   Adding DACL access control entries to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

3. Creating a security policy on page 212
   Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

4. Adding a task to the security policy on page 213
   Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

5. Applying security policies on page 216
   Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

6. Monitoring the security policy job on page 216
   When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

7. Verifying the applied file security on page 217
   You can verify the file security settings to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired settings.

Related concepts

Limits when using the CLI to set file and folder security on page 204
How security descriptors are used to apply file and folder security on page 204
Configuring audit policies on NTFS security-style files and directories on page 417

Related tasks

Configuring standard NTFS file permissions by using the Windows Security tab on page 141
Configuring advanced NTFS file permissions using the Windows Security tab on page 143
Displaying information about file security on NTFS security-style FlexVol volumes on page 187
Displaying information about file security on mixed security-style FlexVol volumes on page 191
Displaying information about file security on UNIX security-style FlexVol volumes on page 194

Creating an NTFS security descriptor

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machine (SVM, formerly known as Vserver) with FlexVol volumes. Later, you will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed-security-style volumes.

By default, when a security descriptor is created, four discretionary access control list ACEs are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY \SYSTEM	Allow	Full Control	this-folder, sub-folders, files

When creating the security descriptor, you must specify the following two parameters:

Required parameters	Description
`-vserver vserver_name`	*SVM name* The name of the SVM that contains the files and folders to which you want to apply the security descriptor.

Required parameters	Description
`-ntfs-sd SD_name`	*Security descriptor* The name to assign to the security descriptor.

You can customize the security descriptor configuration by using the following optional parameters:

Optional parameter	Description
`-owner name_or_SID`	*Owner of the security descriptor* The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\user-name • user-name@DOMAIN • user-name@FQDN If you specify any of the three name formats for the value of `-owner`, keep in mind that the value is case insensitive.
`-group name_or_SID`	*Primary Group of the Owner* Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\group-name • group-name@DOMAIN • group-name@FQDN If you specify any of the three name formats for the value of `-group`, keep in mind that the value is case insensitive. **Note:** Before you can use this parameter, you must change to advanced privilege level by using the `set privilege` command.
`-control-flags-raw Hex_integer`	*Raw control flags* Specifies the control flags in the security descriptor. Available in advanced mode only. **Note:** Before you can use this parameter, you must change to advanced privilege level by using the following command: **set -privilege advanced**

Steps

1. If you want to use advanced parameters, set the privilege level to advanced:

   `set -privilege advanced`

2. Create a security descriptor:

   `vserver security file-directory ntfs create -vserver` *`vserver_name`* `-ntfs-sd` *`SD_name`* *`optional_parameters`*

   Example

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner domain\joe`

3. Verify that security descriptor configuration is correct:

   `vserver security file-directory ntfs show -vserver` *`vserver_name`* `-ntfs-sd` *`SD_name`*

   Example

   `vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1`

   ```
                               Vserver: vs1
                Security Descriptor Name: sd1
         Owner of the Security Descriptor: DOMAIN\joe
   ```

4. If you are in advanced privilege level, return to the admin privilege level:

   `set -privilege admin`

Adding NTFS DACL access control entries to the NTFS security descriptor

Adding DACL access control entries to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

About this task

You can add one or more ACEs (access control entries) to the security descriptor's DACL (discretionary access control list).

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

When adding an ACE to the DACL, you must provide information for the following four required parameters:

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* The name of the Storage Virtual Machine (SVM, formerly known as Vserver) that contains the files and folders to which the security descriptor is applied.
`-ntfs-sd SD_name`	*Security descriptor* The name of the security descriptor to which you want to add DACL entries.
`-access-type` `{deny|allow}`	*Access type* Specifies whether the discretionary access control entry is an *Allow* or *Deny* type of access control.
`-account` `name_or_SID`	*Account* The account to which you want to apply the discretionary access control entry. You can specify the account by using a user name or SID. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\user-name • user-name@DOMAIN • user-name@FQDN If you specify any of the three name formats for the value of `-account`, keep in mind that the value is not case-sensitive.

You can optionally customize DACL entries by specifying what rights you want to allow or deny for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

• Rights
• Advanced rights
• Raw rights (advanced-privilege)

Optional rights parameters	Description

`-rights {no-`
`access|full-`
`control|modify|`
`read-and-execute|`
`read|write}`
	Rights
	You can choose only one of the parameter values.

Optional rights parameters	Description
`-advanced-rights` `advanced_access_right`	*Advanced rights* You can specify one or more of the following advanced-right values by using a comma-delimited list: • read-data • write-data • append-data • read-ea • write-ea • execute-file • delete-child • read-attr • write-attr • delete • read-perm • write-perm • write-owner • full control
`-raw-rights` `Hex_integer`	*Raw rights* You can specify raw rights as a Hex integer. Available in advanced mode only. **Note:** This is an advanced privilege level parameter. Before you can use this parameter, you must change to advanced-privilege level by using the following command: `set -privilege advanced`

Note: If you do not specify rights for the DACL entry, the default is to set the rights to *Full Control*.

You can optionally customize DACL entries by specifying how to apply inheritance.

Optional `apply to` parameter	Description
`-apply-to {this-folder|sub-folder|files}`	*Apply DACL entry to* You can choose one or more of the parameter values by entering a comma-delimited list.

Note: If you do not specify this parameter, the default is to apply this DACL entry to this folder, subfolders, and files.

Steps

1. Add a DACL entry to a security descriptor:

   ```
   vserver security file-directory ntfs dacl add -vserver vserver_name -
   ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID
   optional_parameters
   ```

   Example

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type
   deny -account domain\joe -rights full-control -apply-to this-folder -
   vserver vs1
   ```

2. Verify that the DACL entry is correct:

   ```
   vserver security file-directory ntfs dacl show -vserver vserver_name -
   ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID
   ```

   Example

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                          Vserver: vs1
         Security Descriptor Name: sd1
                    Allow or Deny: deny
              Account Name or SID: DOMAIN\joe
                    Access Rights: full-control
           Advanced Access Rights: -
                         Apply To: this-folder
                    Access Rights: full-control
   ```

Creating a security policy

Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

About this task

The tasks that you add to the security policy contain associations between NTFS security descriptor and file or folder paths; therefore, you should associate the policy with each SVM with FlexVol volumes (containing NTFS or mixed security-style volumes).

There are only two parameters for this command, and both are required.

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* The name of the SVM that contains the files and folders with which you want to associate the policy.
`-policy-name` `policy_name`	*policy_name* The name of the security policy.

Steps

1. Create a security policy:

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

   Example

   ```
   vserver security file-directory policy create -policy-name policy1 -
   vserver vs1
   ```

2. Verify the security policy:

   ```
   vserver security file-directory policy show
   ```

   Example

   ```
   vserver security file-directory policy show
   ```

   ```
          Vserver          Policy Name
          -----------      -------------
             vs1              policy1
   ```

Adding a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. The task contains definitions for the security configuration of a file (or folder) or set of files (or folders).

- A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security.
- A task associates file or folder paths to the security descriptor that needs to be set on the files or folders, and also defines the rules of inheritance.

- Every task in a policy is uniquely identified by the file or folder path.
  A policy cannot have duplicate task entries. There can be only one task per path.
- There can be a maximum of 10,000 tasks entries per policy.
- By associating a task with a security policy, you are associating the policy's assigned security descriptor to the file or folder path in the policy task.

When adding tasks to security policies, you must specify the following four required parameters:

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* Name of the SVM that contains the files and folders to which you want to apply the security descriptor.
`-policy-name` `policy_name`	*Policy name* Name of the security policy to which you want to add the task.
`-path path`	*Path* Path of the files or folders on which to apply the security descriptor associated with this task.
`-ntfs-sd` `SD_name`	*Security descriptor* The name of the security descriptor that you want to associate with the file or folder path in the task. Because it is required parameter, it is recommended that you create the security descriptor and add DACL ACEs (access control entries) and SACL ACEs (if desired) prior to creating the task, then associate the security descriptor with the file or folder path in the task, and finally add the task to the security policy. A security descriptor can contain multiple ACEs, both DACL ACEs and SACL ACEs.

You can customize the security descriptor configuration by using the following optional parameters:

Optional parameter	Description
`-security-type` `{ntfs|nfsv4}`	*Security type* Whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is `ntfs`. **Note:** The `nfsv4` security descriptor type is not supported in this release. If you specify this optional parameter, you must enter `ntfs` for the value of the `-security-type` parameter.

Optional parameter	Description
`-ntfs-mode {propagate| ignore|replace}`	*Propagation mode* Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and folders contained within a parent folder inherit access control and audit information from the parent folder. The three parameters correspond to three types of propagation modes: **Propagate** — The Propagate mode propagates inheritable permissions to all subfolders and files. Existing permissions are not replaced. **Replace** — The Replace mode replaces existing permissions on all subfolders and files with inheritable permissions. **Ignore** — The Ignore mode does not allow permissions on this file or folder to be replaced. If this parameter is not specified, the default value is `propagate`.
`-index-number integer`	*Index position* Specifies the index number of a task. Tasks are applied in order. A task with a larger index number is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list. The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one. **Note:** If you specify an index number that is already assigned to an existing task, the task is added with that index number and the existing task index number is auto arranged to the next number in the table.

Steps

1. Add a task with an associated security descriptor to the security policy:

   ```
   vserver security file-directory policy-task add -vserver vserver_name -
   policy-name policy_name -path path -ntfs-sd SD_name optional_parameters
   ```

   Example

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-
   name policy1 -path /home -security-type ntfs -ntfs-mode propagate -ntfs-
   sd sd1 -index-num 1
   ```

2. Verify the policy task configuration:

```
vserver security file-directory policy-task show -vserver vserver_name -
policy-name policy_name -path path
```

Example

```
vserver security file-directory policy task show
```

```
Vserver: vs1
      Policy: policy1
        Index    File/Folder     Security    NTFS      NTFS Security
                 Path            Type        Mode      Descriptor Name
        -----    --------        --------    ------    -----------------
        1        /home           ntfs        propagate sd1
```

Applying security policies

Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

Required parameters	Description
-vserver vserver_name	*SVM* The name of the SVM that contains the files and folders to which you want to apply the policy with its associated task.
-policy-name policy_name	*Policy_name* The name of the security policy to apply.

Step

1. Apply a security policy:

   ```
   vserver security file-directory policy apply -vserver vserver_name
   -policy-name policy_name
   ```

   Example

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   The policy apply job is scheduled.

Monitoring the security policy job

When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want

to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, use the `-instance` parameter.

Step

1. Monitor the security policy job:

   vserver security file-directory job show -vserver *vserver_name*

   Example

   vserver security file-directory job show -vserver vs1

   ```
   Job ID Name                   Vserver    Node          State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifying the applied file security

You can verify the file security settings to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired settings.

About this task

You must supply the name of the SVM that contains the data and the path to the file and folders on which you want to verify security settings. You can use the optional `-expand-mask` parameter to display detailed information about the security settings.

Step

1. Display file and folder security settings:

   vserver security file-directory show -vserver *vserver_name* -path *path* [-expand-mask true]

   Example

   vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true

   ```
            Vserver: vs1
          File Path: /data/engineering
     Security Style: ntfs
    Effective Style: ntfs
     DOS Attributes: 10
   ```

```
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
       ...0 .... .... .... = Offline
       .... ..0. .... .... = Sparse
       .... .... 0... .... = Normal
       .... .... ..0. .... = Archive
       .... .... ...1 .... = Directory
       .... .... .... .0.. = System
       .... .... .... ..0. = Hidden
       .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... = Generic Read
                             .0.. .... .... .... .... .... .... .... = Generic Write
                             ..0. .... .... .... .... .... .... .... = Generic Execute
                             ...0 .... .... .... .... .... .... .... = Generic All
                             .... ...0 .... .... .... .... .... .... = System Security
                             .... .... ...1 .... .... .... .... .... = Synchronize
                             .... .... .... 1... .... .... .... .... = Write Owner
                             .... .... .... .1.. .... .... .... .... = Write DAC
                             .... .... .... ..1. .... .... .... .... = Read Control
                             .... .... .... ...1 .... .... .... .... = Delete
                             .... .... .... .... ...1 .... .... .... = Write Attributes
                             .... .... .... .... .... 1... .... .... = Read Attributes
                             .... .... .... .... .... .1.. .... .... = Delete Child
                             .... .... .... .... .... ..1. .... .... = Execute
                             .... .... .... .... .... ...1 .... .... = Write EA
                             .... .... .... .... .... .... 1... .... = Read EA
                             .... .... .... .... .... .... .1.. .... = Append
                             .... .... .... .... .... .... ..1. .... = Write
                             .... .... .... .... .... .... ...1 .... = Read

                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... = Generic Read
                             .0.. .... .... .... .... .... .... .... = Generic Write
                             ..0. .... .... .... .... .... .... .... = Generic Execute
                             ...1 .... .... .... .... .... .... .... = Generic All
                             .... ...0 .... .... .... .... .... .... = System Security
                             .... .... ...0 .... .... .... .... .... = Synchronize
                             .... .... .... 0... .... .... .... .... = Write Owner
                             .... .... .... .0.. .... .... .... .... = Write DAC
                             .... .... .... ..0. .... .... .... .... = Read Control
                             .... .... .... ...0 .... .... .... .... = Delete
                             .... .... .... .... ...0 .... .... .... = Write Attributes
                             .... .... .... .... .... 0... .... .... = Read Attributes
                             .... .... .... .... .... .0.. .... .... = Delete Child
                             .... .... .... .... .... ..0. .... .... = Execute
                             .... .... .... .... .... ...0 .... .... = Write EA
                             .... .... .... .... .... .... 0... .... = Read EA
```

```
                                   .... .... .... .... .... .... .... .0.. = Append
                                   .... .... .... .... .... .... .... ..0. = Write
                                   .... .... .... .... .... .... .... ...0 = Read
```

Configuring and applying audit policies on NTFS files and folders using the CLI

There are several steps you must perform to apply audit policies to NTFS files and folders when using the Data ONTAP CLI. First, you create an NTFS security descriptor and add SACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a Storage Virtual Machine (SVM) with FlexVol volumes.

About this task

After applying the security policy, you can monitor the security policy job and then verify the settings on the applied audit policy.

Steps

1. Creating an NTFS security descriptor on page 220
Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machine (SVM, formerly known as Vserver) with FlexVol volumes. Later, you will associate the security descriptor to the file or folder path in a policy task.

2. Adding NTFS SACL access control entries to the NTFS security descriptor on page 222
Adding SACL access control entries to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

3. Creating a security policy on page 225
Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

4. Adding a task to the security policy on page 226
Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

5. Applying security policies on page 229
Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

6. Monitoring the security policy job on page 229
When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if

you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

7. Verifying the applied audit policy on page 230

You can verify the audit policy to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired audit security settings.

Creating an NTFS security descriptor

Creating an NTFS security descriptor is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within Storage Virtual Machine (SVM, formerly known as Vserver) with FlexVol volumes. Later, you will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed-security-style volumes.

By default, when a security descriptor is created, four discretionary access control list ACEs are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY \SYSTEM	Allow	Full Control	this-folder, sub-folders, files

When creating the security descriptor, you must specify the following two parameters:

Required parameters	Description
-vserver vserver_name	*SVM name* The name of the SVM that contains the files and folders to which you want to apply the security descriptor.
-ntfs-sd SD_name	*Security descriptor* The name to assign to the security descriptor.

You can customize the security descriptor configuration by using the following optional parameters:

Optional parameter	Description
`-owner name_or_SID`	*Owner of the security descriptor* The owner of the security descriptor can modify the permissions on the file (or folder) or files (or folders) to which the security descriptor is applied and can give other users the right to take ownership of the object or objects to which the security descriptor is applied. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\user-name • user-name@DOMAIN • user-name@FQDN If you specify any of the three name formats for the value of `-owner`, keep in mind that the value is case insensitive.
`-group name_or_SID`	*Primary Group of the Owner* Specifies the owner group of the security descriptor. You can specify the owner group using either a group name or SID. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\group-name • group-name@DOMAIN • group-name@FQDN If you specify any of the three name formats for the value of `-group`, keep in mind that the value is case insensitive. **Note:** Before you can use this parameter, you must change to advanced privilege level by using the `set privilege` command.
`-control-flags-raw Hex_integer`	*Raw control flags* Specifies the control flags in the security descriptor. Available in advanced mode only. **Note:** Before you can use this parameter, you must change to advanced privilege level by using the following command: `set -privilege advanced`

Steps

1. If you want to use advanced parameters, set the privilege level to advanced:

   `set -privilege advanced`

2. Create a security descriptor:

```
vserver security file-directory ntfs create -vserver vserver_name -ntfs-
sd SD_name optional_parameters
```

Example

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -
owner domain\joe
```

3. Verify that security descriptor configuration is correct:

```
vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd
SD_name
```

Example

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
                                Vserver: vs1
                 Security Descriptor Name: sd1
           Owner of the Security Descriptor: DOMAIN\joe
```

4. If you are in advanced privilege level, return to the admin privilege level:

```
set -privilege admin
```

Adding NTFS SACL access control entries to the NTFS security descriptor

Adding SACL access control entries to the NTFS security descriptor is the second step in creating
NTFS audit policies for files or folders in Storage Virtual Machine (SVM) with FlexVol volumes.
Each entry identifies the user or group that you want to audit. The SACL entry defines whether you
want to audit successful or failed access attempts.

About this task

You can add one or more ACEs (access control entries) to the security descriptor's SACL (system
access control list).

If the security descriptor contains a SACL that has existing ACEs, the command adds the new ACE
to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and
adds the new ACE to it.

When adding an ACE to the SACL, you must provide information for the following four required
parameters:

Required parameters	Description
-vserver vserver_name	*SVM name* The name of the SVM that contains the files and folders to which the security descriptor is applied.

Required parameters	Description
`-ntfs-sd SD_name`	*Security descriptor* The name of the security descriptor to which you want to add SACL entries.
`-access-type {failure|success}`	*Access type* Specifies whether the system access control entry is a *Success* or *Failure* audit type.
`-account name_or_SID`	*Account* The account on which to apply the system access control entry. You can specify the account by using a user name or a SID. You can use any of the following formats when specifying the value for this parameter: • SID • DOMAIN\user-name • user-name@DOMAIN • user-name@FQDN If you specify any of the three name formats for the value of `-account`, keep in mind that the value is not case-sensitive.

You can configure SACL entries by specifying what rights you want to audit for success or failure events for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

• Rights
• Advanced rights
• Raw rights (advanced-privilege)

To audit events, configure one of the three rights parameters:

Optional `rights` parameters	Description
`-rights {no-access|full-control|modify|read-and-execute|read|write}`	*Rights* You can choose only one of the parameter values.

Optional `rights` parameters	Description
`-advanced-rights advanced_access_right`	*Advanced rights* You can specify one or more of the following advanced-right values by using a comma-delimited list: • read-data • write-data • append-data • read-ea • write-ea • execute-file • delete-child • read-attr • write-attr • delete • read-perm • write-perm • write-owner • full control
`-raw-rights Hex_integer`	*Raw rights* You can specify raw rights as a Hex integer. Available in advanced mode only. **Note:** This is an advanced-privilege-level parameter. Before you can use this parameter, you must change to advanced privilege level by using the following command: `set -privilege advanced`

Note: If you do not specify rights for the SACL entry, the default setting is Full Control.

You can optionally customize SACL entries by specifying how to apply inheritance.

Optional `apply to` parameter	Description
`-apply-to {this-folder|sub-folder|files}`	*Apply SACL entry to* You can choose one or more of the parameter values by entering a comma-delimited list.

Note: If you do not specify this parameter, the default is to apply this SACL entry to this folder, subfolders, and files.

Steps

1. Add a SACL entry to a security descriptor:

   vserver security file-directory ntfs sacl add -vserver *vserver_name* -ntfs-sd *SD_name* -access-type {failure|success} -account *name_or_SID* *optional_parameters*

   Example

   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1

2. Verify that the SACL entry is correct:

   vserver security file-directory ntfs sacl show -vserver *vserver_name* -ntfs-sd *SD_name* -access-type {failure|success} -account *name_or_SID*

   Example

   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe

   ```
                                   Vserver: vs1
                    Security Descriptor Name: sd1
        Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
   ```

Creating a security policy

Creating a security policy for Storage Virtual Machines (SVMs) with FlexVol volumes is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks where each task is a single entry that can be applied to files or folders. You later add tasks to the security policy.

About this task

The tasks that you add to the security policy contain associations between NTFS security descriptor and file or folder paths; therefore, you should associate the policy with each SVM with FlexVol volumes (containing NTFS or mixed security-style volumes).

There are only two parameters for this command, and both are required.

Required parameters	Description
`-vserver vserver_name`	*SVM name* The name of the SVM that contains the files and folders with which you want to associate the policy.
`-policy-name policy_name`	*policy_name* The name of the security policy.

Steps

1. Create a security policy:

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

   Example

   `vserver security file-directory policy create -policy-name policy1 - vserver vs1`

2. Verify the security policy:

   `vserver security file-directory policy show`

   Example

   `vserver security file-directory policy show`

   ```
           Vserver          Policy Name
           -----------      -------------
               vs1              policy1
   ```

Adding a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in Storage Virtual Machine (SVM) with FlexVol volumes. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. The task contains definitions for the security configuration of a file (or folder) or set of files (or folders).

- A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security.
- A task associates file or folder paths to the security descriptor that needs to be set on the files or folders, and also defines the rules of inheritance.

- Every task in a policy is uniquely identified by the file or folder path.
  A policy cannot have duplicate task entries. There can be only one task per path.
- There can be a maximum of 10,000 tasks entries per policy.
- By associating a task with a security policy, you are associating the policy's assigned security descriptor to the file or folder path in the policy task.

When adding tasks to security policies, you must specify the following four required parameters:

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* Name of the SVM that contains the files and folders to which you want to apply the security descriptor.
`-policy-name` `policy_name`	*Policy name* Name of the security policy to which you want to add the task.
`-path` `path`	*Path* Path of the files or folders on which to apply the security descriptor associated with this task.
`-ntfs-sd` `SD_name`	*Security descriptor* The name of the security descriptor that you want to associate with the file or folder path in the task. Because it is required parameter, it is recommended that you create the security descriptor and add DACL ACEs (access control entries) and SACL ACEs (if desired) prior to creating the task, then associate the security descriptor with the file or folder path in the task, and finally add the task to the security policy. A security descriptor can contain multiple ACEs, both DACL ACEs and SACL ACEs.

You can customize the security descriptor configuration by using the following optional parameters:

Optional parameter	Description
`-security-type` `{ntfs|nfsv4}`	*Security type* Whether the security descriptor associated with this task is an NTFS or a NFSv4 security descriptor type. If you do not specify a value for this optional parameter, the default is `ntfs`. **Note:** The `nfsv4` security descriptor type is not supported in this release. If you specify this optional parameter, you must enter `ntfs` for the value of the `-security-type` parameter.

Optional parameter	Description
`-ntfs-mode {propagate| ignore|replace}`	*Propagation mode* Specifies how to propagate security settings to child subfolders and files. This setting determines how child files and folders contained within a parent folder inherit access control and audit information from the parent folder. The three parameters correspond to three types of propagation modes: **Propagate** — The Propagate mode propagates inheritable permissions to all subfolders and files. Existing permissions are not replaced. **Replace** — The Replace mode replaces existing permissions on all subfolders and files with inheritable permissions. **Ignore** — The Ignore mode does not allow permissions on this file or folder to be replaced. If this parameter is not specified, the default value is `propagate`.
`-index-number integer`	*Index position* Specifies the index number of a task. Tasks are applied in order. A task with a larger index number is applied after a task with a lower index number. If you do not specify this optional parameter, new tasks are applied to the end of the index list. The range of supported values is 1 through 9999. If there is a gap between the highest existing index number and the value entered for this parameter, the task with this number is considered to be the last task in the policy and is treated as having an index number of the previous highest index plus one. **Note:** If you specify an index number that is already assigned to an existing task, the task is added with that index number and the existing task index number is auto arranged to the next number in the table.

Steps

1. Add a task with an associated security descriptor to the security policy:

   ```
   vserver security file-directory policy-task add -vserver vserver_name -
   policy-name policy_name -path path -ntfs-sd SD_name optional_parameters
   ```

   Example

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-
   name policy1 -path /home -security-type ntfs -ntfs-mode propagate -ntfs-
   sd sd1 -index-num 1
   ```

2. Verify the policy task configuration:

```
vserver security file-directory policy-task show -vserver vserver_name -
policy-name policy_name -path path
```

Example

```
vserver security file-directory policy task show
```

```
  Vserver: vs1
       Policy: policy1
        Index    File/Folder    Security    NTFS      NTFS Security
                 Path           Type        Mode      Descriptor Name
        -----    --------       --------    ------    -----------------
          1      /home          ntfs        propagate sd1
```

Applying security policies

Applying a security policy to Storage Virtual Machines (SVMs) with FlexVol volumes is the last step to creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

Required parameters	Description
`-vserver` `vserver_name`	*SVM* The name of the SVM that contains the files and folders to which you want to apply the policy with its associated task.
`-policy-name` `policy_name`	*Policy_name* The name of the security policy to apply.

Step

1. Apply a security policy:

   ```
   vserver security file-directory policy apply -vserver vserver_name
   -policy-name policy_name
   ```

   Example

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   The policy apply job is scheduled.

Monitoring the security policy job

When applying the security policy to Storage Virtual Machines (SVMs) with FlexVol volumes, you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want

to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, use the `-instance` parameter.

Step

1. Monitor the security policy job:

   vserver security file-directory job show -vserver *vserver_name*

   Example

   vserver security file-directory job show -vserver vs1

   ```
   Job ID Name                   Vserver    Node           State
   ------ --------------------   ----------  --------------  ----------
   53322  Fsecurity Apply        vs1         node1           Success
          Description: File Directory Security Apply Job
   ```

Verifying the applied audit policy

You can verify the audit policy to confirm that the files or folders on the Storage Virtual Machine (SVM) with FlexVol volumes to which you applied the security policy have the desired audit security settings.

About this task

You use the `vserver security file-directory show` command to display audit policy information. You must supply the name of the SVM that contains the data and the path to the data whose file or folder audit policy information you want to display.

Step

1. Display audit policy settings:

   vserver security file-directory show -vserver *vserver_name* -path *path*

   Example

   The following command displays the audit policy information applied to the path "/corp" in SVM vs1. The path has both a SUCCESS and a SUCCESS/FAIL SACL entry applied to it:

   ```
   cluster::> vserver security file-directory show -vserver vs1 -path /
   corp

                      Vserver: vs1
                    File Path: /corp
   ```

```
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|
SA|FA

                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|
CI

                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Commands for managing NTFS security descriptors

There are specific Data ONTAP commands for managing security descriptors. You can create,
modify, delete, and display information about security descriptors.

If you want to...	Use this command...
Create NTFS security descriptors	vserver security file-directory ntfs create
Modify existing NTFS security descriptors	vserver security file-directory ntfs modify
Display information about existing NTFS security descriptors	vserver security file-directory ntfs show
Delete NTFS security descriptors	vserver security file-directory ntfs delete

See the man pages for the vserver security file-directory ntfs commands for more
information.

Commands for managing NTFS DACL access control entries

There are specific Data ONTAP commands for managing DACL access control entries (ACEs). You can add ACEs to NTFS DACLs at any time. You can also manage existing NTFS DACLs by modifying, deleting, and displaying information about ACEs in DACLs.

If you want to...	Use this command...
Create ACEs and add them to NTFS DACLs	`vserver security file-directory ntfs dacl add`
Modify existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl modify`
Display information about existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl show`
Remove existing ACEs from NTFS DACLs	`vserver security file-directory ntfs dacl remove`

See the man pages for the `vserver security file-directory ntfs dacl` commands for more information.

Commands for managing NTFS SACL access control entries

There are specific Data ONTAP commands for managing SACL access control entries (ACEs). You can add ACEs to NTFS SACLs at any time. You can also manage existing NTFS SACLs by modifying, deleting, and displaying information about ACEs in SACLs.

If you want to...	Use this command...
Create ACEs and add them to NTFS SACLs	`vserver security file-directory ntfs sacl add`
Modify existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl modify`
Display information about existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl show`
Remove existing ACEs from NTFS SACLs	`vserver security file-directory ntfs sacl remove`

See the man pages for the `vserver security file-directory ntfs sacl` commands for more information.

Commands for managing security policies

There are specific Data ONTAP commands for managing security policies. You can display information about policies and you can delete policies. You cannot modify a security policy.

If you want to...	Use this command...
Create security policies	**vserver security file-directory policy create**
Display information about security policies	**vserver security file-directory policy show**
Delete security policies	**vserver security file-directory policy delete**

See the man pages for the vserver security file-directory policy commands for more information.

Commands for managing security policy tasks

There are Data ONTAP commands for adding, modifying, removing, and displaying information about security policy tasks.

If you want to...	Use this command...
Add security policy tasks	**vserver security file-directory policy task add**
Modify security policy tasks	**vserver security file-directory policy task modify**
Display information about security policy tasks	**vserver security file-directory policy task show**
Remove security policy tasks	**vserver security file-directory policy task remove**

See the man pages for the vserver security file-directory policy task commands for more information.

Commands for managing security policy jobs

There are Data ONTAP commands for pausing, resuming, stopping, and displaying information about security policy jobs.

If you want to...	Use this command...
Pause security policy jobs	`vserver security file-directory job pause -vserver vserver_name -id integer`
Resume security policy jobs	`vserver security file-directory job resume -vserver vserver_name -id integer`
Display information about security policy jobs	`vserver security file-directory job show -vserver vserver_name` You can determine the job ID of a job using this command.
Stop security policy jobs	`vserver security file-directory job stop -vserver vserver_name -id integer`

See the man pages for the `vserver security file-directory job` commands for more information.

Using security tracing to verify or troubleshoot file and directory access

You can add permission tracing filters to instruct Data ONTAP to log information about why the CIFS server on a Storage Virtual Machine (SVM) with FlexVol volumes allows or denies a client or user's request to perform an operation. This can be useful when you want to verify that your file access security scheme is appropriate or when you want to troubleshoot file access issues.

How security traces work

Security traces allow you to configure a filter that detects client operations over SMB on the Storage Virtual Machine (SVM) with FlexVol volumes, and trace all access checks matching that filter. You can then view the trace results, which provides a convenient summary of the reason that access was allowed or denied.

When you want to verify the security settings for SMB access on files and folders on your SVM or if you are faced with an access problem, you can quickly add a filter to turn on permission tracing.

The following list outlines important facts about how security traces works:

• Data ONTAP applies security traces at the SVM level.

- Each incoming request is screened to see if it matches filtering criteria of any enabled security traces.
- Traces are performed for both file and folder access requests.
- Traces can filter based on the following criteria:

  - Client IP
  - SMB path
  - Windows name
  - UNIX name

- Requests are screened for *Allowed* and *Denied* access response results.
- Each request matching filtering criteria of enabled traces is recorded in the trace results log.
- The storage administrator can configure a timeout on a filter to automatically disable it.
- If a request matches multiple filters, the results from the filter with the highest index number is recorded.
- The storage administrator can print results from the trace results log to determine why an access request was allowed or denied.

Related concepts

How to interpret security trace results on page 245
How security styles affect data access on page 19

Related tasks

Performing security traces on page 236

Types of access checks security traces monitor

Access checks for a file or folder are done based on multiple criteria. Security traces monitor operations on all these criteria.

The types of access checks that security traces monitor include the following:

- Volume and qtree security style
- Effective security of the file system containing the files and folders on which operations are requested
- User mapping
- Share-level permissions
- File-level permissions

Considerations when creating security traces

You should keep several considerations in mind when you create security traces on Storage Virtual Machines (SVMs) with FlexVol volumes. For example, you need to know on which protocols you

can create a trace, which security-styles are supported, and what the maximum number of active traces is.

- You can only create security traces on SVMs with FlexVol volumes.
- Each security trace filter entry is SVM specific.
  You must specify the SVM on which you want to run the trace.
- You can add permission tracing filters for SMB requests only.
- You must set up the CIFS server on the SVM on which you want to create trace filters.
- You can create security traces for files and folders residing on NTFS, UNIX, and mixed security-style volumes and qtrees.
- You can add a maximum of 10 permission tracing filters per SVM.
- You must specify a filter index number when creating or modifying a filter.
  Filters are considered in order of the index number. The criteria in a filter with a higher index number is considered before the criteria with a lower index number. If the request being traced matches criteria in multiple enabled filters, only the filter with the highest index number is triggered.
- After you have created and enabled a security trace filter, you must perform some file or folder requests on a client system to generate activity that the trace filter can capture and log in the trace results log.
- You should add permission tracing filters for file access verification or troubleshooting purposes only.
  Adding permission tracing filters has a minor effect on controller performance.
  When you are done with verification or troubleshooting activity, you should disable or remove all permission tracing filters. Furthermore, the filtering criteria you select should be as specific as possible so that Data ONTAP does not send a large number of trace results to the log.

Performing security traces

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB client that match filter criteria, and viewing the results.

About this task

After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

Steps

1. Creating security trace filters on page 237
   You can create security trace filters that detect SMB client operations on Storage Virtual Machines (SVMs) with FlexVol volumes and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

2. Displaying information about security trace filters on page 239

You can display information about security trace filters configured on your Storage Virtual Machine (SVM). This enables you to see which types of access events each filter traces.

3. Displaying security trace results on page 240
You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB file access issues.

4. Modifying security trace filters on page 242
If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

5. Deleting security trace filters on page 243
When you no longer need a security trace filter entry, you can delete it. Because you can have a maximum of 10 security trace filters per Storage Virtual Machine (SVM), deleting unneeded filters enables you to create new filters if you have reached the maximum.

6. Deleting security trace records on page 244
After you finish using a filter trace record to verify file access security or to troubleshoot SMB client access issues, you can delete the security trace record from the security trace log.

7. Deleting all security trace records on page 244
If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

Related concepts

How security traces work on page 234
Types of access checks security traces monitor on page 235
Considerations when creating security traces on page 235
How to interpret security trace results on page 245
Displaying information about file security and audit policy on FlexVol volumes on page 186

Creating security trace filters

You can create security trace filters that detect SMB client operations on Storage Virtual Machines (SVMs) with FlexVol volumes and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

About this task

There are two required parameters for this command:

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* The name of the SVM that contains the files or folders on which you want to apply the security trace filter.

Required parameters	Description
`-index` `index_number`	*Filter index number* The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10.

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

Filter parameter	Description
`-client-ip` `IP_Address`	This filter specifies the IP address from which the user is accessing the SVM.
`-path` *path*	This filter specifies the path on which to apply the permission trace filter. The value for `-path` can use either of the following formats: • The complete path, starting from the root of the share • A partial path, relative to the root of the share You must use NFS style directory separators in the path value.

`-windows-name`
`win_user_name` or `-unix-name`
`unix_user_name`
	You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter.
	
	Note: Even though you can only trace SMB access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data.

`-trace-allow` `{yes|no}`	Tracing for deny events is always enabled for a security trace filter. You can optionally trace allow events. To trace allow events, you set this parameter to `yes`.
`-enabled {enabled|` `disabled}`	You can enable or disable the security trace filter. By default, the security trace filter is enabled.
`-time-enabled` `integer`	You can specify a timeout for the filter, after which it is disabled.

Steps

1. Create a security trace filter:

```
vserver security trace filter create -vserver vserver_name -index
index_number filter_parameters
```

Example

filter_parameters is a list of optional filter parameters.

For more information, see the man pages for the command.

