SANストレージ管理

ONTAP 9

NetApp
April 24, 2024

目次

SANストレージ管理

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。

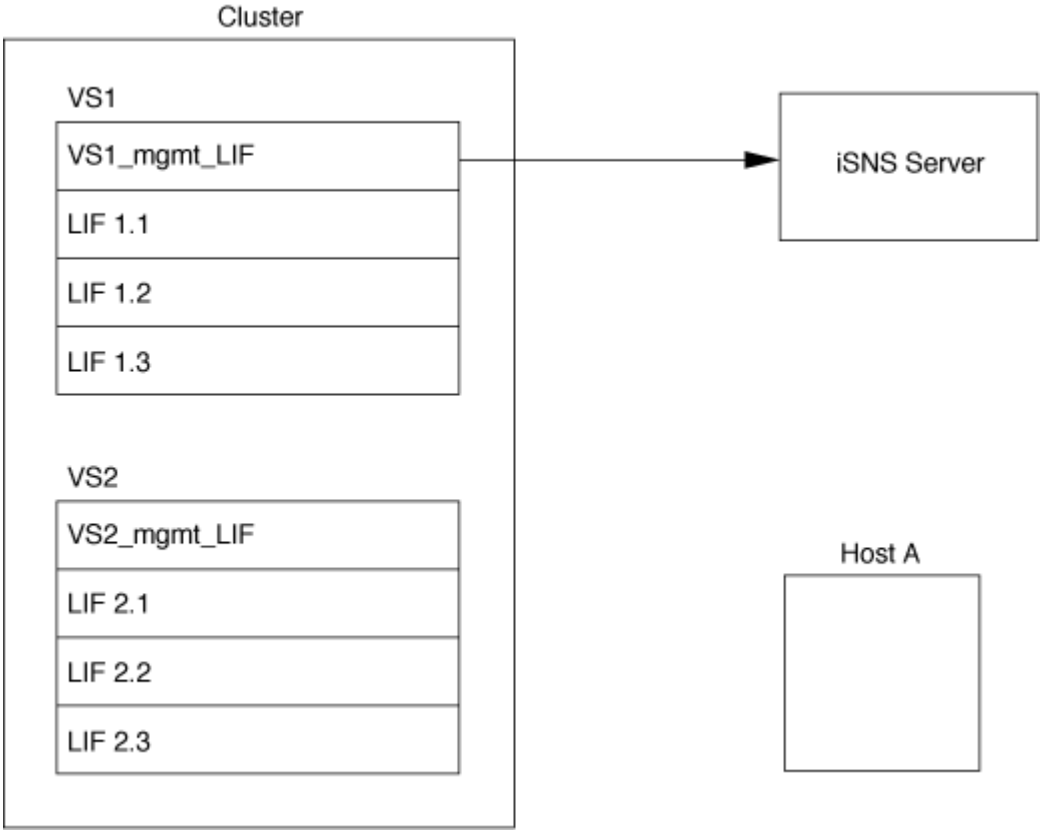
ネットアップでは、 iSNS サーバの提供や再販は行っていません。これらのサーバは、ネットアップがサポー

トするベンダーから入手できます。

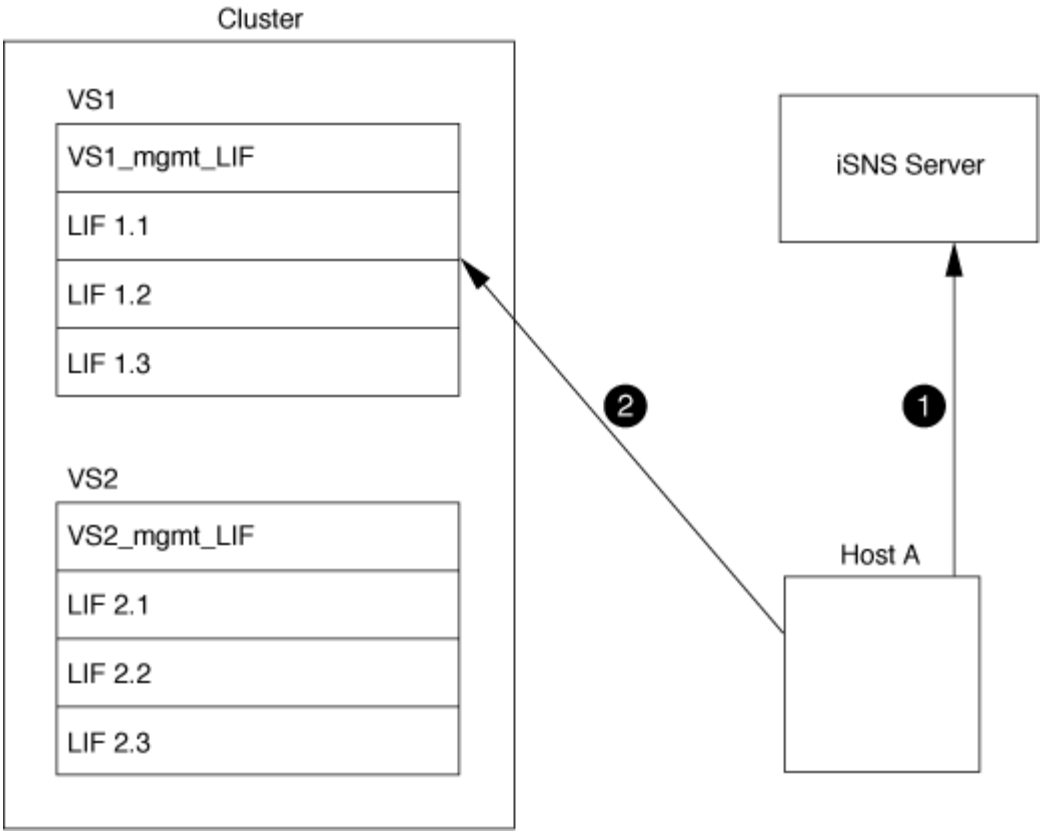
SVMs と **iSNS** サーバの連動

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。

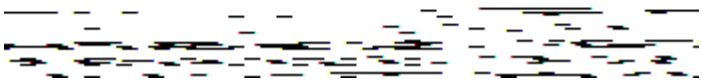
WWN が割り当て時にシーケンシャルでないように見える理由は次のとおりです。

- 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
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。

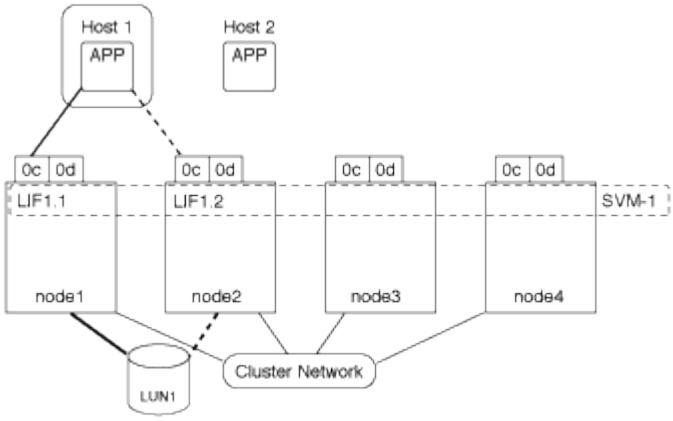
仮想環境での **LUN** へのアクセスの仕組み

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

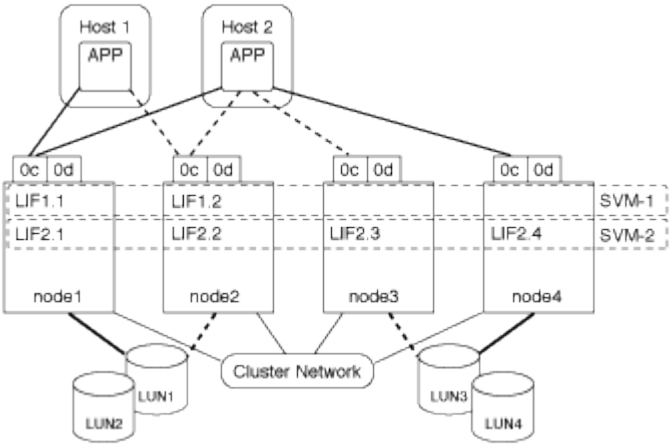
次の例では、ホスト 1 が SVM-1 の LIF1.1 と LIF1.2 に接続して LUN1 にアクセスします。LIF1.1 は物理ポート node1 ： 0c を、 LIF1.2 は node2 ： 0c を使用します。LIF1.1 と LIF1.2 は SVM-1 のみに属しています。SVM-1 のノード 1 またはノード 2 で新しい LUN を作成した場合は、その LUN でもこれらの同じ LIF を使用できます。新しい SVM を作成した場合は、両方のノードの物理ポート 0c または 0d を使用して新しい LIF を作成できます。



クラスタ内の複数の**SVM**を使用した**LUN**へのアクセス例

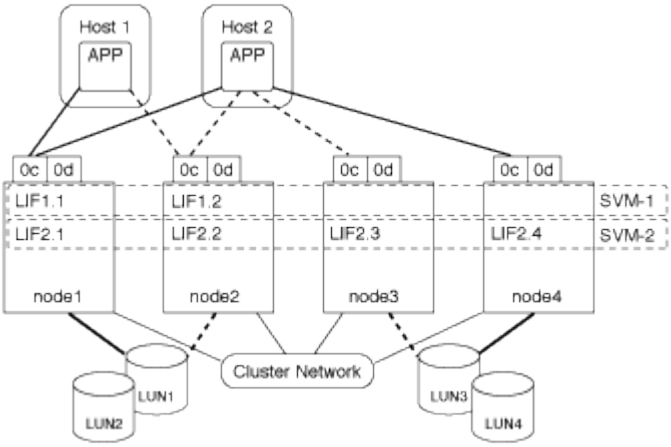
1 つの物理ポートに複数の LIF を設定して、異なる SVM を接続できます。LIF は特定の SVM に関連付けられているため、クラスタノードは受信データトラフィックを正しい SVM に送信できます。次の例では、 1~4 の

