Erstellen von ONTAP Konfigurationen für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server over SMB

ONTAP 9

NetApp
February 12, 2026

Inhalt

Erstellen von ONTAP Konfigurationen für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server over SMB

ONTAP Konfigurationen für unterbrechungsfreien Betrieb mit Hyper-V und SQL Server über SMB erstellen – Übersicht

ONTAP-Konfigurationsschritte müssen zur Vorbereitung auf Hyper-V und SQL Server ausgeführt werden, um unterbrechungsfreien Betrieb über SMB zu gewährleisten.

Bevor Sie die ONTAP Konfiguration für den unterbrechungsfreien Betrieb mit Hyper-V und SQL Server über SMB erstellen, müssen die folgenden Aufgaben ausgeführt werden:

- Auf dem Cluster müssen Zeitdienste eingerichtet werden.
- Für die SVM muss ein Netzwerk eingerichtet werden.
- Die SVM muss erstellt werden.
- Auf der SVM müssen die Daten-LIF-Schnittstellen konfiguriert sein.
- Für die SVM muss DNS konfiguriert sein.
- Für die SVM müssen Services für gewünschte Namen eingerichtet werden.
- Der SMB-Server muss erstellt werden.

Verwandte Informationen

Planen der Konfiguration von Hyper-V oder SQL Server über SMB

Konfigurationsanforderungen und Überlegungen

Überprüfung, ob sowohl Kerberos als auch NTLMv2-Authentifizierung zulässig sind (Hyper-V über SMB-Freigaben)

Für den unterbrechungsfreien Betrieb von Hyper-V über SMB ist erforderlich, dass der CIFS-Server auf einer Daten-SVM und der Hyper-V Server sowohl Kerberos als auch NTLMv2-Authentifizierung gestatten. Sie müssen die Einstellungen sowohl auf dem CIFS-Server als auch auf den Hyper-V-Servern überprüfen, die steuern, welche Authentifizierungsmethoden zulässig sind.

Über diese Aufgabe

Kerberos-Authentifizierung ist erforderlich, wenn eine kontinuierlich verfügbare Freigabverbindung hergestellt wird. Ein Teil des Remote-VSS-Prozesses verwendet die NTLMv2-Authentifizierung. Daher müssen Verbindungen, die beide Authentifizierungsmethoden verwenden, für Hyper-V über SMB-Konfigurationen unterstützt werden.

Die folgenden Einstellungen müssen so konfiguriert sein, dass sowohl Kerberos- als auch NTLMv2-Authentifizierung zugelassen wird:

- Exportrichtlinien für SMB müssen auf der Storage Virtual Machine (SVM) deaktiviert werden.

Sowohl Kerberos als auch NTLMv2-Authentifizierung sind immer auf SVMs aktiviert. Exportrichtlinien können jedoch verwendet werden, um den Zugriff auf Basis der Authentifizierungsmethode zu beschränken.

Exportrichtlinien für SMB sind optional und werden standardmäßig deaktiviert. Wenn Exportrichtlinien deaktiviert sind, sind sowohl Kerberos als auch NTLMv2-Authentifizierung standardmäßig auf einem CIFS-Server zulässig.

- Die Domäne, zu der der CIFS-Server und Hyper-V-Server gehören, muss sowohl Kerberos als auch NTLMv2-Authentifizierung zulassen.

Kerberos-Authentifizierung ist in Active Directory-Domänen standardmäßig aktiviert. Die NTLMv2-Authentifizierung kann jedoch nicht zulässig sein, entweder unter Verwendung von Sicherheitsrichtlinien oder Gruppenrichtlinien.

Schritte

1. Führen Sie folgende Schritte durch, um zu überprüfen, ob Exportrichtlinien auf der SVM deaktiviert sind:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      set -privilege advanced

   b. Stellen Sie sicher, dass die `-is-exportpolicy-enabled` CIFS-Server-Option auf `false`:

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

   c. Zurück zur Administratorberechtigungsebene:

      set -privilege admin

2. Wenn Exportrichtlinien für SMB nicht deaktiviert sind, deaktivieren Sie diese:

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

3. Überprüfen Sie, ob NTLMv2- und Kerberos-Authentifizierung in der Domäne zulässig sind.

   Informationen darüber, welche Authentifizierungsmethoden in der Domäne zulässig sind, finden Sie in der Microsoft TechNet-Bibliothek.

