



Microsoft Hyper-VオヨヒSQL Server ヨウノSMBノセツテイ ONTAP 9

NetApp
December 20, 2024

目次

Microsoft Hyper-VおよびSQL Server向けのSMBの設定	1
Microsoft Hyper-VおよびSQL Server向けのSMBの設定の概要	1
Microsoft Hyper-VおよびSQL Server over SMBソリューション用のONTAPの設定	1
Hyper-VおよびSQL Server over SMBのノンストップオペレーション	2
リモートVSSによる共有ベースのバックアップ	6
Hyper-V over SMBおよびSQL Server over SMB共有でのODXコピーオフロードの使用	10
設定に関する要件と考慮事項	12
SQL ServerおよびHyper-V over SMB構成に関する推奨事項	20
Hyper-VまたはSQL Server over SMB構成の計画	21
Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成の作成	24
Hyper-VおよびSQL Server over SMB構成を管理します。	38
統計を使用してHyper-VおよびSQL Server over SMBのアクティビティを監視する	43
構成がノンストップオペレーションに対応していることを確認する	46

Microsoft Hyper-VおよびSQL ServerのSMBのセッティング

Microsoft Hyper-VおよびSQL Server向けのSMBの設定の概要

ONTAPの機能を使用すると、SMBプロトコルを介したMicrosoftアプリケーション、Microsoft Hyper-V および Microsoft SQL Server の2つのノンストップオペレーションを有効にできます。

これらの手順は、SMBのノンストップオペレーションを実装する場合に使用します。想定している状況は次のとおりです。

- SMBプロトコルの基本的なファイルアクセスが設定されている。
- SVMにあるSMB 3.0以降のファイル共有を有効にして次のオブジェクトを格納する。
 - Hyper-V仮想マシンファイル
 - SQL Serverシステムデータベース

関連情報

ONTAPテクノロジーおよび外部サービスとのやり取りの詳細については、次のテクニカルレポート（TR）を参照してください。 ** ["NetAppテクニカルレポート4172：『Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices』"](#) ["ネットアップテクニカルレポート 4369：『Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP』"](#)

Microsoft Hyper-VおよびSQL Server over SMBソリューション用のONTAPの設定

SMB 3.0以降のファイル共有では、継続的可用性を備えたファイル共有を使用し、Hyper-V仮想マシンファイルまたはSQL ServerのシステムデータベースとユーザーデータベースをSVM上のボリュームに格納し、同時に計画的イベントと計画外イベントのノンストップオペレーション（NDO）を実現できます。

Microsoft Hyper-V over SMB

Hyper-V over SMBソリューションを作成するには、まずMicrosoft Hyper-Vサーバにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoft クラスタ（クラスタ構成を使用する場合）、Hyper-Vサーバ、CIFSサーバによってホストされている共有へのSMB 3.0の継続的可用性を備えた接続、および必要に応じて、SVMボリュームに格納されている仮想マシンファイルを保護するためのバックアップサービスも設定する必要があります。



Hyper-Vサーバは、Windows Server 2012以降で設定する必要があります。Hyper-Vサーバの構成は、スタンドアロン構成とクラスタ構成の両方がサポートされます。

- Microsoft クラスタおよびHyper-Vサーバの作成については、MicrosoftのWebサイトを参照してください。
- SnapManager for Hyper-Vは、Snapshotコピーベースの高速バックアップサービスを容易に実現するホス

トベースのアプリケーションで、Hyper-V over SMB構成と統合できるように設計されています。

Hyper-V over SMB 構成での SnapManager の使用については、SnapManager for Hyper-V インストールガイドを参照してください。

Microsoft SQL Server over SMB

SQL Server over SMBソリューションを作成するには、まずMicrosoft SQL Serverアプリケーションにストレージサービスを提供するようにONTAPを設定する必要があります。また、Microsoftクラスタも設定する必要があります（クラスタ構成を使用している場合）。その後、WindowsサーバにSQL Serverをインストールして設定し、CIFSサーバによってホストされている共有への継続的可用性を備えたSMB 3.0接続を作成します。必要に応じて、SVMボリュームに格納されているデータベースファイルを保護するようにバックアップサービスを設定できます。



Windows Server 2012以降にSQL Serverをインストールして設定する必要があります。スタンダード構成とクラスタ構成の両方がサポートされます。

- Microsoftクラスタの作成およびSQL Serverのインストールと設定の詳細については、MicrosoftのWebサイトを参照してください。
- SnapCenter Plug-in for Microsoft SQL Serverは、Snapshotコピーベースの高速バックアップサービスを容易に実現するホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

SnapCenter Plug-in for Microsoft SQL Serverの使用方法については、のドキュメントを参照してください "[SnapCenter Plug-in for Microsoft SQL Server](#)"。

Hyper-VおよびSQL Server over SMBのノンストップオペレーション

Hyper-V および SQL Server over SMB のノンストップオペレーションとは何ですか

Hyper-VおよびSQL Server over SMBのノンストップオペレーションとは、さまざまな管理タスクの間も、アプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持し、継続的可用性を実現できる機能のことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMBを介したアプリケーションサーバのノンストップオペレーションは、次のとおりです。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
- 計画的なアグリゲートの再配置（ARL）
- LIFの移行とフェイルオーバー
- 計画的なボリュームの移動

SMB経由のノンストップオペレーションを実現するプロトコル

SMB 3.0のリリースに伴い、Microsoftから、Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションのサポートに必要な機能を提供する新しいプロトコルがリリースされました。

ONTAP では、SMB を介したアプリケーションサーバのノンストップオペレーションを実現するために、それらのプロトコルを使用しています。

- SMB 3.0
- 監視

Hyper-VおよびSQL Server over SMB ノンストップオペレーションの概念

Hyper-V over SMB または SQL Server over SMB 解決策を設定する前に理解しておくべきノンストップオペレーション（NDO）の概念があります。

- * 共有の継続的な可用性 *

継続的可用性プロパティが設定されている SMB 3.0 共有。継続的可用性を備えた共有を介して接続しているクライアントは、テイクオーバー、ギブバック、およびアグリゲート移転などのシステム停止を伴うイベントが発生しても、

- * ノード *

クラスタのメンバーである単一のコントローラ。SFO ペアの 2 つのノードを区別するために、1 つのノードを `_local node_name` と呼び、もう 1 つのノードを `_partner node_or_remote node_name` と呼ぶことがあります。ストレージのプライマリ所有者はローカルノードです。セカンダリ所有者は、プライマリ所有者に障害が発生したストレージを制御するパートナーノードです。各ノードは、そのストレージのプライマリ所有者と、そのパートナーストレージのセカンダリ所有者です。

- * 無停止でのアグリゲートの再配置 *

クライアントアプリケーションを中断することなく、クラスタの SFO ペア内のパートナーノード間でアグリゲートを移動できること。

- * 無停止フェイルオーバー *

テイクオーバーを参照してください。

- * 無停止での LIF の移行 *

LIF を介してクラスタに接続されたクライアントアプリケーションを中断することなく、LIF を移行できること。SMB 接続の場合は、SMB 2.0 以降を使用して接続するクライアントでのみ可能です。

- * ノンストップオペレーション *。

クライアントアプリケーションを中断することなく、ONTAP の主な管理およびアップグレード操作を実行でき、ノード障害に耐えられること。全体として、この用語は、無停止テイクオーバー、無停止アップグレード、および無停止移行の各機能を指します。

- * 無停止アップグレード *

アプリケーションを中断することなくノードのハードウェアまたはソフトウェアをアップグレードできること。

- * 無停止ボリューム移動 *

ボリュームを使用しているすべてのアプリケーションを中断することなく、クラスタ内で自由にボリュームを移動できること。SMB 接続の場合、SMB のすべてのバージョンで無停止でのボリューム移動がサポートされます。

- * 永続的ハンドル *

接続が切断した場合に、継続的可用性を備えた接続が透過的に CIFS サーバに再接続できるように設定する SMB 3.0 のプロパティ。永続性ハンドルと同様に、接続中のクライアントとの通信が失われたあとの一定期間、CIFS サーバによって永続的ハンドルが維持されます。ただし、永続的ハンドルは、永続性ハンドルよりも弾力性があります。CIFS サーバは、再接続後のクライアントにハンドルを 60 秒間使用する猶予を与え、その 60 秒間は、ファイルへのアクセスを要求する他のクライアントからのアクセスを拒否します。

永続的ハンドルに関する情報は SFO パートナーの永続的ストレージにミラー化されます。これにより、永続的ハンドルを切断したクライアントが、SFO パートナーによってノードのストレージの所有権が引き継がれた後に、永続性ハンドルを再利用できるようになります。永続的ハンドルは、LIF の移動（永続性ハンドルによってサポートされる）だけでなく、テイクオーバー、ギブバック、およびアグリゲートの再配置についても無停止での処理を提供します。

- * SFO ギブバック *

テイクオーバーイベントから戻るときにホーム位置にアグリゲートを戻します。

- * SFO ペア *

2 つのノードのどちらかが機能を停止した場合に相互にデータを処理するようにコントローラが設定されたノードのペア。システムモデルに応じて、両方のコントローラを 1 つのシャーシに配置することも、別々のシャーシに配置することもできます。2 ノードクラスタでの HA ペアを指します。

- * テイクオーバー *

ストレージのプライマリ所有者が失敗したときに、パートナーがストレージの制御を引き継ぐプロセス。SFO の文脈では、フェイルオーバーとテイクオーバーは同義です。

SMB 3.0の機能が**SMB**共有を介したノンストップオペレーションをサポートする仕組み

SMB 3.0 には、Hyper-V over SMB および SQL Server over SMB 共有のノンストップオペレーションをサポートするためのきわめて重要な機能があります。これには、共有プロパティおよび `_persistent handle_` と呼ばれるファイルハンドルの一種が含まれます `continuously-available`。このハンドルを使用すると、SMBクライアントはファイルオープン状態を再要求し、SMB接続を透過的に再確立できます。

永続的ハンドルは、継続的な可用性が設定された共有に接続する SMB 3.0 対応のクライアントに付与できます。SMB セッションが切断された場合、CIFS サーバは永続的ハンドルの状態に関する情報を保持しま

