



Microsoft Hyper-V 和 SQL Server 的 SMB 配置 ONTAP 9

NetApp
September 12, 2024

目录

Microsoft Hyper-V 和 SQL Server 的 SMB 配置	1
Microsoft Hyper-V 和 SQL Server 的 SMB 配置概述	1
配置基于 SMB 的适用于 Microsoft Hyper-V 和 SQL Server 的 ONTAP 解决方案	1
通过 SMB 实现 Hyper-V 和 SQL Server 无中断运行	2
使用远程 VSS 进行基于共享的备份	6
如何通过 SMB 共享在 Hyper-V 和 SQL Server 中使用 ODX 副本卸载	9
配置要求和注意事项	10
针对 SQL Server 和基于 SMB 的 Hyper-V 配置的建议	17
规划基于 SMB 的 Hyper-V 或 SQL Server 配置	17
创建 ONTAP 配置，以便通过 SMB 使用 Hyper-V 和 SQL Server 实现无中断运行	21
通过 SMB 配置管理 Hyper-V 和 SQL Server	34
使用统计信息通过 SMB 监控 Hyper-V 和 SQL Server 活动	37
验证此配置是否能够无中断运行	41

Microsoft Hyper-V 和 SQL Server 的 SMB 配置

Microsoft Hyper-V 和 SQL Server 的 SMB 配置概述

通过 ONTAP 功能，您可以通过 SMB 协议为 Microsoft Hyper-V 和 Microsoft SQL Server 这两个 Microsoft 应用程序启用无中断运行。

如果要在以下情况下实施 SMB 无中断操作，应使用以下过程：

- 已配置基本 SMB 协议文件访问。
- 您希望启用 SVM 中的 SMB 3.0 或更高版本文件共享以存储以下对象：
 - Hyper-V 虚拟机文件
 - SQL Server 系统数据库

相关信息

有关 ONTAP 技术以及与外部服务交互的追加信息，请参见以下技术报告 (TRs)： * ["NetApp 技术报告 4172：《基于 SMB 3.0 的 Microsoft Hyper-V 与 ONTAP 最佳实践》"](#) * ["NetApp 技术报告 4369：《采用集群模式 Data ONTAP 的 Microsoft SQL Server 和 SnapManager 7.2 for SQL Server 最佳实践》"](#)

配置基于 SMB 的适用于 Microsoft Hyper-V 和 SQL Server 的 ONTAP 解决方案

您可以使用持续可用的 SMB 3.0 及更高版本的文件共享将 Hyper-V 虚拟机文件或 SQL Server 系统数据库和用户数据库存储在 SVM 中的卷上，同时为计划内和计划外事件提供无中断运行（NDO）。

基于 SMB 的 Microsoft Hyper-V

要创建基于 SMB 解决方案的 Hyper-V，必须先配置 ONTAP，以便为 Microsoft Hyper-V 服务器提供存储服务。此外，您还必须配置 Microsoft 集群（如果使用集群配置），Hyper-V 服务器，与 CIFS 服务器托管的共享的持续可用 SMB 3.0 连接以及备份服务（可选），以保护存储在 SVM 卷上的虚拟机文件。



Hyper-V 服务器必须在 Windows 2012 Server 或更高版本上进行配置。独立和集群 Hyper-V 服务器配置均受支持。

- 有关创建 Microsoft 集群和 Hyper-V 服务器的信息，请参见 Microsoft 网站。
- SnapManager for Hyper-V 是一款基于主机的应用程序，可用于提供基于 Snapshot 副本的快速备份服务，旨在与基于 SMB 的 Hyper-V 配置集成。

有关将 SnapManager 与基于 SMB 的 Hyper-V 配置结合使用的信息，请参见 [_Hyper-V SnapManager 安装和管理指南_](#)。

基于 SMB 的 Microsoft SQL Server

要通过 SMB 解决方案创建 SQL Server，必须先配置 ONTAP，以便为 Microsoft SQL Server 应用程序提供存储服务。此外，您还必须配置 Microsoft 集群（如果使用的是集群配置）。然后，您可以在 Windows 服务器上安装和配置 SQL Server，并创建持续可用的 SMB 3.0 连接以连接到 CIFS 服务器托管的共享。您可以选择配置备份服务来保护存储在 SVM 卷上的数据库文件。



必须在 Windows 2012 Server 或更高版本上安装和配置 SQL Server。独立配置和集群配置均受支持。

- 有关创建 Microsoft 集群以及安装和配置 SQL Server 的信息，请参见 Microsoft 网站。
- 适用于 Microsoft SQL Server 的 SnapCenter 插件是一款基于主机的应用程序、它有助于提供基于 Snapshot 副本的快速备份服务、旨在通过 SMB 配置与 SQL Server 集成。

有关使用适用于 Microsoft SQL Server 的 SnapCenter 插件的信息、请参见 ["适用于 Microsoft SQL Server 的 SnapCenter 插件"](#) 文档

通过 SMB 实现 Hyper-V 和 SQL Server 无中断运行

Hyper-V 和基于 SMB 的 SQL Server 无中断运行的含义

Hyper-V 和基于 SMB 的 SQL Server 无中断运行是指通过这些功能的组合，可以使应用程序服务器和包含的虚拟机或数据库保持联机状态，并在执行多项管理任务期间提供持续可用性。这包括存储基础架构的计划内和计划外停机。

支持通过 SMB 对应用程序服务器执行无中断操作的操作包括：

- 计划内接管和交还
- 计划外接管
- 升级
- 计划内聚合重新定位（ARL）
- LIF 迁移和故障转移
- 计划内卷移动

支持通过 SMB 实现无中断操作的协议

随着 SMB 3.0 的发布，Microsoft 发布了新协议，以提供必要的功能，支持通过 SMB 对 Hyper-V 和 SQL Server 执行无中断操作。

ONTAP 在通过 SMB 为应用程序服务器提供无中断运行时使用以下协议：

- SMB 3.0
- 见证

有关基于 SMB 的 Hyper-V 和 SQL Server 无中断运行的关键概念

在通过 SMB 解决方案配置 Hyper-V 或 SQL Server 之前，您应了解有关无中断运行（NDOS）的某些概念。

- * 持续可用共享 *

设置了持续可用共享属性的 SMB 3.0 共享。通过持续可用的共享进行连接的客户端可以在接管，交还和聚合重新定位等中断事件发生后继续运行。

- 节点

作为集群成员的单个控制器。为了区分 SFO 对中的两个节点，一个节点有时称为 *local node*，另一个节点有时称为 *partner node* 或 *remote node*。存储的主所有者是本地节点。辅助所有者是配对节点，在主所有者出现故障时控制存储。每个节点都是其存储的主所有者，也是其配对节点存储的二级所有者。

- * 无中断聚合重新定位 *

能够在集群中 SFO 对内的配对节点之间移动聚合，而不会中断客户端应用程序。

- * 无中断故障转移 *

请参见 *Takeover*。

- * 无中断 LIF 迁移 *

能够执行 LIF 迁移，而不会中断通过 LIF 连接到集群的客户端应用程序。对于 SMB 连接，只有使用 SMB 2.0 或更高版本进行连接的客户端才可以执行此操作。

- * 无中断运行 *。

能够执行主要的 ONTAP 管理和升级操作，并在不中断客户端应用程序的情况下承受节点故障。此术语指的是从整体上收集的无中断接管，无中断升级和无中断迁移功能。

- * 无中断升级 *

能够在不中断应用程序的情况下升级节点硬件或软件。

- * 无中断卷移动 *

可以在整个集群中自由移动卷，而不会中断正在使用该卷的任何应用程序。对于 SMB 连接，所有版本的 SMB 都支持无中断卷移动。

- * 持久性句柄 *

SMB 3.0 的一个属性，允许持续可用的连接在断开连接时透明地重新连接到 CIFS 服务器。与持久句柄类似，在与连接客户端的通信丢失后，CIFS 服务器会将永久性句柄保留一段时间。但是，持久句柄比持久句柄更具弹性。在重新连接后，除了让客户端有机会在 60 秒的窗口内回收句柄之外，CIFS 服务器还会在该 60 秒窗口期间拒绝访问请求访问文件的任何其他客户端。

有关永久性句柄的信息会镜像到 SFO 配对节点的永久性存储上，这样，在 SFO 配对节点接管节点存储所有的事件发生后，具有已断开永久性句柄的客户端可以回收此持久句柄。除了在发生 LIF 移动时提供无中断操作（持久处理支持）之外，永久性句柄还可为接管，交还和聚合重新定位提供无中断操作。

- * SFO 交还 *

从接管事件中恢复时，将聚合返回到其主位置。

- * SFO 对 *

一对节点，其控制器已配置为在其中一个节点停止运行时彼此提供数据。根据系统型号，两个控制器可以位于一个机箱中，也可以位于不同的机箱中。在双节点集群中称为 HA 对。

