创建 ONTAP 配置，以便通过 SMB 使用 Hyper-V 和 SQL Server 实现无中断运行

ONTAP 9

NetApp
February 12, 2026

目录

创建 ONTAP 配置，以便通过 SMB 使用 Hyper-V 和 SQL Server 实现无中断运行

使用基于 SMB 的 Hyper-V 和 SQL Server 概述创建 ONTAP 配置以实现无中断运行

您必须执行多个 ONTAP 配置步骤来准备通过 SMB 实现无中断操作的 Hyper-V 和 SQL Server 安装。

在通过 SMB 为 Hyper-V 和 SQL Server 创建无中断操作的 ONTAP 配置之前，必须完成以下任务：

- 必须在集群上设置时间服务。
- 必须为 SVM 设置网络连接。
- 必须创建 SVM 。
- 必须在 SVM 上配置数据 LIF 接口。
- 必须在 SVM 上配置 DNS 。
- 必须为 SVM 设置所需的名称服务。
- 必须创建SMB服务器。

相关信息

规划基于 SMB 的 Hyper-V 或 SQL Server 配置

配置要求和注意事项

验证是否允许 Kerberos 和 NTLMv2 身份验证（基于 SMB 共享的 Hyper-V ）

基于 SMB 的 Hyper-V 无中断运行要求数据 SVM 上的 CIFS 服务器和 Hyper-V 服务器同时允许 Kerberos 和 NTLMv2 身份验证。您必须验证 CIFS 服务器和 Hyper-V 服务器上用于控制允许使用的身份验证方法的设置。

关于此任务

建立持续可用的共享连接时，需要进行 Kerberos 身份验证。远程 VSS 进程的一部分使用 NTLMv2 身份验证。因此，基于 SMB 的 Hyper-V 配置必须支持使用这两种身份验证方法的连接。

必须将以下设置配置为允许 Kerberos 和 NTLMv2 身份验证：

- 必须在 Storage Virtual Machine （ SVM ）上禁用 SMB 的导出策略。

SVM 上始终启用 Kerberos 和 NTLMv2 身份验证，但导出策略可用于根据身份验证方法限制访问。

SMB 的导出策略是可选的，默认情况下处于禁用状态。如果禁用了导出策略，则默认情况下， CIFS 服务器上允许使用 Kerberos 和 NTLMv2 身份验证。

- CIFS 服务器和 Hyper-V 服务器所属的域必须同时允许 Kerberos 和 NTLMv2 身份验证。

默认情况下， Active Directory 域启用 Kerberos 身份验证。但是，可以使用安全策略设置或组策略禁止 NTLMv2 身份验证。

步骤

1. 执行以下操作，验证是否已在 SVM 上禁用导出策略：
   a. 将权限级别设置为高级：

      set -privilege advanced

   b. 验证是否已 `-is-exportpolicy-enabled` CIFS服务器选项设置为 `false`：

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

   c. 返回到管理权限级别：

      set -privilege admin

2. 如果 SMB 的导出策略未禁用，请禁用它们：

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

3. 验证域中是否允许 NTLMv2 和 Kerberos 身份验证。

   有关确定域中允许使用的身份验证方法的信息，请参见 Microsoft TechNet 库。

4. 如果域不允许进行 NTMLv2 身份验证，请使用 Microsoft 文档中所述的方法之一启用 NTLMv2 身份验证。

示例

以下命令验证是否已在 SVM vs1 上禁用 SMB 的导出策略：

```
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
```

验证域帐户是否映射到ONTAP中的默认UNIX用户

Hyper-V 和 SQL Server 使用域帐户创建与持续可用共享的 SMB 连接。要成功创建连接，计算机帐户必须成功映射到 UNIX 用户。为此，最方便的方法是将计算机帐户映射到默认 UNIX 用户。

关于此任务

Hyper-V 和 SQL Server 使用域计算机帐户创建 SMB 连接。此外， SQL Server 还使用域用户帐户作为服务帐户，该帐户还会建立 SMB 连接。

创建存储虚拟机 (SVM) 时，ONTAP 会自动创建名为 `pcuser` （UID 为 `65534`) 和名为 `pcuser` （GID 为 `65534` ），并将默认用户添加到 `pcuser`团体。如果要在将集群升级到 Data ONTAP 8.2 之前存在的 SVM 上配置基于 SMB 解决方案的 Hyper-V ，则默认用户和组可能不存在。否则，必须先创建它们，然后再配置 CIFS 服务器的默认 UNIX 用户。

步骤

1. 确定是否存在默认 UNIX 用户：

```
vserver cifs options show -vserver <vserver_name>
```

2. 如果未设置默认用户选项，请确定是否存在可指定为默认 UNIX 用户的 UNIX 用户：

```
vserver services unix-user show -vserver <vserver_name>
```

