SMB-Konfiguration für Microsoft Hyper-V und SQL Server

ONTAP 9

NetApp
January 08, 2026

Inhalt

SMB-Konfiguration für Microsoft Hyper-V und SQL Server

SMB-Konfiguration für Microsoft Hyper-V und SQL Server – Überblick

Die ONTAP Funktionen ermöglichen den unterbrechungsfreien Betrieb für zwei Microsoft Applikationen über das SMB-Protokoll – Microsoft Hyper-V und Microsoft SQL Server.

Wenn Sie unter den folgenden Umständen einen unterbrechungsfreien SMB-Betrieb implementieren möchten, sollten Sie diese Verfahren verwenden:

- Der grundlegende Zugriff auf die Datei des SMB-Protokolls wurde konfiguriert.
- Sie möchten SMB 3.0 oder höher File Shares in SVMs aktivieren, um die folgenden Objekte zu speichern:
  - Hyper-V Dateien für Virtual Machines
  - SQL Server Systemdatenbanken

Verwandte Informationen

Weitere Informationen zur ONTAP Technologie und zur Interaktion mit externen Services finden Sie in den folgenden technischen Berichten (TRs): "Technischer Bericht 4172 von NetApp: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices" "Technischer Bericht 4369 von NetApp: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP"

Konfigurieren Sie ONTAP für Microsoft Hyper-V und SQL Server über SMB-Lösungen

Es können kontinuierlich verfügbare SMB 3.0- und höher-Dateifreigaben verwendet werden, um Hyper-V Virtual Machine-Dateien oder SQL Server-Systemdatenbanken und Benutzerdatenbanken auf Volumes in SVMs zu speichern. Gleichzeitig sind bei geplanten und auch ungeplanten Ereignissen ein unterbrechungsfreier Betrieb möglich.

Microsoft Hyper-V über SMB

Zur Erstellung einer Hyper-V over SMB-Lösung müssen Sie ONTAP zuerst konfigurieren, um Storage Services für Microsoft Hyper-V Server bereitzustellen. Sie müssen außerdem Microsoft Cluster (bei Verwendung einer geclusterten Konfiguration), Hyper-V Server, kontinuierlich verfügbare SMB 3.0-Verbindungen zu den Freigaben konfigurieren, die vom CIFS-Server gehostet werden, und optional auch Backup-Services zum Schutz der auf SVM Volumes gespeicherten Virtual Machine-Dateien.

> Die Hyper-V Server müssen auf Windows 2012 Server oder höher konfiguriert sein. Es werden sowohl Standalone- als auch Clustered Hyper-V-Serverkonfigurationen unterstützt.

- Informationen zum Erstellen von Microsoft-Clustern und Hyper-V-Servern finden Sie auf der Microsoft-Website.
- SnapManager für Hyper-V ist eine Host-basierte Applikation zur Vereinfachung schneller Snapshot-basierter Backup-Services. Die Applikation wurde zur Integration in Hyper-V über SMB-Konfigurationen

entwickelt.

Informationen zur Verwendung von SnapManager mit Hyper-V über SMB-Konfigurationen finden Sie unter *SnapManager for Hyper-V Installation and Administration Guide*.

Microsoft SQL Server über SMB

Um eine SQL Server-over-SMB-Lösung zu erstellen, müssen Sie ONTAP zuerst konfigurieren, um Storage-Services für die Microsoft SQL Server Applikation bereitzustellen. Außerdem müssen Sie auch Microsoft Cluster konfigurieren (bei Verwendung einer Cluster-Konfiguration). Anschließend sollten Sie SQL Server auf den Windows-Servern installieren und konfigurieren und kontinuierlich verfügbare SMB 3.0-Verbindungen zu den vom CIFS-Server gehosteten Freigaben erstellen. Sie können optional Backup-Services konfigurieren, um die Datenbankdateien zu schützen, die auf SVM-Volumes gespeichert sind.

SQL Server muss auf Windows 2012 Server oder höher installiert und konfiguriert sein. Es werden sowohl Standalone- als auch Clustered-Konfigurationen unterstützt.

- Informationen zum Erstellen von Microsoft-Clustern sowie zum Installieren und Konfigurieren von SQL Server finden Sie auf der Microsoft-Website.
- Das SnapCenter Plug-in für Microsoft SQL Server ist eine Host-basierte Applikation zur Vereinfachung schneller Snapshot-basierter Backup-Services. Die Lösung wurde zur Integration in SQL Server über SMB Konfigurationen entwickelt.

  Informationen zur Verwendung des SnapCenter-Plug-ins für Microsoft SQL Server finden Sie im "SnapCenter Plug-in für Microsoft SQL Server" Dokument.

Unterbrechungsfreier Betrieb für Hyper-V und SQL Server über SMB

Die Vorteile von unterbrechungsfreiem Betrieb für Hyper-V und SQL Server over SMB

Unterbrechungsfreier Betrieb von Hyper-V und SQL Server über SMB bezieht sich auf die Kombination von Funktionen, mit denen die Applikationsserver und die enthaltenen Virtual Machines oder Datenbanken online bleiben können. Somit wird während vieler administrativer Aufgaben die kontinuierliche Verfügbarkeit sichergestellt. Hierzu zählen sowohl geplante als auch ungeplante Ausfallzeiten der Storage-Infrastruktur.

Zu den unterstützten unterbrechungsfreien Abläufen für Applikations-Server über SMB gehören:

- Geplante Übernahme und Rückgabe
- Ungeplante Übernahme
- Upgrade
- Geplante Aggregatverschiebung (ARL)
- LIF-Migration und Failover
- Geplante Volume-Verschiebung

Protokolle, die einen unterbrechungsfreien Betrieb über SMB ermöglichen

Neben der Einführung von SMB 3.0 hat Microsoft neue Protokolle veröffentlicht, die alle nötigen Funktionen zur Unterstützung des unterbrechungsfreien Betriebs von Hyper-V und SQL Server over SMB bieten.

ONTAP verwendet diese Protokolle für den unterbrechungsfreien Betrieb von Applikations-Servern über SMB:

- SMB 3,0
- Zeuge

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server over SMB

Es gibt bestimmte Konzepte zum unterbrechungsfreien Betrieb (NDOS), die Sie verstehen sollten, bevor Sie Ihre Hyper-V oder SQL Server over SMB-Lösung konfigurieren.

- **Kontinuierlich verfügbarer Share**

  Ein SMB 3.0-Share mit kontinuierlich verfügbarer Share-Eigenschaft. Kunden, die sich über kontinuierlich verfügbare Shares verbinden, können störenden Ereignissen wie Takeover, Giveback und Aggregatverschiebung standhalten.

- **Knoten**

  Ein einziger Controller, der Mitglied eines Clusters ist. Um zwischen den beiden Knoten in einem SFO-Paar zu unterscheiden, wird ein Node manchmal als „*local Node*“ bezeichnet, und der andere Node wird manchmal „*Partner Node*“ oder „*Remote Node*“ genannt. Der primäre Eigentümer des Storage ist der lokale Knoten. Der sekundäre Besitzer, der bei einem Ausfall des primären Eigentümers die Kontrolle über den Storage übernimmt, ist der Partner-Node. Jeder Node ist der primäre Storage-Eigentümer und sekundärer Eigentümer für Storage-Lösungen seiner Partner.

- **Unterbrechungsfreie Aggregatverschiebung**

  Die Möglichkeit, ein Aggregat zwischen Partner-Nodes innerhalb eines SFO-Paars in einem Cluster zu verschieben, ohne Client-Applikationen zu unterbrechen.

- * Unterbrechungsfreier Failover*

  Siehe *Übernahme*.

- **Unterbrechungsfreie LIF-Migration**

  Die Möglichkeit zur Durchführung einer LIF-Migration, ohne dass Client-Applikationen unterbrochen werden, die über diese LIF mit dem Cluster verbunden sind. Bei SMB-Verbindungen ist dies nur für Clients möglich, die eine Verbindung mit SMB 2.0 oder höher herstellen.

- **Unterbrechungsfreier Betrieb**

  Durchführung umfangreicher ONTAP-Management- und Upgrade-Vorgänge sowie die Möglichkeit, Node-Ausfälle ohne Unterbrechung von Client-Applikationen zu bewältigen. Dieser Begriff bezieht sich auf die Sammlung von Funktionen für die unterbrechungsfreie Übernahme, unterbrechungsfreie Upgrades und die

unterbrechungsfreie Migration insgesamt.

- * Unterbrechungsfreies Upgrade*

  Upgrade von Node-Hardware oder -Software ohne Applikationsunterbrechung

- **Unterbrechungsfreie Volume-Verschiebung**

  Volume kann frei im gesamten Cluster verschoben werden, ohne dass dazu Applikationen unterbrochen werden, die das Volume verwenden. Bei SMB-Verbindungen unterstützen alle SMB-Versionen unterbrechungsfreie Verschiebung von Volumes.

- * Persistente Griffe*

  Eine Eigenschaft von SMB 3.0, die kontinuierlich verfügbare Verbindungen ermöglicht, um bei einer Unterbrechung transparent eine Verbindung zum CIFS-Server herzustellen. Ähnlich wie bei langlebigen Griffen werden vom CIFS-Server persistente Griffe über einen Zeitraum gewartet, nachdem die Kommunikation mit dem verbundenen Client verloren gegangen ist. Die persistenten Griffe sind jedoch widerstandsfähiger als die langlebigen Griffe. Der CIFS-Server bietet dem Kunden nicht nur die Möglichkeit, den Griff nach der erneuten Verbindung innerhalb eines 60-sekündigen Fensters zurückzufordern, sondern verweigert auch den Zugriff auf alle anderen Clients, die während dieses 60-Sekunden-Fensters Zugriff auf die Datei anfordern.

  Informationen zu persistenten Griffen werden auf dem persistenten Storage des SFO-Partners gespiegelt, wodurch Clients mit getrennten persistenten Griffen die langlebigen Griffe zurückgewinnen können, nachdem ein Ereignis, bei dem der SFO-Partner die Verantwortung für den Storage des Nodes übernimmt, übernommen hat. Neben dem unterbrechungsfreien Betrieb für Vorgänge bei LIF-Verschiebungen (die dauerhafte Unterstützung bieten) sorgen persistente Griffe für unterbrechungsfreien Betrieb bei Takeover, Giveback und Aggregatverschiebung.

- **SFO-Rückübertragung**

  Die Aggregate werden an den eigenen Standorten zurückgegeben, wenn eine Wiederherstellung nach einem Takeover-Ereignis durchgeführt wird.

- **SFO-Paar**

  Ein Node-Paar, dessen Controller so konfiguriert sind, dass er Daten füreinander bereitstellt, wenn einer der beiden Nodes nicht mehr funktioniert. Je nach Systemmodell können beide Controller sich in einem einzelnen Chassis befinden oder sich die Controller in einem separaten Chassis befinden. Bekannt als HA-Paar in einem Cluster mit zwei Nodes.