す。CIFS サーバは、クライアントが再接続できる 60 秒間は他のクライアント要求をブロックするため、永続的ハンドルを持つクライアントは、ネットワークの切断後にハンドルを再要求できます。永続的ハンドルを持つクライアントは、Storage Virtual Machine (SVM) のいずれかのデータLIFを使用して、同じLIFまたは別のLIFを介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、SFO ペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナーノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、SFO パートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、CIFS サーバへの SMB 3.0 接続を、SVM に割り当てられた別のデータ LIF に透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、CIFSサーバはSMB 3.0接続を透過的にフェイルオーバーできますが、障害によってHyper-VアプリケーションがWindows Serverクラスタ内の別のノードにフェイルオーバーされた場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断状態のファイルハンドルによって、Hyper-Vアプリケーションを別のノードで再起動した場合に、そのアプリケーションへのアクセスがブロックされる可能性があります。「フェイルオーバークラスタリング」は、SMB 3.0の一部で、古い競合するハンドルを無効にするメカニズムを提供して、このシナリオに対処します。このメカニズムを使用すると、Hyper-V クラスタノードに障害が発生した場合に、Hyper-V クラスタを迅速にリカバリできます。

透過的なフェイルオーバーを強化するための監視プロトコルの機能

監視プロトコルにより、SMB 3.0 の継続的な可用性が確保された共有（CA 共有）に対するクライアントフェイルオーバー機能が強化されます。監視を使用すると、LIF のフェイルオーバーのリカバリがバイパスされるため、フェイルオーバーにかかる時間が短縮されます。ノードを使用できなくなると、SMB 3.0 接続のタイムアウトを待たずにアプリケーションサーバに通知されます。

フェイルオーバーはシームレスです。クライアント上で実行されているアプリケーションは、フェイルオーバーが発生したことを認識しません。監視プロトコルを使用できなくてもフェイルオーバー処理に影響はありませんが、監視プロトコルを使用しないフェイルオーバーは効率が落ちます。

監視プロトコルを使用する高度なフェイルオーバーは、次の要件が満たされた場合に実行できます。

- SMB 3.0 が有効になっている SMB 3.0 対応の CIFS サーバでのみ使用できる。
- 共有で、共有の継続的な可用性プロパティが設定されている SMB 3.0 を使用している必要があります。
- アプリケーションサーバの接続先ノードのSFOパートナーに、少なくとも1つ以上、アプリケーションサーバのデータをホストするStorage Virtual Machine (SVM) に割り当てられた稼働中のデータLIFがある。



監視プロトコルは、SFO ペアの間で実行されます。LIF はクラスタ内の任意のノードに移行できるため、すべてのノードがその SFO パートナーの監視プロトコルであることが必要になる場合があります。アプリケーションサーバのデータをホスティングしている SVM がパートナーノード上にアクティブなデータ LIF を持っていない場合、監視プロトコルは、指定されたノード上で SMB 接続の迅速なフェイルオーバーを提供することはできません。したがって、そのような構成の 1 つをホスティングしている SVM には、クラスタ内のすべてのノードに少なくとも 1 つ以上のデータ LIF が必要です。

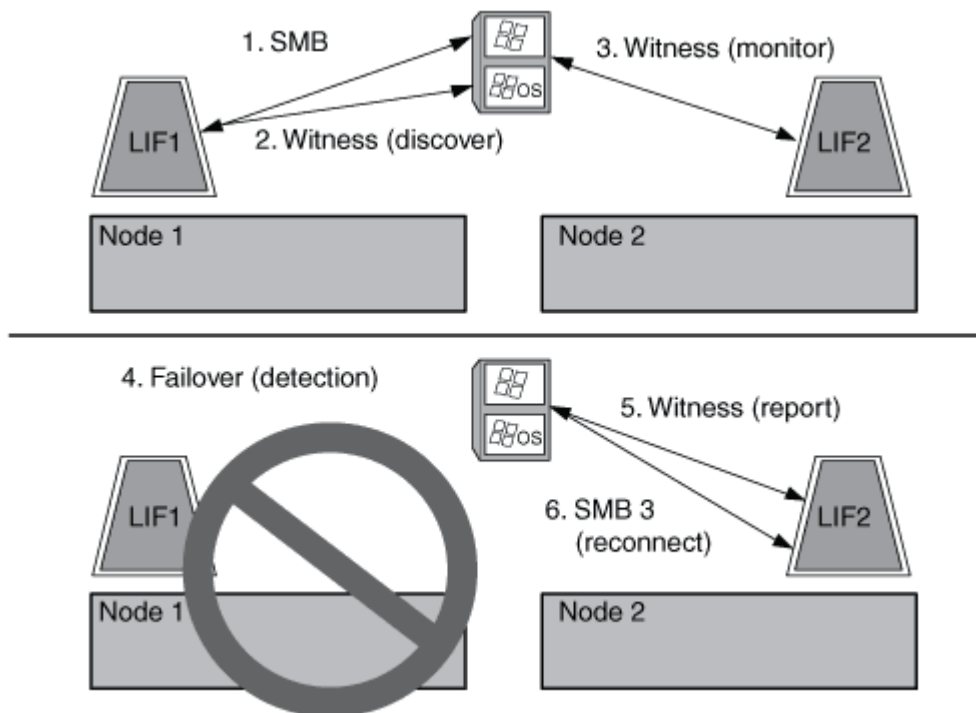
- アプリケーションサーバは、個々の LIF IP アドレスではなく、DNS に格納されている CIFS サーバ名を使用して CIFS サーバに接続する必要があります。

監視プロトコルの仕組み

ONTAPは、ノードのSFOパートナーを監視として使用して、監視プロトコルを実装します。障害が発生した場合、パートナーは障害を迅速に検出し、SMBクライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーションサーバがノード1への継続的可用性を備えたSMB接続を確立すると、CIFSサーバからアプリケーションサーバに監視が利用可能であることが通知されます。
2. アプリケーションサーバは、ノード1に監視サーバのIPアドレスを要求し、Storage Virtual Machine (SVM) に割り当てられたノード2 (SFO パートナー) のデータ LIF の IP アドレスリストを受け取ります。
3. アプリケーションサーバは、いずれかのIPアドレスを選択し、ノード2への監視接続を作成して、ノード1の継続的可用性を備えた接続を移行する必要がある場合に通知されるように登録します。
4. ノード1でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバーイベントが検出され、監視接続を介してアプリケーションサーバに、SMB接続をノード2に移行する必要があることが通知されます。
6. アプリケーションサーバは、SMBセッションをノード2に移行し、クライアントアクセスを中断することなく接続をリカバリします。



リモートVSSによる共有ベースのバックアップ

リモートVSSを使用した共有ベースのバックアップの概要

リモートVSSを使用して、CIFSサーバに格納されているHyper-V仮想マシンファイルの

共有ベースのバックアップを実行できます。

MicrosoftのリモートVSS（ボリュームシャドウコピーサービス）は、既存のMicrosoft VSSインフラを拡張したものです。リモートVSSでは、SMB共有のシャドウコピーをサポートするようにVSSインフラが拡張されました。また、Hyper-Vなどのサーバアプリケーションでは、SMBファイル共有にVHDファイルを格納できます。これらの拡張機能を使用すると、データと構成ファイルを共有に格納する仮想マシンに対して、アプリケーションと整合性のあるシャドウコピーを作成できます。

リモートVSSの概念

ここでは、リモートVSS（ボリュームシャドウコピーサービス）がHyper-V over SMB構成でバックアップサービスでどのように使用されるかを理解するために必要な概念について説明します。

• * VSS（ボリューム・シャドウ・コピー・サービス） *

特定のボリューム上の特定の時点のデータのバックアップコピーまたはSnapshotを作成するMicrosoftのテクノロジー。VSSは、データサーバ、バックアップアプリケーション、ストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

• * リモート VSS（リモートボリュームシャドウコピーサービス） *

SMB 3.0共有を介してデータにアクセスした特定の時点で整合性のあるデータの共有ベースのバックアップコピーを作成するMicrosoftのテクノロジーです。Volume Shadow Copy Service と呼ばれることもあります。

• * シャドウコピー *

共有に含まれるデータセットの明確に定義された特定の時点における複製です。シャドウコピーは、整合性のあるポイントインタイムバックアップを作成するために使用されます。これにより、システムまたはアプリケーションは元のボリューム上のデータを継続的に更新できます。

• * シャドウ・コピー・セット *

1つ以上のシャドウコピーの集まりで、各シャドウコピーが1つの共有に対応します。シャドウコピーセット内のシャドウコピーは、同じ処理でバックアップする必要があるすべての共有を表します。セットに含めるシャドウコピーは、VSS対応アプリケーションのVSSクライアントによって識別されます。

• * シャドウ・コピー・セットの自動リカバリ *

リモートVSSに対応したバックアップアプリケーションのバックアッププロセスの一部。シャドウコピーが格納されているレプリカディレクトリでポイントインタイムの整合性が確保されます。バックアップの開始時に、アプリケーション上のVSSクライアントは、バックアップ用にスケジュールされたデータ（Hyper-Vの場合は仮想マシンファイル）のソフトウェアチェックポイントの取得をアプリケーションにトリガーします。VSSクライアントは、アプリケーションの続行を許可します。シャドウコピーセットが作成されると、リモートVSSによってシャドウコピーセットが書き込み可能になり、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションは、前の手順で作成したソフトウェアチェックポイントを使用して自動リカバリを実行し、シャドウコピーセットをバックアップ用に準備します。自動リカバリでは、チェックポイントの作成後にファイルとディレクトリに加えられた変更を展開することで、シャドウコピーを整合性のある状態にします。自動リカバリは、VSS対応バックアップのオプションの手順です。

- * シャドウ・コピー ID *

シャドウコピーを一意に識別するGUIDです。

- * シャドウ・コピー・セット ID *

同じサーバに対する一連のシャドウコピーIDを一意に識別するGUID。

- * SnapManager for Hyper-V *

Microsoft Windows Server 2012 Hyper-Vのバックアップ/リストア処理を自動化して簡易化するソフトウェアです。リモートVSSと自動リカバリを使用して、SMB共有経由でHyper-Vファイルをバックアップします。