3. 如果未设置默认用户选项，并且没有可指定为默认 UNIX 用户的 UNIX 用户，则创建默认组和默认 UNIX 用户，并将默认用户添加到该组。

   通常，默认用户的用户名是“pcuser”，并且必须分配 UID `65534` .默认组一般被赋予组名“pcuser”。分配给组的GID必须为 `65534`。

   a. 创建默认组：

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. 创建默认用户并将默认用户添加到默认组：

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. 验证是否已正确配置默认用户和默认组：

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

4. 如果未配置 CIFS 服务器的默认用户，请执行以下操作：

   a. 配置默认用户：

   ```
   vserver cifs options modify -vserver <vserver_name> -default-unix
   -user pcuser
   ```

   b. 验证是否已正确配置默认 UNIX 用户：

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

5. 要验证应用程序服务器的计算机帐户是否正确映射到默认用户、请将驱动器映射到驻留在SVM上的共享、然后使用确认Windows用户到UNIX用户的映射 `vserver cifs session show` 命令：

   有关的详细信息 `vserver cifs options`，请参见"ONTAP 命令参考"。

示例

。 `pcuser`用户被指定为 SVM vs1 上的 CIFS 服务器的默认用户。

```
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           : -
```

验证 **SVM** 根卷的安全模式是否设置为 **NTFS**

要确保通过 SMB 成功执行 Hyper-V 和 SQL Server 无中断操作，必须使用 NTFS 安全模式创建卷。由于根卷的安全模式默认应用于在 Storage Virtual Machine （ SVM ）上创建的卷，因此根卷的安全模式应设置为 NTFS 。

关于此任务

- 您可以在创建 SVM 时指定根卷的安全模式。
- 如果创建SVM时未将根卷设置为NTFS安全模式、则可以稍后使用更改安全模式 `volume modify` 命令：

步骤

1. 确定 SVM 根卷的当前安全模式：

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

2. 如果根卷不是 NTFS 安全模式卷，请将安全模式更改为 NTFS ：

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

3. 验证 SVM 根卷是否设置为 NTFS 安全模式：

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

示例

以下命令验证 SVM vs1 上的根卷安全模式是否为 NTFS：

```
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
```

验证是否已配置所需的 CIFS 服务器选项

您必须验证是否已根据 Hyper-V 和 SQL Server 通过 SMB 无中断运行的要求启用和配置所需的 CIFS 服务器选项。

关于此任务

- 必须启用 SMB 2.x 和 SMB 3.0 。
- 要使用性能增强型副本卸载，必须启用 ODX 副本卸载。
- 如果基于 SMB 的 Hyper-V 解决方案使用启用了 VSS 的远程备份服务（仅限 Hyper-V ），则必须启用 VSS 卷影复制服务。

步骤

1. 验证是否已在 Storage Virtual Machine （ SVM ）上启用所需的 CIFS 服务器选项：
   a. 将权限级别设置为高级：

      set -privilege advanced

   b. 输入以下命令：

      vserver cifs options show -vserver *vserver_name*

      以下选项应设置为 `true`：

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (仅限Hyper-V)

2. 如果任何选项未设置为 `true`，执行以下操作：
   a. 将其设置为 `true` 使用 `vserver cifs options modify` 命令：
   b. 验证这些选项是否设置为 `true` 使用 `vserver cifs options show` 命令：
3. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下命令验证是否已在 SVM vs1 上启用基于 SMB 的 Hyper-V 配置所需的选项。在此示例中，必须启用 ODX 副本卸载才能满足选项要求。

```
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
```

为 SMB 多通道配置性能和冗余

从 ONTAP 9.4 开始，您可以配置 SMB 多通道，以便在单个 SMB 会话中提供 ONTAP 与客户端之间的多个连接。这样做可以提高 Hyper-V 和 SQL Server 在 SMB 配置上的吞吐量和容错能力。

开始之前

只有在客户端以 SMB 3.0 或更高版本进行协商时，才能使用 SMB 多通道功能。默认情况下， ONTAP SMB 服务器上会启用 SMB 3.0 及更高版本。

关于此任务

如果在 ONTAP 集群上确定了正确的配置，则 SMB 客户端会自动检测并使用多个网络连接。

SMB 会话中同时连接的数量取决于您部署的 NIC：

- 客户端和 ONTAP 集群上的 * 1G NIC *

  客户端为每个 NIC 建立一个连接，并将会话绑定到所有连接。

- 客户端和 ONTAP 集群上的 * 10 G 及更大容量 NIC *

  客户端为每个 NIC 最多建立四个连接，并将会话绑定到所有连接。客户端可以在多个 10G 及更大容量的 NIC 上建立连接。

您还可以修改以下参数（高级权限）：

- `-max-connections-per-session`

  每个多通道会话允许的最大连接数。默认值为 32 个连接。

  如果要启用比默认连接更多的连接，则必须对客户端配置进行类似的调整，该配置的默认连接数也为 32 个。

- `-max-lifs-per-session`

  每个多通道会话公布的最大网络接口数。默认值为 256 个网络接口。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 在 SMB 服务器上启用 SMB 多通道：

