SANの概念

ONTAP 9

NetApp
April 24, 2024

目次

SANの概念

iSCSI を使用した SAN プロビジョニング

SAN 環境において、ストレージシステムはストレージターゲットデバイスを含むターゲットです。iSCSI および FC では、ストレージターゲットデバイスを LUN （論理ユニット）と呼びます。Non-Volatile Memory Express （ NVMe ） over Fibre Channel では、ストレージターゲットデバイスをネームスペースと呼びます。

iSCSI および FC の場合は LUN 、 NVMe の場合はネームスペースを作成することでストレージを構成します。これらの LUN またはネームスペースに、ホストから Internet Small Computer System Interface （ iSCSI ）または Fibre Channel （ FC ；ファイバチャネル）プロトコルネットワーク経由でアクセスします。

iSCSI ネットワークに接続するために、ホストでは標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の iSCSI Host Bus Adapter （ HBA ；ホストバスアダプタ）を使用します。

FC ネットワークに接続する場合、ホストでは FC HBA または CNA が必要です。

サポートされる FC プロトコルは次のとおりです。

- FC
- FCoE
- NVMe

iSCSI ターゲットノードのネットワーク接続と名前

iSCSI ターゲットノードは、いくつかの方法でネットワークに接続できます。

- ONTAP に統合されているソフトウェアを使用して、イーサネットインターフェイスを介して接続する。
- 複数のシステムインターフェイス上。iSCSIに使用されるインターフェイスで、SMBやNFSなどの他のプロトコルのトラフィックも転送できます。
- ユニファイドターゲットアダプタ（ UTA ）または Converged Network Adapter （ CNA ；統合ネットワークアダプタ）を使用する。

すべての iSCSI ノードには、ノード名が必要です。

iSCSI ノード名の 2 つの形式、つまり、タイプ指定子は、 _iqn と _eui _ です。SVM iSCSI ターゲットでは、常に iqn タイプの指定子が使用されます。イニシエータでは、 iqn タイプ指定子と eui タイプ指定子のどちらも使用できます。

ストレージシステムのノード名

iSCSI を実行している各 SVM には、逆ドメイン名と一意のエンコード番号から成るデフォルトのノード名が付いています。

ノード名は次の形式で表示されます。

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

次の例は、一意のエンコード番号を持つストレージシステムのデフォルトのノード名です。

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

iSCSI の TCP ポート

iSCSI プロトコルは、 TCP ポート番号 3260 を使用するように、 ONTAP で設定されています。

ONTAP では、 iSCSI のポート番号の変更がサポートされていません。ポート番号 3260 は iSCSI 仕様の一部として登録されており、他のアプリケーションやサービスでは使用できません。

関連情報

"ネットアップのマニュアル： ONTAP SAN ホスト構成"

iSCSI サービスの管理

iSCSI サービスの管理

Storage Virtual Machine（SVM）のiSCSI論理インターフェイスでiSCSIサービスの可用性を管理するには、を使用します `vserver iscsi interface enable` または `vserver iscsi interface disable` コマンド

デフォルトでは、すべての iSCSI 論理インターフェイスで iSCSI サービスが有効になっています。

ホストに **iSCSI** を実装する方法

iSCSI は、ハードウェアまたはソフトウェアを使用してホストに実装できます。

iSCSI は、次のいずれかの方法で実装できます。

- ホストの標準イーサネットインターフェイスを使用するイニシエータソフトウェアを使用する。
- iSCSI Host Bus Adapter （ HBA ；ホストバスアダプタ）を使用する。ホストオペレーティングシステムでは、 iSCSI HBA をローカルディスクを搭載した SCSI ディスクアダプタとみなします。
- TCP / IP 処理をオフロードする TCP Offload Engine （ TOE ； TCP オフロードエンジン）アダプタを使用する。

  iSCSI プロトコルの処理は、引き続きホストソフトウェアによって実行されます。

iSCSI 認証の仕組み

iSCSI セッションの第 1 段階では、イニシエータがストレージシステムにログイン要求を送信して、 iSCSI セッションを開始します。ストレージシステムは、このログイン要求を許可または拒否するか、またはログインが不要であると判断します。

iSCSI 認証方法は次のとおりです。

- Challenge Handshake Authentication Protocol （ CHAP ） - イニシエータは CHAP ユーザ名およびパスワードを使用してログインします。

  CHAP パスワードを指定するか、 16 進数のシークレットパスワードを生成できます。CHAP ユーザ名およびパスワードには、次の 2 種類があります。

  - インバウンド - ストレージシステムがイニシエータを認証します。

    CHAP 認証を使用する場合は、インバウンド設定が必要です。

  - アウトバウンド - イニシエータがストレージシステムを認証できるようにするオプションの設定です。

    インバウンドユーザ名およびパスワードをストレージシステムで定義した場合にのみ、アウトバウンド設定を使用できます。

- deny — イニシエータはストレージシステムへのアクセスを拒否されます。
- none — イニシエータの認証は必要ありません

イニシエータとその認証方法の一覧を定義できます。このリストにない環境イニシエータに対して、デフォルトの認証方法を定義することもできます。

関連情報

"Data ONTAP での Windows マルチパス・オプション：ファイバ・チャネルおよび iSCSI"

iSCSI イニシエータのセキュリティ管理

ONTAP は、 iSCSI イニシエータのセキュリティを管理するためのさまざまな機能を備えています。iSCSI イニシエータのリストと各イニシエータに対する認証方法の定義、認証リスト内のイニシエータと関連する認証方法の表示、認証リストに対するイニシエータの追加と削除、リストにないイニシエータに対するデフォルトの iSCSI イニシエータ認証方法の定義を行うことができます。

iSCSI エンドポイントの分離

ONTAP 9.1 以降では、既存の iSCSI セキュリティコマンドが拡張され、 IP アドレスの範囲や複数の IP アドレスを受け入れることができるようになりました。

すべての iSCSI イニシエータは、ターゲットとのセッションまたは接続を確立するときに、発信元 IP アドレスを提供する必要があります。元の IP アドレスがサポート対象外または不明な場合にイニシエータがクラスタにログインできないようにすることで、独自の識別を実現します。サポート対象外または不明な IP アドレスを発信したイニシエータは、 iSCSI セッションレイヤでログインが拒否されるため、クラスタ内の LUN やボリュームにアクセスできません。

この新しい機能を 2 つの新しいコマンドで実装して、既存のエントリを管理します。

イニシエータのアドレス範囲を追加する

でIPアドレス範囲を追加するか、複数のIPアドレスを追加して、iSCSIイニシエータのセキュリティ管理を改善します `vserver iscsi security add-initiator-address-range` コマンドを実行します

```
cluster1::> vserver iscsi security add-initiator-address-range
```

イニシエータのアドレス範囲を削除する

を使用して、IPアドレス範囲または複数のIPアドレスを削除します `vserver iscsi security remove-initiator-address-range` コマンドを実行します

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

CHAP 認証とは

Challenge Handshake Authentication Protocol （ CHAP ）により、 iSCSI イニシエータとターゲットの間で認証に基づいたやり取りが可能になります。CHAP 認証を使用する場合は、イニシエータとストレージシステムの両方で、 CHAP ユーザ名およびパスワードを定義します。

iSCSI セッションの第 1 段階では、イニシエータがストレージシステムにログイン要求を送信して、セッションを開始します。ログイン要求には、イニシエータの CHAP ユーザ名および CHAP アルゴリズムが含まれています。ストレージシステムは CHAP チャレンジで応答します。イニシエータは CHAP 応答を返します。ストレージシステムは応答を検証し、イニシエータを認証します。CHAP パスワードは、応答の計算に使用されます。

