SMB configuration for Microsoft Hyper-V and SQL Server

ONTAP 9

NetApp
February 28, 2022

Table of Contents

SMB configuration for Microsoft Hyper-V and SQL Server

SMB configuration for Microsoft Hyper-V and SQL Server overview

ONTAP features allow you to enable nondisruptive operations for two Microsoft applications over the SMB protocol: Microsoft Hyper-V and Microsoft SQL Server.

You should use these procedures if you want to implement SMB nondisruptive operations under the following circumstances:

- Basic SMB protocol file access has been configured.
- You want to enable SMB 3.0 or later file shares residing in SVMs to store the following objects:
  - Hyper-V virtual machine files
  - SQL Server system databases

Related information

For additional information about ONTAP technology and interaction with external services, see these Technical Reports (TRs): **NetApp Technical Report 4172: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices** NetApp Technical Report 4369: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP

Configure ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

You can use continuously available SMB 3.0 and later file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in SVMs, while at the same time providing nondisruptive operations (NDOs) for both planned and unplanned events.

Microsoft Hyper-V over SMB

To create a Hyper-V over SMB solution, you must first configure ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.

The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with Hyper-V over SMB configurations.

  For information about using SnapManager with Hyper-V over SMB configurations, see *SnapManager for*

Hyper-V Installation and Administration Guide.

Microsoft SQL Server over SMB

To create a SQL Server over SMB solution, you must first configure ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.

SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server, see the Microsoft web site.
- SnapManager for Microsoft SQL Server is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with SQL Server over SMB configurations.

  For information about using SnapManager for Microsoft SQL Server, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

Nondisruptive operations for Hyper-V and SQL Server over SMB

What nondisruptive operations for Hyper-V and SQL Server over SMB means

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover
- Upgrade
- Planned aggregate relocation (ARL)
- LIF migration and failover
- Planned volume move

Protocols that enable nondisruptive operations over SMB

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

- SMB 3.0
- Witness

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

- **Continuously available share**

  An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.

- **Node**

  A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the *local node* and the other node is sometimes called the *partner node* or *remote node*. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner's storage.

- **Nondisruptive aggregate relocation**

  The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.

- **Nondisruptive failover**

  See *Takeover*.

- **Nondisruptive LIF migration**

  The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.

- **Nondisruptive operations**

  The ability to perform major ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.

- **Nondisruptive upgrade**

  The ability to upgrade node hardware or software without application interruption.

- **Nondisruptive volume move**

  The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.

- **Persistent handles**

  A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost. However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

  Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

- **SFO giveback**

  Returning aggregates to their home locations when recovering from a takeover event.

- **SFO pair**

  A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.

- **Takeover**

  The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

How SMB 3.0 functionality supports nondisruptive operations over SMB shares

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the `continuously-available` share property and a type of file handle known as a *persistent handle* that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the continuously available share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the storage virtual machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if

a failure causes the Hyper-V application to fail over to another node in the Windows Server cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. “Failover Clustering” is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

What the Witness protocol does to enhance transparent failover

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

- It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
- The shares must use SMB 3.0 with the continuous availability share property set.
- The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the storage virtual machine (SVM) hosting data for the application servers.

> The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner. The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

