Configure SMB with the CLI

ONTAP 9

NetApp
April 02, 2023

Table of Contents

Configure SMB with the CLI

SMB configuration overview with the CLI

You can use ONTAP 9 CLI commands to configure SMB client access to files contained in a new volume or qtree in a new or existing SVM.

SMB (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

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

- You want to use SMB version 2 or later.
- You want to serve SMB clients only, not NFS clients (not a multiprotocol configuration).
- NTFS file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

  Cluster administrator privileges are required to create SVMs and LIFs. SVM administrator privileges are sufficient for other SMB configuration tasks.

- You want to use the CLI, not System Manager or an automated scripting tool.

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

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

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

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

Other ways to do this in ONTAP

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

SMB configuration workflow

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

Preparation

Assess physical storage requirements

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

Steps

1. Display available space in existing aggregates: `storage aggregate show`

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

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

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

Assess networking requirements

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

Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)

- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

Steps

1. Display the available physical and virtual ports: `network port show`
   - When possible, you should use the port with the highest speed for the data network.
   - All components in the data network must have the same MTU setting for best performance.
2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: `network subnet show`

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

   You can use the default IPspace or a custom IPspace.
4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster: `network options ipv6 show`

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

Decide where to provision new SMB storage capacity

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

Choices

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

  Configuring SMB access to an SVM

  Configuring SMB client access to shared storage

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

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

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

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

  Configuring SMB client access to shared storage

Worksheet for gathering SMB configuration information

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

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

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

  Configuring SMB access to an SVM

  Configuring SMB client access to shared storage

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

  Configuring SMB client access to shared storage

The command man pages contain details about the parameters.

Configuring SMB access to an SVM

Parameters for creating an SVM

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

Field	Description	Your value
`-vserver`	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for new SMB storage capacity.	
`-rootvolume`	A unique name you supply for the SVM root volume.	
`-rootvolume-security-style`	Use the NTFS security style for the SVM.	`ntfs`

Field	Description	Your value
`-language`	Use the default language setting in this workflow.	`C.UTF-8`
`ipspace`	Optional: IPspaces are distinct IP address spaces in which SVMs reside.	

Parameters for creating a LIF

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

Field	Description	Your value
`-lif`	A name you supply for the new LIF.	
`-role`	Use the data LIF role in this workflow.	`data`
`-data-protocol`	Use only the SMB protocol in this workflow.	`cifs`
`-home-node`	The node to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-home-port`	The port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-address`	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
`-netmask`	The network mask and gateway for the LIF.	
`-subnet`	A pool of IP addresses. Used instead of `-address` and `-netmask` to assign addresses and netmasks automatically.	
`-firewall-policy`	Use the default data firewall policy in this workflow.	`data`

Field	Description	Your value
`-auto-revert`	Optional: Specifies whether a data LIF is automatically reverted to its home node on startup or under other circumstances. The default setting is `false`.	

Parameters for DNS host name resolution

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

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

Setting up an SMB server in an Active Directory domain

Parameters for time service configuration

You supply these values with the `cluster time-service ntp server create` command when you are configuring time services.

Field	Description	Your value
`-server`	The host name or IP address of the NTP server for the Active Directory domain.	

Parameters for creating an SMB server in an Active Directory domain

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify domain information.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	

Field	Description	Your value
`-domain`	The fully qualified domain name (FQDN) of the Active Directory domain to associate with the SMB server.	
`-ou`	Optional: The organizational unit within the Active Directory domain to associate with the SMB server. By default, this parameter is set to CN=Computers.	
`-netbios-aliases`	Optional: A list of NetBIOS aliases, which are alternate names to the SMB server name.	
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Setting up an SMB server in a workgroup

Parameters for creating an SMB server in a workgroup

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

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	
`-workgroup`	The name of the workgroup (up to 15 characters).	
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Parameters for creating local users

You supply these values when you create local users by using the `vserver cifs users-and-groups local-user create` command. They are required for SMB servers in workgroups and optional in AD domains.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local user.	
`-user-name`	The name of the local user (up to 20 characters).	
`-full-name`	Optional: The user's full name. If the full name contains a space, enclose the full name within double quotation marks.	
`-description`	Optional: A description for the local user. If the description contains a space, enclose the parameter in quotation marks.	
`-is-account-disabled`	Optional: Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.	