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。



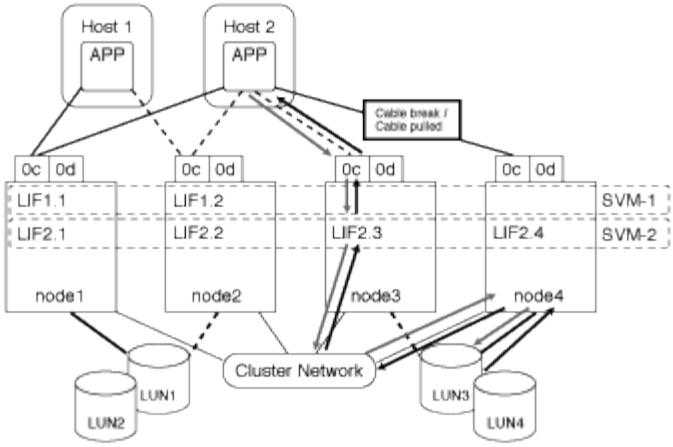
ホストシステムから**LUN**へのアクティブパスまたは最適パスの例

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。

SAN 管理

SANプロビジョニング

SANの管理の概要

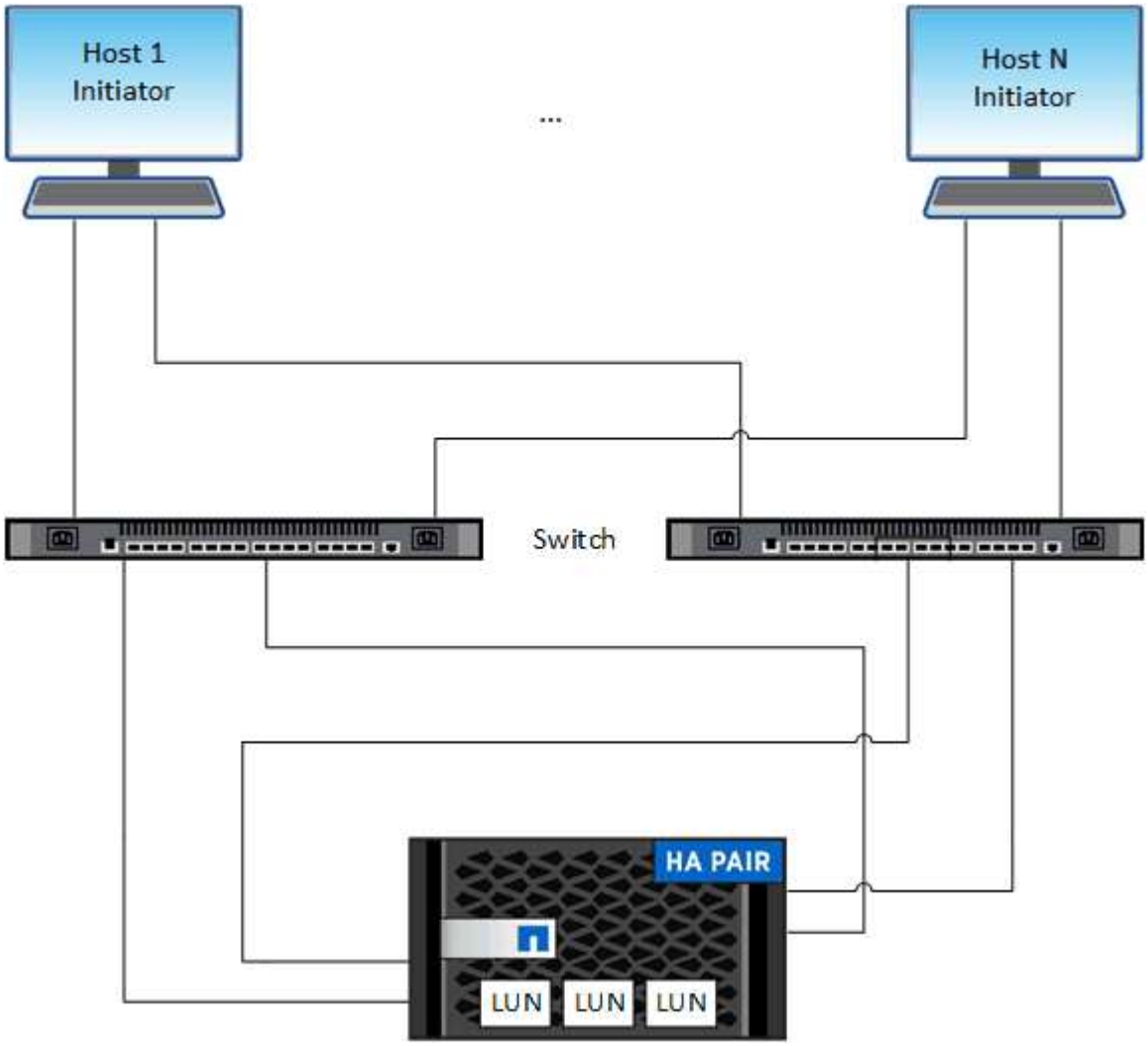
このセクションの内容では、ONTAP 9.7以降のリリースのONTAP コマンドラインイン

ターフェイス（CLI）およびSystem Managerを使用してSAN環境を構成および管理する方法を説明します。

従来の System Manager （ ONTAP 9.7 以前でのみ使用可能）を使用している場合は、次のトピックを参照してください。

- "iSCSI プロトコル"
- "FC/FCoE プロトコル"

iSCSI プロトコルと FC プロトコルを使用して、 SAN 環境にストレージを提供できます。



iSCSI および FC では、ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 LUN を作成して、イニシエータグループ（ igroup ）にマッピングします。イニシエータグループは、 FC ホスト WWPS と iSCSI ホストノード名の表であり、どのイニシエータがどの LUN にアクセスできるかを制御します。

FC ターゲットは FC スイッチおよびホスト側アダプタを介してネットワークに接続され、 World Wide Port Name （ WWPN ；ワールドワイドポート名）で識別されます。 iSCSIターゲットは、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TCPオフロードエンジン（TOE）カード、統合ネットワークアダプタ（CNA）または専用のホストバスアダプタ（HBA）を介してネットワークに接続し、iSCSI修飾名（IQN）で識別されます。

FCoE 用にスイッチを設定します

既存のイーサネットインフラで FC サービスを実行するには、 FCoE 用にスイッチを設定する必要があります。

必要なもの

- SAN 構成がサポートされている必要があります。

  サポートされている構成の詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

- Unified Target Adapter （ UTA ；ユニファイドターゲットアダプタ）をストレージシステムに設置する必要があります。

  UTA2を使用する場合は、に設定する必要があります `cna` モード（Mode）：

- Converged Network Adapter （ CNA ；統合ネットワークアダプタ）をホストにインストールする必要があります。

手順

1. スイッチのマニュアルを使用して、 FCoE 用にスイッチを設定します。
2. クラスタ内の各ノードのDCB設定が正しく設定されていることを確認します。

   ```
   run -node node1 -command dcb show
   ```

   DCB 設定はスイッチに対して行われます。設定が正しくない場合は、スイッチのマニュアルを参照してください。

3. FCターゲットポートのオンラインステータスがのときにFCoEログインが機能していることを確認する `true`。

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   FCターゲットポートのオンラインステータスがの場合 `false`スイッチのマニュアルを参照してください。

関連情報

- "NetApp Interoperability Matrix Tool で確認できます"
- "ネットアップテクニカルレポート 3800 ：『 Fibre Channel over Ethernet （ FCoE ） End-to-End Deployment Guide 』"
- "Cisco MDS 9000 NX-OS および SAN-OS ソフトウェアの構成ガイド"
- "Brocade 製品"

システム要件

LUN のセットアップでは、 LUN を作成し、 igroup を作成して、 LUN を igroup にマッピングします。LUN をセットアップするには、システムが特定の前提条件を満たしている必要があります。

- Interoperability Matrix にサポート対象として掲載されている SAN 構成を使用する。
- で指定した SAN ホストとコントローラの構成の制限を SAN 環境が満たしている必要があります "NetApp Hardware Universe の略" ONTAP ソフトウェアのバージョンに対応している必要があります。
- サポートされているバージョンの Host Utilities がインストールされている。

  詳細については、 Host Utilities のマニュアルを参照してください。

- LUN の所有者ノードと所有者ノードの HA パートナーに SAN LIF がある。

関連情報

- "NetApp Interoperability Matrix Tool で確認できます"
- "ONTAP SAN ホスト構成"
- "ネットアップテクニカルレポート 4017 ：『ファイバチャネル SAN のベストプラクティス』"

LUNを作成する前に理解しておくべきこと

LUNの実際のサイズが少し異なる理由

LUNのサイズについては、次の点に注意してください。

- LUNを作成する場合、LUNの実際のサイズはLUNのOSタイプによって多少異なります。LUN の作成後に LUN の OS タイプを変更することはできません。
- 最大LUNサイズでLUNを作成する場合は、LUNの実際のサイズが若干小さくなる可能性があることに注意してください。ONTAP では、制限値の端数が切り捨てられます。
- 各 LUN のメタデータ用として、 LUN を含むアグリゲートに約 64KB のスペースが必要です。LUN の作成時には、 LUN を含むアグリゲートに LUN のメタデータ用の十分なスペースがあることを確認する必要があります。アグリゲートに LUN のメタデータ用のスペースが十分にないと、一部のホストが LUN にアクセスできなくなる可能性があります。

LUN ID の割り当てに関するガイドライン

通常、デフォルトの LUN ID は 0 で始まり、 LUN をマッピングするたびに 1 ずつ増加します。LUN ID は、ホストによって LUN の場所とパス名に関連付けられます。有効な LUN ID 番号の範囲は、ホストによって異なります。詳細については、 Host Utilities のマニュアルを参照してください。

LUN を igroup にマッピングする場合のガイドラインを次に示します

- LUNは、igroupに一度だけマッピングできます。
- ベストプラクティスとして、1つのLUNをigroupを介して1つの特定のイニシエータにのみマッピングすることを推奨します。
- 1 つのイニシエータを複数の igroup に追加できますが、そのイニシエータをマッピングできる LUN は 1 つだけです。

- 同じ igroup にマッピングされている 2 つの LUN に、同じ LUN ID を使用することはできません。
- igroup およびポートセットには、同じ種類のプロトコルを使用する必要があります。

プロトコル**FC**または**iSCSI**ライセンスを確認して追加します

FC または iSCSI で Storage Virtual Machine （ SVM ）のブロックアクセスを有効にするには、ライセンスが必要です。FCライセンスとiSCSIライセンスは、に含まれています。 "ONTAP One"。

例 **1.** 手順

System Manager の略

ONTAP Oneをお持ちでない場合は、ONTAP System Manager（9.7以降）でFCまたはiSCSIのライセンスを確認して追加します。

1. System Managerで、*[クラスタ]>[設定]>[ライセンス]*を選択します
2. ライセンスが表示されない場合は、を選択します  をクリックし、ライセンスキーを入力します。
3. 「 * 追加」を選択します。

CLI の使用

ONTAP Oneをお持ちでない場合は、ONTAP CLIを使用してFCまたはiSCSIのライセンスを確認して追加します。

1. FCまたはiSCSIのアクティブなライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのアクティブなライセンスがない場合は、ライセンスコードを追加します。

```
license add -license-code <your_license_code>
```

この手順 では、すでにFCプロトコルまたはiSCSIプロトコルが設定されている既存のStorage VMに新しいLUNが作成されます。

新しいStorage VMを作成してFCプロトコルまたはiSCSIプロトコルを設定する必要がある場合は、を参照してください "FC 用に SVM を設定" または "SVM を iSCSI 用に設定"。

FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはdownになります。

LUNは、ホストではディスクデバイスとして表示されます。

> LUN の作成時、 Asymmetric Logical Unit Access （ ALUA ；非対称論理ユニットアクセス）は常に有効になります。ALUA の設定は変更できません。

イニシエータをホストするには、 SVM 内のすべての FC LIF で単一イニシエータゾーニングを使用する必要があります。

ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。

例 **2.** 手順

System Manager の略

ONTAP System Manager（9.7以降）でFCまたはiSCSIプロトコルを使用してSANホストにストレージを提供するためのLUNを作成します。

System Manager Classic（9.7以前で使用可能）を使用してこのタスクを完了するには、を参照してください "Red Hat Enterprise Linux 向けの iSCSI の設定"

手順

1. 該当するをインストールします "SANホストユーティリティ" ホスト。
2. System Manager で、 * Storage > LUNs * をクリックし、 * Add * をクリックします。
3. LUN の作成に必要な情報を入力します。
4. ONTAP のバージョンに応じて、「その他のオプション」をクリックすると、次のいずれかの操作を実行できます。