- **Übernahme**

  Der Prozess, durch den der Partner die Kontrolle über den Storage übernimmt, wenn der primäre Eigentümer dieses Speichers ausfällt. Im Zusammenhang mit SFO sind Failover und Takeover gleichbedeutend.

Funktionsweise von SMB 3.0 unterstützt unterbrechungsfreien Betrieb über SMB-Freigaben

SMB 3.0 bietet entscheidende Funktionen, die einen unterbrechungsfreien Betrieb für Hyper-V und SQL Server über SMB-Freigaben ermöglichen. Dazu gehören die `continuously-available` Share-Eigenschaft und ein Typ von Datei-Handle, bekannt

als *persistent Handle*, mit dem SMB-Clients den offenen Dateistatus zurückfordern und SMB-Verbindungen transparent wiederherstellen können.

Persistente Handles können SMB 3.0-fähigen Clients zugewiesen werden, die eine Verbindung zu einem Share mit der kontinuierlich verfügbaren Share-Eigenschaft herstellen. Wenn die SMB-Sitzung getrennt wird, speichert der CIFS-Server Informationen über den Status eines persistenten Handle. Der CIFS-Server blockiert andere Client-Anforderungen während der 60-Sekunden-Periode, in der der Client wieder verbunden werden darf. Dadurch kann der Client mit dem persistenten Griff nach einer Netzwerkverbindung das Handle zurückfordern. Clients mit persistenten Griffen können die Verbindung mithilfe einer der Daten-LIFs auf der Storage Virtual Machine (SVM) wiederherstellen, indem sie entweder eine erneute Verbindung über dieselbe LIF oder über andere LIF herstellen.

Aggregatverschiebung, -Übernahme und -Rückgabe werden allesamt zwischen SFO-Paaren durchgeführt. Um die Trennung und erneute Verbindung von Sitzungen mit Dateien, die permanente Handles haben, nahtlos zu verwalten, behält der Partner-Knoten eine Kopie aller persistenten Informationen zur Sperre bei. Unabhängig davon, ob das Ereignis geplant oder ungeplant ist, kann der SFO-Partner die Persistent-Handle-Verbindung unterbrechungsfrei managen. Mit dieser neuen Funktion können SMB 3.0-Verbindungen zum CIFS-Server bei klassischen Unterbrechungen transparent und unterbrechungsfrei ein Failover auf eine andere Daten-LIF ausführen, die der SVM zugewiesen ist.

Durch die Verwendung persistenter Handles kann der CIFS-Server ein transparentes Failover von SMB 3.0-Verbindungen durchführen. Wenn ein Ausfall dazu führt, dass die Hyper-V-Applikation ein Failover auf einen anderen Knoten im Windows Server-Cluster durchführt, kann der Client die Dateihandles dieser getrennten Griffe nicht zurückfordern. In diesem Szenario können Datei-Handles im getrennten Status den Zugriff auf die Hyper-V Applikation potenziell blockieren, wenn sie auf einem anderen Node neu gestartet wird. „`Failover Clustering`“ ist ein Bestandteil von SMB 3.0, der dieses Szenario durch die Bereitstellung eines Mechanismus zum ungültig erklären veralteter, konfliktverursachter Griffe behebt. Über diesen Mechanismus kann ein Hyper-V Cluster im Falle eines Hyper-V Cluster Nodes rasch wiederhergestellt werden.

Wie das Witness-Protokoll den transparenten Failover verbessert

Das Witness-Protokoll bietet erweiterte Client-Failover-Funktionen für kontinuierlich verfügbare SMB 3.0-Freigaben (CA-Freigaben). Witness beschleunigt den Failover, da das LIF Failover Recovery-Zeitraum umgehen. Der Applikationsserver wird benachrichtigt, wenn ein Node nicht verfügbar ist, ohne dass die SMB 3.0-Verbindung unterbrochen werden muss.

Der Failover erfolgt nahtlos, wobei die Applikationen auf dem Client nicht bemerken, dass ein Failover aufgetreten ist. Wenn Witness nicht verfügbar ist, werden Failover-Vorgänge weiterhin erfolgreich ausgeführt, das Failover ohne Witness ist jedoch weniger effizient.

Wenn die folgenden Anforderungen erfüllt sind, ist ein erweiterter Failover möglich:

- Sie kann nur mit SMB 3.0-fähigen CIFS-Servern verwendet werden, auf denen SMB 3.0 aktiviert ist.
- Die Shares müssen SMB 3.0 mit der Eigenschaft „Continuous Availability Share“ verwenden.
- Der SFO-Partner des Nodes, an den die Applikationsserver angeschlossen sind, muss mindestens eine logische Schnittstelle der betriebsbereiten Daten besitzen, die der Storage Virtual Machine (SVM) zugewiesen ist, die die Daten der Applikationsserver hostet.

Das Witness-Protokoll wird zwischen SFO-Paaren ausgeführt. Da LIFs zu jedem Node im Cluster migriert werden können, muss möglicherweise jeder Node für seinen SFO Partner als Zeugen dienen. Das Witness-Protokoll ermöglicht keinen schnellen Failover von SMB-Verbindungen auf einem bestimmten Node, wenn für die SVM, die Daten für die Applikationsserver hostet, keine aktive Daten-LIF auf dem Partner-Node vorhanden ist. Daher muss jeder Node im Cluster mindestens eine Daten-LIF pro SVM, die eine dieser Konfigurationen hostet, aufweisen.

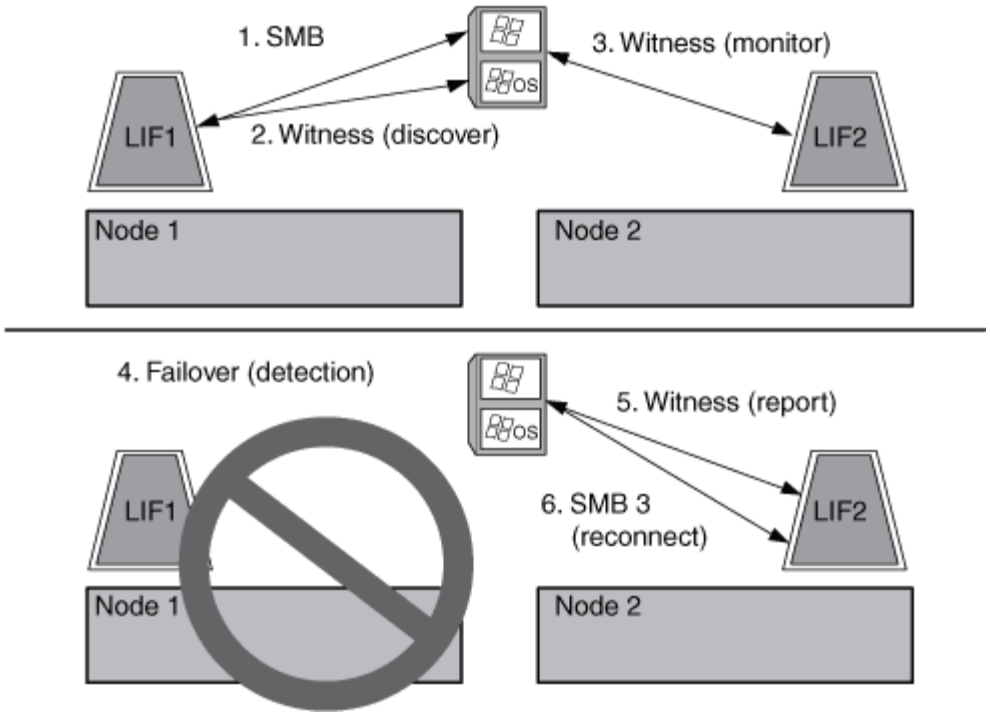
- Die Applikations-Server müssen eine Verbindung zum CIFS-Server herstellen. Dazu wird der CIFS-Servername verwendet, der in DNS gespeichert ist, nicht durch die Verwendung individueller LIF IP-Adressen.

Funktionsweise des Zeugenprotokolls

ONTAP implementiert das Witness-Protokoll mithilfe von SFO-Partner eines Node als Witness. Bei einem Ausfall erkennt der Partner den Ausfall schnell und benachrichtigt den SMB Client.

Das Witness-Protokoll bietet mithilfe des folgenden Verfahrens einen verbesserten Failover:

1. Wenn der Applikations-Server eine kontinuierlich verfügbare SMB-Verbindung zu Node1 herstellt, informiert der CIFS-Server den Applikationsserver darüber, dass Witness verfügbar ist.
2. Der Anwendungsserver fordert die IP-Adressen des Witness-Servers von Node1 an und erhält eine Liste von Node2 (dem SFO-Partner) Daten-LIF-IP-Adressen, die der Storage Virtual Machine (SVM) zugewiesen sind.
3. Der Anwendungsserver wählt eine der IP-Adressen aus, erstellt eine Witness-Verbindung zu Node2 und meldet sich an, benachrichtigt zu werden, wenn die ständig verfügbare Verbindung auf Node1 verschoben werden muss.
4. Wenn auf Node1 ein Failover-Ereignis eintritt, erleichtert Witness Failover-Ereignisse, ist jedoch nicht an der Rückgabe beteiligt.
5. Witness erkennt das Failover-Ereignis und benachrichtigt den Applikationsserver über die Witness Verbindung, dass die SMB-Verbindung zu Node2 verschoben werden muss.
6. Der Anwendungsserver verschiebt die SMB-Sitzung auf Node2 und stellt die Verbindung ohne Unterbrechung des Client-Zugriffs wieder her.



Share-basierte Backups mit Remote VSS

Share-basierte Backups mit Remote VSS – Übersicht

Sie können Remote VSS verwenden, um auf Freigabe basierte Backups von Hyper-V VM-Dateien durchzuführen, die auf einem CIFS-Server gespeichert sind.

Microsoft Remote VSS (Volume Shadow Copy Services) ist eine Erweiterung der bestehenden Microsoft VSS-Infrastruktur. Mit Remote VSS hat Microsoft die VSS-Infrastruktur erweitert, um das Schattenkopieren von SMB-Freigaben zu unterstützen. Darüber hinaus können Serverapplikationen wie Hyper-V VHD-Dateien auf SMB-Dateifreigaben speichern. Mit diesen Erweiterungen ist es möglich, applikationskonsistente Schattenkopien für Virtual Machines zu erstellen, die Daten und Konfigurationsdateien auf Shares speichern.

Remote VSS-Konzepte

Beachten Sie bestimmte Konzepte, die erforderlich sind, um zu verstehen, wie Remote VSS (Volume Shadow Copy Service) von Backup-Services mit Hyper-V over SMB-Konfigurationen verwendet wird.

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

  Eine Microsoft-Technologie, die verwendet wird, um Backup-Kopien oder Snapshots von Daten auf einem bestimmten Volume zu einem bestimmten Zeitpunkt zu erstellen. VSS koordiniert Daten-Server, Backup-Applikationen und Storage Management Software zur Unterstützung der Erstellung und des Managements konsistenter Backups.