Parameters for creating local groups

You supply these values when you create local groups by using the `vserver cifs users-and-groups local-group create` command. They are optional for SMB servers in AD domains and workgroups.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local group.	
`-group-name`	The name of the local group (up to 256 characters).	
`-description`	Optional: A description for the local group. If the description contains a space, enclose the parameter in quotation marks.	

Adding storage capacity to an SMB-enabled SVM

Parameters for creating a volume

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

Field	Description	Your value
`-vserver`	The name of a new or existing SVM that will host the new volume.	
`-volume`	A unique descriptive name you supply for the new volume.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for the new SMB volume.	
`-size`	An integer you supply for the size of the new volume.	
`-security-style`	Use the NTFS security style for this workflow.	`ntfs`
`-junction-path`	Location under root (/) where the new volume is to be mounted.	

Parameters for creating a qtree

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

Field	Description	Your value
`-vserver`	The name of the SVM on which the volume containing the qtree resides.	
`-volume`	The name of the volume that will contain the new qtree.	
`-qtree`	A unique descriptive name you supply for the new qtree, 64 characters or less.	
`-qtree-path`	The qtree path argument in the format `/vol/volume_name/qtree_name\>` can be specified instead of specifying volume and qtree as separate arguments.	

Parameters for creating SMB shares

You supply these values with the `vserver cifs share create` command.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB share.	
`-share-name`	The name of the SMB share that you want to create (up to 256 characters).	
`-path`	The name of the path to the SMB share (up to 256 characters). This path must exist in a volume before creating the share.	
`-share-properties`	Optional: A list of share properties. The default settings are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.	
`-comment`	Optional: A text comment for the server (up to 256 characters). Windows clients can see this SMB share description when browsing on the network.	

Parameters for creating SMB share access control lists (ACLs)

You supply these values with the `vserver cifs share access-control create` command.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB ACL.	
`-share`	The name of the SMB share on which to create.	
`-user-group-type`	The type of the user or group to add to the share's ACL. The default type is `windows`	`windows`
`-user-or-group`	The user or group to add to the share's ACL. If you specify the user name, you must include the user's domain using the "domain\username" format.	
`-permission`	Specifies the permissions for the user or group.	`[ No_access | Read | Change | Full_Control ]`

Configure SMB access to an SVM

Configure SMB access to an SVM

If you do not already have an SVM configured for SMB client access, you must either create and configure a new SVM or configure an existing SVM. Configuring SMB involves opening SVM root volume access, creating an SMB server, creating a LIF, enabling host-name resolution, configuring name services, and if desired, enabling Kerberos security.

Create an SVM

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

Steps

1. Create an SVM: `vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - Use the NTFS setting for the `-rootvolume-security-style` option.
   - Use the default C.UTF-8 `-language` option.
   - The `ipspace` setting is optional.
2. Verify the configuration and status of the newly created SVM: `vserver show -vserver vserver_name`

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

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

Examples

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

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

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

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

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

Verify that the SMB protocol is enabled on the SVM

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

About this task

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

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

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

Steps

1. Check which protocols are currently enabled and disabled for the SVM: `vserver show -vserver vserver_name -protocols`

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

2. If necessary, enable or disable a protocol:
   - To enable the SMB protocol: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - To disable a protocol: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirm that the enabled and disabled protocols were updated correctly: `vserver show -vserver vserver_name -protocols`

Example

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

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

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

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

Open the export policy of the SVM root volume

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

About this task

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

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

Steps

1. If you are using an existing SVM, check the default root volume export policy: `vserver export-policy rule show`

   The command output should be similar to the following:

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

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

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

2. Create an export rule for the SVM root volume: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verify rule creation by using the `vserver export-policy rule show` command.