- * 接管 *

当存储的主所有者出现故障时，配对节点控制存储的过程。在 SFO 环境下，故障转移和接管是同义词。

SMB 3.0 功能如何支持通过 SMB 共享进行无中断操作

SMB 3.0 提供了关键功能，支持通过 SMB 共享对 Hyper-V 和 SQL Server 执行无中断操作。其中包括 continuously-available 共享属性和一种称为 _PER 持式句柄_ 的文件句柄类型、该句柄允许 SMB 客户端回收文件打开状态并透明地重新建立 SMB 连接。

对于连接到具有持续可用共享属性集的共享的支持 SMB 3.0 的客户端，可以将永久性句柄授予这些客户端。如果 SMB 会话已断开连接，则 CIFS 服务器会保留有关永久性句柄状态的信息。在允许客户端重新连接的 60 秒期间，CIFS 服务器会阻止其他客户端请求，从而允许具有永久性句柄的客户端在网络断开连接后回收句柄。具有永久性句柄的客户端可以使用 Storage Virtual Machine (SVM) 上的一个数据 LIF 进行重新连接，方法是通过同一个 LIF 或不同的 LIF 进行重新连接。

聚合重新定位，接管和交还都发生在 SFO 对之间。为了无缝管理具有永久性句柄的文件的会话断开连接和重新连接，配对节点会维护一份所有永久性句柄锁定信息的副本。无论是计划内事件还是计划外事件，SFO 配对节点都可以无中断地管理永久性句柄重新连接。利用这一新功能，与 CIFS 服务器的 SMB 3.0 连接可以透明，无中断地故障转移到传统中断事件中分配给 SVM 的另一个数据 LIF。

尽管使用永久性句柄可以使 CIFS 服务器透明地对 SMB 3.0 连接进行故障转移，但如果故障导致 Hyper-V 应用程序故障转移到 Windows Server 集群中的另一个节点，则客户端无法回收这些已断开的句柄的文件句柄。在这种情况下，如果 Hyper-V 应用程序在其他节点上重新启动，处于 Disconnected 状态的文件句柄可能会阻止其访问。"故障转移集群"是 SMB 3.0 的一部分，可通过提供一种机制来使陈旧的冲突句柄失效来解决此情形。通过这种机制，Hyper-V 集群可以在 Hyper-V 集群节点出现故障时快速恢复。

见证协议如何增强透明故障转移

见证协议为 SMB 3.0 持续可用的共享 (CA 共享) 提供增强的客户端故障转移功能。见证有助于加快故障转移速度，因为它会绕过 LIF 故障转移恢复期间。当节点不可用时，它会通知应用程序服务器，而无需等待 SMB 3.0 连接超时。

故障转移是无缝的，客户端上运行的应用程序不会意识到发生了故障转移。如果见证不可用，则故障转移操作仍会成功执行，但无见证的故障转移效率较低。

满足以下要求时，可以执行见证增强型故障转移：

- 它只能用于启用了 SMB 3.0 的支持 SMB 3.0 的 CIFS 服务器。
- 共享必须使用 SMB 3.0 并设置了持续可用性共享属性。

- 应用程序服务器所连接节点的 SFO 配对节点必须至少为托管应用程序服务器数据的 Storage Virtual Machine （ SVM ） 分配一个运行数据 LIF 。



见证协议在 SFO 对之间运行。由于 LIF 可以迁移到集群中的任何节点，因此任何节点都可能成为其 SFO 配对节点的见证。如果托管应用程序服务器数据的 SVM 在配对节点上没有活动数据 LIF，则见证协议无法为给定节点上的 SMB 连接提供快速故障转移。因此，对于托管其中一种配置的每个 SVM，集群中的每个节点必须至少具有一个数据 LIF。

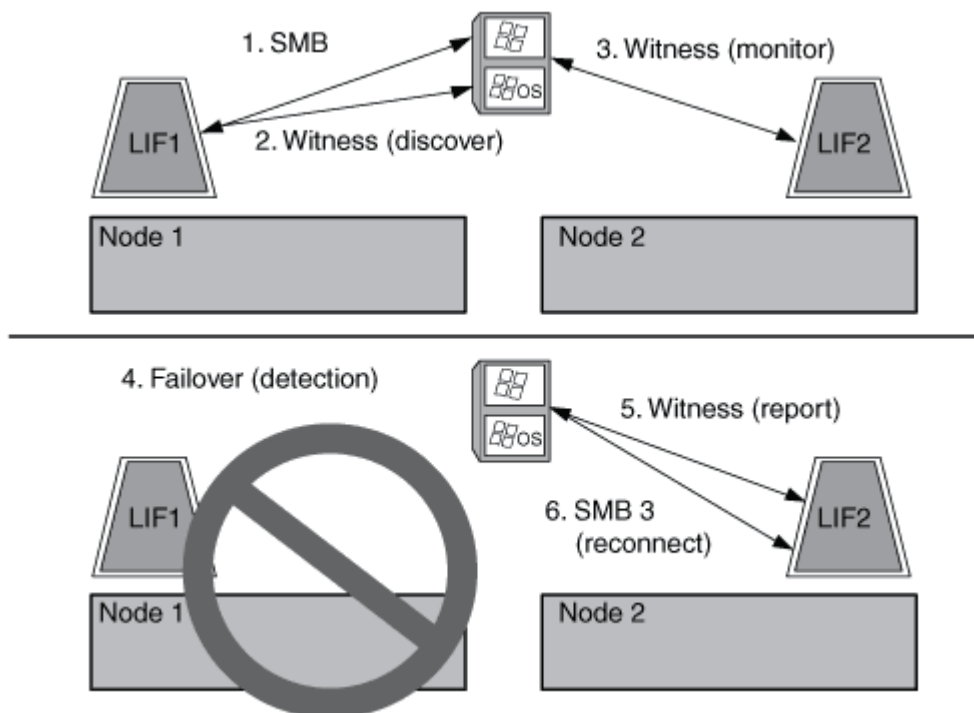
- 应用程序服务器必须使用存储在 DNS 中的 CIFS 服务器名称来连接到 CIFS 服务器，而不是使用单个 LIF IP 地址。

见证协议的工作原理

ONTAP 通过使用节点的 SFO 配对节点作为见证来实施见证协议。如果发生故障，配对节点会快速检测到故障并通知 SMB 客户端。

见证协议可通过以下过程提供增强的故障转移：

- 当应用程序服务器与 Node1 建立持续可用的 SMB 连接时，CIFS 服务器会通知应用程序服务器见证可用。
- 应用程序服务器从 Node1 请求见证服务器的 IP 地址，并接收分配给 Storage Virtual Machine （ SVM ） 的 Node2 （ SFO 配对节点）数据 LIF IP 地址列表。
- 应用程序服务器会选择一个 IP 地址，创建与 Node2 的见证连接，并注册以在 Node1 上持续可用的连接必须移动时收到通知。
- 如果 Node1 上发生故障转移事件，则见证者会协助处理故障转移事件，但不会涉及交还。
- 见证服务器检测故障转移事件，并通过见证连接通知应用程序服务器，SMB 连接必须移至 Node2。
- 应用程序服务器会将 SMB 会话移至 Node2，并在不中断客户端访问的情况下恢复连接。



使用远程 VSS 进行基于共享的备份

使用远程 VSS 进行基于共享的备份概述

您可以使用远程 VSS 对存储在 CIFS 服务器上的 Hyper-V 虚拟机文件执行基于共享的备份。

Microsoft 远程 VSS（卷影复制服务）是现有 Microsoft VSS 基础架构的扩展。借助远程 VSS，Microsoft 扩展了 VSS 基础架构，以支持 SMB 共享的卷影复制。此外，Hyper-V 等服务器应用程序可以将 VHD 文件存储在 SMB 文件共享上。通过这些扩展，可以为在共享上存储数据和配置文件的虚拟机创建应用程序一致的卷影副本。

远程 VSS 概念

您应了解一些必要的概念，以了解备份服务如何使用基于 SMB 的 Hyper-V 配置的远程 VSS（卷影复制服务）。

- * VSS（卷影复制服务） *

一种 Microsoft 技术，用于在特定时间点为特定卷上的数据创建备份副本或快照。VSS 可在数据服务器，备份应用程序和存储管理软件之间进行协调，以支持创建和管理一致的备份。

- * 远程 VSS（远程卷影复制服务） *

一项 Microsoft 技术，用于为在通过 SMB 3.0 共享访问数据的特定时间点处于数据一致状态的数据创建基于共享的备份副本。也称为 *Volume Shadow Copy Service*。

- * 卷影复制 *

共享中包含的一组重复数据，在定义明确的即时状态下运行。卷影副本用于为数据创建一致的时间点备份，从而使系统或应用程序能够继续更新原始卷上的数据。

- * 卷影复制集 *

一个或多个卷影副本的集合，其中每个卷影副本对应于一个共享。卷影副本集中的卷影副本表示必须在同一操作中备份的所有共享。启用了 VSS 的应用程序上的 VSS 客户端可确定要包含在卷影集中的卷影副本。