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

  Eine Microsoft-Technologie, die zum Erstellen gemeinsam genutzter Backup-Kopien von Daten verwendet wird, die sich in einem datenkonsistenten Zustand befinden, zu einem bestimmten Zeitpunkt, zu dem über SMB 3.0 Shares auf die Daten zugegriffen wird. Auch bekannt als *Volume Shadow Copy Service*.

- **Schattenkopie**

  Ein doppelter Datensatz im Share zu einem genau definierten Zeitpunkt. Dank Shadow-Kopien werden konsistente, zeitpunktgenaue Backups von Daten erstellt, sodass das System oder die Applikationen die Daten der ursprünglichen Volumes weiterhin aktualisieren können.

- **Schattenkopiesatz**

  Eine Sammlung von einer oder mehreren Schattenkopien, wobei jede Schattenkopie einer Freigabe entspricht. Die Schattenkopien in einem Schattenkopiesatz stellen alle Freigaben dar, die in demselben Vorgang gesichert werden müssen. Der VSS-Client in der VSS-fähigen Anwendung identifiziert, welche Schattenkopien in den Satz eingeschlossen werden sollen.

- **Schattenkopiesatz automatische Wiederherstellung**

  Der Teil des Backup-Prozesses für VSS-fähige Remote-Backup-Applikationen, bei denen das Replikatverzeichnis mit den Schattenkopien zeitpunktgenaue konsistent erstellt wird. Beim Start des Backups löst der VSS-Client auf der Anwendung die Anwendung aus, um Software-Checkpoints auf den für das Backup vorgesehenen Daten zu erstellen (die virtuellen Maschinendateien im Fall von Hyper-V). Der VSS-Client ermöglicht dann den Fortsetzen der Anwendungen. Nachdem der Schattenkopiesatz erstellt wurde, macht Remote VSS die Schattenkopie beschreibbar und gibt die beschreibbare Kopie den Anwendungen wieder. Die Applikation bereitet den Schattenkopie-Satz für das Backup vor, indem sie eine automatische Wiederherstellung mithilfe des zuvor erstellten Software-Kontrollpunkts durchführt. Die automatische Wiederherstellung sorgt für einen konsistenten Zustand der Schattenkopien, indem die Änderungen seit der Erstellung des Checkpoint an den Dateien und Verzeichnissen vorgenommen werden. Für VSS-fähige Backups ist die automatische Wiederherstellung ein optionaler Schritt.

- **Shadow Copy ID**

  Eine GUID, die eine Schattenkopie eindeutig identifiziert.

- **Schattenkopie Set ID**

  Eine GUID, die eine Sammlung von Schattenkopie-IDs eindeutig auf demselben Server identifiziert.

- **SnapManager für Hyper-V**

  Die Software, die Backup- und Wiederherstellungsvorgänge für Microsoft Windows Server 2012 Hyper-V automatisiert und vereinfacht. SnapManager für Hyper-V verwendet Remote VSS mit automatischer Wiederherstellung, um Hyper-V Dateien über SMB-Freigaben zu sichern.

Verwandte Informationen

Wichtige Konzepte zum unterbrechungsfreien Betrieb von Hyper-V und SQL Server over SMB

Share-basierte Backups mit Remote VSS

Beispiel einer Verzeichnisstruktur, die von Remote VSS verwendet wird

Remote VSS durchquert die Verzeichnisstruktur, in der Hyper-V Dateien virtueller Maschinen gespeichert werden, während dadurch Schattenkopien erstellt werden. Es ist wichtig, zu verstehen, was eine geeignete Verzeichnisstruktur ist, damit Sie erfolgreich Backups von Dateien der Virtual Machine erstellen können.

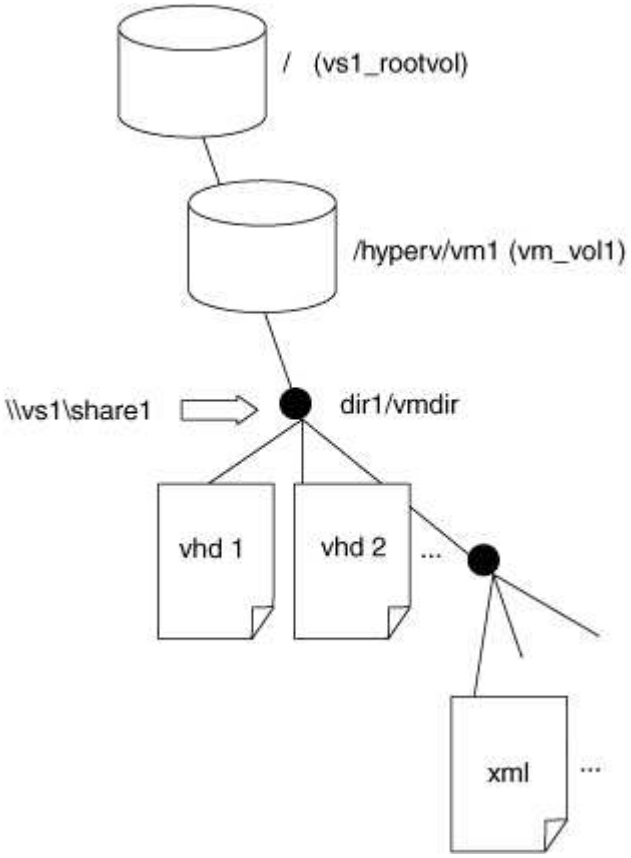
Eine unterstützte Verzeichnisstruktur für die erfolgreiche Erstellung von Schattenkopien entspricht den folgenden Anforderungen:

- Innerhalb der Verzeichnisstruktur, die zum Speichern von VM-Dateien verwendet wird, befinden sich nur Verzeichnisse und normale Dateien.

  Die Verzeichnisstruktur enthält keine Verbindungen, Links oder nicht-reguläre Dateien.

- Alle Dateien für eine Virtual Machine liegen in einem einzigen Share.
- Die Verzeichnisstruktur, die zum Speichern von VM-Dateien verwendet wird, überschreitet nicht die konfigurierte Tiefe des Verzeichnisses für Schattenkopien.
- Das Stammverzeichnis der Freigabe enthält nur virtuelle Computerdateien oder -Verzeichnisse.

In der folgenden Abbildung wird das Volume mit dem Namen vm_vol1 mit einem Verbindungspunkt bei `/hyperv/vm1` der Storage Virtual Machine (SVM) vs1 erstellt. Unterverzeichnisse, die die Dateien der virtuellen Maschine enthalten, werden unter dem Verbindungspunkt erstellt. Auf die Dateien der virtuellen Maschine des Hyper-V Servers wird über share1 mit dem Pfad zugegriffen `/hyperv/vm1/dir1/vmdir`. Der Dienst für die Schattenkopie erstellt Schattenkopien aller VM-Dateien, die sich innerhalb der Verzeichnisstruktur unter Share1 befinden (bis zur konfigurierten Tiefe des Verzeichnisses für die Schattenkopien).



So managt SnapManager für Hyper-V Remote VSS-basierte Backups für Hyper-V über SMB

Mithilfe von SnapManager für Hyper-V können Remote VSS-basierte Backup-Services gemanagt werden. Der Einsatz von SnapManager für einen gemanagten Backup-Service für Hyper-V zur Erstellung platzsparender Backup-Sets bietet zahlreiche Vorteile.

Die Optimierungen bei SnapManager für im Rahmen von Hyper-V gemanagte Backups umfassen Folgendes:

- Die SnapDrive Integration in ONTAP ermöglicht bei der Ermittlung des SMB-Share-Speicherorts die Performance-Optimierung.

  ONTAP stellt SnapDrive den Namen des Volumes zur Verfügung, auf dem sich die Freigabe befindet.

- SnapManager für Hyper-V gibt die Liste der Virtual Machine-Dateien in den SMB-Shares an, die der Schattenkopie-Service kopieren muss.

  Durch die Bereitstellung einer zielorientierten Liste von VM-Dateien muss der Dienst für Schattenkopien nicht von allen Dateien in der Freigabe Schattenkopien erstellen.

- Die Storage Virtual Machine (SVM) behält die Snapshots für SnapManager für Hyper-V zur Verwendung für Restores bei.

  Es gibt keine Backup-Phase. Das Backup ist der platzsparende Snapshot.

SnapManager für Hyper-V bietet mithilfe des folgenden Prozesses Backup- und Restore-Funktionen für HyperV über SMB:

1. Vorbereitung für den Schattenkopie-Vorgang

   Der VSS-Client der SnapManager für Hyper-V Applikation legt den Satz der Schattenkopien fest. Der VSS-Client sammelt Informationen darüber, welche Freigaben in den Schattenkopiesatz einbezogen werden sollen, und stellt diese Informationen ONTAP zur Verfügung. Ein Satz kann eine oder mehrere Schattenkopien enthalten, und eine Schattenkopie entspricht einer Freigabe.

2. Erstellen des SchattenkopieSatzes (bei automatischer Wiederherstellung)

   Für jeden Share im Shadow Copy-Set erstellt ONTAP eine Shadow-Kopie, die dann beschreibbar macht.

3. Legen Sie den Schattenkopiesatz fest

   Nachdem ONTAP die Schattenkopien erstellt hat, sind sie SnapManager für Hyper-V ausgesetzt, sodass VSS Writer die automatische Recovery durchführen können.

4. Automatisches Wiederherstellen des SchattenkopieSatzes

   Während der Erstellung des Schattenkopie-Satzes gibt es einen Zeitraum, in dem aktive Änderungen an den Dateien im Backup-Satz vorgenommen werden. Die VSS-Autoren der Applikation müssen die Schattenkopien aktualisieren, um sicherzustellen, dass sie sich vor dem Backup in einem vollständig konsistenten Zustand befinden.

   > Die Art und Weise, wie das automatische Recovery durchgeführt wird, ist applikationsspezifisch. Remote VSS ist in dieser Phase nicht beteiligt.

5. Abschließen und Reinigen der Schattenkopie

   Der VSS-Client benachrichtigt ONTAP, nachdem die automatische Wiederherstellung abgeschlossen ist. Der Schattenkopiesatz wird schreibgeschützt gemacht und ist dann für die Sicherung bereit. Bei der Verwendung von SnapManager für Hyper-V für Backups werden die Dateien in einem Snapshot zum Backup. Daher wird für die Backup-Phase ein Snapshot für jedes Volume erstellt, das Freigaben im Backup-Set enthält. Nachdem die Sicherung abgeschlossen ist, wird der Satz der Schattenkopien vom CIFS-Server entfernt.

So wird der Offload von ODX Kopien mit Hyper-V und SQL Server über SMB-Freigaben genutzt

Offloaded Data Transfer (ODX), auch bekannt als „*Copy Offload*“, ermöglicht direkte Datentransfers innerhalb und zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen. ONTAP ODX Copy Offload bietet Performance-Vorteile bei Kopiervorgängen auf Ihrem Applikationsserver im Vergleich zur SMB-Installation.