Results

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

Create a LIF

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

Before you begin

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

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

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

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each

node by using the `network interface capacity details show` command (at the advanced privilege level).

- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Steps

1. Create a LIF:

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

   ONTAP 9.5 and earlier

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

   ONTAP 9.6 and later

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

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

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

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

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

   - `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
   - You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
   - When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` man page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default `data` as the LIF role.

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

  > Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

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

2. Verify that the LIF was created successfully:

   ```
   network interface show
   ```

3. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Examples

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

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

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

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

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

```
network interface show

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

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

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

Enable DNS for host-name resolution

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

resolved using external DNS servers.

Before you begin

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

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

About this task

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

Steps

1. Enable DNS on the SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

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

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

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

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

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

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

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

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

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

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

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

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

Set up an SMB server in an Active Directory domain

Configure time services

Before creating an SMB server in an Active Domain controller, you must ensure that the cluster time and the time on the domain controllers of the domain to which the SMB server will belong matches to within five minutes.

About this task

You should configure cluster NTP services to use the same NTP servers for time synchronization that the Active Directory domain uses.

Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

Steps

1. Configure time services by using the `cluster time-service ntp server create` command.
   - To configure time services without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_ip_address`
   - To configure time services with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`

2. Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

   `cluster time-service ntp server show`

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this…	Use this command…
Configure an NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`
Configure an NTP server with symmetric authentication	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Enable symmetric authentication for an existing NTP serverAn existing NTP server can be modified to enable authentication by adding the required key-id.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure a server with a key ID not configured on the NTP server.	`cluster time-service ntp server create -server server_name -key-id key_id` The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.

To do this…	Use this command…
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -authentication disabled`

Create an SMB server in an Active Directory domain

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the Active Directory (AD) domain to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM and to an AD domain controller of the domain to which you want to join the SMB server.

Any user who is authorized to create machine accounts in the AD domain to which you are joining the SMB server can create the SMB server on the SVM. This can include users from other domains.

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

About this task

When creating an SMB server in an Activity Directory domain:

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default setting is to add the SMB server machine account to the Active Directory CN=Computer object.
- You can choose to add the SMB server to a different organizational unit (OU) by using the `-ou` option.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the SMB server.

  Configuring NetBIOS aliases for an SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original servers' names.

The `vserver cifs` man pages contain additional optional parameters and naming requirements.

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

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted. ONTAP requires encryption for domain controller communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3. .

SMB management contains more information about SMB server configuration options.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   If it is not, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in an AD domain: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   When joining a domain, this command might take several minutes to finish.

   The following command creates the SMB server “smb_server01” in the domain “example.com”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   The following command creates the SMB server “smb_server02” in the domain “mydomain.com” and authenticates the ONTAP administrator with a keytab file:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In this example, the command output shows that an SMB server named “SMB_SERVER01” was created on SVM vs1.example.com, and was joined to the “example.com” domain.

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

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                              Authentication Style: domain
                 CIFS Server Administrative Status: up
                           CIFS Server Description: -
                           List of NetBIOS Aliases: -
   ```

4. If desired, enable encrypted communication with the domain controller (ONTAP 9.8 and later): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Examples

The following command creates a SMB server named “smb_server02” on SVM vs2.example.com in the “example.com” domain. The machine account is created in the “OU=eng,OU=corp,DC=example,DC=com” container. The SMB server is assigned a NetBIOS alias.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

The following command enables a user from a different domain, in this case an administrator of a trusted domain, to create a SMB server named “smb_server03” on SVM vs3.example.com. The `-domain` option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the SMB server. The `username` option specifies the administrator of the trusted domain.

- Home domain: example.com
- Trusted domain: trust.lab.com
- Username for the trusted domain: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Create keytab files for SMB authentication

Beginning with ONTAP 9.7, ONTAP supports SVM authentication with Active Directory (AD) servers using keytab files. AD administrators generate a keytab file and make it available to ONTAP administrators as a uniform resource identifier (URI), which is supplied when `vserver cifs` commands require Kerberos authentication with the AD domain.