CHAP 認証を使用する場合のガイドライン

CHAP 認証を使用する場合は、一定のガイドラインに従う必要があります。

- インバウンドユーザ名およびパスワードをストレージシステムで定義している場合は、イニシエータのアウトバウンド CHAP 設定にも同じユーザ名およびパスワードを使用する必要があります。ストレージシステムでアウトバウンドユーザ名およびパスワードも定義して、双方向認証を可能にしている場合は、イニシエータのインバウンド CHAP 設定にも同じユーザ名およびパスワードを使用する必要があります。
- ストレージシステムのインバウンド設定とアウトバウンド設定には、同じユーザ名およびパスワードを使用できません。
- CHAP ユーザ名には 1~128 バイトを使用できます。

  ユーザ名を null にすることはできません。

- CHAP パスワード（ secrets ）には 1~512 バイトを使用できます。

  パスワードには、 16 進数値または文字列を使用できます。16 進数値を使用する場合は、プレフィックス「 0x 」または「 0X 」を付けた値を入力する必要があります。パスワードを null にすることはできません。

ONTAP では、CHAPパスワード（シークレット）に特殊文字、英語以外の文字、数字、およびスペースを使用できます。 ただし、これにはホストの制限があります。 これらのいずれかが特定のホストで許可されていない場合は、使用できません。

たとえば、 Microsoft iSCSI ソフトウェアイニシエータでは、 IPSec 暗号化を使用しない場合、イニシエータとターゲットの両方の CHAP パスワードを 12 バイト以上に設定する必要があります。パスワードの最大長は、 IPSec を使用するかどうかに関係なく 16 バイトです。

その他の制限事項については、イニシエータのマニュアルを参照してください。

イニシエータのインターフェイスを制限する **iSCSI** インターフェイスアクセスリストの使用方法によって、パフォーマンスとセキュリティが向上する可能性があります

iSCSI インターフェイスアクセスリストを使用して、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。これにより、パフォーマンスとセキュリティが向上します。

イニシエータがiSCSIを使用して検出セッションを開始したとき `SendTargets` コマンドを実行すると、アクセスリストにあるLIF（ネットワークインターフェイス）に関連付けられているIPアドレスが受信されます。デフォルトでは、すべてのイニシエータが SVM 内のすべての iSCSI LIF にアクセスできます。アクセスリストを使用すると、イニシエータがアクセスできる SVM 内の LIF の数を制限できます。

Internet Storage Name Service（iSNS）

Internet Storage Name Service （ iSNS ）は、 TCP / IP ストレージネットワークで iSCSI デバイスを自動的に検出して管理できるプロトコルです。iSNS サーバは、 IP アドレス、 iSCSI ノード名 IQN 、ポータルグループなど、ネットワーク上のアクティブな iSCSI デバイスに関する情報を維持します。

iSNS サーバは、サードパーティベンダーから入手できます。ネットワーク内に iSNS サーバがあり、イニシエータとターゲットで使用するように設定および有効化されている場合、 Storage Virtual Machine （ SVM ）の管理 LIF を使用して、その SVM のすべての iSCSI LIF を iSNS サーバに登録できます。登録が完了すると、 iSCSI イニシエータは iSNS サーバを照会して、その SVM のすべての LIF を検出できるようになります。

iSNS サービスを使用する場合は、 Storage Virtual Machine （ SVM ）を Internet Storage Name Service （ iSNS ）サーバに適切に登録する必要があります。

iSNS サーバがネットワークにない場合は、各ターゲットがホストで認識できるように、ターゲットを手動で設定する必要があります。

iSNS サーバの機能

iSNS サーバは、 Internet Storage Name Service （ iSNS ）プロトコルを使用して、 IP アドレス、 iSCSI ノード名（ IQN ）、ポータルグループなど、ネットワーク上のアクティブな iSCSI デバイスに関する情報を維持します。

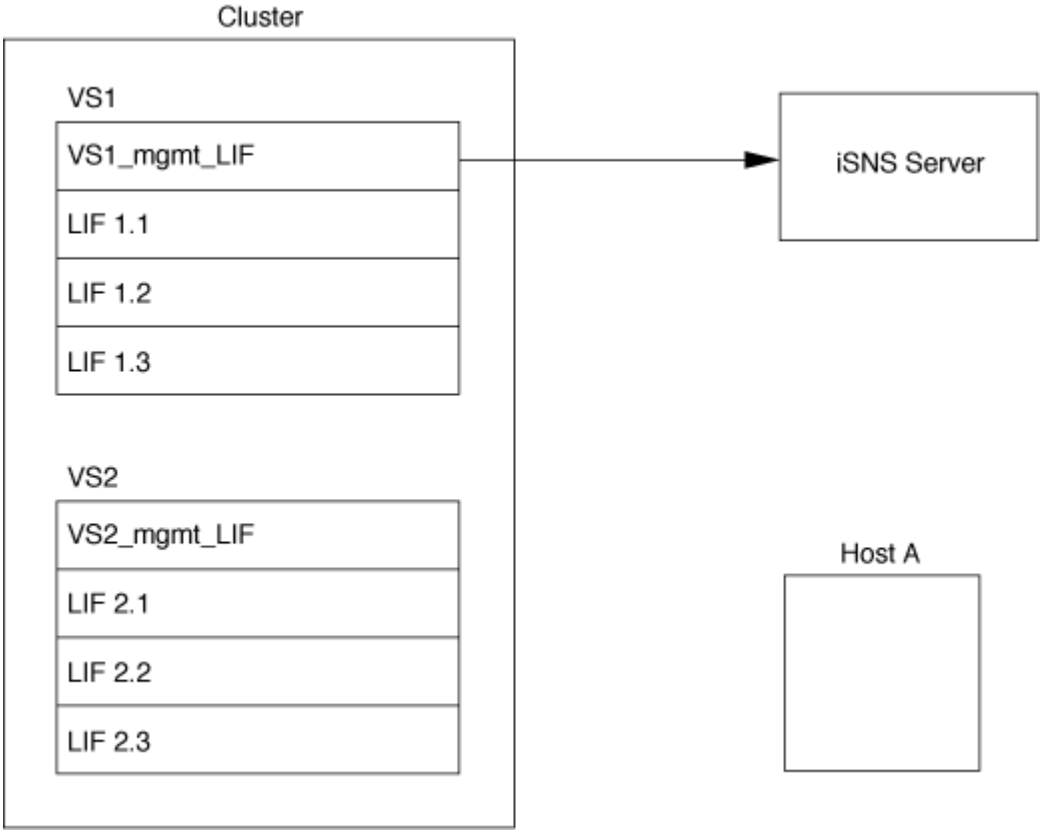
iSNS プロトコルを使用すると、 IP ストレージネットワークで iSCSI デバイスを自動的に検出して管理できます。iSCSI イニシエータは、 iSNS サーバに照会して iSCSI ターゲットデバイスを検出します。