Bei Dateiübertragungen ohne ODX werden die Daten vom CIFS-Quell-Server gelesen und im Netzwerk an den Client-Computer übertragen. Der Clientcomputer überträgt die Daten zurück über das Netzwerk an den Ziel-CIFS-Server. Zusammenfassend liest der Clientcomputer die Daten aus der Quelle und schreibt sie auf das Ziel. Bei der Übertragung von ODX-Dateien werden Daten direkt von der Quelle zum Ziel kopiert.

Da ODX Offloaded Kopien direkt zwischen Quell- und Ziel-Storage erstellt werden, ergeben sich erhebliche Performance-Vorteile. Zu den Performance-Vorteilen gehören eine schnellere Kopierzeit zwischen Quelle und Ziel, eine geringere Ressourcenauslastung (CPU, Speicher) auf dem Client und eine geringere Auslastung der Netzwerk-I/O-Bandbreite.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen
unterstützt:
```

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, derselbe Node, dieselbe Storage Virtual Machine (SVM)

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

Spezifische Anwendungsfälle für den ODX Copy-Offload mit Hyper-V Lösungen:

- Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

  Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

- Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
- Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> ⓘ Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

Spezifische Anwendungsfälle für den ODX Copy-Offload mit SQL Server Lösungen:

- Mit ODX Copy Offload können SQL Server Datenbanken zwischen zugeordneten SMB-Shares oder zwischen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters exportiert und importiert werden.
- ODX Copy Offload wird für Datenbankexporte und -Importe verwendet, wenn sich Quell- und Ziel-Storage im selben Cluster befinden.

Konfigurationsanforderungen und Überlegungen

ONTAP- und Lizenzierungsanforderungen

Bei der Erstellung von SQL Server oder Hyper-V über SMB-Lösungen müssen Sie bestimmte ONTAP- und Lizenzierungsanforderungen beachten, um den unterbrechungsfreien Betrieb auf SVMs zu gewährleisten.

Anforderungen an die ONTAP-Version

- Hyper-V über SMB

  ONTAP unterstützt den unterbrechungsfreien Betrieb über SMB-Freigaben für Hyper-V unter Windows 2012 oder höher.

- SQL Server über SMB

  ONTAP unterstützt den unterbrechungsfreien Betrieb über SMB-Freigaben für SQL Server 2012 oder höher unter Windows 2012 oder höher.

Aktuelle Informationen zu unterstützten Versionen von ONTAP, Windows Server und SQL Server für unterbrechungsfreien Betrieb über SMB-Freigaben finden Sie in der Interoperabilitäts-Matrix.

"NetApp Interoperabilitäts-Matrix-Tool"

Lizenzierungsanforderungen

Die folgenden Lizenzen sind erforderlich:

- CIFS
- FlexClone (nur für Hyper-V über SMB)

  Diese Lizenz ist erforderlich, wenn Remote VSS für Backups verwendet wird. Der Shadow Copy Service verwendet FlexClone, um zeitpunktgenaue Kopien von Dateien zu erstellen, die dann bei der Erstellung eines Backups verwendet werden.

  Eine FlexClone Lizenz ist optional, wenn Sie eine Backup-Methode verwenden, die kein Remote VSS verwendet.

Die FlexClone-Lizenz ist in enthalten"ONTAP One". Wenn Sie nicht über ONTAP One, sollten Sie"Überprüfen Sie, ob die erforderlichen Lizenzen installiert sind", und, wenn nötig, "Installieren Sie sie".

Anforderungen an Netzwerk und LIF-Daten

Sie müssen bestimmte Netzwerk- und Daten-LIF-Anforderungen kennen, wenn Sie SQL Server- oder Hyper-V über SMB-Konfigurationen erstellen, um einen unterbrechungsfreien Betrieb zu gewährleisten.)

Anforderungen an Netzwerkprotokolle

- IPv4- und IPv6-Netzwerke werden unterstützt.
- SMB 3.0 oder höher ist erforderlich.

  SMB 3.0 bietet die Funktionen, die zum Erstellen kontinuierlich verfügbarer SMB-Verbindungen erforderlich sind, damit ein unterbrechungsfreier Betrieb möglich ist.

- DNS-Server müssen Einträge enthalten, die den CIFS-Servernamen den IP-Adressen zuordnen, die den Daten-LIFs auf der Storage Virtual Machine (SVM) zugewiesen sind.

  Die Applikations-Server Hyper-V oder SQL Server führen beim Zugriff auf Virtual Machines- oder Datenbankdateien normalerweise mehrere Verbindungen über mehrere Daten-LIFs durch. Um eine ordnungsgemäße Funktion zu gewährleisten, müssen die Anwendungsserver diese mehrere SMB-Verbindungen herstellen, indem sie den CIFS-Servernamen verwenden, anstatt mehrere Verbindungen zu mehreren eindeutigen IP-Adressen zu machen.

  Außerdem erfordert Witness den DNS-Namen des CIFS-Servers anstelle der einzelnen LIF IP-Adressen.

  Ab ONTAP 9.4 können Sie den Durchsatz und die Fehlertoleranz für Hyper-V und SQL Server über SMB-Konfigurationen verbessern, indem Sie SMB MultiChannel aktivieren. Dazu müssen Sie mehrere 1G, 10G oder größere NICs auf dem Cluster und den Clients einsetzen.

Anforderungen an Daten-LIF

- Die SVM, die die Applikationsserver über SMB-Lösung hostet, muss auf jedem Node im Cluster mindestens eine logische Daten-LIF aufweisen.

  Ein Failover von SVM-Daten-LIFs auf andere Daten-Ports im Cluster ist möglich, einschließlich Nodes, die aktuell keine Daten hosten, die von den Applikationsservern abgerufen werden. Außerdem ist jeder Node

im Cluster immer der SFO-Partner eines Node, mit dem der Applikationsserver verbunden ist, ein potenzieller Witness Node.

- Daten-LIFs dürfen nicht für die automatische Wiederherstellung konfiguriert werden.

  Nach einem Takeover- oder Giveback-Ereignis sollten Sie die Daten-LIFs manuell auf ihre Home-Ports zurücksetzen.

- Alle Daten-LIF-IP-Adressen müssen einen Eintrag in DNS haben und alle Einträge müssen zum CIFS-Servernamen auflösen.

  Die Applikations-Server müssen sich über den CIFS-Servernamen mit SMB-Freigaben verbinden. Konfigurieren Sie die Anwendungsserver nicht, um Verbindungen mithilfe der LIF-IP-Adressen herzustellen.

- Wenn sich der CIFS-Servername von dem SVM-Namen unterscheidet, müssen die DNS-Einträge auf den CIFS-Servernamen auflösen.

SMB-Server- und Volume-Anforderungen für Hyper-V über SMB

Bei der Erstellung von Hyper-V über SMB-Konfigurationen müssen bestimmte SMB-Server- und Volume-Anforderungen bekannt sein, um einen unterbrechungsfreien Betrieb zu gewährleisten.

Anforderungen an SMB-Server

- SMB 3.0 muss aktiviert sein.

  Diese Option ist standardmäßig aktiviert.

- Die standardmäßige CIFS-Serveroption für UNIX-Benutzer muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Erstellen einer SMB-Verbindung. Da für alle SMB-Zugriffe eine erfolgreiche Zuordnung des Windows-Benutzers zu einem UNIX-Benutzerkonto oder zum Standard-UNIX-Benutzerkonto erforderlich ist, muss ONTAP in der Lage sein, das Computerkonto des Anwendungsservers dem UNIX-Standardbenutzerkonto zuzuordnen.

- Automatische Knotenempfehlungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn Sie automatische Node-Empfehlungen für den Zugriff auf Daten außer Hyper-V-Maschinendateien verwenden möchten, müssen Sie für diese Daten eine separate SVM erstellen.

- Sowohl Kerberos als auch NTLM-Authentifizierung müssen in der Domäne erlaubt sein, zu der der SMB-Server gehört.

  ONTAP wirbt nicht für den Kerberos-Service für Remote VSS. Daher sollte die Domain auf NTLM zulassen eingestellt sein.

- Die Funktion „Schattenkopie“ muss aktiviert sein.

  Diese Funktion ist standardmäßig aktiviert.

- Das Windows-Domain-Konto, das der Schattenkopierdienst beim Erstellen von Schattenkopien nutzt, muss Mitglied der lokalen BUILTIN\-Administratoren oder BUILTIN\Backup Operators-Gruppe sein.

Volume-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

  Um NDOS für Applikationsserver bereitzustellen, die kontinuierlich verfügbare SMB-Verbindungen verwenden, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Sie können ein Volume mit gemischtem Sicherheitsstil oder ein UNIX Security-Style-Volume nicht auf ein NTFS Security-Style Volume ändern und es direkt für NDOS über SMB-Freigaben verwenden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Security-Style-Volume ändern und beabsichtigen, es für NDOS über SMB-Freigaben zu verwenden, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Damit Shadow-Copy-Vorgänge erfolgreich durchgeführt werden können, muss auf dem Volume genügend Speicherplatz vorhanden sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

Verwandte Informationen

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

SMB-Server- und Volume-Anforderungen für SQL Server über SMB

Bei der Erstellung von SQL Server über SMB-Konfigurationen müssen bestimmte SMB-Server- und Volume-Anforderungen bekannt sein, um einen unterbrechungsfreien Betrieb zu gewährleisten.

Anforderungen an SMB-Server

- SMB 3.0 muss aktiviert sein.

  Diese Option ist standardmäßig aktiviert.

- Die standardmäßige CIFS-Serveroption für UNIX-Benutzer muss mit einem gültigen UNIX-Benutzerkonto konfiguriert sein.

  Die Anwendungsserver verwenden das Computerkonto beim Erstellen einer SMB-Verbindung. Da für alle SMB-Zugriffe eine erfolgreiche Zuordnung des Windows-Benutzers zu einem UNIX-Benutzerkonto oder zum Standard-UNIX-Benutzerkonto erforderlich ist, muss ONTAP in der Lage sein, das Computerkonto des Anwendungsservers dem UNIX-Standardbenutzerkonto zuzuordnen.

  Darüber hinaus verwendet SQL Server einen Domänenbenutzer als SQL Server-Dienstkonto. Das Servicekonto muss auch dem UNIX-Standardbenutzer zugeordnet werden.

- Automatische Knotenempfehlungen müssen deaktiviert sein (diese Funktion ist standardmäßig deaktiviert).

  Wenn Sie automatische Node-Empfehlungen für den Zugriff auf Daten verwenden möchten, die nicht auf

SQL Server-Datenbankdateien liegen, müssen Sie eine separate SVM für diese Daten erstellen.

- Dem Windows-Benutzerkonto, das für die Installation von SQL Server auf ONTAP verwendet wird, muss die Berechtigung „SeSecurityPrivilege“ zugewiesen werden.

  Diese Berechtigung wird der lokalen BUILTIN\Administrators-Gruppe des SMB-Servers zugewiesen.

Volume-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

  Um NDOS für Applikationsserver bereitzustellen, die kontinuierlich verfügbare SMB-Verbindungen verwenden, muss das Volume, das die Freigabe enthält, ein NTFS-Volume sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Sie können ein Volume mit gemischtem Sicherheitsstil oder ein UNIX Security-Style-Volume nicht auf ein NTFS Security-Style Volume ändern und es direkt für NDOS über SMB-Freigaben verwenden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Security-Style-Volume ändern und beabsichtigen, es für NDOS über SMB-Freigaben zu verwenden, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, kreuzen SQL Server beim Erstellen der Datenbank-Verzeichnisstruktur keine Verbindungen.
- Damit das SnapCenter Plug-in für Backup-Vorgänge von Microsoft SQL Server erfolgreich ist, müssen ausreichend Speicherplatz auf dem Volume verfügbar sein.

  Das Volume, auf dem sich die SQL Server Datenbankdateien befinden, muss groß genug sein, um die Verzeichnisstruktur und alle enthaltenen Dateien innerhalb der Freigabe zu speichern.

Verwandte Informationen

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

Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für Hyper-V über SMB

Sie müssen bestimmte Anforderungen und Überlegungen beachten, wenn Sie kontinuierlich verfügbare Shares für Hyper-V over SMB-Konfigurationen konfigurieren, die einen unterbrechungsfreien Betrieb unterstützen.

Share-Anforderungen

- Freigaben, die von den Anwendungsservern verwendet werden, müssen mit der kontinuierlich verfügbaren Eigenschaft konfiguriert werden.

  Applikations-Server, die sich mit kontinuierlich verfügbaren Shares verbinden, erhalten persistente Handles, über die sie sich unterbrechungsfrei mit SMB-Freigaben verbinden und Dateisperren nach Unterbrechungen wie Takeover, Giveback und Aggregatverschiebung wieder nutzbar machen können.

- Wenn Sie Remote VSS-fähige Backup-Services verwenden möchten, können Sie Hyper-V-Dateien nicht in

Shares mit Verbindungen verschieben.

Im Fall der automatischen Wiederherstellung schlägt die Erstellung von Schattenkopien fehl, wenn beim Überfahren der Freigabe eine Verbindung auftritt. In einem Fall, in dem keine automatische Wiederherstellung erforderlich ist, schlägt die Erstellung von Schattenkopien nicht fehl, aber die Verbindung weist keinen Punkt auf.

- Wenn Sie Remote VSS-fähige Backup-Services mit automatischer Wiederherstellung verwenden möchten, können Sie Hyper-V-Dateien nicht in Freigaben verschieben, die Folgendes enthalten:
  - Symlinks, hardlinks oder widelinks
  - Nicht regelmäßige Dateien

    Die Erstellung von Schattenkopien schlägt fehl, wenn sich Links oder nicht-normale Dateien in der Freigabe zur Schattenkopie befinden. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