オプション	以降で使用できます
• 親ボリュームではなく LUN に QoS ポリシーを割り当て ◦ * その他のオプション > ストレージと最適化 * ◦ パフォーマンスサービスレベル * を選択します。 ◦ ボリューム全体ではなく個々の LUN に QoS ポリシーを適用するには、 * これらのパフォーマンス制限を各 LUN に適用 * を選択します。 デフォルトでは、パフォーマンス制限がボリュームレベルで適用されます。	ONTAP 9.10.1
• 既存の igroup を使用して新しいイニシエータグループを作成します ◦ * 「その他のオプション」 > 「ホスト情報」 * ◦ 既存のイニシエータグループを使用して新しいイニシエータグループを選択します * 。 ▪ 注：他の igroup を含む igroup の OS タイプは、作成後に変更することはできません。	ONTAP 9.9.1
• 概要を igroup またはホストイニシエータに追加します 概要は、 igroup またはホストイニシエータのエイリアスとして機能します。 ◦ * 「その他のオプション」 > 「ホスト情報」 *	ONTAP 9.9.1

• 既存のボリュームに LUN を作成します デフォルトでは、新しいボリュームに新しい LUN が作成されます。 ◦ * その他のオプション > LUN の追加 * ◦ ［ * グループ関連の LUN * ］ を選択します。	ONTAP 9.9.1
• QoS を無効にするか、カスタムの QoS ポリシーを選択します ◦ * その他のオプション > ストレージと最適化 * ◦ パフォーマンスサービスレベル * を選択します。 ▪ 注： ONTAP 9.9.1 以降では、カスタム QoS ポリシーを選択した場合、指定したローカル階層への手動配置を選択することもできます。	ONTAP 9.8

5. FC の場合は、 FC スイッチを WWPN でゾーニングします。イニシエータごとに 1 つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
6. ホストでLUNを検出します。

   VMware vSphereでは、Virtual Storage Console（VSC）を使用してLUNを検出して初期化します。

7. LUNを初期化し、必要に応じてファイルシステムを作成します。
8. ホストがLUNのデータの書き込みと読み取りを実行できることを確認します。

CLI の使用

ONTAP CLIでFCまたはiSCSIプロトコルを使用してSANホストにストレージを提供するためのLUNを作成します。

1. FCまたはiSCSIのライセンスがあることを確認します。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. FCまたはiSCSIのライセンスがない場合は、を使用します `license add` コマンドを実行します

```
license add -license-code <your_license_code>
```

3. SVMでプロトコルサービスを有効にします。

   - iSCSIの場合：*

     ```
     vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
     ```

   - FCの場合：*

     ```
     vserver fcp create -vserver <svm_name> -status-admin up
     ```

4. 各ノードにSVM用のLIFを2つ作成します。

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   ネットアップでは、データを提供するSVMごとに、ノードごとに少なくとも1つのiSCSIまたはFC LIFをサポートしています。ただし、冗長性を確保するには、ノードごとに2つのLIFが必要です。iSCSIの場合は、別 々 のイーサネットネットワークにあるノードごとに少なくとも2つのLIFを設定することを推奨します。

5. LIFが作成され、動作ステータスがになっていることを確認します `online`：

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. LUN を作成します。

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   LUN 名は 255 文字以内で、スペースは使用できません。

   > NVFAIL オプションは、ボリュームで LUN が作成されると、自動的に有効になります。

7. igroup を作成します。

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. LUN を igroup にマッピングします。

```
lun mapping create -vserver <svm__name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. LUN が正しく設定されていることを確認します。

```
lun show -vserver <svm_name>
```

10. 必要に応じて、 "ポートセットを作成してigroupにバインドします"。
11. ホストのマニュアルに記載されている手順に従って、特定のホストでブロックアクセスを有効にします。
12. Host Utilities を使用して FC または iSCSI マッピングを完了し、ホスト上の LUN を検出します。

関連情報

- "SAN の管理の概要"
- "ONTAP SAN ホスト構成"
- "System ManagerでSANイニシエータグループを表示および管理します"
- "ネットアップテクニカルレポート 4017 ：『ファイバチャネル SAN のベストプラクティス』"

NVMeプロビジョニング

NVMe の概要

NVMe （ Non-Volatile Memory Express ）プロトコルを使用して、 SAN 環境にストレージを提供できます。 NVMe プロトコルは、ソリッドステートストレージのパフォーマンスを高めるために最適化されています。

NVMe のストレージターゲットはネームスペースと呼ばれます。 NVMe ネームスペースは、論理ブロックにフォーマットして標準ブロックデバイスとしてホストに提供できる不揮発性ストレージの容量です。 FC および iSCSI で LUN をプロビジョニングして igroup にマッピングする場合と同様に、ネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングします。

NVMe ターゲットは、 FC スイッチを使用する標準的な FC インフラ、またはイーサネットスイッチとホスト側アダプタを使用する標準の TCP インフラを通じてネットワークに接続されます。

NVMeのサポートは、ONTAP のバージョンによって異なります。 を参照してください "NVMeのサポートと制限" を参照してください。

NVMe とは

Nonvolatile Memory Express （ NVMe ）プロトコルは、不揮発性ストレージメディアへのアクセスに使用する転送プロトコルです。

NVMe over Fabrics （ NVMeoF ）は仕様で定義された NVMe の拡張機能であり、 PCIe 以外の接続経由による NVMe ベースの通信を実現します。このインターフェイスを使用すると、外部のストレージエンクロージャをサーバに接続できます。

NVMe は、フラッシュテクノロジから高性能な永続的メモリテクノロジまで、不揮発性メモリを搭載したストレージデバイスに効率的にアクセスできるように設計されています。そのため、ハードディスクドライブ用に設計されたストレージプロトコルのような制限はありません。フラッシュデバイスとソリッドステートデバイス（ SSD ）は、不揮発性メモリ（ NVM ）の一種です。NVM では停電時にもデータが失われません。NVMe はそのメモリにアクセスするための手段です。

NVMe のメリットには、データ転送の速度、生産性、スループット、容量の向上があります。具体的には次のような特性があります。

- NVMe は最大 64 、 000 のキューを使用できるように設計されています。

  各キューには、最大 64 、 000 個のコマンドを同時に保持できます。

- NVMe は、複数のハードウェアベンダーとソフトウェアベンダーでサポートされています
- フラッシュテクノロジを使用すると NVMe の生産性が向上し、応答時間が短縮されます
- NVMe では、 SSD に送信される「検索」ごとに複数のデータ要求を行うことができます。

  NVMe は「要求」のデコードにかかる時間が短く、マルチスレッドプログラムでスレッドロックを必要としません。

- CPUレベルでのボトルネックを防止する機能をサポートし、システムの拡張に応じて並外れた拡張性を実現します。

NVMe ネームスペースについて

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（ NVM ）の容量です。ネームスペースは、 Storage Virtual Machine で NVMe プロトコルが設定されている場合に使用され、 FC および iSCSI プロトコルの LUN に相当します。

NVMe ホストには、 1 つ以上のネームスペースがプロビジョニングされて接続されます。各ネームスペースがさまざまなブロックサイズをサポートできます。

NVMe プロトコルは、複数のコントローラ経由でネームスペースへのアクセスを提供します。ほとんどのオペレーティングシステムでサポートされている NVMe ドライバを使用すると、 Solid State Drive （ SSD ；ソリッドステートドライブ）ネームスペースは標準ブロックデバイスとして表示され、そのままでファイルシステムとアプリケーションを導入できます。

ネームスペース ID （ NSID ）は、コントローラがネームスペースへのアクセスを提供するために使用する識別子です。ホストまたはホストグループに対して NSID を設定する場合は、ホストからボリュームへのアクセスも設定します。論理ブロックは一度に 1 つのホストグループにのみマッピングでき、同じホストグループに複数の NSID が割り当てられることはありません。

NVMe サブシステムについて

NVMe サブシステムには、 1 つ以上の NVMe コントローラ、ネームスペース、 NVM サブシステムポート、 NVM ストレージメディア、およびコントローラと NVM ストレージメディア間のインターフェイスが含まれます。NVMeネームスペースを作成すると、デフォルトではサブシステムにマッピングされません。新しいサブシステムまたは既存のサブシステムをマッピングすることもできます。

関連情報

- "NVMe ストレージをプロビジョニングする"
- "NVMe ネームスペースをサブシステムにマッピングする"
- "SANホストとクラウドクライアントを設定"

NVMeのライセンス要件

ONTAP 9.5 以降では、 NVMe 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。

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
```

NVMeの構成、サポート、制限事項

ONTAP 9.4以降では "Non-Volatile Memory Express（NVMe）" SAN環境ではプロトコルを使用できます。NVMe で使用される物理的なセットアップとゾーニングの手法は従来の FC ネットワークと同じですが、 NVMe は FC-SCSI と比べて帯域幅が広く、 IOPS が高く、レイテンシも低減されます。

NVMeのサポートと制限事項は、ONTAPのバージョン、プラットフォーム、構成によって異なります。具体的な構成の詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。サポートされる制限については、 "Hardware Universe"。

> クラスタあたりの最大ノード数は、Hardware Universeの*サポートされるプラットフォームの混在*で確認できます。

設定

- NVMe構成は、単一ファブリックまたはマルチファブリックを使用してセットアップできます。
- SAN をサポートする SVM ごとに管理 LIF を 1 つ設定する必要があります。
- 異機種混在の FC スイッチファブリックの使用は、組み込みのブレードスイッチ以外はサポートされていません。

  特定の例外については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

- カスケードファブリック、部分メッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、 FC スイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。

ファブリックは 1 つまたは複数のスイッチで構成できます。また、ストレージコントローラは複数のスイッチに接続することができます。

の機能

ONTAPのバージョンに応じて、次のNVMe機能がサポートされます。

ONTAP で開始しています…	NVMeのサポート
9.12.1:	NVMe/FCでの4ノードMetroCluster IP構成 • 9.12.1よりも前のNVMeでは、MetroCluster 構成はサポートされません。 • MetroCluster構成はNVMe/TCPではサポートされません。
9.10.1	ネームスペースのサイズを変更する
9.9.1	• ネームスペースとLUNは同じボリュームに共存できます。
9.8	• プロトコルの共存 SCSI、NAS、NVMeの各プロトコルを同じStorage Virtual Machine（SVM）に配置できます。 ONTAP 9.8より前のバージョンでは、SVMで使用できるプロトコルはNVMeだけです。 *
9.6	• ネームスペース用に512バイトブロック、4096バイトブロック デフォルト値は 4096 です。ホストオペレーティングシステムで 4096 バイトブロックがサポートされていない場合のみ、 512 を使用してください。 • ネームスペースがマッピングされたボリュームの移動
9.5	マルチパスHAペアのフェイルオーバー/ギブバック：

プロトコル

次のNVMeプロトコルがサポートされます。

プロトコル	ONTAP で開始しています…	許可者
TCP	9.10.1	デフォルト

FC	9.4	デフォルト

ONTAP 9.8以降では、同じStorage Virtual Machine（SVM）にSCSI、NAS、NVMeの各プロトコルを設定できます。
ONTAP 9.7以前では、SVMで使用できるプロトコルはNVMeのみです。

ネームスペース

NVMeネームスペースを使用する場合は、次の点に注意する必要があります。

- LUN のデータが失われた場合、ネームスペースからリストアすることはできません。また、その逆も同様です。
- ネームスペースのスペースギャランティはそれを含むボリュームのスペースギャランティと同じになります。
- 7-ModeのData ONTAPからのボリューム移行では、ネームスペースを作成できません。
- ネームスペースでは、次のものはサポートされません。
  - 名前変更中です
  - ボリューム間での移動
  - ボリューム間でのコピー
  - オンデマンドコピー