2. Verify the security trace filter entry:

**vserver security trace filter show -vserver *vserver_name* -index
*index_number***

Examples

The following command creates a security trace filter for any user accessing a file with a share
path \\server\share1\dir1\dir2\file.txt from the IP address 10.10.10.7. The filter
uses a complete path for the -path option. The client's IP address used to access data is
10.10.10.7. The filter times out after 30 minutes:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1 -path /dir1/
dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow  Windows-Name
--------  -----  -----------  ---------------------  -----------  -------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt        no           -
```

The following command creates a security trace filter using a relative path for the -path
option. The filter traces access for a Windows user named "joe". Joe is accessing a file with a
share path \\server\share1\dir1\dir2\file.txt. The filter traces allow and deny
events:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2 -path /dir1/
dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                         Vserver: vs1
                    Filter Index: 2
          Client IP Address to Match: -
                            Path: /dir1/dir2/file.txt
               Windows User Name: mydomain\joe
                  UNIX User Name: -
               Trace Allow Events: yes
                  Filter Enabled: enabled
            Minutes Filter is Enabled: 60
```

Displaying information about security trace filters

You can display information about security trace filters configured on your Storage Virtual Machine
(SVM). This enables you to see which types of access events each filter traces.

Step

1. Display information about security trace filter entries by using the vserver security trace
filter show command.

For more information about using this command, see the man pages.

Examples

The following command displays information about all security trace filters on SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index  Client-IP       Path                  Trace-Allow  Windows-Name
-------- -----  -----------  ----------------------  -----------  -------------
vs1        1    -            /dir1/dir2/file.txt         yes      -
vs1        2    -            /dir3/dir4/                 no       mydomain\joe
```

Displaying security trace results

You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB file access issues.

Before you begin

An enabled security trace filter must exist and operations must have been performed from an SMB client that matches the security trace filter to generate security trace results.

About this task

You can display a summary of all security trace results, or you can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the security trace results contain a large number of records.

If you do not specify any of the optional parameters, the following is displayed:

- Storage Virtual Machine (SVM) name
- Node name
- Security trace index number
- Security style
- Path
- Reason
- User name

  The user name displayed depends on how the trace filter is configured:

If the filter is configured...	Then...
With a UNIX user name	The security trace result displays the UNIX user name.
With a Windows user name	The security trace result displays the Windows user name.
Without a user name	The security trace result displays the Windows user name.

You can customize the output by using optional parameters. Some of the optional parameters that you can use to narrow the results returned in the command output include the following:

Optional parameter	Description
`-fields` `field_name`, ...	Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results.
`-node node_name`	Displays information only about events on the specified node.
`-vserver` `vserver_name`	Displays information only about events on the specified SVM.
`-index integer`	Displays information about the events that occurred as a result of the filter corresponding to the specified index number.
`-client-ip` `IP_address`	Displays information about the events that occurred as a result of file access from the specified client IP address.
`-path path`	Displays information about the events that occurred as a result of file access to the specified path.
`-user-name` `user_name`	Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user.
`-security-style` `security_style`	Displays information about the events that occurred on file systems with the specified security style.

See the man page for information about other optional parameters that you can use with the command.

Step

1. Display security trace filter results by using the `vserver security trace trace-result show` command.

Example

`vserver security trace trace-result show -user-name domain\user`

```
Vserver: vs1

     Node     Index   Filter Details          Reason
     -------- ------- --------------------    ----------------------------
     node1    3       User:domain\user        Access denied by explicit ACE
                      Security Style:mixed
                      Path:/dir1/dir2/

     node1    5       User:domain\user        Access denied by explicit ACE
                      Security Style:unix
                      Path:/dir1/
```

Related concepts

Related references

Modifying security trace filters

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

About this task

You must identify which security trace filter you want to modify by specifying the Storage Virtual Machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

Steps

1. Modify a security trace filter:

   vserver security trace filter modify -vserver *vserver_name* -index *index_number filter_parameters*

   - *vserver_name* is the name of the SVM on which you want to apply a security trace filter.
   - *index_number* is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.
   - *filter_parameters* is a list of optional filter parameters.

2. Verify the security trace filter entry:

   vserver security trace filter show -vserver *vserver_name* -index *index_number*

Example

The following command modifies the security trace filter with the index number 1. The filter traces events for any user accessing a file with a share path \\server \share1\dir1\dir2\file.txt from any IP address. The filter uses a complete path for the -path option. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1 -path /dir1/
dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                              Vserver: vs1
                         Filter Index: 1
            Client IP Address to Match: -
                                 Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                     Trace Allow Events: yes
```

```
                                      Filter Enabled: enabled
                            Minutes Filter is Enabled: 60
```

Deleting security trace filters

When you no longer need a security trace filter entry, you can delete it. Because you can have a maximum of 10 security trace filters per Storage Virtual Machine (SVM), deleting unneeded filters enables you to create new filters if you have reached the maximum.

About this task

To uniquely identify the security trace filter that you want to delete, you must specify the following:

- The name of the SVM to which the trace filter is applied
- The filter index number of the trace filter

Steps

1. Identify the filter index number of the security trace filter entry you want to delete:

vserver security trace filter show -vserver *vserver_name*

Example

vserver security trace filter show -vserver vs1

```
Vserver  Index  Client-IP          Path              Trace-Allow  Windows-Name
-------- -----  -----------  ----------------------  -----------  -------------
vs1       1     -            /dir1/dir2/file.txt       yes         -
vs1       2     -            /dir3/dir4/               no          mydomain\joe
```

2. Using the filter index number information from the previous step, delete the filter entry:

vserver security trace filter delete -vserver *vserver_name* -index *index_number*

Example

vserver security trace filter delete -vserver vs1 -index 1

3. Verify that the security trace filter entry is deleted:

vserver security trace filter show -vserver *vserver_name*

Example

vserver security trace filter show -vserver vs1

```
Vserver  Index  Client-IP          Path              Trace-Allow  Windows-Name
-------- -----  -----------  ----------------------  -----------  -------------
vs1       2     -            /dir3/dir4/               no          mydomain\joe
```

Deleting security trace records

After you finish using a filter trace record to verify file access security or to troubleshoot SMB client access issues, you can delete the security trace record from the security trace log.

About this task

Before you can delete a security trace record, you must know the record's sequence number.

> **Note:** Each Storage Virtual Machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let Data ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.

Steps

1. Identify the sequence number of the record you want to delete:

   `vserver security trace trace-result show -vserver vserver_name -instance`

2. Delete the security trace record:

   `vserver security trace trace-result delete -node node_name -vserver vserver_name -seqnum integer`

   ### Example

   `vserver security trace trace-result delete -vserver vs1 -node node1 - seqnum 999`

   - `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
     This is a required parameter.
   - `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.
     This is a required parameter.
   - `-seqnum integer` is the sequence number of the log event that you want to delete.
     This is a required parameter.

Deleting all security trace records

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

Step

1. Delete all security trace records:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

- -node *node_name* is the name of the cluster node on which the permission tracing event that you want to delete occurred.
- -vserver *vserver_name* is the name of the Storage Virtual Machine (SVM) on which the permission tracing event that you want to delete occurred.

How to interpret security trace results

Security trace results provide the reason that a request was allowed or denied. Output displays the result as a combination of the reason for allowing or denying access and the location within the access checking pathway where access is either allowed or denied. You can use the results to isolate and identify why actions are or are not allowed.

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the Reason field that appears in the trace results log in an Allow result type:

```
Access is allowed because CIFS implicit permission grants requested
access while opening existing file or directory.
```

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the Reason field that appears in the trace results log in a Deny result type:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Example of output from the `Filter details` field

The following is an example of the output from the Filter details field in the trace results log that liste effective security style of the file system containing files and folders match the filter criteria:

```
Security Style: MIXED and NT ACL
```

Related tasks

List of effective security styles on file systems

Security trace results provide information about the effective security style on file systems containing files and folders monitored by trace filters, which helps you understand why access operations are allowed or denied.

It is not always obvious what the effective security style is on files and folders, or what the impact of the effective security style is on a user who is trying to access files or folders over SMB or NFS. The list of effective security styles provided in the following table helps you decide what parameter setting to use when you create trace filters, and helps you interpret trace results obtained when running security traces:

Effective security styles	Description
SECURITY_NONE	Security not set
SECURITY_UNIX_MODEBITS	UNIX and UNIX permissions
SECURITY_UNIX_ACL	UNIX and NFSv4 ACL
SECURITY_UNIX_SD	UNIX and NT ACL
SECURITY_MIXED_MODEBITS	MIXED and UNIX permissions
SECURITY_MIXED_ACL	MIXED and NFSv4 ACL
SECURITY_MIXED_SD	MIXED and NT ACL
SECURITY_NTFS_MODEBITS	NTFS and UNIX permissions
SECURITY_NTFS_ACL	NTFS and NFSv4 ACL
SECURITY_NTFS_SD	NTFS and NT ACL
SECURITY_UNIX	UNIX
SECURITY_MIXED	MIXED
SECURITY_NTFS	NTFS
SECURITY_MODEBITS	UNIX permissions
SECURITY_ACL	NFSv4 ACL
SECURITY_SD	NT ACL

List of reasons and locations for allowing access

Before you can interpret security trace results, you need to have a list of the reasons that access can be allowed. You must also have the list of the locations within the access checking pathway where access can be allowed. This information also aids you in planning your security trace filter.

A complete sentence describing the "Allow" result is derived by concatenating a location to the reason.

List of reasons

The list of "Allow" reasons is provided in the following table:

Access allowed reason
Access is allowed because the operation is trusted and no security is configured
Access is allowed because the user has UNIX root privileges
Access is allowed because the user has UNIX owner privileges
Access is allowed because UNIX implicit permission grants requested access
Access is allowed because the CIFS user is owner
Access is allowed because the user has take ownership privilege
Access is allowed because there is no CIFS ACL
Access is allowed because CIFS implicit permission grants requested access
Access is allowed because the security descriptor is corrupted and the user is a member of the Administrators group
Access is allowed because the ACL is corrupted and the user is a member of the Administrators group
Access is allowed because the user has UNIX permissions
Access is allowed because explicit ACE grants requested access
Access is allowed because the user has audit privileges
Access is allowed because the user has superuser credentials
Access is allowed because inherited ACE grants requested access

List of locations

The list of locations that are concatenated onto a reason are provided in the following table:

Locations within the access checking path...
while traversing the directory.
while truncating the file.
while creating the directory.
while creating the file.
while checking parent's modebits during delete.
while deleting the child.
while checking for child-delete access on the parent.
while reading security descriptor.
while accessing the link.
while creating or writing the file.
while opening existing file or directory.
while setting the attributes.
while traversing the directory.
while reading the file.
while reading the directory.
while deleting the target during rename.
while deleting the child during rename.
while writing data in the parent during rename.
while adding a directory during rename.
while adding a file during rename.
while updating the target directory during rename.
while setting attributes.
while writing to the file.
while extending the coral file.
while creating the vdisk file.
while checking for stale locks before open.
while deleting a file or a directory.

Locations within the access checking path...
while truncating a hidden file.

List of reasons and locations for denying access

Before you can interpret security trace results, you need a list of the reasons that access can be denied. You must also have the list of the locations within the access checking pathway where access can be denied. This information also aids you in planning your security trace filter.

A complete sentence describing the "Deny" result is derived by concatenating a location to the reason.

List of reasons

The list of "Deny" reasons is provided in the following table:

Reasons for denying access
Access is denied by UNIX permissions
Access is denied by an explicit ACE
Access is denied. The requested permissions are not granted by the ACL
Access is denied. The security descriptor is corrupted
Access is denied. The ACL is corrupted
Access is denied. The sticky bit is set on the parent directory and the user is not the owner of file or parent directory
Access is denied. The owner can be changed only by root
Access is denied. The UNIX permissions/uid/gid/NFSv4 ACL can be changed only by owner or root
Access is denied. The GID can be set by owner to a member of its legal group list only if 'Owner can chown' is not set
Access is denied. The file or the directory has readonly bit set
Access is denied. There is no audit privilege
Access is denied. Enforce DOS bits blocks the access
Access is denied. Hidden attribute is set
Access is denied by an inherited ACE

List of locations

The list of locations that are concatenated onto a reason are provided in the following table:

Locations within the access checking path...
while traversing the directory.
while truncating the file.
while creating the directory.
while creating the file.
while checking parent's modebits during delete.
while deleting the child.
while checking for child-delete access on the parent.
while reading security descriptor.
while accessing the link.
while creating or writing the file.
while opening existing file or directory.
while setting the attributes.
while traversing the directory.
while reading the file.
while reading the directory.
while deleting the target during rename.
while deleting the child during rename.
while writing data in the parent during rename.
while adding a directory during rename.
while adding a file during rename.
while updating the target directory during rename.
while setting attributes.
while writing to the file.
while extending the coral file.
while creating the vdisk file.
while checking for stale locks before open.

Locations within the access checking path...
while deleting a file or a directory.
while truncating a hidden file.

Configuring the metadata cache for SMB shares

Metadata caching enables file attribute caching on SMB 1.0 clients to provide faster access to file and folder attributes. You can enable or disable attribute caching on a per-share basis. You can also configure the time-to-live for cached entries if metadata caching is enabled. Configuring metadata caching is not necessary if clients are connecting to shares over SMB 2.x or SMB 3.0.

How SMB metadata caching works

When enabled, the SMB metadata cache stores path and file attribute data for a limited amount of time. This can improve SMB performance for SMB 1.0 clients with common workloads.

For certain tasks, SMB creates a significant amount of traffic that can include multiple identical queries for path and file metadata. You can reduce the number of redundant queries and improve performance for SMB 1.0 clients by using SMB metadata caching to fetch information from the cache instead.

> **Attention:** While unlikely, it is possible that the metadata cache might serve stale information to SMB 1.0 clients. If your environment cannot afford this risk, you should not enable this feature.

Enabling the SMB metadata cache

You can improve SMB performance for SMB 1.0 clients by enabling the SMB metadata cache. By default, SMB metadata caching is disabled.

Step

1. Perform the desired action:

If you want to...	Enter the command...
Enable SMB metadata caching when you create a share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
Enable SMB metadata caching on an existing share	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Related tasks

Configuring the lifetime of SMB metadata cache entries

You can configure the lifetime of SMB metadata cache entries to optimize the SMB metadata cache performance in your environment. The default is 10 seconds.

Before you begin

You must have enabled the SMB metadata cache feature. If SMB metadata caching is not enabled, the SMB cache TTL setting is not used.

Step

1. Perform the desired action:

If you want to configure the lifetime of SMB metadata cache entries when you...	Enter the command...
Create a share	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm] [integers]`
Modify an existing share	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm] [integers]`

You can specify additional share configuration options and properties when you create or modify shares. See the man pages for more information.

Managing file locks

You can display information about the current locks for a Storage Virtual Machine (SVM) as a first step to determining why a client cannot access a volume or file. You can use this information if you need to break file locks.

For information about how file locks affect Infinite Volumes, see the *Clustered Data ONTAP Infinite Volumes Management Guide*.

About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How Data ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as rm, rmdir, and mv can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

How Data ONTAP treats read-only bits

The read-only bit is a binary digit, which holds a value of 0 or 1, that is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use MS-DOS and Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

Data ONTAP can set a read-only bit on a file when an SMB client that uses MS-DOS or Windows creates that file. Data ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For Data ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, Data ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, Data ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, Data ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, Data ONTAP enables the owner's write permission bit for the file.

- Files with the read-only bit enabled are writable only by root.

  Note: Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How Data ONTAP differs from Windows on handling locks on share path components

Unlike Windows, Data ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because Data ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

Displaying information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific Storage Virtual Machine (SVM) or to filter the command's output by other criteria. If you do not specify any parameter, the command displays the following information:

- SVM name
- Volume name of the FlexVol volume or the name of the namespace constituent for the Infinite Volume
- Path of the locked object
- Logical interface name
- Protocol by which the lock was established
- Type of lock
- Client

The vserver locks show command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.

- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each of these lock types. See the man page for the command for more information.

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path                  LIF         Protocol  Lock Type   Client
-------  -------------------------    ----------  --------  ----------  -------
vol1     /vol1/file1                  lif1        nfsv4     share-level -
                   Sharelock Mode: write-deny_none
                                                            delegation  -
                   Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

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

                     Vserver: vs1
                      Volume: data2_2
           Logical Interface: lif2
                 Object Path: /data2/data2_2/intro.pptx
                   Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
               Lock Protocol: cifs
                   Lock Type: share-level
     Node Holding Lock State: node3
                  Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                 Oplock Level: -
      Shared Lock Access Mode: write-deny_none
          Shared Lock is Soft: false
             Delegation Type: -
              Client Address: 10.3.1.3
               SMB Open Type: durable
          SMB Connect State: connected
  SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                     Vserver: vs1
                      Volume: data2_2
           Logical Interface: lif2
                 Object Path: /data2/data2_2/test.pptx
```

```
                      Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
               Lock Protocol: cifs
                   Lock Type: op-lock
   Node Holding Lock State: node3
                  Lock State: granted
 Bytelock Starting Offset: -
    Number of Bytes Locked: -
       Bytelock is Mandatory: -
       Bytelock is Exclusive: -
       Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
   Shared Lock Access Mode: -
         Shared Lock is Soft: -
             Delegation Type: -
              Client Address: 10.3.1.3
                SMB Open Type: -
           SMB Connect State: connected
 SMB Expiration Time (Secs): -
           SMB Open Group ID:
 78a90c59d45ae2l1998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Breaking locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The vserver locks break command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

Steps

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

    The man page for the command contains detailed information.

2. Set the privilege level to advanced:

    set -privilege advanced

3. Perform one of the following actions:

If you want to break a lock by specifying...	Enter the command...
The SVM name, volume name, LIF name, and file path	**vserver locks break -vserver** *vserver_name* **-volume** *volume_name* **-path** *path* **-lif** *lif*
The lock ID	**vserver locks break -lockid** *UUID*

-vserver *vserver_name* specifies the SVM name.

-volume *volume_name* specifies the volume name of the FlexVol volume or the name of the namespace constituent for the Infinite Volume.

`-path` *path* specifies the path.

`-lif` *lif* specifies the logical interface.

`-lockid` specifies the universally unique identifier for the lock.

4. Return to the admin privilege level:

   set -privilege admin

Monitoring SMB activity

You can monitor SMB activity by displaying information about SMB sessions and open files. You can also display information about SMB statistics.

Displaying SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

About this task

You can display information for all sessions on your Storage Virtual Machine (SVM) in summary form by using the `vserver cifs session show` command without any optional parameters. However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the results contain a large number of records.

- You can use the optional `-fields` parameter to display output on the fields you choose.
- Alternatively, you can use the `-instance` parameter to display detailed information about established SMB sessions.

You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display SMB session information for established sessions...	**Enter the following command...**
For all sessions on the SVM in summary form	`vserver cifs session show -vserver vserver_name`
On a specified connection ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
From a specified workstation IP address	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
On the specified LIF IP address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
On a specified node	`vserver cifs session show -vserver vserver_name -node {node_name|local}`
From a specified Windows user	`vserver cifs session show -vserver vserver_name -windows-user user_name` The format for `user_name` is `[domain]\user`.
With a specified authentication mechanism	`vserver cifs session show -vserver vserver_name -auth-mechanism authentication_mechanism` The value for `-auth-mechanism` can be one of the following: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`
With the specified protocol version	`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` **Note:** Continuously available protection is available only on SMB 3.0 sessions. To see continuously available protection status on all qualifying sessions, specify this parameter with the value set to `SMB3`.

If you want to display SMB session information for established sessions...	Enter the following command...
With the specified level of continuously available protection	**vserver cifs session show -vserver *vserver_name* -continuously-available *continuously_available_protection_level*** The value for -continuously-available can be one of the following: • No • Yes • Partial **Note:** If the continuously available status is Partial, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the vserver cifs sessions file show command to determine which files on the established session are not open with continuously available protection.

There are additional optional parameters. See the man page for more information.

Examples

The following example displays session information on sessions SVM vs1 established from a workstation with the IP address of 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                     Open      Idle
ID         ID      Workstation     Windows User    Files     Time
---------- ------- --------------- ------------- ------- ------------
3151272279 1       10.1.1.1        DOMAIN\joe          2          23s
```

The following example displays detailed session information on sessions with continuously available protection on SVM vs1. The connection was made by using the domain computer-machine account:

```
cluster1::> vserver cifs session show -instance -continuously-available Yes
                       Node: node1
                    Vserver: vs1
                 Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
       Workstation IP address: 10.1.1.2
     Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\SERVER1$
                    UNIX User: pcuser
                  Open Shares: 1
```

```
                        Open Files: 1
                        Open Other: 0
                   Connected Time: 10m 43s
                         Idle Time: 1m 19s
                  Protocol Version: SMB3
             Continuously Available: Yes
```

The following example displays session information on sessions using SMB 3.0 on SVM vs1.
The user connected to this share from an SMB 3.0 capable client by using the LIF IP address;
therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made
using Kerberos authentication to connect with continuously available protection:

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                             Node: node1
                          Vserver: vs1
                       Session ID: 1
                   Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
        Workstation IP address: 10.1.1.3
      Authentication Mechanism: NTLMv2
                    Windows User: DOMAIN\administrator
                       UNIX User: pcuser
                     Open Shares: 1
                       Open Files: 0
                       Open Other: 0
                  Connected Time: 6m 22s
                        Idle Time: 5m 42s
                 Protocol Version: SMB3
           Continuously Available: No
```

Displaying information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID,
the hosting volume, the share name, and the share path. You can display information about a file's
continuously available protection level, which is helpful in determining whether an open file is in a
state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed
information is useful when you need to determine SMB session information for particular files within
an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously
available protection and some are not open with continuously available protection (the value for the -
continuously-available field in vserver cifs session show command output is
Partial), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on Storage Virtual
Machines (SVMs) in summary form by using the vserver cifs session file show command
without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional -fields parameter to display output on the fields you choose.
  You can use this parameter either alone or in combination with other optional parameters.
- You can use the -instance parameter to display detailed information about open SMB files.
  You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display open SMB files...	Enter the following command...
On the SVM in summary form	**vserver cifs session file show -vserver** *vserver_name*
On a specified node	**vserver cifs session file show -vserver** *vserver_name* **-node {***node_name***|local}**
On a specified file ID	**vserver cifs session file show -vserver** *vserver_name* **-file-id** *integer*
On a specified SMB connection ID	**vserver cifs session file show -vserver** *vserver_name* **-connection-id** *integer*
On a specified SMB session ID	**vserver cifs session file show -vserver** *vserver_name* **-session-id** *integer*
On the specified hosting aggregate	**vserver cifs session file show -vserver** *vserver_name* **-hosting-aggregate** *aggregate_name*
On the specified volume	**vserver cifs session file show -vserver** *vserver_name* **-hosting-volume** *volume_name*
On the specified SMB share	**vserver cifs session file show -vserver** *vserver_name* **-share** *share_name*
On the specified SMB path	**vserver cifs session file show -vserver** *vserver_name* **-path** *path*

If you want to display open SMB files...	Enter the following command...
With the specified level of continuously available protection	**vserver cifs session file show -vserver *vserver_name* -continuously-available *continuously_available_status*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` **Note:** If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	**vserver cifs session file show -vserver *vserver_name* -reconnected *reconnected_state*** The value for `-reconnected` can be one of the following: • `No` • `Yes` **Note:** If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File       Open Hosting                Continuously
ID      Type       Mode Volume     Share        Available
------- --------- ---- --------- ----------- ------------
41      Regular    r    data      data         Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -
instance
```

```
                    Node: node1
                 Vserver: vs1
                 File ID: 82
           Connection ID: 104617
              Session ID: 1
               File Type: Regular
               Open Mode: rw
   Aggregate Hosting File: aggr1
      Volume Hosting File: data1
              CIFS Share: data1
     Path from CIFS Share: windows\win8\test\test.txt
              Share Mode: rw
             Range Locks: 1
   Continuously Available: Yes
             Reconnected: No
```

Determining which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Step

1. Perform one of the following actions:

If you want to determine...	Enter the following...
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show -object object_name`
Which counters are available at the admin privilege level	`statistics catalog counter show -object object_name`
Which counters are available at the advanced privilege level	`set -privilege advanced` `statistics catalog counter show -object object_name`

See the man pages for more information.

Examples

The following example displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster:

```
cluster1::> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng performance
                                counters

cluster1::> statistics catalog object show -object cifs
```

```
    cifs                          The CIFS object reports activity of the
                                  Common Internet File System protocol
                                  subsystem. This is the Microsoft file-sharing
                                  protocol that evolved from the Server Message
                                  Block (SMB) application layer network
                                  protocol to connect PCs to Network Attached
                                  Storage devices (NAS). This object reports
                                  activity for both SMB and SMB2 revisions of
                                  the CIFS protocol. For information related
                                  only to SMB, see the 'smb1' object. For
                                  information related only to SMB2, see the
                                  'smb2' object.

cluster1::> statistics catalog object show -object nblade_cifs
    nblade_cifs                   Exported counters associated with the
                                  N-Blade's CIFS subsystem and relevant to the
                                  entire node, rather than individual virtual
                                  servers.

cluster1::> statistics catalog object show -object smb1
    smb1                          These counters report activity from the SMB
                                  revision of the protocol. For information
                                  specific to SMB2, see the 'smb2' object. To
                                  see an overview across both revisions, see
                                  the 'cifs' object.

cluster1::> statistics catalog object show -object smb2
    smb2                          These counters report activity from the SMB2
                                  revision of the protocol. For information
                                  specific to SMB, see the 'smb1' object. To
                                  see an overview across both revisions, see
                                  the 'cifs' object.

cluster1::> statistics catalog object show -object hashd
    hashd                         The hashd object provides counters to measure
                                  the performance of the BranchCache hash
                                  daemon.
```

The following example displays information about some of the counters for the cifs object as seen at the advanced-privilege level:

Note: This example does not display all of the available counters for the cifs object. Output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when
directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                      Description
    --------------------------   --------------------------------------------
    active_searches              Number of active searches over SMB and SMB2
    auth_reject_too_many         Authentication refused after too many
                                 requests were made in rapid succession
    avg_directory_depth          Average number of directories crossed by SMB
                                 and SMB2 path-based commands
    avg_junction_depth           Average number of junctions crossed by SMB
                                 and SMB2 path-based commands
    branchcache_hash_fetch_fail  Total number of times a request to fetch hash
                                 data failed. These are failures when
                                 attempting to read existing hash data. It
                                 does not include attempts to fetch hash data
                                 that has not yet been generated.
    branchcache_hash_fetch_ok    Total number of times a request to fetch hash
                                 data succeeded.
```

```
          branchcache_hash_sent_bytes Total number of bytes sent to clients
                                      requesting hashes.
          branchcache_missing_hash_bytes
                                      Total number of bytes of data that had to be
                                      read by the client because the hash for that
                                      content was not available on the server.
          change_notifications_outstanding
                                      Number of active change notifications over
                                      SMB and SMB2
          cifs_latency                Average latency for CIFS operations
          cifs_latency_base           Total observed CIFS operations to be used as
                                      a base counter for CIFS average latency
                                      calculation
          cifs_ops                    Total number of CIFS operations
          cifs_read_ops               Total number of CIFS read operations
          cifs_write_ops              Total number of CIFS write operations

     [...]
```

Related tasks

Displaying statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

Before you begin

You must have collected data samples by using the statistics start and optional statistics stop commands before you can display information about objects. For more information about these commands, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Step

1. Perform one of the following actions:

If you want to display statistics for...	Enter the following command...
All versions of SMB	**statistics show -object cifs**
SMB 1.0	**statistics show -object smb1**
SMB 2.x and SMB 3.0	**statistics show -object smb2**
CIFS subsystem of the node	**statistics show -object nblade_cifs**
Multiprotocol audit	**statistics show -object audit_ng**
BranchCache hash service	**statistics show -object hashd**

See the man page for each command for more information.

Related tasks

Deploying CIFS client-based services

You can deploy a number of CIFS client-based services, such as accessing files in Snapshot copies using the Previous Versions Windows Properties tab; and configuring offline folders, roaming profiles, and folder redirection.

Using offline files to allow caching of files for offline use

Data ONTAP supports the Microsoft Offline Files feature, or *client-side caching*, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

• No caching
  Disables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.
• Manual caching
  Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.
• Automatic document caching
  Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.
• Automatic program caching

Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

Related concepts

Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM on page 272

Using folder redirection to store data on a CIFS server on page 273

Using BranchCache to cache SMB share content at a branch office on page 298

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Requirements for using offline files

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

Data ONTAP version requirements

Data ONTAP 8.2 and later releases support offline files.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports offline files on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports offline files on SMB 1.0.

Windows client requirements

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix at *support.netapp.com/matrix*.

Considerations when deploying offline files

There are some important considerations you need to understand when you deploy offline files on home directory shares that have the showsnapshot share property set on home directories.

If the showsnapshot share property is set on a home directory share that has offline files configured, Windows clients cache all of the Snapshot copies under the ~snapshot folder in the user's home directory.

Windows clients cache all of the Snapshot copies under the home directory if one of more of the following is true:

- The user makes the home directory available offline from the client.
  The contents of the ~snapshot folder in the home directory is included and made available offline.
- The user configures folder redirection to redirect a folder such as My Documents to the root of a home directory residing on the CIFS server share.
  Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the ~snapshot folder is included in the cached offline content.

Note: Offline file deployments where the ~snapshot folder is included in offline files should be avoided. The Snapshot copies in the ~snapshot folder contain all data on the volume at the point at which Data ONTAP created the Snapshot copy. Therefore, creating an offline copy of the ~snapshot folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.

Configuring offline files support on SMB shares using the CLI

You can configure offline files support using the Data ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

About this task

When configuring offline files support, you can choose one of the following four offline files settings:

Setting	Description
none	Disallows Windows clients from caching any files on this share.
manual	Allows users on Windows clients to manually select files to be cached.
documents	Allows Windows clients to cache user documents that are used by the user for offline access.
programs	Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

Steps

1. Perform the appropriate action:

If you want to configure offline files on...	Enter the command...
A new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none|manual|documents|programs}`
An existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none|manual|documents|programs}`

2. Verify that the SMB share configuration is correct:

   `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named "data1" with offline files set to
`documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path /
data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share vserver cifs share show -vserver vs1 -share-
name data1 -instance

                      Vserver: vs1
                        Share: data1
     CIFS Server NetBIOS Name: VS1
                         Path: /data1
             Share Properties: oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: Offline files
                    Share ACL: Everyone / Full Control
 File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: documents
 Vscan File-Operations Profile: standard
```

The following command modifies an existing SMB share named "data1" by changing the
offline files setting to `manual` and adding values for the file and directory mode creation
mask:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1 -
offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share vserver cifs share show -vserver vs1 -share-
```

```
name data1 -instance

                        Vserver: vs1
                          Share: data1
        CIFS Server NetBIOS Name: VS1
                           Path: /data1
               Share Properties: oplocks
                                 browsable
                                 changenotify
             Symlink Properties: enable
       File Mode Creation Mask: 644
 Directory Mode Creation Mask: 777
                  Share Comment: Offline files
                      Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: -
                    Volume Name: -
                  Offline Files: manual
  Vscan File-Operations Profile: standard
```

Related tasks

Creating an SMB share on a CIFS server on page 131
Adding or removing share properties on an existing SMB share on page 135

Configuring offline files support on SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer and select **Manage**.

2. On the left panel, select **Computer Management**.

3. Select **Action > Connect to another computer**.

The Select Computer dialog box appears.

4. Type the name of the CIFS server or click **Browse** to locate the CIFS server.

If the name of CIFS server is the same as the Storage Virtual Machine (SVM) host name, type the SVM name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click **OK**.

6. In the console tree, click **System Tools > Shared Folders**.

7. Click **Shares**.

8. In the results pane, right-click the share.

9. Click **Properties**.

   Properties for the share you selected are displayed.

10. In the **General** tab, click **Offline Settings**.

    The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.

12. Click **OK**.

Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM

Data ONTAP supports storing Windows roaming profiles on a CIFS server associated with the Storage Virtual Machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability
  A user's unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows Vista, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.
- Simplified computer replacement
  Because all of the user's profile information is maintained separately on the network, a user's profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

Related concepts

Requirements for using roaming profiles

Before you can use Microsoft's roaming profiles with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

Data ONTAP version requirements

Data ONTAP 8.2 and later support roaming profiles.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports roaming profiles on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports roaming profiles on SMB 1.0.

Windows client requirements

Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix at *support.netapp.com/matrix*.

Configuring roaming profiles

If you want to automatically make a user's profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server 2012, you can use the Active Directory Administration Center.

Steps

1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows 2012 and later servers).

2. Locate the user for which you want to configure a roaming profile.

3. Right-click the user and click **Properties**.

4. On the **Profile** tab, enter the profile path to the share where you want to store the user's roaming profile, followed by `%username%`.

   For example, a profile path might be the following: `\\vs1.example.com\profiles\ %username%`. The first time a user logs in, `%username%` is replaced with the user's name.

   Note: In the path `\\vs1.example.com\profiles\%username%`, `profiles` is the share name of a share on Storage Virtual Machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click **OK**.

Using folder redirection to store data on a CIFS server

Data ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

- `Documents`, `Desktop`, and `Start Menu` are examples of folders that you can redirect.
- Users can redirect folders from their Windows client.
- Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
- If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
- Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

Related concepts

Using offline files to allow caching of files for offline use on page 267
Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM on page 272

Requirements for using folder redirection

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of Data ONTAP and SMB and which Windows clients support the feature.

Data ONTAP version requirements

Clustered Data ONTAP 8.2 and later support Microsoft folder redirection.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports Microsoft's folder redirection on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports Microsoft's folder redirection on SMB 1.0.

Windows client requirements

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix at *support.netapp.com/matrix*.

Configuring folder redirection

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

Steps

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.

2. Click **Properties**.

   Properties for the share you selected are displayed.

3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.

   For example, if you want to redirect a folder to the `data` folder in a home directory that is mapped to `Q:\`, specify `Q:\data` as the target.

4. Click **OK**.

   For more information about configuring offline folders, consult the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](#)

How to access the ~snapshot directory from Windows clients using SMB 2.x

The method that you use to access the `~snapshot` directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the `~snapshot` directory when using SMB 2.x connections to successfully access data stored in Snapshot copies.

The SVM administrator controls whether users on Windows clients can view and access the `~snapshot` directory on a share by enabling or disabling the `showsnapshot` share property.

When the `showsnapshot` share property is disabled, a user on a Windows client using SMB 2.x cannot view the `~snapshot` directory and cannot access Snapshot copies within the `~snapshot` directory, even when manually entering the path to the `~snapshot` directory or to specific Snapshot copies within the directory.

When the `showsnapshot` share property is enabled, a user on a Windows client using SMB 2.x still cannot view the `~snapshot` directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden `~snapshot` directory by manually appending `\~snapshot` to the end of the share path. The hidden `~snapshot` directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden `~snapshot` directory is not accessible from non-junction subdirectories within the share.

