



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

ONTAP 9

NetApp
November 14, 2022

Table of Contents

- Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB 1
 - Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB overview 1
 - Verify that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares) 1
 - Verify that domain accounts map to the default UNIX user 3
 - Verify that the security style of the SVM root volume is set to NTFS 5
 - Verify that required CIFS server options are configured 6
 - Configure SMB Multichannel for performance and redundancy 7
 - Create NTFS data volumes 10
 - Create continuously available SMB shares 11
 - Add the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares) 12
 - Configure the VSS shadow copy directory depth (for Hyper-V over SMB shares) 13

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 SMB server must be created.

Related information

[Plan 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 NTLMv2 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::*> vservers cifs options show -vservers vs1 -fields vservers,is-
exportpolicy-enabled

vservers  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 an SVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server’s default UNIX user.

Steps

1. Determine whether there is a default UNIX user:

```
vservers cifs options show -vservers vservers_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:

```
vservers services unix-user show -vservers vservers_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: **+ vservers services unix-group create -vservers**

```
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::> vsriver 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::> vsriver cifs options modify -vsriver vs1 -default-unix-user
pcuser

cluster1::> vsriver 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 -vsriver vsriver_name -fields vsriver,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\
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 | <code>volume create -vserver <i>vserver_name</i> -volume <i>volume_name</i> -aggregate <i>aggregate_name</i> -size integer[KB MB GB TB PB] -junction-path <i>path</i></code> |
| Not NTFS | <code>volume create -vserver <i>vserver_name</i> -volume <i>volume_name</i> -aggregate <i>aggregate_name</i> -size integer[KB MB GB TB PB] -security-style ntfs -junction-path <i>path</i></code> |

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 vs1 -junction
```

2. Create a continuously available SMB share:

```
vs1 cifs share create -vserver vs1 -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 `vs1 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

```

| Vserver | Volume | Active | Junction Path | Junction 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
```


Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.