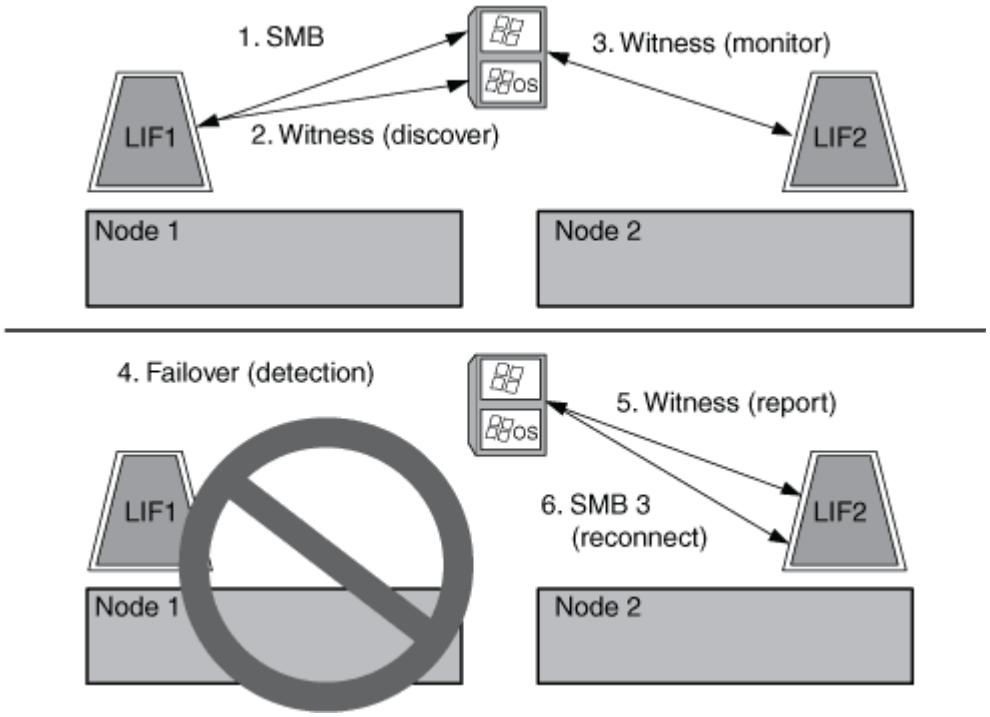
How the Witness protocol works

ONTAP implements the Witness protocol by using a node’s SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.
2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the storage virtual machine (SVM).
3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.
4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.
5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.

6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.



Share-based backups with Remote VSS

Share-based backups with Remote VSS overview

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

- **VSS (Volume Shadow Copy Service)**

  A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.

- **Shadow copy**

  A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

- **Shadow copy set**

  A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

- **Shadow copy set automatic recovery**

  The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

- **Shadow copy ID**

  A GUID that uniquely identifies a shadow copy.

- **Shadow copy set ID**

  A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

- **SnapManager for Hyper-V**

  The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

Related information

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

Share-based backups with Remote VSS

Example of a directory structure used by Remote VSS

Remote VSS traverses the directory structure that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is, so that you can successfully create backups of virtual machine files.

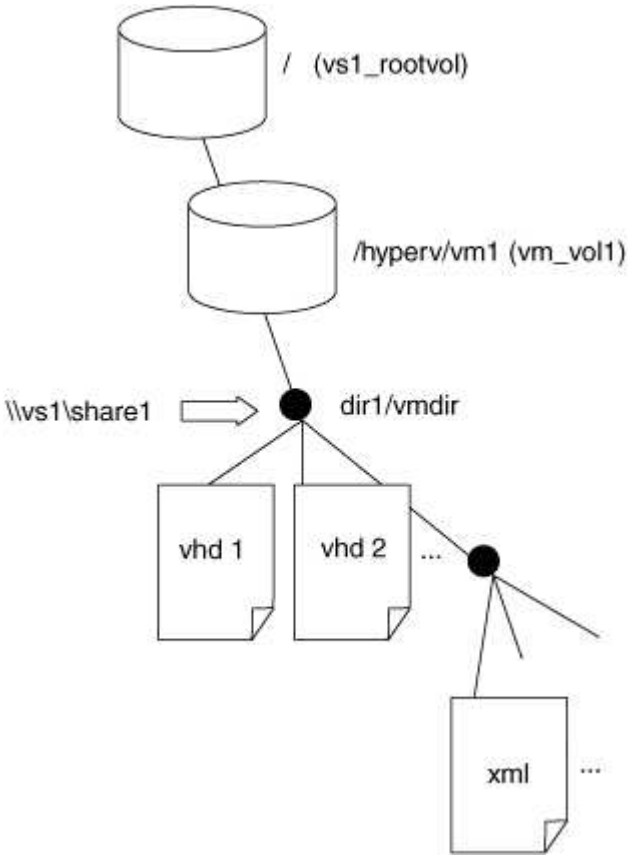
A supported directory structure for the successful creation of shadow copies conforms to the following requirements:

- Only directories and regular files are present within the directory structure that is used to store virtual machine files.

  The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.
- The directory structure that is used to store virtual machine files does not exceed the configured depth of the shadow copy directory.
- The root directory of the share contains only virtual machine files or directories.

In the following illustration, the volume named vm_vol1 is created with a junction point at `/hyperv/vm1` on storage virtual machine (SVM) vs1. Subdirectories to contain the virtual machine files are created under the junction point. The virtual machine files of the Hyper-V server are accessed over share1 that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files that are contained within the directory structure under share1 (up to the configured depth of the shadow copy directory).