- * 卷影复制设置自动恢复 *

启用了 VSS 的远程备份应用程序的备份过程的一部分，其中包含卷影副本的副本目录在时间点上保持一致。备份开始时，应用程序上的 VSS 客户端会触发应用程序对计划备份的数据（Hyper-V 中的虚拟机文件）进行软件检查。然后，VSS 客户端允许应用程序继续运行。创建卷影副本集后，远程 VSS 会使卷影副本集可写，并将可写副本公开给应用程序。应用程序使用先前的软件检查点执行自动恢复，从而准备卷影副本集以进行备份。自动恢复会撤消自创建检查点以来对文件和目录所做的更改，从而使卷影副本处于一致状态。对于启用了 VSS 的备份，自动恢复是一个可选步骤。

- * 卷影复制 ID *

用于唯一标识卷影副本的 GUID。

- * 卷影复制集 ID *

一个 GUID，用于唯一标识一组卷影复制 ID 到同一服务器。

- * 适用于 Hyper-V 的 SnapManager *

一款可自动执行和简化 Microsoft Windows Server 2012 Hyper-V 备份和还原操作的软件 SnapManager for Hyper-V 使用具有自动恢复功能的远程 VSS 通过 SMB 共享备份 Hyper-V 文件。

相关信息

[有关基于 SMB 的 Hyper-V 和 SQL Server 无中断运行的关键概念](#)

[使用远程 VSS 进行基于共享的备份](#)

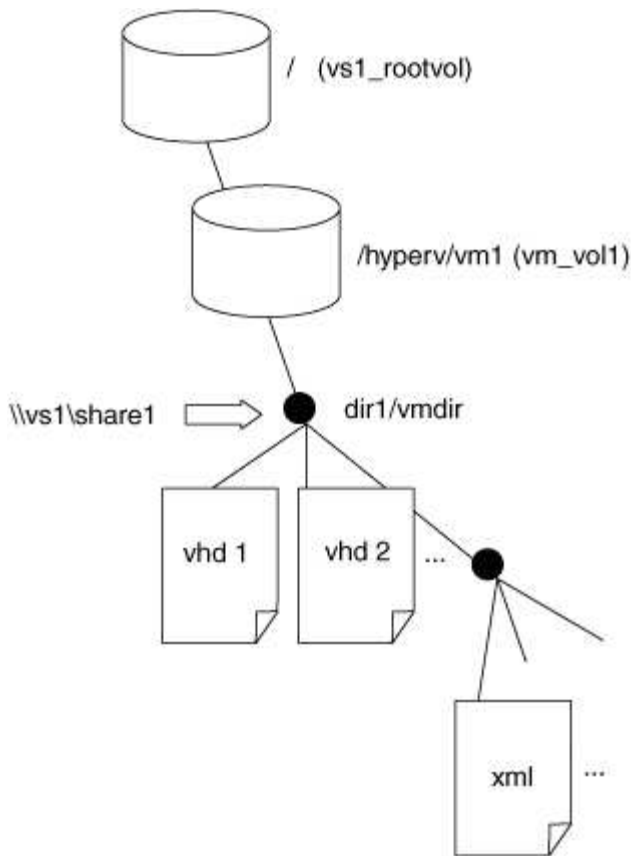
远程 VSS 使用的目录结构示例

远程 VSS 会在创建卷影副本时遍历存储 Hyper-V 虚拟机文件的目录结构。了解什么是合适的目录结构非常重要，这样您才能成功创建虚拟机文件的备份。

成功创建卷影副本所支持的目录结构符合以下要求：

- 用于存储虚拟机文件的目录结构中仅存在目录和常规文件。
目录结构不包含接合，链接或非常规文件。
- 虚拟机的所有文件都位于一个共享中。
- 用于存储虚拟机文件的目录结构不会超过卷影副本目录的已配置深度。
- 共享的根目录仅包含虚拟机文件或目录。

在下图中、创建了名为 vm_vol1 的卷、其中接合点位于 /hyperv/vml 在 Storage Virtual Machine (SVM) 的 VS1 上。包含虚拟机文件的子目录会在接合点下创建。Hyper-V 服务器的虚拟机文件通过具有路径的共享 1 进行访问 /hyperv/vml/dir1/vmdir。卷影复制服务会为共享 1 下的目录结构中包含的所有虚拟机文件创建卷影副本（直到卷影复制目录的已配置深度为止）。



SnapManager for Hyper-V 如何通过 SMB 管理 Hyper-V 基于 VSS 的远程备份

您可以使用 SnapManager for Hyper-V 管理基于 VSS 的远程备份服务。使用适用于 Hyper-V 的 SnapManager 托管备份服务创建节省空间的备份集具有一定优势。

Hyper-V 托管备份的 SnapManager 优化包括以下内容：

- SnapDrive 与 ONTAP 的集成可在发现 SMB 共享位置时实现性能优化。

ONTAP 为 SnapDrive 提供共享所在卷的名称。

- SnapManager for Hyper-V 指定卷影复制服务需要复制的 SMB 共享中的虚拟机文件列表。

通过提供目标虚拟机文件列表，卷影复制服务无需为共享中的所有文件创建卷影副本。

- Storage Virtual Machine （ SVM ）会保留 SnapManager for Hyper-V 的 Snapshot 副本以用于还原。

没有备份阶段。备份是节省空间的 Snapshot 副本。

SnapManager for Hyper-V 可通过以下过程为基于 SMB 的 HyperV 提供备份和还原功能：

1. 准备卷影复制操作

SnapManager for Hyper-V 应用程序的 VSS 客户端会设置卷影副本集。VSS 客户端收集有关卷影副本集中要包含的共享的信息，并将此信息提供给 ONTAP 。一个卷集可能包含一个或多个卷影副本，一个卷影副本对应于一个共享。

2. 创建卷影副本集（如果使用自动恢复）

对于卷影副本集中包含的每个共享，ONTAP 会创建一个卷影副本并使卷影副本可写。

3. 公开卷影副本集

在 ONTAP 创建卷影副本后，这些副本会公开到 SnapManager for Hyper-V 中，以便应用程序的 VSS 写入程序可以执行自动恢复。

4. 自动恢复卷影副本集

在创建卷影副本集期间，会有一段时间对备份集中的文件进行活动更改。应用程序的 VSS 写入程序必须更新卷影副本，以确保它们在备份之前处于完全一致的状态。



自动恢复的执行方式取决于应用程序。此阶段不涉及远程 VSS。

5. 完成并清理卷影副本集

VSS 客户端会在完成自动恢复后通知 ONTAP。卷影副本集将设为只读，然后准备好进行备份。使用 SnapManager for Hyper-V 进行备份时，Snapshot 副本中的文件将成为备份；因此，在备份阶段，系统会为包含备份集中共享的每个卷创建 Snapshot 副本。备份完成后，卷影副本集将从 CIFS 服务器中删除。

如何通过 SMB 共享在 Hyper-V 和 SQL Server 中使用 ODX 副本卸载

卸载数据传输（Offloaded Data Transfer，ODX）也称为 *copy offload*，可在兼容存储设备内部或之间直接传输数据，而无需通过主机计算机传输数据。通过 SMB 安装在应用程序服务器上执行复制操作时，ONTAP ODX 副本卸载功能可为您带来性能优势。

在非 ODX 文件传输中，将从源 CIFS 服务器读取数据，并通过网络传输到客户端计算机。客户端计算机通过网络将数据传输回目标 CIFS 服务器。总之，客户端计算机从源读取数据并将其写入目标。使用 ODX 文件传输时，数据会直接从源复制到目标。

由于 ODX 卸载副本是直接源存储和目标存储之间执行的，因此具有显著的性能优势。实现的性能优势包括：源和目标之间的复制时间更短，客户端上的资源利用率（CPU，内存）更低，网络 I/O 带宽利用率更低。

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

以下使用情形支持使用 ODX 副本和移动：

- 卷内

源文件或 LUN 与目标文件或 LUN 位于同一个卷中。

- 卷间，同一节点，同一 Storage Virtual Machine（SVM）

源文件或 LUN 和目标文件或 LUN 位于同一节点上的不同卷上。数据属于同一个 SVM。

- 卷间，不同节点，相同 SVM

源文件或 LUN 和目标文件或 LUN 位于不同节点上的不同卷上。数据属于同一个 SVM。

- SVM 间，同一节点

源和目标文件或 LUN 位于同一节点上的不同卷上。数据属于不同的 SVM。

- SVM 间，不同节点

源和目标文件或 LUN 位于不同节点上的不同卷上。数据属于不同的 SVM。

Hyper-V 解决方案中 ODX 副本卸载的具体使用情形包括：

- 您可以使用 ODX 副本卸载直通与 Hyper-V 在虚拟硬盘（VHD）文件内部或之间复制数据，或者在同一集群中映射的 SMB 共享和连接的 iSCSI LUN 之间复制数据。