AD administrators can create the keytab files using the standard Windows Server `ktpass` command. The command should be run on the primary domain where authentication is required. The `ktpass` command can be used to generate keytab files only for primary domain users; keys generated using trusted-domain users are not supported.

Keytab files are generated for specific ONTAP admin users. As long as the admin user's password does not change, the keys generated for the specific encryption type and domain will not change. Therefore, a new keytab file is required whenever the admin user's password is changed.

The following encryption types are supported:

- AES256-SHA1
- DES-CBC-MD5

  ONTAP does not support DES-CBC-CRC encryption type.

- RC4-HMAC

AES256 is the highest encryption type and should be used if enabled on the ONTAP system.

Keytab files can be generated by specifying either the admin password or by using a randomly-generated password. However, at any given time only one password option can be used, because a private key specific to the admin user is needed at the AD server for decrypting the keys inside the keytab file. Any change in the private key for a specific admin will invalidate the keytab file.

Set up an SMB server in a workgroup

Set up an SMB server in a workgroup overview

Setting up an SMB server as a member in a workgroup consists of creating the SMB server, and then creating local users and groups.

You can configure an SMB server in a workgroup when the Microsoft Active Directory domain infrastructure is not available.

An SMB server in workgroup mode supports only NTLM authentication and does not support Kerberos authentication.

Create an SMB server in a workgroup

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the workgroup to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM.

About this task

SMB servers in workgroup mode do not support the following SMB features:

- SMB3 Witness protocol
- SMB3 CA shares
- SQL over SMB
- Folder Redirection
- Roaming Profiles

- Group Policy Object (GPO)
- Volume Snapshot Service (VSS)

The `vserver cifs` man pages contain additional optional configuration parameters and naming requirements.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   If it is not, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in a workgroup: `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

   The following command creates the SMB server “smb_server01” in the workgroup “workgroup01”:

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In the following example, the command output shows that a SMB server named “smb_server01” was created on SVM vs1.example.com in the workgroup “workgroup01”:

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                     NetBIOS Domain/Workgroup Name: workgroup01
                       Fully Qualified Domain Name: -
                               Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                    Workgroup Name: workgroup01
                               Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

After you finish

For a CIFS server in a workgroup, you must create local users, and optionally local groups, on the SVM.

Related information

SMB management

Create local user accounts

You can create a local user account that can be used to authorize access to data contained in the SVM over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

About this task

Local user functionality is enabled by default when the SVM is created.

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account.

The `vserver cifs users-and-groups local-user` man pages contain details about optional parameters and naming requirements.

Steps

1. Create the local user: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   The following optional parameters might be useful:

   - `-full-name`

     The users's full name.

   - `-description`

     A description for the local user.

   - `-is-account-disabled {true|false}`

     Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.

   The command prompts for the local user's password.

2. Enter a password for the local user, and then confirm the password.
3. Verify that the user was successfully created: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Example

The following example creates a local user "SMB_SERVER01\sue", with a full name "Sue Chang", associated with SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Create local groups

You can create local groups that can be used for authorizing access to data associated with the SVM over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

About this task

Local group functionality is enabled by default when the SVM is created.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can specify a group name with or without the local domain name, and you can optionally specify a description for the local group. You cannot add a local group to another local group.

The `vserver cifs users-and-groups local-group` man pages contain details about optional parameters and naming requirements.

Steps

1. Create the local group: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   The following optional parameter might be useful:

   - `-description`

     A description for the local group.

2. Verify that the group was successfully created: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Example

The following example creates a local group “SMB_SERVER01\engineering” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                   Description
---------------- ---------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators       Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators     Backup Operators group
vs1.example.com  BUILTIN\Power Users          Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

After you finish

You must add members to the new group.

Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group, or if you want users to have privileges associated with that group.

