SMB protocol support

The server implements the SMB protocols as used by Microsoft Windows platforms. From the client perspective, the server is indistinguishable from a Windows file server.

It provides all of the normal file-serving functions, including:

- Share manipulation (for example, add, list, and delete).
- File manipulation (for example, read, write, create, delete, move, and copy).
- File locking and byte-range locking.
- File access control using standard Windows ACLs.
- File and directory attributes (for example, read-only, and archive).
- Automatic creation of user home directories.

Note

The server does not support the following SMB features:

- Windows Extended Attributes (note that this should not be confused with NFS or POSIX xattr).
- BranchCache.
- Support for remote management from Server Manager (Windows Server 2012 or later).
- SMB2 large read/write MTU (NAS Server limited to 64KiB).
- SMB3 Directory Leasing.
- SMB Direct (SMB3 over RDMA).
- Offloaded Data Transfer (ODX).
- Library storage (for Hyper-V management tools).

Prerequisites

To enable SMB access to the server:

- Enter a CIFS license key.
- Enable the CIFS service.
- Configure the server.

Depending on the security model used on the SMB network, configure the server using one of the following methods:

Security Model	Client Authentication	Configuration Method
NT Domain security	NT 4 only	Add server to NT domain

Security Model	Client Authentication	Configuration Method
Active Directory	NT 4 only	Add server to NT domain
	Kerberos and NT 4	Join Active Directory

When configured to join an Active Directory, the server functions the same way as a server added to an NT domain, except that after joining an Active Directory, the server can authenticate clients using the Kerberos protocol as well as NT 4-style authentication. Most modern Windows clients support both authentication methods, though a number of older Windows clients only support NT 4-style authentication.

Supported clients

The server supports platforms and clients that are compliant with SMB versions 1, 2, 2.1, and 3.

Domain controller interaction

The storage server relies on Windows domain controllers to authenticate users and to obtain user information (for example, group membership). The server automatically discovers and connects to the fastest and most reliable domain controllers. Because operating conditions can change over time, the server selects the best domain controller every 10 minutes.

By default, when authenticating clients in an Active Directory, the server uses the time maintained by the domain controller, automatically adjusting for any clock inconsistencies.

Dynamic DNS

The storage server supports DNS and DDNS. For more information, see the Network Administration Guide.

SMB (CIFS) Statistics

SMB statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

Supported SMB versions

The NAS server supports the SMB file sharing protocols with the following versions: SMB1, SMB2.0, SMB2.1, SMB3.

Server version	Default max supported SMB version
11.2 and earlier	SMB1
11.3 and later	SMB2

The maximum supported SMB version advertised by the NAS server can be configured using the smb-max-supported-version CLI command (see below). The maximum supported SMB dialect is not server or cluster-wide - it is set on a per-

EVS basis.

The NAS server supports UCS-2 character encoding when using the SMB protocols (the character set is not negotiable when using the SMB2 protocol).
Notes

- A valid CIFS license is required in order to enable SMB2 or SMB3 support (CIFS is a dialect of SMB). For more information about license keys, refer to the Server and Cluster Administration Guide.
- One of the features of SMB is the ability to assign rights to machine (computer) accounts. The feature acts the same way as authentication of a normal user for an SMB session and can be used for authentication using machine accounts (SessionSetup SMB requests), and for management (add, delete, list) of rights for machine accounts. A machine account is generated automatically by the operating system and registered in Active Directory. It can be used for authentication within a domain. Machine account authentication can be only done by an application which has built-in support. For example, Hyper-V server allows storing virtual machines on remote shares. Such shares should allow full access for the machine account of a computer running Hyper-V server. Authenticated connections using machine accounts will show up in "connection" command output as if it was a normal user connection. The man pages for cifs-saa and cacls-add include an example of computer account use.

Specifying the SMB version for use by the EVS

To specify a version of the SMB protocol for use by the EVS, use the following commands:

- smb-max-supported-version - sets or displays the maximum supported version for both the NAS server and the client. The default is SMB2.
- smb-min-supported-version - limits the minimum supported version for both the NAS server and the client. The default is SMB1.

Note SMB2 cannot be enabled if there are NT4 names and no ADS names configured on the server.

Disabling SMB1

To disable SMB1 on the NAS server, use the following command:

smb-min-supported-version 2

This command sets the minimum SMB version on the NAS server to SMB2, therefore preventing any new clients connecting using SMB1.

Notes

- When a client initiates an SMB connection it advertises support for several versions/dialects. The server will choose the maximum version/dialect the client provides that is within its configured maximum/minimum. For example, a client that supports SMB1, SMB2 and SMB2.1 can establish an SMB2 connection if the max-supported version on the server is set to SMB2.
- Some SMB clients cache the connection type they last used with a server. If they last used SMB2/2.1/3, they may not offer SMB1 as an option until they are restarted.
- Existing SMB/SMB2/SMB3 client connections will continue to function after the minimum supported version has been raised.

Supported SMB3 functionality for Hyper-V

The NAS server supports SMB3 functionality for Microsoft Hyper-V over SMB shares, including transparent failover, continuous availability, and shadow copies.

- **Continuous Availability:** Enables files that are opened using SMB3 on a continuously available share to survive network failures or cluster node failures. For example, if one cluster node fails, the client transparently reconnects to another cluster node without interruption to the client applications.

  If a continuously available share is changed from a cluster to a single server, and then back to a cluster, the server keeps the continuous availability of the share.
  NoteContinuous Availability can impact SMB performance and should only be enabled where it is required, such as with Microsoft Hyper-V or Microsoft SQL Server. When this feature is in use, it is also recommended that the Administrator disables DDNS on the server.
- **Persistent file handles:** Enables clients to transparently reconnect to disconnected SMB sessions. A persistent handle is preserved after a disconnection and blocks any attempts to open files while it waits for the client to reconnect.
- **VSS for SMB file shares:** The File Server Remote VSS (Volume Shadow Copy Service) Protocol (FSRVP) is a protocol for Windows Server 2012 that creates shadow copies of file shares on a remote computer. This protocol is most commonly deployed with Hyper-V and enables backup applications to create application-consistent backup and restore of VSS-aware applications storing data on network file shares.
- **Service Witness Protocol:** Enables a registered client to receive notification of any state changes on a continuously available server, without needing to wait for the connection to time out. This ensures that there is a fast notification and recovery time from an unplanned failure, such as a network loss.
- **SMB3 Multichannel:** Enables file servers to use multiple network connections simultaneously. This increases the network performance and availability of the file servers, and improves data throughput and fault tolerance. With SMB3 Multichannel, applications can utilize all available network bandwidth and increase resilience during network failures.

SMB3 Multichannel support

SMB3 Multichannel enables file servers to use multiple network connections simultaneously. This feature increases the network performance and availability of the file servers.

SMB3 Multichannel benefits include:

- Automatic configuration.
- Client-side network processing on multiple CPU cores.
- Increased data throughput.
- Increased fault tolerance.
- Resilience during network failures.

SMB3 Multichannel is automatically enabled if the EVS is configured for version 3 of the SMB protocol. To set the version, use the smb-max-supported-version 3 command.

CLI commands

All settings for Multichannel are per EVS. Use the following CLI commands to configure or view the maximum channels per session:

- smb3-multichannel-max-channels-per-session-set

  Sets the maximum number of channels for all subsequent sessions.
  - Default: 32 channels
  - Minimum: 2 channels
  - Maximum: 64 channels
- smb-multichannel-max-channels-per-session-show

  Shows the maximum number of channels per session.

For more information about the CLI commands, see the *Command Line Reference*.