这样，子操作系统中的副本就可以传递到底层存储。

- 创建固定大小的 VHD 时，ODX 用于使用众所周知的置零令牌以零初始化磁盘。
- 如果源存储和目标存储位于同一集群上，则使用 ODX 副本卸载进行虚拟机存储迁移。



要利用 Hyper-V ODX 副本卸载直通的使用情形，子操作系统必须支持 ODX，而子操作系统的磁盘必须是 SCSI 磁盘，并由支持 ODX 的存储（SMB 或 SAN）提供支持。子操作系统上的 IDE 磁盘不支持 ODX 直通。

SQL Server 解决方案中 ODX 副本卸载的具体使用情形包括：

- 您可以使用 ODX 副本卸载在映射的 SMB 共享之间或同一集群中的 SMB 共享和连接的 iSCSI LUN 之间导出和导入 SQL Server 数据库。
- 如果源存储和目标存储位于同一集群上，则 ODX 副本卸载用于数据库导出和导入。

配置要求和注意事项

ONTAP 和许可要求

在 SVM 上创建 SQL Server 或基于 SMB 的 Hyper-V 解决方案以实现无中断运行时，您需要了解某些 ONTAP 和许可要求。

ONTAP 版本要求

- 基于 SMB 的 Hyper-V

对于在 Windows 2012 或更高版本上运行的 Hyper-V，ONTAP 支持通过 SMB 共享进行无中断操作。

- 基于 SMB 的 SQL Server

对于在 Windows 2012 或更高版本上运行的 SQL Server 2012 或更高版本，ONTAP 支持通过 SMB 共享进行无中断操作。

有关通过 SMB 共享实现无中断操作所支持的 ONTAP，Windows Server 和 SQL Server 版本的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

许可要求

需要以下许可证：

- CIFS
- FlexClone（仅适用于基于 SMB 的 Hyper-V）

如果使用远程 VSS 进行备份，则需要此许可证。卷影复制服务使用 FlexClone 为文件创建时间点副本，然后在创建备份时使用这些副本。

如果您使用的备份方法不使用远程 VSS，则 FlexClone 许可证是可选的。

FlexClone 许可证包含在中 ["ONTAP One"](#)。如果您没有 ONTAP One，则应这样做 ["验证是否已安装所需的许可证"](#)，如有必要，["安装它们"](#)。

网络和数据 LIF 要求

在创建 SQL Server 或基于 SMB 的 Hyper-V 配置以实现无中断运行时，您需要了解特定的网络和数据 LIF 要求。

网络协议要求

- 支持 IPv4 和 IPv6 网络。
- 需要 SMB 3.0 或更高版本。

SMB 3.0 提供了创建持续可用的 SMB 连接所需的功能，以实现无中断运行。

- DNS 服务器必须包含将 CIFS 服务器名称映射到为 Storage Virtual Machine（SVM）上的数据 LIF 分配的 IP 地址的条目。

在访问虚拟机或数据库文件时，Hyper-V 或 SQL Server 应用程序服务器通常会通过多个数据 LIF 建立多个连接。为了正常运行，应用程序服务器必须使用 CIFS 服务器名称进行多个 SMB 连接，而不是与多个唯一 IP 地址建立多个连接。

见证还需要使用 CIFS 服务器的 DNS 名称，而不是单个 LIF IP 地址。

从 ONTAP 9.4 开始，您可以通过启用 SMB 多通道来提高基于 SMB 配置的 Hyper-V 和 SQL 服务器的吞吐量和容错能力。为此，您必须在集群和客户端上部署多个 1G，10G 或更大的 NIC。

数据 LIF 要求

- 通过 SMB 解决方案托管应用程序服务器的 SVM 必须在集群中的每个节点上至少具有一个可运行的数据 LIF。

SVM 数据 LIF 可以故障转移到集群中的其他数据端口，包括当前未托管应用程序服务器访问的数据的节

点。此外，由于见证节点始终是应用程序服务器所连接节点的 SFO 配对节点，因此集群中的每个节点都可能是见证节点。

- 不能将数据 LIF 配置为自动还原。

发生接管或交还事件后，您应手动将数据 LIF 还原到其主端口。

- 所有数据 LIF IP 地址都必须在 DNS 中有一个条目，并且所有条目都必须解析为 CIFS 服务器名称。

应用程序服务器必须使用 CIFS 服务器名称连接到 SMB 共享。您不能将应用程序服务器配置为使用 LIF IP 地址进行连接。

- 如果 CIFS 服务器名称与 SVM 名称不同，则 DNS 条目必须解析为 CIFS 服务器名称。

基于 SMB 的 Hyper-V 的 SMB 服务器和卷要求

在创建基于 SMB 的 Hyper-V 配置以实现无中断运行时，您需要了解特定的 SMB 服务器和卷要求。

SMB 服务器要求

- 必须启用 SMB 3.0。

默认情况下，此选项处于启用状态。

- 必须使用有效的 UNIX 用户帐户配置默认 UNIX 用户 CIFS 服务器选项。

应用程序服务器在创建 SMB 连接时使用计算机帐户。由于所有 SMB 访问都要求 Windows 用户成功映射到 UNIX 用户帐户或默认 UNIX 用户帐户，因此 ONTAP 必须能够将应用程序服务器的计算机帐户映射到默认 UNIX 用户帐户。

- 必须禁用自动节点转介（默认情况下，此功能处于禁用状态）。

如果要使用自动节点转介来访问 Hyper-V 计算机文件以外的数据，则必须为该数据创建单独的 SVM。

- SMB 服务器所属的域必须允许 Kerberos 和 NTLM 身份验证。

ONTAP 不会为远程 VSS 公布 Kerberos 服务；因此，应将域设置为允许 NTLM。

- 必须启用卷影复制功能。

默认情况下，此功能处于启用状态。

- 卷影复制服务在创建卷影副本时使用的 Windows 域帐户必须是 SMB 服务器本地 BUILTIN\Administrators 或 BUILTIN\Backup Operators 组的成员。

卷要求：

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

要使用持续可用的 SMB 连接为应用程序服务器提供 NDOS，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能通过

SMB 共享将其直接用于 NDOS 。如果您将混合安全模式卷更改为 NTFS 安全模式卷，并打算通过 SMB 共享将其用于 NDOS ，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到包含的所有文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 要成功执行卷影复制操作，卷上必须有足够的可用空间。

可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。此要求仅支持具有自动恢复功能的适用场景卷影副本。

相关信息

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

基于 SMB 的 SQL Server 的 SMB 服务器和卷要求

在创建基于 SMB 的 SQL Server 配置以实现无中断运行时，您需要了解特定的 SMB 服务器和卷要求。

SMB 服务器要求

- 必须启用 SMB 3.0 。

默认情况下，此选项处于启用状态。

- 必须使用有效的 UNIX 用户帐户配置默认 UNIX 用户 CIFS 服务器选项。

应用程序服务器在创建 SMB 连接时使用计算机帐户。由于所有 SMB 访问都要求 Windows 用户成功映射到 UNIX 用户帐户或默认 UNIX 用户帐户，因此 ONTAP 必须能够将应用程序服务器的计算机帐户映射到默认 UNIX 用户帐户。

此外，SQL Server 还使用域用户作为 SQL Server 服务帐户。服务帐户还必须映射到默认 UNIX 用户。

- 必须禁用自动节点转介（默认情况下，此功能处于禁用状态）。

如果要使用自动节点转介来访问 SQL Server 数据库文件以外的数据，则必须为该数据创建一个单独的 SVM 。

- 必须为用于在 ONTAP 上安装 SQL Server 的 Windows 用户帐户分配 SeSecurityPrivilege 权限。

此权限将分配给 SMB 服务器本地 BUILTIN\Administrators 组。

卷要求：

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

要使用持续可用的 SMB 连接为应用程序服务器提供 NDOS ，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能通过 SMB 共享将其直接用于 NDOS 。如果您将混合安全模式卷更改为 NTFS 安全模式卷，并打算通过 SMB 共享将其用于 NDOS ，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到包含的所有文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 尽管包含数据库文件的卷可以包含接合，但在创建数据库目录结构时，SQL Server 不会跨越接合。
- 要使适用于Microsoft SQL Server的SnapCenter 插件备份操作成功、卷上必须具有足够的可用空间。