About this task

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- To remove a member from a local group, ONTAP must be able to resolve their name to a SID.

Steps

1. Add a member to or remove a member from a group.
   - Add a member: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     You can specify a comma-delimited list of local users, domain users, or domain groups to add to the

specified local group.

- Remove a member: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

Examples

The following example adds a local user “SMB_SERVER01\sue” to the local group “SMB_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

The following example removes the local users “SMB_SERVER01\sue” and “SMB_SERVER01\james” from the local group “SMB_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verify enabled SMB versions

Your ONTAP 9 release determines which SMB versions are enabled by default for connections with clients and domain controllers. You should verify that the SMB server supports the clients and functionality required in your environment.

About this task

For connections with both clients and domain controllers, you should enable SMB 2.0 and later whenever possible. For security reasons, you should avoid using SMB 1.0, and you should disable it if you have verified that it is not required in your environment.

In ONTAP 9, SMB versions 2.0 and later are enabled by default for client connections, but the version of SMB 1.0 enabled by default depends on your ONTAP release.

- Beginning with ONTAP 9.1 P8, SMB 1.0 can be disabled on SVMs.

  The `-smb1-enabled` option to the `vserver cifs options modify` command enables or disables SMB 1.0.

- Beginning with ONTAP 9.3, it is disabled by default on new SVMs.

If your SMB server is in an Active Directory (AD) domain, you can enable SMB 2.0 to connect to a domain controller (DC) beginning with ONTAP 9.1. Doing so is necessary if you have disabled SMB 1.0 on DCs. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default for DC connections.

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

SMB management contains details about supported SMB versions and functionality.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Verify which SMB versions are enabled: `vserver cifs options show`

   You can scroll down the list to view the SMB versions enabled for client connections, and if you are configuring an SMB server in an AD domain, for AD domain connections.

3. Enable or disable the SMB protocol for client connections as required:
   - To enable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version true`
   - To disable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version false` Possible values for `smb_version`:
   - `-smb1-enabled`
   - `-smb2-enabled`
   - `-smb3-enabled`
   - `-smb31-enabled` The following command enables SMB 3.1 on SVM vs1.example.com:

   ```
   cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31
   -enabled true
   ```

4. If your SMB server is in an Active Directory domain, enable or disable the SMB protocol for DC connections as required:
   - To enable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true`
   - To disable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false`
5. Return to the admin privilege level: `set -privilege admin`

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data LIF.
3. If you use NetBIOS aliases, create an Alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Configure SMB client access to shared storage

Configure SMB client access to shared storage

To provide SMB client access to shared storage on an SVM, you must create a volume or qtree to provide a storage container, and then create or modify a share for that container. You can then configure share and file permissions, and test access from client systems.

Before you begin

- SMB must be completely set up on the SVM.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to an Active Directory domain or workgroup configuration must be complete.

Create a volume or qtree storage container

Create a volume

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

Before you begin

The SVM security style must be NTFS, and SMB should be set up and running.

About this task

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

Steps

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

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

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

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

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

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

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

2. Verify that the volume was created with the desired junction point: `volume show -vserver vserver_name -volume volume_name -junction`

Examples

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

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

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

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

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

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

Create a qtree

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

Before you begin

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

Steps

1. Create the qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

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

2. Verify that the qtree was created with the desired junction path: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Example

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

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

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

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

Requirements and considerations for creating an SMB share

Before creating an SMB share, you must understand requirements for share paths and share properties, particularly for home directories.

Creating an SMB share entails specifying a directory path structure (using the `-path` option in the `vserver cifs share create` command) that clients will access. The directory path corresponds to the junction path for a volume or qtree that you created in the SVM namespace. The directory path and corresponding junction path must exist before creating your share.

Share paths have the following requirements:

- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be put in quotes (for example, `"/new volume/mount here"`).
- If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial “\\” in the UNC path), then the **Security** tab in the Windows Properties box is unavailable.