その他の制限事項

ONTAP の次の機能は、 **NVMe** 構成ではサポートされません。

- 同期
- Virtual Storage Console の略

次の説明は、 **ONTAP 9.4** を実行しているノードのみに該当します。

- NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
- NVMe LIF を作成する前に、 NVMe サービスを作成する必要があります。

関連情報

"最新SANのベストプラクティス"

NVMe用の**Storage VM**を設定する

ノードで NVMe プロトコルを使用する場合は、 SVM を NVMe 専用に設定する必要があります。

作業を開始する前に

FC アダプタまたはイーサネットアダプタで NVMe がサポートされている必要があります。サポートされるアダプタの一覧については、を参照してください "NetApp Hardware Universe の略"。

例 **3.** 手順

System Manager の略

ONTAP System Manager（9.7以降）でNVMe用のStorage VMを設定します。

新しい**Storage VM**に**NVMe**を設定してください	既存の**Storage VM**に**NVMe**を設定
1. System Managerで、* Storage > Storage VM* をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* nvme」を選択します。 4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。	1. System Manager で、 * Storage > Storage VM* をクリックします。 2. 設定するStorage VMをクリックします。 3. [設定]タブをクリックし、をクリックします をクリックします。 4. 「* NVMe/FCを有効にする」または「* NVMe/FCを有効にする」および「*保存」を選択します。

CLI の使用

ONTAP CLIを使用して、NVMe用のStorage VMを設定します。

1. 既存の SVM を使用しない場合は、作成します。

```
vserver create -vserver <SVM_name>
```

   a. SVM が作成されたことを確認します。

```
vserver show
```

2. クラスタに NVMe または TCP 対応アダプタがインストールされていることを確認します。

   NVMeの場合：

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   TCPの場合：

```
network port show
```

3. ONTAP 9.7 以前を実行している場合は、 SVM からすべてのプロトコルを削除します。

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

ONTAP 9.8 以降では、 NVMe を追加するときに他のプロトコルを削除する必要はありません。

4. SVM に NVMe プロトコルを追加します。

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. ONTAP 9.7 以前を実行している場合は、 SVM で許可されているプロトコルが NVMe だけであることを確認します。

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

に表示されるプロトコルはNVMeのみです `allowed protocols` 列（Column）：

6. NVMe サービスを作成します。

```
vserver nvme create -vserver <SVM_name>
```

7. NVMe サービスが作成されたことを確認します。

```
vserver nvme show -vserver <SVM_name>
```

。 `Administrative Status` SVMのがと表示されている必要があります `up`。

8. NVMe/FC LIF を作成します。
   - ONTAP 9.9.1以前の場合、FC：

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -role data -data-protocol fc-nvme -home-node <home_node> -home
     -port <home_port>
     ```

   - ONTAP 9.10.1以降、FCまたはTCPの場合：

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -service-policy <default-data-nvme-tcp | default-data-nvme-fc>
     -data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
     -home-port <home_port> -status-admin up -failover-policy disabled
     -firewall-policy data -auto-revert false -failover-group
     <failover_group> -is-dns-update-enabled false
     ```

9. HA パートナーノードに NVMe/FC LIF を作成します。

- ONTAP 9.9.1以前の場合、FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- ONTAP 9.10.1以降、FCまたはTCPの場合：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. NVMe/FC LIF が作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

11. LIF と同じノードにボリュームを作成します。

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

自動効率化ポリシーに関する警告メッセージが表示された場合は無視してかまいません。

NVMe ストレージをプロビジョニングする

次の手順に従って、既存のStorage VMでNVMe対応ホスト用のネームスペースを作成し、ストレージをプロビジョニングします。

ONTAP 9.8 以降では、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。

作業を開始する前に

Storage VM が NVMe 用に設定され、 FC または TCP 転送がすでにセットアップされている必要があります。

System Manager の略

ONTAP System Manager（9.7以降）を使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

手順

1. System Manager で、 * Storage > NVMe 名前空間 * をクリックし、 * Add * をクリックします。

   新しいサブシステムを作成する必要がある場合は、 * その他のオプション * をクリックします。

2. ONTAP 9.8 以降を実行していて、 QoS を無効にする場合やカスタムの QoS ポリシーを選択する場合は、「その他のオプション」をクリックし、「 * ストレージおよび最適化 * 」で「 * パフォーマンスサービスレベル * 」を選択します。
3. FC スイッチを WWPN でゾーニングイニシエータごとに 1 つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。
4. ホストで、新しいネームスペースを検出します。
5. ネームスペースを初期化し、ファイルシステムでフォーマットします。
6. ホストがネームスペースに対してデータの書き込みと読み取りを実行できることを確認します。

CLI の使用

ONTAP のCLIを使用して、NVMeプロトコルを使用してストレージを提供するネームスペースを作成します。

この手順 は、NVMeプロトコル用に設定済みの既存のStorage VMにNVMeネームスペースとサブシステムを作成し、ネームスペースをサブシステムにマッピングしてホストシステムからのデータアクセスを許可します。

NVMe用にStorage VMを設定する必要がある場合は、を参照してください "NVMe 用に SVM を設定します"。

手順

1. SVM が NVMe 用に設定されていることを確認します。

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` がの下に表示されます `allowed-protocols` 列（Column）：

2. NVMe ネームスペースを作成します。

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. NVMe サブシステムを作成します。

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMe サブシステムの名前では大文字と小文字が区別されます。1~96文字で指定する必要があります。特殊文字を使用できます。

4. サブシステムが作成されたことを確認します。

```
vserver nvme subsystem show -vserver <svm_name>
```

。 `nvme` の下にサブシステムが表示されます `Subsystem` 列（Column）：

5. ホストから NQN を取得します。
6. ホストの NQN をサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

ネームスペースは、 1 つのサブシステムにのみマッピングできます。

8. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <svm_name> -instance
```

サブシステムがと表示されます `Attached subsystem`。

NVMe ネームスペースをサブシステムにマッピングする

NVMeネームスペースをサブシステムにマッピングすると、ホストからのデータアクセスが可能になります。 NVMeネームスペースは、ストレージのプロビジョニング時にサブシステムにマッピングすることも、ストレージのプロビジョニング後にマッピングすることもできます。

ONTAP 9.14.1以降では、特定のホストに対するリソース割り当てに優先順位を付けることができます。デフォルトでは、NVMeサブシステムに追加されたホストには標準優先度が与えられます。ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。 高い優先

度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

> ONTAP 9.13.1以前でサブシステムに追加されたホストを高い優先度で指定するには、次の手順を実行します。 ホスト優先度の変更。

作業を開始する前に

ネームスペースとサブシステムはすでに作成されている必要があります。ネームスペースとサブシステムを作成する必要がある場合は、を参照してください "NVMe ストレージをプロビジョニングする"。

手順

1. ホストから NQN を取得します。
2. ホストの NQN をサブシステムに追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

   ホストのデフォルト優先度をregularからhighに変更する場合は、 `-priority high` オプションこのオプションは、ONTAP 9.14.1以降で使用できます。

3. ネームスペースをサブシステムにマッピングします。

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

   ネームスペースは、 1 つのサブシステムにのみマッピングできます。

4. ネームスペースがサブシステムにマッピングされていることを確認します。

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

   サブシステムがと表示されます `Attached subsystem`。

LUNを管理します

LUN QoS ポリシーグループを編集します

ONTAP 9.10.1 以降の System Manager を使用して、複数の LUN のサービス品質（ QoS ）ポリシーを同時に割り当てたり削除したりできます。

> QoSポリシーがボリュームレベルで割り当てられている場合は、ボリュームレベルで変更する必要があります。 QoS ポリシーは、もともと LUN レベルで割り当てられていた場合にのみ、LUN レベルで編集できます。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 編集する LUN を選択します。

   一度に複数の LUN を編集する場合は、その LUN が同じ Storage Virtual Machine （ SVM ）に属している必要があります。同じ SVM に属していない LUN を選択した場合は、 QoS ポリシーグループを編集するオプションは表示されません。

3. [* その他 *] をクリックし、 [* QoS ポリシーグループの編集 *] を選択します。

LUNをネームスペースに変換します

ONTAP 9.11.1以降では、ONTAP CLIを使用して、既存のLUNをNVMeネームスペースにインプレース変換できます。

必要なもの

- 指定したLUNには、igroupにマッピングされている既存のLUNを含めることはできません。
- MetroCluster が設定されたSVM内やSM-BC関係にあるLUNは使用できません。
- LUNをプロトコルエンドポイントにしたり、プロトコルエンドポイントにバインドしたりすることはできません。
- LUNにゼロ以外のプレフィックスやサフィックスストリームを含めることはできません。
- LUNをSnapshotの一部にしたり、SnapMirror関係のデスティネーション側に読み取り専用LUNとして配置したりすることはできません。

ステップ

1. LUNをNVMeネームスペースに変換します。

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

LUN をオフラインにします

ONTAP 9.10.1 以降の場合、 System Manager を使用して LUN をオフラインにできます。ONTAP 9.10.1 より前のバージョンでは、 ONTAP CLI を使用して LUN をオフラインにする必要があります。

System Manager の略

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 1 つまたは複数の LUN をオフラインにします

実行する処理	操作
単一の LUN をオフラインにします	LUN 名の横にあるをクリックします ⋮ をクリックし、 * オフラインにする * を選択します。
複数の LUN をオフラインにします	1. オフラインにする LUN を選択します。 2. 「 * 詳細」をクリックし、「 * オフラインにする * 」を選択します。

CLI の使用

CLI を使用する場合、一度にオフラインにできる LUN は 1 つだけです。

ステップ

1. LUN をオフラインにします。

```
lun offline <lun_name> -vserver <SVM_name>
```

LUNのサイズを変更します

LUNのサイズは増やすことも減らすこともできます。

Solaris LUN のサイズは変更できません。

LUN のサイズを拡張する

LUN の拡張後のサイズは、 ONTAP のバージョンによって異なります。

ONTAPバージョン	LUN の最大サイズ
ONTAP 9.12.1P2以降	AFF、FAS、ASAプラットフォームの場合は128TB
ONTAP 9.8以降	• オールフラッシュSANアレイ（ASA）プラットフォームの場合は128TB • ASA以外のプラットフォームの場合は16TB
ONTAP 9.5、9.6、9.7	16TB

ONTAP 9.4 以前	元のLUNサイズの10倍ですが、最大LUNサイズである16TBを超えることはありません。 たとえば、100GBで作成したLUNは1、000GBまでしか拡張できません。 LUNの実際の最大サイズが正確に16TBであるとは限りません。 ONTAP では、制限値の端数が切り捨てられます。

サイズを拡張するときに、 LUN をオフラインにする必要はありません。ただし、サイズを拡張したあとでホストがサイズの変更を認識するには、ホスト上の LUN を再スキャンする必要があります。

のコマンドリファレンスページを参照してください `lun resize` コマンドを使用してLUNのサイズ変更の詳細を確認してください。

例 **4.** 手順

System Manager の略

ONTAP System Managerを使用してLUNのサイズを拡張する（9.7以降）。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. をクリックします ⋮ をクリックし、 * Edit * を選択します。
3. Storage and Optimization では、**LUN**のサイズが拡張され、 Save *が表示されます。

CLI の使用

ONTAP CLIを使用してLUNのサイズを拡張する。

1. LUN のサイズを拡張します。

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. 拡張した LUN のサイズを確認します。