ネットアップでは、 iSNS サーバの提供や再販は行っていません。これらのサーバは、ネットアップがサポートするベンダーから入手できます。

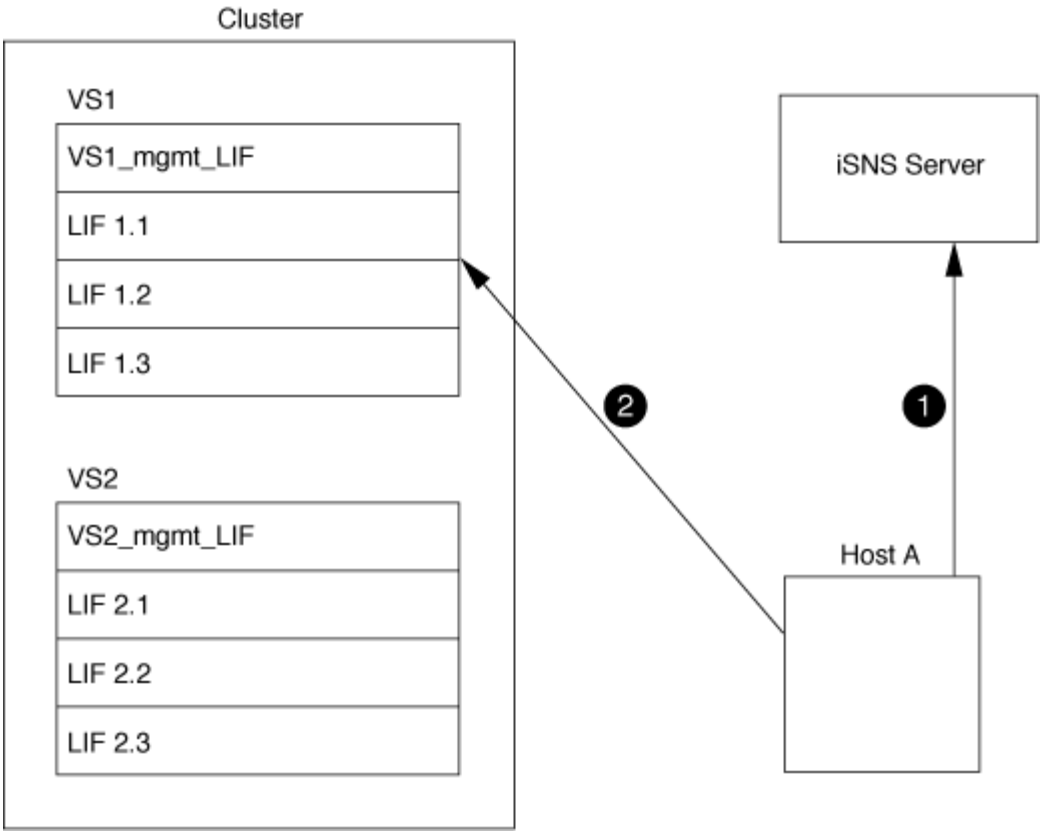
SVMs と **iSNS** サーバの連動

iSNS サーバは、 Storage Virtual Machine （ SVM ）の管理 LIF を介して各 SVM と通信します。管理 LIF は、特定の SVM のすべての iSCSI ターゲットのノード名、エイリアス、およびポータル情報を iSNS サーバに登録します。

次の例では、SVM「VS1」はSVM管理LIF「VS1_mgmt_LIF'」を使用してiSNSサーバに登録しています。iSNS に登録中、 SVM はすべての iSCSI LIF を SVM 管理 LIF を介して iSNS サーバに送信します。iSNS の登録が完了すると、iSNSサーバには「VS1」でiSCSIを提供するすべてのLIFのリストが格納されます。複数の SVMs があるクラスタでは、 iSNS サービスを使用する個々の SVM が iSNS サーバに登録する必要があります。



次の例では、iSNSサーバによるターゲットへの登録が完了すると、ホストAがiSNSサーバを介して「VS1」のすべてのLIFを検出できるようになります（手順1を参照）。ホストAが「VS1」のLIFの検出を完了すると、ホストAは「VS1」の任意のLIFとの接続を確立できます（手順2を参照）。「VS2」の管理LIF「VS2_mgmt_LIF」がiSNSサーバに登録されるまで、ホストAは「VS2」内のLIFを認識しません。



ただし、インターフェイスアクセスリストを定義すると、ホストがターゲットへのアクセスに使用できるのはインターフェイスアクセスリストに定義された LIF のみになります。

一度 iSNS が設定されると、 SVM の設定を変更するたびに ONTAP によって iSNS サーバが自動的に更新されます。

設定を変更してからONTAPからiSNSサーバに更新情報が送信されるまでには、数分程度の遅れが生じる可能性があります。iSNSサーバのiSNS情報を強制的に更新します。 `vserver iscsi isns update`

iSNS を管理するためのコマンド

ONTAP には、 iSNS サービスを管理するコマンドが用意されています。

状況	使用するコマンド
iSNS サービスを設定する	`vserver iscsi isns create`
iSNS サービスを開始する	`vserver iscsi isns start`
iSNS サービスを変更する	`vserver iscsi isns modify`
iSNS サービス設定を表示します	`vserver iscsi isns show`
登録済みの iSNS 情報を強制的に更新します	`vserver iscsi isns update`

iSNS サービスを停止します	`vserver iscsi isns stop`
iSNS サービスを削除します	`vserver iscsi isns delete`
コマンドのマニュアルページを表示します	`man` *`command name`*

詳細については、各コマンドのマニュアルページを参照してください。

FC を使用した SAN プロビジョニング

ONTAP で FC SAN を実装する方法について理解する際に必要となる重要な概念について説明します。

FC ターゲットノードをネットワークに接続する方法

ストレージシステムとホストはいずれもアダプタを備えており、ケーブルを使用して FC スイッチに接続できます。

ノードを FC SAN に接続すると、各 SVM の LIF の World Wide Port Name （ WWPN ；ワールドワイドポート名）がスイッチのファブリックネームサービスに登録されます。SVM の WWNN と各 LIF の WWPN は、ONTAP によって自動的に割り当てられます。

> FC を使用してホストから直接ノードに接続することはできません。 NPIV が必要なため、スイッチを使用する必要があります。 iSCSI セッションでは、ネットワークルーティングされた接続または直接接続された接続で通信が可能です。ただし、どちらの方法も ONTAP でサポートされています。

FC ノードの識別方法

FC を使用して設定された各 SVM は、 World Wide Node Name （ WWNN ）で識別されます。

WWPN の使用方法

WWPN により、 FC をサポートするように設定されている SVM 内の各 LIF が識別されます。これらの LIF はクラスタ内の各ノードの物理 FC ポートを利用します。これらのポートには、 FC ターゲットカード、 UTA 、または UTA2 としてノードの FC または FCoE として設定することができます。

- igroup を作成します

  ホストの HBA の WWPN は、 igroup の作成に使用します。igroup は、特定 LUN へのホストアクセスの制御に使用します。igroup を作成するには、 FC ネットワーク内の一連のイニシエータの WWPN を指定します。ストレージシステム上の LUN を igroup にマッピングすると、グループ内のすべてのイニシエータに対し、その LUN へのアクセスを許可することができます。LUN にマッピングされている igroup に WWPN が含まれていないホストは、その LUN にアクセスできません。つまり、そのホストでは、 LUN がディスクとして表示されません。

  ポートセットを作成して、特定のターゲットポートでのみ LUN を表示することもできます。ポートセットは、 FC ターゲットポートをグループ化したものです。ポートセットには igroup をバインドできます。

この igroup 内のすべてのホストは、ポートセット内のターゲットポートからのみ各 LUN にアクセスできます。

- FC LIF を一意に識別します

  WWPN は、 FC 論理インターフェイスを一意に識別します。ホストの OS は、 WWNN と WWPN を組み合わせて使用して、 SVM および FC LIF を識別します。一部のオペレーティングシステムでは、パーシスタントバインディングがないと、ホスト上の同じターゲット ID に LUN が表示されません。

WWN の割り当ての仕組み

WWN は、 ONTAP でシーケンシャルに作成されます。ただし、 ONTAP による割り当て方法が原因で、 WWN がシーケンシャルに割り当てられていないように見える場合があります。

各アダプタには WWPN および WWNN があらかじめ設定されていますが、 ONTAP ではあらかじめ設定された値が使用されません。その代わりに、 ONTAP はオンボードイーサネットポートの MAC アドレスに基づいて、固有の WWPN または WWNN を割り当てます。

WWN が割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- WWN は、クラスタ内のすべてのノードと Storage Virtual Machine （ SVM ）で一意に割り当てられます。
- 解放された WWN はリサイクルされ、利用可能な名前のプールに再び追加されます。

FC スイッチの識別方法

ファイバチャネルスイッチでは、デバイス自体に 1 つの Worldwide Node Name （ WWNN ；ワールドワイドノード名）があり、デバイスの各ポートに 1 つの Worldwide Port Name （ WWPN ；ワールドワイドポート名）があります。