> **Example**
>
> With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the "eng" share can access the `~snapshot` directory by manually appending `\~snapshot` to the share path at the root of the share and at every junction point in the path. The hidden `~snapshot` directory is accessible from the following three paths:

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume         junction-path
------- ------------   ----------------------------------------
vs1     vs1_root       /
vs1     vs1_vol1       /eng
vs1     vs1_vol2       /eng/projects1
vs1     vs1_vol3       /eng/projects2

cluster1::> vserver cifs share show
Vserver   Share   Path     Properties    Comment   ACL
--------  ------  -------  ----------    --------  ----------
vs1       eng     /eng     oplocks       -         Everyone / Full Control
                           changenotify
                           browsable
                           showsnapshot
```

Recovering files and folders using Previous Versions

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

Previous Versions functionality provides a method for users to browse through the Snapshot copies or to restore data from a Snapshot copy without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made Snapshot copies available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in Snapshot copies is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshot copies are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

Requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of Data ONTAP and SMB, and which Windows clients, support it. You also need to know about the Snapshot copy setting requirement.

Data ONTAP version requirements

Data ONTAP 8.2 and later supports Previous Versions.

SMB protocol version requirements

For Storage Virtual Machine (SVM) with FlexVol volumes, Data ONTAP supports Previous Versions on all versions of SMB.

For SVM with Infinite Volume, Data ONTAP supports Previous Versions on SMB 1.0.

Windows client requirements

Before a user can use Previous Versions to access data in Snapshot copies, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix at *support.netapp.com/matrix*.

Requirements for Snapshot copy settings

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

Using the Previous Versions tab to view and manage Snapshot copy data

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in Snapshot copies without needing to involve the Storage Virtual Machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in Snapshot copies of data stored on the SVM if the administrator has enabled Snapshot copies on the volume containing the share, and if the administrator configures the share to show Snapshot copies.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.

2. Right-click the file or folder in the mapped network drive whose Snapshot copies you want to view or manage.

3. Click **Properties**.

   Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

   A list of available Snapshot copies of the selected file or folder is displayed in the Folder versions: box. The listed Snapshot copies are identified by the Snapshot copy name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.

6. Perform the appropriate action:

If you want to...	Do the following...
View data from that Snapshot copy	Click **Open**.
Create a copy of data from that Snapshot copy	Click **Copy**.

   Data in Snapshot copies is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing Snapshot data, close the **Properties** dialog box by clicking **OK**.

   For more information about using the Previous Versions tab to view and manage Snapshot data, consult the Microsoft TechNet Library.

Related information

   Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Determining whether Snapshot copies are available for Previous Versions use

You can view Snapshot copies from the Previous Versions tab only if an enabled Snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to Snapshot copies. Determining Snapshot copy availability is helpful when assisting a user with Previous Versions access.

Steps

1. Determine whether the volume on which the share data resides has automatic Snapshot copies enabled and whether clients have access to Snapshot directories:

   ```
   volume show -vserver vserver-name -volume volume-name -fields
   vserver,volume,snapdir-access,snapshot-policy,snapshot-count
   ```

The output displays what Snapshot policy is associated with the volume, whether client Snapshot directory access is enabled, and the number of available Snapshot copies.

2. Determine whether the associated Snapshot policy is enabled:

volume snapshot policy show -policy *policy-name*

3. List the available Snapshot copies:

volume snapshot show -volume *volume_name*

For more information about configuring and managing Snapshot policies and Snapshot schedules, see the *Clustered Data ONTAP Data Protection Guide*.

Example

The following example displays information about Snapshot policies associated with the volume named "data1" that contains the shared data and available Snapshot copies on "data1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                  Number of Is
Policy Name       Schedules Enabled Comment
----------------- --------- ------- ----------------------------------
default                   3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule        Count     Prefix                SnapMirror Label
    --------------- -----     --------------------- -------------------
    hourly              6     hourly                -
    daily               2     daily                 daily
    weekly              2     weekly                weekly

cluster1::> volume snapshot show -volume data1
                                                    ---Blocks---
Vserver  Volume  Snapshot                 State       Size Total% Used%
-------- ------- ------------------------ -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015   valid      408KB    0%    1%
                 daily.2012-12-22_0010    valid      420KB    0%    1%
                 daily.2012-12-23_0010    valid      192KB    0%    0%
                 weekly.2012-12-23_0015   valid      360KB    0%    1%
                 hourly.2012-12-23_1405   valid      196KB    0%    0%
                 hourly.2012-12-23_1505   valid      196KB    0%    0%
                 hourly.2012-12-23_1605   valid      212KB    0%    0%
                 hourly.2012-12-23_1705   valid      136KB    0%    0%
                 hourly.2012-12-23_1805   valid      200KB    0%    0%
                 hourly.2012-12-23_1905   valid      184KB    0%    0%
```

Related tasks

Creating a Snapshot configuration to enable Previous Versions access

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

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated Snapshot policy, associate a Snapshot policy to the volume and enable it by using the `volume modify` command.

   For more information about using the `volume modify` command, see the man pages.

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

   For more information about using the `volume modify` command, see the man pages.

3. Verify that Snapshot policies are enabled and that access to Snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

   For more information about using the `volume show` and `volume snapshot policy show` commands, see the man pages.

   For more information about configuring and managing Snapshot policies and Snapshot schedules, see the *Clustered Data ONTAP Data Protection Guide*

Considerations when restoring directories that contain junctions

There are certain considerations you need to know about when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related concepts

Deploying CIFS server-based services

You can deploy a number of CIFS server-based services that can provide you with enhanced functionality for your CIFS deployment. CIFS server-based services include dynamic home directories, SMB access to UNIX symbolic links, BranchCache remote office caching, automatic node referrals, ODX copy offload, and folder security using access-based enumeration (ABE).

Managing home directories

You can use Data ONTAP home directory functionality to create users' home directories on the CIFS server and automatically offer each user a dynamic share to their home directory without creating an individual SMB share for each user.

How Data ONTAP enables dynamic home directories

Data ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the Storage Virtual Machine (SVM)).

There are four variables that determine how a user is mapped to a directory:

Share name   This is the name of the share that you create that the user connects to. It can be static (for example, home), dynamic (for example, %w), or a combination of the two. You must set the home directory property for this share.

The share name can use the following dynamic names:

- %w (the user's Windows user name)
- %d (the user's Windows domain name)
- %u (the user's mapped UNIX user name)

Share path   This is the relative path, defined by the share and therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, home), dynamic (for example, %w), or a combination of the two (for example, eng/%w).

Search paths   This is the set of absolute paths from the root of the SVM that you specify that directs the Data ONTAP search for home directories. You specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, Data ONTAP tries them in the order specified until it finds a valid path.

Directory   This is the user's home directory that you create for the user. It is usually the user's name. You must create it in one of the directories defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home - share path: `%w`
- Home directory share name #2: `%w` - share path: `%d/%w`
- Search path #1: `/aggr0home/home`
- Search path #2: `/aggr1home/home`
- Search path #3: `/aggr2home/home`
- Home directory: `/aggr1home/home/jsmith`

Scenario 1: The user connects to `\\vs1\home`. This matches the first home directory share name and generates the relative path `jsmith`. Data ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/aggr0home/home/jsmith` does not exist; moving on to search path #2.
- `/aggr1home/home/jsmith` does exist, therefore search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. Data ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/aggr0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/aggr1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/aggr2home/home/acme/jsmith` does not exist; the home directory does not exist, therefore the connection fails.

Related tasks

Adding a home directory share

If you want to use the SMB home directory feature, you must add at least one share with the home directory property included in the share properties.

About this task

You can create a home directory share at the time you create the share using the `vserver cifs share create` command, or you can change an existing share into a home directory share at any time using the `vserver cifs share modify` command.

To create a home directory share, you must include the `homedirectory` value in the `-share-properties` option when you create or modify a share. You can specify the share name and share path using variables that are dynamically expanded when the user connects to their home directory. Available variables that you can use in the path are `%w`, `%d`, and `%u`, corresponding to the Windows user name, domain, and mapped UNIX user name respectively.

Steps

1. Add a home directory share by entering the following command:

   `vserver cifs share create -vserver vserver -share-name share_name -path path -share-properties homedirectory[,...]`

   `-vserver vserver` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

   `-share-name share-name` specifies the home directory share name.

   `-path path` specifies the relative path to the home directory.

   `-share-properties homedirectory[,...]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

2. Verify that you successfully added the home directory share using the `vserver cifs share show` command.

Example

The following command creates a home directory share named %w. The `oplocks`, `browsable`, and `changenotify` share properties are set in addition to setting the `homedirectory` share property:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w -
share-properties oplocks,browsable,changenotify,homedirectory


vs1::> vserver cifs share show -vserver vs1 -share-name %w
Vserver     Share     Path          Properties      Comment  ACL
----------  --------  ------------  --------------  --------  -----------
```

```
vs1        %w        %w         oplocks         -         Everyone / Full
Control

                                browsable
                                changenotify
                                homedirectory
```

Related concepts

Related tasks

Adding a home directory search path

If you want to use Data ONTAP SMB home directories, you must add at least one home directory search path.

About this task

You can add a home directory search path by using the `vserver cifs home-directory search-path add` command.

The `vserver cifs home-directory search-path add` command checks the path specified in the `-path` option during command execution. If the specified path does not exist, the command generates a message prompting for whether you want to continue. You choose **y** or **n**. If you choose **y** to continue, Data ONTAP creates the search path. However, you must create the directory structure before you can use the search path in the home directory configuration. If you choose not to continue, the command fails; the search path is not created. You can then create the path directory structure and rerun the `vserver cifs home-directory search-path add` command.

Steps

1. Add a home directory search path by entering the following command:

    vserver cifs home-directory search-path add -vserver *vserver* -path *path*

    `-vserver *vserver*` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

    `-path *path*` specifies the directory path to the search path.

2. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

> **Example**
>
> The following example adds the path /home1 to the home directory configuration on SVM vs1.
>
> ```
> cluster::> vserver cifs home-directory search-path add -vserver vs1
> -path /home1
>
> vs1::> vserver cifs home-directory search-path show
> Vserver     Position Path
> ----------- -------- -----------------
> vs1          1        /home1
> ```
>
> The following example attempts to add the path /home2 to the home directory configuration on SVM vs1. The path does not exist. The choice is made to not continue.
>
> ```
> cluster::> vserver cifs home-directory search-path add -vserver vs1
> -path /home2
> Warning: The specified path "/home2" does not exist in the namespace
>          belonging to Vserver "vs1".
> Do you want to continue? {y|n}: n
> ```

Related concepts

[How Data ONTAP enables dynamic home directories](#) on page 281

Related tasks

[Adding a home directory share](#) on page 283

Creating a home directory configuration using the %w and %d variables

You can create a home directory configuration using the %w and %d variables. Users can then connect to their home share using dynamically created shares.

Steps

1. Optional: Create a qtree to contain user's home directories by entering the following command:

   volume qtree create -vserver *vserver_name* -qtree-path *qtree_path*

2. Optional: Verify that the qtree is using the correct security style by entering the following command:

   volume qtree show

3. Optional: If the qtree is not using the desired security style, change the security style using the volume qtree security command.

4. Add a home directory share by entering the following command:

`vserver cifs share create -vserver vserver -share-name %w -path %d/%w - share-properties homedirectory[,...]`

`-vserver vserver` specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

`-share-name %w` specifies the home directory share name. Data ONTAP dynamically creates the share name as each user connects to their home directory. The share name will be of the form *windows_user_name*.

`-path %d/%w` specifies the relative path to the home directory. The relative path is dynamically created as each user connects to their home directory and will be of the form *domain/windows_user_name*.

`-share-properties homedirectory[,...]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.

6. Add a home directory search path by entering the following command:

`vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver` specifies the CIFS-enabled SVM on which to add the search path.

`-path path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

8. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

For example, if you created a qtree with the path of `/vol/vol1/users` and the user name whose directory you want to create is mydomain\user1, you would create a directory with the following path: `/vol/vol1/users/mydomain/user1`.

If you created a volume named "home1" mounted at `/home1`, you would create a directory with the following path: `/home1/mydomain/user1`.

9. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

For example, if user mydomain\user1 wants to connect to the directory created in Step 8 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %d/%w.
- The search path that is used to contain the home directories, /home1, is a volume configured with NTFS security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from Windows hosts. You can also use this type of configuration when users access their home directories from Windows and UNIX hosts and the file system administrator uses Windows-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                        Vserver: vs1
                          Share: %w
       CIFS Server NetBIOS Name: VS1
                           Path: %d/%w
               Share Properties: oplocks
                                 browsable
                                 changenotify
                                 homedirectory
             Symlink Properties: enable
        File Mode Creation Mask: -
   Directory Mode Creation Mask: -
                  Share Comment: -
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                    Volume Name: -
                  Offline Files: manual
   Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /
home1

cluster::> vserver cifs home-directory search-path show
Vserver      Position Path
----------- -------- ----------------
vs1          1        /home1
```

Related concepts

[Additional home directory configurations](#) on page 291

Related tasks

[Configuring home directories using the %u variable](#) on page 288

Configuring home directories using the %u variable

You can create a home directory configuration where you designate the share name using the `%w` variable but you use the `%u` variable to designate the relative path to the home directory share. Users can then connect to their home share using dynamically shares created using their Windows user name without being aware of the actual name or path of the home directory.

Steps

1. Optional: Create a qtree to contain user's home directories by entering the following command:

   volume qtree create -vserver *vserver_name* -qtree-path *qtree_path*

2. Optional: Verify that the qtree is using the correct security style by entering the following command:

   volume qtree show

3. Optional: If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.

4. Add a home directory share by entering the following command:

   vserver cifs share create -vserver *vserver* -share-name %w -path %u - share-properties homedirectory ,...]

   `-vserver` *vserver* specifies the CIFS-enabled Storage Virtual Machine (SVM) on which to add the search path.

   `-share-name` `%w` specifies the home directory share name. The share name is dynamically created as each user connects to their home directory and is of the form *windows_user_name*.

   > **Note:** You can also use the `%u` variable for the `-share-name` option. This creates a relative share path that uses the mapped UNIX user name.

   `-path` `%u` specifies the relative path to the home directory. The relative path is created dynamically as each user connects to their home directory and is of the form *mapped_UNIX_user_name*.

   > **Note:** The value for this option can contain static elements as well. For example, `eng/%u`.

   `-share-properties homedirectory[,...]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.

6. Add a home directory search path by entering the following command:

   vserver cifs home-directory search-path add -vserver *vserver* -path *path*

   `-vserver` *vserver* specifies the CIFS-enabled SVM on which to add the search path.

-path `path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

8. Optional: If the UNIX user does not exist, create the UNIX user using the `vserver services unix-user create` command.

   Note: The UNIX user name to which you map the Windows user name must exist before mapping the user.

9. Optional: Create a name mapping for the Windows user to the UNIX user using the following command:

   vserver name-mapping create -vserver *vserver_name* **-direction** *win-unix* **-priority** *integer* **-pattern** *windows_user_name* **-replacement** *unix_user_name*

   Note: If name mappings already exist that map Windows users to UNIX users, you do not have to perform the mapping step.

   The Windows user name is mapped to the corresponding UNIX user name. When the Windows user connects to their home directory share, they connect to a dynamically created home directory with a share name that corresponds to their Windows user name without being aware that the directory name corresponds to the UNIX user name.

10. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

    For example, if you created a qtree with the path of `/vol/vol1/users` and the mapped UNIX user name of the user whose directory you want to create is "unixuser1", you would create a directory with the following path: `/vol/vol1/users/unixuser1`.

    If you created a volume named "home1" mounted at `/home1`, you would create a directory with the following path: `/home1/unixuser1`.

11. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

    For example, if user mydomain\user1 maps to UNIX user unixuser1 and wants to connect to the directory created in Step 10 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %u.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with UNIX security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from both Windows hosts or Windows and UNIX hosts and the file system administrator uses UNIX-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                       Vserver: vs1
                         Share: %w
       CIFS Server NetBIOS Name: VS1
                          Path: %u
              Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
            Symlink Properties: enable
        File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                 Share Comment: -
                     Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                   Volume Name: -
                 Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /
home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5         Pattern: user1
                                   Replacement: unixuser1
```

Related concepts

Related tasks

Additional home directory configurations

You can create additional home directory configurations using the %w, %d, and %u variables, which enables you to customize the home directory configuration to meet your needs.

You can create a number of home directory configurations using a combination of variables and static share names and variables and static search paths. The following table provides some examples illustrating how you use variables and static names to create different home directory configurations:

Paths created when `/vol/vol1/user` contains home directories...	Share command...
To create a share path \\vs1\~ that directs the user to `/vol/vol1/user/win_username`	`vserver cifs share create -share-name ~ -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path \\vs1\cifs.homedir that directs the user to `/vol/vol1/user/win_username`	`vserver cifs share create -share-name CIFS.HOMEDIR -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path \\vs1\~win_username that directs the user to `/vol/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path \\vs1\win_username that directs the user to `/vol/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path \\vs1\win_username that directs the user to `/vol/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path \\vs1\unix_username that directs the user to `/vol/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Home directory shares require unique user names

Be careful to assign unique user names when creating home directory shares using the %w (Windows user name) or %u (UNIX user name) variables to generate shares dynamically. The share name is mapped to your user name.

Two problems can occur when a static share's name and a user's name are the same:

*   When the user lists the shares on a cluster using the net view command, two shares with the same user name are displayed.
*   When the user connects to that share name, the user is always connected to the static share and cannot access the home directory share with the same name.

For example, there is a share named "administrator" and you have an "administrator" Windows user name. If you create a home directory share and connect to that share, you get connected to the "administrator" static share, not to your "administrator" home directory share.

You can resolve the issue with duplicate share names by following any of these steps:

*   Renaming the static share so that it no longer conflicts with the user's home directory share.
*   Giving the user a new user name so that it no longer conflicts with the static share name.
*   Creating a CIFS home directory share with a static name such as "home" instead of using the %w parameter to avoid conflicts with the share names.

Commands for managing search paths

There are specific Data ONTAP commands for managing search paths for CIFS home directory configurations. For example, there are commands for adding, removing, and displaying information about search paths. There is also a command for changing the search path order.

If you want to...	Use this command...
Add a search path	vserver cifs home-directory search-path add
Display search paths	vserver cifs home-directory search-path show
Change the search path order	vserver cifs home-directory search-path reorder
Remove a search path	vserver cifs home-directory search-path remove

See the man page for each command for more information.

Configuring SMB client access to UNIX symbolic links

You can configure the CIFS server to provide SMB client access to UNIX symbolic links. The symbolic links can point to files within the volume that contain the share, or to files that are contained in other volumes on the Storage Virtual Machine (SVM), or even to volumes contained on other SVMs.

How Data ONTAP enables you to provide SMB client access to UNIX symbolic links

You must understand certain concepts about how Data ONTAP enables you to manage symbolic links. This is important to provide access to SMB users connecting to the Storage Virtual Machine (SVM).

A symbolic link is a file created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, it is redirected to the target file or directory that the symbolic link refers to.

Data ONTAP provides SMB clients the ability to follow UNIX symbolic links configured on the SVM. This feature is optional and you can configure it on a per-share basis with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

There are two types of symbolic links:

Relative   A relative symbolic link contains a reference to the file or directory relative to its parent directory. Therefore, the path of the file it is referring to should not begin with a slash (/). A relative symbolic link always refers to a file or directory within the same file system. If you enable symbolic links on a share, relative symbolic links work without further configuration.

Absolute   An absolute symbolic link contains a reference to a file or directory in the form of an absolute path. Therefore, the path of the file it is referring to should begin with a slash (/). It is treated as an absolute path location of the file from the root of the file system. An absolute symbolic link can refer to a file or directory within or outside of the file system of the symbolic link. If the target is not in the same local file system, the symbolic link is called a *widelink*. If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination CIFS path. When creating absolute symbolic link mappings, you specify whether it is a local or widelink. If you create an

absolute symbolic link to a file or directory outside of the local share but set the locality to local, Data ONTAP disallows access to the target.

Note that if a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory that the widelink refers to. Data ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

Related concepts

Limits when configuring UNIX symbolic links for SMB access

You need to be aware of certain limits when configuring UNIX symbolic links for SMB access.

Limit	Description
45	Maximum length of the CIFS server name that you can specify when using an FQDN for the CIFS server name. **Note:** You can alternatively specify the CIFS server name as a NetBIOS name, which is limited to 15 characters.
80	Maximum length of the share name.
256	Maximum length of the UNIX path that you can specify when creating a symbolic link or when modifying an existing symbolic link's UNIX path. The UNIX path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.
256	Maximum length of the CIFS path that you can specify when creating a symbolic link or when modifying an existing symbolic link's CIFS path. The CIFS path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.
2048	Maximum number of symbolics links you can create per Storage Virtual Machine (SVM).

Related tasks

Configuring UNIX symbolic link support on SMB shares

You can configure UNIX symbolic link support on SMB shares by specifying a symbolic link share-property setting when you create SMB shares or at any time by modifying existing SMB shares.

UNIX symbolic link support is enabled by default. You can also disable UNIX symbolic link support on a share.

About this task

When configuring UNIX symbolic link support for SMB shares, you can choose one of the following settings:

Setting	Description
`enable`	This setting specifies that symbolic links are enabled for read-write access. This is the default setting.
`enable,read_only`	This setting specifies that symbolic links are enabled for read-only access. This setting is the only multiple-value setting allowed. For example, `hide,read_only` is not a valid setting.
`hide`	This setting specifies that SMB clients are prevented from seeing symbolic links.
`""` (null, not set)	This setting disables symbolic links on the share.
`–` (not set)	This setting disables symbolic links on the share.

Steps

1. Perform the appropriate action:

If you want to...	Enter the command...
Configure or disable symbolic link support on a new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable|hide| read_only|""|-},...]`
Configure or disable symbolic link support on an existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable|hide|read_only|""|-},...]`

2. Verify that the SMB share configuration is correct:
   `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

> **Example**
>
> The following command creates an SMB share named "data1" with the UNIX symbolic link configuration set to `enable`:
>
> ```
> cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path /
> data1 -symlink-properties enable
> ```

```
cluster1::> vserver cifs share vserver cifs share show -vserver vs1 -share-
name data1 -instance

                      Vserver: vs1
                        Share: data1
      CIFS Server NetBIOS Name: VS1
                         Path: /data1
             Share Properties: oplocks
                               browsable
                               changenotify
            Symlink Properties: enable
       File Mode Creation Mask: -
  Directory Mode Creation Mask: -
                 Share Comment: -
                     Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: -
                   Volume Name: -
                 Offline Files: manual
  Vscan File-Operations Profile: standard
```

Related tasks

Creating symbolic link mappings for SMB shares

You can create mappings of UNIX symbolic links for SMB shares. You can either create a relative symbolic link, which refers to the file or folder relative to its parent folder, or you can create an absolute symbolic link, which refers to the file or folder using an absolute path.

About this task

Widelinks are not accessible from Mac OS X clients. When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails.

Step

1. To create symbolic link mappings for SMB shares, enter the following command:

   vserver cifs symlink create -vserver *virtual_server_name* -unix-path *path* -share-name *share_name* -cifs-path *path* [-cifs-server *server_name*] [-locality {local|widelink}] [-home-directory {true|false}]

   -vserver *virtual_server_name* specifies the Storage Virtual Machine (SVM) name.

   -unix-path *path* specifies the UNIX path. The UNIX path must begin with a slash (/) and must end with a slash (/).

   -share-name *share_name* specifies the name of the SMB share to map.

   -cifs-path *path* specifies the CIFS path. The CIFS path must begin with a slash (/) and must end with a slash (/).

-cifs-server *server_name* specifies the CIFS server name. The CIFS server name can be specified as a DNS name (for example, mynetwork.cifs.server.com), IP address, or NetBIOS name. The NetBIOS name can be determined by using the vserver cifs show command. If this optional parameter is not specified, the default value is the NetBIOS name of the local CIFS server.

-locality {local|widelink} specifies whether to create a local or wide symbolic link. A local symbolic link maps to the local SMB share, and a wide symbolic link maps to any SMB share on the network. If you do not specify this optional parameter, the default value is widelink.

-home-directory {true|false} specifies whether the target share is a home directory. Even though this parameter is optional, you must set this parameter to true when the target share is configured as a home directory. The default is false.

Example

The following command creates a symbolic link mapping on the SVM named vs1. It has the UNIX path /src/, the SMB share name "SOURCE", the CIFS path /mycompany/source/, and the CIFS server IP address 123.123.123.123, and it is a widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/ -
share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Related concepts

How Data ONTAP enables you to provide SMB client access to UNIX symbolic links on page 293

Related tasks

Configuring UNIX symbolic link support on SMB shares on page 294

Commands for managing symbolic link mappings

There are specific Data ONTAP commands for managing symbolic link mappings.

If you want to...	Use this command...
Create a symbolic link mapping	vserver cifs symlink create
Display information about symbolic link mappings	vserver cifs symlink show
Modify a symbolic link mapping	vserver cifs symlink modify
Delete a symbolic link mapping	vserver cifs symlink delete

See the man page for each command for more information.

Using BranchCache to cache SMB share content at a branch office

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. The Data ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on Storage Virtual Machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

Related concepts

Requirements, considerations, and recommendations

Before you can use the BranchCache feature with your Storage Virtual Machine (SVM) with FlexVol volumes, you need to be aware of certain requirements, considerations, and recommendations. For example, you need to know about Data ONTAP support for the feature. You also need to know about SMB version support and about supported Windows hosts.

Related tasks

BranchCache version support

You should be aware of which BranchCache versions Data ONTAP supports.

Data ONTAP supports BranchCache 1 and the enhanced BranchCache 2:

- When you configure BranchCache on the CIFS server for the Storage Virtual Machine (SVM), you can enable BranchCache 1, BranchCache 2, or all versions.
  By default, all versions are enabled.
- If you enable only BranchCache 2, the remote office Windows client machines must support BranchCache 2.
  Only SMB 3.0 or later clients support BranchCache 2.

For more information about BranchCache versions, see the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](technet.microsoft.com/en-us/library/)

Network protocol support requirements

You must be aware of the network protocol requirements for implementing Data ONTAP BranchCache.

You can implement the Data ONTAP BranchCache feature over IPv4 and IPv6 networks using SMB 2.1 or later.

All CIFS servers and branch office machines participating in the BranchCache implementation must have the SMB 2.1 or later protocol enabled. SMB 2.1 has protocol extensions that allow a client to participate in a BranchCache environment. This is the minimum SMB protocol version that offers BranchCache support. SMB 2.1 supports version BranchCache version 1.

If you want to use BranchCache version 2, SMB 3.0 is the minimum supported version. All CIFS servers and branch office machines participating in a BranchCache 2 implementation must have SMB 3.0 or later enabled.

If you have remote offices where some of the clients support only SMB 2.1 and some of the clients support SMB 3.0, you can implement a BranchCache configuration on the CIFS server that provides caching support over both BranchCache 1 and BranchCache 2.

Note: Even though the Microsoft BranchCache feature supports using both the HTTP/HTTPS and SMB protocols as file access protocols, Data ONTAP BranchCache only supports the use of SMB.

Data ONTAP and Windows hosts version requirements

Data ONTAP and branch office Windows hosts must meet certain version requirements before you can configure BranchCache.

Before configuring BranchCache, you must ensure that the version of Data ONTAP on the cluster and participating branch office clients support SMB 2.1 or later and support the BranchCache feature. If you configure Hosted Cache mode, you must also ensure that you use a supported host for the cache server.

BranchCache 1 is supported on the following Data ONTAP versions and Windows hosts:

- Content server: Storage Virtual Machine (SVM) with Data ONTAP 8.2 or later
- Cache server: Windows Server 2008 R2 or Windows Server 2012 or later
- Peer or client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 or Windows Server 2012 or later

BranchCache 2 is supported on the following Data ONTAP versions and Windows hosts:

- Content server: SVM with Data ONTAP 8.2 or later
- Cache server: Windows Server 2012 or later
- Peer or client: Windows 8 or Windows Server 2012 or later

For the latest information about which Windows clients support BranchCache, see the Interoperability Matrix at *support.netapp.com/matrix*.

Reasons Data ONTAP invalidates BranchCache hashes

Understanding the reasons why Data ONTAP invalidates hashes can be helpful as you plan your BranchCache configuration. It can help you decide which operating mode you should configure and can help you choose on which shares to enable BranchCache.

Data ONTAP must manage BranchCache hashes to ensure that hashes are valid. If a hash is not valid, Data ONTAP invalidates the hash and computes a new hash the next time that content is requested, assuming that BranchCache is still enabled.

Data ONTAP invalidates hashes for the following reasons:

- The server key is modified.
  If the server key is modified, Data ONTAP invalidates all hashes in the hash store.
- A hash is flushed from the cache because the BranchCache hash store maximum size has been reached.
  This is a tunable parameter and can be modified to meet your business requirements.
- A file is modified either through SMB or NFS access.
- A file for which there are computed hashes is restored using the snap restore command.
- A volume that contains SMB shares that are BranchCache-enabled is restored using the snap restore command.

Considerations when choosing the hash store location

When configuring BranchCache, you choose where to store hashes and what size the hash store should be. Understanding certain considerations when choosing the hash store location and size can help you plan your BranchCache configuration on a CIFS-enabled Storage Virtual Machine (SVM).

- You should locate the hash store on a volume where atime updates are permitted.
  The access time on a hash file is used to keep frequently accessed files in the hash store. If atime updates are disabled, the creation time is used for this purpose. It is preferable to use atime to track frequently used files.
- You cannot store hashes on read-only file systems such as SnapMirror destinations and SnapLock volumes.
- If the maximum size of the hash store is reached, older hashes are flushed to make room for new hashes.
  You can increase the maximum size of the hash store to reduce the amount of hashes that are flushed from the cache.
- If the volume on which you store hashes is unavailable or full, or if there is an issue with intra-cluster communication where the BranchCache service cannot retrieve hash information, BranchCache services are not available.
  The volume might be unavailable because it is offline or because the storage administrator specified a new location for the hash store.

This does not cause issues with file access. If access to the hash store is impeded, Data ONTAP returns a Microsoft-defined error to the client, which causes the client to request the file using the normal SMB read request.

Related concepts

Managing and monitoring the BranchCache configuration on page 310

Related tasks

Configuring BranchCache on the CIFS server on page 302

BranchCache recommendations

Before you configure BranchCache, there are certain recommendations you should keep in mind when deciding on which SMB shares you want to enable BranchCache caching.

You should keep the following recommendations in mind when deciding on which operating mode to use and on which SMB shares to enable BranchCache:

- The benefits of BranchCache are reduced when the data to be remotely cached changes frequently.
- BranchCache services are beneficial for shares containing file content that is reused by multiple remote office clients or by file content that is repeatedly accessed by a single remote user.
- Consider enabling caching for read-only content such as data in Snapshot copies and SnapMirror destinations.

Configuring BranchCache

You configure BranchCache on your CIFS server using Data ONTAP commands. To implement BranchCache, you must also configure your clients, and optionally your hosted cache servers at the branch offices where you want to cache content.

If you configure BranchCache to enable caching on a share-by-share basis, you must enable BranchCache on the SMB shares for which you want to provide BranchCache caching services.

Prerequisites for configuring BranchCache

After meeting some prerequisites, you can set up BranchCache.

The following requirements must be met before configuring BranchCache on the CIFS server for your Storage Virtual Machine (SVM):

- Data ONTAP 8.2 or later must be installed on all nodes in the cluster.
- CIFS must be licensed and a CIFS server must be configured.
- IPv4 or IPv6 network connectivity must be configured.
- For BranchCache 1, SMB 2.1 or later must be enabled.
- For BranchCache 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

Configuring BranchCache on the CIFS server

You can configure BranchCache to provide BranchCache services on a per-share basis.
Alternatively, you can configure BranchCache to automatically enable caching on all SMB shares.

About this task

You can configure BranchCache on SVMs with FlexVol volumes.

- You can create an all-shares BranchCache configuration if want to offer caching services for all
  content contained within all SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for
  content contained within selected SMB shares on the CIFS server.

You must specify the following parameters when configuring BranchCache:

Required parameters	Description
SVM name	BranchCache is configured on a per SVM basis. You must specify on which CIFS-enabled SVM you want to configure the BranchCache service.
Path to hash store	BranchCache hashes are stored in regular files on the SVM volume. You must specify the path to an existing directory where you want Data ONTAP to store the hash data.
	The destination path must be read-writable. Read-only paths, such as Snapshot directories are not allowed. You can store hash data in a volume that contains other data or you can create a separate volume to store hash data.
	The BranchCache hash path can contain blanks and any valid file name characters.

You can optionally specify the following parameters:

Optional parameters	Description
Supported Versions	Data ONTAP support BranchCache 1 and 2. You can enable version 1, version 2, or both versions. The default is to enable both versions.
Maximum size of hash store	You can specify the size to use for the hash data store. If the hash data exceeds this value, Data ONTAP deletes older hashes to make room for newer hashes. The default size for the hash store is 1 GB.
	BranchCache performs more efficiently if hashes are not discarded in an overly aggressive manner. If you determine that hashes are discarded frequently because the hash store is full, you can increase the hash store size by modifying the BranchCache configuration.

Optional parameters	Description
Server key	You can specify a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you do not specify a server key, one is randomly generated when you create the BranchCache configuration. You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.
Operating mode	The default is to enable BranchCache on a per-share basis. • To create a BranchCache configuration where you enable BranchCache on a per-share basis, you can either not specify this optional parameter or you can specify `per-share`. • To automatically enable BranchCache on all shares, you must set the operating mode to `all-shares`.

Steps

1. Enable SMB 2.1 and 3.0 as needed:

    a) Set the privilege level to advanced:

    `set -privilege advanced`

    b) Check the configured SVM SMB settings to determine whether all needed versions of SMB are enabled:

    `vserver cifs options show -vserver vserver_name`

    c) If necessary, enable SMB 2.1:

    `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

    The command enables both SMB 2.0 and SMB 2.1.

    d) If necessary, enable SMB 3.0:

    `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

    e) Return to the admin privilege level:

    `set -privilege admin`

2. Configure BranchCache:

    `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

The specified hash storage path must exist and must reside on a volume managed by the SVM. The path must also be located on a read-writable volume. The command fails if the path is read-only or does not exist.

If you want to use the same server key for additional SVM BranchCache configurations, record the value you enter for the server key. The server key does not appear when you display information about the BranchCache configuration.

3. Verify that the BranchCache configuration is correct:

   vserver cifs branchcache show -vserver *vserver_name*

Examples

The following commands verify that both SMB 2.1 and 3.0 are enabled and configure BranchCache to automatically enable caching on all SMB shares on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1

                                          Vserver: vs1
                              Default UNIX User: pcuser
                  Read Grants Exec for Mode Bits: disabled
    Windows Internet Name Service (WINS) Addresses: -
                Enable/Disable all SMB2 Protocols: true
                 Enable/Disable the SMB3 Protocol: true
Maximum Simultaneous Operations per TCP Connection: 255
        Maximum Depth of Directories to Shadow Copy: 5
            Enable/Disable the Copy Offload Feature: true
                              Default UNIX Group: -
      Enable/Disable the Shadow Copy Feature (VSS): true
                Refer Clients to More Optimal LIFs: false
            Enable/Disable Local User Authentication: true
               Enable/Disable Local Users and Groups: true
                Enable/Disable Reparse Point Support: true
            Enable/Disable Export Policies for CIFS: false
Enable/Disable Enumeration of Trusted Domain and Search Capability: true
Size of File System Sector Reported to SMB Clients (bytes): 4096

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /
hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                   Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
              Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

The following commands verify that both SMB 2.1 and 3.0 are enabled, configure BranchCache to enable caching on a per-share basis on SVM vs1, and verify the BranchCache configuration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1

                                         Vserver: vs1
                              Default UNIX User: pcuser
                    Read Grants Exec for Mode Bits: disabled
    Windows Internet Name Service (WINS) Addresses: -
                 Enable/Disable all SMB2 Protocols: true
                  Enable/Disable the SMB3 Protocol: true
Maximum Simultaneous Operations per TCP Connection: 255
       Maximum Depth of Directories to Shadow Copy: 5
            Enable/Disable the Copy Offload Feature: true
                                 Default UNIX Group: -
       Enable/Disable the Shadow Copy Feature (VSS): true
                 Refer Clients to More Optimal LIFs: false
            Enable/Disable Local User Authentication: true
               Enable/Disable Local Users and Groups: true
                Enable/Disable Reparse Point Support: true
             Enable/Disable Export Policies for CIFS: false
Enable/Disable Enumeration of Trusted Domain and Search Capability: true
Size of File System Sector Reported to SMB Clients (bytes): 4096

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /
hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related concepts

Related tasks

Where to find information about configuring BranchCache at the remote office

After configuring BranchCache on the CIFS server, you must install and configure BranchCache on client computers and, optionally, on caching servers at your remote office. Microsoft provides instructions for configuring BranchCache at the remote office.

Instructions for configuring branch office clients and, optionally, caching servers to use BranchCache are on the Microsoft BranchCache web site at *Microsoft BranchCache: technet.microsoft.com/EN-US/NETWORK/DD425028*.

Configuring BranchCache-enabled SMB shares

After you configure BranchCache on the CIFS server and at the branch office, you can enable BranchCache on SMB shares that contain content that you want to allow clients at branch offices to cache.

BranchCache caching can be enabled on all SMB shares on the CIFS server or on a share-by-share basis.

- If you enable BranchCache on a share-by-share basis, you can enable BranchCache as you create the share or by modifying existing shares.
  If you enable caching on an existing SMB share, Data ONTAP begins computing hashes and sending metadata to clients requesting content as soon as you enable BranchCache on that share.
- Any clients that have an existing SMB connection to a share do not get BranchCache support if BranchCache is subsequently enabled on that share.
  Data ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.

Note: If BranchCache on a SMB share is subsequently disabled, Data ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server).

Creating a BranchCache-enabled SMB share

You can enable BranchCache on an SMB share when you create the share by setting the `branchcache` share property.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.
  This is the default setting when you create a share.

- You can also specify additional optional share parameters when you create the BranchCache-enabled share.
- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the Storage Virtual Machine (SVM).
  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.
- Since there are no default share properties applied to the share when you use the `-share-properties` parameter, you must specify all other share properties that you want applied to the share in addition to the `branchcache` share property by using a comma-delimited list.
- For more information, see the man page for the `vserver cifs share create` command.

Steps

1. Create a BranchCache-enabled SMB share:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties branchcache[,...]

   - `-path` *path* specifies the path to the share.
   - Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes.

2. Verify that the BranchCache share property is set on the SMB share by using the `vserver cifs share show` command.

Example

The following command creates a BranchCache-enabled SMB share named "data" with a path of /data on SVM vs1. By default, the offline files setting is set to `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /
data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name
data
                      Vserver: vs1
                        Share: data
       CIFS Server NetBIOS Name: VS1
                         Path: /data
              Share Properties: branchcache
                                oplocks
                                browsable
                                changenotify
            Symlink Properties: enable
        File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Related tasks

Enabling BranchCache on an existing SMB share

You can enable BranchCache on an existing SMB share by adding the `branchcache` share property to the existing list of share properties.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.

  If the existing share's offline files setting is not set to manual caching, you must configure it by modifying the share.
- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the Storage Virtual Machine (SVM).

  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.
- When you add the `branchcache` share property to the share, existing share settings and share properties are preserved.

  The BranchCache share property is added to the existing list of share properties. For more information about using the `vserver cifs share properties add` command, see the man pages.

Steps

1. If necessary, configure the offline files share setting for manual caching:

   a) Determine what the offline files share setting is by using the `vserver cifs share show` command.

   b) If the offline files share setting is not set to manual, change it to the required value:

   vserver cifs share modify -vserver *vserver_name* -share-name *share_name* -offline-files manual

2. Enable BranchCache on an existing SMB share:

   vserver cifs share properties add -vserver *vserver_name* -share-name *share_name* -share-properties branchcache

3. Verify that the BranchCache share property is set on the SMB share:

   vserver cifs share show -vserver *vserver_name* -share-name *share_name*

Example

The following command enables BranchCache on an existing SMB share named "data2" with a path of /data2 on SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                         Vserver: vs1
                           Share: data2
        CIFS Server NetBIOS Name: VS1
                            Path: /data2
                Share Properties: oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
               Symlink Properties: -
         File Mode Creation Mask: -
    Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
     File Attribute Cache Lifetime: 10s
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                         Vserver: vs1
                           Share: data2
        CIFS Server NetBIOS Name: VS1
                            Path: /data2
                Share Properties: oplocks
                                  browsable
                                  showsnapshot
                                  changenotify
                                  branchcache
               Symlink Properties: -
         File Mode Creation Mask: -
    Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
     File Attribute Cache Lifetime: 10s
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
```

Related tasks

Managing and monitoring the BranchCache configuration

You manage the BranchCache configuration by modifying BranchCache parameters, changing the server secret key, configuring BranchCache to pre-compute hashes, flushing the hash cache, and configuring BranchCache GPOs. You can also display information about BranchCache statistics.