4. Wenn die Domäne die NTMLv2-Authentifizierung nicht zulässt, aktivieren Sie die NTLMv2-Authentifizierung mithilfe einer der in der Microsoft-Dokumentation beschriebenen Methoden.

Beispiel

Mit den folgenden Befehlen wird sichergestellt, dass Exportrichtlinien für SMB auf SVM vs1 deaktiviert sind:

```
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
```

Überprüfen Sie, ob die Domänenkonten dem standardmäßigen UNIX-Benutzer in ONTAP zugeordnet sind

Hyper-V und SQL Server verwenden Domänenkonten, um SMB-Verbindungen für kontinuierlich verfügbare Freigaben zu erstellen. Um die Verbindung erfolgreich zu erstellen, muss das Computerkonto einem UNIX-Benutzer erfolgreich zugeordnet werden. Der bequemste Weg dies zu erreichen ist, das Computerkonto dem standardmäßigen UNIX-Benutzer zuzuordnen.

Über diese Aufgabe

Hyper-V und SQL Server verwenden die Domänencomputer-Konten, um SMB-Verbindungen zu erstellen. Darüber hinaus verwendet SQL Server ein Domain-Benutzerkonto als Dienstkonto, das auch SMB-Verbindungen erstellt.

Wenn Sie eine Storage Virtual Machine (SVM) erstellen, erstellt ONTAP automatisch den Standardbenutzer mit dem Namen `pcuser` (mit einer UID von `65534`) und die Gruppe namens `pcuser` (mit einer GID von `65534`) und fügt den Standardbenutzer zum `pcuser` Gruppe. Wenn Sie eine Hyper-V über SMB-Lösung auf einer SVM konfigurieren, die vor dem Upgrade des Clusters auf Data ONTAP 8.2 vorhanden war, sind Benutzer und Gruppen möglicherweise nicht vorhanden. Wenn dies nicht der Fall ist, müssen Sie diese erstellen, bevor Sie den UNIX-Standardbenutzer des CIFS-Servers konfigurieren.

Schritte

1. Legen Sie fest, ob ein UNIX-Standardbenutzer vorhanden ist:

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

2. Wenn die Standardbenutzeroption nicht festgelegt ist, legen Sie fest, ob ein UNIX-Benutzer als Standardbenutzer festgelegt werden kann:

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

3. Wenn die Option „Standardbenutzer“ nicht festgelegt ist und kein UNIX-Benutzer vorhanden ist, der als UNIX-Standardbenutzer festgelegt werden kann, erstellen Sie die Standardgruppe und den UNIX-Standardbenutzer und fügen Sie den Standardbenutzer der Gruppe hinzu.
4. Die Standardgruppe erhält im Allgemeinen den Gruppennamen „pcuser“ Die der Gruppe zugewiesene GID muss sein `65534`.
   a. Erstellen Sie die Standardgruppe:

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

   b. Erstellen Sie den Standardbenutzer und fügen Sie den Standardbenutzer der Standardgruppe hinzu:

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

   c. Überprüfen Sie, ob der Standardbenutzer und die Standardgruppe richtig konfiguriert sind:

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

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

5. Wenn der Standardbenutzer des CIFS-Servers nicht konfiguriert ist, führen Sie Folgendes aus:
   a. Konfigurieren Sie den Standardbenutzer:

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

   b. Vergewissern Sie sich, dass der UNIX-Standardbenutzer richtig konfiguriert ist:

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

6. Um zu überprüfen, ob das Computerkonto des Anwendungsservers dem Standardbenutzer ordnungsgemäß zugeordnet ist, ordnen Sie ein Laufwerk einer auf der SVM befindlichen Freigabe zu, und bestätigen Sie die Windows-Benutzer-UNIX-Benutzerzuordnung mit dem `vserver cifs session show` Befehl.

   Erfahren Sie mehr über `vserver cifs options` in der "ONTAP-Befehlsreferenz".

Beispiel

Die folgenden Befehle stellen fest, dass der Standardbenutzer des CIFS-Servers nicht festgelegt ist, stellen aber fest, dass der `pcuser` Benutzer und `pcuser` Gruppe existiert. Die `pcuser` Der Benutzer wird als

Standardbenutzer des CIFS-Servers auf SVM vs1 zugewiesen.

```
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            : -
```

Überprüfen Sie, ob der Sicherheitstil des SVM-Root-Volumes auf NTFS festgelegt ist

Um sicherzustellen, dass der unterbrechungsfreie Betrieb für Hyper-V und SQL Server über SMB erfolgreich ist, müssen Volumes mit NTFS-Sicherheitsstil erstellt werden. Da der Sicherheitsstil des Root-Volumes standardmäßig auf Volumes angewendet wird, die auf der SVM (Storage Virtual Machine) erstellt wurden, sollte der Sicherheitstyp des Root-Volumes auf NTFS festgelegt werden.