たとえば、次の図は、 16 ポート Brocade スイッチの各ポートに WWPN がどのように割り当てられているかを示しています。特定のスイッチのポートの番号付けについては、そのスイッチ用にベンダーが提供するマニュアルを参照してください。

ポート* 0 *、WWPN 20： **00** ：00：60：69：51：06：b4

ポート* 1 *、WWPN 20： **01** ：00：60：69：51：06：b4

ポート * 14 * 、 WWPN 20 ： **0e** 00 ： 60 ： 69 ： 51 ： 06 ： b4

ポート * 15 * 、 WWPN 20 ： **0f** ： 00 ： 60 ： 69 ： 51 ： 06 ： B4

NVMe を使用した SAN プロビジョニング

ONTAP 9.4 以降では、 SAN 環境で NVMe/FC がサポートされます。NVMe/FC では、FC および iSCSI で LUN をプロビジョニングして igroup にマッピングするのと同様に、ネームスペースとサブシステムをプロビジョニングし、ネームスペースをサブシステムにマッピングすることができます。

NVMe ネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリの容量です。ネームスペースは FC および iSCSI プロトコルの LUN に相当し、 NVMe サブシステムは igroup に相当します。NVMe サブシステムはイニシエータに関連付けることができ、これにより関連付けられたイニシエータからサブシステム内のネームスペースにアクセスできるようになります。

> NVMe ネームスペースは、機能的には LUN に似ていますが、 LUN でサポートされるすべての機能がサポートされるわけではあり

ONTAP 9.5 以降では、 NVMe を使用したホスト側のデータアクセスをサポートするにはライセンスが必要です。ONTAP 9.4 で NVMe が有効になっている場合、 ONTAP 9.5 へのアップグレード後に 90 日間の猶予期間中にライセンスを取得する必要があります。ある場合 "ONTAP One"にはNVMeライセンスが含まれています。ライセンスを有効にするには、次のコマンドを使用します。

```
system license add -license-code NVMe_license_key
```

関連情報

"ネットアップテクニカルレポート 4684 ：『 Implementing and Configuring Modern SANs with NVMe/FC 』"

SANボリユウム

SAN ボリュームについての概要

ONTAP には、基本的なボリュームプロビジョニングオプションとして、シックプロビジョニング、シンプロビジョニング、セミシックプロビジョニングの 3 つが用意されています。各オプションでは、ボリュームスペースおよび ONTAP ブロック共有テクノロジでのスペース要件がさまざまな方法で管理されます。これらのオプションの仕組みを理解することで、環境に最も適したオプションを選択できるようになります。

> SAN LUN と NAS 共有を同じ FlexVol に配置することは推奨されません。SAN LUN と FlexVol NAS 共有それぞれに専用の FlexVol ボリュームをプロビジョニングしてください。これにより、管理とレプリケーションの導入が簡易化され、 Active IQ Unified Manager （旧 OnCommand Unified Manager ）での FlexVol ボリュームのサポート方法が統一されます。

ボリュームのシンプロビジョニング

シンプロビジョニングボリュームは、作成時に ONTAP によって追加のスペースが確保されることはありません。ボリュームにデータが書き込まれるときに、書き込み処理に対応するために必要なアグリゲート内のストレージをボリュームが要求します。シンプロビジョニングボリュームを使用する場合はアグリゲートをオーバーコミットできますが、アグリゲートの空きスペースが不足すると、必要なスペースをボリュームが確保できなくなる可能性があります。

シンプロビジョニングFlexVol を作成するには、そのボリュームを設定します `-space-guarantee` オプションをに設定します `none`。

ボリュームのシックプロビジョニング

シックプロビジョニングボリュームを作成すると、ボリューム内のブロックにいつでも書き込むことができるように、 ONTAP はアグリゲートから十分なストレージを確保します。シックプロビジョニングを使用するようにボリュームを構成する場合は、圧縮や重複排除などの ONTAP の Storage Efficiency 機能を使用して、事前に必要となる大容量のストレージをオフセットすることができます。

シックプロビジョニングFlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo` （サービスレベル目標）オプションをに設定します `thick`。

ボリュームのセミシックプロビジョニング

セミシックプロビジョニングを利用するボリュームを作成すると、 ONTAP はボリュームサイズに相当するストレージスペースをアグリゲートから確保します。ブロック共有テクノロジでブロックが使用されているためにボリュームの空きスペースが不足しそうになると、 ONTAP は保護データオブジェクト（ Snapshot コピー、 FlexClone ファイル、 FlexClone LUN ）を削除して、該当するオブジェクトが保持しているスペースを解放します。上書きに必要なスペースを確保できる速度で ONTAP が保護データオブジェクトを削除できるかぎり、書き込み処理は続行されます。これは「ベストエフォート」書き込み保証と呼ばれます。

- 注： * セミシックプロビジョニングを使用するボリュームでは、次の機能はサポートされていません。
- 重複排除、圧縮、コンパクションなどの Storage Efficiency テクノロジ
- Microsoft オフロードデータ転送（ ODX ）

セミシックプロビジョニングFlexVol ボリュームを作成するには、そのボリュームを設定します `-space-slo`（サービスレベル目標）オプションをに設定します `semi-thick`。

スペースリザーブファイルおよびスペースリザーブ **LUN** で使用します

スペースリザーブファイルまたはスペースリザーブ LUN は、ストレージの作成時にそのストレージに割り当てられるものです。ネットアップではこれまで、スペース・リザベーションが無効になっている LUN （スペース・リザーブなしの LUN ）を「シン・プロビジョニング LUN 」と呼んできました。

- 注意： * スペースリザーブなしのファイルは、一般的に「シンプロビジョニングされたファイル」とは呼ばれません。

次の表に、スペースリザーブファイルおよびスペースリザーブ LUN で使用できる 3 つのボリュームプロビジョニングオプションの主な違いを示します。

ボリュームのプロビジョニング	**LUN/file** のスペースリザベーション	上書きします	保護データ [2]	ストレージ効率 [3]
厚み（ Thick ）	サポートされます	保証された ^1	保証	サポートされます
シン	効果はありません	なし	保証	サポートされます

ボリュームのプロビジョニング	**LUN/file** のスペースリザベーション	上書きします	保護データ [2]	ストレージ効率 [3]
セミシック	サポートされます	ベストエフォート ^1 ^	ベストエフォート	サポート対象外

- メモ *
  1. 上書きの保証またはベストエフォートの上書き保証が行われるには、 LUN またはファイルでスペースリザベーションが有効になっている必要があります。
  2. 保護データには、 Snapshot コピーおよび自動削除の対象とマークされた FlexClone ファイルと FlexClone LUN （バックアップクローン）が含まれます。
  3. Storage Efficiency には、重複排除、圧縮、自動削除の対象とマークされていない FlexClone ファイルと FlexClone LUN （アクティブクローン）、および FlexClone サブファイル（コピーオフロードに使用）が含まれます。

SCSI シンプロビジョニング **LUN** のサポート

ONTAP は、 T10 SCSI シンプロビジョニング LUN に加え、ネットアップのシンプロビジョニング LUN もサポートしています。T10 SCSI シンプロビジョニングを使用すると、ホストアプリケーションで、 LUN のスペース再生やブロック環境の LUN スペース監視機能などの SCSI 機能をサポートできます。使用する SCSI ホストソフトウェアも、 T10 SCSI シンプロビジョニングをサポートしている必要があります。

ONTAP を使用します `space-allocation` LUNでのT10シンプロビジョニングのサポートを有効または無効にするための設定。ONTAP を使用します `space-allocation enable` LUNでT10 SCSIシンプロビジョニングを有効にするための設定。

。 `[-space-allocation {enabled|disabled}]` ONTAP でT10シンプロビジョニングのサポートを有効または無効にする方法、およびT10 SCSIシンプロビジョニングを有効にする方法の詳細については、『Command Reference Manual』のコマンドを参照してください。

"ONTAP 9 のコマンド"