```
lun show -vserver <SVM_name_>
```

ONTAP の処理では、 LUN の実際の最大サイズが端数を切り捨てられるため、想定値よりも少し小さくなります。また、 LUN の実際のサイズは、 LUN の OS タイプによって多少異なります。サイズの正確な値を取得するには、 advanced モードで次のコマンドを実行します。

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. ホスト上の LUN を再スキャンします。
2. ホストのマニュアルに従って、新しく作成した LUN のサイズをホストファイルシステムに認識させます。

LUN のサイズを縮小します

LUN のサイズを縮小する前に、ホストが LUN データを含むブロックを小さい LUN サイズの境界に移行する必要があります。LUNデータを含むブロックを切り捨てずにLUNを適切に縮小するには、SnapCenterなどのツールを使用する必要があります。LUN のサイズを手動で縮小することは推奨されません。

LUN のサイズを縮小すると、サイズが縮小されたことが ONTAP からイニシエータに自動的に通知されます。ただし、ホストが新しい LUN サイズを認識するには、ホストで追加の手順が必要になる場合があります。ホストのファイル構造のサイズの縮小に固有の情報については、ホストのマニュアルを参照してください。

LUN を移動します

Storage Virtual Machine （ SVM ）内のボリューム間で LUN を移動できますが、 SVM 間で LUN を移動することはできません。SVM 内のボリューム間で移動される LUN はただちに移動され、接続が失われることはありません。

必要なもの

LUNでSelective LUN Map（SLM；選択的LUNマップ）を使用している場合は、 "SLMレポートノードリストの変更" LUNを移動する前に、デスティネーションノードとそのHAパートナーを追加します。

このタスクについて

重複排除、圧縮、コンパクションなどの Storage Efficiency 機能は、 LUN の移動時には保持されません。これらは、 LUN の移動の完了後に再適用する必要があります。

Snapshot コピーによるデータ保護はボリュームレベルで行われます。そのため、移動した LUN にはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用の Snapshot コピーが確立されていない場合、 LUN の Snapshot コピーは作成されません。また、 LUN のすべての Snapshot コピーは、これらの Snapshot コピーが削除されないかぎり、元のボリュームに保持されます。

次のボリュームに LUN を移動することはできません。

- SnapMirror デスティネーションボリューム
- SVM ルートボリューム

次のタイプの LUN は移動できません。

- ファイルから作成された LUN
- NVFail 状態の LUN
- 負荷共有関係にある LUN
- プロトコルエンドポイントクラスの LUN

サイズが 1TB 以上で os_type が Solaris の LUN では、 LUN の移動時にホストでタイムアウトが発生する場合があります。このタイプの LUN では、移動を開始する前に LUN をアンマウントする必要があります。

例 **5.** 手順

System Manager の略

ONTAP System Manager（9.7以降）を搭載したLUNを移動します。

ONTAP 9.10.1 以降では、単一の LUN を移動するときに System Manager で新しいボリュームを作成できます。 ONTAP 9.8 および 9.9.8.1 では、 LUN の移動を開始する前に、 LUN の移動先のボリュームが存在している必要があります。

手順

1. System Manager で、 * Storage > LUNs * をクリックします。
2. 移動するLUNを右クリックし、 ⋮ をクリックし、 * LUN の移動 * を選択します。

   ONTAP 9.10.1 では、 LUN を既存のボリューム * または新しいボリューム * に移動するように選択します。

   新しいボリュームを作成する場合は、ボリュームの仕様を指定します。

3. [移動（ Move ）] をクリックします。

CLI の使用

ONTAP CLIを使用してLUNを移動します。

1. LUN を移動します。

   ```
   lun move start
   ```

   ごく短時間、移動した LUN が元のボリュームと移動後のボリュームの両方に表示されます。これは移動が完了するまでの一時的な状態で、想定内の動作です。

2. 移動のステータスを追跡し、正常に完了したことを確認します。

   ```
   lun move show
   ```

関連情報

- "選択的 LUN マップ"

LUN を削除します

不要になった LUN は Storage Virtual Machine （ SVM ）から削除できます。

必要なもの

LUN を削除する前に、その igroup から LUN のマッピングを解除する必要があります。

手順

1. アプリケーションやホストが LUN を使用していないことを確認します。
2. igroup から LUN のマッピングを解除します。

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. LUNを削除します。

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. LUNが削除されたことを確認します。

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

LUNをコピーする前に理解しておくべきこと

LUNをコピーする前に、次の点に注意してください。

クラスタ管理者は、を使用して、クラスタ内のStorage Virtual Machine（SVM）間でLUNをコピーできます `lun copy` コマンドを実行しますクラスタ管理者は、を使用してStorage Virtual Machine（SVM）ピア関係を確立する必要があります `vserver peer create` SVM間のLUNコピー処理を実行する前のコマンド。ソースボリューム内に SIS クローン用の十分なスペースが必要です。

Snapshotコピー内のLUNをのソースLUNとして使用できます `lun copy` コマンドを実行しますを使用してLUNをコピーする場合 `lun copy` コマンドを実行すると、LUNコピーの読み取りと書き込みがすぐに可能になります。LUN コピーの作成によってソース LUN が変更されることはありません。ソース LUN と LUN コピーは、 LUN シリアル番号の異なる一意の LUN として存在します。ソース LUN に対する変更は LUN コピーに反映されず、 LUN コピーに対する変更はソース LUN に反映されません。ソース LUN の LUN マッピングは新しい LUN にコピーされないため、 LUN コピーをマッピングする必要があります。

Snapshot コピーによるデータ保護はボリュームレベルで行われます。そのため、ソース LUN のボリュームとは異なるボリュームに LUN をコピーする場合、デスティネーション LUN にはデスティネーションボリュームのデータ保護形式が適用されます。デスティネーションボリューム用の Snapshot コピーが確立されていない場合、 LUN コピーの Snapshot コピーは作成されません。

LUN のコピーはノンストップオペレーションです。

次の種類の LUN はコピーできません。

- ファイルから作成された LUN
- NVFAIL 状態の LUN
- 負荷共有関係にある LUN
- プロトコルエンドポイントクラスの LUN

LUN の設定済みスペースと使用済みスペースを確認します

LUN の設定済みスペースと実際に使用されているスペースを把握しておくと、スペース再生時に再生可能なスペースの量、データを含むリザーブスペースの量、および LUN の設定済みの合計サイズと実際に使用されているサイズを特定するのに役立ちます。

ステップ

1. LUN の設定済みスペースと実際に使用されているスペースを表示します。

   ```
   lun show
   ```

   次の例は、 vs3 という Storage Virtual Machine （ SVM ）内の LUN の設定済みスペースと実際に使用されているスペースを示しています。

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- -----------------       ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

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

SCSIシンプロビジョニングがホストでサポートされている場合は、ONTAPで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することができます。 スペース割り当てを有効にすると、ボリュームのスペースが不足し、ボリューム内のLUNが書き込みを受け付けられなくなったときに、ONTAPからホストに通知されます。ONTAPは、ホストでデータが削除されたときにも自動的にスペースを再生します。

SCSI シンプロビジョニングをサポートしないホスト上では、 LUN が含まれているボリューム内のスペースが不足し自動拡張できなくなったときに、 ONTAP によってその LUN はオフラインになります。SCSIシンプロビジョニングをサポートするホストでは、スペースが不足してもONTAPはLUNをオフラインにしません。LUN は読み取り専用モードでオンライン状態を維持し、 LUN が書き込みを受け付けられなくなったことがホストに通知されます。

また、SCSIシンプロビジョニングをサポートするホストでデータが削除されると、ホスト側のスペース管理

によって、ホストファイルシステムで削除されたデータのブロックが識別され、自動的に1つ以上の `SCSI UNMAP` ストレージシステム上の対応するブロックを解放するコマンド。

作業を開始する前に

スペース割り当てを有効にするには、SCSIシンプロビジョニングがホストでサポートされている必要があります。SCSIシンプロビジョニングは、SCSI SBC-3標準で定義されている論理ブロックプロビジョニングを使用します。この標準をサポートするホストだけが、 ONTAP の SCSI シンプロビジョニングを使用できます。

現在、スペース割り当てを有効にした場合の SCSI シンプロビジョニングに対応しているホストは次のとおりです。

- Citrix XenServer 6.5以降
- ESXi 5.0以降
- Oracle Linux 6.2 UEKカーネル以降
- RHEL 6.2以降
- SLES11以降
- Solaris 11.1以降
- Windows の場合

このタスクについて

デフォルトでは、スペース割り当てはすべてのLUNに対して無効になっています。LUNをオフラインにしてスペース割り当てを有効にしてから、ホストがスペース割り当てが有効になったことを認識するには、ホストで検出を実行する必要があります。

手順

1. LUNをオフラインにします。

```
lun modify -vserver vserver_name -volume volume_name -lun lun_name
-state offline
```

2. スペース割り当てを有効にします。

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-space-allocation enabled
```

3. スペース割り当てが有効になっていることを確認します。

```
lun show -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-fields space-allocation
```