Über diese Aufgabe

- Sie können beim Erstellen der SVM den Sicherheitsstil für das Root-Volume festlegen.
- Wenn die SVM nicht erstellt wird und das Root-Volume nicht auf den NTFS-Sicherheitsstil eingestellt ist, können Sie den Sicherheitsstil später mithilfe des `volume modify` Befehls ändern.

Schritte

1. Legen Sie den aktuellen Sicherheitsstil des SVM Root Volume fest:

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

2. Wenn das Root-Volume kein NTFS-Sicherheitsstil-Volume ist, ändern Sie den Sicherheitsstil in NTFS:

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

3. Überprüfen Sie, ob das SVM-Root-Volume auf den NTFS-Sicherheitsstil eingestellt ist:

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

Beispiel

Mit den folgenden Befehlen wird sichergestellt, dass der Sicherheitsstil des Root-Volumes NTFS auf SVM vs1 lautet:

```
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
```

Vergewissern Sie sich, dass die erforderlichen CIFS-Serveroptionen konfiguriert sind

Sie müssen überprüfen, ob die erforderlichen CIFS-Serveroptionen aktiviert und gemäß den Anforderungen für unterbrechungsfreien Betrieb von Hyper-V und SQL Server über SMB konfiguriert sind.

Über diese Aufgabe

- SMB 2.x und SMB 3.0 müssen aktiviert sein.
- ODX Copy-Offload muss aktiviert sein, um eine Performance-fördernde Copy-Offload zu nutzen.
- VSS Shadow Copy Services müssen aktiviert sein, wenn die Hyper-V-over-SMB-Lösung Remote VSS-fähige Backup-Services verwendet (nur Hyper-V).

Schritte

1. Vergewissern Sie sich, dass die erforderlichen CIFS-Serveroptionen auf der SVM (Storage Virtual Machine) aktiviert sind:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Geben Sie den folgenden Befehl ein:

      `vserver cifs options show -vserver *vserver_name*`

      Die folgenden Optionen sollten auf eingestellt werden `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Nur Hyper-V)
2. Wenn eine der Optionen nicht auf eingestellt `true` ist, führen Sie die folgenden Schritte aus:

a. Setzen Sie sie `true` mit dem `vserver cifs options modify` Befehl auf.

b. Überprüfen Sie `true` mit dem `vserver cifs options show` Befehl, ob die Optionen auf festgelegt sind.

3. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Mit den folgenden Befehlen wird überprüft, ob die erforderlichen Optionen für die Hyper-V über SMB-Konfiguration auf SVM vs1 aktiviert sind. In diesem Beispiel muss eine ODX Copy-Offload-Funktion aktiviert werden, um die Optionsanforderungen zu erfüllen.

```
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
```

Konfigurieren Sie SMB Multichannel für Performance und Redundanz

Ab ONTAP 9.4 können Sie SMB Multichannel so konfigurieren, dass in einer einzigen SMB-Session mehrere Verbindungen zwischen ONTAP und Clients hergestellt werden können. Dadurch werden Durchsatz und Fehlertoleranz für Hyper-V und SQL Server über SMB-Konfigurationen verbessert.

Bevor Sie beginnen

Sie können die SMB-Multichannel-Funktionen nur verwenden, wenn Clients mit SMB 3.0 oder höheren Versionen verhandeln. SMB 3.0 und höher ist auf dem ONTAP SMB-Server standardmäßig aktiviert.

Über diese Aufgabe

SMB-Clients erkennen automatisch mehrere Netzwerkverbindungen, wenn eine ordnungsgemäße Konfiguration auf dem ONTAP Cluster identifiziert wird.

Die Anzahl der gleichzeitigen Verbindungen in einer SMB-Sitzung hängt von den bereitgestellten NICs ab:

- **1G NICs auf Client und ONTAP Cluster**

  Der Client stellt eine Verbindung pro NIC her und bindet die Sitzung an alle Verbindungen.

- **10G und mehr Kapazität NICs auf Client und ONTAP Cluster**

  Der Client stellt bis zu vier Verbindungen pro NIC her und bindet die Sitzung an alle Verbindungen. Der Client kann Verbindungen auf mehreren 10G und NICs mit höherer Kapazität einrichten.