ボリュームのプロビジョニングオプションを設定

ボリュームにシンプロビジョニング、シックプロビジョニング、またはセミシックプロビジョニングを設定できます。

このタスクについて

を設定します `-space-slo` オプションをに設定します `thick` 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません `volume create` または `volume modify` ボリュームを設定するコマンド `-space-guarantee` オプション
- 上書きに必要なスペースの 100% がリザーブされます。を使用することはできません `volume modify` ボリュームを設定するコマンド `-fractional-reserve` オプション

を設定します `-space-slo` オプションをに設定します `semi-thick` 次のことを確認します。

- ボリューム全体がアグリゲートに事前に割り当てられます。を使用することはできません `volume`

`create` または `volume modify` ボリュームを設定するコマンド `-space-guarantee` オプション

- スペースは上書き用にリザーブされません。を使用できます `volume modify` ボリュームを設定するコマンド `-fractional-reserve` オプション
- Snapshot コピーの自動削除が有効になります。

ステップ

1. ボリュームのプロビジョニングオプションを設定します。

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   。 `-space-guarantee` オプションのデフォルトはです `none` （AFF システムの場合）およびAFF以外のDPボリュームの場合。それ以外の場合は、デフォルトでになります `volume`。既存のFlexVol ボリュームの場合は、を使用します `volume modify` プロビジョニングオプションを設定するコマンド。

   次のコマンドを使うと、 SVM vs1 上の vol1 にシンプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にシックプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   次のコマンドを使うと、 SVM vs1 上の vol1 にセミシックプロビジョニングが設定されます。

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

SAN ボリュームの構成オプション

LUN が含まれているボリュームに対してさまざまなオプションを設定する必要があります。ボリュームオプションの設定方法によって、ボリューム内の LUN で使用可能なスペースの量が決まります。

自動拡張

自動拡張は有効または無効にすることができます。有効にすると、 ONTAP では、ボリュームのサイズを事前設定した最大サイズまで自動的に拡張できます。ボリュームの自動拡張をサポートするには、使用可能なスペースを包含アグリゲートに確保する必要があります。そのため、自動拡張を有効にする場合は、包含アグリゲートの空きスペースを監視し、必要に応じて追加してください。

自動拡張は、 Snapshot の作成時にはトリガーできません。自動拡張が有効になっていても、ボリュームに十分なスペースがないと Snapshot の作成は失敗します。

自動拡張が無効な場合、ボリュームのサイズに変更はありません。

自動縮小

自動縮小は有効または無効にすることができます。有効にすると、 ONTAP では、ボリュームで消費されたスペースの量が事前設定したしきい値を下回った場合に、ボリューム全体のサイズを自動的に縮小できます。これにより、ボリュームで未使用の空きスペースの自動的な解放が開始されて、ストレージ効率が向上します。

Snapshot の自動削除

Snapshot の自動削除では、次のいずれかの場合に、 Snapshot コピーが自動的に削除されます。

- ボリュームがフルに近い状態の場合
- Snapshot リザーブスペースがフルに近い状態の場合
- オーバーライトリザーブスペースがフルの場合

古いものから順に、または新しいものから順に Snapshot コピーを削除するように Snapshot の自動削除を設定できます。Snapshot の自動削除では、クローンボリュームや LUN 内の Snapshot コピーにリンクされている Snapshot コピーは削除されません。

自動拡張と Snapshot の自動削除の両方が有効な場合にボリュームで追加のスペースが必要になると、デフォルトでは、 ONTAP は最初に自動拡張をトリガーして、必要なスペースを確保しようとします。自動拡張で十分なスペースを確保できない場合は、 Snapshot の自動削除がトリガーされます。

Snapshot リザーブ

Snapshot リザーブは、 Snapshot コピー用にリザーブされるボリューム内のスペースの量を定義します。Snapshot リザーブに割り当てられたスペースを他の目的に使用することはできません。Snapshot リザーブ用に割り当てられたすべてのスペースが使用された場合、 Snapshot コピーはボリューム上の追加スペースを消費します。

SAN 環境でのボリューム移動に関する要件

LUN またはネームスペースを含むボリュームを移動する場合は、一定の要件を満たす必要があります。

- ボリュームに 1 つ以上の LUN が含まれている場合は、クラスタ内の各ノードに接続する LUN （ LIF ）ごとに少なくとも 2 つのパスが必要です。

  これにより、単一点障害が排除され、コンポーネント障害に備えてシステムの運用を継続することができます。

- ボリュームにネームスペースが含まれている場合は、クラスタで ONTAP 9.6 以降が実行されている必要があります。

  ONTAP 9.5 を実行する NVMe 構成では、ボリューム移動はサポートされません。

フラクショナルリザーブの設定に関する考慮事項

フラクショナルリザーブは、 _lun overwrite reserve _ とも呼ばれ、 FlexVol ボリューム

内のスペースリザーブ LUN およびファイルのオーバーライトリザーブを無効にすることができます。これはストレージ利用率を最大限に高めるのに役立ちますが、スペース不足による書き込みエラーが悪影響を及ぼす環境では、この設定を利用する場合の要件を確認しておく必要があります。

フラクショナルリザーブ設定はパーセンテージで表され、有効な値はのみです `0` および `100` パーセントフラクショナルリザーブ設定はボリュームの属性です。

フラクショナルリザーブをに設定しています `0` ストレージ利用率が向上します。ただし、ボリュームの空きスペースがなくなると、ボリュームギャランティがに設定されていても、ボリュームに格納されたデータにアクセスするアプリケーションでデータを利用できなくなる可能性があります `volume`。ただし、ボリュームを適切に設定して使用することで、書き込みが失敗する可能性を最小限に抑えることができます。ONTAP では、フラクショナルリザーブがに設定されたボリュームに対して「ベストエフォート」の書き込み保証が提供されます `0` 次の要件の_all_が満たされている場合：

- 重複排除を使用していません
- 圧縮を使用していません
- FlexClone サブファイルが使用されていません
- すべての FlexClone ファイルと FlexClone LUN で自動削除が有効になっています

  これはデフォルト設定ではありません。FlexClone ファイルや FlexClone LUN の自動削除は、作成時に設定するか作成後に変更して明示的に有効にする必要があります。

- ODX コピーオフロードと FlexClone コピーオフロードは使用されていません
- ボリュームギャランティがに設定されている `volume`
- ファイルまたはLUNのスペースリザベーションはです `enabled`
- ボリュームのSnapshotリザーブがに設定されている `0`
- ボリュームSnapshotコピーの自動削除はです `enabled` を使用しています `destroy`を削除します `lun_clone,vol_clone,cifs_share,file_clone,sfsr`をクリックします `volume`

  この設定では、必要に応じて FlexClone ファイルと FlexClone LUN も削除されます。

変更率が高いと、上記の必要な設定をすべて行っていても、まれに Snapshot コピーの自動削除が追いつかなくなり、ボリュームのスペースが不足することがあります。

また、必要に応じてボリュームの自動拡張機能を使用することで、ボリュームの Snapshot コピーの自動削除が発生する可能性を抑えることができます。自動拡張機能を有効にする場合は、関連付けられたアグリゲートの空きスペースを監視する必要があります。アグリゲートの空きスペースがなくなり、ボリュームを拡張できなくなると、ボリュームの空きスペースがなくなったときに削除される Snapshot コピーが増える可能性があります。

上記の設定要件をすべて満たすことができず、ボリュームのスペース不足を防ぐ必要がある場合は、ボリュームのフラクショナルリザーブ設定をに設定する必要があります `100`。これにより、事前に確保する必要がある空きスペースは増えますが、上記のテクノロジを使用する場合でもデータ変更処理が確実に実行されるようになります。