SQL Server 数据库文件所在的卷必须足够大，才能容纳数据库目录结构以及驻留在共享中的所有包含的文件。

相关信息

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

基于 SMB 的 Hyper-V 的持续可用共享要求和注意事项

在为支持无中断运行的基于 SMB 的 Hyper-V 配置配置配置持续可用的共享时，您需要了解某些要求和注意事项。

共享要求

- 应用程序服务器使用的共享必须配置为具有持续可用属性集。

连接到持续可用共享的应用程序服务器会收到永久性句柄，使其能够无中断地重新连接到 SMB 共享，并在发生接管，交还和聚合重新定位等中断事件后回收文件锁定。

- 如果要使用启用了 VSS 的远程备份服务，则不能将 Hyper-V 文件放入包含接合的共享中。

在自动恢复情形下，如果在遍历共享时遇到接合，则卷影副本创建将失败。在非自动恢复情况下，卷影副本创建不会失败，但接合不会指向任何内容。

- 如果要将启用了 VSS 的远程备份服务与自动恢复结合使用，则不能将 Hyper-V 文件置于包含以下内容的共享中：

- 符号链接，硬链接或 Widelink
- 非常规文件

如果共享中存在指向卷影副本的任何链接或非常规文件，则卷影副本创建将失败。此要求仅支持具有自动恢复功能的适用场景卷影副本。

- 要成功执行卷影复制操作，卷上必须有足够的可用空间（仅适用于基于 SMB 的 Hyper-V）。

可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。此要求仅支持具有自动恢复功能的适用场景卷影副本。

- 不得在应用程序服务器使用的持续可用共享上设置以下共享属性：

- 主目录
- 属性缓存
- BranchCache

注意事项

- 持续可用的共享支持配额。

- 基于 SMB 的 Hyper-V 配置不支持以下功能：
 - 审核
 - fpolicy
- 不会对使用的SMB共享执行病毒扫描 continuously-availability 参数设置为 Yes。

基于 SMB 的 SQL Server 的持续可用共享要求和注意事项

在为支持无中断运行的基于 SMB 的 SQL Server 配置配置配置持续可用的共享时，您需要了解某些要求和注意事项。

共享要求

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

要使用持续可用的 SMB 连接为应用程序服务器提供无中断运行，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能直接使用卷通过 SMB 共享执行无中断操作。如果将混合安全模式卷更改为 NTFS 安全模式卷，并打算使用该卷通过 SMB 共享执行无中断操作，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到所有包含的文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 应用程序服务器使用的共享必须配置为具有持续可用属性集。

连接到持续可用共享的应用程序服务器会收到永久性句柄，使其能够无中断地重新连接到 SMB 共享，并在发生接管，交还和聚合重新定位等中断事件后回收文件锁定。

- 尽管包含数据库文件的卷可以包含接合，但在创建数据库目录结构时，SQL Server 不会跨越接合。
- 要使适用于Microsoft SQL Server的SnapCenter 插件操作成功、卷上必须具有足够的可用空间。

SQL Server 数据库文件所在的卷必须足够大，才能容纳数据库目录结构以及驻留在共享中的所有包含的文件。

- 不得在应用程序服务器使用的持续可用共享上设置以下共享属性：
 - 主目录
 - 属性缓存
 - BranchCache

分享注意事项

- 持续可用的共享支持配额。
- 基于 SMB 的 SQL Server 配置不支持以下功能：
 - 审核
 - fpolicy
- 不会对使用的SMB共享执行病毒扫描 continuously-availability 共享属性集。

基于 SMB 的 Hyper-V 配置的远程 VSS 注意事项

在对基于 SMB 的 Hyper-V 配置使用支持远程 VSS 的备份解决方案时，您需要了解一些注意事项。

常规远程 VSS 注意事项

- 每个 Microsoft 应用程序服务器最多可配置 64 个共享。

如果卷影副本集中的共享超过 64 个，则卷影复制操作将失败。这是 Microsoft 的要求。

- 每个 CIFS 服务器仅允许设置一个活动卷影副本。

如果正在同一 CIFS 服务器上执行卷影复制操作，则卷影复制操作将失败。这是 Microsoft 的要求。

- 在远程 VSS 创建卷影副本的目录结构中，不允许使用任何接合。
 - 在自动恢复情形下，如果在遍历共享时遇到接合，则卷影副本创建将失败。
 - 在非自动恢复情形下，卷影副本创建不会失败，但接合不会指向任何内容。

仅适用于具有自动恢复功能的卷影副本的远程 VSS 注意事项

某些限制仅适用于具有自动恢复功能的卷影副本。

- 创建卷影副本时，最多允许五个子目录的深度。

这是卷影复制服务创建卷影副本备份集所使用的目录深度。如果包含虚拟机文件的目录嵌套深度超过五个级别，则卷影副本创建将失败。这样可以限制克隆共享时的目录遍历。可以使用 CIFS 服务器选项更改最大目录深度。

- 卷上的可用空间量必须足够。

可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。

- 在远程 VSS 创建卷影副本的目录结构中，不允许使用任何链接或非常规文件。

如果共享中存在指向卷影副本的任何链接或非常规文件，则卷影副本创建将失败。克隆过程不支持这些设置。

- 目录上不允许使用 NFSv4 ACL。

虽然卷影复制创建会保留文件上的 NFSv4 ACL，但目录上的 NFSv4 ACL 会丢失。

- 创建卷影副本集最多允许 60 秒。

Microsoft 规范最多允许 60 秒创建卷影副本集。如果 VSS 客户端无法在此时间内创建卷影副本集，则卷影复制操作将失败；因此，这会限制卷影副本集中的文件数。备份集中可包含的文件或虚拟机的实际数量各不相同；该数量取决于多种因素，必须根据每个客户环境来确定。

基于 SMB 的 SQL Server 和 Hyper-V 的 ODX 副本卸载要求

如果要迁移虚拟机文件或直接将数据库文件从源导出和导入目标存储位置，而无需通过应用程序服务器发送数据，则必须启用 ODX 副本卸载。对于将 ODX 副本卸载与 SQL Server 和基于 SMB 的 Hyper-V 解决方案结合使用，您必须了解一些特定要求。

使用 ODX 副本卸载可显著提高性能。默认情况下，此 CIFS 服务器选项处于启用状态。

- 要使用 ODX 副本卸载，必须启用 SMB 3.0 。
- 源卷必须至少为 1.25 GB 。
- 必须在使用副本卸载的卷上启用重复数据删除。
- 如果使用压缩卷，则压缩类型必须是自适应的，并且仅支持压缩组大小 8K 。

不支持二级压缩类型

- 要使用 ODX 副本卸载功能在磁盘内部和磁盘之间迁移 Hyper-V 子系统，必须将 Hyper-V 服务器配置为使用 SCSI 磁盘。

默认情况下，配置 IDE 磁盘，但如果使用 IDE 磁盘创建磁盘，则迁移子系统时 ODX 副本卸载将不起作用。

针对 SQL Server 和基于 SMB 的 Hyper-V 配置的建议

要确保 SQL Server 和基于 SMB 的 Hyper-V 配置稳健且正常运行，您需要熟悉配置解决方案时建议的最佳实践。

一般建议

- 将应用程序服务器文件与常规用户数据分开。

如果可能，请将整个 Storage Virtual Machine （SVM）及其存储专用于应用程序服务器的数据。

- 为了获得最佳性能，请勿在用于存储应用程序服务器数据的 SVM 上启用 SMB 签名。
- 为了获得最佳性能并提高容错能力，请启用 SMB 多通道，以便在一个 SMB 会话中提供 ONTAP 与客户端之间的多个连接。
- 请勿在 Hyper-V 或基于 SMB 的 SQL Server 配置中使用的共享以外的任何共享上创建持续可用的共享。
- 对用于持续可用性的共享禁用更改通知。
- 请勿与聚合重新定位（Aggregate Relocation，ARL）同时执行卷移动，因为 ARL 具有暂停某些操作的阶段。
- 对于基于 SMB 的 Hyper-V 解决方案，请在创建集群模式虚拟机时使用来宾 iSCSI 驱动器。共享 .VHDX 在 ONTAP SMB 共享中、基于 SMB 的 Hyper-V 不支持文件。

规划基于 SMB 的 Hyper-V 或 SQL Server 配置

填写卷配置工作表

通过此工作表，您可以轻松地记录为 SQL Server 和基于 SMB 的 Hyper-V 配置创建卷时所需的值。

对于每个卷，必须指定以下信息：

- Storage Virtual Machine （SVM）名称

所有卷的 SVM 名称都相同。

- Volume name
- Aggregate name

您可以在集群中任何节点上的聚合上创建卷。

- Size
- Junction path

在创建用于存储应用程序服务器数据的卷时，应牢记以下几点：

- 如果根卷没有 NTFS 安全模式，则必须在创建卷时将安全模式指定为 NTFS。

默认情况下，卷会继承 SVM 根卷的安全模式。

- 应使用默认卷空间保证配置卷。
- 您可以选择配置自动调整大小空间管理设置。
- 您应设置用于确定 Snapshot 副本空间预留的选项 0。
- 必须禁用应用于卷的 Snapshot 策略。

如果禁用了 SVM Snapshot 策略，则无需为卷指定 Snapshot 策略。这些卷将继承 SVM 的 Snapshot 策略。如果 SVM 的 Snapshot 策略未禁用，并且配置为创建 Snapshot 副本，则必须在卷级别指定 Snapshot 策略，并且必须禁用该策略。启用了卷影复制服务的备份和 SQL Server 备份可管理 Snapshot 副本的创建和删除。