  - Damit Shadow-Copy-Vorgänge erfolgreich durchgeführt werden können, müssen ausreichend Speicherplatz auf dem Volume vorhanden sein (nur für Hyper-V über SMB).

    Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind. Diese Anforderung gilt nur für Schattenkopien mit automatischer Recovery.

- Die folgenden Freigabeigenschaften dürfen nicht auf kontinuierlich verfügbaren Freigaben festgelegt werden, die von den Anwendungsservern verwendet werden:
  - Home Directory damit füllt
  - Caching von Attributen
  - BranchCache

Überlegungen

- Kontingente werden für kontinuierlich verfügbare Aktien unterstützt.
- Die folgende Funktion wird für Hyper-V über SMB-Konfigurationen nicht unterstützt:
  - Prüfung
  - FPolicy
- Der Virenscan wird nicht auf SMB-Freigaben mit dem `continuously-availability` auf eingestellten Parameter durchgeführt `Yes`.

Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für SQL Server über SMB

Beachten Sie bestimmte Anforderungen und Überlegungen, wenn Sie kontinuierlich verfügbare Shares für SQL Server über SMB-Konfigurationen konfigurieren, die einen unterbrechungsfreien Betrieb unterstützen.

Share-Anforderungen

- Volumes, die zur Speicherung von Dateien virtueller Maschinen verwendet werden, müssen als NTFS Sicherheitsstil Volumes erstellt werden.

Um für Applikationsserver einen unterbrechungsfreien Betrieb zu ermöglichen, der kontinuierlich verfügbare SMB-Verbindungen verwendet, muss das Volume, das den Share enthält, ein NTFS-Volume sein. Außerdem muss es immer ein NTFS-Volume gewesen sein. Ein Volume mit gemischtem Sicherheitsstil bzw. ein UNIX Volume kann nicht auf ein NTFS Sicherheitsstil Volume geändert und direkt für unterbrechungsfreien Betrieb über SMB-Freigaben verwendet werden. Wenn Sie ein Volume mit gemischtem Sicherheitsstil in ein NTFS-Sicherheitsstil-Volume ändern und diese für unterbrechungsfreien Betrieb über SMB-Freigaben verwenden möchten, müssen Sie manuell eine ACL oben auf dem Volume platzieren und diese ACL auf alle enthaltenen Dateien und Ordner übertragen. Andernfalls können Migrationen virtueller Maschinen oder Exporte von Datenbankdateien und Importe, wo Dateien auf ein anderes Volume verschoben werden, fehlschlagen, wenn entweder die Quell- oder Ziel-Volumes zunächst als gemischte oder UNIX-SicherheitsVolumes erstellt und später in NTFS-Sicherheitsstil geändert wurden.

- Freigaben, die von den Anwendungsservern verwendet werden, müssen mit der kontinuierlich verfügbaren Eigenschaft konfiguriert werden.

  Applikations-Server, die sich mit kontinuierlich verfügbaren Shares verbinden, erhalten persistente Handles, über die sie sich unterbrechungsfrei mit SMB-Freigaben verbinden und Dateisperren nach Unterbrechungen wie Takeover, Giveback und Aggregatverschiebung wieder nutzbar machen können.

- Obwohl das Volume, das die Datenbankdateien enthält, Verbindungen enthalten kann, kreuzen SQL Server beim Erstellen der Datenbank-Verzeichnisstruktur keine Verbindungen.
- Damit das SnapCenter Plug-in für den Betrieb von Microsoft SQL Server erfolgreich ist, müssen Sie über genügend Speicherplatz auf dem Volume verfügen.

  Das Volume, auf dem sich die SQL Server Datenbankdateien befinden, muss groß genug sein, um die Verzeichnisstruktur und alle enthaltenen Dateien innerhalb der Freigabe zu speichern.

- Die folgenden Freigabeigenschaften dürfen nicht auf kontinuierlich verfügbaren Freigaben festgelegt werden, die von den Anwendungsservern verwendet werden:
  - Home Directory damit füllt
  - Caching von Attributen
  - BranchCache

Überlegungen teilen

- Kontingente werden für kontinuierlich verfügbare Aktien unterstützt.
- Die folgende Funktion wird für SQL Server über SMB-Konfigurationen nicht unterstützt:
  - Prüfung
  - FPolicy
- Der Virus-Scan wird nicht auf SMB-Shares mit den `continuously-availability` Eigenschaften der Freigabe durchgeführt.

Überlegungen zu Remote VSS für Hyper-V über SMB-Konfigurationen

Beachten Sie bei der Verwendung von Remote VSS-fähigen Backup-Lösungen für Hyper-V über SMB-Konfigurationen bestimmte Überlegungen.

Allgemeine Überlegungen zu Remote VSS

- Pro Microsoft Applikations-Server können maximal 64 Shares konfiguriert werden.

Der Vorgang der Schattenkopie schlägt fehl, wenn mehr als 64 Shares in einem Schattenkopiesatz vorhanden sind. Dies ist eine Anforderung von Microsoft.

- Pro CIFS-Server ist nur ein aktiver Schattenkopiesatz zulässig.

  Ein Vorgang der Schattenkopie schlägt fehl, wenn auf demselben CIFS-Server kontinuierlich eine Schattenkopie durchgeführt wird. Dies ist eine Anforderung von Microsoft.

- In der Verzeichnisstruktur, in der Remote VSS eine Schattenkopie erstellt, sind keine Verbindungen zulässig.
  - Im Fall der automatischen Wiederherstellung schlägt die Erstellung von Schattenkopien fehl, wenn beim Überfahren der Freigabe eine Verbindung auftritt.
  - In einem Fall eines nicht automatischen Recovery schlägt die Erstellung von Schattenkopien nicht fehl, aber die Verbindung weist keinen Punkt auf.

Überlegungen zu Remote-VSS, die nur für Schattenkopien mit automatischem Recovery gelten

Bestimmte Grenzwerte gelten nur für Schattenkopien mit automatischer Recovery.

- Für die Erstellung von Schattenkopien ist eine maximale Verzeichnistiefe von fünf Unterverzeichnissen zulässig.

  Dies ist die Verzeichnistiefe, über die der Service für Schattenkopien einen Backup-Satz erstellt. Die Erstellung von Schattenkopien schlägt fehl, wenn Verzeichnisse, die eine virtuelle Maschinendatei enthalten, tiefer als fünf Ebenen geschachtelt sind. Dies soll den Verzeichnistversal beim Klonen der Freigabe begrenzen. Die maximale Verzeichnistiefe kann über eine CIFS-Serveroption geändert werden.

- Die Menge an verfügbarem Speicherplatz auf dem Volume muss ausreichend sein.

  Der verfügbare Speicherplatz muss mindestens so groß sein wie der kombinierte Speicherplatz, der von allen Dateien, Verzeichnissen und Unterverzeichnissen genutzt wird, die sich in den Freigaben befinden, die in der Sicherungskopie der Schattenkopie enthalten sind.

- Innerhalb der Verzeichnisstruktur, auf der Remote VSS eine Schattenkopie erstellt, sind keine Links oder nicht reguläre Dateien zulässig.

  Die Erstellung von Schattenkopien schlägt fehl, wenn sich Links oder nicht-normale Dateien in der Freigabe zur Schattenkopie befinden. Sie werden vom Klonprozess nicht unterstützt.

- Auf Verzeichnissen sind keine NFSv4-ACLs zulässig.

  Obwohl durch die Erstellung von Schattenkopien die NFSv4 ACLs auf Dateien erhalten bleiben, gehen die NFSv4 ACLs auf Verzeichnissen verloren.

- Maximal 60 Sekunden können Schattenkopien erstellt werden.

  Microsoft-Spezifikationen erlauben die Erstellung des SchattenkopieSatzes auf maximal 60 Sekunden. Wenn der VSS-Client nicht innerhalb dieses Zeitraums den Schattenkopiesatz erstellen kann, schlägt der Vorgang der Schattenkopie fehl. Dadurch wird die Anzahl der Dateien in einem Schattenkopiesatz eingeschränkt. Die tatsächliche Anzahl der Dateien oder Virtual Machines, die in einem Backup-Satz enthalten sein können, variiert. Diese Zahl ist von vielen Faktoren abhängig und muss für die jeweilige Kundenumgebung festgelegt werden.

Offloaded Data Transfer von ODX für SQL Server und Hyper-V über SMB

ODX Copy Offload muss aktiviert werden, wenn Sie Dateien für Virtual Machines migrieren oder Datenbankdateien direkt vom Quell- zum Ziel-Storage exportieren und importieren möchten, ohne Daten durch die Applikationsserver zu senden. Es gelten bestimmte Anforderungen, die Sie über die Nutzung von ODX Copy Offload mit SQL Server und Hyper-V over SMB-Lösungen wissen müssen.

Der Einsatz von ODX Copy Offload bietet einen erheblichen Performance-Vorteil. Diese CIFS-Serveroption ist standardmäßig aktiviert.

- SMB 3.0 muss aktiviert sein, um ODX Copy Offload zu nutzen.
- Die Quell-Volumes müssen mindestens 1.25 GB betragen.
- Die Deduplizierung muss für Volumes aktiviert sein, die zusammen mit dem Copy-Offload verwendet werden.
- Bei Verwendung von komprimierten Volumes muss der Komprimierungstyp anpassungsfähig sein und es muss nur die Größe der Komprimierungsgruppe 8K unterstützt werden.

  Der Typ der sekundären Komprimierung wird nicht unterstützt

- Damit Hyper-V Gastsysteme innerhalb und zwischen Festplatten mit ODX Copy Offload migriert werden können, müssen die Hyper-V Server für die Verwendung von SCSI-Festplatten konfiguriert werden.

  Standardmäßig werden IDE-Festplatten konfiguriert, aber ODX Copy Offload funktioniert nicht, wenn Gäste migriert werden, wenn Festplatten mit IDE-Festplatten erstellt werden.

Empfehlungen für SQL Server- und Hyper-V-Konfigurationen über SMB

Damit Ihre SQL Server- und Hyper-V-over-SMB-Konfigurationen robust und betriebsbereit sind, müssen Sie bei der Konfiguration der Lösungen mit den empfohlenen Best Practices vertraut sein.

Allgemeine Empfehlungen

- Trennen Sie Applikations-Server-Dateien von allgemeinen Benutzerdaten.

  Falls möglich, widmen Sie eine komplette Storage Virtual Machine (SVM) und deren Storage für die Daten des Applikations-Servers.

- Um eine optimale Performance zu erzielen, sollten Sie SMB-Signaturen nicht auf SVMs aktivieren, die zum Speichern der Daten des Applikationsservers verwendet werden.
- Wenn SMB MultiChannel in einer SMB-Sitzung mehrere Verbindungen zwischen ONTAP und Clients bereitstellen soll, wird eine optimale Performance und eine verbesserte Fehlertoleranz erzielt.
- Erstellen Sie keine kontinuierlich verfügbaren Freigaben auf anderen Freigaben als in der Hyper-V- oder SQL Server-Konfiguration über SMB.
- Deaktivieren Sie die Änderungsbenachrichtigungen für Shares, die für kontinuierliche Verfügbarkeit verwendet werden.

- Führen Sie keine Volume-Verschiebung gleichzeitig mit der Aggregatverschiebung (ARL) durch, da ARL über Phasen verfügt, bei denen einige Vorgänge unterbrochen werden.
- Für Hyper-V over SMB-Lösungen verwenden Sie iSCSI-Laufwerke in-Guest, wenn Sie geclusterte Virtual Machines erstellen. Gemeinsam genutzte `.VHDX` Dateien werden für Hyper-V über SMB in ONTAP SMB-Freigaben nicht unterstützt.

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

Füllen Sie das Arbeitsblatt für die Volume-Konfiguration aus

Das Arbeitsblatt bietet eine einfache Möglichkeit, die Werte aufzuzeichnen, die Sie beim Erstellen von Volumes für SQL Server- und Hyper-V-Konfigurationen über SMB benötigen.

Für jedes Volume müssen Sie die folgenden Informationen angeben:

- Name der Storage Virtual Machine (SVM

  Der SVM-Name ist für alle Volumes gleich.

- Volume-Name
- Aggregatname

  Sie können Volumes auf Aggregaten erstellen, die sich auf einem beliebigen Node im Cluster befinden.

- Größe
- Verbindungspfad

Beachten Sie Folgendes beim Erstellen von Volumes, die zum Speichern von Anwendungsserverdaten verwendet werden:

- Wenn der NTFS-Sicherheitsstil für das Root-Volume nicht vorhanden ist, müssen Sie beim Erstellen des Volumes den Sicherheitsstil als NTFS angeben.

  Standardmäßig übernehmen Volumes den Sicherheitsstil des SVM-Root-Volume.

- Die Volumes sollten mit der standardmäßigen Volume-Speicherplatzzusage konfiguriert werden.
- Optional können Sie die Einstellung zur automatischen Speicherplatzverwaltung konfigurieren.
- Sie sollten die Option einstellen, die die Snapshot-Platzreserve bestimmt auf `0`.
- Die auf das Volume angewendete Snapshot-Richtlinie muss deaktiviert werden.

  Wenn die SVM-Snapshot-Richtlinie deaktiviert ist, müssen Sie keine Snapshot-Richtlinie für die Volumes angeben. Die Volumes übernehmen die Snapshot-Richtlinie für die SVM. Wenn die Snapshot-Richtlinie für die SVM nicht deaktiviert ist und für die Erstellung von Snapshots konfiguriert ist, müssen Sie eine Snapshot-Richtlinie auf Volume-Ebene angeben und diese Richtlinie muss deaktiviert werden. Shadow Copy Service-aktivierte Backups und SQL Server-Backups verwalten die Erstellung und Löschung von Snapshots.

- Die Load-Sharing-Spiegelungen für die Volumes können nicht konfiguriert werden.

Verbindungspfade, auf denen Sie Freigaben erstellen möchten, die von den Anwendungsservern verwendet werden, sollten ausgewählt werden, damit sich unter dem Freigabepunkt keine miteinander verbunden Volumes befinden.

Wenn Sie beispielsweise virtuelle Maschinendateien auf vier Volumes mit den Namen „`vol1`“, „`vol2`“, „`vol3`“ und „`vol4`“ speichern möchten, können Sie den im Beispiel gezeigten Namespace erstellen. Sie können dann Freigaben für die Anwendungsserver unter den folgenden Pfaden erstellen: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` Und `/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
```