関連情報

[Hyper-VオヨヒSQLServeroverSMBノノンストツフオヘレエシヨニカンスルキナ概念](#)

[リモートVSSによる共有ベースのバックアップ](#)

リモートVSSで使用されるディレクトリ構造の例

リモートVSSは、シャドウコピーの作成時に、Hyper-V仮想マシンファイルが格納されているディレクトリ構造をトラバースします。仮想マシンファイルのバックアップを正常に作成できるように、適切なディレクトリ構造について理解しておくことが重要です。

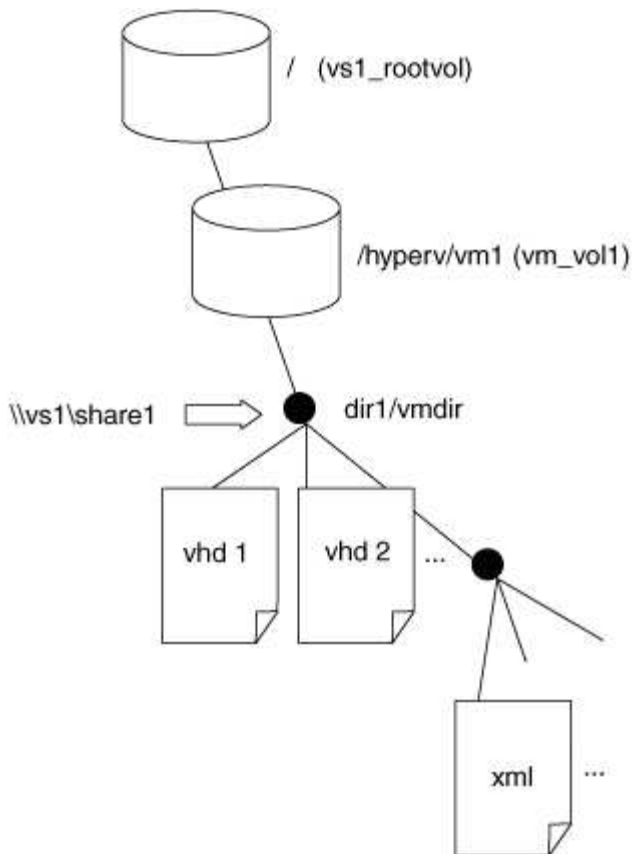
シャドウコピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 仮想マシンファイルの格納に使用されるディレクトリ構造内に存在するのは、ディレクトリと通常のファイルだけです。

ディレクトリ構造には、ジャンクション、リンク、または通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシンファイルの格納に使用されるディレクトリ構造が、設定されているシャドウコピーのディレクトリ階層を超えることはありません。
- 共有のルートディレクトリには、仮想マシンファイルまたはディレクトリのみが含まれています。

次の図では、Storage Virtual Machine (SVM) vs1上でジャンクションポイントをにしてvm_vol1という名前のボリュームが作成されています /hyperv/vm1。ジャンクションポイントの下に、仮想マシンファイルを格納するサブディレクトリが作成されます。Hyper-Vサーバの仮想マシンファイルには、パスのshare1を介してアクセスします /hyperv/vm1/dir1/vmdir。シャドウコピーサービスによって、share1の下のディレクトリ構造（設定されたシャドウコピーのディレクトリ階層まで）に格納されているすべての仮想マシンファイルのシャドウコピーが作成されます。



SnapManager for Hyper-VによるHyper-V over SMBのリモートVSSベースのバックアップの管理方法

SnapManager for Hyper-V を使用して、リモート VSS ベースのバックアップサービス进行管理できます。スペース効率に優れたバックアップセットを作成するには、SnapManager for Hyper-V で管理されているバックアップサービスを使用すると効果的です。

Hyper-V で管理されているバックアップ向けに SnapManager を最適化するには、次のようなものがあります。

- SnapDrive と ONTAP の統合により、SMB 共有の場所を検出する際のパフォーマンスが最適化されます。

ONTAP は、共有が存在するボリュームの名前を SnapDrive に提供します。

- SnapManager for Hyper-V は、シャドウコピーサービスでコピーする必要がある SMB 共有内の仮想マシンファイルのリストを指定します。

仮想マシンファイルの対象リストを指定することで、シャドウコピーサービスで、共有内のすべてのファイルのシャドウコピーを作成する必要がなくなります。

- Storage Virtual Machine (SVM) に、Hyper-V がリストアに使用するための SnapManager の Snapshot コピーが保持されます。

バックアップフェーズはありません。バックアップは、スペース効率に優れた Snapshot コピーです。

SnapManager for Hyper-V は、次のプロセスを使用して、Hyper-V over SMB のバックアップとリストアの機能を提供します。

1. シャドウコピー処理を準備しています

SnapManager for Hyper-V アプリケーションの VSS クライアントが、シャドウコピーセットを設定します。VSS クライアントは、どの共有をシャドウコピーセットに含めるかに関する情報を収集し、この情報を ONTAP に提供します。セットには 1 つ以上のシャドウコピーが含まれる場合があり、1 つのシャドウコピーが 1 つの共有に対応します。

2. シャドウコピーセットの作成（自動リカバリが使用される場合）

シャドウコピーセットに含まれている共有ごとに、ONTAP がシャドウコピーを作成し、シャドウコピーを書き込み可能にします。

3. シャドウコピーセットの公開

ONTAP によって作成されたシャドウコピーが Hyper-V 用の SnapManager に公開され、アプリケーションの VSS ライターが自動リカバリを実行できるようになります。

4. シャドウコピーセットを自動的にリカバリします

シャドウコピーセットの作成中に、バックアップセットに含まれているファイルにアクティブな変更が発生する時間帯があります。アプリケーションの VSS ライターは、シャドウコピーを更新して、バックアップ前に完全な整合性が確保された状態にする必要があります。



自動リカバリの実行方法はアプリケーションに固有です。リモート VSS はこのフェーズには関連しません。

5. シャドウコピーセットの完了とクリーンアップを行います

自動リカバリの完了後に、VSS クライアントが ONTAP に通知します。シャドウコピーセットが読み取り専用になり、バックアップできる状態になります。バックアップに SnapManager for Hyper-V を使用する場合は、Snapshot コピー内のファイルがバックアップになるため、バックアップフェーズでは、バックアップセット内の共有を含むボリュームごとに Snapshot コピーが作成されます。バックアップが完了すると、シャドウコピーセットが CIFS サーバから削除されます。

Hyper-V over SMB および SQL Server over SMB 共有での ODX コピーオフロードの使用方法

Offloaded Data Transfer（ODX；オフロードデータ転送）は `_copy offloaded_` と呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やストレージデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。ONTAP ODX コピーオフロードを使用すると、アプリケーションサーバで SMB インストール経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX 以外のファイル転送では、ソース CIFS サーバからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーション CIFS サーバに転送します。要約すると、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODX ファイル転送では、データがソースからデスティネーションに直接

コピーされます。

ODXオフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現されるパフォーマンス上のメリットには、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用率（CPU、メモリ）の削減、ネットワークI/O帯域幅の使用量の削減などがあります。

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

ODXコピーと移動の使用は次のユースケースでサポートされます。

- ボリューム内

ソースとデスティネーションのファイルまたはLUNは、同じボリューム内にあります。

- ボリュームが異なり、ノードとStorage Virtual Machine (SVM) は同じ

ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- ボリュームとノードが異なり、SVMは同じ

ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは同じSVMに所有されます。

- SVMが異なり、ノードは同じ

ソースとデスティネーションのファイルまたはLUNは、同じノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

- SVMとノードが異なる

ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。データは複数のSVMに所有されます。

Hyper-VソリューションでのODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- Hyper-VでODXコピーオフロードのパススルーを使用すると、仮想ハードディスク (VHD) ファイル内またはVHDファイル間でデータをコピーしたり、同じクラスタ内のマッピングされたSMB共有と接続されたiSCSI LUNの間でデータをコピーしたりできます。

これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定VHDを作成する場合、ODXを使用してディスクを初期化します。初期化された既知のトークンを使用してディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合、ODXコピーオフロードを使用して仮想マシンのストレージを移行します。



Hyper-VでのODXコピーオフロードのパススルーのユースケースを利用するには、ゲストオペレーティングシステムでODXがサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODXをサポートするストレージ（SMBまたはSAN）から作成されたSCSIディスクである必要があります。ゲストオペレーティングシステムのIDEディスクは、ODXパススルーをサポートしていません。

SQL ServerソリューションでのODXコピーオフロードの具体的なユースケースには、次のようなものがあります。

- ODXコピーオフロードを使用すると、マッピングされたSMB共有間、または同じクラスタ内のSMB共有と接続されたiSCSI LUNの間でSQL Serverデータベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合は、ODXコピーオフロードを使用してデータベースのエクスポートとインポートを行います。

設定に関する要件と考慮事項

ONTAPとライセンスの要件

SVMでノンストップオペレーションを実現するSQL Server over SMBまたはHyper-V over SMBソリューションを作成するときは、ONTAPとライセンスの特定の要件について理解しておく必要があります。

ONTAPのバージョンの要件

- Hyper-V over SMB

ONTAPでは、Windows Server 2012以降で実行されるHyper-VでのSMB共有を介したノンストップ オペレーションがサポートされます。

- SQL Server over SMB

ONTAPでは、Windows Server 2012以降で実行されるSQL Server 2012以降でのSMB共有を介したノンストップ オペレーションがサポートされます。

SMB共有を介したノンストップ オペレーションがサポートされるONTAP、Windows Server、およびSQL Serverのバージョンの最新情報については、Interoperability Matrixを参照してください。

["NetApp Interoperability Matrix Tool"](#)

ライセンス要件

次のライセンスが必要です。

- CIFS
- FlexClone（Hyper-V over SMBのみ）

このライセンスは、バックアップにリモートVSSを使用する場合に必要になります。シャドウ コピー サービスでは、バックアップの作成時に使用されるファイルのポイントインタイム コピーを作成するため