- 您不能为卷配置负载共享镜像。

应选择要创建应用程序服务器使用的共享的接合路径，以便在共享入口点下方没有接合卷。

例如，如果要将虚拟机文件存储在名为 "vol1"，"vol2"，"vol3" 和 "vol4" 的四个卷上，则可以创建示例中所示的命名空间。然后、您可以通过以下路径为应用程序服务器创建共享： /data1/vol1， /data1/vol2， /data2/vol3，和 /data2/vol4。

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active			
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

信息类型	值
_Volume 1：卷名称，聚合，大小，接合路径 _	
Volume 2：卷名称、聚合、大小、接合路径	
Volume 3：卷名称、聚合、大小、接合路径	
Volume 4：卷名称、聚合、大小、接合路径	
Volume 5：卷名称、聚合、大小、接合路径	
Volume 6：卷名称、聚合、大小、接合路径	
附加卷：卷名称，聚合，大小，接合路径 _	

填写 **SMB** 共享配置工作表

使用此工作表可记录在为 SQL Server 和基于 SMB 的 Hyper-V 配置创建持续可用的 SMB 共享时所需的值。

有关 **SMB** 共享属性和配置设置的信息

对于每个共享，必须指定以下信息：

- Storage Virtual Machine （SVM）名称
- Share name
- 路径
- 共享属性

您必须配置以下两个共享属性：

- oplocks
- continuously-available

不能设置以下共享属性：

- homedirectory attributecache
- branchcache
- access-based-enumeration
 - 必须禁用符号链接(的值 `-symlink-properties` 参数必须为空[""])


有关共享路径的信息

如果您使用远程 VSS 备份 Hyper-V 文件，则在从 Hyper-V 服务器到存储虚拟机文件的存储位置建立 SMB 连接时，选择要使用的共享路径非常重要。虽然可以在命名空间中的任意位置创建共享，但 Hyper-V 服务器使用的共享路径不应包含接合卷。不能对包含接合点的共享路径执行卷影复制操作。

在创建数据库目录结构时，SQL Server 无法跨越接合。您不应为包含接合点的 SQL Server 创建共享路径。

例如、在显示的命名空间中、如果要将虚拟机文件或数据库文件存储在卷"vol1"、“vol2”、“vol3”和"vol4"上、则应在以下路径为应用程序服务器创建共享： /data1/vol1， /data1/vol2， /data2/vol3， 和 /data2/vol4。

Vserver	Volume	Junction Active	Junction Path	Junction 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



但您可以在上创建共享 /data1 和 /data2 用于管理管理的路径、则不能将应用程序服务器配置为使用这些共享来存储数据。

规划工作表

信息类型	值
_Volume 1： SMB 共享名称和路径 _	
Volume 2: SMB共享名称和路径	
Volume 3: SMB共享名称和路径	

信息类型	值
Volume 4: SMB共享名称和路径	
Volume 5: SMB共享名称和路径	
Volume 6: SMB共享名称和路径	
Volume 7: SMB共享名称和路径	
_Additional volumes : SMB 共享名称和路径 _	

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

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

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

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

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

相关信息

[规划基于 SMB 的 Hyper-V 或 SQL Server 配置](#)

[配置要求和注意事项](#)

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

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

关于此任务

建立持续可用的共享连接时，需要进行 Kerberos 身份验证。远程 VSS 进程的一部分使用 NTLMv2 身份验证。

因此，基于 SMB 的 Hyper-V 配置必须支持使用这两种身份验证方法的连接。

必须将以下设置配置为允许 Kerberos 和 NTLMv2 身份验证：

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

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

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

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

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

步骤

1. 执行以下操作，验证是否已在 SVM 上禁用导出策略：

- a. 将权限级别设置为高级：

```
set -privilege advanced
```

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

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

- c. 返回到管理权限级别：

```
set -privilege admin
```

2. 如果 SMB 的导出策略未禁用，请禁用它们：

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

3. 验证域中是否允许 NTLMv2 和 Kerberos 身份验证。

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

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

示例

以下命令验证是否已在 SVM vs1 上禁用 SMB 的导出策略：


```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields vservers,is-
exportpolicy-enabled

vservers  is-exportpolicy-enabled
-----  -----
vs1       false

cluster1::*> set -privilege admin
```

验证域帐户是否映射到默认 UNIX 用户

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

关于此任务

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

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

步骤

1. 确定是否存在默认 UNIX 用户：

```
vservers cifs options show -vservers vservers_name
```

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

```
vservers services unix-user show -vservers vservers_name
```

3. 如果未设置默认用户选项，并且没有可指定为默认 UNIX 用户的 UNIX 用户，请创建默认 UNIX 用户和默认组，然后将默认用户添加到组中。

通常，系统会为默认用户提供用户名 "pcuser"，并且必须为其分配 UID 65534。默认组通常被指定为组名称 "pcuser"。分配给组的 GID 必须为 65534。

- a. 创建默认组：

```
vservers services unix-group create -vservers vservers_name -name pcuser -id 65534
```

- b. 创建默认用户并将默认用户添加到默认组：

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

- c. 验证是否已正确配置默认用户和默认组：

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

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

4. 如果未配置 CIFS 服务器的默认用户，请执行以下操作：

- a. 配置默认用户：

```
vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*
```

- b. 验证是否已正确配置默认 UNIX 用户：

```
vserver cifs options show -vserver vserver_name
```

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

有关使用此命令的详细信息，请参见手册页。

示例

以下命令确定未设置 CIFS 服务器的默认用户，但确定 "pcuser" 用户和 "pcuser" 组存在。在 SVM vs1 上，将 "pcuser" 用户分配为 CIFS 服务器的默认用户。

```
cluster1::> vserver cifs options show
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : -
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

```
cluster1::> vserver services unix-user show
```

	User	User	Group	Full
Vserver	Name	ID	ID	Name

```
-----
```

```

vs1      nobody      65535  65535  -
vs1      pcuser       65534  65534  -
vs1      root         0       1       -

cluster1::> vserver services unix-group show -members
Vserver      Name              ID
vs1          daemon          1
      Users: -
vs1          nobody          65535
      Users: -
vs1          pcuser          65534
      Users: -
vs1          root            0
      Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -

```

验证 **SVM** 根卷的安全模式是否设置为 **NTFS**

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

关于此任务

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

步骤

1. 确定 SVM 根卷的当前安全模式：

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

2. 如果根卷不是 NTFS 安全模式卷，请将安全模式更改为 NTFS：

```
volume modify -vserver vs1 -volume root_volume_name -security-style ntfs
```

3. 验证 SVM 根卷是否设置为 NTFS 安全模式：

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

示例

以下命令验证 SVM vs1 上的根卷安全模式是否为 NTFS：

```
cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root      unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style ntfs

cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root      ntfs
```

验证是否已配置所需的 CIFS 服务器选项

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

关于此任务

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

步骤

1. 验证是否已在 Storage Virtual Machine （ SVM ） 上启用所需的 CIFS 服务器选项：

a. 将权限级别设置为高级：

```
set -privilege advanced
```

b. 输入以下命令：

```
vserver cifs options show -vserver vs1
```

以下选项应设置为 true：

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

2. 如果任何选项未设置为 true，执行以下操作：

- a. 将其设置为 true 使用 `vserver cifs options modify` 命令：
- b. 验证这些选项是否设置为 true 使用 `vserver cifs options show` 命令：

3. 返回到管理权限级别：

```
set -privilege admin
```

示例

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

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::*> set -privilege admin
```

为 SMB 多通道配置性能和冗余

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

开始之前

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

关于此任务

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

SMB 会话中同时连接的数量取决于您部署的 NIC：

- 客户端和 ONTAP 集群上的 * 1G NIC *

客户端为每个 NIC 建立一个连接，并将会话绑定到所有连接。

- 客户端和 ONTAP 集群上的 * 10 G 及更大容量 NIC *

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

您还可以修改以下参数（高级权限）：

- `-max-connections-per-session`

每个多通道会话允许的最大连接数。默认值为 32 个连接。

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

- `-max-lifs-per-session`

每个多通道会话公布的最大网络接口数。默认值为 256 个网络接口。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 在 SMB 服务器上启用 SMB 多通道：

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

3. 验证 ONTAP 是否正在报告 SMB 多通道会话：

```
vserver cifs session show
```

4. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下示例显示了有关所有 SMB 会话的信息，其中显示了单个会话的多个连接：

```
cluster1::> vservers cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s
Administrator
```

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

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

创建 NTFS 数据卷

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

关于此任务

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

创建数据卷时，不应在包含以下内容的卷中创建接合点：

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



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

步骤

1. 输入相应的命令以创建数据卷：

如果要在根卷安全模式为 ... 的 SVM 中创建卷	输入命令 ...
NTFS	<code>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
非 NTFS	<code>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. 验证卷配置是否正确：

```
volume show -vserver vservers_name -volume volume_name
```