Related concepts

Considerations when choosing the hash store location on page 300

Modifying BranchCache configurations

You can modify the configuration of the BranchCache service on Storage Virtual Machines (SVMs), including changing the hash store directory path, the hash store maximum directory size, the operating mode, and which BranchCache versions are supported. You can also increase the size of the volume that contains the hash store.

Steps

1. Perform the appropriate action:

If you want to...	Enter the following...
Modify the hash store directory size	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB|MB|GB|TB|PB]}`
Increase the size of the volume that contains the hash store	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k|m|g|t]` If the volume containing the hash store fills up, you might be able to increase the size of the volume. You can specify the new volume size as a number followed by a unit designation. See the *Clustered Data ONTAP Logical Storage Management Guide* for more information about increasing volume size.

If you want to...	Enter the following...
Modify the hash store directory path	**vserver cifs branchcache modify -vserver** *vserver_name* **-hash-store-path** *path* **-flush-hashes {true|false}** The BranchCache hash path can contain blanks and any valid file name characters. If you modify the hash store path, -flush-hashes is a required parameter that specifies whether you want Data ONTAP to flush the hashes from the original hash store location. • If you specify true for the value of -flush-hashes, Data ONTAP deletes the hashes in the original location and creates new hashes in the new location as new requests are made by BranchCache-enabled clients. • If set to false, the hashes are not flushed. In this case, you can choose to reuse the existing hashes later by changing the hash store path back to the original location.
Change the operating mode	**vserver cifs branchcache modify -vserver** *vserver_name* **-operating-mode** *mode* The possible values for -operating-mode are as follows: • per-share • all-shares • disable **Note:** You should be aware of the following when modifying the operating mode: • Data ONTAP advertises BranchCache support for a share when the SMB session is set up. • Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.
Change the BranchCache version support	**vserver cifs branchcache modify -vserver** *vserver_name* **-versions {v1-enable|v2-enable|enable-all}**

2. Verify the configuration changes by using the vserver cifs branchcache show command.

Displaying information about BranchCache configurations

You can display information about BranchCache configurations on Storage Virtual Machines (SVMs) with FlexVol volumes, which can be used when verifying a configuration or when determining current settings before modifying a configuration.

Step

1. Perform one of the following actions:

If you want to display...	Enter this command...
Summary information about BranchCache configurations on all SVMs	`vserver cifs branchcache show`
Detailed information about the configuration on a specific SVM	`vserver cifs branchcache show -vserver vserver_name`

Example

The following example displays information about the BranchCache configuration on SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

Changing the BranchCache server key

You can change the BranchCache server key by modifying the BranchCache configuration on the Storage Virtual Machine (SVM) and specifying a different server key.

About this task

You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key.

When you change the server key, you must also flush the hash cache. After flushing the hashes, Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Steps

1. Change the server key by using the following command:

   `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   - `-server-key text` specifies the text string to use as the server key.
   - If the server key contains any spaces, enclose the server key in quotation marks.
   - When configuring a new server key, you must also specify `-flush-hashes` and set the value to `true`.

2. Verify that the BranchCache configuration is correct by using the `vserver cifs branchcache show` command.

Example

The following example sets a new server key that contains spaces and flushes the hash cache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                               Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related concepts

Pre-computing BranchCache hashes on specified paths

You can configure the BranchCache service to pre-compute hashes for a single file, for a directory, or for all files in a directory structure. This can be helpful if you want to compute hashes on data in a BranchCache-enabled share during off, non-peak hours.

Before you begin

You must use the statistics start and optional statistics stop commands if you want to collect a data sample before you display hash statistics. For more information about these commands, see the Clustered Data ONTAP System Administration Guide for Cluster Administrators.

About this task

- You must specify the Storage Virtual Machine (SVM) and path on which you want to pre-compute hashes.
- You must also specify whether you want hashes computed recursively.
- If you want hashes computed recursively, the BranchCache service traverses the entire directory tree under the specified path, and computes hashes for each eligible object.

Steps

1. Perform the appropriate command:

If you want to pre-compute hashes on...	Enter the command...
A single file or directory	**vserver cifs branchcache hash-create -vserver** *vserver_name* **-path** *path* **-recurse false**
Recursively on all files in a directory structure	**vserver cifs branchcache hash-create -vserver** *vserver_name* **-path** *path* **-recurse true**

-path*path* is specified as an absolute path.

2. Verify that hashes are being computed by using the statistics command:

   a) Display statistics for the hashd object on the desired SVM instance:

      statistics show -object hashd -instance *vserver_name*

   b) Verify that the number of hashes created is increasing by repeating the command.

Examples

The following example creates hashes on the path /data and on all contained files and subdirectories on SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data -
recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                              11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                0
```

```
branchcache_hash_rejected                                              0
branchcache_hash_store_bytes                                           0
branchcache_hash_store_size                                            0
instance_name                                                        vs1
node_name                                                          node1
node_uuid
                                        11111111-1111-1111-1111-111111111111
process_name                                                           -
```

Flushing hashes from the SVM BranchCache hash store

You can flush all cached hashes from the BranchCache hash store on the Storage Virtual Machine (SVM). This can be useful if you have changed the branch office BranchCache configuration. For example, if you recently reconfigured the caching mode from distributed caching to hosted caching mode, you would want to flush the hash store.

About this task

After flushing the hashes, Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Step

1. Flush the hashes from the BranchCache hash store:

   vserver cifs branchcache hash-flush -vserver *vserver_name*

   ### Example

   vserver cifs branchcache hash-flush -vserver vs1

Displaying BranchCache statistics

You can display BranchCache statistics to, among other things, identify how well caching is performing, determine whether your configuration is providing cached content to clients, and determine whether hash files were deleted to make room for more recent hash data.

About this task

The hashd statistic object contain counters that provide statistical information about BranchCache hashes. You can collect and display information about the hashd object at the admin-privilege level. The cifs statistic object contain counters that you can use at the advanced-privilege level that provide statistical information about BranchCache-related activity.

Steps

1. Display the BranchCache-related counters by using the statistics catalog counter show command.

   For more information about statistics counters, see the man page for this command.

Example

```
cluster1::> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    -------------------------- --------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file was
                                deleted to make room for more recent hash
                                data. This happens if the hash store size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash data.
    branchcache_hash_store_size Total space used to store BranchCache hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when
directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    -------------------------- --------------------------------------------
    active_searches             Number of active searches over SMB and SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch hash
                                data failed. These are failures when
                                attempting to read existing hash data. It
                                does not include attempts to fetch hash data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had to be
                                read by the client because the hash for that
                                content was not available on the server.
    ....Output truncated....
```

2. Collect BranchCache-related statistics by using the statistics start and statistics stop commands.

For more information about collecting statistics, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

Example

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

3. Display the collected BranchCache statistics by using the statistics show command.

If you want to display statistics for counters that are available only in advanced-privilege level, you must run the statistics show command at the advanced-privilege level. For more information about displaying statistical information, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators.*

Example

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

Related tasks

Support for BranchCache Group Policy Objects

Data ONTAP BranchCache provides support for BranchCache Group Policy Objects (GPOs), which allow centralized management for certain BranchCache configuration parameters. There are two GPOs used for BranchCache, the Hash Publication for BranchCache GPO and the Hash Version Support for BranchCache GPO.

Hash Publication for BranchCache GPO	The Hash Publication for BranchCache GPO corresponds to the -operating-mode parameter. When GPO updates occur, this value is applied to Storage Virtual Machine (SVM) objects contained within the organizational unit (OU) to which the group policy applies.
Hash Version Support for BranchCache GPO	The Hash Version Support for BranchCache GPO corresponds to the -versions parameter. When GPO updates occur, this value is applied to SVM objects contained within the organizational unit to which the group policy applies.

Related concepts

Displaying information about BranchCache Group Policy Objects

You can display information about the CIFS server's Group Policy Object (GPO) configuration to determine whether BranchCache GPOs are defined for the domain to which the CIFS server belongs and, if so, what the allowed settings are. You can also determine whether BranchCache GPO settings are applied to the CIFS server.

About this task

Even though a GPO setting is defined within the domain to which the CIFS server belongs, it is not necessarily applied to the organizational unit (OU) containing the CIFS-enabled Storage Virtual Machine (SVM). Applied GPO setting are the subset of all defined GPOs that are applied to the CIFS-enabled SVM. BranchCache settings applied through GPOs override settings applied through the CLI.

Steps

1. Display the defined BranchCache GPO setting for the Active Directory domain by using the `vserver cifs group-policy show-defined` command.

Example

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

Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
```

```
      Level: Domain
      Status: enabled
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache : all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7

    GPO Name: Resultant Set of Policy
      Status: disabled
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
```

2. Display the BranchCache GPO setting applied to the CIFS server by using the `vserver cifs group-policy show-applied` command.

Example

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

Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7

    GPO Name: Resultant Set of Policy
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
```

Related tasks

Enabling or disabling GPO support on a CIFS server on page 95

Disabling BranchCache on SMB shares

If you do not want to provide BranchCache caching services on certain SMB shares but you might want to provide caching services on those shares later, you can disable BranchCache on a share-by-share basis. If you have BranchCache configured to offer caching on all shares but you want to temporarily disable all caching services, you can modify the BranchCache configuration to stop automatic caching on all shares.

If BranchCache on an SMB share is subsequently disabled after first being enabled, Data ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server on the Storage Virtual Machine (SVM)).

Related concepts

Configuring BranchCache-enabled SMB shares on page 306

Disabling BranchCache on a single SMB share

If you do not want to offer caching services on certain shares that previously offered cached content, you can disable BranchCache on an existing SMB share.

Step

1. Enter the following command:

   vserver cifs share properties remove -vserver *vserver_name* **-share-name** *share_name* **-share-properties branchcache**

   The BranchCache share property is removed. Other applied share properties remain in effect.

   Example

   The following command disables BranchCache on an existing SMB share named "data2":

   ```
   cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                         Vserver: vs1
                           Share: data2
        CIFS Server NetBIOS Name: VS1
                            Path: /data2
                 Share Properties: oplocks
                                   browsable
                                   changenotify
                                   attributecache
                                   branchcache
               Symlink Properties: -
           File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                        Share ACL: Everyone / Full Control
   ```

```
File Attribute Cache Lifetime: 10s
                 Volume Name: -
               Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                        Vserver: vs1
                          Share: data2
        CIFS Server NetBIOS Name: VS1
                           Path: /data2
                Share Properties: oplocks
                                  browsable
                                  changenotify
                                  attributecache
             Symlink Properties: -
        File Mode Creation Mask: -
   Directory Mode Creation Mask: -
                  Share Comment: -
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: 10s
                    Volume Name: -
                  Offline Files: manual
Vscan File-Operations Profile: standard
```

Stopping automatic caching on all SMB shares

If your BranchCache configuration automatically enables caching on all SMB shares on each Storage
Virtual Machine (SVM) with FlexVol volumes, you can modify the BranchCache configuration to
stop automatically caching content for all SMB shares.

About this task

To stop automatic caching on all SMB shares, you change the BranchCache operating mode to per-
share caching.

Steps

1. Configure BranchCache to stop automatic caching on all SMB shares by entering the following
   command:

   vserver cifs branchcache modify -vserver *vserver_name* **-operating-mode
   per-share**

2. Verify that the BranchCache configuration is correct:

   vserver cifs branchcache show -vserver *vserver_name*

Example

The following command changes the BranchCache configuration on Storage Virtual Machine
(SVM, formerly known as Vserver) vs1 to stop automatic caching on all SMB shares:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                              Vserver: vs1
           Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Disabling or enabling BranchCache on the SVM

You can disable BranchCache on the Storage Virtual Machine (SVM) if you temporarily do not want to offer caching services on that SVM. You can easily offer caching services again in the future by enabling BranchCache on the SVM.

What happens when you disable or reenable BranchCache on the CIFS server

If you previously configured BranchCache but do not want the branch office clients to use cached content, you can disable caching on the CIFS server. You must be aware of what happens when you disable BranchCache.

When you disable BranchCache, Data ONTAP no longer computes hashes or sends the metadata to the requesting client. However, there is no interruption to file access. Thereafter, when BranchCache-enabled clients request metadata information for content they want to access, Data ONTAP responds with a Microsoft-defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the Storage Virtual Machine (SVM).

After BranchCache is disabled on the CIFS server, SMB shares do not advertise BranchCache capabilities. To access data on new SMB connections, clients make normal read SMB requests.

You can reenable BranchCache on the CIFS server at any time.

- Because the hash store is not deleted when you disable BranchCache, Data ONTAP can use the stored hashes when replying to hash requests after you reenable BranchCache, provided that the requested hash is still valid.
- Any clients that have made SMB connections to BranchCache-enabled shares during the time when BranchCache was disabled do not get BranchCache support if BranchCache is subsequently reenabled.
  This is because Data ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that established sessions to BranchCache-enabled shares while BranchCache was disabled need to disconnect and reconnect to use cached content for this share.

Note: If you do not want to save the hash store after you disable BranchCache on a CIFS server, you can manually delete it. If you reenable BranchCache, you must ensure that the hash store directory exists. After BranchCache is reenabled, BranchCache-enabled shares advertise

BranchCache capabilities. Data ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Disabling or enabling BranchCache

You can disable BranchCache on the Storage Virtual Machine (SVM) with FlexVol volumes by changing the BranchCache operating mode to `disabled`. You can enable BranchCache at any time by changing the operating mode to either offer BranchCache services per-share or automatically for all shares.

Steps

1. Run the appropriate command:

If you want to...	Then enter the following...
Disable BranchCache	**vserver cifs branchcache modify -vserver** *vserver_name* **-operating-mode disable**
Enable BranchCache per share	**vserver cifs branchcache modify -vserver** *vserver_name* **-operating-mode per-share**
Enable BranchCache for all shares	**vserver cifs branchcache modify -vserver** *vserver_name* **-operating-mode all-shares**

2. Verify that the BranchCache operating mode is configured with the desired setting:

vserver cifs branchcache show -vserver *vserver_name*

Example

The following example disables BranchCache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
            Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Deleting the BranchCache configuration on SVMs

You can delete the BranchCache configuration if you no longer want to offer caching services on that Storage Virtual Machine (SVM).

What happens when you delete the BranchCache configuration

If you previously configured BranchCache but do not want the Storage Virtual Machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, Data ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether Data ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, Data ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

Deleting the BranchCache configuration

The command you use for deleting the BranchCache service on your Storage Virtual Machine (SVM) differs depending on whether you want to delete or keep existing hashes.

Step

1. Run the appropriate command:

If you want to...	Then enter the following...
Delete the BranchCache configuration and delete existing hashes	**vserver cifs branchcache delete -vserver** ***vserver_name* -flush-hashes true**
Delete the BranchCache configuration but keep existing hashes	**vserver cifs branchcache delete -vserver** ***vserver_name* -flush-hashes false**

> **Example**
>
> The following example deletes the BranchCache configuration on SVM vs1 and deletes all existing hashes:
>
> ```
> cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes true
> ```

What happens to BranchCache when reverting

It is important to understand what happens when you revert Data ONTAP to a release that does not support BranchCache.

*   When you revert to a version of Data ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information.

    Instead, they request the actual content using normal SMB read requests. In response to the request for content, the CIFS server sends the actual content that is stored on the Storage Virtual Machine (SVM).
*   When a node hosting a hash store is reverted to a release that does not support BranchCache, the storage administrator needs to manually revert the BranchCache configuration using a command that is printed out during the revert.

    This command deletes the BranchCache configuration and hashes.

    After the revert completes, the storage administrator can manually delete the directory that contained the hash store if desired.

Related concepts

[Deleting the BranchCache configuration on SVMs](#) on page 323

Improving Microsoft remote copy performance

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer.

Data ONTAP supports ODX for both the SMB and SAN protocols. The source can be either a CIFS server or LUN, and the destination can be either a CIFS server or LUN.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

For SMB environments, this functionality is only available when both the client and the storage server support SMB 3.0 and the ODX feature. For SAN environments, this functionality is only available when both the client and the storage server support the ODX feature. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used irrespective of whether you drag-and-drop files through

Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

Related concepts

Improving client response time by providing SMB automatic node referrals with Auto Location on page 332
How ODX copy offload is used with Hyper-V and SQL Server over SMB shares on page 351

How ODX works

ODX copy offload uses a token-based mechanism for reading and writing data within or between ODX-enabled CIFS servers. Instead of routing the data through the host, the CIFS server sends a small token, which represents the data, to the client. The ODX client presents that token to the destination server, which then can transfer the data represented by that token from the source to the destination.

When an ODX client learns that the CIFS server is ODX-capable, it opens the source file and requests a token from the CIFS server. After opening the destination file, the client uses the token to instruct the server to copy the data directly from the source to the destination.

Note: The source and destination can be on the same Storage Virtual Machine (SVM) or on different SVMs, depending on the scope of the copy operation.

The token serves as a point-in-time representation of the data. As an example, when you copy data between storage locations, a token representing a data segment is returned to the requesting client, which the client copies to the destination, thereby removing the need to copy the underlying data through the client.

Data ONTAP supports tokens that represent 8 MB of data. ODX copies of greater than 8 MB are performed by using multiple tokens, with each token representing 8 MB of data.

The following figure explains the steps that are involved with an ODX copy operation:
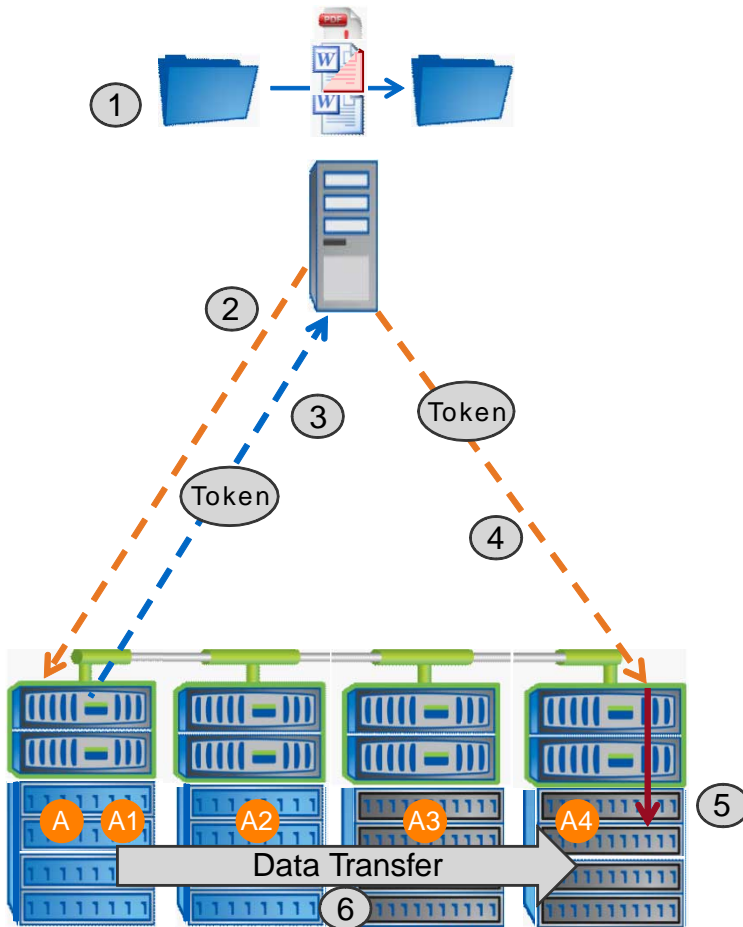
1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.

2. The ODX-capable client automatically translates this transfer request into an ODX request. The ODX request that is sent to the CIFS server contains a request for a token.

3. If ODX is enabled on the CIFS server and the connection is over SMB 3.0, the CIFS server generates a token, which is a logical representation of the data on the source.

4. The client receives a token that represents the data and sends it with the write request to the destination CIFS server.
   This is the only data that is copied over the network from the source to the client and then from the client to the destination.

5. The token is delivered to the storage subsystem.

6. The SVM internally performs the copy or move.
   If the file that is copied or moved is larger than 8 MB, multiple tokens are needed to perform the copy. Steps 2 through 6 as performed as needed to complete the copy.

> **Note:** If there is a failure with the ODX offloaded copy, the copy or move operation falls back to traditional reads and writes for the copy or move operation. Similarly, if the destination CIFS server does not support ODX or ODX is disabled, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

Requirements for using ODX

Before you can use ODX for copy offloads with your Storage Virtual Machine (SVM) with FlexVol volumes, you need to be aware of certain requirements.

Data ONTAP version requirements

Clustered Data ONTAP 8.2 and later releases support ODX for copy offloads.

SMB version requirements

- Clustered Data ONTAP supports ODX with SMB 3.0 and later.
- SMB 3.0 must be enabled on the CIFS server before ODX can be enabled:
    - Enabling ODX also enables SMB 3.0, if it is not already enabled.
    - Disabling SMB 3.0 also disables ODX.

Windows server and client requirements

Before a user can use ODX for copy offloads, the Windows client must support the feature. Support for ODX starts with Windows 2012 Server and Windows 8.

For the latest information about which Windows clients support ODX, see the Interoperability Matrix at *support.netapp.com/matrix*.

Volume requirements

- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- Compression must *not* be enabled on volumes used with copy offload.

Considerations for using ODX

Before you can use ODX for copy offload, you need to be aware of certain considerations. For example, you need to know on which types of volumes you can use ODX and you need to understand the intra-cluster and inter-cluster ODX considerations.

Volume considerations

You must keep the following volume considerations in mind:

- You cannot use ODX for copy offload with the following volume configurations:

- Source volume size is less than 1.25 GB
  The volume size must be 1.25 GB or larger to use ODX.
- Read-only volumes
  ODX is not used for file and folders residing in load sharing mirrors or in SnapMirror or
  SnapVault destination volumes.
- FlexCache volumes
- If the source volume is compressed
- If the source volume is not deduplicated

- ODX copies are supported only for intra-cluster copies.
  You cannot use ODX to copy files or folders to a volume in another cluster.
- ODX is supported for Storage Virtual Machines (SVMs) with FlexVol volumes.
  You cannot use ODX to copy data to or from volumes in SVMs with Infinite Volume.

Other considerations

There are some additional considerations you should keep in mind:

- In SMB environments, to use ODX for copy offload, the files must be 256 kb or larger.
  Smaller files are transferred using a traditional copy operation.
- ODX copy offload uses deduplication as part of the copy process.
  If you do not want deduplication to occur on SVM volumes when copying or moving data, you
  should disable ODX copy offload on that SVM.
- The application that performs the data transfer must be written to support ODX.
  Application operations that support ODX include the following:

  - Hyper-V management operations, such as creating and converting virtual hard disks (VHDs),
    managing Snapshot copies, and copying files between virtual machines
  - Windows Explorer operations
  - Windows PowerShell copy commands
  - Windows command prompt copy commands
    Robocopy at the Windows command prompt supports ODX.

    Note: The applications must be running on Windows servers or clients that support ODX.

    For more information about supported ODX applications on Windows servers and clients,
    consult the Microsoft TechNet Library.

Related information

  Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Use cases for ODX

You should be aware of the use cases for using ODX on SVMs with FlexVol volumes so that you
can determine under what circumstances this feature provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data
across remote servers. If the Windows server or client does not support ODX or the ODX copy

offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume. The copy is performed by using FlexClone file technology, which provides additional remote copy performance benefits.
- Inter-volume, same node, same SVM

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.
- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.
- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.
- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

There are some additional special use cases:

- With the Data ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

  You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided the SMB shares and LUNs are on the same cluster.
- Hyper-V provides some additional use cases for ODX copy offload:

  - You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

    This allows copies from guest operating systems to pass through to the underlying storage.
  - When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
  - ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

  Note: To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Enabling or disabling ODX

You can enable or disable ODX on Storage Virtual Machines (SVMs) with FlexVol volumes. The default is to enable support for ODX copy offload if SMB 3.0 is also enabled.

Before you begin

SMB 3.0 must be enabled.

About this task

If you disable SMB 3.0, Data ONTAP also disables SMB ODX. If you reenable SMB 3.0, you must manually reenable SMB ODX.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want ODX copy offload to be...	Enter the command...
Enabled	**`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`**
Disabled	**`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`**

3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following example enables ODX copy offload on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload-enabled
true

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

Related references

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

Auto Location uses SMB automatic node referrals to increase SMB client performance on Storage Virtual Machines (SVMs) with FlexVol volumes. Automatic node referrals automatically redirect the requesting client to a LIF on the node SVM that is hosting the FlexVol volume in which the data resides, which can lead to improved client response times.

When an SMB client connects to an SMB share hosted on the SVM, it might connect using a LIF that is on a node that does not own the requested data. The node to which the client is connected accesses data owned by another node by using the cluster network. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data:

- Data ONTAP provides this functionality by using Microsoft DFS referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else.
  A node makes a referral when it determines that there is an SVM LIF on the node containing the data.
- Automatic node referrals are supported for IPv4 and IPv6 LIF IP addresses.
- Referrals are made based on the location of the root of the share through which the client is connected.
- The referral occurs during SMB negotiation.
  The referral is made before the connection is established. After Data ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

  Note: If a share spans multiple junction points and some of the junctions are to volumes contained on other nodes, data within the share is spread across multiple nodes. Because Data ONTAP provides referrals that are local to the root of the share, Data ONTAP must use the cluster network to retrieve the data contained within these non-local volumes.

  With this type of namespace architecture, automatic node referrals might not provide significant performance benefits.

If the node hosting the data does not have an available LIF, Data ONTAP establishes the connection using the LIF chosen by the client. After a file is opened by an SMB client, it continues to access the file through the same referred connection.

If, for any reason, the CIFS server cannot make a referral, there is no disruption to SMB service. The SMB connection is established as if automatic node referrals were not enabled.

Related concepts

Requirements and considerations when using automatic node referrals

Before you can use SMB automatic node referrals, also known as *autolocation*, you need to be aware of certain requirements, including which versions of Data ONTAP support the feature. You also need to know about supported SMB protocol versions and certain other special considerations.

Data ONTAP version and license requirements

- Data ONTAP 8.2 and later support SMB automatic node referrals.
- All nodes in the cluster must be running a version of Data ONTAP that supports automatic node referrals.
- CIFS must be licensed, and a CIFS server must exist on the Storage Virtual Machine (SVM).

SMB protocol version requirements

- For SVMs with FlexVol volumes, Data ONTAP supports automatic node referrals on all versions of SMB.
- For SVMs with Infinite Volume, Data ONTAP supports automatic node referrals on SMB 1.0.

SMB client requirements

All Microsoft clients supported by Data ONTAP support SMB automatic node referrals.

For the latest information about which Windows clients Data ONTAP supports, see the Interoperability Matrix at *support.netapp.com/matrix*.

NTLM authentication requirements when making a referred SMB connection

NTLM authentication must be allowed on the domain containing the CIFS server and on the domains containing clients that want to use automatic node referrals.

When making a referral, the CIFS server refers an IP address to the Windows client. Because NTLM authentication is used when making a connection using an IP address, Kerberos authentication is not performed for referred connections.

This happens because the Windows client cannot craft the service principal name used by Kerberos (which are of the form service/NetBIOS name and service/FQDN), which means the client cannot request a Kerberos ticket to the service.

Considerations when using automatic node referrals with the home directory feature

When shares are configured with the home directory share property enabled, there can be one or more home directory search paths configured for a home directory configuration. The search paths can point to volumes contained on each node containing SVM volumes. Clients receive a referral

and, if an active, local data LIF is available, connect through a referred LIF that is local to the home user's home directory.

There are considerations when SMB 1.0 clients access dynamic home directories with automatic node referrals enabled. This is because SMB 1.0 clients require the automatic node referral before they have authenticated, thus, before the CIFS server has the user's name. However, CIFS home directory access works correctly for SMB 1.0 clients if the following are true:

- CIFS home directories are configured to use simple names such as "%w" (Windows user name), or "%u" (mapped Unix user name) and not domain-name style names "%d\%w " (domain-name \user-name).
- When creating home directory shares, the CIFS home directory shares names are configured with variables ("%w" or "%u") and not with static names such as "HOME".

For SMB 2.x and SMB 3.0 clients, there are no special considerations when accessing home directories using automatic node referrals.

Considerations when disabling automatic node referrals on CIFS servers with existing referred connections

If you disable automatic node referrals after the option has been enabled, clients currently connected to a referred LIF keep the referred connection. Because Data ONTAP uses DFS referrals as the mechanism for SMB automatic node referrals, clients can even reconnect to the referred LIF after you disable the option until the client's cached DFS referral for the referred connection times out. This is true even in the case of a revert to a version of Data ONTAP that does not support automatic node referrals. Clients continue to use referrals until the DFS referral times out from the client's cache.

Considerations when using automatic node referrals with Mac OS clients

Mac OS X clients do not support SMB automatic node referrals, even though the Mac OS supports Microsoft's Distributed File System (DFS). Windows clients make a DFS referral request before connecting to an SMB share. Clustered Data ONTAP provides a referral to a data LIF found on the same node that hosts the requested data, which leads to improved client response times. Although the Mac OS supports DFS, Mac OS clients do not behave exactly like Windows clients in this area.

Related concepts

Managing home directories on page 281

Support for automatic node referrals

Before you enable automatic node referrals, you should be aware that certain Data ONTAP functionality does not support referrals.

- The following types of volumes do not support automatic node referrals:
  - FlexCache target volumes
  - Read-only members of a load-sharing mirror

- Destination volume of a data-protection mirror

  When determining locality, if the target component belongs to a FlexCache cache volume, it is considered local access and bypasses automatic referrals. If a referral is generated, it only reflects the LIFs on the node hosting the origin (writable) volume.

- Node referrals do not move alongside a LIF move.

  If a client is using a referred connection over an SMB 2.x or SMB 3.0 connection and a data LIF moves nondisruptively, the client continues to use the same referred connection, even if the LIF is no longer local to the data.

- Node referrals do not move alongside a volume move.

  If a client is using a referred connection over any SMB connection and a volume move occurs, the client continues to use the same referred connection, even if the volume is no longer located on the same node as the data LIF.

- Node referrals are not supported on Storage Virtual Machines (SVMs) containing Hyper-V over SMB configurations.

  You must not enable automatic node referrals if you wish to use the Witness protocol for faster nondisruptive failover with Hyper-V over SMB solutions.

Enabling or disabling SMB automatic node referrals

You can enable SMB automatic node referrals to increase SMB client access performance. You can disable automatic node referrals if you do not want Data ONTAP to make referrals to SMB clients.

Before you begin

A CIFS server must be configured and running on the Storage Virtual Machine (SVM) with FlexVol volumes.

About this task

Automatic node referrals are enabled and disabled on SVM basis. The functionality is disabled by default. Automatic node referrals are not supported on SVMs containing Hyper-V over SMB configurations. You must set the option to `false` if the SVM hosts Hyper-V over SMB configurations.

This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want SMB node automatic referrals to be...	Enter the command...
Enabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

The option setting takes effect for new SMB sessions. Clients with existing connection can utilize node referral only when their existing cache timeout expires.

3. Return to the admin privilege level:

   `set -privilege admin`

Related references

Using statistics to monitor automatic node referral activity

To determine how many SMB connections are referred, you can monitor automatic node referral activity by using the `statistics` command. By monitoring referrals you can determine the extent to which automatic referrals are locating connections on nodes that host the shares and whether you should redistribute your data LIFs to provide better local access to shares on the CIFS server.

About this task

The `cifs` object provides several counters at the advanced privilege level that are helpful when monitoring SMB automatic node referrals:

- `node_referral_issued`
  Number of clients that have been issued a referral to the share root's node after the client connected using a LIF hosted by a node different from the share root's node.
- `node_referral_local`
  Number of clients that connected using a LIF hosted by the same node that hosts the share root. Local access generally provides optimal performance.
- `node_referral_not_possible`
  Number of clients that have not been issued a referral to the node hosting the share root after connecting using a LIF hosted by a node different from the share root's node. This is because an active data LIF for the share root's node was not found.
- `node_referral_remote`
  Number of clients that connected using a LIF hosted by a node different from the node that hosts the share root. Remote access might result in degraded performance.

You can monitor automatic node referral statistics on your Storage Virtual Machine (SVM) by collecting and viewing data for a specific time period (a sample). You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping

data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

> **Note:** To evaluate and use the information you gather from the `statistics` command, you should understand the distribution of clients in your environments.

For more information about using the `statistics` command, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. View automatic node referral statistics by using the `statistics` command.

   Example

   This example views automatic node referral statistics by collecting and viewing data for a sampled time period:

   a. Start the collection:

   `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. Wait for the desired collection time to elapse.

   c. Stop the collection:

   `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   d. View the automatic node referral statistics:

   `statistics show -sample-id sample1 -counter *node*`

   ```
   Object: cifs
   Instance: vs1
   Start-time: 2/4/2013 19:27:02
   End-time: 2/4/2013 19:30:11
   Cluster: cluster1

       Counter                                     Value
       -------------------------- --------------------------
       node_name                                   node1
       node_referral_issued                            0
       node_referral_local                             1
       node_referral_not_possible                      2
       node_referral_remote                            2
       ...
   ```

```
        node_name                                          node2
        node_referral_issued                               2
        node_referral_local                                1
        node_referral_not_possible                         0
        node_referral_remote                               2
        ...
```

Output displays counters for all nodes participating in SVM vs1. For clarity, only output fields related to automatic node referral statistics are provided in the example.

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

Related tasks

Displaying statistics on page 265

How to monitor client-side SMB automatic node referral information using a Windows client

To determine what referrals are made from the client's perspective, you can use the Windows dfsutil.exe utility.

The Remote Server Administration Tools (RSAT) kit available with Windows 7 and later clients contains the dfsutil.exe utility. Using this utility, you can display information about the contents of the referral cache as well as view information about each referral that the client is currently using. You can also use the utility to clear the client's referral cache. For more information, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Providing folder security on shares with access-based enumeration

When access-based enumeration (ABE) is enabled on an SMB share, users who do not have permission to access the contents of a shared folder do not see that shared resource displayed in their environment.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify shared resources. However, they do not allow you to control whether shared folders or files are visible to users who do not have permission to access them. This could pose problems if the names of shared folders or files describe sensitive information, such as the names of customers or products under development.

Access-based enumeration (ABE) extends share properties to include the enumeration of shared resources. ABE therefore enables you to filter the display of shared resources based on user access rights. In addition to protecting sensitive information in your workplace, ABE enables you to

simplify the display of large directory structures for the benefit of users who do not need access to your full range of content.

Enabling or disabling access-based enumeration on SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares to allow or prevent users from seeing shared resources that they do not have permission to access.

About this task

By default, ABE is disabled.

Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable ABE on a new share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` `path` specifies the path to the share. Path separators can be backward or forward slashes, although Data ONTAP displays them as forward slashes. You can specify additional optional share settings and additional share properties when you create an SMB share. For more information, see the man page for the `vserver cifs share create` command.
Enable ABE on an existing share	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Existing share properties are preserved. The ABE share property is added to the existing list of share properties.
Disable ABE on an existing share	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Other share properties are preserved. Only the ABE share property is removed from the list of share properties.

2. Verify that the share configuration is correct by using the `vserver cifs share show` command.

Examples

The following example creates an ABE SMB share named "sales" with a path of `/sales` on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. The share is created with `access-based-enumeration` as a share property:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path /
sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                        Vserver: vs1
                          Share: sales
       CIFS Server NetBIOS Name: VS1
                           Path: /sales
               Share Properties: access-based-enumeration
                                 oplocks
                                 browsable
                                 changenotify
             Symlink Properties: enable
       File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                  Share Comment: -
                      Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                    Volume Name: -
                  Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example adds the access-based-enumeration share property to an SMB
share named "data2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server   share-name share-properties
-------  ---------- --------------------------------------------------------
vs1      data2      oplocks,browsable,changenotify,access-based-enumeration
```

Related tasks

Creating an SMB share on a CIFS server on page 131
Adding or removing share properties on an existing SMB share on page 135

Enabling or disabling access-based enumeration from a Windows client

You can enable or disable access-based enumeration (ABE) on SMB shares from a Windows client,
which allows you to configure this share setting without needing to connect to the CIFS server.