にFlexCloneが使用されます。

リモートVSSを使用しないバックアップ方式を使用する場合、FlexCloneライセンスはオプションです。

FlexCloneライセンスには含まれていない"ONTAP One"です。ONTAP Oneがない場合は、必要に"必要なライセンスがインストールされていることを確認する"に応じて、必要に応じて"インストールする"を実行する必要があります。

ネットワークとデータLIFの要件

ノンストップオペレーション用にSQL Server over SMBまたはHyper-V over SMB構成を作成する場合は、一定のネットワークとデータLIFの要件について理解しておく必要があります。

ネットワークプロトコルの要件

- IPv4およびIPv6ネットワークがサポートされています。
- SMB 3.0以降が必要です。

SMB 3.0には、ノンストップオペレーションを実現するために必要な、継続的可用性を備えたSMB接続の確立に必要な機能が用意されています。

- DNSサーバには、CIFSサーバ名をStorage Virtual Machine (SVM) 上のデータLIFに割り当てられたIPアドレスにマッピングするエントリが格納されている必要があります。

通常、Hyper-VまたはSQL Serverアプリケーションサーバは、仮想マシンまたはデータベースファイルへのアクセス時に複数のデータLIFを介して複数の接続を確立します。正常に機能するためには、アプリケーションサーバは、複数の一意のIPアドレスへの複数の接続を確立するのではなく、CIFSサーバ名を使用してこれらの複数のSMB接続を確立する必要があります。

監視でも、個々のLIF IPアドレスではなく、CIFSサーバのDNS名を使用する必要があります。

ONTAP 9.4以降では、SMBマルチチャネルを有効にすることで、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスを向上させることができます。そのためには、クラスタとクライアントに1G、10G、またはそれ以上のNICを複数導入する必要があります。

データLIFの要件

- SMB経由のアプリケーションサーバソリューションをホストするSVMには、クラスタ内のすべてのノードに稼働しているデータLIFが少なくとも1つ必要です。

SVMデータLIFは、アプリケーションサーバがアクセスするデータを現在ホストしていないノードを含む、クラスタ内の他のデータポートにフェイルオーバーできます。さらに、監視ノードは常にアプリケーションサーバが接続されているノードのSFOパートナーであるため、クラスタ内のすべてのノードが監視ノードになる可能性があります。

- データLIFは、自動的にリバートされるように設定しないでください。

テイクオーバーまたはギブバックの発生後、データLIFをホームポートに手動でリバートする必要があります。

- すべてのデータLIFのIPアドレスがDNSにエントリを持ち、すべてのエントリがCIFSサーバ名に解決される必要があります。

アプリケーションサーバは、CIFSサーバ名を使用してSMB共有に接続する必要があります。LIFのIPアドレスを使用して接続を確立するようにアプリケーションサーバを設定しないでください。

- CIFSサーバ名がSVM名と異なる場合は、DNSエントリがCIFSサーバ名に解決される必要があります。

Hyper-V over SMB用のSMBサーバとボリュームの要件

ノンストップオペレーション用にHyper-V over SMB構成を作成する場合、一定のSMBサーバとボリュームの要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

- 自動ノードリファラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

Hyper-Vマシンファイル以外のデータへのアクセスに自動ノードリファラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- SMBサーバが属しているドメインで、KerberosとNTLMの両方の認証が許可されている必要があります。

ONTAPはリモートVSSに対してKerberosサービスをアドバタイズしないため、ドメインはNTLMを許可するように設定する必要があります。

- シャドウコピー機能が有効になっている必要があります。

この機能はデフォルトで有効になっています。

- シャドウコピーサービスでシャドウコピーの作成時に使用されるWindowsドメインアカウントが、SMBサーバのローカルのBUILTIN\AdministratorsグループまたはBUILTIN\Backup Operatorsグループに属している必要があります。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含む

ボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です。

使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

関連情報

"Microsoft TechNetライブラリ : technet.microsoft.com/en-us/library/"

SQL Server over SMB ノ SMB サアハトホリユウムノヨウケン

ノンストップオペレーション用にSQL Server over SMB構成を作成する場合は、SMBサーバとボリュームの一定の要件について理解しておく必要があります。

SMBサーバの要件

- SMB 3.0が有効になっている必要があります。

これはデフォルトで有効になっています。

- デフォルトのUNIXユーザのCIFSサーバオプションが、有効なUNIXユーザアカウントを使用して設定されている必要があります。

アプリケーションサーバは、SMB接続の作成時にマシンアカウントを使用します。すべてのSMBアクセスで、Windowsユーザが1つのUNIXユーザアカウントまたはデフォルトのUNIXユーザアカウントに正常にマッピングされている必要があるため、ONTAPは、アプリケーションサーバのマシンアカウントをデフォルトのUNIXユーザアカウントにマッピングできる必要があります。

また、SQL ServerはドメインユーザをSQL Serverサービスアカウントとして使用します。サービスアカウントは、デフォルトのUNIXユーザにもマッピングする必要があります。

- 自動ノードリファラルを無効にする必要があります（この機能はデフォルトで無効になっています）。

SQL Serverデータベースファイル以外のデータへのアクセスに自動ノードリファラルを使用する場合は、そのデータ用のSVMを別途作成する必要があります。

- ONTAPへのSQL Serverのインストールに使用するWindowsユーザアカウントには、SeSecurityPrivilege権限を割り当てる必要があります。

この権限は、SMBサーバのローカルのBUILTIN\Administratorsグループに割り当てられます。

ボリュームの要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

継続的可用性を備えたSMB接続を使用してアプリケーションサーバのNDOを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したNDOに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、SMB共有を介したNDOに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダにそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

関連情報

"Microsoft TechNetライブラリ : technet.microsoft.com/en-us/library/"

Hyper-V over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするHyper-V over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項について理解しておく必要があります。

共有の要件

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- リモートVSSに対応したバックアップサービスを使用する場合は、ジャンクションを含む共有にHyper-Vファイルを配置することはできません。

自動リカバリの場合、共有のトラバース時にジャンクションが見つかったら、シャドウコピーの作成は失敗します。自動リカバリ以外の場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

- リモートVSSに対応したバックアップサービスと自動リカバリを使用する場合は、次の内容を含む共有

にHyper-Vファイルを配置できません。

- シンボリックリンク、ハードリンク、またはワイドリンク
- 通常以外のファイル

シャドウコピーを実行する共有にリンクまたは通常以外のファイルがある場合、シャドウコピーの作成は失敗します。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

- シャドウコピー処理を正常に実行するには、ボリュームに十分な利用可能スペースが必要です（Hyper-V over SMB の場合のみ）。

使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。この要件は、自動リカバリを使用するシャドウコピーにのみ適用されます。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
 - ホームディレクトリ
 - 属性のキャッシュ
 - BranchCache

考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- Hyper-V over SMB構成では、次の機能はサポートされません。
 - 監査
 - FPolicy
- パラメータがに設定され Yes`ているSMB共有ではウィルススキャンは実行されません`continuously-availability。

SQL Server over SMBでの継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートするSQL Server over SMB構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項について理解しておく必要があります。

共有の要件

- 仮想マシンファイルを格納するボリュームは、NTFSセキュリティ形式のボリュームとして作成する必要があります。

継続的可用性を備えたSMB接続を使用してアプリケーションサーバのノンストップオペレーションを実現するには、共有を含むボリュームがNTFSボリュームである必要があります。さらに、常にNTFSボリュームである必要があります。mixedセキュリティ形式のボリュームまたはUNIXセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに直接使用することはできません。mixedセキュリティ形式のボリュームをNTFSセキュリティ形式のボリュームに変更し、そのボリュームをSMB共有を介したノンストップオペレーションに使用する場合は、ボリュームの最上位にACLを手動で配置し、格納されているすべてのファイルおよびフォルダ

にそのACLを適用する必要があります。そうしないと、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポート/インポートが、ソースボリュームまたはデスティネーションボリュームが最初はmixedセキュリティ形式またはUNIXセキュリティ形式のボリュームとして作成され、あとでNTFSセキュリティ形式に変更された場合に失敗する可能性があります。

- アプリケーションサーバで使用される共有には、continuously-availableプロパティが設定されている必要があります。

継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとにSMB共有に無停止で再接続し、ファイルロックを再要求できます。

- データベースファイルを含むボリュームにジャンクションを含めることはできますが、SQL Serverではデータベースディレクトリ構造の作成時にジャンクションをまたぐことはありません。
- SnapCenter Plug-in for Microsoft SQL Serverの処理を成功させるには、ボリュームに十分な利用可能スペースが必要です。

SQL Serverデータベースファイルが配置されているボリュームには、データベースディレクトリ構造と、共有内に格納されているすべてのファイルを格納できる十分なサイズが必要です。

- アプリケーションサーバで使用される継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
 - ホームディレクトリ
 - 属性のキャッシュ
 - BranchCache

共有に関する考慮事項

- クォータは継続的可用性を備えた共有でサポートされます。
- SQL Server over SMB構成では、次の機能はサポートされません。
 - 監査
 - FPolicy
- 共有プロパティが設定されているSMB共有ではウィルススキャンは実行されません continuously-availability。

Hyper-V over SMB コウセイニカンスルリモートVSSニカンスルコウリヨシコウ

Hyper-V over SMB 構成用のリモート VSS に対応したバックアップソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

一般的なリモート VSS の考慮事項

- Microsoft のアプリケーションサーバ 1 つにつき、最大 64 の共有を設定できます。

1 つのシャドウコピーセットに 64 個を超える共有がある場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。
- アクティブなシャドウコピーセットは、1 台の CIFS サーバで 1 つしか許可されません。

同じCIFSサーバでシャドウコピー処理を実行中の場合、シャドウコピー処理は失敗します。これはMicrosoftの要件です。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
 - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかったら、シャドウコピーの作成は失敗します。
 - 自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

自動リカバリを行うシャドウコピーのみに適用されるリモート **VSS** の考慮事項

一部の制限は、自動リカバリを行うシャドウコピーにのみ適用されます。

- シャドウコピーの作成で許可される最大サブディレクトリ階層は 5 層です。

これは、シャドウコピーサービスによってシャドウコピーバックアップセットが作成されるディレクトリ階層です。仮想マシンファイルを含むディレクトリのネストレベルが 5 よりも深い場合、シャドウコピーの作成は失敗します。この目的は、共有のクローニング時におけるディレクトリのトラバースを制限することです。最大ディレクトリ階層は CIFS サーバオプションを使用して変更できます。