How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with ONTAP provides performance optimization when discovering SMB share location.

  ONTAP provides SnapDrive with the name of the volume where the share resides.

- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

  By providing a targeted list of virtual machine files, the shadow copy service does not need to create shadow copies of all the files in the share.

- The storage virtual machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.

  There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation

   The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

2. Creating the shadow copy set (if automatic-recovery is used)

   For every share included in the shadow copy set, ONTAP creates a shadow copy and makes the shadow copy writable.

3. Exposing the shadow copy set

   After ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

4. Automatically recovering the shadow copy set

   During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.

   The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

5. Completing and cleaning up the shadow copy set

   The VSS client notifies ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

This functionality is available on Windows Server 2012 servers. ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same storage virtual machine (SVM)

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

> To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

- You can use ODX copy offload to export and import SQL Server databases between mapped SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.
- ODX copy offload is used for database exports and imports if the source and destination storage is on the same cluster.

Configuration requirements and considerations

ONTAP and licensing requirements

You need to be aware of certain ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs.

ONTAP version requirements

- Hyper-V over SMB

  ONTAP supports nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.

- SQL Server over SMB

  ONTAP supports nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)

  This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to

create point-in-time copies of files that are then used when creating a backup.

A FlexClone license is optional if you use a backup method that does not use Remote VSS.

Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations).

Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.

  SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.

- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the storage virtual machine (SVM).

  The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple connections to multiple unique IP addresses.

  Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

  Beginning with ONTAP 9.4, you can improve throughput and fault tolerance for Hyper-V and SQL server over SMB configurations by enabling SMB Multichannel. To do so, you must have multiple 1G, 10G, or larger NICs deployed on the cluster and clients.

Data LIF requirements

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.

  SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.

- Data LIFs must not be configured to automatically revert.

  After a takeover or giveback event, you should manually revert the data LIFs to their home ports.

- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name.

  The application servers must connect to SMB shares by using the CIFS server name. You must not configure the application servers to make connections by using the LIF IP addresses.

- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

SMB server and volume requirements for Hyper-V over SMB

You need to be aware of certain SMB server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.

- Both Kerberos and NTLM authentication must be allowed in the domain to which the SMB server belongs.

  ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.

- Shadow copy functionality must be enabled.

  This functionality is enabled by default.

- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the SMB server local BUILTIN\Administrators or BUILTIN\Backup Operators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- For shadow copy operations to succeed, you must have enough available space on the volume.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

SMB server and volume requirements for SQL Server over SMB

You need to be aware of certain SMB server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

  Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.

- The Windows user account used for installing SQL Server on ONTAP must be assigned the SeSecurityPrivilege privilege.

  This privilege is assigned to the SMB server local BUILTIN\Administrators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.

The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

Share requirements

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.

  In the auto-recovery case, the shadow copy creation fails if a junction is encountered while traversing the share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files

    The shadow copy creation fails if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.

  - For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).

    The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache
  - Access-based enumerations

Considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for Hyper-V over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` parameter set to `Yes`.

Continuously available share requirements and considerations for SQL Server over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

Share requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapManager for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.

  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

- Access-based enumerations

Share considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for SQL Server over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` share property set.

Remote VSS considerations for Hyper-V over SMB configurations

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

General Remote VSS considerations

- A maximum of 64 shares can be configured per Microsoft application server.

  The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.

- Only one active shadow copy set per CIFS server is allowed.

  A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.

- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.
  - In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
  - In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

Remote VSS considerations that apply only for shadow copies with automatic recovery

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation.

  This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine file are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

- Amount of available space on the volume must be adequate.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

- No links or non-regular files are allowed within the directory structure on which Remote VSS creates a

shadow copy.

The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy. The clone process does not support them.

- No NFSv4 ACLs are allowed on directories.

  Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

- A maximum of 60 seconds is allowed to create a shadow copy set.

  Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

ODX copy offload requirements for SQL Server and Hyper-V over SMB

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

- SMB 3.0 must be enabled to use ODX copy offload.
- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

  Secondary compression type is not supported

- To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.

  The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

Recommendations for SQL Server and Hyper-V over SMB configurations

To be sure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

General recommendations

- Separate application server files from general user data.

  If possible, devote an entire storage virtual machine (SVM) and its storage for the application server's data.

- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- For best performance and improved fault tolerance, enable SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as aggregate relocation (ARL) because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use in-guest iSCSI drives when creating clustered virtual machines. Shared `.VHDX` files are not supported for Hyper-V over SMB in ONTAP SMB shares.

Plan the Hyper-V or SQL Server over SMB configuration

Complete the volume configuration worksheet

The worksheet provides an easy way to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all volumes.

- Volume name
- Aggregate name

  You can create volumes on aggregates located on any node in the cluster.

- Size
- Junction path

You should keep the following in mind when creating volumes used to store application server data:

- If the root volume does not have NTFS security style, you must specify the security style as NTFS when you create the volume.

  By default, volumes inherit the security style of the SVM root volume.

- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the Snapshot copy space reserve to `0`.

- The Snapshot policy applied to the volume must be disabled.

  If the SVM Snapshot policy is disabled, then you do not need to specify a Snapshot policy for the volumes. The volumes inherit the Snapshot policy for the SVM. If the Snapshot policy for the SVM is not disabled and is configured to create Snapshot copies, you must specify a Snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage Snapshot copy creation and deletion.

- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named “vol1”, “vol2”, “vol3”, and “vol4”, you can create the namespace shown in the example. You can then create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Types of information	Values
Volume 1: Volume name, aggregate, size, junction path	
Volume 2: Volume name, aggregate, size, junction path	
Volume 3: Volume name, aggregate, size, junction path	
Volume 4: Volume name, aggregate, size, junction path	
Volume 5: Volume name, aggregate, size, junction path	
Volume 6: Volume name, aggregate, size, junction path	

Types of information	Values
Additional volumes: Volume name, aggregate, size, junction path	

Complete the SMB share configuration worksheet

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

Information about SMB shares properties and configuration settings

For each share, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all shares

- Share name
- Path
- Share properties

  You must configure the following two share properties:

  - `oplocks`
  - `continuously-available`

The following share properties must not be set:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`

  With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

  - Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null [""]).

Information about share paths

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on

volumes “vol1”, “vol2”, “vol3”, and “vol4”, you should create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     data1        true     /data1                  RW_volume
vs1     vol1         true     /data1/vol1             RW_volume
vs1     vol2         true     /data1/vol2             RW_volume
vs1     data2        true     /data2                  RW_volume
vs1     vol3         true     /data2/vol3             RW_volume
vs1     vol4         true     /data2/vol4             RW_volume
```

Although you can create shares on the `/data1` and `/data2` paths for administrative management, you must not configure the application servers to use those shares to store data.

Planning worksheet

Types of information	Values
Volume 1: SMB share name and path	
Volume 2: SMB share name and path	
Volume 3: SMB share name and path	
Volume 4: SMB share name and path	
Volume 5: SMB share name and path	
Volume 6: SMB share name and path	
Volume 7: SMB share name and path	
Additional volumes: SMB share names and paths	

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB overview

There are several ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you create the ONTAP configuration for nondisruptive operations with Hyper-V and SQL Server over SMB, the following tasks must be completed:

- Time services must be set up on the cluster.
- Networking must be set up for the SVM.
- The SVM must be created.
- Data LIF interfaces must be configured on the SVM.
- DNS must be configured on the SVM.
- Desired names services must be set up for the SVM.
- The CIFS server must be created.

Related information

Planning the Hyper-V or SQL Server over SMB configuration

Configuration requirements and considerations

Verify that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

About this task

Kerberos authentication is required when making a continuously available share connection. Part of the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the storage virtual machine (SVM).

Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can be used to restrict access based on authentication method.

Export policies for SMB are optional and are disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication are allowed on a CIFS server by default.

- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and NTLMv2 authentication.

Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2 authentication can be disallowed, either using Security Policy settings or Group Policies.

Steps

1. Perform the following to verify that export policies are disabled on the SVM:
   a. Set the privilege level to advanced:

```
set -privilege advanced
```

b. Verify that the `-is-exportpolicy-enabled` CIFS server option is set to `false`:

vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

c. Return to the admin privilege level:

set -privilege admin

2. If export policies for SMB are not disabled, disable them:

vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

   For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTMLv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

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

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

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

Verify that domain accounts map to the default UNIX user

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

When you create a storage virtual machine (SVM), ONTAP automatically creates the default user named “pcuser” (with a UID of `65534`) and the group named “pcuser” (with a GID of `65534`), and adds the default user to the “pcuser” group. If you are configuring a Hyper-V over SMB solution on anSVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server’s default UNIX user.

Steps

1. Determine whether there is a default UNIX user:

   vserver cifs options show -vserver *vserver_name*

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

   vserver services unix-user show -vserver *vserver_name*

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default UNIX user and the default group, and add the default user to the group.

   Generally, the default user is given the user name “pcuser” and must be assigned the UID of `65534`. The default group is generally given the group name “pcuser”. The GID assigned to the group must be `65534`.

   a. Create the default group: + **vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534**

   b. Create the default user and add the default user to the default group: + **vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534**

   c. Verify that the default user and default group are configured correctly: + **vserver services unix-user show -vserver *vserver_name*** + **vserver services unix-group show -vserver *vserver_name* -members**

4. If the CIFS server’s default user is not configured, perform the following:

   a. Configure the default user:

      vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser***

   b. Verify that the default UNIX user is configured correctly:

      vserver cifs options show -vserver *vserver_name*

5. To verify that the application server’s computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the `vserver cifs session show` command.

   For more information about using this command, see the man pages.

Example

The following commands determine that the CIFS server’s default user is not set, but determines that the “pcuser” user and “pcuser” group exist. The “pcuser” user is assigned as the CIFS server’s default user on SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

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



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

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

Verify that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the storage virtual machine (SVM), the security style of the root volume should be set to NTFS.

About this task

- You can specify the root volume security style at the time you create the SVM.
- If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the `volume modify` command.

Steps

1. Determine the current security style of the SVM root volume:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Verify that the SVM root volume is set to NTFS security style:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verify that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

Steps

1. Verify that the required CIFS server options are enabled on the storage virtual machine (SVM):
   a. Set the privilege level to advanced:

      `set -privilege advanced`

   b. Enter the following command:

      `vserver cifs options show -vserver vserver_name`

      The following options should be set to `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Hyper-V only)
2. If any of the options are not set to `true`, perform the following:
   a. Set them to `true` by using the `vserver cifs options modify` command.
   b. Verify that the options are set to `true` by using the `vserver cifs options show` command.
3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements.

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

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

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

Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance for Hyper-V and SQL server over SMB configurations.

What you'll need

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

About this task

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

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

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

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

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

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

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

- **-max-connections-per-session**

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

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

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

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

Steps

1. Set the privilege level to advanced:

   set -privilege advanced

2. Enable SMB Multichannel on the SMB server:

   vserver cifs options modify -vserver *vserver_name* -is-multichannel-enabled true

3. Verify that ONTAP is reporting SMB Multichannel sessions:

   vserver cifs session show options

4. Return to the admin privilege level:

   set -privilege admin

Example

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

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

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

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

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Create NTFS data volumes

You must create NTFS data volumes on the storage virtual machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over SMB application servers. Use the volume configuration worksheet to create your data volumes.

About this task

There are optional parameters that you can use to customize a data volume. For more information about customizing volumes, see the xref:./smb-hyper-v-sql/Logical storage management.

As you create your data volumes, you should not create junction points within a volume that contains the following:

- Hyper-V files for which ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server

If you inadvertently create a volume that uses mixed or UNIX security style, you cannot change the volume to an NTFS security style volume and then directly use it to create continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V and SQL Server over SMB do not work correctly unless the volumes used in the configuration are created as NTFS security-style volumes.You must either delete the volume and re-create the volume with NTFS security style, or you can map the volume on a Windows host and apply an ACL at the top of the volume and propagate the ACL to all files and folders in the volume.

Steps

1. Create the data volume by entering the appropriate command:

If you want to create a volume in an SVM where the root volume security style is…	Enter the command…
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
Not NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. Verify that the volume configuration is correct:

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

Create continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

Steps

1. Display information about the existing data volumes and their junction paths:

   volume show -vserver *vserver_name* -junction

2. Create a continuously available SMB share:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - You can optionally add a comment to the share configuration.
   - By default, the offline files share property is configured on the share and is set to `manual`.

- ONTAP creates the share with the Windows default share permission of `Everyone` / `Full Control`.

3. Repeat the previous step for all shares in the share configuration worksheet.
4. Verify that your configuration is correct by using the `vserver cifs share show` command.
5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the **Windows Properties** window.

Example

The following commands create a continuously available share named “data2” on storage virtual machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the `-symlink` parameter to `""`:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                  Junction
Vserver   Volume     Active   Junction Path    Path Source
--------- ---------- -------- ---------------- ------------
vs1       data       true     /data            RW_volume
vs1       data1      true     /data/data1      RW_volume
vs1       data2      true     /data/data2      RW_volume
vs1       vs1_root   -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                     Vserver: vs1