  This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

Share property defaults can be changed:

- The default initial properties for all shares are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.
- It is optional to specify share properties when you create a share.

However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all of the share properties that you want to apply to the share using a comma-delimited list.

- To designate a home directory share, use the `homedirectory` property.

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

  You cannot add or remove this property after creating the share.

Home directory shares have the following requirements:

- Before creating SMB home directories, you must add at least one home directory search path by using the `vserver cifs home-directory search-path add` command.
- Home directory shares specified by the value of `homedirectory` on the `-share-properties` parameter must include the `%w` (Windows user name) dynamic variable in the share name.

  The share name can additionally contain the `%d` (domain name) dynamic variable (for example, `%d/%w`) or a static portion in the share name (for example, `home1_%w`).

- If the share is used by administrators or users to connect to other users' home directories (using options to the `vserver cifs home-directory modify` command), the dynamic share name pattern must be preceded by a tilde (`~`).

SMB management and `vserver cifs share` man pages have additional information.

Create an SMB share

You must create an SMB share before you can share data from an SMB server with SMB clients. When you create a share, you can set share properties, such as designating the share as a home directory. You can also customize the share by configuring optional settings.

Before you begin

The directory path for the volume or qtree must exist in the SVM namespace before creating the share.

About this task

When you create a share, the default share ACL (default share permissions) is `Everyone / Full Control`. After testing access to the share, you should remove the default share ACL and replace it with a more secure alternative.

Steps

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

   The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

2. Create an SMB share associated with the specified SVM: `vserver cifs share create -vserver`

```
vserver_name -share-name share_name -path path [-share-properties
share_properties,...] [other_attributes] [-comment text]
```

3. Verify that the share was created:`vserver cifs share show -share-name share_name`

Examples

The following command creates an SMB share named “SHARE1” on SVM `vs1.example.com`. Its directory path is `/users`, and it is created with default properties.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

   b. On the newly created drive, create a test file, and then delete the file.

   You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

Before you begin

You must have decided which users or groups will be given access to the share.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

Steps

1. Delete the default share ACL:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a…	Enter the command…
Windows user	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Windows group	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the "`vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$         BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales      DOMAIN\"Sales Team"     windows     Change
```

The following commands give `Change` permission to the local Windows group named “Tiger Team” and `Full_Control` permission to the local Windows user named “Sue Chang” for the “datavol5” share on the "`vs1`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configure NTFS file permissions in a share

To enable file access to the users or groups who have access to a share, you must configure NTFS file permissions on files and directories in that share from a Windows client.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

SMB management and your Windows documentation contain information about how to set standard and advanced NTFS permissions.

Steps

1. Log in to a Windows client as an administrator.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the SMB server name containing the share that contains the data to which you want to apply permissions and the name of the share.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\SHARE1`.

      You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Select the file or directory for which you want to set NTFS file permissions.
5. Right-click the file or directory, and then select **Properties**.
6. Select the **Security** tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

7. Click **Edit**.

   The Permissions for <Object> box opens.

8. Perform the desired actions:

If you want to….	Do the following…
Set standard NTFS permissions for a new user or group	a. Click **Add**. The Select User, Computers, Service Accounts, or Groups window opens. b. In the **Enter the object names to select** box, type the name of the user or group on which you want to add NTFS permission. c. Click **OK**.

If you want to….	Do the following…
Change or remove standard NTFS permissions from a user or group	In the **Group or user names** box, select the user or group that you want to change or remove.

9. Perform the desired actions:

If you want to…	Do the following
Set standard NTFS permissions for a new or existing user or group	In the **Permissions for <Object>** box, select the **Allow** or **Deny** boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click **Remove**.

If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

10. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

Verify user access

You should test that the users you configured can access the SMB share and the files it contains.

Steps

1. On a Windows client, log in as one of the users who now has access to the share.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the share name you will provide to users.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\share1`.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.
4. Create a test file, verify that it exists, write text to it, and then remove the test file.

Copyright information

Trademark information