- ボリューム上に利用可能なスペースが十分ある必要があります。

使用可能なスペースは、シャドウコピーバックアップセットに含まれる共有内のすべてのファイル、ディレクトリ、およびサブディレクトリで使用される合計スペース以上にする必要があります。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、リンクまたは通常以外のファイルは許可されません。

シャドウコピーの作成は、そのシャドウコピーに対応する共有内にリンクまたは通常以外のファイルがある場合には失敗します。これらのファイルはクローニングプロセスでサポートされていません。

- ディレクトリに対する NFSv4 ACL は許可されません。

シャドウコピーの作成では、ファイルの NFSv4 ACL は維持されますが、ディレクトリの NFSv4 ACL は失われます。

- シャドウコピーセットの作成に許可される時間は最大 60 秒です。

Microsoft の仕様により、シャドウコピーセットの作成に許可される時間は最大 60 秒です。この時間内に VSS クライアントでシャドウコピーセットを作成できない場合、シャドウコピー処理は失敗します。したがって、シャドウコピーセット内のファイル数には制限があります。バックアップセットに含めることができる実際のファイル数または仮想マシン数は、一定ではなく、多くの要因に依存するため、お客様の環境ごとに判断する必要があります。

SQL ServerおよびHyper-V over SMBでのODXコピーオフロードの要件

アプリケーションサーバ経由でデータを送信せずに、仮想マシンファイルを移行する場合や、データベースファイルをソースストレージからデスティネーションストレージに直接エクスポートおよびインポートする場合は、ODX コピーオフロードが有効になっ

ている必要があります。ODX コピーオフロードと SQL Server および Hyper-V over SMB ソリューションを使用する場合は、理解しておくべきいくつかの要件があります。

ODX コピーオフロードを使用すると、パフォーマンスが大幅に向上します。この CIFS サーバオプションは、デフォルトで有効に設定されています。

- ODX コピーオフロードを使用するには、SMB 3.0 が有効になっている必要があります。
- ソースボリュームは1.25GB以上である必要があります。
- コピーオフロードに使用するボリュームで重複排除を有効にする必要があります。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは8Kのみです。

二次圧縮形式はサポートされません

- ODX コピーオフロードを使用して Hyper-V ゲストをディスク内やディスク間で移行するには、Hyper-V サーバが SCSI ディスクを使用するように設定されている必要があります。

デフォルトでは IDE ディスクが設定されますが、ディスクが IDE ディスクを使用して作成されている場合は、ゲストの移行時に ODX コピーオフロードは機能しません。

SQL ServerおよびHyper-V over SMB構成に関する推奨事項

SQL Server over SMB および Hyper-V over SMB 構成が安定して機能するようにするには、ソリューションの設定に関する推奨されるベストプラクティスについて理解しておく必要があります。

一般的な推奨事項

- アプリケーションサーバのファイルは一般的なユーザデータとは別に格納します。

可能な場合は、Storage Virtual Machine (SVM) とそのストレージ全体をアプリケーションサーバのデータ専用にしします。

- パフォーマンスを最大限に高めるには、アプリケーションサーバのデータを格納する SVM で SMB 署名を無効にします。
- パフォーマンスの最適化とフォールトトレランスの向上を図るためには、SMB マルチチャネルを有効にして、1つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立できるようにします。
- Hyper-VまたはSQL Server over SMB構成で使用する共有以外では、継続的可用性を備えた共有を作成しないでください。
- 継続的な可用性を確保するために使用される共有については、変更通知を無効に
- アグリゲートの再配置 (ARL) には一部の処理が一時停止するフェーズがあるため、ARL と同時にボリュームの移動を実行しないようにします。
- Hyper-V over SMBソリューションでは、クラスタ化された仮想マシンを作成するときにゲスト内iSCSIドライバを使用します。ONTAP SMB共有のHyper-V over SMBでは共有 `VHDX` ファイルはサポートされません。

Hyper-VまたはSQL Server over SMB構成の計画

ボリューム構成ワークシートに記入する

このワークシートを使用すると、SQL Server および Hyper-V over SMB 構成用のボリュームを作成する際に必要となる値を簡単に記録できます。

ボリュームごとに、次の情報を指定する必要があります。

- Storage Virtual Machine (SVM) 名

SVM 名はすべてのボリュームで同じです。

- ボリューム名
- アグリゲート名

ボリュームは、クラスタ内のノード上のアグリゲートに作成できます。

- サイズ
- ジャンクションパス

アプリケーションサーバのデータを格納するボリュームの作成時には、次の事項を考慮してください。

- ルートボリュームのセキュリティ形式が NTFS でない場合は、ボリュームの作成時にセキュリティ形式を NTFS として指定する必要があります。

デフォルトで、ボリュームは SVM ルートボリュームのセキュリティ形式を継承します。

- ボリュームには、デフォルトのボリュームスペースギャランティを設定する必要があります。
- 必要に応じて、スペースのオートサイズ管理を設定できます。
- Snapshot コピーのスペースリザベーションを決定するオプションは、に設定する必要があります 0。
- ボリュームに適用される Snapshot ポリシーを無効にする必要があります。

SVM の Snapshot ポリシーが無効になっている場合は、ボリュームの Snapshot ポリシーを指定する必要はありません。ボリュームは SVM の Snapshot ポリシーを継承します。SVM の Snapshot ポリシーが無効になっておらず、Snapshot コピーを作成するように設定されている場合は、Snapshot ポリシーをボリュームレベルで指定し、そのポリシーを無効にする必要があります。Snapshot コピーの作成と削除は、シャドウコピーサービス対応のバックアップと SQL Server バックアップによって管理されます。

- ボリュームに負荷共有ミラーを設定することはできません。

アプリケーションサーバで使用される共有を作成するジャンクションパスを選択する際は、共有エントリポイントの下に結合されたボリュームが含まれないようにする必要があります。

たとえば、仮想マシンファイルを「vol1」、「vol2」、「vol3」、および「vol4」という名前の4つのボリュームに格納する場合は、例に示すネームスペースを作成できます。その後、アプリケーションサーバの共有をパス、 /data1/vol2 /data2/vol3、およびに /data2/vol4`作成できます ` /data1/vol1。

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

情報の種類	値
ボリューム1：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム2：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム3：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム4：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム5：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
ボリューム6：ボリューム名、アグリゲート、サイズ、ジャンクションパス	
追加ボリューム：ボリューム名、アグリゲート、サイズ、ジャンクションパス _	

SMB共有設定ワークシートに記入する

このワークシートを使用して、SQL ServerおよびHyper-V over SMB構成用の継続的可用性を備えたSMB共有を作成する際に必要となる値を記録してください。

SMB共有のプロパティと設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine (SVM) 名

SVM 名はすべての共有で同じです

- 共有名
- パス
- 共有プロパティ

次の2つの共有プロパティを設定する必要があります。

- oplocks
- continuously-available

次の共有プロパティは設定しないでください。

- homedirectory attributecache
- branchcache
- access-based-enumeration
 - シンボリックリンクを無効にする必要があります（パラメータの値`-symlink-properties`はnull [""]にする必要があります）。

共有パスに関する情報

リモートVSSを使用してHyper-Vファイルをバックアップする場合は、Hyper-Vサーバから仮想マシンファイルの格納場所へのSMB接続を確立する際に使用する共有パスの選択が重要になります。共有はネームスペース内の任意のポイントに作成できますが、Hyper-Vサーバで使用される共有のパスに結合されたボリュームを含めることはできません。ジャンクションポイントを含む共有パスでシャドウコピー処理を実行することはできません。

データベースディレクトリ構造を作成する場合、SQL Serverはジャンクションを横断できません。ジャンクションポイントを含むSQL Serverの共有パスは作成しないでください。

たとえば、次に示すネームスペースを例にとると、仮想マシンファイルまたはデータベースファイルをボリューム「vol1」、「vol2」、「vol3」、および「vol4」に格納する場合、アプリケーションサーバの共有をパス、`/data1/vol2`、`/data2/vol3`およびに`/data2/vol4`作成する必要があります`/data1/vol1`。

Vserver	Volume	Junction		Junction	
		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	



管理用にパスと`/data2`パスに共有を作成することはできます`/data1`が、データの格納にこれらの共有を使用するようにアプリケーションサーバを設定しないでください。

情報の種類	値
ボリューム1：SMB共有名とパス	
ボリューム2：SMB共有名とパス	
ボリューム3：SMB共有名とパス	
ボリューム4：SMB共有名とパス	
ボリューム5：SMB共有名とパス	
ボリューム6：SMB共有名とパス	
ボリューム7：SMB共有名とパス	
追加ボリューム：SMB共有名およびパス	

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成の作成

Hyper-VおよびSQL Server over SMBでノンストップオペレーションをシミュレーションするONTAP構成の作成

SMBを介したノンストップオペレーションを実現するHyper-VおよびSQL Server環境を使用するためには、ONTAPの設定手順をいくつか実行する必要があります。

Hyper-V over SMBおよびSQL Server over SMBでノンストップオペレーションを実現するONTAP構成を作成する前に、次のタスクを完了しておく必要があります。

- クラスタでタイムサービスをセットアップする必要があります。
- SVM用のネットワークをセットアップします。
- SVMを作成します。
- SVMでデータLIFインターフェイスが設定されている必要があります。
- SVMでDNSが設定されている必要があります。
- SVMに必要なネームサービスをセットアップします。
- SMBサーバを作成しておく必要があります。

関連情報

[Hyper-VまたはSQL Server over SMB構成の計画](#)

Kerberos認証とNTLMv2認証の両方が許可されていることの確認 (Hyper-V over SMB 共有)

Hyper-V over SMB のノンストップオペレーションを実行する場合、データ SVM の CIFS サーバおよび Hyper-V サーバで Kerberos 認証と NTLMv2 認証の両方が許可されていなければなりません。CIFS サーバと Hyper-V サーバの両方について、使用できる認証方法を制御する設定を確認する必要があります。