                       Share: data2
     CIFS Server NetBIOS Name: VS1
                        Path: /data/data2
            Share Properties: oplocks
                              continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Add the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require

privileges not assigned by default to domain users.

What you'll need

The domain account used for installing the SQL Server must already exist.

About this task

When adding the privilege to the SQL Server installer's account, ONTAP might validate the account by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Add the "SeSecurityPrivilege" privilege:

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   The value for the `-user-or-group-name` parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Example

The following command adds the "SeSecurityPrivilege" privilege to the SQL Server installer's account in the EXAMPLE domain for storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configure the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which ONTAP should create shadow copies.

What you'll need

The VSS shadow copy feature must be enabled.

About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to `0`, ONTAP creates shadow copies for all subdirectories.

Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Set the VSS shadow copy directory depth to the desired level:

   ```
   vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth
   integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
   ```

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Manage Hyper-V and SQL Server over SMB configurations

Configure existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the `homedirectory` share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

The following share properties must be configured:

- `continuously-available`
- `oplocks`

The following share properties must not be set. If they are present in the list of current share properties, they

need to be removed from the continuously available share:

- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps

1. Display the current share parameter settings and the current list of configured share properties:

   vserver cifs share show -vserver *vserver_name* -share-name *share_name*

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the `vserver cifs share properties modify` command.

   You can disable symlinks by setting the value of the `-symlink` parameter to `""`.

   - You can disable symlinks by setting the value of the `-symlink` parameter to `""`.
   - You can set the `-offline-files` parameter to the correct setting by specifying `manual`.

3. Add the `continuously-available` share property, and, if needed, the `oplocks` share property:

   vserver cifs share properties add -vserver *vserver_name* -share-name *share_name* -share-properties continuously-available[,oplock]

   If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

   vserver cifs share properties remove -vserver *vserver_name* -share-name *share_name* -share-properties properties[,…]

   You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

   vserver cifs share show -vserver *vserver_name* -share-name *share_name* -fields symlink-properties,offline-files

6. Verify that the list of configured share properties is correct:

   vserver cifs shares properties show -vserver *vserver_name* -share-name share_name

Examples

The following example shows how to configure an existing share named “share1” on storage virtual machine (SVM) vs1 for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the `-symlink` parameter to "".

- The `-offline-file` parameter is modified and set to `manual`.
- The `continuously-available` share property is added to the share.
- The `oplocks` share property is already in the list of share properties; therefore, it does not need to be added.
- The `attributecache` share property is removed from the share.
- The `browsable` share property is optional for a continuously available share used for NDOs with application servers over SMB and is retained as one of the share properties.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Enable or disable VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

About this task

You can enable or disable VSS shadow copies at any time.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want VSS shadow copies to be…	Enter the command…
Enabled	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
Disabled	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following commands enable VSS shadow copies on SVM vs1:

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

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

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

Use statistics to monitor Hyper-V and SQL Server over SMB activity

Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to determine…	Enter…
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show object` *`object_name`*
Which counters are available	`statistics catalog counter show object` *`object_name`*

   See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:

> This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ---------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Display SMB statistics

You can display various SMB statistics to monitor performance and diagnose issues.

Steps

1. Use the `statistics start` and optional `statistics stop` commands to collect a data sample.

   For more information about these commands, see the System Administration Reference.

2. Perform one of the following actions:

If you want to display statistics for…	Enter the following command…
All versions of SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x and SMB 3.0	**`statistics show -object smb2`**
CIFS subsystem of the node	**`statistics show -object nblade_cifs`**

See the man page for more information.

Verify that the configuration is capable of nondisruptive operations

Use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

Alert ID	Severity	Condition
`HaNotReadyCifsNdo_Alert`	Major	One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.

Alert ID	Severity	Condition
NoStandbyLifCifsNdo_Alert	Minor	The storage virtual machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.

Display nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

Steps

1. Monitor health status by performing the appropriate action:

If you want to display…	Enter the command…
The health status of the system, which reflects the overall status of individual health monitors	**system health status show**
Information about the health status of the CIFS-NDO subsystem	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

If you want to display information about…	Enter the command…
The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status	**system health config show -subsystem CIFS-NDO**
The CIFS-NDO alerts that a health monitor can potentially generate	**system health alert definition show -subsystem CIFS-NDO**
CIFS-NDO health monitor policies, which determine when alerts are raised	**system health policy definition show -monitor node-connect**

Use the `-instance` parameter to display detailed information.

Examples

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

The following output shows detailed information about the configuration and status of the health monitor of the CIFS-NDO subsystem:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verify the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to provide seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.

About this task

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

For proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Steps

1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:

   vserver cifs shares show -vserver *vserver_name*

2. Verify that the SMB shares are configured for continuous availability:

   vserver cifs shares properties show -vserver *vserver_name*

Examples

The following example displays the share setting for a share named “share1” on storage virtual machine (SVM, formerly known as Vserver) vs1. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the `Symlink Properties` field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                     Vserver: vs1
                       Share: share1
     CIFS Server NetBIOS Name: VS1
                        Path: /data/share1
            Share Properties: oplocks
                              continuously-available
          Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Verify LIF status

Even if you configure storage virtual machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

About this task

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

Steps

1. Display information about configured LIFs for the SVM:

   network interface show -vserver *vserver_name*

   In this example, “lif1” is not located on the home port.

   ```
   network interface show -vserver vs1
   ```

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2      e0d
   false
               lif2         up/up    10.0.0.129/24    node2      e0d
   true
   ```