Arten von Informationen	Werte
Volume 1: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 2: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 3: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 4: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 5: Volume-Name, Aggregat, Größe, Verbindungspfad	
Volume 6: Volume-Name, Aggregat, Größe, Verbindungspfad	
Zusätzliche Volumes: Volume-Name, Aggregat, Größe, Verbindungspfad	

Füllen Sie das Konfigurationsarbeitsblatt für die SMB-Freigabe aus

Verwenden Sie dieses Arbeitsblatt, um die Werte aufzuzeichnen, die Sie beim Erstellen kontinuierlich verfügbarer SMB-Freigaben für SQL Server und Hyper-V über SMB-Konfigurationen benötigen.

Informationen zu SMB-Freigaben und Konfigurationseinstellungen

Für jede Freigabe müssen Sie die folgenden Informationen angeben:

- Name der Storage Virtual Machine (SVM

  Der SVM-Name ist für alle Freigaben gleich

- Freigabename
- Pfad
- Eigenschaften freigeben

  Sie müssen die folgenden beiden Freigabegenschaften konfigurieren:

  - `oplocks`
  - `continuously-available`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Symlinks müssen deaktiviert werden (der Wert für den `-symlink-properties` Parameter muss null sein [""]).

Informationen zu Freigabungspfaden

Wenn Sie Hyper-V-Dateien mithilfe von Remote VSS sichern, ist es wichtig, die Wahl der Freigabungspfade zu wählen, die bei der Herstellung von SMB-Verbindungen von den Hyper-V Servern zu den Speicherorten verwendet werden, an denen die Dateien der Virtual Machine gespeichert sind. Auch wenn Freigaben an jedem Punkt im Namespace erstellt werden können, sollten Pfade für Shares, die von den Hyper-V Servern genutzt werden, keine miteinander verbunden Volumes enthalten. Vorgänge von Schattenkopien können nicht auf Freigabepfaden ausgeführt werden, die Verbindungspunkte enthalten.

SQL Server kann beim Erstellen der Datenbank-Verzeichnisstruktur keine Kreuzungen durchführen. Sie sollten keine Freigabepfade für SQL Server erstellen, die Verbindungspunkte enthalten.

Wenn Sie beispielsweise die Dateien der virtuellen Maschine oder der Datenbank auf den Volumes „`vol1`“, „`vol2`“, „`vol3`“ und „`vol4`“ speichern möchten, sollten Sie Freigaben für die Anwendungsserver auf den folgenden Pfaden erstellen: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` Und `/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
```

Sie können Freigaben auf dem und `/data2` Pfade für die Verwaltung erstellen `/data1`. Konfigurieren Sie die Anwendungsserver nicht so, dass diese Freigaben zum Speichern von Daten verwendet werden.

Planungsarbeitsblatt

Arten von Informationen	Werte
_Volume 1: Name und Pfad der SMB-Freigabe	
_Volume 2: Name und Pfad der SMB-Freigabe	
_Volume 3: Name und Pfad der SMB-Freigabe	
_Volume 4: Name und Pfad der SMB-Freigabe	
_Volume 5: Name und Pfad der SMB-Freigabe	
_Volume 6: Name und Pfad der SMB-Freigabe	
_Volume 7: Name und Pfad der SMB-Freigabe	
Additional Volumes: SMB share Names and Paths	

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
   ```

Managen Sie Hyper-V und SQL Server über SMB-Konfigurationen

Konfigurieren Sie vorhandene Shares für kontinuierliche Verfügbarkeit

Sie können vorhandene Shares so ändern, dass diese kontinuierlich verfügbaren Shares werden, die mit den Hyper-V und SQL Server Applikationsserver für den unterbrechungsfreien Zugriff auf Hyper-V Virtual Machines, Konfigurationsdateien und SQL Server Datenbankdateien verwendet werden.

Über diese Aufgabe

Vorhandene Freigaben können nicht als kontinuierlich verfügbare Freigabe für unterbrechungsfreien Betrieb bei Applikations-Servern über SMB verwendet werden, wenn der Share folgende Merkmale aufweist:

- Wenn die `homedirectory` Share-Eigenschaft für diese Freigabe festgelegt ist
- Wenn die Freigabe aktivierte Symlink oder widelinks enthält
- Wenn die Freigabe Verbindungen unter dem Stammverzeichnis der Freigabe enthält

Sie müssen überprüfen, ob die beiden folgenden Freigabeparameter richtig eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standard) oder auf eingestellt `none`.
- Symlinks müssen deaktiviert sein.