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. 验证 ONTAP 是否正在报告 SMB 多通道会话：

```
vserver cifs session show
```

4. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下示例显示了有关所有 SMB 会话的信息，其中显示了单个会话的多个连接：

```
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
```

以下示例显示了有关 session-id 为 1 的 SMB 会话的详细信息：

```
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: -
```

创建 NTFS 数据卷

您必须先在 Storage Virtual Machine （ SVM ）上创建 NTFS 数据卷，然后才能配置持续可用的共享，以便通过 SMB 应用程序服务器与 Hyper-V 或 SQL Server 结合使用。使用卷配置工作表创建数据卷。

关于此任务

您可以使用可选参数自定义数据卷。有关自定义卷的详细信息，请参见 "逻辑存储管理"。

创建数据卷时，不应在包含以下内容的卷中创建接合点：

- ONTAP 为其创建卷影副本的 Hyper-V 文件
- 使用 SQL Server 备份的 SQL Server 数据库文件

> 如果无意中创建了使用混合安全模式或 UNIX 安全模式的卷，则无法将此卷更改为 NTFS 安全模式卷，然后直接使用此卷创建持续可用的共享以实现无中断运行。除非将配置中使用的卷创建为 NTFS 安全模式卷，否则基于 SMB 的 Hyper-V 和 SQL Server 的无中断操作无法正常运行。您必须删除卷并使用 NTFS 安全模式重新创建卷， 或者，您也可以在 Windows 主机上映射卷，并应用卷顶部的 ACL ，然后将 ACL 传播到卷中的所有文件和文件夹。

步骤

1. 输入相应的命令以创建数据卷：

如果要在根卷安全模式为 ... 的 **SVM** 中创建卷	输入命令 ...
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
非 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. 验证卷配置是否正确：

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

创建持续可用的 **SMB** 共享

创建数据卷后，您可以创建持续可用的共享，应用程序服务器可使用这些共享访问 Hyper-V 虚拟机，配置文件和 SQL Server 数据库文件。创建 SMB 共享时，应使用共享配置工作表。

步骤

1. 显示有关现有数据卷及其接合路径的信息：

   volume show -vserver *vserver_name* -junction

2. 创建持续可用的 SMB 共享：

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

   - 您可以选择向共享配置添加注释。
   - 默认情况下、脱机文件共享属性在共享上配置、并设置为 `manual`。
   - ONTAP会使用的Windows默认共享权限创建共享 `Everyone / Full Control`。

3. 对共享配置工作表中的所有共享重复上述步骤。
4. 使用验证您的配置是否正确 `vserver cifs share show` 命令：
5. 通过将驱动器映射到每个共享并使用 * Windows 属性 * 窗口配置文件权限，在持续可用的共享上配置 NTFS 文件权限。

示例

以下命令会在 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上创建名为 `data2` 的持续可用共享。通过设置禁用符号链接 `-symlink` 参数设置为 `""`：

```
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
```

将 SeSecurityPrivilege 权限添加到用户帐户（对于 SMB 共享的 SQL Server ）

必须为用于安装 SQL 服务器的域用户帐户分配 `SeSecurityPrivilege` 特权，才能在 CIFS 服务器上执行某些操作，这些操作需要默认情况下未分配给域用户的权限。

开始之前

用于安装 SQL Server 的域帐户必须已存在。

关于此任务

在将权限添加到 SQL Server 安装程序的帐户时， ONTAP 可能会通过联系域控制器来验证此帐户。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 添加 " SeSecurityPrivilege " 权限：

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

   的值 -user-or-group-name 参数是用于安装SQL Server的域用户帐户的名称。

2. 验证是否已将此权限应用于此帐户：

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

示例

以下命令会将 " SeSecurityPrivilege " 权限添加到 Storage Virtual Machine （ SVM ） vs1 的示例域中的 SQL Server 安装程序帐户：

```
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
```

配置 VSS 卷影复制目录深度（对于基于 SMB 共享的 Hyper-V ）

您也可以在 SMB 共享中配置用于创建卷影副本的目录的最大深度。如果要手动控制 ONTAP 应在其上创建卷影副本的子目录的最大级别，此参数非常有用。

开始之前

必须启用 VSS 卷影复制功能。

关于此任务

默认情况下，最多为五个子目录创建卷影副本。如果此值设置为 0，ONTAP将为所有子目录创建卷影副本。

> 尽管您可以指定卷影副本集目录深度包含五个以上的子目录或所有子目录，但 Microsoft 要求必须在 60 秒内完成卷影副本集创建。如果无法在此时间内完成卷影副本集创建，则会失败。您选择的卷影复制目录深度不能使创建时间发生原因超过时间限制。

步骤

1. 将权限级别设置为高级：

   set -privilege advanced

2. 将 VSS 卷影复制目录深度设置为所需级别：

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

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

3. 返回到管理权限级别：

   set -privilege admin