2. If some of the LIFs are not on their home ports, perform the following steps:
   a. For each LIF, determine what the LIF’s home port is:

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. For each LIF, determine whether the LIF's home port is up:

network port show -node *node_name* -port *port* -fields port,link

`network port show -node node1 -port e0d -fields port,link`

```
node       port link
---------- ---- ----
node1      e0d  up
```

In this example, "lif1" should be migrated back to its home port, `node1:e0d`.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the `up` state, resolve the problem so that these interfaces are up.
4. If needed, revert the LIFs to their home ports:

network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

5. Verify that each node in the cluster has an active LIF for the SVM:

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determine whether SMB sessions are continuously available

Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you to identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display SMB session information…	Enter the following command…
For all sessions on the SVM in summary form	**vserver cifs session show -vserver *vserver_name***
On a specified connection ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
From a specified workstation IP address	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
On a specified LIF IP address	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
On a specified node	**vserver cifs session show -vserver *vserver_name* -node {node_name|local}**

If you want to display SMB session information…	Enter the following command…
From a specified Windows user	**vserver cifs session show -vserver *vserver_name* -windows -user *user_name*** The format for `user_name` is `[domain]\user`.
With a specified authentication mechanism	**vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism** The value for `-auth-mechanism` can be one of the following: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`
With a specified protocol version	**vserver cifs session show -vserver *vserver_name* -protocol -version protocol_version** The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to `SMB3` or later.

If you want to display SMB session information…	Enter the following command…
With a specified level of continuously available protection	**vserver cifs session show -vserver *vserver_name* -continuously-available *continuously_available_protection_level*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` • `Partial` If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
With a specified SMB signing session status	**vserver cifs session show -vserver *vserver_name* -is -session-signed {true|false}**

Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                  Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can also display information about the continuously available protection level of a file, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously -available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

  You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

  You can use this parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	**vserver cifs session file show -vserver *vserver_name***
On a specified node	**vserver cifs session file show -vserver *vserver_name* -node {node_name|local}**
On a specified file ID	**vserver cifs session file show -vserver *vserver_name* -file-id integer**
On a specified SMB connection ID	**vserver cifs session file show -vserver *vserver_name* -connection-id integer**
On a specified SMB session ID	**vserver cifs session file show -vserver *vserver_name* -session-id integer**
On the specified hosting aggregate	**vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name***
On the specified volume	**vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name***
On the specified SMB share	**vserver cifs session file show -vserver *vserver_name* -share *share_name***
On the specified SMB path	**vserver cifs session file show -vserver *vserver_name* -path *path***

If you want to display open SMB files…	Enter the following command…
With the specified level of continuously available protection	**vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` ⓘ If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	**vserver cifs session file show -vserver *vserver_name* -reconnected *reconnected_state*** The value for `-reconnected` can be one of the following: • `No` • `Yes` ⓘ If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```