4. LUN をオンラインにします。

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-state online
```

5. ホストですべてのディスクを再スキャンして、が変更されたことを確認します `-space-allocation` オプションが正しく検出されました。

LUN に対する **I/O** パフォーマンスは、ストレージ **QoS** を使用して制御および監視できます

LUN への入出力（ I/O ）パフォーマンスは、 LUN をストレージ QoS ポリシーグループに割り当てることによって制御できます。I/O パフォーマンスを制御することで、ワークロードが特定のパフォーマンス目標を達成できるようにしたり、他のワークロードに悪影響を与えるワークロードを抑制したりできます。

このタスクについて

ポリシーグループは最大スループット制限（ 100MB/s など）を適用します。ポリシーグループは最大スループットを指定せずに作成することもでき、ワークロードの制御に先立ってパフォーマンスを監視できます。

FlexVol および LUN が含まれている Storage Virtual Machine （ SVM ）をポリシーグループに割り当てることもできます。

ポリシーグループへの LUN の割り当てについては、次の要件に注意してください。

- LUN は、ポリシーグループが属する SVM に含まれている必要があります。

  SVM は、ポリシーグループを作成するときに指定します。

- LUN をポリシーグループに割り当てた場合、その LUN を含むボリュームまたは SVM をポリシーグループに割り当てることはできなくなります。

ストレージ QoS の使用方法の詳細については、を参照してください "システムアドミニストレーションリファレンス"。

手順

1. を使用します `qos policy-group create` コマンドを使用してポリシーグループを作成します。
2. を使用します `lun create` コマンドまたはを実行します `lun modify` コマンドにを指定します `-qos -policy-group` LUNをポリシーグループに割り当てるためのパラメータ。
3. を使用します `qos statistics` パフォーマンスデータを表示するためのコマンド。
4. 必要に応じて、を使用します `qos policy-group modify` コマンドを使用してポリシーグループの最大スループット制限を調整します。

LUN を効果的に監視するためのツール

LUN を効果的に監視し、スペース不足になるのを防ぐためのツールが用意されています。

- Active IQ Unified Manager は、環境内のすべてのクラスタのすべてのストレージを管理するための無償ツールです。

- System Manager は、 ONTAP に組み込まれているグラフィカルユーザインターフェイスです。クラスタレベルで必要なストレージを手動で管理できます。
- OnCommand Insight を使用すると、ストレージインフラの状況を一元的に確認できます。また、自動監視やアラートの機能、および LUN 、ボリューム、アグリゲートでストレージスペース不足が発生したときにレポートする機能を設定できます。

移行した **LUN** の機能と制限

SAN 環境では、 7-Mode ボリュームを ONTAP に移行する際にサービスの中断が必要です。移行を完了するには、ホストをシャットダウンする必要があります。移行後は、ホスト構成を更新してから、 ONTAP でデータの提供を開始する必要があります

ホストをシャットダウンできる時間帯にメンテナンスのスケジュールを設定して、移行を完了する必要があります。

Data ONTAP 7-Mode から ONTAP に移行された LUN には、 LUN の管理方法に影響を及ぼす特定の機能と制限があります。

移行した LUN では、次の操作を実行できます。

- を使用してLUNを表示します `lun show` コマンドを実行します
- を使用して、7-Modeボリュームから移行したLUNのインベントリを表示します `transition 7-mode show` コマンドを実行します
- 7-Mode Snapshot コピーからボリュームをリストアします

  ボリュームをリストアすると、 Snapshot コピーにキャプチャされたすべての LUN が移行されます

- を使用して、7-Mode Snapshotコピーから単一のLUNをリストアします `snapshot restore-file` コマンドを実行します
- 7-Mode Snapshot コピー内の LUN のクローンを作成します
- 7-Mode Snapshot コピーにキャプチャされた LUN から特定の範囲のブロックをリストアする
- 7-Mode Snapshot コピーを使用して、ボリュームの FlexClone を作成します

移行した LUN では、次の操作を実行することはできません。

- ボリューム内にキャプチャされた Snapshot コピーでバックアップされた LUN クローンにアクセスします

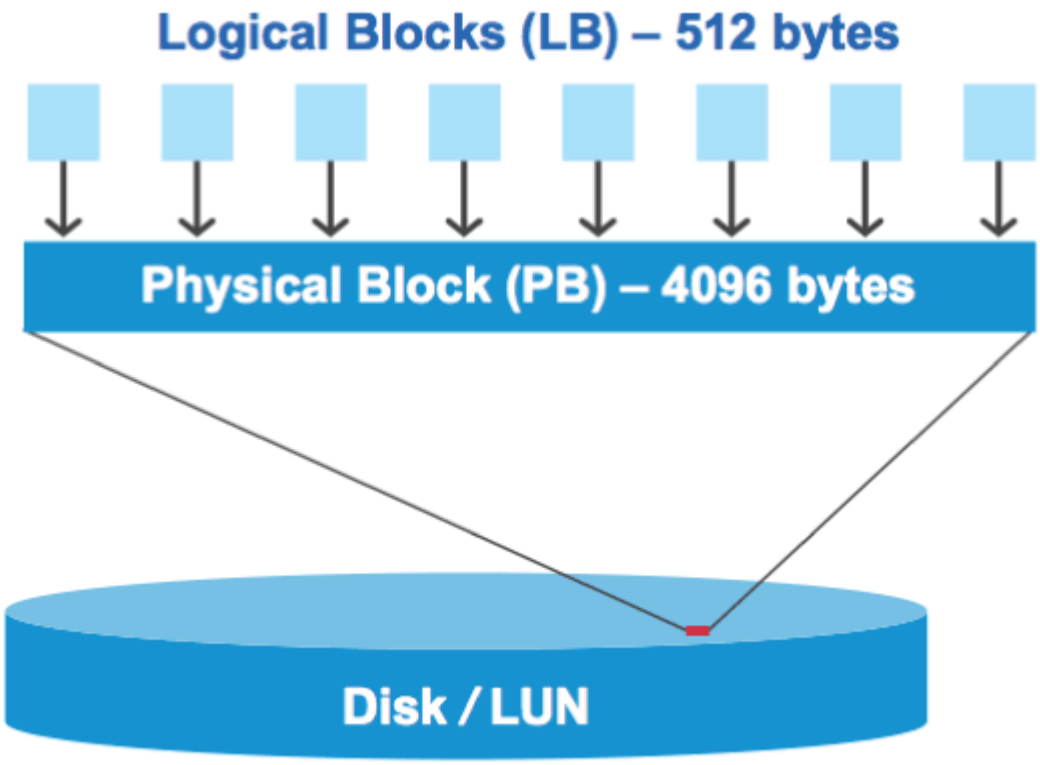
関連情報

"コピーベースの移行"

適切にアライメントされた **LUN** における **I/O** のミスアライメントの概要

ONTAP では、適切にアライメントされた LUN における I/O のミスアライメントが報告されることがあります。一般に、このようなミスアライメントの警告は、 LUN が適切にプロビジョニングされていて、パーティションテーブルが適正であることに確信があれば無視してかまいません。

LUN とハードディスクはどちらもストレージをブロックとして提供します。ホスト上のディスクのブロックサイズは 512 バイトなので、 LUN はそのサイズのブロックをホストに提供しますが、実際はよりサイズの大きい 4KB のブロックを使用してデータを格納します。ホストで使用される 512 バイトのデータブロックは論理ブロックと呼ばれ、LUN がデータの格納に使用する 4KB のデータブロックは物理ブロックと呼ばれます。つまり、 4KB の各物理ブロックに 512 バイトの論理ブロックが 8 個あります。



ホストオペレーティングシステムは、任意の論理ブロックで読み取りまたは書き込みの I/O 処理を開始できます。I/O 処理がアライメントされているとみなされるのは、 I/O 処理が物理ブロック内の最初の論理ブロックで開始される場合のみです。I/O 処理が物理ブロックの最初の論理ブロック以外のブロックで開始される場合は、 I/O がミスアライメントされているとみなされます。ONTAP は、 LUN におけるミスアライメントを自動検出して報告します。ただし、ミスアライメント I/O が検出されたからといって、 LUN もミスアライメントされているとは限りません。適切にアライメントされた LUN でも、ミスアライメント I/O が報告される場合があります。

さらに調査が必要な場合は、Knowledge Baseの記事を参照してください "LUNのミスアライメントされたIOを特定する方法"

アライメントの問題を修正するためのツールの詳細については、 + を参照してください

- "Windows Unified Host Utilities 7.1"
- "Virtual Storage Console for VMware vSphere インストレーションアドミニストレーションガイド"

LUN の OS タイプを使用して I/O アライメントを実行する

ONTAP 9.7以前では、推奨されるONTAP LUNを使用する必要があります。 `ostype` OSパーティショニングスキームとのI/Oアライメントを実現するために、オペレーティングシステムに最も近い値。

ホスト OS で採用されるパーティションスキームは I/O のミスアライメントの大きな要因です。一部のONTAP LUN `ostype` 値は、ホストオペレーティングシステムがアライメントするデフォルトのパーティシ

ョニングスキームを有効にするために、「プレフィックス」と呼ばれる特別なオフセットを使用します。

> 場合によっては、 I/O アライメントを実行するためにカスタムパーティションテーブルが必要になることがあります。ただし、の場合 `ostype` "`prefix`"の値がより大きい値 `0`カスタムパーティションを使用すると、ミスアライメントI/Oが発生する可能性があります。

ONTAP 9.7以前でプロビジョニングされたLUNの詳細については、技術情報アーティクルを参照してください。 "LUNでアライメントされていないIOを特定する方法"。

> ONTAP 9.8以降でプロビジョニングされる新しいLUNには、すべてのLUN OSタイプでプレフィックスとサフィックスサイズが0に設定されます。I/Oは、デフォルトでサポートされるホストOSとアライメントされている必要があります。

Linux 固有の I/O アライメントに関する注意事項があります

Linux ディストリビューションでは、データベース、各種ボリュームマネージャ、ファイルシステム用の raw デバイスなど、さまざまな方法で LUN を使用できます。raw デバイスまたは論理ボリューム内の物理ボリュームとして使用する場合、 LUN にパーティションを作成する必要はありません。

RHEL 5 以前および SLES 10 以前の場合、ボリュームマネージャを使用せずに LUN を使用する場合は、LUN をパーティショニングして、アライメントされたオフセットから始まる 1 つのパーティションを設定する必要があります。これは、 8 つの論理ブロックの偶数の倍数であるセクターです。

Solaris LUN 固有の I/O アライメントに関する注意事項があります

を使用するかどうかを決定する際には、さまざまな要因を考慮する必要があります `solaris` ostypeまたは `solaris_efi` ostype

を参照してください "Solaris Host Utilities Installation and Administration Guide" を参照してください。

ESX ブート LUN はミスアライメントとしてレポートされます

ESX ブート LUN として使用される LUN は通常、ミスアライメントとして ONTAP から報告されます。ESX は、ブート LUN 上に複数のパーティションを作成するため、アライメントが非常に困難です。ミスアライメント I/O の合計容量は小さいため、ミスアライメントされた ESX ブート LUN は通常、パフォーマンス上の問題を生じません。VMwareでLUNが正しくプロビジョニングされていることを前提とします `ostype`アクションは必要ありません。

関連情報

"VMware vSphere 、その他の仮想環境、およびネットアップストレージシステム用のゲスト VM ファイルシステムのパーティションとディスクのアライメント"

LUN がオフラインになった場合の問題への対処方法

書き込みに使用できるスペースがない場合、 LUN はデータの整合性を保持するためにオフラインになります。LUN がスペース不足やオフラインになる原因はさまざまですが、いくつかの方法で問題に対処できます。

状況	可能です
アグリゲートがいっぱいです	• ディスクを追加します。 • を使用します `volume modify` 使用可能なスペースがあるボリュームを縮小するコマンド。 • 使用可能なスペースがあるスペースギャランティボリュームがある場合は、ボリュームのスペースギャランティをに変更します `none` を使用 `volume modify` コマンドを実行します
ボリュームがフルの状態であるが、包含アグリゲートに利用可能なスペースがある	• スペースギャランティボリュームの場合は、を使用します `volume modify` コマンドを使用してボリュームのサイズを拡張します。 • シンプロビジョニングボリュームの場合は、を使用します `volume modify` コマンドを使用して、ボリュームの最大サイズを拡張します。 ボリュームの自動拡張が有効になっていない場合は、を使用します `volume modify -autogrow -mode` 有効にします。 • を使用して、Snapshotコピーを手動で削除します `volume snapshot delete` コマンドを入力するか、を使用します `volume snapshot autodelete modify` Snapshotコピーを自動的に削除するコマンド。

関連情報

"ディスクとローカル階層（アグリゲート）の管理"

"論理ストレージ管理"

ホストで **iSCSI LUN** が表示されない場合のトラブルシューティング

ホストでは、 iSCSI LUN がローカルディスクとして表示されます。ストレージシステムの LUN をホストがディスクとして使用できない場合は、構成設定を確認してください。

設定	対処方法：
ケーブル配線	ホストとストレージシステムの間のケーブルが適切に接続されていることを確認します。

設定	対処方法：
ネットワーク接続	ホストとストレージシステムの間に TCP / IP 接続が確立されていることを確認します。 • ストレージシステムのコマンドラインから、 iSCSI に使用されているホストインターフェイスを ping します。 `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • ホストのコマンドラインから、 iSCSI に使用されているストレージシステムインターフェイスを ping します。 `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*
システム要件	各構成コンポーネントが、認定された製品であることを確認します。ホスト OS のサービスパックレベル、イニシエータバージョン、 ONTAP バージョンなどのシステム要件を満たしていることも確認してください。Interoperability Matrix に最新のシステム要件が記載されています。
ジャンボフレーム	構成でジャンボフレームを使用している場合は、ネットワークパス内のすべてのデバイスでジャンボフレームが有効になっていることを確認します。ホストイーサネット NIC 、ストレージシステム、およびすべてのスイッチです。
iSCSI サービスのステータス	iSCSI サービスのライセンスがあり、ストレージシステムで開始されていることを確認します。
イニシエータログイン	イニシエータがストレージシステムにログインしていることを確認します。状況に応じて `iscsi initiator show` コマンド出力にログインしているイニシエータが表示されないため、ホストのイニシエータ設定をチェックしてください。イニシエータのターゲットとしてストレージシステムが設定されていることも確認してください。
iSCSI ノード名（ IQN ）	正しいイニシエータのノード名を igroup 設定で使用していることを確認します。イニシエータのツールおよびコマンドをホストで使用し、イニシエータのノード名を表示できます。igroup およびホストで設定したイニシエータのノード名は、互いに一致する必要があります。