Step

1. From a Windows client that supports ABE, enter the following command:

   **abecmd [/enable | /disable] [/server *CIFS_server_name*] {/all |
   share_name}**

   For more information about the abecmd command, see your Windows client documentation.

Configuring Data ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

With the new capabilities provided in Data ONTAP 8.2 and later, you can now use continuously available SMB 3.0 file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in Storage Virtual Machines (SVMs) with FlexVol volumes, while at the same time providing nondisruptive operations (NDOs) for both planned and unplanned events.

Microsoft Hyper-V over SMB

To create a Hyper-V over SMB solution, you must first configure Data ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.

Note: The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with Hyper-V over SMB configurations.

  For information about using SnapManager with Hyper-V over SMB configurations, see *SnapManager for Hyper-V Installation and Administration Guide*.

Microsoft SQL Server over SMB

To create a SQL Server over SMB solution, you must first configure Data ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server 2012 on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.

Note: SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server 2012, see the Microsoft web site.
- SnapManager for Microsoft SQL Server is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with SQL Server over SMB configurations.

For information about using SnapManager for Microsoft SQL Server, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

What nondisruptive operations for Hyper-V and SQL Server over SMB means

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover
- Upgrade
  To perform a nondisruptive upgrade (NDU), all nodes in the cluster must be running a version of clustered Data ONTAP that supports this functionality.

  - Data ONTAP 8.2 is the first release that supports NDUs for Hyper-V over SMB solutions; therefore, nondisruptive upgrades are supported if all nodes in the cluster are running Data ONTAP 8.2 or later, including upgrades within the Data ONTAP 8.2 release family.
  - Data ONTAP 8.2.1 is the first release that supports NDUs for SQL Server over SMB solutions; therefore, nondisruptive upgrades are supported if all nodes in the cluster are running Data ONTAP 8.2.1 or later, including upgrades within the Data ONTAP 8.2 release family to releases later than Data ONTAP 8.2.1.
- Planned aggregate relocation (ARL)
- LIF migration and failover
- Planned volume move

Related concepts

Protocols that enable nondisruptive operations over SMB

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

Data ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

- SMB 3.0
- Witness

Related concepts

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

Continuously available share	An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.
Node	A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the *local node* and the other node is sometimes called the *partner node* or *remote node*. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner's storage.
Nondisruptive aggregate relocation	The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.
Nondisruptive failover	See *Takeover*.
Nondisruptive LIF migration	The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.
Nondisruptive operations	The ability to perform major clustered Data ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.
Nondisruptive upgrade	The ability to upgrade node hardware or software without application interruption.
Nondisruptive volume move	The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.
Persistent handles	A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost.

However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

SFO giveback	Returning aggregates to their home locations when recovering from a takeover event.
SFO pair	A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.
Takeover	The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

Related concepts

How SMB 3.0 functionality supports nondisruptive operations over SMB shares

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the new `continuously-available` share property and a new type of file handle known as a *persistent handle* that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the continuously available share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the Storage Virtual Machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner

node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if a failure causes the Hyper-V application to fail over to another node in the Windows Server 2012 cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. "Failover Clustering" is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

Related concepts

Supported SMB 3.0 functionality on page 70

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367

Enabling or disabling SMB 3.0 on page 73

Configuring existing shares for continuous availability on page 382

What the Witness protocol does to enhance transparent failover

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

* It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
* The shares must use SMB 3.0 with the continuous availability share property set.
* The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the Storage Virtual Machine (SVM) hosting data for the application servers.

    Note: The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner.

    The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner

node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367
Verifying LIF status on page 394

How the Witness protocol works

Data ONTAP implements the Witness protocol by using a node's SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.

2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the Storage Virtual Machine (SVM).

3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.

4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.

5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.

6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.
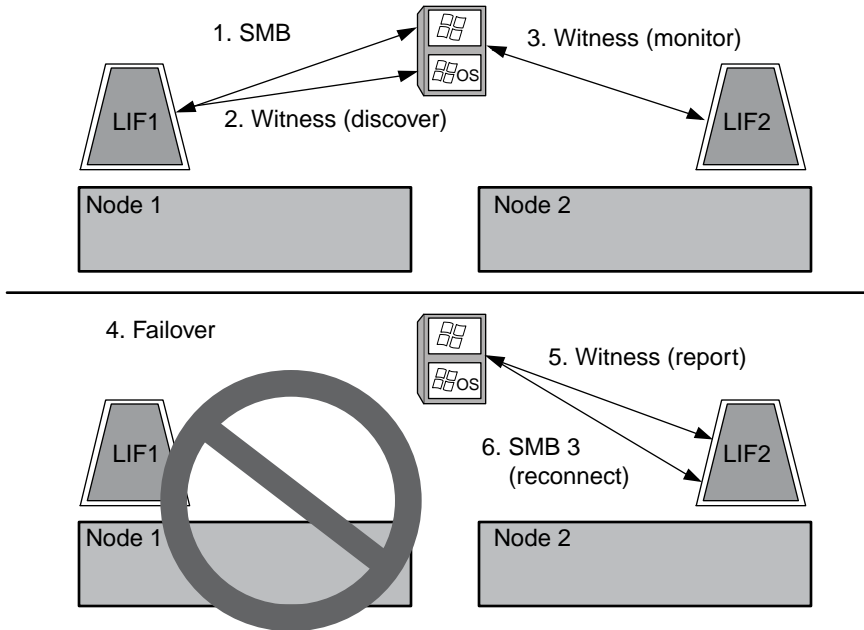
Share-based backups with Remote VSS

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367
Enabling or disabling VSS shadow copies for Hyper-V over SMB backups on page 385

Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

VSS (Volume Shadow Copy Service)	A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.
Remote VSS (Remote Volume Shadow Copy Service)	A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.
Shadow copy	A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.
Shadow copy set	A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.
Shadow copy set automatic recovery	The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.
Shadow copy ID	A GUID that uniquely identifies a shadow copy.
Shadow copy set ID	A GUID that uniquely identifies a collection of shadow copy IDs to the same server.
SnapManager for Hyper-V	The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses

Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

Related concepts

Example of a directory structure used by Remote VSS

Remote VSS traverses the directory structure on the that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is so that backups of virtual machine files succeed.

A supported directory structure for successful shadow copy creation conforms to the following requirements:

- Only directories and regular files are present within the directory structure used to store virtual machine files.
  The directory structure does not contain junctions, links, or non-regular files.
- All files for a virtual machine reside within a single share.
- The directory structure used to store virtual machine files does not exceed the configured shadow copy directory depth.
- The root directory of the share contains only virtual machine files or directories.

In the following example, the volume named vm_vol1 is created with a junction point at `/hyperv/vm1` on Storage Virtual Machine (SVM) vs1. Subdirectories to contain the virtual machine files are created under the junction point. The Hyper-V server's virtual machine files are accessed over share1 that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files contained within the directory structure under share1 (up to the configured shadow copy directory depth).
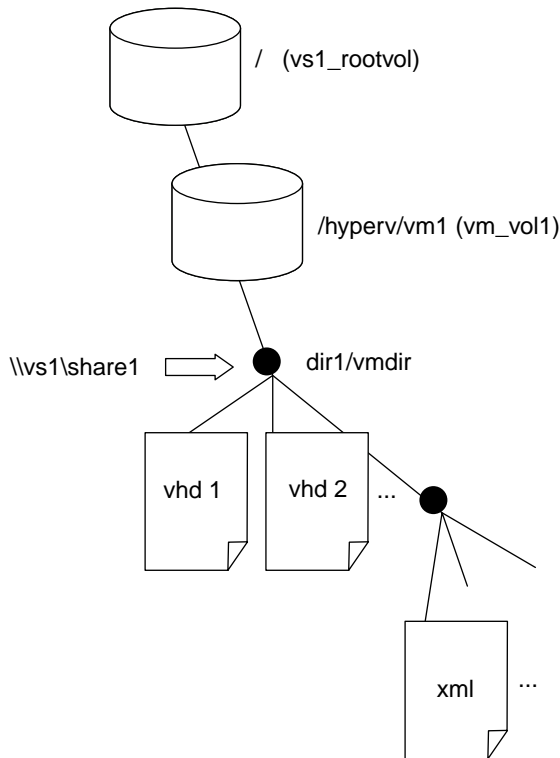
How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

*   SnapDrive integration with Data ONTAP provides performance optimization when discovering SMB share location.

    Data ONTAP provides SnapDrive with the name of the volume where the share resides.
*   SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

    By providing a targeted list of virtual machine files, the shadow copy service does not need to creates shadow copies of all the files in the share.
*   The Storage Virtual Machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.

    There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation

   The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to Data ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

2. Creating the shadow copy set (if automatic-recovery is used)

   For every share included in the shadow copy set, Data ONTAP creates a shadow copy and makes the shadow copy writable.

3. Exposing the shadow copy set

   After Data ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

4. Automatically recovering the shadow copy set

   During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.

   Note: The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

5. Completing and cleaning up the shadow copy set

   The VSS client notifies Data ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Data ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

This functionality is available on Windows Server 2012 servers. Data ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

The following use cases support using ODX copies and moves:

* Intra-volume

  The source and destination files or LUNs are within the same volume. The copy is performed by using FlexClone file technology, which provides additional remote copy performance benefits.
* Inter-volume, same node, same Storage Virtual Machine (SVM)

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.
* Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.
* Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.
* Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

* You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

  This allows copies from guest operating systems to pass through to the underlying storage.
* When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
* ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

  Note: To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

* You can use ODX copy offload to export and import SQL Server databases between mapped SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.
* ODX copy offload is used for database exports and imports if the source and destination storage is on the same cluster.

Related concepts

Improving Microsoft remote copy performance on page 325

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367

Configuration requirements and considerations

There are certain requirements and considerations that you must consider while planning and configuring SQL Server and Hyper-V application servers for NDOs over SMB shares.

Related concepts

Planning the configuration on page 361
Considerations for reverting Hyper-V over SMB configurations on page 386

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367

Data ONTAP and licensing requirements

You need to be aware of certain Data ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs with FlexVol volumes.

Hyper-V and SQL Server over SMB solutions are not supported on SVMs with Infinite Volume.

Data ONTAP version requirements

- Hyper-V over SMB
  Clustered Data ONTAP 8.2 and later releases support nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.
- SQL Server over SMB
  Clustered Data ONTAP 8.2.1 and later releases in the 8.2 release family support nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of Data ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix at *support.netapp.com/matrix*.

Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)

This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to create point-in-time copies of files that are then used when creating a backup. A FlexClone license is optional if you use a backup method that does not use Remote VSS.

Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations).

Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.
  SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.
- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the Storage Virtual Machine (SVM).
  The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple connections to multiple unique IP addresses.
  Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

Data LIF requirements

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.
  SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.
- Data LIFs must not be configured to automatically revert.
  After a takeover or giveback event, you should manually revert the data LIFs to their home ports.
- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name.
  The application servers must connect to SMB shares by using the CIFS server name. You must not configure the application servers to make connections by using the LIF IP addresses.
- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

CIFS server and volume requirements for Hyper-V over SMB

You need to be aware of certain CIFS server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

CIFS server requirements

- SMB 3.0 must be enabled.
  This is enabled by default.
- The default UNIX user CIFS server option must be configured with a valid UNIX user account.
  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, Data ONTAP must be able to map the application server's machine account to the default UNIX user account.
- Automatic node referrals must be disabled.
  Automatic node referrals are disabled by default. If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.
- Both Kerberos and NTLM authentication must be allowed in the domain to which the CIFS server belongs.
  Data ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.
- Shadow copy functionality must be enabled.
  This functionality is enabled by default.
- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the CIFS server's local BUILTIN\Administrators or BUILTIN\Backup Operators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.
  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.
- For shadow copy operations to succeed, you must have enough available space on the volume.
  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](technet.microsoft.com/en-us/library/)

CIFS server and volume requirements for SQL Server over SMB

You need to be aware of certain CIFS server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

CIFS server requirements

- SMB 3.0 must be enabled.
  This is enabled by default.
- The default UNIX user CIFS server option must be configured with a valid UNIX user account.
  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, Data ONTAP must be able to map the application server's machine account to the default UNIX user account.
  Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.
- Automatic node referrals must be disabled.
  Automatic node referrals are disabled by default. If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.
- The Windows user account used for installing SQL Server on Data ONTAP must be assigned the SeSecurityPrivilege privilege.
  This privilege is assigned to the CIFS server's local BUILTIN\Administrators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.
  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.
- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.
  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

Share requirements

- Shares used by the application servers must be configured with the continuously available property set.
  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events such as takeover, giveback, and aggregate relocation.
- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.
  In the auto-recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.
- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files
    The shadow copy creation will fail if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.
  - For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).
    The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.
- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Change notify
  - Attribute caching
  - BranchCache
  - Access-based enumerations

  Note: With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

Considerations

- Quotas are not supported on continuously available shares.
  Even if a quota is specified, the continuously available share ignores quota policies.
- The following functionality is not supported for Hyper-V over SMB configurations:

  - Auditing
  - FPolicy
  - FlexCache

- Virus scanning is not performed on SMB shares with the continuously-availability parameter set to `Yes`.

Continuously available share requirements and considerations for SQL Server over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

Share requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.
  To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.
- Shares used by the application servers must be configured with the continuously available property set.
  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events such as takeover, giveback, and aggregate relocation.
- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.
  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.
- The following share properties must not be set on continuously available shares used by the application servers:

  - Home directory

- Change notify
- Attribute caching
- BranchCache
- Access-based enumerations

    Note: With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

Share considerations

- Quotas are not supported on continuously available shares.
  Even if a quota is specified, the continuously available share ignores quota policies.
- The following functionality is not supported for SQL Server over SMB configurations:

    - Auditing
    - FPolicy
    - FlexCache

- Virus scanning is not performed on SMB shares with the `continuously-availability` share property set.

Remote VSS considerations for Hyper-V over SMB configurations

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

General Remote VSS considerations

- A maximum of 64 shares can be configured per Microsoft application server.
  The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.
- Only one active shadow copy set per CIFS server is allowed.
  A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.
- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.

    - In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
    - In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

Remote VSS considerations that apply only for shadow copies with automatic recovery

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation.

This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine file are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

* Amount of available space on the volume must be adequate.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

* No links or non-regular files are allowed within the directory structure on which Remote VSS creates a shadow copy.

  The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy. The clone process does not support them.

* No NFSv4 ACLs are allowed on directories.

  Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

* A maximum of 60 seconds is allowed to create a shadow copy set.

  Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

ODX copy offload requirements for SQL Server and Hyper-V over SMB

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

* SMB 3.0 must be enabled to use ODX copy offload.
* Source volumes must be a minimum of 1.25 GB.
* Deduplication must be enabled on volumes used with copy offload.
* Compression must *not* be enabled on volumes used with copy offload.
* To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.

  The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

Recommendations for SQL Server and Hyper-V over SMB configurations

To ensure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

General recommendations

- Separate application server files from general user data.
  If possible, devote an entire Storage Virtual Machine (SVM) and its storage for the application server's data.
- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as ARL because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use iSCSI drives when creating virtual machines or when adding disks to an existing virtual machine.

Planning the configuration

Before you configure Hyper-V or SQL Server over SMB for nondisruptive operations, you must understand the choices you need to make. You should plan your volume, LIF, and share configuration prior to performing the configuration. This can help you create a configuration that follows the best practices and recommendations.

Related concepts

Configuration requirements and considerations on page 353

Related tasks

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB on page 367

Completing the data LIF and network configuration worksheet

Use this worksheet to record the values that you need when creating data LIFs and completing the network configuration for SQL Server and Hyper-V over SMB configurations.

Information for creating LIFs on the SVM

Types of information	Values
Data LIF names The name to give to the logical network interfaces that clients use when accessing data from the CIFS server. The Storage Virtual Machine (SVM) must have at least one data LIF on every node in the cluster. You can provide descriptive names for the interfaces, such as naming the data LIFs according to the node assigned as their home node. For example, you can name a LIF whose home node is node1 "lif1", a LIF whose home node is node2 "lif2", and so on.	
Protocols allowed on the data LIFs Protocols that can use the data LIFs (CIFS, NFS, FlexCache, iSCSI, and FC). This is an optional setting. By default, CIFS, NFS, and FlexCache are allowed. **Note:** You cannot modify the list of protocols that can use the LIF after the LIF is created.	
Data LIF home node The node to which the logical interface returns when the LIF is reverted to its home port. Record a home node for each data LIF.	
Data LIF home port The port to which the logical interface returns when the LIF is reverted to its home port. Record a home port for each data LIF.	
Data LIF IP addresses Record an IP address for each data LIF. All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.	
Data LIF network mask Record the netmask for the data LIFs.	

Types of information	Values
Optional custom routing groups for the data Data ONTAP automatically creates a routing group that is appropriate for the netmask provided when creating the data LIF. If an appropriate routing group exists, Data ONTAP assigns the existing routing group to the LIF. You can optionally create your own custom routing group.	
Data LIF default gateway IP address Record the IP address of the default gateway.	
Optional static routes for the data LIF You can configure optional static routes for the routing group assigned to the data LIFs.	

Information for DNS entries on the DNS server for the data LIFS

After you configure your data LIFs, the DNS administrator must create DNS "A" and "PTR" records for the IP addresses assigned to the data LIFs. To load balance client connections to the assigned data IP addresses, you must create multiple "A" records that all point to the same host name. DNS will load balance connections that are made using the host name to the assigned IP addresses in a round-robin fashion.

Note: If you assigned the CIFS server a name that is different from the SVM name, you must create DNS entries that point to the CIFS server name instead of the SVM name. Clients must use the CIFS server name when connecting to continuously available SMB shares, not the SVM name.

For example, if you create a CIFS server named "CIFS1" in the EXAMPLE.LOCAL domain that is hosted on the SVM named "vs1" and assign the IP addresses 10.1.1.1, 10.1.1.2, 10.1.1.3, and 10.1.1.4 to the four data LIFs, your DNS "A" record entries are as follows:

```
10.1.1.1 A CIFS1.EXAMPLE.COM CIFS1
10.1.1.2 A CIFS1.EXAMPLE.COM CIFS1
10.1.1.3 A CIFS1.EXAMPLE.COM CIFS1
10.1.1.4 A CIFS1.EXAMPLE.COM CIFS1
```

There are alternative methods for creating the data LIF DNS records and managing DNS load balancing for the CIFS server. Data ONTAP supports onboard SVM DNS load balancing using DNS delegation. To learn more about SVM DNS load balancing, see the section about balancing network loads in the *Clustered Data ONTAP Network Management Guide*. To learn more about configuring DNS load balancing using delegation and conditional forwarding, see the knowledge base article *How to set up DNS load balancing in Cluster-Mode* on the support site: *support.netapp.com*.

Types of information	Values
DNS A and PTR records for the CIFS server You need to create "A" and "PTR" records for IP addresses assigned to the data LIFs. The host name for these records is the CIFS server name.	

Completing the volume configuration worksheet

Use this worksheet to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- Storage Virtual Machine (SVM) name
  The SVM name is the same for all volumes.
- Volume name
- Aggregate name
  You can create volumes on aggregates located on any node in the cluster.
- Size
- Junction path
- NTFS security style
  If the root volume has NTFS security style, all volumes contained on the SVM inherit the NTFS security style. If the root volume does not have NTFS security style, you must specify the security style when you create the volume.

You should keep the following in mind when creating volumes used to store application server data:

- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the Snapshot copy space reserve to 0.
- The Snapshot policy applied to the volume must be disabled.
  If the SVM Snapshot policy is disabled, then you do not need to specify a Snapshot policy for the volumes. The volumes inherit the Snapshot policy for the SVM. If the Snapshot policy for the SVM is not disabled and is configured to create Snapshot copies, you must specify a Snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage Snapshot copy creation and deletion.
- You cannot configure volumes as FlexCache volumes.
- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named "vol1", "vol2", "vol3", and "vol4", you can create the namespace shown in the example. You can then create shares for the application servers at the following paths: /data1/vol1, /data1/vol2, /data2/vol3, and /data2/vol4.

```
                        Junction                              Junction
Vserver Volume          Active    Junction Path               Path Source
------- ------------    --------  -------------------         -----------
vs1     data1           true      /data1                      RW_volume
vs1     vol1            true      /data1/vol1                 RW_volume
vs1     vol2            true      /data1/vol2                 RW_volume
vs1     data2           true      /data2                      RW_volume
vs1     vol3            true      /data2/vol3                 RW_volume
vs1     vol4            true      /data2/vol4                 RW_volume
```

Types of information	Values
Volume 1: Volume name, aggregate, size, junction path	
Volume 2: Volume name, aggregate, size, junction path	
Volume 3: Volume name, aggregate, size, junction path	
Volume 4: Volume name, aggregate, size, junction path	
Volume 5: Volume name, aggregate, size, junction path	
Volume 6: Volume name, aggregate, size, junction path	
Additional volumes: Volume name, aggregate, size, junction path	

Completing the SMB share configuration worksheet

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

Information about SMB shares properties and configuration settings

For each share, you must specify the following information:

- Storage Virtual Machine (SVM) name
  The SVM name is the same for all shares
- Share name
- Path
- Share properties
  You must configure the following two share properties:

  - oplocks

- `continuously-available`

The following share properties must not be set:

- `homedirectory`
- `changenotify`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

> **Note:** With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

- Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null [""]).

Information about share paths

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on volumes "vol1", "vol2", "vol3", and "vol4", you should create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                         Junction                           Junction
Vserver  Volume          Active    Junction Path            Path Source
-------  ------------    --------  -------------------      -----------
vs1      data1           true       /data1                  RW_volume
vs1      vol1            true       /data1/vol1             RW_volume
vs1      vol2            true       /data1/vol2             RW_volume
vs1      data2           true       /data2                  RW_volume
vs1      vol3            true       /data2/vol3             RW_volume
vs1      vol4            true       /data2/vol4             RW_volume
```

> **Note:** Although you can create shares on the `/data1` and `/data2` paths for administrative management, you must not configure the application servers to use those shares to store data.

Planning worksheet

Types of information	Values
Volume 1: SMB share name and path	

Types of information	Values
Volume 2: SMB share name and path	
Volume 3: SMB share name and path	
Volume 4: SMB share name and path	
Volume 5: SMB share name and path	
Volume 6: SMB share name and path	
Volume 7: SMB share name and path	
Additional volumes: SMB share names and paths	

Creating Data ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

There are several Data ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you begin

You must have already created an SVM, configured DNS, set up desired names services, and created the CIFS server.

Steps

1. Verifying that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares) on page 369
Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

2. Verifying that domain accounts map to the default UNIX user on page 370
Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

3. Verifying that the security style of the SVM root volume is set to NTFS on page 372
To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the Storage Virtual Machine (SVM), the security style of the root volume should be set to NTFS.

4. Verifying that required CIFS server options are configured on page 373
   You must verify that the required CIFS server options are enabled and configured according to
   requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

5. Verifying that automatic node referrals are disabled on page 375
   Automatic node referrals are not supported for nondisruptive operations with Hyper-V and SQL
   Server over SMB configurations. You must verify that automatic node referrals are disabled on
   CIFS servers that provide nondisruptive operations for application servers over SMB.

6. Creating data LIFs (cluster administrators only) on page 376
   Before Hyper-V and SQL Server application servers can connect to continuously available shares,
   you must create data LIFs for the Storage Virtual Machine (SVM).

7. Creating NTFS data volumes on page 378
   You must create NTFS data volumes on the Storage Virtual Machine (SVM) before you can
   configure continuously available shares for use with Hyper-V or SQL Server over SMB
   application servers. Use the volume configuration worksheet to create your data volumes.

8. Creating continuously available SMB shares on page 379
   After you create your data volumes, you can create the continuously available shares that the
   application servers use to access Hyper-V virtual machine and configuration files and SQL Server
   database files. You should use the share configuration worksheet as you create the SMB shares.

9. Adding the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares) on
page 380
   The domain user account used for installing the SQL server must be assigned the
   "SeSecurityPrivilege" privilege to perform certain actions on the CIFS server that require
   privileges not assigned by default to domain users.

10. Configuring the VSS shadow copy directory depth (for Hyper-V over SMB shares) on page 381
    Optionally, you can configure the maximum depth of directories within SMB shares on which to
    create shadow copies. This parameter is useful if you want to manually control the maximum level
    of subdirectories on which Data ONTAP should create shadow copies.

Related concepts

Planning the configuration on page 361
Configuration requirements and considerations on page 353

Verifying that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

About this task

Kerberos authentication is required when making a continuously available share connection. Part of the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the Storage Virtual Machine (SVM).
  Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can be used to restrict access based on authentication method.
  Prior to Data ONTAP 8.2, configuring export policies for SMB access was a requirement. Export policies control what types of authentication are allowed when accessing data using NAS protocols.
  Starting with Data ONTAP 8.2 and later releases, export policies for SMB are optional and are disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication are allowed on a CIFS server by default.
- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and NTLMv2 authentication.
  Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2 authentication can be disallowed, either using Security Policy settings or Group Policies.

Steps

1. Perform the following to verify that export policies are disabled on the SVM:
   a) Set the privilege level to advanced:

   `set -privilege advanced`
   b) Verify that the `-is-exportpolicy-enabled` CIFS server option is set to `false`:

   `vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled`
   c) Return to the admin privilege level:

   `set -privilege admin`

2. If export policies for SMB are not disabled, disable them:

   `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTMLv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver   is-exportpolicy-enabled
--------  -----------------------
vs1       false

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

Verifying that domain accounts map to the default UNIX user

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

Starting with Data ONTAP 8.2 and later releases, when you create a Storage Virtual Machine (SVM), Data ONTAP automatically creates the default user named "pcuser" (with a UID of 65534) and the group named "pcuser" (with a GID of 65534), and adds the default user to the "pcuser" group. If you are configuring a Hyper-V over SMB solution on an SVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server's default UNIX user.

Steps

1. Determine whether there is a default UNIX user:

   vserver cifs options show -vserver *vserver_name*

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

vserver services unix-user show -vserver *vserver_name*

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default UNIX user and the default group, and add the default user to the group.

   Generally, the default user is given the user name "pcuser" and must be assigned the UID of 65534. The default group is generally given the group name "pcuser". The GID assigned to the group must be 65534.

   a) Create the default group:

      vserver services unix-group create -vserver *vserver_name* **-name pcuser -id 65534**

   b) Create the default user and add the default user to the default group:

      vserver services unix-user create -vserver *vserver_name* **-user pcuser -id 65534 -primary-gid 65534**

   c) Verify that the default user and default group are configured correctly:

      vserver services unix-user show -vserver *vserver_name*

      vserver services unix-group show -vserver *vserver_name* **-members**

4. If the CIFS server's default user is not configured, perform the following:

   a) Configure the default user:

      vserver cifs options modify -vserver *vserver_name* **-default-unix-user pcuser**

   b) Verify that the default UNIX user is configured correctly:

      vserver cifs options show -vserver *vserver_name*

5. To verify that the application server's computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the vserver cifs sessions show command.

   For more information about using this command, see the man pages.

Example

The following commands determine that the CIFS server's default user is not set, but determines that the "pcuser" user and "pcuser" group exist. The "pcuser" user is assigned as the CIFS server's default user on SVM vs1:

```
cluster1::> vserver cifs options show

                                    Vserver: vs1
                          Default UNIX User: -
                Read Grants Exec for Mode Bits: disabled
Windows Internet Name Service (WINS) Addresses: -
                         Default UNIX Group: -


cluster1::> vserver services unix-user show
```

```
          User               User    Group  Full
Vserver   Name               ID      ID     Name
--------- --------------     ------  ------ ---------------
vs1       nobody             65535   65535  -
vs1       pcuser             65534   65534  -
vs1       root               0       1      -

cluster1::> vserver services unix-group show -members
Vserver         Name               ID
vs1             daemon             1
     Users: -
vs1             nobody             65535
     Users: -
vs1             pcuser             65534
     Users: -
vs1             root               0
     Users: -

cluster1::> vserver cifs options modify -default-unix-user pcuser

cluster1::> vserver cifs options show

                                     Vserver: vs1
                          Default UNIX User: pcuser
                Read Grants Exec for Mode Bits: disabled
Windows Internet Name Service (WINS) Addresses: -
                          Default UNIX Group: -
```

Verifying that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the Storage Virtual Machine (SVM), the security style of the root volume should be set to NTFS.

About this task

- You can specify the root volume security style at the time you create the SVM.
- If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the volume modify command.

Steps

1. Determine the current security style of the SVM root volume:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:

   volume modify -vserver *vserver_name* -volume *root_volume_name* -security-style ntfs

3. Verify that the SVM root volume is set to NTFS security style:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver   volume      security-style
--------  ----------  --------------
vs1       vs1_root    unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver   volume      security-style
--------  ----------  --------------
vs1       vs1_root    ntfs
```

Verifying that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

Steps

1. Perform the following to verify that the required CIFS server options are enabled on the Storage Virtual Machine (SVM):

   a) Set the privilege level to advanced:

      set -privilege advanced

   b) Enter the following command:

      vserver cifs options show -vserver *vserver_name*

      The following options should be set to true:

      - -smb2-enabled
      - -smb3-enabled
      - -copy-offload-enabled
      - -shadowcopy-enabled (Hyper-V only)

2. If any of the options are not set to true, perform the following:

   a) Set them to true by using the vserver cifs options modify command.

   b) Verify that the options are set to `true` by using the `vserver cifs options show` command.

3. Return to the admin privilege level:

```
set -privilege admin
```

Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show

                                           Vserver: vs1
                                Default UNIX User: pcuser
                     Read Grants Exec for Mode Bits: disabled
     Windows Internet Name Service (WINS) Addresses: -
                   Enable/Disable all SMB2 Protocols: true
                    Enable/Disable the SMB3 Protocol: true
Maximum Simultaneous Operations per TCP Connection: 255
        Maximum Depth of Directories to Shadow Copy: 5
             Enable/Disable the Copy Offload Feature: false
                                 Default UNIX Group: -
       Enable/Disable the Shadow Copy Feature (VSS): true
                 Refer Clients to More Optimal LIFs: false
            Enable/Disable Local User Authentication: true
                Enable/Disable Local Users and Groups: true
                Enable/Disable Reparse Point Support: true
            Enable/Disable Export Policies for CIFS: false
Enable/Disable Enumeration of Trusted Domain and Search Capability: true
Size of File System Sector Reported to SMB Clients (bytes): 4096

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload-
enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver   copy-offload-enabled
--------  --------------------
vs1       true

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

Verifying that automatic node referrals are disabled

Automatic node referrals are not supported for nondisruptive operations with Hyper-V and SQL Server over SMB configurations. You must verify that automatic node referrals are disabled on CIFS servers that provide nondisruptive operations for application servers over SMB.

About this task

Automatic node referrals are disabled by default. If you have enabled them on the CIFS server that will provide nondisruptive services over SMB shares, you must disable them.