创建持续可用的 **SMB** 共享

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

步骤

1. 显示有关现有数据卷及其接合路径的信息：

```
volume show -vserver vservers_name -junction
```

2. 创建持续可用的 SMB 共享：

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

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

3. 对共享配置工作表中的所有共享重复上述步骤。

4. 使用验证您的配置是否正确 `vserver cifs share show` 命令：

5. 通过将驱动器映射到每个共享并使用 * Windows 属性 * 窗口配置文件权限，在持续可用的共享上配置 NTFS 文件权限。

示例

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

```

cluster1::> volume show -vserver vs1 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

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

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

您需要的内容

用于安装 SQL Server 的域帐户必须已存在。

关于此任务

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

步骤

1. 添加 "SeSecurityPrivilege" 权限：

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

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

2. 验证是否已将此权限应用于此帐户：

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

示例

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

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name EXAMPLE\SQLInstaller -privileges  
SeSecurityPrivilege  
  
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1  
Vserver      User or Group Name          Privileges  
-----  
vs1          EXAMPLE\SQLInstaller       SeSecurityPrivilege
```

配置 VSS 卷影复制目录深度（对于基于 SMB 共享的 Hyper-V）

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

您需要的内容

必须启用 VSS 卷影复制功能。

关于此任务

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



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

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 将 VSS 卷影复制目录深度设置为所需级别：

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

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

3. 返回到管理权限级别：

```
set -privilege admin
```

通过 SMB 配置管理 Hyper-V 和 SQL Server

配置现有共享以实现持续可用性

您可以修改现有共享，使其成为持续可用的共享，Hyper-V 和 SQL Server 应用程序服务器可使用这些共享无中断地访问 Hyper-V 虚拟机和配置文件以及 SQL Server 数据库文件。

关于此任务

如果现有共享具有以下特征，则不能使用该共享作为持续可用的共享，以便通过 SMB 与应用程序服务器进行无中断操作：

- 如果 homedirectory 共享属性已在该共享上设置
- 如果共享包含已启用的符号链接或 Widelink
- 如果共享包含位于共享根目录下的接合卷

您必须验证以下两个共享参数是否设置正确：

- 。 -offline-files 参数设置为任一 manual (默认值)或 none。
- 必须禁用符号链接。

必须配置以下共享属性：

- continuously-available
- oplocks

不得设置以下共享属性。如果它们位于当前共享属性列表中，则需要从持续可用的共享中删除它们：

- attributecache
- branchcache

步骤

1. 显示当前共享参数设置和当前已配置共享属性列表：

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

2. 如有必要、请使用命令修改共享参数以禁用符号链接、并将脱机文件设置为manual. vserver cifs share modify

- 您可以通过设置的值来禁用符号链接 `-symlink` 参数设置为 `""`。
- 您可以设置 `-offline-files` 参数到正确的设置 `manual`。

3. 添加共享属性、如果需要、还添加 `continuously-available oplocks` 共享属性：

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

如果 `oplocks` 尚未设置共享属性、必须将其与一起添加 `continuously-available` 共享属性。

4. 删除持续可用的共享不支持的任何共享属性：

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

您可以通过使用逗号分隔列表指定共享属性来删除一个或多个共享属性。

5. 验证是否已 `-symlink` 和 `-offline-files` 参数设置正确：

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

6. 验证已配置的共享属性列表是否正确：

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

示例

以下示例显示了如何在具有基于SMB的应用程序服务器的Storage Virtual Machine (SVM)"VS1"上为NDOS配置名为"share1"的现有共享：

- 通过将参数设置为，可以在共享上禁用符号链接 `-symlink ""`。
- `-offline-file` 参数已修改并设置为 `manual`。
- `continuously-available` 共享属性将添加到共享中。
- `oplocks` 共享属性已在共享属性列表中、因此无需添加。
- `attributecache` 共享属性将从共享中删除。
- `browsable` 对于在SMB上使用应用程序服务器的NDO中使用的持续可用共享、共享属性是可选的、并保留为共享属性之一。

```
cluster1::> vsriver cifs share show -vsriver 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::> vsriver cifs share modify -vsriver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsriver cifs share show -vsriver vs1 -share-name share1
-fields symlink-properties,offline-files
vsriver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1::> vsriver cifs share properties show -vsriver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                 browsable
                 continuously-available
```

为基于 **SMB** 的 **Hyper-V** 备份启用或禁用 **VSS** 卷影副本

如果使用 VSS 感知型备份应用程序备份存储在 SMB 共享上的 Hyper-V 虚拟机文件，则必须启用 VSS 卷影复制。如果您不使用 VSS 感知型备份应用程序，则可以禁用 VSS 卷影复制。默认情况下，启用 VSS 卷影复制。

关于此任务
您可以随时启用或禁用 VSS 卷影副本。

步骤

- 1. 将权限级别设置为高级：

```
set -privilege advanced
```

- 2. 执行以下操作之一：

VSS 卷影副本的目标位置	输入命令 ...
enabled	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code>
已禁用	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code>

- 3. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下命令可在 SVM vs1 上启用 VSS 卷影副本：

```
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
```

使用统计信息通过 **SMB** 监控 **Hyper-V** 和 **SQL Server** 活动

确定可用的统计信息对象和计数器

在获取有关 CIFS ， SMB ， 审核和 BranchCache 哈希统计信息以及监控性能的信息之前， 您必须了解哪些对象和计数器可用于获取数据。

步骤

- 1. 将权限级别设置为高级：

```
set -privilege advanced
```

- 2. 执行以下操作之一：

要确定的内容	输入 ...
哪些对象可用	<code>statistics catalog object show</code>
可用的特定对象	<code>statistics catalog object show object <i>object_name</i></code>
哪些计数器可用	<code>statistics catalog counter show object <i>object_name</i></code>

有关哪些对象和计数器可用的详细信息， 请参见手册页。

- 3. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下命令显示与集群中的 CIFS 和 SMB 访问相关的选定统计信息对象的说明， 如高级权限级别所示：


```
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
```

以下命令显示有关的某些计数器的信息 `cifs` 对象、如高级权限级别所示：



此示例不会显示的所有可用计数器 `cifs` 对象；输出被截断。

```
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

[...]

显示 SMB 统计信息

您可以显示各种 SMB 统计信息来监控性能和诊断问题。

步骤

- 1. 使用 `statistics start` 和可选 `statistics stop` 用于收集数据样本的命令。
- 2. 执行以下操作之一：

要显示统计信息的对象	输入以下命令 ...
SMB 的所有版本	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x 和 SMB 3.0	<code>statistics show -object smb2</code>
节点的SMB子系统	<code>statistics show -object nblade_cifs</code>

详细了解 `statistics` 命令：

- ["statistics show"](#)
- ["统计信息启动"](#)
- ["统计信息停止"](#)

验证此配置是否能够无中断运行

使用运行状况监控来确定无中断运行状态是否正常

运行状况监控可提供有关整个集群中的系统运行状况的信息。运行状况监控器可通过 SMB 监控 Hyper-V 和 SQL Server 配置，以确保应用程序服务器无中断运行（NDO）。如果状态为 `degraded`，则可以查看有关问题的详细信息，包括可能发生原因和建议的恢复操作。

有多个运行状况监控器。ONTAP 可监控各个运行状况监控器的整体系统运行状况和运行状况。节点连接运行状况监控器包含 CIFS-NDO 子系统。监控器具有一组运行状况策略，可在某些物理条件可能导致中断时触发警报，如果存在中断情况，则会生成警报并提供有关更正操作的信息。对于基于 SMB 的 NDO 配置，将针对以下两种情况生成警报：

警报 ID	severity	条件
HaNotReadyCifsNdo_Alert	major	节点上聚合中某个卷托管的一个或多个文件已通过持续可用的 SMB 共享打开，并承诺在发生故障时会持久存在；但是，与配对节点的 HA 关系未配置或运行状况不佳。

警报 ID	severity	条件
NoStandbyLifCifsNdo_Alert	次要	Storage Virtual Machine （SVM）正在通过节点主动通过 SMB 提供数据，并且在持续可用的共享上持久打开了 SMB 文件；但是，其配对节点不会公开 SVM 的任何活动数据 LIF。

使用系统运行状况监控功能显示无中断运行状态

您可以使用 `system health` 用于显示有关集群的整体系统运行状况和CI-NDO子系统运行状况的信息、响应警报、配置未来警报以及显示有关如何配置运行状况监控的信息的命令。

步骤

1. 通过执行相应的操作来监控运行状况：

要显示的内容	输入命令 ...
系统的运行状况，反映单个运行状况监控器的整体状态	system health status show
有关 CIFS-NDO 子系统运行状况的信息	system health subsystem show -subsystem CIFS-NDO -instance

2. 显示有关如何通过执行相应操作配置 CIFS-NDO 警报监控的信息：

要显示的信息	输入命令 ...
CIFS-NDO 子系统运行状况监控器的配置和状态，例如受监控节点，初始化状态和状态	system health config show -subsystem CIFS-NDO
CIFS-NDO 警报，运行状况监控器可能会生成此警报	system health alert definition show -subsystem CIFS-NDO
CIFS-NDO 运行状况监控策略，用于确定何时发出警报	system health policy definition show -monitor node-connect



使用 `-instance` 用于显示详细信息的参数。

示例

以下输出显示了有关集群和 CIFS-NDO 子系统的整体运行状况的信息：