Die folgenden Freigabeigenschaften müssen konfiguriert werden:

- `continuously-available`
- `oplocks`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden. Wenn sie in der Liste der aktuellen Share-Eigenschaften vorhanden sind, müssen sie aus der kontinuierlich verfügbaren Freigabe entfernt werden:

- `attributecache`

- `branchcache`

Schritte

1. Die aktuellen Einstellungen für den Freigabeparameter und die aktuelle Liste der konfigurierten Freigabeneigenschaften anzeigen:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Ändern Sie bei Bedarf die Freigabeparameter, um Symlinks zu deaktivieren und Offline-Dateien mit dem Befehl auf manuell zu setzen `vserver cifs share modify`.
   - Sie können Symlinks deaktivieren, indem Sie den Wert des `-symlink` Parameters auf setzen `""`.
   - Sie können den `-offline-files` Parameter auf die richtige Einstellung einstellen, indem `manual` Sie angeben.
3. Fügen Sie die Eigenschaft „Share“ und, falls erforderlich, die Eigenschaft „Share“ hinzu `continuously-available` `oplocks`:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Wenn die `oplocks` Eigenschaft `continuously-available` „Share“ noch nicht festgelegt ist, müssen Sie sie zusammen mit der Eigenschaft „Share“ hinzufügen.

4. Entfernen Sie alle Share-Eigenschaften, die nicht auf kontinuierlich verfügbaren Freigaben unterstützt werden:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Sie können eine oder mehrere Share-Eigenschaften entfernen, indem Sie die Share-Eigenschaften mit einer kommagetrennten Liste angeben.

5. Stellen Sie sicher, dass die `-symlink` `-offline-files` Parameter und korrekt eingestellt sind:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Vergewissern Sie sich, dass die Liste der konfigurierten Freigabeigenschaften korrekt ist:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Beispiele

Im folgenden Beispiel wird gezeigt, wie eine vorhandene Freigabe namens „share1“ auf der Storage Virtual Machine (SVM) „vs1“ für NDOS mit einem Applikations-Server über SMB konfiguriert wird:

- Symlinks werden für die Freigabe deaktiviert, indem der Parameter auf gesetzt `-symlink` `""`wird.
- Der `-offline-file` Parameter wird geändert und auf gesetzt `manual`.
- Die `continuously-available` Freigabeeigenschaft wird der Freigabe hinzugefügt.
- Die `oplocks` Share-Eigenschaft befindet sich bereits in der Liste der Share-Eigenschaften. Sie muss daher nicht hinzugefügt werden.
- Die `attributecache` Freigabeeigenschaft wird aus der Freigabe entfernt.
- Die `browsable` Share-Eigenschaft ist optional für einen kontinuierlich verfügbaren Share, der für NDOS mit Anwendungsservern über SMB verwendet wird, und wird als eine der Share-Eigenschaften beibehalten.

```
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
```

Aktivieren oder Deaktivieren von VSS-Schattenkopien für Hyper-V über SMB-Backups

Wenn Sie eine VSS-kompatible Backup-Applikation zur Sicherung von Dateien der Hyper-V Virtual Machine verwenden, die auf SMB Shares gespeichert sind, muss VSS Shadow Copy aktiviert sein. Sie können die VSS-Schattenkopie deaktivieren, wenn Sie keine VSS-kompatiblen Backup-Anwendungen verwenden. Die Standardeinstellung besteht darin, die VSS-Schattenkopie zu aktivieren.

Über diese Aufgabe

Sie können VSS-Schattenkopien jederzeit aktivieren oder deaktivieren.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Führen Sie eine der folgenden Aktionen aus:

Wenn VSS Shadow Kopien sein sollen…	Geben Sie den Befehl ein…
Aktiviert	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true`**
Deaktiviert	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false`**

3. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Beispiel

Mit den folgenden Befehlen lassen sich VSS-Schattenkopien auf SVM vs1 aktivieren:

```
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
```

Verwenden Sie Statistiken, um Hyper-V und SQL Server über SMB-Aktivitäten zu überwachen

Legen Sie fest, welche Statistikobjekte und Zähler in ONTAP zur Verfügung stehen

Bevor Informationen über CIFS, SMB, Auditing und BranchCache Hash-Statistiken und die Performance überwacht werden können, müssen Unternehmen wissen, welche Objekte und Zähler verfügbar sind, von denen sie Daten beziehen können.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Sie können ermitteln, ob…	Eingeben…
Welche Objekte sind verfügbar	`statistics catalog object show`
Verfügbare spezifische Objekte	`statistics catalog object show -object` *`object_name`*
Welche Zähler stehen zur Verfügung	`statistics catalog counter show -object` *`object_name`*

   Erfahren Sie mehr über `statistics catalog object show` Und `statistics catalog counter show` im "ONTAP-Befehlsreferenz" .

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Beispiele

Mit dem folgenden Befehl werden Beschreibungen ausgewählter Statistikobjekte angezeigt, die mit dem CIFS- und SMB-Zugriff im Cluster in Verbindung stehen, wie sie auf der erweiterten Berechtigungsebene angezeigt werden:

```
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
```

Mit dem folgenden Befehl werden Informationen zu einigen der Zähler für das `cifs` Objekt angezeigt, die auf der erweiterten Berechtigungsebene angezeigt werden:

> In diesem Beispiel werden nicht alle verfügbaren Zähler für das `cifs` Objekt angezeigt; die Ausgabe wird abgeschnitten.

```
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


[...]
```

Erfahren Sie mehr über `statistics start` in der "ONTAP-Befehlsreferenz".

Zeigt SMB-Statistiken in ONTAP an

Sie können verschiedene SMB-Statistiken anzeigen, um die Performance zu überwachen und Probleme zu diagnostizieren.

Schritte

1. Verwenden Sie die `statistics start` `statistics stop` Befehle und optional, um ein Datenbeispiel zu erfassen.
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie Statistiken anzeigen möchten für…	Geben Sie den folgenden Befehl ein…
Alle SMB-Versionen	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x und SMB 3.0	**`statistics show -object smb2`**
SMB-Subsystem des Node	**`statistics show -object nblade_cifs`**

Verwandte Informationen

- "Statistiken zeigen"
- "Statistikstart"
- "Statistikstopp"

Vergewissern Sie sich, dass die Konfiguration einen unterbrechungsfreien Betrieb ermöglicht

Bestimmen Sie mithilfe der Statusüberwachung, ob der Status des unterbrechungsfreien Betriebs ordnungsgemäß ist

Das Systemzustandsüberwachungs-Tool bietet Informationen zum Systemzustand im gesamten Cluster. Die Systemzustandsüberwachung überwacht Hyper-V und SQL Server over SMB Konfigurationen, um einen unterbrechungsfreien Betrieb (NDOS) für die Applikations-Server zu gewährleisten. Wenn der Status „beeinträchtigt“ lautet, können Sie Details zum Problem anzeigen, einschließlich der wahrscheinlichen Ursache und der empfohlenen Wiederherstellungsmaßnahmen.

Es gibt mehrere Integritätsmonitore. ONTAP überwacht sowohl den gesamten Systemzustand als auch den Systemzustand für einzelne Systemzustandmonitore. Die Node-Systemzustandsüberwachung enthält das CIFS-NDO-Subsystem. Die Überwachung verfügt über eine Reihe von Integritätsrichtlinien, mit denen Warnungen ausgelöst werden, wenn bestimmte physische Bedingungen zu Unterbrechungen führen können, und wenn ein störender Zustand vorhanden ist, werden Warnmeldungen erzeugt und Informationen zu Korrekturmaßnahmen angezeigt. Für den unterbrechungsfreien Betrieb über SMB-Konfigurationen werden Warnmeldungen für die beiden folgenden Bedingungen generiert:

Alarm-ID	Schweregrad	Zustand
HaNotReadyCifsNdo_Alert	Major	Eine oder mehrere Dateien, die von einem Volume in einem Aggregat auf dem Node gehostet werden, wurden durch eine kontinuierlich verfügbare SMB-Freigabe geöffnet, die im Falle eines Ausfalls Persistenz verspricht. Die HA-Beziehung zum Partner ist jedoch entweder nicht konfiguriert oder nicht in einem ordnungsgemäßen Zustand.
NoStandbyLifCifsNdo_Alert	Gering	Die Storage Virtual Machine (SVM) stellt Daten über SMB aktiv über einen Node bereit. SMB-Dateien werden dauerhaft über kontinuierlich verfügbare Freigaben geöffnet, während der Partner-Node jedoch keine aktiven Daten-LIFs für die SVM offenlegt.

Anzeigen des unterbrechungsfreien Betriebs mithilfe der Monitoring des Systemzustands

Sie können die `system health` Befehle verwenden, um Informationen zum allgemeinen Systemzustand des Clusters und zum Systemzustand des CIFS-NDO-Subsystems anzuzeigen, auf Meldungen zu reagieren, zukünftige Warnmeldungen zu konfigurieren und Informationen zur Konfiguration des Systemzustands-Monitorings anzuzeigen.

Schritte

1. Überwachen Sie den Systemzustand, indem Sie die entsprechende Aktion durchführen:

Sie möchten Folgendes anzeigen:	Geben Sie den Befehl ein…
Der Integritätsstatus des Systems, der den Gesamtstatus einzelner Integritätsmonitore wiedergibt	**system health status show**
Informationen zum Systemzustand des CIFS-NDO-Subsystems	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Zeigen Sie Informationen zum Konfigurieren der CIFS-NDO-Alarmüberwachung durch Ausführen der entsprechenden Aktionen an:

Wenn Sie Informationen über… anzeigen möchten	Geben Sie den Befehl ein…
Konfiguration und Status der Systemzustandsüberwachung für das CIFS-NDO-Subsystem, z. B. überwachte Nodes, Initialisierungsstatus und Status	**system health config show -subsystem CIFS-NDO**
Die CIFS-NDO-Warnungen, die von einer Systemzustandsüberwachung potenziell generiert werden können	**system health alert definition show -subsystem CIFS-NDO**
CIFS-NDO-Richtlinien zur Systemzustandsüberwachung, die bestimmen, wann Warnmeldungen ausgegeben werden	**system health policy definition show -monitor node-connect**

Verwenden Sie den `-instance` Parameter, um detaillierte Informationen anzuzeigen.

Beispiele

In der folgenden Ausgabe werden Informationen zum Gesamtstatus des Clusters und des CIFS-NDO-Subsystems angezeigt:

```
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
```

In der folgenden Ausgabe werden ausführliche Informationen zur Konfiguration und zum Status der Systemzustandsüberwachung des CIFS-NDO-Subsystems angezeigt:

```
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
```

Überprüfen Sie die kontinuierlich verfügbare Konfiguration der SMB-Freigaben

Zur Unterstützung eines unterbrechungsfreien Betriebs müssen Hyper-V und SQL Server SMB-Freigaben als kontinuierlich verfügbare Freigaben konfiguriert werden. Darüber hinaus gibt es bestimmte andere Freigabeinstellungen, die Sie überprüfen müssen. Sie sollten überprüfen, ob die Freigaben ordnungsgemäß konfiguriert sind, um einen unterbrechungsfreien Betrieb für die Applikations-Server sicherzustellen, falls geplante oder ungeplante Unterbrechungen vorliegen.

Über diese Aufgabe

Sie müssen überprüfen, ob die beiden folgenden Freigabeparameter richtig eingestellt sind:

- Der `-offline-files` Parameter ist entweder auf `manual` (Standard) oder auf eingestellt `none`.
- Symlinks müssen deaktiviert sein.