フラクショナルリザーブ設定のデフォルト値と有効値は、ボリュームのギャランティによって異なります。

ボリュームギャランティ	デフォルトのフラクショナルリザーブ	使用できる値
ボリューム	100	0、100
なし	0	0、100

SANホスト側のスペース管理

シンプロビジョニング環境において、ホストファイルシステムで解放されたスペースをストレージシステム側で管理するプロセスを担っているのがホスト側のスペース管理です。

ホストファイルシステムでは、新しいデータの格納に使用できるブロックはどれか、また、有効なデータを含んでいるため上書きしてはならないブロックはどれかを追跡するための情報がメタデータに記録されます。このメタデータは LUN 内に格納されます。ホストファイルシステム内でファイルが削除されると、ファイルシステムのメタデータが更新され、削除されたファイルのブロックが空きスペースとしてマークされます。ファイルシステム内の合計空きスペースが再計算され、新しく解放されたブロック分のスペースが組み入れられます。ストレージシステム側では、こうしたメタデータの更新が、ホストによって実行される他の書き込みとまったく相違ないものとして認識されます。このため、ストレージシステム側では、削除が行われた事実が検知されません。

その結果、ホスト側と基盤のストレージシステム側で報告される空きスペース容量に不一致が生じます。たとえば、新しくプロビジョニングされた 200GB の LUN がストレージシステムによってホストに割り当てられているとします。ホストとストレージシステムの両方で、 200GB の空きスペースが報告されます。ホストに 100GB のデータが書き込まれた場合。この時点で、ホストとストレージシステムの両方で、使用済みスペースが 100GB 、未使用スペースが 100GB と報告されます。

次に、ホストから 50GB のデータが削除されました。この時点で、ホストは使用済みスペースが 50GB 、未使用スペースが 150GB であると報告します。ただし、ストレージシステムから報告される使用済みスペースは 100GB 、未使用スペースは 100GB です。

ホスト側のスペース管理では、さまざまな方法を使用して、ホストとストレージシステム間のスペースの差分を調整します。

SnapCenter によるホスト管理の簡易化

SnapCenter ソフトウェアを使用すると、 iSCSI ストレージや FC ストレージに関連する管理作業とデータ保護作業を簡単に行うことができます。SnapCenter は、 Windows ホストと UNIX ホストに対応するオプションの管理パッケージです。

SnapCenter ソフトウェアを使用すると、ストレージプールから簡単に仮想ディスクを作成して複数のストレージシステムに分散したり、ストレージのプロビジョニングタスクを自動化したりできます。また、ホストのデータと整合性のある Snapshot コピーや Snapshot コピーからのクローンの作成プロセスが簡易化されます。

詳細については、ネットアップ製品のドキュメントを参照してください "SnapCenter"。

関連リンク

"SCSI シンプロビジョニング LUN のスペース割り当てを有効にします"

igroup について

initiator group （ igroup ；イニシエータグループ）は、 FC プロトコルホスト WWPN または iSCSI ホストノード名のテーブルです。igroup を定義して LUN にマッピングし、どのイニシエータが LUN にアクセスできるかを制御できます。

通常は、ホストのイニシエータポートまたはソフトウェアイニシエータがすべて LUN にアクセスできることが必要とされます。マルチパスソフトウェアを使用しているか、またはクラスタホストがある場合、各イニシエータポートまたは各クラスタホストのソフトウェアイニシエータは同じ LUN への冗長パスを必要とします。

LUN にアクセスできるイニシエータを指定する igroup は LUN の作成前後どちらでも作成できますが、 LUN を igroup にマッピングするには igroup を作成しておく必要があります。

igroup には複数のイニシエータを含めることができ、複数の igroup に同じイニシエータを含めることができます。ただし、同じイニシエータを持つ複数の igroup に 1 つの LUN をマッピングすることはできません。1 つのイニシエータを、 ostype が異なる複数の igroup のメンバーにすることはできません。

igroup による LUN アクセスの提供例

複数の igroup を作成して、ホストで利用できる LUN を定義することができます。たとえば、ホストクラスタを使用している場合、いくつかの igroup を使用して、クラスタ内の 1 つのホストだけ、またはすべてのホストに特定の LUN が認識されるように設定できます。

次の表に、ストレージシステムにアクセスする 4 つのホストについて、 4 つの igroup によって LUN にアクセスできるようにする方法を示します。クラスタ化したホスト（ Host3 および Host4 ）は、両方とも同一 igroup （ group3 ）のメンバーであり、この igroup にマッピングされている LUN にアクセスできます。group4 という igroup には Host4 の WWPN が含まれ、パートナーには表示されないローカルな情報が格納されます。

HBA WWPN 、 **IQN** 、または **EUI** のホスト	**igroup** 数	**igroup** に追加されている **WWPN** 、 **IQN** 、 **EUI**	**igroup** にマッピングされている **LUN**
Host1 、シングルパス（ iSCSI ソフトウェアイニシエータ） iqn.1991-05.com.microsoft:host1	グループ 1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2 、マルチパス（ HBA × 2 ） 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 6b ： 3c 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 02 ： 3c	グループ2	10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 6b ： 3c 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 02 ： 3c	`/vol/vol2/lun2`

HBA WWPN 、 **IQN** 、または **EUI** のホスト	**igroup** 数	**igroup** に追加されている **WWPN** 、 **IQN** 、 **EUI**	**igroup** にマッピングされている **LUN**
Host3 、マルチパス、ホスト 4 でクラスタ構成 10：00：00：00：c9：2b：32：1b 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 41 ： 02	グループ 3	10：00：00：00：c9：2b：32：1b 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 41 ： 02 10：00：00：00：c9：2b：51：2c 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 47 ： A2	`/vol/vol2/qtree1/lun3`
Host4 、マルチパス、クラスタ構成（ Host3 には認識されない） 10：00：00：00：c9：2b：51：2c 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 47 ： A2	グループ 4	10：00：00：00：c9：2b：51：2c 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 47 ： A2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

igroup のイニシエータの WWPN と iSCSI ノード名を指定します

igroup の作成時に、イニシエータの iSCSI ノード名と WWPN を指定できます。それらをあとから指定することもできます。LUN の作成時にイニシエータの iSCSI ノード名と WWPN を指定するように選択した場合は、必要に応じてそれらをあとから削除できます。

Host Utilities のマニュアルに記載されている手順に従って、 WWPN を取得し、特定のホストに関連付けられている iSCSI ノード名を確認します。ESX ソフトウェアを実行しているホストでは、 Virtual Storage Console を使用します。

VMware と Microsoft のコピーオフロードによるストレージ仮想化

VMware と Microsoft のコピーオフロードによるストレージ仮想化の概要

VMware と Microsoft は、パフォーマンスとネットワークスループットを向上させるために、コピーオフロード処理をサポートしています。VMware と Windows それぞれのオペレーティングシステム環境で、コピーオフロード機能を使用するための要件を満たすように、システムを設定する必要があります。

VMware と Microsoft のコピーオフロードを仮想環境で使用する場合は、 LUN をアライメントする必要があります。LUN がアライメントされていないと、パフォーマンスが低下

仮想 **SAN** 環境を使用する利点

Storage Virtual Machine （ SVM ）と LIF を使用して仮想環境を作成すると、 SAN 環境をクラスタ内のすべてのノードに拡張できます。