Steps

1. Perform the following to verify that automatic node referrals are disabled on the CIFS server:

   a) Set the privilege level to advanced:

      `set -privilege advanced`

   b) Verify that the `-is-referral-enabled` CIFS server option is set to `false`:

      `vserver cifs options show -vserver vserver_name -fields is-referral-enabled`

2. If automatic node referrals are not disabled, perform the following:

   a) Disable automatic node referrals:

      `vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   b) Verify that the new setting is correct:

      `vserver cifs options show -vserver vserver_name -fields is-referral-enabled`

3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following commands verify that automatic node referrals are disabled on Storage Virtual Machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields is-referral-
enabled

vserver  is-referral-enabled
-------- -------------------
vs1      false
```

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

Creating data LIFs (cluster administrators only)

Before Hyper-V and SQL Server application servers can connect to continuously available shares, you must create data LIFs for the Storage Virtual Machine (SVM).

Before you begin

You must have the list of IP addresses to assign to the data LIFs.

About this task

- You can associate data LIFs with ports that are assigned the data role.
- To use host names to connect to the CIFS server data ports, you must create DNS "A" and "PTR" record entries that assign the IP addresses to the FQDN of the CIFS server.
- You must not configure the data LIFs that carry traffic for the application servers to automatically revert to their home nodes.

This task can only be completed by a cluster administrator.

Steps

1. Determine what data ports are available:

   network port show -role data

2. Using the information in the planning worksheet, create the SVM data LIFs:

   network interface create -vserver *vserver_name* -lif *lif_name* -role data -home-node *node_name* -home-port *port* -address -netmask-length *integer*

   For more information about configuring LIFs, see the *Clustered Data ONTAP Network Management Guide*.

   After the command executes, the following message is displayed: Info: Your interface was created successfully; the routing group <routing_group_name> was created. An associated routing group is automatically created when you create the first data LIF in an IP subnet. A routing group is a container for SVM routes, including the default route.

3. Record the name of the routing group.

4. Create a default (static) route for the data LIFs:

   network routing-groups route create -vserver *vserver_name* -routing-group *routing_group_name* -destination 0.0.0.0/0 -gateway *gateway_IP_address*

5. Verify that the LIF network configuration is correct by using the network interface show and network routing-groups route show commands.

For more information about configuring network solutions, see the *Clustered Data ONTAP Network Management Guide*.

6. Create the DNS "A" and "PTR" records for the data LIF IP addresses assigned to the CIFS server.

Example

The following commands create a data LIF on each node in the cluster for SVM vs1:

- The CIFS server name is "CIFS1", and it is a member of the IEPUB.LOCAL domain.
- A default route is added to the routing group that was automatically created during LIF creation.
- The following DNS "A" records and the corresponding "PTR" records are added to the DNS server

```
10.1.1.128 A CIFS1.IEPUB.LOCAL CIFS1
10.1.1.129 A CIFS1.IEPUB.LOCAL CIFS1
10.1.1.130 A CIFS1.IEPUB.LOCAL CIFS1
10.1.1.131 A CIFS1.IEPUB.LOCAL CIFS1
```

```
cluster1::> network port show -role data
                                    Auto-Negot  Duplex     Speed (Mbps)
Node   Port   Role          Link   MTU Admin/Oper  Admin/Oper Admin/Oper
------ ------ ------------  ----  ----- ----------- ---------- ------------
node1
       a0a    data          down  1500  true/-      auto/-     auto/-
       e0c    data          up    1500  true/true   full/full  auto/1000
       e0d    data          up    1500  true/true   full/full  auto/1000
       e1b    data          up    1500  true/true   full/full  auto/1000
       e1c    data          down  1500  true/true   full/half  auto/10
       e1d    data          down  1500  true/true   full/half  auto/10
node2
       e0c    data          up    1500  true/true   full/full  auto/1000
       e0d    data          up    1500  true/true   full/full  auto/1000
       e1b    data          up    1500  true/true   full/full  auto/1000
       e1c    data          down  1500  true/true   full/half  auto/10
       e1d    data          down  1500  true/true   full/half  auto/10
node3
       e0c    data          up    1500  true/true   full/full  auto/1000
       e0d    data          up    1500  true/true   full/full  auto/1000
       e1b    data          up    1500  true/true   full/full  auto/1000
       e1c    data          down  1500  true/true   full/half  auto/10
       e1d    data          down  1500  true/true   full/half  auto/10
node4
       e0c    data          up    1500  true/true   full/full  auto/1000
       e0d    data          up    1500  true/true   full/full  auto/1000
       e1b    data          up    1500  true/true   full/full  auto/1000
       e1c    data          down  1500  true/true   full/half  auto/10
       e1d    data          down  1500  true/true   full/half  auto/10

cluster1::> network interface create -vserver vs1 -lif lif1 -role data -
home-node node1 -home-port e1b -address 10.1.1.128 -netmask-length 24

Info: Your interface was created successfully; the routing group
d10.1.1.0/24 was created

cluster1::> network interface create -vserver vs1 -lif lif2 -role data -
home-node node2 -home-port e1b -address 10.1.1.129 -netmask-length 24
```

```
cluster1::> network interface create -vserver vs1 -lif lif3 -role data -
home-node node3 -home-port e1b -address 10.1.1.130 -netmask-length 24
cluster1::> network interface create -vserver vs1 -lif lif4 -role data -
home-node node4 -home-port e1b -address 10.1.1.131 -netmask-length 24

cluster1::> network routing-groups route create -vserver vs1 -routing-
group  d10.1.1.0/24 -destination 0.0.0.0/0 -gateway  10.1.1.1

cluster1::> network interface show -vserver vs1
          Logical    Status     Network         Current     Current  Is
Vserver   Interface  Admin/Oper Address/Mask    Node        Port     Home
--------- ---------- ---------- --------------- ----------  -------  ----
vs1
          lif1       up/up      10.1.1.128/24   node1       e1b      true
          lif2       up/up      10.1.1.129/24   node2       e1b      true
          lif3       up/up      10.1.1.130/24   node3       e1b      true
          lif4       up/up      10.1.1.131/24   node4       e1b      true

cluster1::> network routing-groups route show -vserver vs1
          Routing
Vserver   Group           Destination    Gateway      Metric
--------- ------------    ------------- ----------    ------
vs1       d10.1.1.0/24    0.0.0.0/0      10.1.1.1      20
```

Creating NTFS data volumes

You must create NTFS data volumes on the Storage Virtual Machine (SVM) before you can
configure continuously available shares for use with Hyper-V or SQL Server over SMB application
servers. Use the volume configuration worksheet to create your data volumes.

About this task

There are optional parameters that you can use to customize a data volume. For more information
about customizing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

As you create your data volumes, you should not create junction points within a volume that contains
the following:

- Hyper-V files for which Data ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server

Note: If you inadvertently create a volume that uses mixed or UNIX security style, you cannot
change the volume to an NTFS security style volume and then directly use it to create
continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V
and SQL Server over SMB do not work correctly unless the volumes used in the configuration are
created as NTFS security-style volumes.

You must either delete the volume and re-create the volume with NTFS security style, or you can
map the volume on a Windows host and apply an ACL at the top of the volume and propagate the
ACL to all files and folders in the volume.

Steps

1. Create the data volume by entering the appropriate command:

If you want to create a volume in an SVM where the root volume security style is...	Enter the command...
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Not NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -security-style ntfs -junction-path path`

2. Verify that the volume configuration is correct:

   `volume show -vserver vserver_name -volume volume_name`

Creating continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

Steps

1. Display information about the existing data volumes and their junction paths:

   `volume show -vserver vserver_name -junction`

2. Create a continuously available SMB share by entering the following command:

   `vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties oplocks,continuously-available -symlink "" [-comment text]`

   - You can optionally add a comment to the share configuration.
   - By default, the offline files share property is configured on the share and is set to `manual`.
   - Data ONTAP creates the share with the Windows default share permission of `Everyone /Full Control`.

3. Repeat the previous step for all shares in the share configuration worksheet.

4. Verify that your configuration is correct by using the `vserver cifs share show` command.

5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the **Windows Properties** window.

Example

The following commands create a continuously available share named "data2" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the -symlink parameter to "":

```
cluster1::> volume show -vserver vs1 -junction
                       Junction                     Junction
Vserver   Volume      Active   Junction Path        Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data                RW_volume
vs1       data1       true     /data/data1          RW_volume
vs1       data2       true     /data/data2          RW_volume
vs1       vs1_root    -        /                    -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path /
data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                          Vserver: vs1
                            Share: data2
        CIFS Server NetBIOS Name: VS1
                             Path: /data/data2
                 Share Properties: oplocks
                                   continuously-available
                Symlink Properties: -
           File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
```

Adding the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the "SeSecurityPrivilege" privilege to perform certain actions on the CIFS server that require privileges not assigned by default to domain users.

Before you begin

The domain account used for installing the SQL Server must already exist.

About this task

When adding the privilege to the SQL Server installer's account, Data ONTAP might validate the account by contacting the domain controller. The command might fail if Data ONTAP cannot contact the domain controller.

Steps

1. Add the "SeSecurityPrivilege" privilege:

    ```
    vserver cifs users-and-groups privilege add-privilege -vserver
    vserver_name -user-or-group-name account_name -privileges
    SeSecurityPrivilege
    ```

    The value for the -user-or-group-name parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

    ```
    vserver cifs users-and-groups privilege show -vserver vserver_name -user-
    or-group-name account_name
    ```

    > **Example**
    >
    > The following command adds the "SeSecurityPrivilege" privilege to the SQL Server installer's account in the EXAMPLE domain for Storage Virtual Machine (SVM) vs1:
    >
    > ```
    > cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
    > vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges SeSecurityPrivilege
    >
    > cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
    > Vserver    User or Group Name          Privileges
    > ---------  --------------------        --------------
    > vs1        EXAMPLE\SQLinstaller         SeSecurityPrivilege
    > ```

Configuring the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which Data ONTAP should create shadow copies.

Before you begin

The VSS shadow copy feature must be enabled.

About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to 0, Data ONTAP creates shadow copies for all subdirectories.

> **Note:** Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Set the VSS shadow copy directory depth to the desired level:

   `vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth integer`

   Example

   `vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6`

3. Return to the admin privilege level:

   `set -privilege admin`

Managing Hyper-V and SQL Server over SMB configurations

There are certain Data ONTAP tasks that you can perform to manage Hyper-V and SQL Server over SMB configurations.

Related tasks

Configuring existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the homedirectory share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The -offline-files parameter is set to either manual (the default) or none.
- Symlinks must be disabled.

The following share properties must be configured:

- `continuously-available`
- `oplocks`

The following share properties must not be set. If they are present in the list of current share properties, they need to be removed from the continuously available share:

- `changenotify`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps

1. Display the current share parameter settings and the current list of configured share properties:

   `vserver cifs share show -vserver vserver_name -share-name share_name`

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the `vserver cifs share properties modify` command.

   You can disable symlinks by setting the value of the `-symlink` parameter to `""`.

   - You can disable symlinks by setting the value of the `-symlink` parameter to `""`.
   - You can set the `-offline-files` parameter to the correct setting by specifying `manual`.

3. Add the `continuously-available` share property, and, if needed, the `oplocks` share property:

   `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties continuously-available[,oplock]`

   If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

   `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties properties[,...]`

   You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

   `vserver cifs share show -vserver vserver_name -share-name share_name -fields symlink-properties,offline-files`

6. Verify that the list of configured share properties is correct:

   `vserver cifs shares properties show -vserver vserver_name -share-name share_name`

Examples

The following example shows how to configure an existing share named "share1" on Storage
Virtual Machine (SVM) vs1 for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the -symlink parameter to "".
- The -offline-file parameter is modified and set to manual.
- The continuously-available share property is added to the share.
- The oplocks share property is already in the list of share properties; therefore, it does not
  need to be added.
- The attributecache and changenotify share properties are removed from the share.
- The browsable share property is optional for a continuously available share used for
  NDOs with application servers over SMB and is retained as one of the share properties.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                       Vserver: vs1
                         Share: share1
       CIFS Server NetBIOS Name: vs1
                          Path: /data
              Share Properties: oplocks
                                browsable
                                changenotify
                                attributecache
            Symlink Properties: enable
       File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                     Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1 -
offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name share1 -fields
symlink-properties,offline-files
vserver   share-name symlink-properties offline-files
--------  ---------- ------------------ -------------
vs1       share1     -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

          Vserver: vs1
            Share: share1
Share Properties: oplocks
```

```
                          browsable
                          continuously-available
```

Enabling or disabling VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

About this task

You can enable or disable VSS shadow copies at any time.

Steps

1. Set the privilege level to advanced:

   set -privilege advanced

2. Perform one of the following actions:

If you want VSS shadow copies to be...	Enter the command...
Enabled	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
Disabled	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. Return to the admin privilege level:

   set -privilege admin

   > **Example**
   >
   > The following commands enable VSS shadow copies on SVM vs1:
   >
   > ```
   > cluster1::> set -privilege advanced
   > Warning: These advanced commands are potentially dangerous; use them
   > only when directed to do so by technical support personnel.
   > Do you wish to continue? (y or n): y
   >
   > cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
   > true
   >
   > cluster1::*> set -privilege admin
   > ```

Considerations for reverting Hyper-V over SMB configurations

Before you revert to a Data ONTAP version that does not support nondisruptive operations for Hyper-V over SMB, you must be aware of certain considerations to ensure that you are prepared for the revert.

Before you revert, you must consider the following and take action where necessary:

- If you are reverting to a version of Data ONTAP that does not support SMB 3.0 and persistent handle locks, operations such as failover and giveback are disruptive because Hyper-V servers cannot reclaim disconnected durable handles.
- There must be no file access by the Hyper-V servers to virtual machine files when you revert:
  - You can use the Hyper-V application to migrate virtual machine files to another storage device or to local storage.
  - You can power down all virtual machines and manually terminate Hyper-V server connections to the data LIFs.

    Data ONTAP disables SMB 3.0 before reverting; therefore, if the SMB connections are not manually terminated, Data ONTAP terminates them during the revert.
- You cannot use the Hyper-V over SMB solution if you revert to a version of Data ONTAP that does not support it.

  You must configure the Hyper-V servers to use connected LUNs to store and access virtual machine files. You must then copy the virtual machine files from the SMB shares to the connected LUNs.
- To revert, there can be no ongoing Remote VSS shadow copy operations.

  If there are any, you must wait for the operations to finish or manually abort them before proceeding with the revert. If you need to abort any shadow copy operations, contact technical support for assistance. Upon a revert, Data ONTAP does not delete existing Snapshot copies.

Considerations for reverting SQL Server over SMB configurations

Before you revert to a Data ONTAP version that does not support nondisruptive operations for SQL Server over SMB shares, you must be aware of certain considerations to ensure that you are prepared for the revert.

Before you revert, you must consider the following and take action where necessary:

- If you are reverting to a version of Data ONTAP that does not support SMB 3.0 and persistent handle locks, operations such as failover and giveback are disruptive because SQL Server servers cannot reclaim disconnected durable handles.
- There must be no file access by the SQL Server servers to database files when you revert:
  - You can use the SQL Server application to migrate database files to another storage device or to local storage.
  - You can shut down all SQL Server databases and manually terminate SQL Server connections to the data LIFs.

Data ONTAP disables SMB 3.0 before reverting; therefore, if the SMB connections are not manually terminated, Data ONTAP terminates them during the revert.

- You cannot use the SQL Server SMB 3.0 continuously available shares for nondisruptive operations if you revert to a version of Data ONTAP that does not support it.

  You must configure the SQL Server servers to use connected LUNs to store and access database files. You must then move the database files from the SMB shares to the connected LUNs.

Using statistics to monitor Hyper-V and SQL Server over SMB activity

You can display various CIFS and SMB statistics to monitor Hyper-V and SQL Server over SMB activity. For example, you can obtain information about the number of SMB sessions, the number of sessions from clients with continuously available capability, and the number of reconnection requests.

Related tasks

[Determining whether SMB sessions are continuously available](#) on page 395

Determining which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Step

1. Perform one of the following actions:

If you want to determine...	Enter the following...
Which objects are available	**statistics catalog object show**
Specific objects that are available	**statistics catalog object show -object** *object_name*
Which counters are available at the admin privilege level	**statistics catalog counter show -object** *object_name*
Which counters are available at the advanced privilege level	**set -privilege advanced** **statistics catalog counter show -object** *object_name*

See the man pages for more information.

Examples

The following example displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster:

```
cluster1::> statistics catalog object show -object audit
    audit_ng                  CM object for exporting audit_ng performance
                              counters

cluster1::> statistics catalog object show -object cifs
    cifs                      The CIFS object reports activity of the
                              Common Internet File System protocol
                              subsystem. This is the Microsoft file-sharing
                              protocol that evolved from the Server Message
                              Block (SMB) application layer network
                              protocol to connect PCs to Network Attached
                              Storage devices (NAS). This object reports
                              activity for both SMB and SMB2 revisions of
                              the CIFS protocol. For information related
                              only to SMB, see the 'smb1' object. For
                              information related only to SMB2, see the
                              'smb2' object.

cluster1::> statistics catalog object show -object nblade_cifs
    nblade_cifs               Exported counters associated with the
                              N-Blade's CIFS subsystem and relevant to the
                              entire node, rather than individual virtual
                              servers.

cluster1::> statistics catalog object show -object smb1
    smb1                      These counters report activity from the SMB
                              revision of the protocol. For information
                              specific to SMB2, see the 'smb2' object. To
                              see an overview across both revisions, see
                              the 'cifs' object.

cluster1::> statistics catalog object show -object smb2
    smb2                      These counters report activity from the SMB2
                              revision of the protocol. For information
                              specific to SMB, see the 'smb1' object. To
                              see an overview across both revisions, see
                              the 'cifs' object.

cluster1::> statistics catalog object show -object hashd
    hashd                     The hashd object provides counters to measure
                              the performance of the BranchCache hash
                              daemon.
```

The following example displays information about some of the counters for the `cifs` object as seen at the advanced-privilege level:

Note: This example does not display all of the available counters for the `cifs` object. Output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only when
directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                   Description
    ------------------------- ---------------------------------------------
    active_searches           Number of active searches over SMB and SMB2
```

```
        auth_reject_too_many        Authentication refused after too many
                                    requests were made in rapid succession
        avg_directory_depth         Average number of directories crossed by SMB
                                    and SMB2 path-based commands
        avg_junction_depth          Average number of junctions crossed by SMB
                                    and SMB2 path-based commands
        branchcache_hash_fetch_fail Total number of times a request to fetch hash
                                    data failed. These are failures when
                                    attempting to read existing hash data. It
                                    does not include attempts to fetch hash data
                                    that has not yet been generated.
        branchcache_hash_fetch_ok   Total number of times a request to fetch hash
                                    data succeeded.
        branchcache_hash_sent_bytes Total number of bytes sent to clients
                                    requesting hashes.
        branchcache_missing_hash_bytes
                                    Total number of bytes of data that had to be
                                    read by the client because the hash for that
                                    content was not available on the server.
        change_notifications_outstanding
                                    Number of active change notifications over
                                    SMB and SMB2
        cifs_latency                Average latency for CIFS operations
        cifs_latency_base           Total observed CIFS operations to be used as
                                    a base counter for CIFS average latency
                                    calculation
        cifs_ops                    Total number of CIFS operations
        cifs_read_ops               Total number of CIFS read operations
        cifs_write_ops              Total number of CIFS write operations

[...]
```

Related tasks

Displaying SMB statistics

You can display various SMB statistics to monitor performance and diagnose issues.

Steps

1. Use the `statistics start` and optional `statistics stop` commands to collect a data sample.

   For more information about these commands, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

2. Perform one of the following actions:

If you want to display statistics for...	Enter the following command...
All versions of SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x and SMB 3.0	`statistics show -object smb2`

If you want to display statistics for...	Enter the following command...
CIFS subsystem of the node	`statistics show -object nblade_cifs`

See the man page for more information.

Verifying that the configuration is capable of nondisruptive operations

You can verify that the Hyper-V or SQL Server over SMB configuration is healthy and able to perform operations nondisruptively by displaying health monitor information, verifying that the SMB shares are shared persistently, and by verifying the status of the LIF configuration.

How to use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. Data ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

Alert ID	Severity	Condition
`HaNotReadyCifsNdo_Alert`	Major	One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.
`NoStandbyLifCifsNdo_Alert`	Minor	The Storage Virtual Machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.

Displaying nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

About this task

For more information about using system health monitoring, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Monitor health status by performing the appropriate action:

If you want to display...	Enter the command...
The health status of the system, which reflects the overall status of individual health monitors	`system health status show`
Information about the health status of the CIFS-NDO subsystem	`system health subsystem show -subsystem CIFS-NDO -instance`

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

If you want to display information about...	Enter the command...
The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status	`system health config show -subsystem CIFS-NDO`
The CIFS-NDO alerts that a health monitor can potentially generate	`system health alert definition show -subsystem CIFS-NDO`
CIFS-NDO health monitor policies, which determine when alerts are raised	`system health policy definition show -monitor node-connect`

Note: Use the `-instance` parameter to display detailed information.

Examples

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                     Subsystem: CIFS-NDO
                        Health: ok
          Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
```

The following output shows detailed information about the configuration and status of the
health monitor of the CIFS-NDO subsystem:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                            Node: node1
                         Monitor: node-connect
                       Subsystem: SAS-connect, HA-health, CIFS-NDO
                          Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                         Context: node_context
                      Aggregator: system-connect
                        Resource: SasAdapter, SasDisk, SasShelf, HaNodePair,
                                  HaICMailbox, CifsNdoNode, CifsNdoNodeVserver
Subsystem Initialization Status: initialized
     Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0

                            Node: node2
                         Monitor: node-connect
                       Subsystem: SAS-connect, HA-health, CIFS-NDO
                          Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                         Context: node_context
                      Aggregator: system-connect
                        Resource: SasAdapter, SasDisk, SasShelf, HaNodePair,
                                  HaICMailbox, CifsNdoNode, CifsNdoNodeVserver
Subsystem Initialization Status: initialized
     Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0, 1.0
```

Verifying the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as
continuously available shares. Additionally, there are certain other share settings that you must
check. You should verify that the shares are properly configured to ensure seamless nondisruptive
operations for the application servers if there are planned or unplanned disruptive events.

About this task

You must verify that the two following share parameters are set correctly:

- The -offline-files parameter is set to either manual (the default) or none.
- Symlinks must be disabled.

To ensure proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `changenotify`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps

1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:
   vserver cifs shares show -vserver *vserver_name*

2. Verify that the SMB shares are configured for continuous availability:
   vserver cifs shares properties show -vserver *vserver_name*

Examples

The following example displays the share setting for a share named "share1" on Storage Virtual Machine (SVM, formerly known as Vserver) vs1. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the *Symlink Properties* field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
      CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
              Share Properties: oplocks
                                continuously-available
            Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named "share1" on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver     Share   Properties
---------   ------  ----------
vs1         share1  oplocks
                    continuously-available
```

Verifying LIF status

Even though you configured the Storage Virtual Machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have data LIFs on each node in the cluster, during day-to-day operations some data LIFs might have moved to ports on another node. You need to verify LIF status and take any necessary corrective actions.

About this task

To provide seamless nondisruptive operation support, all SVM data LIFs must be associated with their home port. If some of the configured LIFs are not currently associated with their home port, you need to fix any port issues and then revert the LIFs to their home port.

Steps

1. Display information about configured data LIFS for the SVM:

   network interface show -vserver *vserver_name*

   Each node in the cluster should have at least one data LIF for the SVM, and the LIFs should be associated with the LIF's home port.

2. If some of the data LIFs are not on their home port, perform the following:

   a) For each data LIF, determine what the LIF's home port is:

   network interface show -vserver *vserver_name* -lif *lif_name* -failover

   b) For each data LIF, determine whether the LIF's home port is up:

   network port show -node *node_name* -port *port* -fields node,port,role,link

3. If any of the home port network interfaces to which the data LIFs should be associated are not in the up state, resolve the problem so that these interfaces are up.

4. If needed, revert the LIFs back to the home port:

   network interface revert -vserver *vserver_name* -lif *lif_name*

5. Verify that each node in the cluster has an active data LIF for the SVM:

   network interface show -vserver *vserver_name*

   Example

   The following commands verify that SVM vs1 has at least one data LIF on every node in the cluster, by associating all data LIFs for SVM vs1 with their home port:

   ```
   cluster1::> network interface show -vserver vs1
               Logical     Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask      Node       Port    Home
   ----------- ---------- ---------- ---------------- ---------- ------- ----
   vs1
               lif1       up/up      10.1.1.128/24     node3      e1b     false
   ```

```
                   lif2          up/up    10.1.1.129/24    node2     e1b    true
                   lif3          up/up    10.1.1.130/24    node3     e1b    true
                   lif4          up/up    10.1.1.131/24    node2     e1b    false
cluster1::> network interface show -vserver vs1 -lif lif1 -failover
         Logical      Home            Failover    Failover
Vserver  Interface    Node:Port       Policy      Group
-------- -----------  --------------- ----------- ---------------
vs1
         lif1         node1:e1b       nextavail   system-defined
                   Failover Targets: node1:e1b, node1:e1c,
                                     node1:e1d, node1:a0a,
                                     node1:e0c, node1:e0d,
                                     node3:e1b, node3:e1c,
                                     node3:e1d, node3:e0c,
                                     node3:e0d
cluster1::> network interface show -vserver vs1 -lif lif4 -failover
         Logical      Home            Failover    Failover
Vserver  Interface    Node:Port       Policy      Group
-------- -----------  --------------- ----------- ---------------
vs1
         lif4         node4:e1b       nextavail   system-defined
                   Failover Targets: node4:e1b, node4:e1c,
                                     node4:e1d, node4:e0c,
                                     node4:e0d, node2:e1b,
                                     node2:e1c, node2:e1d,
                                     node2:e0c, node2:e0d
cluster1::> network port show -node node1 -port e1b -fields node,port,role,link
node    port role link
------  ---- ---- ----
node1   e1b  data up

cluster1::> network port show -node node4 -port e1b -fields node,port,role,link
node    port role link
------  ---- ---- ----
node4   e1b  data up

cluster1::> network interface revert -vserver vs1 -lif lif1

cluster1::> network interface revert -vserver vs1 -lif lif4

cluster1::> network interface show -vserver vs1
         Logical      Status     Network          Current    Current Is
Vserver  Interface    Admin/Oper Address/Mask     Node       Port    Home
-------- -----------  ---------- ---------------- ---------- ------- ----
vs1
         lif1         up/up      10.1.1.128/24    node1      e1b     true
         lif2         up/up      10.1.1.129/24    node2      e1b     true
         lif3         up/up      10.1.1.130/24    node3      e1b     true
         lif4         up/up      10.1.1.131/24    node4      e1b     true
```

Related tasks

Determining whether SMB sessions are continuously available

You can display information about SMB sessions and SMB open files to determine whether they are continuously available.

Related tasks

Displaying SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

About this task

You can display information for all sessions on your Storage Virtual Machine (SVM) in summary form by using the `vserver cifs session show` command without any optional parameters. However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the results contain a large number of records.

- You can use the optional `-fields` parameter to display output on the fields you choose.
- Alternatively, you can use the `-instance` parameter to display detailed information about established SMB sessions.

You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display SMB session information for established sessions...	Enter the following command...
For all sessions on the SVM in summary form	`vserver cifs session show -vserver vserver_name`
On a specified connection ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
From a specified workstation IP address	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
On the specified LIF IP address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`

If you want to display SMB session information for established sessions...	**Enter the following command...**
On a specified node	`vserver cifs session show -vserver vserver_name -node {node_name|local}`
From a specified Windows user	`vserver cifs session show -vserver vserver_name -windows-user user_name` The format for `user_name` is `[domain]\user`.
With a specified authentication mechanism	`vserver cifs session show -vserver vserver_name -auth-mechanism authentication_mechanism` The value for `-auth-mechanism` can be one of the following: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`
With the specified protocol version	`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` **Note:** Continuously available protection is available only on SMB 3.0 sessions. To see continuously available protection status on all qualifying sessions, specify this parameter with the value set to `SMB3`.

If you want to display SMB session information for established sessions...	Enter the following command...
With the specified level of continuously available protection	**vserver cifs session show -vserver** *vserver_name* **-continuously-available** *continuously_available_protection_level* The value for -continuously-available can be one of the following: • No • Yes • Partial **Note:** If the continuously available status is Partial, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the vserver cifs sessions file show command to determine which files on the established session are not open with continuously available protection.

There are additional optional parameters. See the man page for more information.

Examples

The following example displays session information on sessions SVM vs1 established from a workstation with the IP address of 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open       Idle
ID         ID      Workstation     Windows User    Files      Time
---------- ------- --------------- ------------- ------- ------------
3151272279  1       10.1.1.1        DOMAIN\joe          2        23s
```

The following example displays detailed session information on sessions with continuously available protection on SVM vs1. The connection was made by using the domain computer-machine account:

```
cluster1::> vserver cifs session show -instance -continuously-available Yes
                       Node: node1
                    Vserver: vs1
                 Session ID: 1
              Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                  UNIX User: pcuser
                 Open Shares: 1
```

```
              Open Files: 1
              Open Other: 0
          Connected Time: 10m 43s
               Idle Time: 1m 19s
        Protocol Version: SMB3
   Continuously Available: Yes
```

The following example displays session information on sessions using SMB 3.0 on SVM vs1.
The user connected to this share from an SMB 3.0 capable client by using the LIF IP address;
therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made
using Kerberos authentication to connect with continuously available protection:

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                     Node: node1
                  Vserver: vs1
               Session ID: 1
            Connection ID: 3151272607
Incoming Data LIF IP Address: 10.2.1.2
    Workstation IP address: 10.1.1.3
  Authentication Mechanism: NTLMv2
             Windows User: DOMAIN\administrator
                UNIX User: pcuser
              Open Shares: 1
               Open Files: 0
               Open Other: 0
           Connected Time: 6m 22s
                Idle Time: 5m 42s
         Protocol Version: SMB3
   Continuously Available: No
```

Displaying information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID,
the hosting volume, the share name, and the share path. You can display information about a file's
continuously available protection level, which is helpful in determining whether an open file is in a
state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed
information is useful when you need to determine SMB session information for particular files within
an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously
available protection and some are not open with continuously available protection (the value for the -
continuously-available field in vserver cifs session show command output is
Partial), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on Storage Virtual
Machines (SVMs) in summary form by using the vserver cifs session file show command
without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.
  You can use this parameter either alone or in combination with other optional parameters.
- You can use the `-instance` parameter to display detailed information about open SMB files.
  You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display open SMB files...	Enter the following command...
On the SVM in summary form	`vserver cifs session file show -vserver vserver_name`
On a specified node	`vserver cifs session file show -vserver vserver_name -node {node_name|local}`
On a specified file ID	`vserver cifs session file show -vserver vserver_name -file-id integer`
On a specified SMB connection ID	`vserver cifs session file show -vserver vserver_name -connection-id integer`
On a specified SMB session ID	`vserver cifs session file show -vserver vserver_name -session-id integer`
On the specified hosting aggregate	`vserver cifs session file show -vserver vserver_name -hosting-aggregate aggregate_name`
On the specified volume	`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`
On the specified SMB share	`vserver cifs session file show -vserver vserver_name -share share_name`
On the specified SMB path	`vserver cifs session file show -vserver vserver_name -path path`

If you want to display open SMB files...	Enter the following command...
With the specified level of continuously available protection	**vserver cifs session file show -vserver** *vserver_name* **-continuously-available** *continuously_available_status* The value for -continuously-available can be one of the following: • No • Yes **Note:** If the continuously available status is No, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	**vserver cifs session file show -vserver** *vserver_name* **-reconnected** *reconnected_state* The value for -reconnected can be one of the following: • No • Yes **Note:** If the reconnected state is No, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is Yes, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File       Open Hosting                Continuously
ID      Type       Mode Volume     Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular    r    data      data        Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82 -
instance
```

```
                   Node: node1
                Vserver: vs1
                File ID: 82
          Connection ID: 104617
             Session ID: 1
              File Type: Regular
              Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
   Path from CIFS Share: windows\win8\test\test.txt
             Share Mode: rw
            Range Locks: 1
 Continuously Available: Yes
            Reconnected: No
```

Auditing NAS file access events on SVMs with FlexVol volumes

Auditing for NAS file access events is a security measure that enables you to track and log SMB and NFS file and folder access events on objects stored on Storage Virtual Machines (SVMs) with FlexVol volumes. This helps you track potential security problems and provides evidence of any file access security breaches.

How auditing works

Before you plan and configure your auditing configuration, you should understand how auditing works.

Basic auditing concepts

To understand auditing in Data ONTAP, you should be aware of some basic auditing concepts.

Staging files	The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.
Staging volume	A dedicated volume created by Data ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled Storage Virtual Machines (SVMs) with volumes in that particular aggregate. There is no multi-tenancy for staging volumes. For instance, audit records are not separated by SVM in the staging volumes.
	Cluster administrators can view, modify, or delete staging volumes, but only Data ONTAP can create staging volumes.
System volumes	FlexVol volumes that contain special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.
Consolidation task	A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

How the Data ONTAP auditing process works

The Data ONTAP auditing process is different than the Microsoft auditing process. Before you configure auditing, you should understand how the Data ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs with FlexVol volumes. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.

  The log directory must already exist. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the following error:

  ```
  The specified path "/<path>" does not exist in the namespace belonging
  to Vserver "<Vserver_name>"
  ```

  Configuration creation fails if the directory exists but contains symlinks.
- Auditing schedules the consolidation task.

After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or CIFS servers are stopped or restarted.

Event log consolidation

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task ensures that all the remaining logs are consolidated.

Guaranteed auditing

By default, auditing is guaranteed. Data ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

Consolidation process when a node is unavailable

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's SFO partner (or the HA partner in the case of a two-node cluster) is available.

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.
- If the SFO partner is not available, the task creates a partial log file.

  When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix .partial to the consolidated file name.
- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that point of time.
- All audit records are preserved.

Event log rotation

Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

Process when auditing is disabled on the SVM

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as job delete. Users are no longer allowed to delete the auditing consolidation job.

Related concepts

Related tasks

Related references

Aggregate space considerations when enabling auditing

When an auditing configuration is created and auditing is enabled on at least one Storage Virtual Machine (SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

Related concepts

Auditing requirements and considerations

Before you configure and enable auditing on your Storage Virtual Machine (SVM) with FlexVol volumes, you need to be aware of certain requirements and considerations.

- Before you can enable auditing on your SVM, all nodes in the cluster must be running Data ONTAP 8.2 or later.
- The maximum number of audit-enabled SVMs supported in a cluster is 50.
- Auditing is not tied to CIFS or NFS licensing.
  You can configure and enable auditing even if CIFS and NFS licenses are not installed on the cluster.
- NFS auditing supports security ACEs (type U).
- For NFS auditing, there is no mapping between mode bits and audit ACEs.
  When converting ACLs to mode bits, audit ACEs are skipped. When converting mode bits to ACLs, audit ACEs are not generated.
- The directory specified in the auditing configuration must exist.
  If it does not exist, the command to create the auditing configuration fails.
- The directory specified in the auditing configuration must meet the following requirements:

  - The directory must not contain symbolic links.
    If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.
  - You must specify the directory by using an absolute path.
    You should not specify a relative path, for example, /vs1/../.

- Auditing is dependent on having available space in the staging volumes.
  You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.
- Auditing is dependent on having available space in the volume containing the directory where converted audit event logs are stored.
  You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of audit logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the audit logs in the volume.

Related concepts

[Planning the auditing configuration](#) on page 410

What the supported audit event log formats are

Supported file formats for the converted audit event logs are EVTX and XML file formats.

You can specify the type of file format when you create the auditing configuration. By default, Data ONTAP converts the binary logs to the EVTX file format.

Related tasks

[Creating a file and directory auditing configuration on SVMs](#) on page 414

Viewing audit event logs

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the EVTX or XML file formats.

- EVTX file format
  You can open the converted EVTX audit event logs as saved files using Microsoft Event Viewer.
  There are two options that you can use when viewing event logs using Event Viewer:
  - General view
    Information that is common to all events is displayed for the event record. In this version of Data ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.
  - Detailed view
    A friendly view and a XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.
- XML file format

You can view and process XML audit event logs on third-party applications that support the XML file format. XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about obtaining the XML schema and documents related to XML definitions, contact technical support or your account team.

Related concepts

How the Data ONTAP auditing process works on page 404

Related tasks

Manually rotating the audit event logs on page 427

SMB file and folder access events that can be audited

Data ONTAP can audit certain SMB file and folder access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

The following SMB file and folder access events can be audited:

Event ID (EVT/EVTX)	Event	Description	Category
560/4656	Open Object/ Create Object	OBJECT ACCESS: Object (file or directory) open.	File Access
563/4659	Open Object with the Intent to Delete	OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete.	File Access
564/4660	Delete Object	OBJECT ACCESS: Delete Object (file or directory). Data ONTAP generates this event when a Windows client attempts to delete the object (file or directory).	File Access
567/4663	Read Object/ Write Object/Get Object Attributes/Set Object Attributes	OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute). **Note:** For this event, Data ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. This prevents Data ONTAP from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.	File Access

Event ID (EVT/EVTX)	Event	Description	Category
N/A/4664	Hard link	OBJECT ACCESS: An attempt was made to create a hard link.	File Access
N/A/N/A Data ONTAP Event ID 9999	Rename Object	OBJECT ACCESS: Object renamed. This is a Data ONTAP event. It is not currently supported by Windows as a single event.	File Access
N/A/N/A Data ONTAP Event ID 9998	Unlink Object	OBJECT ACCESS: Object unlinked. This is a Data ONTAP event. It is not currently supported by Windows as a single event.	File Access

Note: The object path printed in an audit record is the relative path from the root of the containing volume. For example, consider the following volume information:

```
                          Junction                      Junction
Vserver    Volume         Active    Junction Path       Path Source
---------  ------------   --------  ------------------  -----------
vs1        data           true      /data               RW_volume
vs1        data1          true      /data/data1         RW_volume
```

If a user accesses a file with the path `/data/data1/dir1/file.txt`, the path used in the `<ObjectName>` tag in the event contained in the audit logs is `/data1/dir1/file.txt`.

Related concepts

[Configuring audit policies on NTFS security-style files and directories](#) on page 417

NFS file and directory access events that can be audited

Data ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

• READ
• OPEN
• CLOSE
• READDIR
• WRITE
• SETATTR
• CREATE
• LINK
• OPENATTR

- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

Related tasks

Planning the auditing configuration

Before you configure auditing on Storage Virtual Machines (SVMs) with FlexVol volumes, you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which of two methods are used when rotating the consolidated and converted audit logs. You can specify one of the two following methods when you configure auditing:

- Rotate logs based on log size
  This is the default method used to rotate logs.
- Rotate logs based on a schedule

Parameters common to all auditing configurations

There are two required parameters that you must specify when you create the auditing configuration. There are also two optional parameters that you can specify. The first optional parameter determines how many audit logs are retained in the audit log directory The second optional parameter specifies which log file format to use for the audit logs.

You can use the following list to determine what values to use for the parameters that are common to all auditing configurations:

Type of information	Option	Required	Include	Your values
SVM name Name of the SVM on which to create the auditing configuration. The SVM must already exist.	`-vserver vserver_name`	Yes	Yes	
Log destination path Specifies where the converted audit logs are stored. The path must already exist on the SVM. If the path is not valid, the audit configuration command fails.	`-destination text`	Yes	Yes	
Log file output format Determines the output format of the audit logs. The output format can be either Data ONTAP-specific XML or Microsoft Windows EVTX log format. By default, the output format is EVTX.	`-format {xml|evtx}`	No		
Log files rotation limit Determines how many audit log files to retain before rotating the oldest log file out. A value of 0 indicates that all the log files are retained. The default value is 0. For example, if you enter a value of 5, the last five log files are retained.	`-rotate-limit integer`	No		

Parameters used for determining when to rotate audit event logs

Rotate logs based on log size

The default is to rotate audit logs based on size. The default log size is 100 MB. If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation. If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size:

Type of information	Option	Required	Include	Your values
Log file size limit Determines the audit log file size limit.	`-rotate-size {integer[KB|MB|GB|TB|PB]}`	No		

Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you configure time-based log rotation parameters, logs are rotated based on the configured schedule instead of log size.
- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
- The rotation schedule is calculated by using all the time-related values.

  For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.

- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

  For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

  For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

Type of information	Option	Required	Include	Your values
Log rotation schedule: Month Determines the monthly schedule for rotating audit logs. Valid values are `January` through `December`, and `all`. For example, you can specify that the audit log is to be rotated during the months January, March, and August.	`-rotate-schedule-month` *chron_month*	No		

Type of information	Option	Required	Include	Your values
Log rotation schedule: Day of week Determines the daily (day of week) schedule for rotating audit logs. Valid values are `January` through `December`, and `all`. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week.	`-rotate-schedule-dayofweek` `chron_dayofweek`	No		
Log rotation schedule: Day Determines the day of the month schedule for rotating the audit log. Valid values range from `1` through `31`. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month.	`-rotate-schedule-day` `chron_dayofmonth`	No		
Log rotation schedule: Hour Determines the hourly schedule for rotating the audit log. Valid values range from `0` (midnight) to `23` (11:00 p.m.). Specifying `all` rotates the audit logs every hour. For example, you can specify that the audit log is to be rotated at 6 (6 a.m.) and 18 (6 p.m.).	`-rotate-schedule-hour` `chron_hour`	No		
Log rotation schedule: Minute Determines the minute schedule for rotating the audit log. Valid values range from `0` to `59`. For example, you can specify that the audit log is to be rotated at the 30th minute.	`-rotate-schedule-minute` `chron_minute`	Yes, if configuring schedule-based log rotation; otherwise, no.		

Related concepts

Configuring file and folder audit policies on page 417
Auditing requirements and considerations on page 406
What the supported audit event log formats are on page 407

Related tasks

Creating a file and directory auditing configuration on SVMs

Creating a file and directory auditing configuration on your Storage Virtual Machine (SVM) with FlexVol volumes includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Steps

1. Creating the auditing configuration on page 415
   Before you can begin auditing file and directory events, you must create an auditing configuration on the Storage Virtual Machine (SVM).

2. Enabling auditing on the SVM on page 416
   After you finish setting up the auditing configuration, you must enable auditing on the Storage Virtual Machine (SVM).

3. Verifying the auditing configuration on page 416
   After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Related concepts

Related tasks

Creating the auditing configuration

Before you can begin auditing file and directory events, you must create an auditing configuration on the Storage Virtual Machine (SVM).

Step

1. Using the information in the planning worksheet, create the auditing configuration by using the appropriate command:

If you want to create an auditing configuration that rotates audit logs based on...	Enter the command...
Log size	**vserver audit create -vserver** *vserver_name* **-destination** *path* **[-format {xml|evtx}] [-rotate-limit** *integer*] **[-rotate-size {***integer*[**KB|MB|GB|TB|PB**]}]**
A schedule	**vserver audit create -vserver** *vserver_name* **-destination** *path* **[-format {xml|evtx}] [-rotate-limit** *integer*] **[-rotate-schedule-month** *chron_month*] **[-rotate-schedule-dayofweek** *chron_dayofweek*] **[-rotate-schedule-day** *chron_dayofmonth*] **[-rotate-schedule-hour** *chron_hour*] **-rotate-schedule-minute** *chron_minute* **Note:** The -rotate-schedule-minute parameter is required if configuring time-based audit log rotation.

Examples

The following example creates an audit configuration for SVM vs1. The log format is EVTX (the default). The logs are stored in the /audit_log directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -
rotate-size 200MB
```

The following example creates an audit configuration for SVM vs1 using size-based rotation. The log format is EVTX (the default). The log file size limit is 200 MB, and the log rotation limit is 5:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -
rotate-size 200MB -rotate-limit 5
```

The following example creates an audit configuration for SVM vs1 using time-based rotation. The log format is EVTX (the default). The audit logs are rotated monthly, at 12:30 p.m. on all days of the week:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -
rotate-size 200MB -rotate-schedule-month all -rotate-schedule-dayofweek all
-rotate-schedule-hour 12 -rotate-schedule-minute 30
```

Enabling auditing on the SVM

After you finish setting up the auditing configuration, you must enable auditing on the Storage Virtual Machine (SVM).

Before you begin

The SVM audit configuration must already exist.

Step

1. Enable auditing on the SVM:

   vserver audit enable -vserver *vserver_name*

   ### Example

   vserver audit enable -vserver vs1

Verifying the auditing configuration

After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Step

1. Verify the auditing configuration:

   vserver audit show -instance -vserver *vserver_name*

   ### Example

   The following example displays in list form all audit configuration information for Storage Virtual Machine (SVM) vs1. The EVTX-formatted logs are stored in the /audit_log directory. The log file size limit is 200 MB, and the logs are rotated when they reach 200 MB in size. Auditing is enabled:

   vserver audit show -instance -vserver vs1

   ```
                       Vserver: vs1
                 Auditing state: true
          Log Destination Path: /audit_log
   ```

```
                    Log Format: evtx
           Log File Size Limit: 200MB
     Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
       Log Rotation Schedule: Day: -
      Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
               Rotation Schedules: -
        Log Files Rotation Limit: 0
```

Configuring file and folder audit policies

Implementing auditing on file and folder access events is a two-step process. First you must create and enable an auditing configuration on Storage Virtual Machines (SVMs) with FlexVol volumes. Second, you must configure audit policies on the files and folders that you want to monitor. You can configure audit policies to monitor both successful and failed access attempts.

You can configure both SMB and NFS audit polices. SMB and NFS audit policies have different configuration requirements and audit capabilities.

If the appropriate audit policies are configured, Data ONTAP monitors SMB and NFS access events as specified in the audit policies only if the SMB or NFS servers are running.

Related concepts

How the Data ONTAP auditing process works on page 404
SMB file and folder access events that can be audited on page 408
Displaying information about audit policies applied to files and directories on page 422

Configuring audit policies on NTFS security-style files and directories

Before you can audit file and directory operations, you must configure audit policies on the files and directories for which you want to collect audit information. This is in addition to setting up and enabling the audit configuration. You can configure NTFS audit policies by using the Windows Security tab or by using the Data ONTAP CLI.

Related concepts

Limits when using the CLI to set file and folder security on page 204
How security descriptors are used to apply file and folder security on page 204

Related tasks

Configuring NTFS audit policies using the Windows Security tab on page 418
Displaying information about audit policies using the Windows Security tab on page 422
Displaying information about NTFS audit policies on FlexVol volumes using the CLI on page 197
Configuring and applying file security on NTFS files and folders using the CLI on page 205

Configuring NTFS audit policies using the Windows Security tab

You can configure audit policies on files and directories by using the **Windows Security** tab in the Windows Properties window. This is the same method used when configuring audit polices on data residing on a Windows client, which enables customers to use the same GUI interface that they are accustomed to using.

Before you begin

Auditing must be configured on the Storage Virtual Machine (SVM) that contains the data to which you are applying SACLs.

About this task

Configuring NTFS audit policies is done by adding entries to NTFS system access control lists (SACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain discretionary access control lists (DACLs) for applying file and folder access permissions, system access control lists (SACLs) for file and folder auditing, or both SACLs and DACLs.

You can set NTFS audit policies for auditing access on individual files and folders using the Windows Security tab in the Windows Properties window by completing the following steps on a Windows host:

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** box:
    a) Select a **Drive** letter.
    b) In the **Folder** box, type the CIFS server name that contains the share holding the data you would like to audit and the name of the share.

    #### Example

    If your CIFS server name is "CIFS_SERVER" and your share is named "share1", you should enter \\CIFS_SERVER\share1.

    > **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

    c) Click **Finish**.

    The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to enable auditing access.

4. Right-click on the file or directory, and select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Perform the desired actions:

If you want to....	Do the following
Set up auditing for a new user or group	a. Click **Add**. b. In the **Enter the object name to select** box, type the name of the user or grout that you want to add. c. Click **OK**.
Remove auditing from a user or group	a. In the **Enter the object name to select** box, select the user or group that you want to remove. b. Click **Remove**. c. Click **OK**. d. Skip the rest of this procedure.
Change auditing for a user or group	a. In the **Enter the object name to select** box, select the user or group that you want to change. b. Click **Edit**. c. Click **OK**.

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for <object> box opens.

9. In the **Apply to** box, select how you want to apply this auditing entry.

    You can select one of the following:

    - **This folder, subfolders and files**
    - **This folder and subfolders**
    - **This folder only**
    - **This folder and files**
    - **Subfolders and files only**
    - **Subfolders only**
    - **Files only**

    If you are setting up auditing on a single file, the **Apply to** box is not active. The **Apply to** defaults to **This object only**.

    Note: Since auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

10. In the **Access** box, select what you want audited and whether you want to audit successful events, failure events or both.

    - To audit successful events, select the **Success** box.
    - To audit failure events, select the **Failure** box.

    You can audit the following events:

    - **Full control**
    - **Traverse folder / execute file**
    - **List folder / read data**
    - **Read attributes**
    - **Read extended attributes**
    - **Create files / write data**
    - **Create folders / append data**
    - **Write attributes**
    - **Write extended attributes**
    - **Delete subfolders and files**
    - **Delete**
    - **Read permissions**
    - **Change permissions**
    - **Take ownership**

        Note: Select only the actions that you need to monitor to meet your security requirements. For more information on these auditable events, see your Windows documentation.

11. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select **Apply these auditing entries to objects and/or containers within this container only** box.

12. Click **Apply**.

13. After you finish adding, removing, or editing auditing entries, click **OK**.

    The Auditing Entry for <object> box closes.

14. In the **Auditing** box, select the inheritance settings for this folder.

    You can choose one of the following:

    - Select the **Include inheritable auditing entries from this object's parent** box.
    - Select the **Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object** box.
    - Select both boxes.
    - Select neither box.

    If you are setting SACLs on a single file, the **Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object** box is not present in the Auditing dialog box.

Note: Select only the minimal level that provides the auditing events that meet your security requirements.

15. Click **OK**.

   The Auditing box closes.

Related concepts

SMB file and folder access events that can be audited on page 408

Related tasks

Configuring and applying audit policies on NTFS files and folders using the CLI on page 219
Displaying information about NTFS audit policies on FlexVol volumes using the CLI on page 197
Displaying information about audit policies using the Windows Security tab on page 422

How to configure NTFS audit policies using the Data ONTAP CLI

You can configure audit policies on files and folders using the Data ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the vserver security file-directory command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this Data ONTAP command family. See the man pages for more information about using these commands to configure and add NTFS SACLs to files and folders.

Related concepts

SMB file and folder access events that can be audited on page 408

Related tasks

Configuring and applying audit policies on NTFS files and folders using the CLI on page 219
Displaying information about NTFS audit policies on FlexVol volumes using the CLI on page 197

Configuring auditing for UNIX security style files and directories

You configure auditing for UNIX security style files and directories by adding audit ACEs to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events for security purposes.

About this task

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an

existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

Steps

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.

   For more information about manipulating ACLs, see the man pages of your NFS client.

2. Append the desired audit ACEs.

3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

Related tasks

Displaying information about NFSv4 audit policies on FlexVol volumes using the CLI on page 200

Related references

NFS file and directory access events that can be audited on page 409

Displaying information about audit policies applied to files and directories

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

Related concepts

Configuring file and folder audit policies on page 417

Displaying information about audit policies using the Windows Security tab

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

About this task

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.

2. Complete the **Map Network Drive** dialog box:

   a) Select a **Drive** letter.

   b) In the **Folder** box, type the IP address or CIFS server name of the Storage Virtual Machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

   Example

   If your CIFS server name is "CIFS_SERVER" and your share is named "share1", you should enter `\\CIFS_SERVER\share1`.

   > **Note:** You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

   c) Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you display auditing information.

4. Right-click on the file or directory, and select **Properties**.

5. Select the **Security** tab.

6. Click **Advanced**.

7. Select the **Auditing** tab.

8. Click **Continue**.

   The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.

9. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.

10. Click **Edit**.

    The Auditing entry for <object> box opens.

11. In the **Access** box, view the current SACLs that are applied to the selected object.

12. Click **Cancel** to close the **Auditing entry for <object>** box.

13. Click **Cancel** to close the **Auditing** box.

Displaying information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective-security styles are, what permissions are applied, and information about

system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the Storage Virtual Machine (SVM) that contains the path to the files or directories whose audit information you want to display. If you want to customize the output, you can use the following optional parameters to display information only about file and directory security that matches the specified parameters:

Optional parameter	Description
`-fields` `fieldsname`, ...	You can use this parameter to display information on the fields you specify. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about all entries.
`-volume-name` `volume_name`	Displays information where the specified path is relative to the specified volume. If this parameter is not specified, the SVM root volume is taken as default.
`-share-name` `share_name`	Displays information where the specified path is relative to the root of the specified share. If this parameter is not specified, the SVM root volume is taken as default.
`-lookup-names` `{true|false}`	Displays information where the information about owner and group is set to one of the following: • `true` displays information where the lookup name is stored as a name. • `false` displays information where the lookup name is stored as a SID.
`-expand-mask` `{true|false}`	Displays information where the hexadecimal bit mask entry is set to one of the following: • `true` displays information where the bit mask entries are store in expanded form. • `false` displays information where the bit mask entries are store in collapsed form.
`-security-style` `{unix|ntfs|mixed|` `unified}`	Displays information for files and directories with paths in volumes of the specified security style. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release. This is the associated security type of the volume or qtree.

Optional parameter	Description
`-effective-style {unix|ntfs|mixed| unified}`	Displays information for files and directories with the specified effective security style on the path. This command is not supported for SVMs with Infinite Volumes; therefore, the `unified` value is not valid for this release.
	This is the security scheme in effect for a given file or directory. A file or directory can have one of two security styles, either NTFS or UNIX. The effective security style is important with mixed security-style volumes and qtrees since a file or directory can have either NTFS-effective or UNIX-effective security (but not both).
`-dos-attributes hex_integer`	Displays information only for files and directories with the specified DOS attributes.
`-text-dos-attr text`	Displays information only for files and directories with the specified text DOS attributes.
`-expanded-dos- attr text`	Displays information only for files and directories with the specified extended DOS attributes.
`-user-id unix_user_ID`	Displays information only for files and directories with the specified UNIX user ID.
`-group-id unix_group_ID`	Displays information only for files and directories with the specified UNIX group ID.
`-mode-bits octal_permissions`	Displays information only for files and directories with the specified UNIX mode bits in Octal form.
`-text-mode-bits text`	Displays information only for files and directories with the specified UNIX mode bits in text form.
`-acls system_acls`	Displays information only for files and directories with the specified ACLs. You can enter the following information: • Type of ACL, which can be NTFS or NFSv4 • Control bits in the security descriptors • Owner, which applies only in the case of NTFS security descriptors. • Group, which applies only in the case of NTFS security descriptors. • Access Control Entries (ACEs) which includes both discretionary access control list (DACL) and system access control list (SACL) access control entries (ACEs) in the ACL.

Note: NTFS security-style volumes and qtrees use only NTFS system access control lists for audit policies. Mixed security-style volumes and qtrees can contain some files and directories that are of NTFS security style, which can have NTFS audit policies applied to them.

Step

1. Display audit policy settings:

   vserver security file-directory show -vserver *vserver_name* -path *path optional_parameters*

   Example

   The following example displays the audit policy information about the path /corp in SVM vs1. This NTFS-security-style path has a NTFS-effective security style. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry:

   vserver security file-directory show -vserver vs1 -path /corp

   ```
              Vserver: vs1
            File Path: /corp
       Security Style: ntfs
      Effective Style: ntfs
       DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
         Unix User Id: 0
        Unix Group Id: 0
       Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                 ACLs: NTFS Security Descriptor
                       Control:0x8014
                       Owner:DOMAIN\Administrator
                       Group:BUILTIN\Administrators
                       SACL - ACEs
                         ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                         SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                       DACL - ACEs
                         ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                         ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                         ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                         ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
   ```

Managing auditing configurations

You can manage Storage Virtual Machine (SVM) auditing configurations by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing configurations, modifying auditing configurations, and deleting auditing configurations. You also need to understand what happens when reverting to a release where auditing is not supported.

Related concepts

Manually rotating the audit event logs

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific Storage Virtual Machine (SVM) before Data ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

Step

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

   ### Example

   `vserver audit rotate-log -vserver vs1`

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (`XML` or `EVTX`), and can be viewed by using the appropriate application.

Related concepts

Viewing audit event logs on page 407

Related tasks

Creating a file and directory auditing configuration on SVMs on page 414

Enabling and disabling auditing on SVMs

You can enable or disable auditing on Storage Virtual Machines (SVMs) with FlexVol volumes. You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

Before you begin

The Storage Virtual Machine (SVM) auditing configuration must already exist before you enable auditing. Disabling auditing does not delete the auditing configuration.

Steps

1. Perform the appropriate command:

If you want auditing to be...	Enter the command...
Enabled	**`vserver audit enable -vserver vserver_name`**
Disabled	**`vserver audit disable -vserver vserver_name`**

2. Verify that auditing is in the desired state:

   `vserver audit show -vserver vserver_name`

Examples

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

 Vserver      State  Log Format Target Directory
 ----------- ------ ---------- --------------------
 vs1          true   evtx       /audit_log
```

The following example disables auditing for SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

 Vserver      State  Log Format Target Directory
 ----------- ------ ---------- --------------------
 vs1          false  evtx       /audit_log
```

Related tasks

Displaying information about auditing configurations

You can display information about auditing configurations for Storage Virtual Machines (SVMs)
with FlexVol volumes. The information can help you determine whether the configuration is what
you want in place for each SVM. The displayed information also enables you to verify whether an
auditing configuration is enabled.

About this task

You can display detailed information about auditing configurations on all SVMs or you can
customize what information is displayed in the output by specifying optional parameters. If you do
not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be true or false
  If the audit state is true, auditing is enabled. If the audit state is false, auditing is disabled.
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

Step

1. Display information about the auditing configuration by using the vserver audit show
   command.

   For more information about using the command, see the man pages.

Examples

The following example displays the name, audit state, and target directory for all SVMs:

```
cluster1::> vserver audit show

 Vserver     State  Log Format Target Directory
 ----------- ------ ---------- --------------------
 vs1         false  evtx       /audit_log
```

The following example displays SVM names and details about the audit log for all SVMs:

```
cluster1::> vserver audit show -log-save-details

            Rotation                             Rotation
 Vserver    File Size Rotation Schedule          Limit
 ----------- --------- ------------------------ --------
 vs1         100MB     -                        0
```

The following example displays, in list form, all audit configuration information about all
SVMs:

```
cluster1::> vserver audit show -instance

                           Vserver: vs1
                    Auditing state: true
               Log Destination Path: /audit_log
                        Log Format: evtx
                Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                Rotation Schedules: -
           Log Files Rotation Limit: 0
```

Related tasks

[Creating a file and directory auditing configuration on SVMs](#) on page 414

Commands for modifying auditing configurations

If you want to change an auditing setting for your Storage Virtual Machine (SVM), you can modify
the current configuration at any time.

If you want to...	Use this command...
Modify the log destination path	`vserver audit modify` with the `-destination` parameter

If you want to...	Use this command...
Enabling automatic saves based on internal log file size	`vserver audit modify` with the `-rotate-size` parameter
Enabling automatic saves based on a time interval	`vserver audit modify` with the `-rotate-schedule-month`, `-rotate-schedule-dayofweek`, `-rotate-schedule-day`, `-rotate-schedule-hour`, and `-rotate-schedule-minute` parameters
Specifying the maximum number of saved log files	`vserver audit modify` with the `-rotate-limit` parameter

See the man page for the `vserver audit modify` command for more information.

Deleting an auditing configuration

In you no longer want to audit file and directory events on the Storage Virtual Machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

Steps

1. Disable the auditing configuration:

   vserver audit disable -vserver *vserver_name*

   Example

   vserver audit disable -vserver vs1

2. Delete the auditing configuration:

   vserver audit delete -vserver *vserver_name*

   Example

   vserver audit delete -vserver vs1

Related tasks

What the process is when reverting

If you plan to revert the cluster you should be aware of the process Data ONTAP follows when reverting and there are auditing-enabled Storage Virtual Machines (SVMs) in the cluster. You must take certain actions before reverting.

Reverting to a version of Data ONTAP that supports auditing, but does not support the EVTX log format

Support for the EVTX log format starts with Data ONTAP 8.2.1 in the 8.2 release family. If you are reverting to Data ONTAP 8.2, a version that supports auditing, but does not support the EVTX log format, you do not need to disable auditing on auditing-enabled SVMs before you revert. However, for each auditing configuration on the cluster (enabled or disabled), you must change the log format to the XML log format prior to reverting.

Reverting to a version of Data ONTAP that does not supports auditing

Support for auditing starts with Data ONTAP 8.2. If you plan to revert the cluster to a Data ONTAP release that does not support auditing and you have audit-enabled Storage Virtual Machines (SVMs), you should be aware of the process Data ONTAP follows when reverting.

- Prior to revert, you must manually disable and delete all auditing configurations on all SVMs in the cluster.

  When you disable auditing on all SVMs in the cluster, Data ONTAP consolidates and converts all auditing logs in the staging files for all SVMs. All converted audit logs are stored in the event log directory location specified in the auditing configuration for each audit-enabled SVM. The converted event logs are available post-revert.

- When you delete all auditing configurations across the cluster, Data ONTAP deletes all staging volumes.

  There is no need to manually delete staging volumes.

- During the revert, each file that has an NFSv4.x ACL is checked to determine whether the ACL contains an audit ACE.

  If it does, the complete ACL is dropped.

Related tasks

Troubleshooting auditing and staging volume space issues

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created,

which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

Related concepts

[Aggregate space considerations when enabling auditing](#) on page 406

How to troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You need to know how to troubleshoot space issues related to event log volumes.

- Storage Virtual Machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.
- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

  Note: If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

For more information about viewing information about volumes and increasing volume size, see the *Clustered Data ONTAP Logical Storage Management Guide*.

For more information about viewing information about aggregates and managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

How to troubleshoot space issues related to the staging volumes (cluster administrators only)

If any of the volumes containing staging files for your Storage Virtual Machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, a cluster administrator needs to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact the cluster administrator to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: `No space left on device`. Only the cluster administrator can view information about staging volumes.

If there is insufficient space in the staging volumes, the cluster administrators can resolve the space issues by increasing the size of the volume.

> **Note:** If the aggregate that contains the staging volume is full, then the size of the aggregate must be increased before the cluster administrator can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

For more information about viewing information about volumes and increasing volume size, see the *Clustered Data ONTAP Logical Storage Management Guide.*

For more information about viewing information about aggregates and managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide.*

Using FPolicy for file monitoring and management on SVMs with FlexVol volumes

FPolicy is a file access notification framework that is used to monitor and manage file access events on Storage Virtual Machines (SVMs) with FlexVol volumes.

The framework generates notifications that are sent to either external FPolicy servers or to Data ONTAP. FPolicy supports event notifications for files and directories that are accessed using NFS and SMB.

> **Note:** FPolicy is not supported on SVMs with Infinite Volume.

How FPolicy works

Before you plan and create your FPolicy configuration, you should understand the basics of how FPolicy works.

What the two parts of the FPolicy solution are

There are two parts to an FPolicy solution. The Data ONTAP FPolicy framework manages activities on the cluster and sends notifications to external FPolicy servers. External FPolicy servers process notifications sent by Data ONTAP FPolicy.

The Data ONTAP framework creates and maintains the FPolicy configuration, monitors file events, and sends notifications to external FPolicy servers. Data ONTAP FPolicy provides the infrastructure that allows communication between external FPolicy servers and Storage Virtual Machine (SVM) nodes.

The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the node. What happens as a result of the notification processing depends on the application and whether the communication between the node and the external servers is asynchronous or synchronous.

Related concepts

What synchronous and asynchronous notifications are

FPolicy sends notifications to external FPolicy servers via the FPolicy interface. The notifications are sent either in synchronous or asynchronous mode. The notification mode determines what Data ONTAP does after sending notifications to FPolicy servers.

Asynchronous notifications	With asynchronous notifications, the node does not wait for a response from the FPolicy server, which enhances overall throughput of the system. This type of notification is suitable for applications where the FPolicy server does not require that any action be taken as a result of notification evaluation. For example, asynchronous notifications are used when the Storage Virtual Machine (SVM) administrator wants to monitor and audit file access activity.
Synchronous notifications	When configured to run in synchronous mode, the FPolicy server must acknowledge every notification before the client operation is allowed to continue. This type of notification is used when an action is required based on the results of notification evaluation. For example, synchronous notifications are used when the SVM administrator wants to either allow or deny requests based on criteria specified on the external FPolicy server.

Related concepts

How control channels are used for FPolicy communication on page 436
How privileged data access channels are used for synchronous communication on page 436

Synchronous and asynchronous applications

There are many possible uses for FPolicy applications, both asynchronous and synchronous.

Asynchronous applications are ones where the external FPolicy server does not alter access to files or directories or modify data on the Storage Virtual Machine (SVM). For example:

- File access and audit logging
- Storage resource management

Synchronous applications are ones where data access is altered or data is modified by the external FPolicy server. For example:

- Quota management
- File access blocking
- File archiving and hierarchical storage management
- Encryption and decryption services
- Compression and decompression services

You can use the SDK for FPolicy to identify and implement other applications as well.

Roles that cluster components play with FPolicy implementation

The cluster, the contained Storage Virtual Machines (SVMs), and data LIFs all play a role in an FPolicy implementation.

cluster	The cluster contains the FPolicy management framework and maintains and manages information about all FPolicy configurations in the cluster.
SVM	An FPolicy configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources. One SVM configuration cannot monitor and send notifications for file access requests that are made for data residing on another SVM.
	FPolicy configurations can be defined on the admin SVM. After configurations are defined on the admin SVM, they can be seen and used in all SVMs.
data LIFs	Connections to the FPolicy servers are made through data LIFs belonging to the SVM with the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

How FPolicy works with external FPolicy servers

After FPolicy is configured and enabled on the Storage Virtual Machine (SVM), FPolicy runs on every node on which the SVM participates. FPolicy is responsible for establishing and maintaining connections with external FPolicy servers (FPolicy servers), for notification processing, and for managing notification messages to and from FPolicy servers.

Additionally, as part of connection management, FPolicy has the following responsibilities:

- Ensures that file notification flows through the correct LIF to the FPolicy server.
- Ensures that when multiple FPolicy servers are associated with a policy, load balancing is done when sending notifications to the FPolicy servers.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.

How control channels are used for FPolicy communication

FPolicy initiates a control channel connection to an external FPolicy server from the data LIFs of each node participating on a Storage Virtual Machine (SVM). FPolicy uses control channels for transmitting file notifications; therefore, an FPolicy server might see multiple control channel connections based on SVM topology.

How privileged data access channels are used for synchronous communication

With synchronous use cases, the FPolicy server accesses data residing on the Storage Virtual Machine (SVM) through a privileged data access path. Access through the privileged path exposes

the complete file system to the FPolicy server. It can access data files to collect information, to scan files, read files, or write into files.

Because the external FPolicy server can access the entire file system from the root of the SVM through the privileged data channel, the privileged data channel connection must be secure.

Related concepts

[What granting super user credentials for privileged data access means](#) on page 437

How FPolicy connection credentials are used with privileged data access channels

The FPolicy server makes privileged data access connections to cluster nodes by using a specific Windows user credential that is saved with the FPolicy configuration. SMB is the only supported protocol for making a privileged data access channel connection.

If the FPolicy server requires privileged data access, the following conditions must be met:

- A CIFS license must be enabled on the cluster.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.

When making a data channel connection, FPolicy uses the credential for the specified Windows user name. Data access is made over the admin share ONTAP_ADMIN$.

What granting super user credentials for privileged data access means

Data ONTAP uses the combination of the IP address and the user credential configured in the FPolicy configuration to grant super user credentials to the FPolicy server.

Super user status grants the following privileges when the FPolicy server accesses data:

- Avoid permission checks
  The user avoids checks on files and directory access.
- Special locking privileges
  Data ONTAP allows read, write, or modify access to any file regardless of existing locks. If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.
- Bypass any FPolicy checks
  Access does not generate any FPolicy notifications.

How FPolicy manages policy processing

There might be multiple FPolicy policies assigned to your Storage Virtual Machine (SVM); each with a different priority. To create an appropriate FPolicy configuration on the SVM, it is important to understand how FPolicy manages policy processing.

Each file access request is initially evaluated to determine which policies are monitoring this event. If it is a monitored event, information about the monitored event along with interested policies is passed to FPolicy where it is evaluated. Each policy is evaluated in order of the assigned priority.

You should consider the following recommendations when configuring policies:

- When you want a policy to always be evaluated before other policies, configure that policy with a higher priority.
- If the success of requested file access operation on a monitored event is a prerequisite for a file request that is evaluated against another policy, give the policy that controls the success or failure of the first file operation a higher priority.

  For example, if one policy manages FPolicy file archiving and restore functionality and a second policy manages file access operations on the online file, the policy that manages file restoration must have a higher priority so that the file is restored before the operation managed by the second policy can be allowed.
- If you want all policies that might apply to a file access operation to be evaluated, give synchronous policies a lower priority.

You can reorder policy priorities for existing policies by modifying the policy sequence number. However, to have FPolicy evaluate policies based on the modified priority order, you must disable and reenable the policy with the modified sequence number.

Related concepts

[Planning the FPolicy policy configuration](#) on page 458

What the node-to-external FPolicy server communication process is

To properly plan your FPolicy configuration, you should understand what the node-to-external Fpolicy server communication process is.

Every node that participates on each Storage Virtual Machine (SVM) initiates a connection to an external FPolicy server (FPolicy server) using TCP/IP. Connections to the FPolicy servers are set up using node data LIFs; therefore, a participating node can set up a connection only if the node has an operational data LIF for the SVM.

Each FPolicy process on participating nodes attempts to establish a connection with the FPolicy server when the policy is enabled. It uses the IP address and port of the FPolicy external engine specified in the policy configuration.

The connection establishes a control channel from each of the nodes participating on each SVM to the FPolicy server through the data LIF. In addition, if IPv4 and IPv6 data LIF addresses are present on the same participating node, FPolicy attempts to establish connections for both IPv4 and IPv6. Therefore, in a scenario where the SVM extends over multiple nodes or if both IPv4 and IPv6 addresses are present, the FPolicy server must be ready for multiple control channel setup requests from the cluster after the FPolicy policy is enabled on the SVM.

For example, if a cluster has three nodes—Node1, Node2, and Node3—and SVM data LIFs are spread across only Node2 and Node3, control channels are initiated only from Node2 and Node3, irrespective of the distribution of data volumes. Say that Node2 has two data LIFs—LIF1 and LIF2 —that belong to the SVM and that the initial connection is from LIF1. If LIF1 fails, FPolicy attempts to establish a control channel from LIF2.
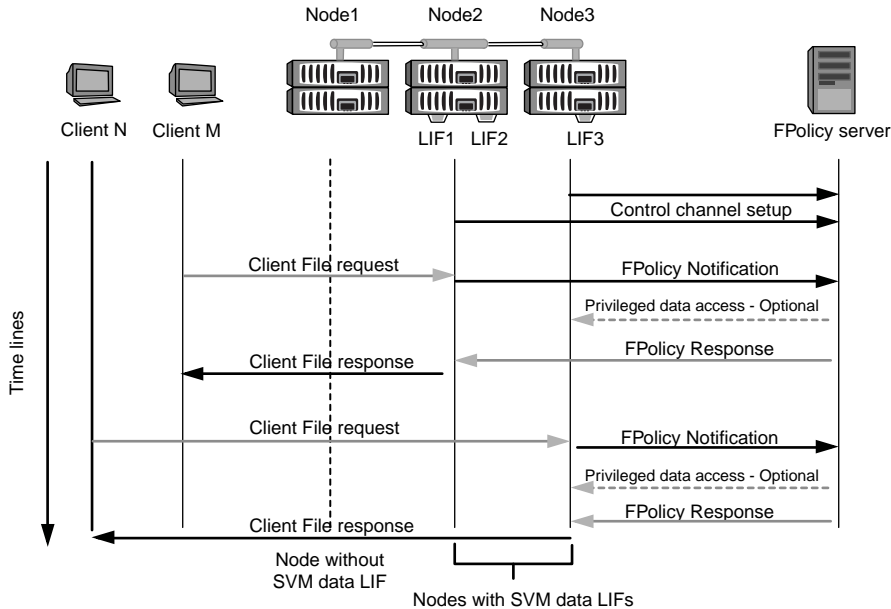
How FPolicy manages external communication during LIF migration or failover

Data LIFs can be migrated to data ports in the same node or to data ports on a remote node.

When a data LIF fails over or is migrated, a new control channel connection is made to the FPolicy server. FPolicy can then retry SMB and NFS client requests that timed out, with the result that new notifications are sent to the external FPolicy servers. The node rejects FPolicy server responses to original, timed-out SMB and NFS requests.