タスクの内容

Kerberos 認証は、継続的可用性を備えた共有への接続を確立する際に必要になります。また、リモート VSS のプロセスで NTLMv2 認証が使用されます。そのため、Hyper-V over SMB 構成に対しては、両方の認証方法を使用した接続がサポートされている必要があります。

Kerberos 認証と NTLMv2 認証の両方が許可されるように、次の設定を行う必要があります。

- Storage Virtual Machine (SVM) で SMB のエクスポートポリシーが無効になっている必要があります。

SVM では、Kerberos 認証と NTLMv2 認証がどちらも常に有効になりますが、エクスポートポリシーを使用することで認証方法に基づいてアクセスを制限することが可能です。

SMB のエクスポートポリシーは省略可能で、デフォルトでは無効になっています。エクスポートポリシーが無効になっている場合、CIFS サーバでは Kerberos 認証と NTLMv2 認証の両方がデフォルトで許可されません。

- CIFS サーバと Hyper-V サーバが属するドメインで、Kerberos 認証と NTLMv2 認証の両方を許可する必要があります。

Kerberos 認証は、Active Directory ドメインではデフォルトで有効になります。ただし、NTLMv2 認証は、セキュリティポリシーの設定またはグループポリシーで禁止されている場合があります。

手順

1. 次の手順に従って、SVM でエクスポートポリシーが無効になっていることを確認します。

- a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- b. CIFSサーバオプションがに設定されている `false` ことを確認し `-is-exportpolicy-enabled` ます。

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

- c. admin権限レベルに戻ります。

```
set -privilege admin
```

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

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

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

ドメインで許可されている認証方法を確認する方法については、Microsoft TechNetライブラリを参照してください。

4. ドメインで NTLMv2 認証が許可されていない場合は、Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

例

次に、SVM vs1でSMBのエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

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

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

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

ドメインアカウントがデフォルトの**UNIX**ユーザにマッピングされていることを確認する

Hyper-V および SQL Server では、継続的可用性を備えた共有への SMB 接続を作成する際にドメインアカウントを使用します。接続を作成するには、コンピュータアカウントが UNIX ユーザに正しくマッピングされている必要があります。そのための最も便利な方法は、コンピュータアカウントをデフォルトの UNIX ユーザにマッピングすることです。

タスクの内容

Hyper-V および SQL Server は、ドメインコンピュータアカウントを使用して SMB 接続を作成します。また、SQL Server は、SMB 接続を作成するサービスアカウントとしてドメインユーザアカウントを使用します。

Storage Virtual Machine (SVM) を作成すると、ONTAPによってデフォルトユーザ「pcuser」（UIDが）とグループ「pcuser」（GIDが 65534）が自動的に作成され 65534、デフォルトユーザが「pcuser」グループに追加されます。クラスタをData ONTAP 8.2にアップグレードする前に使用していたSVMでHyper-V over SMBソリューションを設定する場合は、デフォルトのユーザとグループが存在していない可能性があります。デフォルトの UNIX ユーザを設定していない場合は、CIFS サーバのデフォルトの UNIX ユーザを設定する前に、デフォルトのユーザとグループを作成する必要があります。

手順

1. デフォルトの UNIX ユーザが存在するかどうかを確認します。

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

2. デフォルトユーザオプションが設定されていない場合は、デフォルトの UNIX ユーザとして指定できる UNIX ユーザが存在するかどうかを確認します。

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

3. デフォルトユーザオプションが設定されておらず、デフォルトの UNIX ユーザとして指定できる UNIX ユーザも存在しない場合は、デフォルトの UNIX ユーザとデフォルトのグループを作成し、デフォルトのユーザをそのグループに追加します。

通常、デフォルトユーザにはユーザ名「pcuser」が与えられ、のUIDを割り当てる必要があります。
`65534`デフォルトのグループには`通常`グループ名として pcuser が与えられますグループに割り当てるGIDはである必要があります`65534`ます。

- a. デフォルトグループを作成します。**+ vserver services unix-group create -vserver vserver_name -name pcuser -id 65534**
- b. デフォルトユーザを作成し、デフォルトグループに追加します。**+ vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534**
- c. デフォルトのユーザとデフォルトグループが正しく設定されていることを確認します。**vserver services unix-user show -vserver vserver_name++ vserver services unix-group show -vserver vserver_name -members**

4. CIFS サーバのデフォルトのユーザが設定されていない場合は、次の手順を実行します。

- a. デフォルトユーザを設定します。

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

- b. デフォルトの UNIX ユーザが正しく設定されていることを確認します。

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

5. アプリケーションサーバのコンピュータアカウントがデフォルトのユーザに正しくマッピングされていることを確認するには、SVMの共有にドライブをマッピングし、コマンドを使用してWindowsユーザとUNIXユーザのマッピングを確認します `vserver cifs session show`。

このコマンドの使用方法の詳細については、マニュアルページを参照してください。

例

次のコマンドでは、CIFS サーバのデフォルトのユーザが設定されていないことがわかりますが、「pcuser」ユーザと「pcuser」グループは存在します。「pcuser」ユーザは、SVM vs1 上の CIFS サーバのデフォルトのユーザとして割り当てられています。

```
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::> vservice unix-user show
```

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

```
cluster1::> vservice unix-group show -members
```

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0
	Users: -	

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

```
cluster1::> vservice 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           : -
```

SVMルートボリュームのセキュリティ形式がNTFSに設定されていることを確認する

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合は、ボリュームを NTFS セキュリティ形式で作成する必要があります。ルートボリュームのセキュリティ形式には、Storage Virtual Machine (SVM) で作成されたボリュームのデフォルトが適用されるため、ルートボリュームのセキュリティ形式はNTFSに設定する必要があります。

タスクの内容

- ルートボリュームのセキュリティ形式は SVM の作成時に指定できます。
- SVMの作成時にルートボリュームのセキュリティ形式をNTFS以外に設定した場合は、あとでコマンドを使用してセキュリティ形式を変更できます `volume modify`。

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

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

2. ルートボリュームのセキュリティ形式が NTFS 以外になっている場合は、セキュリティ形式を NTFS に変更します。

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

3. SVM のルートボリュームのセキュリティ形式が NTFS に設定されていることを確認します。

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

例

次に、SVM vs1のルートボリュームのセキュリティ形式がNTFSになっていることを確認するコマンドの例を示します。

```
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
```

必要なCIFSサーバオプションが設定されていることの確認

Hyper-V および SQL Server over SMB のノンストップオペレーションを実行する場合、必要な CIFS サーバオプションが有効になっており、要件に従って適切に設定されていることを確認する必要があります。

タスクの内容

- SMB 2.x と SMB 3.0 が有効になっている必要があります。
- パフォーマンスが向上したコピーオフロードを使用するには、ODX コピーオフロードが有効になっている必要があります。
- Hyper-V over SMB 解決策でリモート VSS に対応したバックアップサービスを使用する場合は、VSS シャドウコピーサービスが有効になっている必要があります（Hyper-V のみ）。

手順

1. Storage Virtual Machine (SVM) で必要なCIFSサーバオプションが有効になっていることを確認します。
 - a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

- b. 次のコマンドを入力します。

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

次のオプションをに設定する必要があり `true` ます。

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

2. いずれかのオプションがに設定されていない場合は true、次の手順を実行します。
 - a. コマンドを使用して `vserver cifs options modify`` に設定します `true`。
 - b. コマンドを使用して、``vserver cifs options show`` オプションがに設定されていることを確認し `true` ます。
3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次に、SVM vs1でHyper-V over SMB構成の必須オプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、ODX コピーオフロードのオプションを有効にする必要があります。


```

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 smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vservers smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false         true

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

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

cluster1::*> set -privilege admin

```

パフォーマンスと冗長性を確保するためのSMBマルチチャネルの設定

ONTAP 9.4以降では、SMBマルチチャネルを設定して、1つのSMBセッションでONTAPとクライアントの間に複数の接続を確立できます。これにより、Hyper-V over SMBおよびSQL Server over SMB構成のスループットとフォールトトレランスが向上します。

開始する前に

SMBマルチチャネル機能は、クライアントがSMB 3.0以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMBサーバではSMB 3.0以降がデフォルトで有効になっています。

タスクの内容

SMBクライアントは、ONTAPクラスタで適切な設定が見つかり、複数のネットワーク接続を自動的に検出して使用します。

SMBセッションでの同時接続数は、導入しているNICによって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

クライアントはNICごとに1つの接続を確立し、すべての接続にセッションをバインドします。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

クライアントはNICごとに最大4つの接続を確立し、すべての接続にセッションをバインドします。クライアントは、10G以上の容量の複数のNICで接続を確立できます。

また、次のパラメータを変更することもできます（advanced権限）。

- `-max-connections-per-session`

マルチチャネルセッションごとに許可される最大接続数。デフォルトの接続数は32です。

デフォルトよりも多くの接続を有効にする場合は、クライアント設定を調整する必要があります（デフォルトの接続数は32）。

- `-max-lifs-per-session`

マルチチャネルセッションごとにアドバタイズされるネットワークインターフェイスの最大数。デフォルトは256のネットワークインターフェイスです。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. SMBサーバでSMBマルチチャネルを有効にします。

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

3. ONTAPがSMBマルチチャネルセッションを報告していることを確認します。

```
vserver cifs session show
```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次の例は、すべてのSMBセッションに関する情報を表示します。1つのセッションに対する複数の接続が表示されています。

```

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\
4s                                               Administrator
0