- 分散管理

  SVM の任意のノードにログインして、クラスタ内のすべてのノードを管理できます。

- データアクセスの向上

  MPIO と ALUA を使用することで、 SVM のどのアクティブな iSCSI LIF または FC LIF からでもデータにアクセスできます。

- LUN アクセスの制御

  SLM とポートセットを使用すると、イニシエータによって LUN へのアクセスに使用される LIF を制限できます。

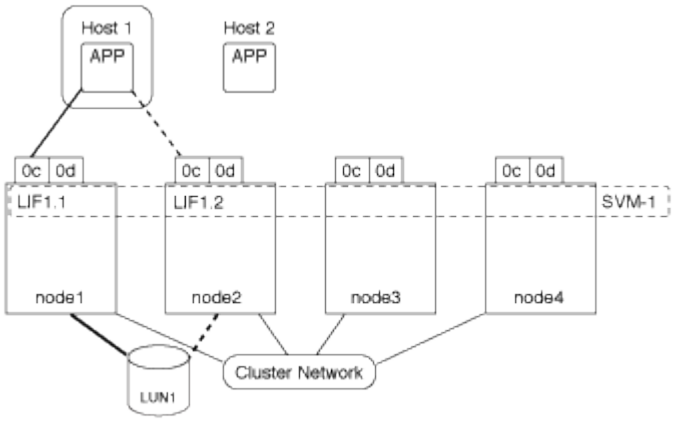
仮想環境での **LUN** へのアクセスの仕組み

仮想環境では、ホスト（クライアント）は LIF を使用して、最適パスおよび非最適パス経由で LUN にアクセスします。

LIF は、 SVM を物理ポートに接続する論理インターフェイスです。複数の SVMs で同じポート上に複数の LIF を設定できますが、 1 つの LIF は 1 つの SVM に属します。LUN には、 SVM の LIF を介してアクセスできます。

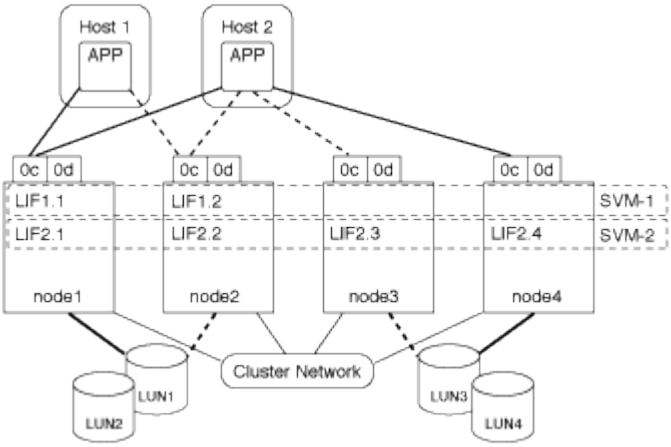
クラスタ内の**1**つの**SVM**を使用した**LUN**へのアクセス例

次の例では、ホスト 1 が SVM-1 の LIF1.1 と LIF1.2 に接続して LUN1 にアクセスします。LIF1.1 は物理ポート node1 ： 0c を、 LIF1.2 は node2 ： 0c を使用します。LIF1.1 と LIF1.2 は SVM-1 のみに属しています。SVM-1 のノード 1 またはノード 2 で新しい LUN を作成した場合は、その LUN でもこれらの同じ LIF を使用できます。新しい SVM を作成した場合は、両方のノードの物理ポート 0c または 0d を使用して新しい LIF を作成できます。



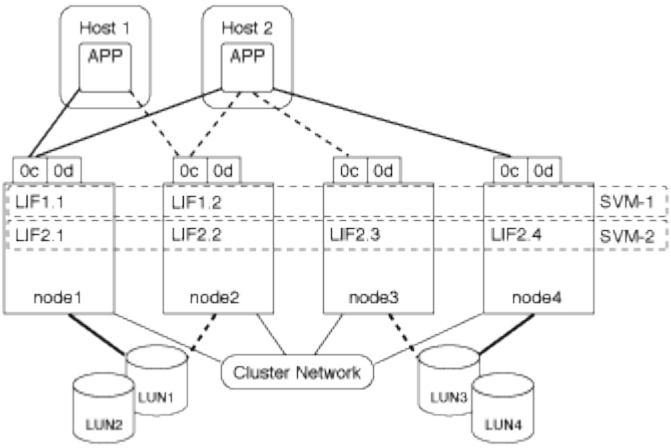
クラスタ内の複数の**SVM**を使用した**LUN**へのアクセス例

1 つの物理ポートに複数の LIF を設定して、異なる SVM を接続できます。LIF は特定の SVM に関連付けられているため、クラスタノードは受信データトラフィックを正しい SVM に送信できます。次の例では、 1~4 の各ノードに、各ノードの物理ポート 0c を使用して SVM-2 用の LIF を 1 つずつ設定しています。ホスト 1 は SVM-1 の LIF1.1 と LIF1.2 に接続して LUN1 にアクセスします。ホスト 2 は、 SVM-2 の LIF2.1 と LIF2.2 に接続して LUN2 にアクセスします。両方の SVM がノード 1 とノード 2 の物理ポート 0c を共有しています。SVM-2 には追加の LIF があり、ホスト 2 はこの LIF を使用して LUN3 と LUN4 にアクセスします。これらの LIF はノード 3 とノード 4 の物理ポート 0c を使用します。複数の SVMs でそれらのノードの物理ポートを共有できます。



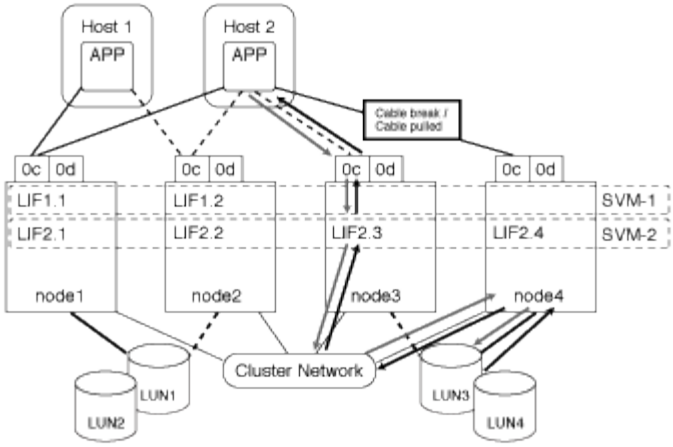
ホストシステムから**LUN**へのアクティブパスまたは最適パスの例

アクティブパスまたは最適パスでは、データトラフィックはクラスタネットワークを経由せずに、 LUN への最短ルートをとります。LUN1 へのアクティブパスまたは最適パスは、物理ポート 0c を使用してノード 1 の LUN1 1. を経由します。ホスト 2 には、アクティブパスまたは最適パスが 2 つあります。 1 つは node1 へのパスで、 LIF2.1 は物理ポート 0c を共有し、もう 1 つは node4 、 LIF2.4 は物理ポート 0c を使用します。



ホストシステムから**LUN**へのアクティブパスまたは非最適（間接）パスの例

アクティブパスまたは非最適（間接）パスでは、データトラフィックはクラスタネットワークを経由します。この問題は、ホストからのアクティブパスまたは最適パスがすべて使用できず、トラフィックを処理できない場合にのみ発生します。ホスト 2 から SVM-2 LIF2.4 へのパスが失われた場合は、クラスタネットワークを経由して LUN3 と LUN4 にアクセスします。ホスト 2 からのアクセスには、ノード 3 の LIF2.3 が使用されます。トラフィックは、クラスタネットワークスイッチに入ったあと、 LUN3 と LUN4 にアクセスできるようノード 4 にバックアップされます。次に、クラスタネットワークスイッチ経由で逆方向に戻り、 LIF2.3 経由でホスト 2 にバックアウトされます。このアクティブパスまたは非最適パスは、 LIF2.4 へのパスがリストアされるか、ノード 4 のもう 1 つの物理ポートで SVM-2 の新しい LIF が確立されるまで使用されます。



= :allow-uri-read:

ESX ホストの VMware VAAI パフォーマンスを向上させます

ONTAP では、 ESX ホストで ESX 4.1 以降が実行されている場合、 VMware vStorage APIs for Array Integration （ VAAI ）の一部の機能がサポートされます。これらの機能を使用すると、 ESX ホストからストレージシステムに処理の負荷をオフロードし、ネットワークスループットを向上させることができます。これらの機能は、正しい環境の ESX ホストで自動的に有効になります。