LUN マッピング	LUN が igroup にマッピングされていることを確認します。ストレージ・システムのコンソールで、次のいずれかのコマンドを使用できます。 • `lun mapping show` すべてのLUN、およびLUNがマッピングされているigroupを表示します。 • `lun mapping show -igroup` 特定のigroupにマッピングされているLUNを表示します。

設定	対処方法：
iSCSI LIF が有効になります	iSCSI 論理インターフェイスが有効になっていることを確認する。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

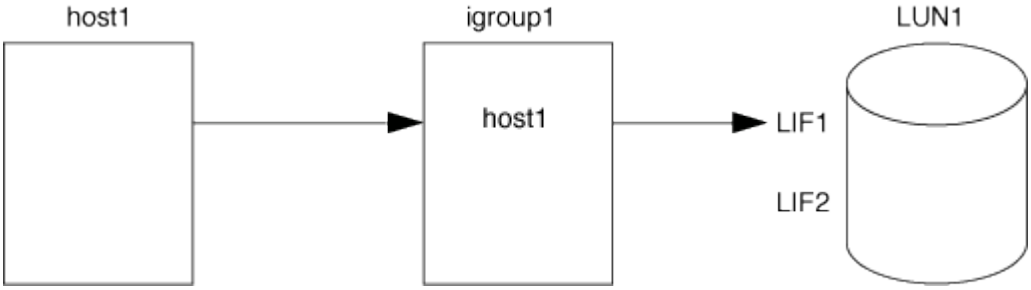
igroupとポートセットを管理します

ポートセットと**igroup**によって**LUN**アクセスを制限する方法

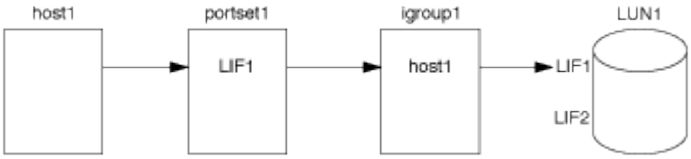
Selective LUN Map（SLM；選択的なLUNマップ）に加えて、igroupおよびポートセットを使用してLUNへのアクセスを制限することもできます。

ポートセットとSLMを併用すると、特定のターゲットのアクセスを特定のイニシエータのみに制限できます。SLM とポートセットを併用する場合、 LUN には、その LUN を所有するノードおよびノードの HA パートナーのポートセットに含まれる一連の LIF 経由でアクセス可能になります。

次の例で、initiator1にはポートセットがありません。ポートセットがない場合、initiator1はLIF1とLIF2の両方を経由してLUN1にアクセスできます。



ポートセットを使用すると、LUN1へのアクセスを制限できます。次の例では、 initiator1 は LIF1 経由でのみ LUN1 にアクセスできます。ただし、LIF2はportset1に含まれないため、LIF2経由でLUN1にアクセスすることはできません。



関連情報

- 選択的 LUN マップ
- ポートセットを作成して igroup にバインドします

SANイニシエータと**igroup**を表示および管理します

System Managerを使用して、イニシエータグループ（igroup）とイニシエータを表示および管理できます。

このタスクについて

- イニシエータグループは、ストレージシステム上の特定のLUNにアクセスできるホストを識別します。
- イニシエータグループとイニシエータグループは、作成後に編集または削除することもできます。
- SANイニシエータグループとイニシエータを管理するには、次のタスクを実行します。
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

SANイニシエータグループを表示および管理します

System Managerを使用して、イニシエータグループ（igroup）のリストを表示できます。 リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストが表示されます。 リストが大きい場合は、ページの右下隅にあるページ番号をクリックすると、リストの追加ページを表示できます。

   列には、igroupに関するさまざまな情報が表示されます。 9.11.1以降では、igroupの接続ステータスも表示されます。 ステータスアラートにカーソルを合わせると詳細が表示されます。

2. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。
   - * 検索 *
   - *ダウンロード*リスト。
   - *リストの*または*隠す*列を表示します。
   - *リスト内のデータをフィルタリングします。
3. リストから操作を実行できます。
   - をクリックします + Add をクリックしてigroupを追加します。
   - igroup名をクリックすると、そのigroupの詳細が表示されます。* Overview *ページが表示されます。

     概要*ページでは、igroupに関連付けられているLUNを確認できます。また、処理を開始してLUNの作成やLUNのマッピングを行うこともできます。「*すべてのSANイニシエータ」をクリックしてメインリストに戻ります。

   - igroupにカーソルを合わせ、をクリックします ⋮ をクリックしてigroupを編集または削除します。
   - igroup名の左側の領域にカーソルを合わせ、チェックボックスをオンにします。イニシエータグループに追加をクリックすると、そのigroupを別のigroupに追加できます。
   - Storage VM *列で、Storage VMの名前をクリックして詳細を確認します。

SANイニシエータを表示および管理します

System Managerを使用して、イニシエータのリストを表示できます。 リストから追加の処理を実行できます。

手順

1. System Managerで、* Hosts > SAN Initiator Groups *をクリックします。

   イニシエータグループ（igroup）のリストが表示されます。

2. イニシエータを表示するには'次の手順に従います

   - FCイニシエータの一覧を表示するには、* FCイニシエータ*タブをクリックします。
   - iSCSIイニシエータのリストを表示するには、* iSCSIイニシエータ*タブをクリックします。

     各列には、イニシエータに関するさまざまな情報が表示されます。

   9.11.1以降では、イニシエータの接続ステータスも表示されます。ステータスアラートにカーソルを合わせると詳細が表示されます。

3. （オプション）：リストの右上にあるアイコンをクリックすると、次のタスクを実行できます。
   - * Search *：特定のイニシエータを一覧表示します。
   - *ダウンロード*リスト。
   - *リストの*または*隠す*列を表示します。
   - *リスト内のデータをフィルタリングします。

ネストされた**igroup**を作成する

ONTAP 9.9.1以降では、他の既存のigroupで構成されるigroupを作成できます。

1. System Manager で、 * Host > SAN Initiator Groups * をクリックし、 * Add * をクリックします。
2. igroup 名 * と * 概要 * を入力します。

   概要は igroup のエイリアスとして機能します。

3. Storage VM * および * Host Operating System * を選択します。

   ネストされた igroup の OS タイプは、 igroup の作成後は変更できません。

4. イニシエータグループメンバー * で、 * 既存のイニシエータグループ * を選択します。
   - Search * を使用して、追加する igroup を検索して選択できます。

igroup を複数の **LUN** にマッピングします

ONTAP 9.9.1以降では、igroupを複数のLUNに同時にマッピングできます。

1. System Manager で、 * Storage > LUNs * をクリックします。
2. マッピングする LUN を選択します。
3. [* 詳細 *] をクリックし、 [* イニシエータ・グループへのマップ *] をクリックします。

   選択した igroup が、選択した LUN に追加されます。 既存のマッピングは上書きされません。

ポートセットを作成して **igroup** にバインドします

の使用に加えて、を使用します "センタクテキ LUN マツフ SLM"では、ポートセットを作成し、ポートセットをigroupにバインドして、イニシエータがLUNへのアクセスに使用するLIFをさらに制限できます。

ポートセットをigroupにバインドしない場合、igroup内のすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナーのすべてのLIFからマップ済みのLUNにアクセスできます。

必要なもの

少なくとも 1 つの LIF と 1 つの igroup が必要です。

インターフェイスグループを使用しないかぎり、 iSCSI と FC の冗長性を確保するために推奨される LIF の数は 2 個です。インターフェイスグループを使用する場合に推奨される LIF の数は 1 個です。

このタスクについて

ノード上にLIFが3つ以上あり、特定のイニシエータを一部のLIFに制限する場合は、ポートセットとSLMを併用する方が効果的です。ポートセットを使用しない場合は、LUNへのアクセス権を持つすべてのイニシエータが、LUNを所有するノードおよび所有者ノードのHAパートナー経由でノード上のすべてのターゲットにアクセスできます。

例 **6.** 手順

System Manager の略

ONTAP 9.10.1 以降の System Manager を使用して、ポートセットを作成し、 igroup にバインドできます。

ONTAP 9.10.1より前のリリースでポートセットを作成してigroupにバインドする必要がある場合は、ONTAP CLI手順 を使用する必要があります。

1. System Manager で、 * Network > Overview > portsets * をクリックし、 * Add * をクリックします。
2. 新しいポートセットの情報を入力し、 * Add * をクリックします。
3. [*Hosts] ＞ [SAN Initiator Groups] をクリックします
4. ポートセットを新しい igroup にバインドするには、 * Add * をクリックします。

   ポートセットを既存の igroup にバインドするには、 igroup を選択し、をクリックします ⋮をクリックし、 * イニシエータグループの編集 * をクリックします。

関連情報

"イニシエータとigroupを表示および管理します"

CLI の使用

1. 適切な LIF を含むポートセットを作成します。

   ```
   portset create -vserver vserver_name -portset portset_name -protocol
   protocol -port-name port_name
   ```

   FCを使用する場合は、を指定します `protocol` パラメータの形式 `fcp`。iSCSIを使用している場合は、を指定します `protocol` パラメータの形式 `iscsi`。

2. igroup をポートセットにバインドします。

   ```
   lun igroup bind -vserver vserver_name -igroup igroup_name -portset
   portset_name
   ```

3. ポートセットと LIF が正しいことを確認します。

   ```
   portset show -vserver vserver_name
   ```

   ```
   Vserver   Portset   Protocol Port Names    Igroups
   --------- --------- -------- ------------- --------
   vs3       portset0  iscsi    lif0,lif1     igroup1
   ```

ポートセットを管理します

に加えて "センタクテキ LUN マツフ SLM"では、ポートセットを使用して、イニシエータが LUN へのアクセスに使用する LIF をさらに制限できます。

ONTAP 9.10.1以降のSystem Managerを使用して、ポートセットに関連付けられているネットワークインターフェイスを変更し、ポートセットを削除できます。

ポートセットに関連付けられているネットワークインターフェイスを変更します

1. System Managerで、*[ネットワーク]>[概要]>[ポートセット]*を選択します。
2. 編集するポートセットを選択します ⋮ をクリックし、「 * ポートセットの編集」を選択します。

ポートセットを削除します

1. System Manager で、 * Network > Overview > portsets * をクリックします。
2. 単一のポートセットを削除するには、ポートセットを選択し、を選択します ⋮ 次に、 [ポートセットの削除] を選択します。

   複数のポートセットを削除するには、ポートセットを選択し、 * 削除 * をクリックします。

選択的 **LUN** マップの概要

選択的 LUN マップ（ SLM ）を使用すると、ホストから LUN へのパスの数を減らすことができます。SLM を使用して新しい LUN マップを作成すると、 LUN を所有するノードとその HA パートナーのパス経由でのみ LUN にアクセスできます。

SLM を使用すると、ホストごとに 1 つの igroup を管理でき、システム停止を伴わない LUN の移動処理がサポートされます。ポートセットの操作や LUN の再マッピングは不要です。

"ポートセット" SLMと併用すると、特定のターゲットのアクセスを特定のイニシエータだけに制限できます。SLM とポートセットを併用する場合、 LUN には、その LUN を所有するノードおよびノードの HA パートナーのポートセットに含まれる一連の LIF 経由でアクセス可能になります。

新しい LUN マップでは SLM がデフォルトで有効になります。

SLM が **LUN** マップで有効かどうかを判断します

ONTAP 9リリースで作成されたLUNと以前のバージョンから移行されたLUNが環境内に混在している場合は、特定のLUNで選択的LUNマップ（SLM）が有効になっているかどうかを確認しなければならないことがあります。

の出力に表示される情報を使用できます `lun mapping show -fields reporting-nodes, node` コマンドを使用して、LUNマップでSLMが有効になっているかどうかを確認します。SLMが有効になっていない場合は、コマンド出力の「reporting-nodes」列の下のセルにと表示されます。SLMが有効な場合、「nodes」列の下に表示されるノードのリストが「reporting-nodes」列に複製されます。

SLM レポートノードリストを変更します

LUN または LUN が含まれているボリュームを同じクラスタ内の別のハイアベイラビリティ（ HA ）ペアに移動する場合は、移動を開始する前に選択的 LUN マップ（ SLM ）のレポートノードリストを変更して、最適化されたアクティブな LUN パスを維持する必要があります。

手順

1. デスティネーションノードとそのパートナーノードをアグリゲートまたはボリュームのレポートノードリ

ストに追加します。

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-
destination-volume _volume_name_]
```