```

次の例は、セッションID 1のSMBセッションに関する詳細情報を表示します。

```

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データボリュームを作成する

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継続的可用性を備えた共有を設定する前に、Storage Virtual Machine (SVM) 上に

NTFS データボリュームを作成する必要があります。ボリューム構成ワークシートを使用して、データボリュームを作成します。

タスクの内容

データボリュームのカスタマイズに使用できるオプションのパラメータが用意されています。ボリュームのカスタマイズの詳細については、を参照して"[論理ストレージ管理](#)"ください。

データボリュームの作成時に、次の項目を含むボリューム内にはジャンクションポイントを作成しないでください。

- ONTAP によってシャドウコピーが生成される Hyper-V ファイル
- SQL Server を使用してバックアップされる SQL Server データベースファイル



mixed セキュリティ形式または UNIX セキュリティ形式を使用するボリュームを誤って作成した場合、そのボリュームを NTFS セキュリティ形式のボリュームに変更して、ノンストップオペレーション用の継続的可用性を備えた共有の作成に直接使用することはできません。Hyper-V over SMBおよびSQL Server over SMBのノンストップオペレーションは、この構成で使用するボリュームをNTFSセキュリティ形式のボリュームとして作成しないと正しく機能しません。ボリュームを削除してNTFSセキュリティ形式でボリュームを再作成するか、Windowsホストでボリュームをマッピングしてボリューム上部にACLを適用し、ボリューム内のすべてのファイルとフォルダにACLを適用します。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する SVM のルートボリュームのセキュリティ形式	入力するコマンド
NTFS	<pre>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</pre>
NTFS ではありません	<pre>volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB]- security-style ntfs -junction-path path</pre>

2. ボリュームの設定が正しいことを確認します。

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

継続的可用性を備えたSMB共有の作成

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

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

2. 継続的可用性を備えたSMB共有を作成します。

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

- 必要に応じて、共有設定にコメントを追加できます。
 - デフォルトでは、オフラインファイル共有プロパティは共有に設定され、に設定されます。 manual
 - ONTAPによって、Windowsのデフォルトの共有権限である/ Full Control`が設定された共有が作成されます `Everyone。
3. 共有設定ワークシートのすべての共有について同じ手順を繰り返します。
 4. コマンドを使用して、設定が正しいことを確認し `vserver cifs share show`ます。
 5. 継続的な可用性が確保された共有に NTFS ファイル権限を設定するには、各共有にドライブをマッピングし、Windows のプロパティ * ウィンドウを使用してファイル権限を設定します。

例

次のコマンドを実行すると、Storage Virtual Machine (SVM、旧 Vserver) vs1 上に「data2」という名前の継続的可用性を備えた共有が作成されます。シンボリックリンクを無効にするには、パラメータをに `""` 設定し `-symlink` ます。

```

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

```

ユーザアカウント（**SMB共有のSQL Server用**）に**SeSecurityPrivilege**権限を追加する

SQL Server のインストールに使用するドメインユーザアカウントには、デフォルトではドメインユーザに割り当てられていない権限を必要とする特定の操作を CIFS サーバで実行するために、「すべてのユーザ」権限を割り当てる必要があります。

必要なもの

SQL Server のインストールに使用するドメインアカウントがすでに存在している必要があります。

タスクの内容

SQL Server インストーラのアカウントに権限を追加するときに、ONTAP がドメインコントローラに照会してアカウントを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. “s eepleed” 権限を追加します。

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

パラメータの値 `user-or-group-name` は、SQL Server のインストールに使用するドメインユーザアカウントの名前です。

2. 権限がアカウントに適用されていることを確認します。

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

例

次のコマンドでは、Storage Virtual Machine (SVM) vs1 の EXAMPLE ドメインにある SQL Server インストールのアカウントに「s eepleed」権限を追加しています。

```
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
```

VSSシャドウコピーのディレクトリ階層の設定 (Hyper-V over SMB共有用)

必要に応じて、シャドウコピーを作成する SMB 共有のディレクトリの最大階層を設定できます。このパラメータは、ONTAP によってシャドウコピーが作成されるサブディレクトリの最大レベルを手動で制御する場合に役立ちます。

必要なもの

VSS シャドウコピー機能を有効にする必要があります。

タスクの内容

デフォルトでは、最大 5 つのサブディレクトリにシャドウコピーが作成されます。値がに設定されている場合 0、ONTAP はすべてのサブディレクトリにシャドウコピーを作成します。



シャドウコピーセットのディレクトリ階層は 6 個以上のサブディレクトリまたはすべてのサブディレクトリを含むことができますが、シャドウコピーセットの作成は 60 秒以内に完了しなければならないという Microsoft の要件があります。この時間内に完了できない場合、シャドウコピーセットの作成は失敗します。作成時間が制限時間を超えないようにシャドウコピーのディレクトリ階層原因を設定しないでください。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. VSS シャドウコピーのディレクトリ階層を目的のレベルに設定します。

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

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

3. admin権限レベルに戻ります。

```
set -privilege admin
```

Hyper-VおよびSQL Server over SMB構成を管理します。

継続的可用性を確保するための既存の共有の設定

既存の共有を変更して、継続的可用性を備えた共有にすることができます。この共有は、Hyper-VおよびSQL ServerアプリケーションサーバがHyper-V仮想マシンおよび構成ファイルおよびSQL Serverデータベースファイルに無停止でアクセスするために使用します。

タスクの内容

既存の共有に次の特徴がある場合、SMBを介したアプリケーションサーバでノンストップオペレーションを実現する継続的可用性を備えた共有として使用することはできません。

- その共有に共有プロパティが設定されている場合 `homedirectory`
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルートの下にジャンクションされたボリュームが含まれている場合

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files``パラメータは（デフォルト）または ``none``に設定されます ``manual``。
- シンボリックリンクを無効にする必要があります。

次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。現在の共有プロパティのリストに含まれている場合は、継続的可用性を備えた共有から削除する必要があります。

- `attributecache`
- `branchcache`

手順

1. 現在の共有パラメータの設定と、設定済みの共有プロパティの現在のリストを表示します。

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

2. 必要に応じて、コマンドを使用して共有パラメータを変更し、シンボリックリンクを無効にし、オフラインファイルをmanualに設定し vserver cifs share modify ます。
 - シンボリックリンクを無効にするには、パラメータの値をに `""` 設定し `-symlink` ます。
 - を指定すると、パラメータを正しい設定に manual` 設定できます ` -offline-files。
3. 共有プロパティを追加し、必要に応じて共有プロパティを追加し continuously-available oplocks ます。

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

共有プロパティがまだ設定されていない場合は oplocks、共有プロパティと一緒に追加する必要があります continuously-available。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

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

共有プロパティをカンマで区切って指定すると、1つ以上の共有プロパティを削除できます。

5. パラメータと ` -offline-files `パラメータが正しく設定されていることを確認し ` -symlink ` ます。

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

6. 設定済みの共有プロパティのリストが正しいことを確認します。

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

例

次の例は、Storage Virtual Machine (SVM) 「vs1」に「share1」という名前の既存の共有をSMBを介したアプリケーションサーバでのNDO用に設定する方法を示しています。

- パラメータをに設定すると、共有でシンボリックリンクが無効になります `-symlink ""`。

- ``-offline-file`` パラメータが変更され、に設定され ``manual`` ます。
- ``continuously-available`` 共有プロパティが共有に追加されます。
- ``oplocks`` 共有プロパティはすでに共有プロパティのリストに含まれているため、追加する必要はありません。
- ``attributecache`` 共有プロパティが共有から削除されます。
- ``browsable`` 共有プロパティは、SMBを介したアプリケーションサーバでのNDOに使用される継続的可用性を備えた共有では省略可能で、共有プロパティの1つとして保持されます。

```
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
```

Hyper-V over SMBバックアップ用のVSSシャドウコピーの有効化と無効化

VSS 対応バックアップアプリケーションを使用して、SMB 共有に格納された Hyper-V 仮想マシンファイルをバックアップする場合は、VSS シャドウコピーを有効にする必要があります。VSS 対応バックアップアプリケーションを使用しない場合は、VSS シャドウコピーを無効にできます。デフォルトでは、VSS シャドウコピーは有効になっています。

タスクの内容

VSS シャドウコピーはいつでも有効または無効にできます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

VSS シャドウコピーの設定	入力するコマンド
有効	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</pre>
無効にする	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</pre>

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドを実行すると、SVM vs1 で VSS シャドウコピーが有効になります。

```
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
```

統計を使用してHyper-VおよびSQL Server over SMBのアクティビティを監視する

使用可能な統計オブジェクトとカウンタの確認

CIFS、SMB、監査、およびBranchCacheハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	<code>statistics catalog object show</code>
使用可能な特定のオブジェクト	<code>statistics catalog object show object <i>object_name</i></code>
使用可能なカウンタ	<code>statistics catalog counter show object <i>object_name</i></code>

使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した統計オブジェクトの説明が表示されます。

```
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
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が表示され`cifs`ます。



この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありません。出力は省略されています。

```
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

