



Konfigurationsanforderungen und Überlegungen

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap/smb-hyper-v-sql/licensing-requirements-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

Inhalt

Konfigurationsanforderungen und Überlegungen	1
ONTAP- und Lizenzierungsanforderungen	1
Anforderungen an die ONTAP-Version	1
Lizenzierungsanforderungen	1
Anforderungen an Netzwerk und LIF-Daten	1
Anforderungen an Netzwerkprotokolle	2
Anforderungen an Daten-LIF	2
SMB-Server- und Volume-Anforderungen für Hyper-V über SMB	2
Anforderungen an SMB-Server	3
Volume-Anforderungen	3
SMB-Server- und Volume-Anforderungen für SQL Server über SMB	4
Anforderungen an SMB-Server	4
Volume-Anforderungen	4
Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für Hyper-V über SMB	5
Share-Anforderungen	5
Überlegungen	6
Kontinuierlich verfügbare Share-Anforderungen und Überlegungen für SQL Server über SMB	6
Share-Anforderungen	6
Überlegungen teilen	7
Überlegungen zu Remote VSS für Hyper-V über SMB-Konfigurationen	7
Allgemeine Überlegungen zu Remote VSS	7
Überlegungen zu Remote-VSS, die nur für Schattenkopien mit automatischem Recovery gelten	8
Offloaded Data Transfer von ODX für SQL Server und Hyper-V über SMB	8

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 über 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 Virensan 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 über 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.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGliche EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.