Sie können auch die folgenden Parameter (erweiterte Berechtigung) ändern:

- `-max-connections-per-session`

  Die maximal zulässige Anzahl von Verbindungen pro Multichannel-Sitzung. Die Standardeinstellung ist 32 Verbindungen.

  Wenn Sie mehr Verbindungen als die Standardverbindung aktivieren möchten, müssen Sie vergleichbare Anpassungen an der Client-Konfiguration vornehmen, die auch über 32 Standardverbindungen verfügt.

- `-max-lifs-per-session`

  Die maximale Anzahl der pro Multichannel-Sitzung angekündigten Netzwerkschnittstellen. Die Standardeinstellung ist 256 Netzwerkschnittstellen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. SMB-Multichannel auf dem SMB-Server aktivieren:

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

3. Vergewissern Sie sich, dass ONTAP Berichte über SMB-Multichannel-Sitzungen erstellt:

```
vserver cifs session show
```

4. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Beispiel

Im folgenden Beispiel werden Informationen zu allen SMB-Sitzungen angezeigt und mehrere Verbindungen für eine einzelne Sitzung angezeigt:

```
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
```

Im folgenden Beispiel werden ausführliche Informationen über eine SMB-Sitzung mit Session-id 1 angezeigt:

```
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: -
```

NTFS-Daten-Volumes erstellen

Sie müssen NTFS-Daten-Volumes auf der Storage Virtual Machine (SVM) erstellen, bevor Sie kontinuierlich verfügbare Shares für die Verwendung mit Hyper-V oder SQL Server über SMB Applikationsserver konfigurieren können. Erstellen Sie Ihre Daten-Volumes mithilfe des Arbeitsblatts zur Volume-Konfiguration.

Über diese Aufgabe

Sie können optionale Parameter zum Anpassen eines Daten-Volumes verwenden. Weitere Informationen zum Anpassen von Volumes finden Sie im "Logisches Storage-Management".

Bei der Erstellung von Daten-Volumes sollten keine Verbindungspunkte innerhalb eines Volumes erstellt werden, die die folgenden Elemente enthalten:

- Hyper-V Dateien, bei denen ONTAP Schattenkopien erstellt
- SQL Server Datenbankdateien, die mit SQL Server gesichert werden

Wenn Sie versehentlich ein Volume erstellen, das gemischten oder UNIX Sicherheitsstil nutzt, können Sie das Volume nicht auf ein NTFS-Sicherheitsformat ändern und dann direkt verwenden, um kontinuierlich verfügbare Shares für den unterbrechungsfreien Betrieb zu erstellen. Unterbrechungsfreier Betrieb von Hyper-V und SQL Server über SMB funktioniert nicht ordnungsgemäß, es sei denn, die in der Konfiguration verwendeten Volumes werden als NTFS SicherheitsVolumes erstellt. Sie müssen entweder das Volume löschen und das Volume mit NTFS-Sicherheitsstil neu erstellen. Sie können das Volume auch auf einem Windows-Host zuordnen und eine ACL oben auf dem Volume anwenden sowie die ACL auf alle Dateien und Ordner im Volume übertragen.

Schritte

1. Erstellen Sie das Daten-Volume mit dem entsprechenden Befehl:

Wenn Sie ein Volume in einer SVM erstellen möchten, wo sich der Sicherheitsstil für das Root-Volume befindet…	Geben Sie den Befehl ein…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Nicht 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. Vergewissern Sie sich, dass die Volume-Konfiguration korrekt ist:

   `volume show -vserver vserver_name -volume volume_name`

Kontinuierlich verfügbare SMB-Freigaben erstellen

Nach der Erstellung Ihrer Daten-Volumes können Sie die kontinuierlich verfügbaren Freigaben erstellen, die von den Applikationsservern für den Zugriff auf Hyper-V Virtual Machine-, Konfigurations- und SQL Server-Datenbankdateien verwendet werden. Beim Erstellen der SMB-Freigaben sollten Sie das Konfigurationsarbeitsblatt für die Freigabe verwenden.

Schritte

1. Informationen zu den vorhandenen Daten-Volumes und ihren Verbindungspfaden anzeigen:

   `volume show -vserver vserver_name -junction`

2. Kontinuierlich verfügbare SMB-Freigabe erstellen:

   `vserver cifs share create -vserver vserver_name -share-name share_name -path`

***path* -share-properties oplocks,continuously-available -symlink "" [-comment text]**

- Optional können Sie der Share-Konfiguration einen Kommentar hinzufügen.
- Standardmäßig ist die Eigenschaft Offline Files Share auf der Freigabe konfiguriert und auf festgelegt `manual`.
- ONTAP erstellt die Freigabe mit der Windows-Standardfreigabeberechtigung von `Everyone` / `Full Control`.