```
[...]
```

ONTAPのSMB統計を表示します。

パフォーマンスを監視して問題を診断するために、さまざまなSMB統計を表示すること

ができます。

手順

1. コマンドとオプションの `statistics stop` コマンドを使用して、`statistics start` データサンプルを収集します。
2. 次のいずれかを実行します。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.xおよびSMB 3.0	<code>statistics show -object smb2</code>
ノードのSMBサブシステム	<code>statistics show -object nblade_cifs</code>

リンクの詳細については、コマンドリファレンスを参照してください。<https://docs.netapp.com/us-en/ONTAP-CLI/statistics-show.html>、リンク：<https://docs.netapp.com/us-en/ONTAP-CLI/statistics-start.html>[`statistics start`、およびリンク：<https://docs.netapp.com/us-en/ONTAP-CLI/statistics-stop.html>[`statistics stop`^]コマンドの詳細[`statistics show`]については、『ONTAPコマンドリファレンス』を参照してください。

構成がノンストップオペレーションに対応していることを確認する

ヘルス監視を使用してノンストップオペレーションのステータスが正常かどうかを確認する

ヘルスマニタを使用すると、クラスタ全体のシステムヘルスステータスに関する情報が得られます。ヘルスマニタは Hyper-V over SMB および SQL Server over SMB 構成を監視して、アプリケーションサーバの Nondisruptive Operation (NDO ; ノンストップオペレーション) を実現します。ステータスがデグレードの場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を確認できます。

ヘルスマニタはいくつかあります。ONTAP では、システム全体の健全性と個々のヘルスマニタの健全性の両方が監視されます。ノード接続ヘルスマニタには、CIFS-NDO サブシステムが含まれています。モニタには一連のヘルスポリシーがあり、特定の物理的な条件によってシステムが停止する可能性がある場合にアラートをトリガーするポリシーと、システム停止が発生している場合にアラートが生成し、対処方法に関する情報を提供するポリシーがあります。SMB を介した NDO 構成では、アラートは次の 2 つの状態で生成されます。

アラートID	重大度	条件
HaNotReadyCifsNdo_Alert	メジャー	ノード上のアグリゲート内のボリュームでホストされている1つ以上のファイルが、継続的可用性を備えたSMB共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずですが、パートナーとのHA関係が設定されていないか正常ではありません。
NoStandbyLifCifsNdo_Alert	マイナー	Storage Virtual Machine (SVM) はノードから SMB を介してアクティブにデータを提供しており、SMB ファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードが SVM のアクティブなデータ LIF を公開していない。

システムヘルスの監視を使用してノンストップオペレーションのステータスを表示します。

コマンドを使用すると、クラスタのシステムヘルス全体およびCIFS-NDOサブシステムのヘルスに関する情報の表示、アラートへの応答、以降のアラートの設定、ヘルスマニタの設定に関する情報の表示を行うことができます `system health`。

手順

1. 適切な操作を実行して、ヘルスステータスを監視します。

表示する項目	入力するコマンド
個々のヘルスマニタのステータス全体が反映された、システムのヘルスステータス	system health status show
CIFS-NDO サブシステムのヘルスステータスに関する情報	system health subsystem show -subsystem CIFS-NDO -instance

2. 適切な操作を実行して、CIFS-NDO アラートの監視がどのように設定されているかに関する情報を表示します。

表示する情報	入力するコマンド
監視対象のノード、初期化状態、ステータスなど、CIFS-NDO サブシステムのヘルスマニタの設定とステータス	system health config show -subsystem CIFS-NDO

表示する情報	入力するコマンド
ヘルスマニタで生成される可能性がある CIFS-NDO アラート	system health alert definition show -subsystem CIFS-NDO
アラートが発行されるタイミングを決定する、CIFS-NDO ヘルスマニタのポリシー	system health policy definition show -monitor node-connect



詳細な情報を表示するには、パラメータを使用し `-instance` ます。

例

次の出力は、クラスタおよび CIFS-NDO サブシステムのヘルスステータス全体に関する情報を示しています。

```
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
```

次の出力は、CIFS-NDO サブシステムのヘルスマニタの設定とステータスに関する詳細な情報を示しています。

```

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

```

継続的可用性を備えたSMB共有の設定の確認

ノンストップオペレーションをサポートするには、Hyper-V および SQL Server の SMB 共有が継続的可用性を備えた共有として設定されている必要があります。また、それ以外にも、いくつかの共有設定について確認が必要になります。計画的または計画外の停止が発生する状況でアプリケーションサーバのノンストップオペレーションをシームレスに実行できるように、共有が適切に設定されていることを確認してください。

タスクの内容

次の2つの共有パラメータが正しく設定されていることを確認する必要があります。

- `-offline-files` パラメータは（デフォルト）または ``none`` に設定されます ``manual``。
- シンボリックリンクを無効にする必要があります。

ノンストップオペレーションが適切に実行されるようにするには、次の共有プロパティを設定する必要があります。

- `continuously-available`
- `oplocks`

次の共有プロパティは設定しないでください。

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

手順

1. オフラインファイルがまたは ``disabled`` に設定されていること、およびシンボリックリンクが無効になっていることを確認し ``manual`` ます。

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

2. SMB 共有が継続的可用性を確保するように設定されていることを確認します。

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

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上の「share1」という名前の共有の共有設定を表示します。オフラインファイルはに設定され、シンボリックリンクは無効になってい ``manual`` ます（出力フィールドにハイフンが表示され ``Symlink Properties`` ます）。

```

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

```

次の例は、SVM vs1 上の「share1」という名前の共有の共有プロパティを表示します。

```

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

```

LIFステータスの確認

Hyper-VおよびSQL Server over SMB構成のStorage Virtual Machine (SVM) をクラスタ内の各ノードにLIFを配置するように設定した場合でも、日常業務中に一部のLIFが別のノードのポートに移動することがあります。LIF のステータスを確認して、必要な措置を講じる必要があります。

タスクの内容

シームレスなノンストップオペレーションの運用支援を提供するには、クラスタ内の各ノードの SVM に少なくとも 1 つの LIF を配置し、すべての LIF をホームポートに関連付ける必要があります。設定されている LIF の中に現在ホームポートに関連付けられていないものがある場合は、ポートの問題を修正してから、対応するホームポートに LIF をリバートする必要があります。

手順

1. 設定されている SVM の LIF に関する情報を表示します。

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

この例では、「lif1」はホームポートに配置されていません。

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is 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					

2. 対応するホームポートに関連付けられていない LIF がある場合は、次の手順を実行します。

a. それぞれの LIF について、LIF のホームポートを確認します。

```
network interface show -vserver vs1 -lif lif1 -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. それぞれの LIF について、LIF のホームポートが up 状態になっているかどうかを確認します。

```
network port show -node node1 -port e0d -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

node	port	link
node1	e0d	up

+ この例では、「lif1」をホームポートに戻す必要があります node1:e0d。

3. LIFを関連付けるホームポートのネットワークインターフェイスが状態になっていない場合は up、問題を解決してup状態にします。

4. 必要に応じて、ホームポートに LIF をリバートします。

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

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

5. クラスタ内の各ノードにアクティブな SVM の LIF があることを確認します。

```
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						
true	lif1	up/up	10.0.0.128/24	node1	e0d	
true	lif2	up/up	10.0.0.129/24	node2	e0d	

SMBセッションの継続的可用性の確認

SMBセッション情報を表示する

SMB接続、SMB Session ID、セッションを使用しているワークステーションのIPアドレスなど、確立されているSMBセッションに関する情報を表示できます。セッションのSMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

タスクの内容

SVM上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。
と入力して、使用できるフィールドを指定できます `-fields ?`。
- パラメータを使用すると、確立されたSMBセッションに関する詳細情報を表示できます `-instance`。
- パラメータまたは `-instance``パラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます ``-fields`。

手順

1. 次のいずれかを実行します。

表示する SMB セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	vserver cifs session show -vserver vserver_name
指定した接続IDのファイル	vserver cifs session show -vserver vserver_name -connection-id integer
指定したワークステーションのIPアドレスから	vserver cifs session show -vserver vserver_name -address workstation_IP_address
指定したLIF IPアドレスのファイル	vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address
指定したノードのオブジェクト	<code>*vserver cifs session show -vserver vserver_name -node {node_name</code>
local}*`	指定したWindowsユーザからのセッション
vserver cifs session show -vserver vserver_name -windows-user user_name の形式 user_name`は です `[domain]\user。	指定した認証メカニズムを使用している場合
vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism には、次のいずれかの値 を `auth-mechanism` 指 定できます。 • NTLMv1 • NTLMv2 • Kerberos • Anonymous	指定したプロトコルバージョンを使用している場合

表示する SMB セッション情報	入力するコマンド
<pre> vserver cifs session show -vserver vserver_name -protocol-version protocol_version </pre> <p>には、次のいずれかの値を `protocol-version` 指定できます。</p> <ul style="list-style-type: none"> • SMB1 • SMB2 • SMB2_1 • SMB3 • SMB3_1 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。SMB3</p> </div>	<p>指定したレベルの継続的可用性を備えた保護を使用しているセッション</p>



表示する SMB セッション情報	入力するコマンド
<pre> vserver cifs session show -vserver vserver_name -continuously -available continuously_avail able_protection_le vel </pre> <p>には、次のいずれかの値を`-continuously-available`指定できません。</p> <ul style="list-style-type: none"> • No • Yes • Partial 	<p>指定したSMB署名セッションステータスのセッション</p>

例

次のコマンドを実行すると、IPアドレスが10.1.1.1のワークステーションから確立されたSVM vs1上のセッションに関するセッション情報が表示されます。

```
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
```

次のコマンドを実行すると、SVM vs1上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。接続はドメインアカウントを使用して行われました。

```
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
```

cifs

次のコマンドを実行すると、SVM vs1上のSMB 3.0とSMBマルチチャネルを使用しているセッションに関するセッション情報が表示されます。この例では、ユーザはLIF IPアドレスを使用してSMB 3.0対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトのNTLMv2になっています。継続的可用性を備えた保護を使用して接続するには、Kerberos認証を使用して接続を確立する必要があります。

```

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

```

開いている**SMB**ファイルに関する情報を表示する

SMB接続とSession ID、ホスティングボリューム、共有名、共有パスなど、開いているSMBファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

タスクの内容

確立されたSMBセッションで開いているファイルに関する情報を表示できます。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値`-continuously-available`は`Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。`

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine (SVM) 上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。


- パラメータを使用すると、開いているSMBファイルに関する詳細情報を表示できます `-instance`。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

手順

1. 次のいずれかを実行します。

表示する開いている SMB ファイル	入力するコマンド
SVM上のファイル (要約形式)	<code>vserver cifs session file show -vserver vserver_name</code>
指定したノードのオブジェクト	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*`</code>	指定したファイルIDのファイル
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	指定したSMB接続IDのファイル
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	指定したSMB Session IDのファイル
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	指定したホストアグリゲートのファイル
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	指定したボリュームのファイル
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	指定したSMB共有のファイル
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	指定したSMBパスのファイル

表示する開いている SMB ファイル	入力するコマンド
vserver cifs session file show -vserver vserver_name -path path	指定したレベルの継続的可用性を備えた保護を使用している
vserver cifs session file show -vserver vserver_name -continuously -available continuously_available_status	指定した再接続状態のファイル
<p>には、次のいずれかの値を ` -continuously-available ` 指定できます。</p> <ul style="list-style-type: none"> • No • Yes 	
 <p>継続的可用性のステータスがの場合には No、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。</p>	

出力結果の絞り込みに使用できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例では、SVM vs1の開いているファイルに関する情報を表示します。

```
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
```

次の例では、SVM vs1のファイルID 82の開いているSMBファイルに関する詳細情報を表示します。

```
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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。