SMB server support

ONTAP 9

NetApp
January 18, 2023

Table of Contents

SMB server support

SMB server support overview

You can enable and configure SMB servers on storage virtual machines (SVMs) to let SMB clients access files on your cluster.

- Each data SVM in the cluster can be bound to exactly one Active Directory domain.
- Data SVMs do not need to be bound to the same domain.
- Multiple SVMs can be bound to the same domain.

You must configure the SVMs and LIFs that you are using to serve data before you can create an SMB server. If your data network is not flat, you might also need to configure IPspaces, broadcast domains, and subnets. The *Network Management Guide* contains details.

Related information

Network management

Modify SMB servers

System administration

Supported SMB versions and functionality

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. In ONTAP 9, all SMB versions are supported; however, default SMB 1.0 support depends on your ONTAP version. You should verify that the ONTAP SMB server supports the clients and functionality required in your environment.

The latest information about which SMB clients and domain controllers ONTAP supports is available in the *Interoperability Matrix Tool*.

SMB 2.0 and later versions are enabled by default for ONTAP 9 SMB servers, and can be enabled or disabled as needed. The following table shows SMB 1.0 support and default configuration.

SMB 1.0 functionality:	**In these ONTAP 9 releases:**			
	9.0	9.1	9.2	9.3 and later
Is enabled by default	Yes	Yes	Yes	No
Can be enabled or disabled	No	Yes*9.1 P8 or later required.	Yes	Yes

Default settings for SMB 1.0 and 2.0 connections to domain controllers also depend on the ONTAP version. More information is available in the `vserver cifs security modify` man page. For environments with existing CIFS servers running SMB 1.0, you should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

The following table shows which SMB features are supported in each SMB version. Some SMB features are enabled by default and some require additional configuration.

This functionality:	**Requires enablement:**	**Is supported in ONTAP 9 for these SMB versions:**				
		1.0	2.0	2.1	3.0	3.1.1
Legacy SMB 1.0 functionality		X	X	X	X	X
Durable handles			X	X	X	X
Compounded operations			X	X	X	X
Asynchronous operations			X	X	X	X
Increased read and write buffer sizes			X	X	X	X
Increased scalability			X	X	X	X
SMB signing	X	X	X	X	X	X
Alternate Data Stream (ADS) file format	X	X	X	X	X	X
Large MTU (enabled by default beginning with ONTAP 9.7)	X			X	X	X
Lease oplocks				X	X	X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:				
Continuously available shares	X				X	X
Persistent handles					X	X
Witness					X	X
SMB encryption: AES-128-CCM	X				X	X
Scale out (required by CA shares)					X	X
Transparent failover					X	X
SMB Multichannel (beginning with ONTAP 9.4)	X				X	X
Preauthentication integrity						X
Cluster client failover v.2 (CCFv2)						X
SMB encryption: AES-128-GCM (beginning with ONTAP 9.1)	X					X

Related information

Using SMB signing to enhance network security

Setting the SMB server minimum authentication security level

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

NetApp Technical Report 4543: SMB Protocol Best Practices

NetApp Interoperability

Unsupported Windows features

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

ONTAP does not support the following Windows features:

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

Configure NIS or LDAP name services on the SVM

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

Before you begin

You must have customized your name services database configuration to match your name service infrastructure.

About this task

SVMs use the name services ns-switch databases to determine the order in which to look up the sources for a given name service database. The ns-switch source can be any combination of “files”, “nis”, or “ldap”. For the groups database, ONTAP attempts to get the group memberships from all configured sources and then uses the consolidated group membership information for access checks. If one of these sources is unavailable at the time of obtaining UNIX group information, ONTAP cannot get the complete UNIX credentials and subsequent access checks might fail. Therefore, you must always check that all ns-switch sources are configured for the group database in the ns-switch settings.

The default is to have the SMB server map all Windows users to the default UNIX user that is stored in the local `passwd` database. If you want to use the default configuration, configuring NIS or LDAP UNIX user and group name services or LDAP user mapping is optional for SMB access.

Steps

1. If UNIX user, group, and netgroup information is managed by NIS name services, configure NIS name services:

   a. Determine the current ordering of name services by using the `vserver services name-service ns-switch show` command.

      In this example, the three databases (`group`, `passwd`, and `netgroup`) that can use `nis` as a name service source are using only `files` as a source.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                  Source
      Vserver         Database       Enabled      Order
      --------------- ------------   ---------    ---------
      vs1             hosts          true         dns,
                                                  files
      vs1             group          true         files
      vs1             passwd         true         files
      vs1             netgroup       true         files
      vs1             namemap        true         files
      ```

      You must add the `nis` source to the `group` and `passwd` databases, and optionally to the `netgroup` database.

   b. Adjust the name service ns-switch database ordering as desired by using the `vserver services name-service ns-switch modify` command.

      For best performance, you should not add a name service to a name service database unless you plan on configuring that name service on the SVM.

      If you modify the configuration for more than one name service database, you must run the command separately for each name service database that you want to modify.

      In this example, `nis` and `files` are configured as sources for the `group` and `passwd` databases, in that order. The rest of the name service databases are unchanged.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database group
      -sources nis,files vserver services name-service ns-switch modify -vserver
      vs1 -database passwd -sources nis,files
      ```

   c. Verify that the ordering of name services is correct by using the `vserver services name-service ns-switch show` command.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

```
                                                    Source
Vserver         Database       Enabled              Order
--------------- ------------   ---------            ---------
vs1             hosts          true                 dns,
                                                    files
vs1             group          true                 nis,
                                                    files
vs1             passwd         true                 nis,
                                                    files
vs1             netgroup       true                 files
vs1             namemap        true                 files
```

d. Create the NIS name service configuration:
`vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,… -active true+`

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

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

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

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

```
Vserver       Domain              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   10.0.0.60
```

2. If UNIX user, group, and netgroup information or name mapping is managed by LDAP name services, configure LDAP name services by using the information located NFS management.

How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should

still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

Example

The following example displays the name service switch configuration for the SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

Copyright information

Trademark information