How FPolicy manages external communication during node failover

If the cluster node that hosts the data ports used for FPolicy communication fails, Data ONTAP breaks the connection between the FPolicy server and the node.

The impact of cluster failover to the FPolicy server can be mitigated by configuring the LIF manager to migrate the data port used in FPolicy communication to another active node. After the migration is complete, a new connection is established using the new data port.

If the LIF manager is not configured to migrate the data port, the FPolicy server must wait for the failed node to come up. After the node is up, a new connection is initiated from that node with a new Session ID.

Note: The FPolicy server detects broken connections with the keep-alive protocol message. The timeout for purging the session ID is determined when configuring FPolicy. The default keep-alive timeout is two minutes.

How FPolicy services work across SVM namespaces

Data ONTAP provides a unified Storage Virtual Machine (SVM) namespace. Volumes across the cluster are joined together by junctions to provide a single, logical file system. The FPolicy server is aware of the namespace topology and provides FPolicy services across the namespace.

The namespace is specific to and contained within the SVM; therefore, you can see the namespace only from the SVM context. Namespaces have the following characteristics:

- A single namespace exists in each SVM, with the root of the namespace being the root volume, represented in the namespace as slash (/).
- All other volumes have junction points below the root (/).
- Volume junctions are transparent to clients.
- A single NFS export can provide access to the complete namespace; otherwise, export policies can export specific volumes.
- SMB shares can be created on the volume or on qtrees within the volume, or on any directory within the namespace.
- The namespace architecture is flexible.

  Examples of typical namespace architectures are as follows:

  - A namespace with a single branch off of the root
  - A namespace with multiple branches off of the root
  - A namespace with multiple unbranched volumes off of the root

Related concepts

FPolicy configuration types

There are two basic FPolicy configuration types. One configuration uses external FPolicy servers to process and act upon notifications. The other configuration does not use external FPolicy servers; instead, it uses the Data ONTAP internal, native FPolicy server for simple file blocking based on extensions.

External FPolicy server configuration	The notification is sent to the FPolicy server, which screens the request and applies rules to determine whether the node should allow the requested file operation. For synchronous policies, the FPolicy server then sends a response to the node to either allow or block the requested file operation.
Native FPolicy server configuration	The notification is screened internally. The request is allowed or denied based on file extension settings configured in the FPolicy scope.

Related concepts

Planning the FPolicy policy configuration on page 458
Creating the FPolicy configuration on page 464

When to create a native FPolicy configuration

Native FPolicy configurations use the Data ONTAP internal FPolicy engine to monitor and block file operations based on the file's extension. This solution does not require external FPolicy servers (FPolicy servers). Using a native file blocking configuration is appropriate when this simple solution is all that is needed.

Native file blocking enables you to monitor any file operations that match configured operation and filtering events and then deny access to files with particular extensions. This is the default configuration.

This configuration provides a means to block file access based only on the file's extension. For example, to block files that contain mp3 extensions, you configure a policy to provide notifications for certain operations with target file extensions of mp3. The policy is configured to deny mp3 file requests for operations that generate notifications.

The following applies to native FPolicy configurations:

- The same set of filters and protocols that are supported by FPolicy server-based file screening are also supported for native file blocking.
- Native file blocking and FPolicy server-based file screening applications can be configured at the same time.
  To do so, you can configure two separate FPolicy policies for the Storage Virtual Machine (SVM), with one configured for native file blocking and one configured for FPolicy server-based file screening.
- The native file blocking feature only screens files based on the extensions and not on the content of the file.
- In the case of symbolic links, native file blocking uses the file extension of the root file.

When to create a configuration that uses external FPolicy servers

FPolicy configurations that use external FPolicy servers to process and manage notifications provide robust solutions for use cases where more than simple file blocking based on file extension is needed.

You should create a configuration that uses external FPolicy servers when you want to do such things as monitor and record file access events, provide quota services, perform file blocking based on criteria other than simple file extensions, provide data migration services using hierarchical storage management applications, or provide a fine-grained set of policies that monitor only a subset of data in the Storage Virtual Machine (SVM).

Requirements, considerations, and best practices for configuring FPolicy

Before you create and configure FPolicy configurations on your Storage Virtual Machines (SVMs) with FlexVol volumes, you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

Related concepts

Ways to configure FPolicy

FPolicy features are configured either through the command line interface (CLI) or through APIs. This guide uses the CLI to create, manage, and monitor an FPolicy configuration on the cluster.

Requirements for setting up FPolicy

Before you configure and enable FPolicy on your Storage Virtual Machine (SVM), you need to be aware of certain requirements.

- All nodes in the cluster must be running a version of Data ONTAP that supports FPolicy.
- If you are not using the Data ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.
- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy policies are enabled.
- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.
- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:
  - CIFS must be licensed on the cluster.
    Privileged data access is accomplished using SMB connections.
  - A user credential must be configured for accessing files over the privileged data channel.
  - The FPolicy server must run under the credentials configured in the FPolicy configuration.

Related concepts

Best practices and recommendations when setting up FPolicy

When setting up FPolicy on Storage Virtual Machines (SVMs), you need to be familiar with configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

- External FPolicy servers (FPolicy servers) should be placed in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.
- The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing, especially if policies are configured for synchronous screening.
- It is recommended to disable the FPolicy policy before making any configuration changes.
  For example, if you want to add or modify an IP address in the FPolicy external engine configured for the enabled policy, you should first disable the policy.
- If you configure FPolicy to monitor FlexCache volumes, it is recommended that you do not configure FPolicy to monitor `read` and `get attr` file operations on the FlexCache volumes.
  This is because Data ONTAP needs to retrieve inode-to-path (I2P) data with these operations, and this data cannot be retrieved from the FlexCache volume. Instead, the I2P request is forwarded to the origin volume, with the result that the performance benefits from FlexCache are not realized when FPolicy is used to monitor `read` and `get attr` operations on FlexCache volumes.
- The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests.
  The optimal ratio depends on the application for which the FPolicy server is being used.

Related concepts

Related tasks

Important revert considerations

You must understand and act on some important revert considerations before reverting to a Data ONTAP release that does not support FPolicy.

Before reverting to a version of Data ONTAP that does not support FPolicy, the following conditions must be met:

- Every file on which FPolicy servers set the offline bit must be either deleted or replaced with the original files before disabling FPolicy and reverting to a version of Data ONTAP that does not support FPolicy.
  If you do not replace the files with the offline bit set with the original files prior to reverting, clients access the stub files instead of the files to which the stub refers.

- FPolicy functionality must be disabled on the cluster by disabling every FPolicy policy on the cluster.

What the steps for setting up an FPolicy configuration are

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the Storage Virtual Machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.

   The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal "native" FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

2. Create an FPolicy event.

   An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

3. Create an FPolicy policy.

   The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal "native" FPolicy server.

   A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.

   A policy's boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

4. Configure the policy scope.

   The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.

   Note: Exclude lists take precedence over include lists.

5. Enable the FPolicy policy.

   When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring

file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).

Note: If the policy uses native file blocking, an external engine is not configured or associated with the policy.

Related concepts

Planning the FPolicy configuration on page 445
Creating the FPolicy configuration on page 464

Planning the FPolicy configuration

Before you create an FPolicy configuration, you must understand what is involved in each step of the configuration. You need to decide what settings you need to use when performing the configuration and record them in the planning worksheets.

You need to plan for the following configuration tasks:

- Creating the FPolicy external engine
- Creating the FPolicy policy event
- Creating the FPolicy policy
- Creating the FPolicy policy scope

FPolicy is supported on Storage Virtual Machines (SVMs) with FlexVol volumes. FPolicy is not supported on SVMs with Infinite Volume.

Related concepts

What the steps for setting up an FPolicy configuration are on page 444
Creating the FPolicy configuration on page 464

Planning the FPolicy external engine configuration

Before you configure the FPolicy external engine (external engine), you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

What it means to create an external engine

Creating the external engine means defining the information that FPolicy needs to make and manage connections to the external FPolicy servers (FPolicy servers). The external engine configuration defines the following configuration information:

- Storage Virtual Machine (SVM) name
- Engine name

- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- How to authenticate the connection between the node and the FPolicy server

  If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.
- How to manage the connection (advanced privilege settings)

  This includes parameters that define such things as timeout values, retry values, keep-alive values, and maximum request values.

What the basic external engine parameters are

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:

Type of information	Option
SVM Specifies the SVM name that you want to associate with this external engine. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver` `vserver_name`
Engine name Specifies the name to assign to the external engine configuration. You must specify the engine name later when you create the FPolicy policy. This associates the external engine with the policy.	`-engine-name` `engine_name`
Primary FPolicy servers Specifies the primary FPolicy servers to which the node sends notifications for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses. If more than one primary server IP address is specified, every node on which the SVM participates creates a control connection to every specified primary FPolicy server at the time the policy is enabled. If you configure multiple primary FPolicy servers, notifications are sent to the FPolicy servers in a round-robin fashion.	`-primary-servers` `IP_address`,...
Port number Specifies the port number of the FPolicy service.	`-port integer`

Type of information	Option
Secondary FPolicy servers Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses. Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion.	`-secondary-servers` `IP_address,...`
External engine type Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode. When set to `synchronous`, file request processing sends a notification to the FPolicy server, but then does not continue until after receiving a response from the FPolicy server. At that point, request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to `asynchronous`, file request processing sends a notification to the FPolicy server, and then continues.	`-extern-engine-type` `external_engine_type` The value for this parameter can be one of the following: • `synchronous` • `asynchronous`

Type of information	Option

SSL option for communication with FPolicy server
 	
Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information:
 	
• When set to `no-auth`, no authentication takes place.
  The communication link is established over TCP.
• When set to `server-auth`, the SVM authenticates the FPolicy server.
  If you choose this value, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.
• When set to `mutual-auth`, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM.
  If you choose this value, before creating the external engine, the administrator must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM.
 	
The public certificate of CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client_ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.
 	
If you choose to configure mutual SSL authentication, then you must also configure the `-certificate-common-name`, `-certificate-serial`, and `-certifcate-ca` parameters.
	`-ssl-option {no-auth|server-auth|mutual-auth}`

Certificate FQDN or custom common name Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-common-name` parameter.	`-certificate-common-name` *text*
Certificate serial number Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-serial` parameter.	`-certificate-serial` *text*

Type of information	Option
Certificate authority Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certifcate-ca` parameter.	`-certifcate-ca` `text`

What the advanced external engine options are

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

Type of information	Option
Timeout for canceling a request Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) that the node waits for a response from the FPolicy server. If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server. The range for this value is `0` through `100`. If the value is set to `0`, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is `20s`.	`-reqs-cancel-` `timeout` *integer*[h|m|s]
Timeout for aborting a request Specifies the timeout in hours (`h`), minutes (`m`), or seconds (`s`) for aborting a request. The range for this value is `0` through `200`.	`-reqs-abort-` `timeout` *integer*[h|m|s]

Interval for sending status requests
 	
Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a status request is sent to the FPolicy server.
 	
The range for this value is `0` through `50`. If the value is set to `0`, the option is disabled and status request messages are not sent to the FPolicy server. The default is `10s`.
	`-status-req-`
	`interval`
	integer[h|m|s]

Type of information	Option
Maximum outstanding requests on the FPolicy server Specifies the maximum number of outstanding requests that can be queued on the FPolicy server. The range for this value is `1` through `10000`. The default is `50`.	`-max-server-reqs` `integer`
Timeout for disconnecting a nonresponsive FPolicy server Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) after which the connection to the FPolicy server is terminated. The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within the this timeout period. The maximum allowed number of requests is either `50` (the default) or the number specified by the `max-server-reqs-` parameter. The range for this value is `1` through `100`. The default is `60s`.	`-server-progress-` `timeout` `integer`[h|m|s]

Interval for sending keep-alive messages to the FPolicy server
 	
Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages detect half-open connections.
 	
The range for this value is `10` through `600`. If the value is set to `0`, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is `120s`.
	`-keep-alive-`
	`interval-`
	`integer`[h|m|s]

Maximum reconnect attempts Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken. The range for this value is `0` through `20`. The default is `5`.	`-max-connection-` `retries` `integer`

Completing the FPolicy external engine configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

Information for a basic external engine configuration

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage Virtual Machine (SVM) name	Yes	Yes	

Type of information	Required	Include	Your values
Engine name	Yes	Yes	
Primary FPolicy servers	Yes	Yes	
Port number	Yes	Yes	
Secondary FPolicy servers	No		
External engine type	No		
SSL option for communication with external FPolicy server	Yes	Yes	
Certificate FQDN or custom common name	No		
Certificate serial number	No		
Certificate authority	No		

Information for advanced external engine parameters

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

Type of information	Required	Include	Your values
Timeout for canceling a request	No		
Timeout for aborting a request	No		
Interval for sending status requests	No		
Maximum outstanding requests on the FPolicy server	No		
Timeout for disconnecting a nonresponsive FPolicy server	No		
Interval for sending keep-alive messages to the FPolicy server	No		
Maximum reconnect attempts	No		

Planning the FPolicy event configuration

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

*   Storage Virtual Machine (SVM) name
*   Event name
*   Which protocols to monitor
    FPolicy can monitor SMB, NFSv3, and NFSv4 file access operations.
*   Which file operations to monitor
    Not all file operations are valid for each protocol.
*   Which file filters to configure
    Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.
*   Whether to monitor volume operations

    Note: There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following are the valid combinations for the three parameters:

    *   You can specify the `-protocol` and `-file-operations` parameters.
    *   You can specify all three of the parameters.
    *   You can specify none of the parameters.

What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

Type of information	Option
SVM Specifies the SVM name that you want to associate with this FPolicy event. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver` `vserver_name`
Event name Specifies the name to the FPolicy event configuration. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name.	`-event-name` `event_name`
Protocol Specifies which protocol to configure for the FPolicy event. The list for `-protocol` can include one of the following values: • `cifs` • `nfsv3` • `nfsv4` **Note:** If you specify `-protocol`, then you must specify a valid value in the `-file-operations` parameter. As the protocol version changes, the valid values might change.	`-protocol protocol`

Type of information	Option
File operations Specifies the list of file operations for the FPolicy event. The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values: • `close` for file close operations • `create` for file create operations • `create-dir` for directory create operations • `delete` for file delete operations • `delete_dir` for directory delete operations • `getattr` for get attribute operations • `link` for link operations • `lookup` for lookup operations • `open` for file open operations • `read` for file read operations • `write` for file write operations • `rename` for file rename operations • `rename_dir` for directory rename operations • `setattr` for set attribute operations • `symlink` for symbolic link operations **Note:** If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter.	`-file-operations` *file_operations*,...

Type of information	Option

Filters
 	
Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:
 	
• `monitor-ads` to filter the client request for alternate data stream
• `close-with-modification` to filter the client request for close with modification
• `close-without-modification` to filter the client request for close without modification
• `first-read` to filter the client request for first read
• `first-write` to filter the client request for first write
• `offline-bit` to filter the client request for offline bit set
  Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.
• `open-with-delete-intent` to filter the client request for open with delete intent
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.
• `open-with-write-intent` to filter client request for open with write intent
  Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.
• `write-with-size-change` to filter the client request for write with size change
 	
Note: If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.
	`-filters` *filter*, …

Is volume operation required Specifies whether volume operation monitoring is required. The default is `false`.	`-volume-operation` `{true|false}`

List of supported file operation and filter combinations that FPolicy can monitor for SMB

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported file operations	Supported filters
close	monitor-ads, offline-bit, close-with-modification, close-without-modification
create	monitor-ads, offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	monitor-ads, offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit
open	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent
read	monitor-ads, offline-bit, first-read
write	monitor-ads, offline-bit, first-write, write-with-size-change
rename	monitor-ads, offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	monitor-ads, offline-bit

List of supported file operation and filter combinations that FPolicy can monitor for NFSv3

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported file operations	Supported filters
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.

Supported file operations	Supported filters
link	offline-bit
lookup	offline-bit
read	offline-bit
write	offline-bit, write-with-size-change
rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit
symlink	offline-bit

List of supported file operation and filter combinations that FPolicy can monitor for NFSv4

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

Supported file operations	Supported filters
close	offline-bit
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit
link	offline-bit
lookup	offline-bit
open	offline-bit
read	offline-bit
write	offline-bit, write-with-size-change
rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit

Supported file operations	Supported filters
symlink	offline-bit

Completing the FPolicy event configuration worksheet

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage Virtual Machine (SVM) name	Yes	Yes	
Event name	Yes	Yes	
Protocol	No		
File operations	No		
Filters	No		
Is volume operation required	No		

Planning the FPolicy policy configuration

Before you configure the FPolicy policy, you must understand what it means to create an FPolicy policy. You must understand what configuration options are available. You also need to understand why you might want to attach more than one event to an FPolicy policy. This information helps you as you determine what values that you want to set.

What it means to create an FPolicy policy

Creating the FPolicy policy means associating a specific Storage Virtual Machine (SVM), an FPolicy event, and an FPolicy external engine (external engine) to an FPolicy policy. You also specify the following:

- Whether mandatory screening is required for this policy.
- Whether to use the Data ONTAP native external engine for simple file blocking or whether to specify an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management.
- Whether you want to associate more than one FPolicy event to the policy.

  An event is specific to a protocol. You can use a single FPolicy policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy.

- Whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection.

  If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.

What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy configuration parameters to help you plan your configuration:

Type of information	Option
SVM Specifies the SVM name on which you want to create an FPolicy policy. Each FPolicy configuration is defined within a single SVM. The external engine, FPolicy event, FPolicy scope, and FPolicy policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver` `vserver_name`
Policy name Specifies the name of the FPolicy policy. The name can be up to 256 characters long and is a string that can only contain any combination of ASCII-range alphanumeric characters (`a` through `z`, `A` through `Z`, and `0` through `9`), "`_`", and "`.`".	`-policy-name` `policy_name`
Event names Specifies a comma-delimited list of events to associate with the FPolicy policy. The events must already exist.	`-events` `event_name`, ...
External engine name Specifies the name of the external engine to associate with the FPolicy policy. The external engine must already exist. An external engine contains information required by the node to send notifications to an FPolicy server. The default value for this parameter is `native`. This means that, if you do not specify a value for the external engine, the default native external engine is used. The native external engine is internal to Data ONTAP and is used if you want to configure native file blocking and you do not want to use FPolicy servers. If you want to use the native external engine, you can either not specify a value for this parameter or you can specify `native` as the value.	`-engine` `engine_name`

Type of information	Option
Is mandatory screening required Specifies whether mandatory file access screening is required. This parameter specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When set to `true`, file access events are denied. When set to `false`, file access events are allowed. The default is `true`.	`-is-mandatory` `{true|false}`

Allow privileged access
 	
Specifies whether the FPolicy servers can have privileged access to monitored data.
 	
With this option set to `yes`, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data channel. The default is `no`.
	`-allow-`
	`privileged-access`
	`{yes|no|}`

Privileged user name Specifies the user name of the account the FPolicy servers use for privileged data access. The value for this parameter should use the "domain\user name" format. If `-allow-privileged-access` is set to `no`, any value set for this parameter is ignored.	`-privileged-user-` `name` *user_name*

Related concepts

Completing the FPolicy policy worksheet

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy policy.

You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage Virtual Machine (SVM) name	Yes	Yes	
Policy name	Yes	Yes	
Event names	Yes	Yes	

Type of information	Required	Include	Your values
External engine name	Yes	Yes	
Is mandatory screening required	No		
Allow privileged access	No		
Privileged user name	No		

Planning the FPolicy scope configuration

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

What it means to create an FPolicy scope

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The Storage Virtual Machine (SVM) is the basic boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply, and you must designate to which SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the "include" options. Notifications are not generated for file access events where matches are found in the "exclude" options.

The FPolicy scope configuration defines the following configuration information:

- SVM name
- Policy name
- The shares to include or exclude from what gets monitored
- The export policies to include or exclude from what gets monitored
- The volumes to include or exclude from what gets monitored
- The file extensions to include or exclude from what gets monitored
- Whether to do file extension checks on directory objects

Note: There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any SVM administrator can create the scope for that cluster policy. In the event that the SVM administrator creates a scope for that cluster FPolicy policy, the

cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

What the scope rules of precedence are

The following rules of precedence apply to scope configurations:

- When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.
- When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.
- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists. The `-file-extensions-to-exclude` parameter is checked first before the `-file-extensions-to-include` parameter is checked.

What the FPolicy scope configuration contains

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:

> **Note:** When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can contain regular expressions and can include metacharacters such as "?" and "*".

Type of information	Option
SVM Specifies the SVM name on which you want to create an FPolicy scope. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver` *vserver_name*
Policy name Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist.	`-policy-name` *policy_name*
Shares to include Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied.	`-shares-to-include` *share_name*, ...
Shares to exclude Specifies a comma-delimited list of shares to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-shares-to-exclude` *share_name*, ...

Type of information	Option
Volumes to include Specifies a comma-delimited list of volumes to monitor for the FPolicy policy to which the scope is applied.	`-volumes-to-include` `volume_name, ...`
Volumes to exclude Specifies a comma-delimited list of volumes to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-volumes-to-exclude` `volume_name, ...`
Export policies to include Specifies a comma-delimited list of export policies to monitor for the FPolicy policy to which the scope is applied.	`-export-policies-to-include` `export_policy_name, ...`
Export policies to exclude Specifies a comma-delimited list of export policies to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-export-policies-to-exclude` `export_policy_name, ...`
File extensions to include Specifies a comma-delimited list of file extensions to monitor for the FPolicy policy to which the scope is applied.	`-file-extensions-to-include` `file_extensions, ...`
File extension to exclude Specifies a comma-delimited list of file extensions to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-file-extensions-to-exclude` `file_extensions, ...`
Is file extension check on directory enabled Specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to `true`, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to `false`, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match.	`-is-file-extension-check-on-directories-enabled {true|false|}`

Completing the FPolicy scope worksheet

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage Virtual Machine (SVM) name	Yes	Yes	
Policy name	Yes	Yes	
Shares to include	No		
Shares to exclude	No		
Volumes to include	No		
Volumes to exclude	No		
Export policies to include	No		
Export policies to exclude	No		
File extensions to include	No		
File extension to exclude	No		
Is file extension check on directory enabled	No		

Creating the FPolicy configuration

There are several steps you must perform to creating an FPolicy configuration. First, you must plan your configuration. Then, you create an FPolicy external engine, an FPolicy event, and an FPolicy policy. You then create an FPolicy scope and attach it to the FPolicy policy, and then enable the FPolicy policy.

FPolicy is supported on Storage Virtual Machines (SVMs) with FlexVol volumes. FPolicy is not supported on SVMs with Infinite Volume.

Steps

1. Creating the FPolicy external engine on page 465
   The first step to creating an FPolicy configuration is to create an external engine. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the native external engine for simple file blocking, you do not need to configure an external engine.

2. Creating the FPolicy event on page 466
   As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

3. Creating the FPolicy policy on page 466

After creating an FPolicy external engine and FPolicy events, you create the FPolicy policy. The policy associates an external engine and one or more events to the policy. The FPolicy policy also specifies whether mandatory screening is required and whether the external FPolicy servers (FPolicy servers) have privileged access to data on the Storage Virtual Machine (SVM).

4. Creating the FPolicy scope on page 466
After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

5. Enabling the FPolicy policy on page 467
After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

Related concepts

What the steps for setting up an FPolicy configuration are on page 444
Planning the FPolicy configuration on page 445
Requirements, considerations, and best practices for configuring FPolicy on page 442
Displaying information about FPolicy configurations on page 469

Creating the FPolicy external engine

The first step to creating an FPolicy configuration is to create an external engine. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the native external engine for simple file blocking, you do not need to configure an external engine.

Before you begin

The external engine worksheet should be completed.

Steps

1. Create the FPolicy external engine:

```
vserver fpolicy policy external-engine create -vserver-name vserver_name
-engine-name engine_name -primary-servers IP_address,... -port integer -
ssl-option {no-auth|server-auth|mutual-auth} optional_parameters
```

2. Verify the FPolicy external engine configuration:

```
vserver fpolicy policy external-engine show -vserver vserver_name
```

Creating the FPolicy event

As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

Before you begin

The FPolicy event worksheet should be completed.

Steps

1. Create the FPolicy event:

   vserver fpolicy policy event create -vserver-name *vserver_name* **-event-name** *event_name* **optional_parameters**

2. Verify the FPolicy event configuration:

   vserver fpolicy policy event show -vserver *vserver_name*

Creating the FPolicy policy

After creating an FPolicy external engine and FPolicy events, you create the FPolicy policy. The policy associates an external engine and one or more events to the policy. The FPolicy policy also specifies whether mandatory screening is required and whether the external FPolicy servers (FPolicy servers) have privileged access to data on the Storage Virtual Machine (SVM).

Before you begin

- The FPolicy policy worksheet should be completed.
- If you plan on configuring the policy to use FPolicy servers, the external engine must exist.
- At least one FPolicy event that you plan on associating with the FPolicy policy must exist.

Steps

1. Create the FPolicy policy by entering the following command:

   vserver fpolicy policy create -vserver-name *vserver_name* **-policy-name** *policy_name* **-events** *event_name,...* **-engine** *engine_name* **optional_parameters**

2. Verify the FPolicy policy configuration:

   vserver fpolicy policy show -vserver *vserver_name*

Creating the FPolicy scope

After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy

policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

Before you begin

The FPolicy scope worksheet must be completed. The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event.

Steps

1. Create the FPolicy scope:

   ```
   vserver fpolicy policy scope create -vserver-name vserver_name -policy-
   name policy_name optional_parameters
   ```

2. Verify the FPolicy scope configuration:

   ```
   vserver fpolicy policy scope show -vserver vserver_name
   ```

Enabling the FPolicy policy

After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

Before you begin

The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event. The FPolicy policy scope must exist and must be assigned to the FPolicy policy.

About this task

The priority is used when multiple policies are enabled on the Storage Virtual Machine (SVM) and more than one policy has subscribed to the same file access event. Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.

   Note: A policy cannot be enabled on the admin SVM.

Steps

1. Enable the FPolicy policy by entering the following command:

   ```
   vserver fpolicy enable -vserver-name vserver_name -policy-name
   policy_name -sequence-number integer
   ```

2. Verify that the FPolicy policy is enabled:

   ```
   vserver fpolicy show -vserver vserver_name
   ```

Modifying FPolicy configurations

You can modify FPolicy configurations by modifying the elements that make up the configuration. You can modify external engines, FPolicy events, FPolicy scopes, and FPolicy policies. You can also enable or disable FPolicy policies. When you disable the FPolicy policy, file monitoring is discontinued for that policy.

It is recommended to disable the FPolicy policy before modifying the configuration.

Related concepts

Creating the FPolicy configuration on page 464
Managing FPolicy server connections on page 473

Commands for modifying FPolicy configurations

You can modify FPolicy external engines, events, scopes, and policies.

If you want to modify...	Use this command...
External engines	`vserver fpolicy policy external-engine modify`
Events	`vserver fpolicy policy event modify`
Scopes	`vserver fpolicy policy scope modify`
Policies	`vserver fpolicy policy modify`

See the man pages for the commands for more information.

Related references

Commands for displaying information about FPolicy configurations on page 470

Enabling or disabling FPolicy policies

You can enable FPolicy policies after the configuration is complete. Enabling the policy sets its priority and starts file access monitoring for the policy. You can disable FPolicy policies if you want to stop file access monitoring for the policy.

Before you begin

Before enabling FPolicy policies, the FPolicy configuration must be completed.

About this task

- The priority is used when multiple policies are enabled on the Storage Virtual Machine (SVM) and more than one policy has subscribed to the same file access event.
- Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.
- If you want to change the priority of an FPolicy policy, you must disable the policy and then reenable it using the new sequence number.

Step

1. Perform the appropriate action:

If you want to...	Enter the following command...
Enable an FPolicy policy	**vserver fpolicy enable -vserver-name** *vserver_name* **- policy-name** *policy_name* **-sequence-number** *integer*
Disable an FPolicy policy	**vserver fpolicy disable -vserver-name** *vserver_name* **- policy-name** *policy_name*

Related tasks

Displaying information about FPolicy configurations

You might want to display information about FPolicy configurations to determine whether the configuration for each Storage Virtual Machine (SVM) is correct or to verify that an FPolicy policy configuration is enabled. You can display information about FPolicy external engines, FPolicy events, FPolicy scopes, and FPolicy policies.

Related concepts

How the show commands work

It is helpful when displaying information about the FPolicy configuration to understand how the show commands work.

A show command without additional parameters displays information in a summary form. Additionally, every show command has the same two mutually exclusive optional parameters, - instance and -fields.

When you use the `-instance` parameter with a `show` command, the command output displays detailed information in a list format. In some cases, the detailed output can be lengthy and include more information than you need. You can use the `-fields` *fieldname[,fieldname...]* parameter to customize the output so that it displays information only for the fields you specify. You can identity which fields that you can specify by entering `?` after the `-fields` parameter.

> **Note:** The output of a `show` command with the `-fields` parameter might display other relevant and necessary fields related to the requested fields.

Every `show` command has one or more optional parameters that filter that output and enable you to narrow the scope of information displayed in command output. You can identity which optional parameters are available for a command by entering `?` after the `show` command.

The `show` command supports UNIX-style patterns and wildcards to enable you to match multiple values in command-parameters arguments. For example, you can use the wildcard operator (*), the NOT operator (!), the OR operator (|), the range operator (integer...integer), the less-than operator (<), the greater-than operator (>), the less-than or equal to operator (<=), and the greater-than or equal to operator (>=) when specifying values.

For more information about using UNIX-style patterns and wildcards, see the "Using the Data ONTAP command-line interface" section of the *Clustered Data ONTAP System Administration Guide for SVM Administrators*.

Commands for displaying information about FPolicy configurations

You use the `fpolicy show` commands to display information about the FPolicy configuration, including information about FPolicy external engines, events, scopes, and policies.

If you want to display information about FPolicy...	Use this command...
External engines	`vserver fpolicy policy external-engine show`
Events	`vserver fpolicy policy event show`
Scopes	`vserver fpolicy policy scope show`
Policies	`vserver fpolicy policy show`

See the man pages for the commands for more information.

Displaying information about FPolicy policy status

You can display information about the status for FPolicy policies to determine whether a policy is enabled, what external engine it is configured to use, what the sequence number is for the policy, and to which Storage Virtual Machine (SVM) the FPolicy policy is associated.

About this task

If you do not specify any parameter, the command displays the following information:

- SVM name
- Policy name
- Policy sequence number
- Policy status

In addition to displaying information about policy status for FPolicy policies configured on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output, or `-fields ?` to determine what fields you can use.

Step

1. Display filtered information about FPolicy policy status by using the appropriate command:

If you want to display status information about policies...	Enter the command...
On the cluster	`vserver fpolicy show`
That have the specified status	`vserver fpolicy show -status {on|off}`
On a specified SVM	`vserver fpolicy show -vserver vserver_name`
With the specified policy name	`vserver fpolicy show -policy-name policy_name`
With the specified sequence number	`vserver fpolicy show -sequence-number integer`
That use the specified external engine	`vserver fpolicy show -engine engine_name`

The following example displays the information about FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show
  Vserver      Policy                        Sequence  Status Engine
                                             Number
  -----------  --------------------------    --------  ------ ---------
  FPolicy      cserver_policy                      -   off    eng1
  vs1          v1p1                                -   off    eng2
  vs1          v1p2                                -   off    native
  vs1          v1p3                                -   off    native
  vs1          cserver_policy                      -   off    eng1
  vs2          v1p1                                3   on     native
  vs2          v1p2                                1   on     eng3
  vs2          cserver_policy                      2   on     eng1
```

Displaying information about enabled FPolicy policies

You can display information about enabled FPolicy policies to determine what FPolicy external engine it is configured to use, what the priority is for the policy, and to which Storage Virtual Machine (SVM) the FPolicy policy is associated.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy priority

You can use command parameters to filter the command's output by specified criteria.

Step

1. Display information about enabled FPolicy policies by using the appropriate command:

If you want to display information about enabled policies...	Enter the command...
On the cluster	**vserver fpolicy show-enabled**
On a specified SVM	**vserver fpolicy show-enabled -vserver** *vserver_name*
With the specified policy name	**vserver fpolicy show-enabled -policy-name** *policy_name*
With the specified sequence number	**vserver fpolicy show-enabled -priority** *integer*

The following example displays the information about enabled FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver             Policy Name              Priority

------------------ ------------------------ ----------
vs1                pol_native               native
vs1                pol_native2              native
vs1                pol1                     2
vs1                pol2                     4
```

Managing FPolicy server connections

You can manage your FPolicy server connections by connecting to external FPolicy servers, disconnecting from external FPolicy servers, or displaying information about connections and connection status.

Related concepts

What the two parts of the FPolicy solution are on page 434

What synchronous and asynchronous notifications are on page 435

How FPolicy works with external FPolicy servers on page 436

What the node-to-external FPolicy server communication process is on page 438

Connecting to external FPolicy servers

To enable file processing, you might need to manually connect to an external FPolicy server if the connection has previously been terminated. A connection is terminated after the server timeout is reached or due to some error. Alternatively, the administrator might manually terminate a connection.

About this task

If a fatal error occurs, the connection to the FPolicy server can be terminated. After resolving the issue that caused the fatal error, you must manually reconnect to the FPolicy server.

Steps

1. Connect to the external FPolicy server by using the `vserver fpolicy engine-connect` command.

   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is connected by using the `vserver fpolicy show-engine` command.

   For more information about the command, see the man pages.

Disconnecting from external FPolicy servers

You might need to manually disconnect from an external FPolicy server. This might be desirable if the FPolicy server has issues with notification request processing or if you need to perform maintenance on the FPolicy server.

Steps

1. Disconnect from the external FPolicy server by using the `vserver fpolicy engine-disconnect` command.

   For more information about the command, see the man pages.

2. Verify that the external FPolicy server is disconnected by using the `vserver fpolicy show-engine` command.

   For more information about the command, see the man pages.

Displaying information about connections to external FPolicy servers

You can display status information about connections to external FPolicy servers (FPolicy servers) for the cluster or for a specified Storage Virtual Machine (SVM). This information can help you determine which FPolicy servers are connected.

About this task

If you do not specify any parameter, the command displays the following information:

- SVM name
- Node name
- FPolicy policy name
- FPolicy server IP address
- FPolicy server status
- FPolicy server type

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter **?** after the `-fields` parameter to find out which fields you can use.

Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

If you want to display connection status information about...	Enter the command...
FPolicy servers that you specify	**vserver fpolicy show-engine -server _IP_address_**
FPolicy servers for a specified SVM	**vserver fpolicy show-engine -vserver _vserver_name_**
FPolicy servers that are attached with a specified policy	**vserver fpolicy show-engine -policy-name _policy_name_**
FPolicy servers with the server status that you specify	**vserver fpolicy show-engine -server-status _status_** The server status can be one of the following: • `connected` • `disconnected` • `connecting` • `disconnecting`
FPolicy servers with the specified type	**vserver fpolicy show-engine -server-type _type_** The FPolicy server type can be one of the following: • `primary` • `secondary`
FPolicy servers that were disconnected with the specified reason	**vserver fpolicy show-engine -disconnect-reason _text_** Disconnect can be due to multiple reasons. The following are common reasons for disconnect: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

This example displays information about external engine connections to FPolicy servers on SVM vs1:

```
cluster1::> vserver fpolicy show-engine -vserver vs1
 FPolicy                                     Server-      Server-
 Vserver Policy     Node          Server      status       type
```

```
 ------- --------- ------------ ------------- ----------- ---------
 vs1     policy1   node1        1.1.1.1       connected   primary
```

This example displays information only about connected FPolicy servers:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
 node       vserver policy-name server
 ---------- ------- ----------- -------
 node1      vs1     policy1     1.1.1.1
```

Copyright information

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Customer Fitness, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at *www.ibm.com/legal/copytrade.shtml*.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

* NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
* Telephone: +1 (408) 822-6000
* Fax: +1 (408) 822-4501
* Support telephone: +1 (888) 463-8277

Index

C

M

Q

R

W

X