Für einen ordnungsgemäßen unterbrechungsfreien Betrieb müssen die folgenden Freigabeigenschaften festgelegt werden:

- `continuously-available`
- `oplocks`

Die folgenden Freigabeigenschaften dürfen nicht festgelegt werden:

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

Schritte

1. Stellen Sie sicher, dass die Offline-Dateien auf `manual` oder eingestellt `disabled` sind und dass Symlinks deaktiviert sind:

   vserver cifs shares show -vserver *vserver_name*

2. Vergewissern Sie sich, dass die SMB-Freigaben für kontinuierliche Verfügbarkeit konfiguriert sind:

   vserver cifs shares properties show -vserver *vserver_name*

Beispiele

Im folgenden Beispiel wird die Share-Einstellung für einen Share mit dem Namen „`share1`“ auf Storage Virtual Machine (SVM, früher als Vserver bezeichnet) vs1 angezeigt. Offline-Dateien werden auf gesetzt `manual` und Symlinks sind deaktiviert (durch einen Bindestrich in der `Symlink Properties` Feldausgabe gekennzeichnet):

```
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
```

Im folgenden Beispiel werden die Share-Eigenschaften für eine Freigabe mit dem Namen „`share1`“ auf SVM vs1 angezeigt:

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

LIF-Status überprüfen

Selbst wenn Sie Storage Virtual Machines (SVMs) mit Hyper-V und SQL Server über SMB-Konfigurationen konfigurieren, um LIFs auf jedem Node in einem Cluster zu nutzen, während des täglichen Betriebs verschieben einige LIFs möglicherweise zu Ports auf einem anderen Node. Sie müssen den LIF-Status überprüfen und erforderliche Korrekturmaßnahmen ergreifen.

Über diese Aufgabe

Um einen nahtlosen, unterbrechungsfreien Betrieb zu ermöglichen, muss jeder Node in einem Cluster mindestens eine logische Schnittstelle für die SVM haben. Dabei müssen alle LIFs einem Home-Port zugeordnet sein. Wenn einige der konfigurierten LIFs derzeit nicht mit ihrem Home-Port verknüpft sind, müssen Sie beliebige Port-Probleme beheben und die LIFs anschließend auf ihren Home-Port zurücksetzen.

Schritte

1. Informationen zu konfigurierten LIFs für die SVM anzeigen:

   network interface show -vserver *vserver_name*

In diesem Beispiel befindet sich „`lif1`“ nicht auf dem 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
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

2. Wenn sich einige der LIFs nicht auf ihren Home-Ports befinden, führen Sie die folgenden Schritte aus:

   a. Bestimmen Sie für jede LIF, was der Home Port des LIF ist:

      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. Bestimmen Sie für jede LIF, ob der Home Port des LIF aktiv ist:

      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 diesem Beispiel sollte „`lif1`“ zurück zu seinem Heimathafen migriert werden, `node1:e0d`.

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

3. Wenn eine der Home Port-Netzwerkschnittstellen, denen die LIFs zugeordnet sein sollten `up`, nicht im Status sind, lösen Sie das Problem, damit diese Schnittstellen verfügbar sind. Erfahren Sie mehr über `up`

in der "ONTAP-Befehlsreferenz".

4. Setzen Sie bei Bedarf die LIFs auf ihre Home-Ports zurück:

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

   network interface revert -vserver vs1 -lif lif1

   Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".

5. Überprüfen Sie, ob jeder Node im Cluster über eine aktive LIF für die SVM verfügt:

   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
```

Ermitteln Sie, ob SMB-Sitzungen kontinuierlich verfügbar sind

Zeigt SMB-Sitzungsinformationen an

Sie können Informationen zu festgelegten SMB-Sitzungen anzeigen, einschließlich der SMB-Verbindung und der Sitzungs-ID sowie der IP-Adresse der Workstation über die Sitzung. Sie können Informationen zur SMB-Protokollversion der Sitzung und zum kontinuierlich verfügbaren Sicherungslevel anzeigen, sodass Sie leichter feststellen können, ob die Session den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen zu allen Sitzungen Ihrer SVM in zusammengefassener Form anzeigen. In vielen Fällen ist jedoch die Menge der zurückgegebenen Ausgabe groß. Sie können die in der Ausgabe angezeigten Informationen anpassen, indem Sie optionale Parameter angeben:

- Mit dem optionalen `-fields` Parameter können Sie die Ausgabe der ausgewählten Felder anzeigen.

  Sie können eingeben `-fields ?`, um festzulegen, welche Felder Sie verwenden können.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen zu etablierten SMB-Sitzungen anzuzeigen.

- Sie können den `-fields` Parameter oder den `-instance` Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	**Geben Sie den folgenden Befehl ein…**
Für alle Sitzungen auf der SVM in Übersichtsform	**vserver cifs session show -vserver *vserver_name***
Bei einer angegebenen Verbindungs-ID	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
Von einer angegebenen IP-Adresse der Workstation	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Auf einer angegebenen LIF-IP-Adresse	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Auf einem angegebenen Node	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	Von einem angegebenen Windows-Benutzer
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* Das Format für `user_name` ist `[domain]\user`.	Mit einem angegebenen Authentifizierungsmechanismus

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism Der Wert für `-auth -mechanism` kann einer der folgenden Werte sein: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Mit einer angegebenen Protokollversion

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version` Der Wert für `-protocol-version` kann einer der folgenden Werte sein: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Mit einem festgelegten Maß an kontinuierlich verfügbarem Schutz

Wenn Sie SMB-Sitzungsinformationen anzeigen möchten…	Geben Sie den folgenden Befehl ein…
`vserver cifs session show -vserver vserver_name -continuously -available continuously_available_protection_level` Der Wert für `-continuously -available` kann einer der folgenden Werte sein: • `No` • `Yes` • `Partial` Wenn der Status „kontinuierlich verfügbar `Partial`“ lautet, bedeutet dies, dass die Sitzung mindestens eine offene kontinuierlich verfügbare Datei enthält, die Sitzung jedoch einige Dateien enthält, die nicht mit kontinuierlich verfügbarem Schutz geöffnet	Mit einem angegebenen SMB Signing Session Status

Beispiele

Mit dem folgenden Befehl werden die Sitzungsinformationen für die Sitzungen auf SVM vs1 angezeigt, die von einer Workstation mit der IP-Adresse 10.1.1.1 eingerichtet wurden:

```
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
```

Mit dem folgenden Befehl werden ausführliche Sitzungsinformationen für Sitzungen mit kontinuierlich verfügbarem Schutz für SVM vs1 angezeigt. Die Verbindung wurde über das Domain-Konto hergestellt.

```
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
```

Mit dem folgenden Befehl werden Sitzungsinformationen zu einer Sitzung mit SMB 3.0 und SMB Multichannel in SVM vs1 angezeigt. Im Beispiel hat der Benutzer über einen SMB 3.0-fähigen Client mithilfe der LIF-IP-Adresse eine Verbindung zu dieser Freigabe hergestellt. Daher wurde der Authentifizierungsmechanismus standardmäßig auf NTLMv2 festgelegt. Die Verbindung muss über die Kerberos-Authentifizierung hergestellt

werden, um eine Verbindung mit kontinuierlich verfügbarem Schutz herzustellen.

```
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
```

Zeigt Informationen zu geöffneten SMB-Dateien in ONTAP an

Sie können Informationen zu offenen SMB-Dateien anzeigen, einschließlich SMB-Verbindung und Session-ID, Hosting-Volume, Share-Name und Freigabepfad. Sie können auch Informationen zum kontinuierlich verfügbaren Sicherungsniveau einer Datei anzeigen. So können Sie herausfinden, ob sich eine offene Datei in einem Zustand befindet, der den unterbrechungsfreien Betrieb unterstützt.

Über diese Aufgabe

Sie können Informationen über offene Dateien in einer festgelegten SMB-Sitzung anzeigen. Die angezeigten Informationen sind nützlich, wenn Sie SMB-Sitzungsinformationen für bestimmte Dateien innerhalb einer SMB-Sitzung bestimmen müssen.

Wenn Sie zum Beispiel eine SMB-Sitzung haben, in der einige der geöffneten Dateien mit kontinuierlich verfügbarem Schutz geöffnet sind und einige nicht mit kontinuierlich verfügbarem Schutz geöffnet sind (der Wert für das `-continuously-available` Feld in der `vserver cifs session show` Befehlsausgabe ist `Partial`), können Sie mit diesem Befehl bestimmen, welche Dateien nicht kontinuierlich verfügbar sind.

Sie können Informationen für alle offenen Dateien in festgelegten SMB-Sitzungen auf Storage Virtual Machines (SVMs) in zusammengefasster Form anzeigen, indem Sie den `vserver cifs session file show` Befehl ohne optionale Parameter verwenden.

In vielen Fällen ist jedoch die zurückgegebene Menge an Output groß. Sie können die in der Ausgabe angezeigten Informationen durch optionale Parameter anpassen. Dies kann hilfreich sein, wenn Sie Informationen nur für einen kleinen Teil der offenen Dateien anzeigen möchten.

- Sie können den optionalen `-fields` Parameter verwenden, um die Ausgabe in den ausgewählten Feldern anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

- Sie können den `-instance` Parameter verwenden, um detaillierte Informationen über offene SMB-Dateien anzuzeigen.

  Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
Auf der SVM in Übersichtsform	**vserver cifs session file show -vserver *vserver_name***
Auf einem angegebenen Node	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Für eine angegebene Datei-ID
vserver cifs session file show -vserver *vserver_name* -file-id integer	Für eine angegebene SMB-Verbindungs-ID
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Für eine angegebene SMB-Session-ID
vserver cifs session file show -vserver *vserver_name* -session-id integer	Auf dem angegebenen Hosting-Aggregat
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	Auf dem angegebenen Volume
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	In der angegebenen SMB-Freigabe

Wenn Sie öffnen SMB-Dateien anzeigen möchten…	Geben Sie den folgenden Befehl ein…
vserver cifs session file show -vserver *vserver_name* -share *share_name*	Auf dem angegebenen SMB-Pfad
vserver cifs session file show -vserver *vserver_name* -path *path*	Mit der angegebenen Stufe des kontinuierlichen verfügbaren Schutzes
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* Der Wert für `-continuously-available` kann einer der folgenden Werte sein: • `No` • `Yes` Wenn der Status „kontinuierlich verfügbar `No`“ lautet, bedeutet dies, dass diese offenen Dateien nicht unterbrechungsfrei nach Takeover und Giveback wiederhergestellt werden können. Sie sind auch bei der allgemeinen Aggregatverschiebung zwischen den Partnern in einer Hochverfügbarkeitbeziehung nicht wiederherstellbar.	Mit dem angegebenen Status „erneut verbunden“

Es gibt weitere optionale Parameter, mit denen Sie die Ausgabeergebnisse verfeinern können. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Beispiele

Im folgenden Beispiel werden Informationen über offene Dateien auf SVM vs1 angezeigt:

```
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
```

Im folgenden Beispiel werden ausführliche Informationen über offene SMB-Dateien mit der Datei-ID 82 auf SVM vs1 angezeigt:

```
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
```