VAAI 機能は、次の SCSI コマンドをサポートします。

- `EXTENDED_COPY`

  この機能により、ホストは、データ転送の際にホストに影響を与えることなく、 LUN 間または LUN 内のデータ転送を開始できます。その結果、 ESX CPU サイクルが節約され、ネットワークスループットが増加します。拡張コピー機能は「コピーオフロード」とも呼ばれ、仮想マシンのクローニングなどで使用されます。ESX ホストからコピーオフロード機能が呼び出されると、ホストネットワークを経由せずにストレージシステム内でデータがコピーされます。コピーオフロードでは、次の方法でデータが転送されます。

  - LUN 内で組み合わせることができます
  - ボリューム内の LUN 間
  - Storage Virtual Machine （ SVM ）内の異なるボリューム上の LUN 間
  - クラスタ内の異なるSVM上のLUN間 この機能を呼び出すことができない場合、ESXホストは自動的に標準の読み取りコマンドと書き込みコマンドをコピー処理に使用します。

- `WRITE_SAME`

  この機能により、すべてゼロなどの繰り返しパターンをストレージアレイに書き込む処理がオフロードされます。この機能は、ファイルをゼロで埋める場合などに使用されます。

- `COMPARE_AND_WRITE`

  特定のファイルへの同時アクセス制限がバイパスされ、仮想マシンのブートなどの処理が高速になります。

VAAI 環境を使用するための要件

VAAI 機能は ESX オペレーティングシステムの一部であり、環境を正しく設定すると、 ESX ホストによって自動的に起動されます。

環境の要件は次のとおりです。

- ESX ホストで ESX 4.1 以降が実行されている必要があります。
- VMware データストアをホストするネットアップストレージシステムで ONTAP を実行する。
- （コピーオフロードのみ） VMware コピー操作のソースとデスティネーションの両方が同じクラスタ内の同じストレージシステムでホストされている。

> コピーオフロード機能は、現時点では、異なるストレージシステムでホストされている VMware データストア間のコピーに対応していません。

VAAI 機能が **ESX** でサポートされているかどうかを確認します

ESX オペレーティングシステムで VAAI 機能がサポートされているかどうかを確認するには、 vSphere Client を確認するか、他の方法でホストにアクセスします。ONTAP はデフォルトで SCSI コマンドをサポートします。

ESX ホストの詳細設定を確認して、 VAAI 機能が有効になっているかどうかを確認できます。次の表に、SCSI コマンドと対応する ESX コントロールの名前を示します。

SCSIコマンド	**ESX** コントロール名（ **VAAI** 機能）
extended_copy の実行が可能です	`HardwareAcceleratedMove`
WRITE_Same	`HardwareAcceleratedInit`
_ と _ を比較します	`HardwareAcceleratedLocking`

Microsoft オフロードデータ転送（ **ODX** ）

Microsoft Offloaded Data Transfer （ ODX ；オフロードデータ転送）は _ コピーオフロード _ とも呼ばれ、この機能を使用すると、ストレージデバイス内または互換性がある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では、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。

ODX 以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でホストに転送されます。ホストは、データをネットワーク経由でデスティネーションに転送します。ODX ファイル転送では、ホストを経由せずに、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とデスティネーションの間で直接実行されるため、同じボリューム内でコピーを実行するとパフォーマンスが大幅に向上します。たとえば、同じボリュームコピーのコピー時間の短縮、クライアントでのCPUとメモリの使用量の削減、ネットワークI/O帯域幅の使用量の削減などが挙げられます。複数のボリュームにコピーが存在する場合は、ホストベースのコピーに比べてパフォーマンスが大幅に向

上することはありません。

SAN 環境で ODX を使用できるのは、ホストとストレージシステムの両方で ODX がサポートされている場合のみです。ODX がサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロードファイル転送が自動的かつ透過的に使用されます。ODX は、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

ODX を使用するための要件

コピーオフロードに ODX を使用する場合は、ボリュームのサポートに関する考慮事項、システム要件、およびソフトウェア機能の要件について理解しておく必要があります。

ODX を使用するためのシステム要件は次のとおりです。

- ONTAP

  サポート対象のバージョンの ONTAP では、 ODX が自動的に有効になります。

- ソースボリュームの最小サイズは 2GB です

  最適なパフォーマンスを確保するには、 260GB 以上のソースボリュームが必要です。

- Windows クライアントでの ODX のサポート

  ODX は、 Windows Server 2012 以降および Windows 8 以降でサポートされます。サポート対象の Windows クライアント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 で確認できます"

- コピーアプリケーションによる ODX のサポート

  データ転送を実行するアプリケーションが ODX をサポートする必要があります。ODX がサポートされるアプリケーション処理は次のとおりです。

  - Virtual Hard Disk （ VHD ；仮想ハードディスク）の作成および変換、 Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、 Hyper-V の管理処理
  - エクスプローラでの操作
  - Windows PowerShell の copy コマンド
  - Windows コマンドプロンプトの copy コマンド WindowsサーバおよびクライアントでサポートされるODXアプリケーションの詳細については、Microsoft TechNetライブラリを参照してください。

- 圧縮されたボリュームを使用する場合は、圧縮グループサイズを 8K にする必要があります。

  32K の圧縮グループサイズはサポートされていません。

ODX を次のタイプのボリュームで使用することはできません。

- 容量が 2GB 未満のソースボリューム
- 読み取り専用ボリューム

- "FlexCache ボリューム"

  ODXはFlexCache元のボリュームでサポートされます。

- "セミシックプロビジョニングされたボリューム"

特別なシステムファイルの要件

qtree で見つかった ODX ファイルを削除できます。テクニカルサポートから指示されないかぎり、他の ODX システムファイルは削除または変更しないでください。

ODX 機能を使用する場合、システムのすべてのボリュームに ODX システムファイルが存在します。これらのファイルによって、 ODX 転送時に使用されるデータのポイントインタイムビューが有効になります。次のシステムファイルは、データのオフロード先となる LUN またはファイルがある各ボリュームのルートレベルにあります。

- `.copy-offload` （非表示のディレクトリ）
- `.tokens` （非表示の下のファイル `.copy-offload` ディレクトリ）

を使用できます `copy-offload delete-tokens -path dir_path -node` *`node_name`* ODXファイルを含むqtreeを削除するコマンド。

ODX のユースケース

SVM で ODX を使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODX をサポートする Windows サーバおよびクライアントでは、リモートサーバ間でデータをコピーする際に、デフォルトでコピーオフロードが使用されます。Windows サーバまたはクライアントで ODX がサポートされていない場合や、 ODX コピーオフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODX コピーおよび移動の使用は、以下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 SVM は同じです

  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 は同じです

  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、ノードは同じです

  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。データは異なる SVM に所有されます。

- SVM とノードが異なります

  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。データは異なる SVM に所有されます。

- クラスタ間

  ソース LUN とデスティネーション LUN は、異なるクラスタの異なるノード上の異なるボリュームにあります。これはSANでのみサポートされ、SMBでは機能しません。

その他にも、いくつかの特殊なユースケースがあります。

- ONTAP の ODX の実装で ODX を使用すると、 SMB 共有と FC / iSCSI で接続された仮想ドライブとの間でファイルをコピーできます。

  SMB 共有と LUN が同じクラスタにある場合は、 Windows エクスプローラ、 Windows CLI または PowerShell 、 Hyper-V 、または ODX をサポートするその他のアプリケーションを使用して、 SMB 共有と接続された LUN 間の ODX コピーオフロードを使用してファイルをシームレスにコピーまたは移動できます。

- Hyper-V では、さらに次のようなユースケースでも ODX コピーオフロードが使用されます。

  - Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（ VHD ）ファイル内および VHD ファイル間でのデータのコピー、または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 の間でのデータのコピーを実行できます。

    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 を作成する際に、 ODX を使用して、既知の初期化済みトークンによっ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に、 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用途を活用するには、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ディスクが IDE ディスクの場合、 ODX のパススルーはサポートされません。