3. Wiederholen Sie den vorherigen Schritt für alle Freigaben im Arbeitsblatt zur Freigabe-Konfiguration.
4. Überprüfen Sie mit dem `vserver cifs share show` Befehl, ob Ihre Konfiguration korrekt ist.
5. Konfigurieren Sie NTFS-Dateiberechtigungen auf den kontinuierlich verfügbaren Freigaben, indem Sie jedem Share ein Laufwerk zuordnen und Dateiberechtigungen über das Fenster **Windows-Eigenschaften** konfigurieren.

Beispiel

Mit den folgenden Befehlen wird eine kontinuierlich verfügbare Freigabe namens „`data2`“ auf der Storage Virtual Machine (SVM, ehemals Vserver genannt) vs1 erstellt. Symlinks werden deaktiviert, indem der `-symlink` Parameter auf `""`folgende Einstellung gesetzt wird:

```
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
```

Fügen Sie dem Benutzerkonto die Berechtigung „SeSecurityPrivilege“ hinzu (für SQL Server von SMB-Freigaben)

Das Domänenbenutzerkonto, das für die Installation des SQL-Servers verwendet wird, muss der Berechtigung `SeSecurityPrivilege` zugewiesen werden, um bestimmte Aktionen auf dem CIFS-Server auszuführen, die Berechtigungen erfordern, die den Domänenbenutzern standardmäßig nicht zugewiesen sind.

Bevor Sie beginnen

Das für die Installation des SQL Servers verwendete Domänenkonto muss bereits vorhanden sein.

Über diese Aufgabe

Wenn Sie dem SQL Server-Installer-Konto die Berechtigung hinzufügen, überprüft ONTAP möglicherweise das Konto, indem Sie sich an den Domain-Controller wenden. Der Befehl schlägt möglicherweise fehl, wenn

ONTAP den Domain-Controller nicht kontaktieren kann.

Schritte

1. Fügen Sie die Berechtigung `SeSecurityPrivilege` hinzu:

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

   Der Wert für den `-user-or-group-name` Parameter ist der Name des Domänenbenutzerkontos, das für die Installation des SQL Servers verwendet wird.

2. Überprüfen Sie, ob die Berechtigung auf das Konto angewendet wird:

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

Beispiel

Mit dem folgenden Befehl wird das SQL Server-Installationsprogramm in der BEISPIELDOMÄNE für Storage Virtual Machine (SVM) vs1 mit der Berechtigung `SeSecurityPrivilege` ausgestattet:

```
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
```

Verzeichnistiefe der VSS-Schattenkopie konfigurieren (für Hyper-V über SMB-Freigaben)

Optional können Sie die maximale Tiefe von Verzeichnissen in SMB-Freigaben konfigurieren, auf denen Schattenkopien erstellt werden sollen. Dieser Parameter ist nützlich, wenn Sie manuell die maximale Ebene von Unterverzeichnissen steuern möchten, auf denen ONTAP Schattenkopien erstellen soll.

Bevor Sie beginnen

Die Funktion „VSS Shadow Copy“ muss aktiviert sein.

Über diese Aufgabe

Standardmäßig werden Schattenkopien für maximal fünf Unterverzeichnisse erstellt. Wenn der Wert auf gesetzt `0` ist, erstellt ONTAP Schattenkopien für alle Unterverzeichnisse.

Obwohl Sie angeben können, dass die Verzeichnistiefe des Schattenkopiefests mehr als fünf Unterverzeichnisse oder alle Unterverzeichnisse enthält, muss die Erstellung von Schattenkopien innerhalb von 60 Sekunden abgeschlossen sein. Die Erzeugung des SchattenkopieSatzes schlägt fehl, wenn dieser nicht innerhalb dieser Zeit abgeschlossen werden kann. Die von Ihnen gewählte Tiefe des Schattenkopien-Verzeichnisses darf nicht dazu führen, dass die Erstellungszeit die Zeitgrenze überschreitet.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   set -privilege advanced

2. Legen Sie die Verzeichnistiefe der VSS-Schattenkopie auf die gewünschte Ebene fest:

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

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

3. Zurück zur Administratorberechtigungsebene:

   set -privilege admin