```
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
```

以下输出显示了有关 CIFS-NDO 子系统运行状况监控器的配置和状态的详细信息：

```

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

```

验证持续可用的 **SMB** 共享配置

要支持无中断运行，必须将 Hyper-V 和 SQL Server SMB 共享配置为持续可用的共享。此外，您还必须检查某些其他共享设置。如果发生计划内或计划外中断事件，您应验证共享是否已正确配置，以便为应用程序服务器提供无缝无中断运行。

关于此任务

您必须验证以下两个共享参数是否设置正确：

- `-offline-files` 参数设置为任一 `manual` (默认值)或 `none`。

- 必须禁用符号链接。

要实现正确的无中断运行，必须设置以下共享属性：

- continuously-available
- oplocks

不能设置以下共享属性：

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

步骤

1. 验证脱机文件是否设置为 manual 或 disabled 并禁用符号链接：

```
vserver cifs shares show -vserver vserver_name
```

2. 验证 SMB 共享是否已配置为持续可用性：

```
vserver cifs shares properties show -vserver vserver_name
```

示例

以下示例显示了 Storage Virtual Machine （SVM，以前称为 Vserver）vs1 上名为 share1 的共享的共享设置。脱机文件设置为 manual 和符号链接已禁用(在中使用连字符指定) Symlink Properties 字段输出)：

```
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
```

以下示例显示了 SVM vs1 上名为 share1 的共享的共享属性：

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

验证 LIF 状态

即使您将采用 Hyper-V 和基于 SMB 的 SQL Server 配置的 Storage Virtual Machine （SVM）配置为在集群中的每个节点上都具有 LIF，在日常操作期间，某些 LIF 也可能会移至另一节点上的端口。您必须验证 LIF 状态并采取任何必要的更正操作。

关于此任务

要提供无缝，无中断的操作支持，集群中的每个节点必须至少为 SVM 配置一个 LIF，并且所有 LIF 都必须与主端口关联。如果某些已配置的 LIF 当前未与其主端口关联，则必须修复任何端口问题，然后将 LIF 还原到其主端口。

步骤

- 1. 显示有关为 SVM 配置的 LIF 的信息：

network interface show -vsriver vsriver_name

在此示例中， "lif1` " 不位于主端口上。

network interface show -vsriver vs1

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1						
	lif1	up/up	10.0.0.128/24	node2	e0d	false
	lif2	up/up	10.0.0.129/24	node2	e0d	true

- 2. 如果某些 LIF 不在其主端口上，请执行以下步骤：
 - a. 对于每个 LIF，确定 LIF 的主端口是什么：

network interface show -vsriver vsriver_name -lif lif_name -fields home-node,home-port

network interface show -vsriver vs1 -lif lif1 -fields home-node,home-port


```

vserver lif  home-node  home-port
-----
vs1      lif1 node1      e0d

```

- b. 对于每个 LIF ，确定 LIF 的主端口是否已启动：

```
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

```

+ 在此示例中、"lif1"应迁移回其主端口、node1:e0d。

- 如果应与这些IF关联的任何主端口网络接口不在中 up 请解决此问题、使这些接口正常运行。
- 如果需要，请将 LIF 还原到其主端口：

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

```
network interface revert -vserver vs1 -lif lif1
```

- 验证集群中的每个节点是否都具有适用于 SVM 的活动 LIF：

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	
true	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

确定 SMB 会话是否持续可用

显示 SMB 会话信息

您可以显示有关已建立的 SMB 会话的信息，包括 SMB 连接和会话 ID 以及使用会话的工作站的 IP 地址。您可以显示有关会话的 SMB 协议版本和持续可用保护级别的信息，这有助于确定会话是否支持无中断操作。

关于此任务

您可以摘要形式显示 SVM 上所有会话的信息。但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息：

- 您可以使用可选 `-fields` 用于显示有关所选字段的输出的参数。

您可以输入 `-fields ?` 以确定您可以使用哪些字段。

- 您可以使用 `-instance` 用于显示有关已建立 SMB 会话的详细信息参数。
- 您可以使用 `-fields` 参数或 `-instance` 参数单独使用或与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

要显示 SMB 会话信息的项	输入以下命令 ...
SVM 上的所有会话的摘要形式	<code>vserver cifs session show -vserver vserver_name</code>
指定的连接 ID	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
指定的工作站 IP 地址	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
指定的 LIF IP 地址	<code>vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address</code>
在指定节点上	<code>`*vserver cifs session show -vserver vserver_name -node {node_name</code>
local}*	指定的 Windows 用户

要显示 SMB 会话信息的项	输入以下命令 ...
vserver cifs session show -vserver vserver_name -windows-user user_name 的格式 user_name 为 [domain]\user。	使用指定的身份验证机制
vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism 的值 -auth -mechanism 可以是以下选项之一： <ul style="list-style-type: none">• NTLMv1• NTLMv2• Kerberos• Anonymous	使用指定的协议版本

要显示 SMB 会话信息的项	输入以下命令 ...
<pre> vserver cifs session show -vserver vserver_name -continuously -available continuously_avail able_protection_le vel </pre> <p> 的值 <code>-continuously</code> <code>-available</code> 可以是以下选项之一： </p> <ul style="list-style-type: none"> • No • Yes • Partial <div>  <p> 持续可用状态为 Partial，这意味着会话至少包含一个打开的持续可用文件，但会话中的某些文件未使用持续可用保护打开。您可以使用 <code>vserver cifs session s file show</code> 命令、用于确定已建立会话中哪些文件未在持续可用的保护下打开。 </p> </div>	具有指定的 SMB 签名会话状态

示例

以下命令显示 SVM vs1 上从 IP 地址为 10.1.1.1 的工作站建立的会话的会话信息：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

以下命令显示 SVM vs1 上具有持续可用保护的会话的详细会话信息。此连接是使用域帐户建立的。

```
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
```

以下命令显示 SVM vs1 上使用 SMB 3.0 和 SMB 多通道的会话的会话信息。在此示例中，用户使用 LIF IP 地址从支持 SMB 3.0 的客户端连接到此共享；因此，身份验证机制默认为 NTLMv2。必须使用 Kerberos 身份验证进行连接，以获得持续可用的保护。

```
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
```

显示有关打开的 **SMB** 文件的信息

您可以显示有关打开的 SMB 文件的信息，包括 SMB 连接和会话 ID，托管卷，共享名称和共享路径。您还可以显示有关文件的持续可用保护级别的信息，这有助于确定打开的文件是否处于支持无中断操作的状态。

关于此任务

您可以显示有关已建立的 SMB 会话上打开的文件的信息。如果需要确定 SMB 会话中特定文件的 SMB 会话信息，则显示的信息非常有用。

例如、如果您有一个SMB会话、其中一些打开的文件已打开且具有持续可用的保护、而另一些文件未打开且具有持续可用的保护(的值 `-continuously-available` 字段输入 `vserver cifs session show` 命令输出为 `Partial`)、则可以使用此命令确定哪些文件不持续可用。

您可以使用以摘要形式显示Storage Virtual Machine (SVM)上已建立的SMB会话上的所有打开文件的信息 `vserver cifs session file show` 命令、而不带任何可选参数。

但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息。如果您只想查看一小部分打开文件的信息，这将非常有用。

- 您可以使用可选 `-fields` 用于显示所选字段的输出的参数。

您可以单独使用此参数，也可以与其他可选参数结合使用。

- 您可以使用 `-instance` 用于显示有关打开的SMB文件的详细信息的参数。

您可以单独使用此参数，也可以与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

如果要显示打开的 SMB 文件 ...	输入以下命令 ...
以摘要形式显示在 SVM 上	<code>vserver cifs session file show -vserver vserver_name</code>
在指定节点上	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*`</code>	指定的文件 ID
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	指定的 SMB 连接 ID
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	指定的 SMB 会话 ID
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	在指定的托管聚合上
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	在指定卷上
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	指定的 SMB 共享上
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	指定的 SMB 路径上
<code>vserver cifs session file show -vserver vserver_name -path path</code>	具有指定级别的持续可用保护

如果要显示打开的 SMB 文件 ...	输入以下命令 ...
<pre>vserver cifs session file show -vserver vserver_name -continuously -available continuously_available_status</pre> <p>的值 <code>-continuously-available</code> 可以是以下选项之一：</p> <ul style="list-style-type: none">• No• Yes <div><p>持续可用状态为 No，这意味着这些打开的文件无法从接管和恢复中无系统地恢复。它们也无法从高可用性关系中的合作伙伴之间的常规聚合重新定位中恢复。</p></div>	具有指定的重新连接状态

您可以使用其他可选参数来细化输出结果。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上打开的文件的信息：

```
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
```

以下示例显示了有关 SVM vs1 上文件 ID 82 的已打开 SMB 文件的详细信息：

```
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
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。