一貫した命名規則がある場合は、を使用して複数のLUNマッピングを同時に変更できます *igroup_prefix** ではなく *igroup_name*。

2. ホストを再スキャンして、新しく追加したパスを検出します。
3. OS で必要な場合は、マルチパスネットワーク I/O （ MPIO ）構成に新しいパスを追加します。
4. 必要な移動処理のためのコマンドを実行して、処理が完了するまで待ちます。
5. I/O がアクティブパスまたは最適パス経由で処理されていることを確認します。

```
lun mapping show -fields reporting-nodes
```

6. レポートノードリストから、前の LUN 所有者とそのパートナーノードを削除します。

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

7. 既存の LUN マップから LUN が削除済みであることを確認します。

```
lun mapping show -fields reporting-nodes
```

8. ホスト OS の古いデバイスのエントリを削除します。
9. 必要に応じて、マルチパス構成ファイルを変更します。
10. ホストを再スキャンして古いパスが削除されたことを確認します。[+]
    ホストを再スキャンする手順については、ホストのマニュアルを参照してください。

iSCSI プロトコルを管理します

最適なパフォーマンスを実現できるようにネットワークを設定します

イーサネットネットワークによってパフォーマンスは大きく変わります。特定の設定値を選択することで、 iSCSI に使用するネットワークのパフォーマンスを最大限に高めることができます。

手順

1. ホストポートとストレージポートを同じネットワークに接続します。

同じスイッチに接続することを推奨します。ルーティングは絶対に使用しないでください。

2. 最も速度の速いポートを選択して、それらを iSCSI 専用にします。

   10GbE ポートが最適です。最小要件は 1GbE ポートです。

3. すべてのポートでイーサネットフロー制御を無効にします。

   が表示されます "Network Management の略" CLI を使用してイーサネットポートのフロー制御を設定するため。

4. ジャンボフレームを有効にします（通常は MTU が 9000 ）。

   イニシエータ、ターゲット、スイッチを含む、データパス内のすべてのデバイスでジャンボフレームがサポートされている必要があります。サポートされていない場合にジャンボフレームを有効にすると、ネットワークのパフォーマンスが大幅に低下

SVM を **iSCSI** 用に設定

iSCSI 用に Storage Virtual Machine （ SVM ）を設定するには、 SVM 用の LIF を作成し、それらの LIF に iSCSI プロトコルを割り当てる必要があります。

このタスクについて

iSCSI プロトコルを使用してデータを提供するそれぞれの SVM について、各ノードに少なくとも 1 つの iSCSI LIF が必要です。冗長性を確保するには、各ノードに少なくとも 2 つの LIF を作成する必要があります。

例 **7.** 手順

System Manager の略

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

新しい**Storage VM**で**iSCSI**を設定	既存の**Storage VM**で**iSCSI**を設定
1. System Managerで、* Storage > Storage VM* をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* iSCSI *」を選択します。 4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 +各ノードに少なくとも2つのネットワークインターフェイスが必要です。 5. [保存（ Save ）] をクリックします。	1. System Manager で、 * Storage > Storage VM* をクリックします。 2. 設定するStorage VMをクリックします。 3. [設定]タブをクリックし、をクリックします ⚙ をクリックします。 4. Enable iSCSI（iSCSIを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 +各ノードに少なくとも2つのネットワークインターフェイスが必要です。 5. [保存（ Save ）] をクリックします。

CLI の使用

ONTAP CLIを使用してiSCSI用のStorage VMを設定します。

1. SVM が iSCSI トラフィックをリスンするようにします。

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. iSCSI に使用する各ノードに、 SVM 用の LIF を作成します。
   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. LIF が正しく設定されたことを確認します。

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

4. iSCSI が正常に稼働していること、およびその SVM のターゲット IQN を確認します。

   ```
   vserver iscsi show –vserver vserver_name
   ```

5. ホストから、 LIF への iSCSI セッションを作成します。

関連情報

"NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"

イニシエータのセキュリティポリシー方式を定義します

イニシエータとその認証方法の一覧を定義できます。ユーザ定義の認証方法がない環境イニシエータに対するデフォルトの認証方法を変更することもできます。

このタスクについて

製品のセキュリティポリシーアルゴリズムを使用して一意のパスワードを生成することも、使用するパスワードを手動で指定することもできます。

> すべてのイニシエータが 16 進数 CHAP シークレットパスワードをサポートしているわけ

手順

1. を使用します `vserver iscsi security create` イニシエータのセキュリティポリシー方式を作成するコマンド。

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. 画面に表示されるコマンドに従ってパスワードを追加します。

   インバウンドとアウトバウンドの CHAP ユーザ名およびパスワードを使用して、イニシエータ iqn.1991-05.com.microsoft:host1 のセキュリティポリシー方式を作成します。

関連情報

- iSCSI 認証の仕組み
- CHAP認証

SVM の **iSCSI** サービスを削除します

Storage Virtual Machine （ SVM ）の不要になった iSCSI サービスは削除できます。

必要なもの

iSCSI サービスを削除するには、 iSCSI サービスの管理ステータスが「所有」状態である必要があります。を使用すると、管理ステータスをdownに切り替えることができます `vserver iscsi modify` コマンドを実行します

手順

1. を使用します `vserver iscsi modify` コマンドを使用してLUNへのI/Oを停止します。

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. を使用します `vserver iscsi delete` コマンドを使用してSVMからiSCSIサービスを削除します。

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. を使用します `vserver iscsi show command` をクリックして、SVMからiSCSIサービスが削除されたことを確認します。

   ```
   vserver iscsi show -vserver vs1
   ```

iSCSI セッションのエラーリカバリの詳細については、こちらを参照してください

iSCSI セッションのエラーリカバリレベルを上げると、 iSCSI エラーリカバリの詳細情報を確認できます。高いレベルのエラーリカバリを使用すると、原因で iSCSI セッションのパフォーマンスが少し低下する可能性があります。

このタスクについて

デフォルトでは、 ONTAP は iSCSI セッションに対してエラーリカバリレベル 0 を使用するように設定されています。エラーリカバリレベル 1 または 2 に対応したイニシエータを使用している場合は、エラーリカバリレベルを上げるように選択できます。変更したセッションのエラーリカバリレベルは、新しく作成するセッションにのみ影響し、既存のセッションには影響しません。

ONTAP 9.4以降では `max-error-recovery-level` オプションはではサポートされていません `iscsi show` および `iscsi modify` コマンド

手順

1. advanced モードに切り替えます。

   ```
   set -privilege advanced
   ```

2. を使用して現在の設定を確認します `iscsi show` コマンドを実行します

   ```
   iscsi show -vserver vs3 -fields max-error-recovery-level
   ```

   ```
   vserver max-error-recovery-level
   ------- ------------------------
   vs3     0
   ```

3. を使用してエラーリカバリレベルを変更します `iscsi modify` コマンドを実行します

   ```
   iscsi modify -vserver vs3 -max-error-recovery-level 2
   ```

SVM を **iSNS** サーバに登録する

を使用できます `vserver iscsi isns` iSNSサーバに登録するようにStorage Virtual Machine（SVM）を設定するコマンド。

このタスクについて

。 `vserver iscsi isns create` コマンドは、SVMをiSNSサーバに登録するように設定します。SVM には、 iSNS サーバの設定や管理を行うコマンドはありません。iSNS サーバを管理するには、 iSNS サーバのベンダーが提供するサーバ管理ツールまたはインターフェイスを使用します。

手順

1. iSNS サーバで、 iSNS サービスが開始しており、サービスを提供可能な状態であることを確認します。
2. データポートに SVM 管理 LIF を作成します。

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

3. SVM に iSCSI サービスがない場合は作成します。

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. iSCSI サービスが正常に作成されたことを確認します。

   ```
   iscsi show -vserver SVM_name
   ```

5. SVM のデフォルトルートが存在していることを確認します。

   ```
   network route show -vserver SVM_name
   ```

6. SVM のデフォルトルートが存在しない場合は、デフォルトルートを作成します。

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

7. iSNS サービスに登録するように SVM を設定します。

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   IPv4 アドレスファミリーと IPv6 アドレスファミリーの両方がサポートされています。iSNS サーバのアドレスファミリーは、 SVM 管理 LIF のアドレスファミリーと同じである必要があります。

   たとえば、 IPv4 アドレスを使用する SVM 管理 LIF を、 IPv6 アドレスを使用する iSNS サーバに接続することはできません。

8. iSNS サービスが実行されていることを確認します。

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. iSNS サービスが実行されていない場合は、 iSNS サービスを開始します。

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

ストレージシステム上の **iSCSI** エラーメッセージを解決します

iSCSI関連の一般的なエラーメッセージは、で確認できます `event log show` コマンドを実行しますこれらのメッセージの意味と、特定された問題の解決方法を把握する必要があります。

次の表に、最も一般的なエラーメッセージと、それらを解決する手順を示します。

メッセージ	説明	対処方法：
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	このインターフェイスの iSCSI サービスが有効になっていません。	を使用できます `iscsi interface enable` コマンドを実行してインターフェイスでiSCSIサービスを有効にします。例： `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	指定されたイニシエータに対して CHAP が正しく設定されていません。	CHAP 設定をチェックします。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。 • ストレージシステムのインバウンドクレデンシャルは、イニシエータのアウトバウンドクレデンシャルと一致する必要があります • ストレージシステムのアウトバウンドクレデンシャルは、イニシエータのインバウンドクレデンシャルと一致する必要があります

iSCSI LIFの自動フェイルオーバーの有効化または無効化

ONTAP 9.11.1以降にアップグレードした場合は、ONTAP 9.10.1以前で作成したすべてのiSCSI LIFでLIFの自動フェイルオーバーを手動で有効にする必要があります。

ONTAP 9.11.1以降では、オールフラッシュSANアレイプラットフォームでiSCSI LIFのLIFの自動フェイルオーバーを有効にすることができます。ストレージフェイルオーバーが発生すると、iSCSI LIFはホームノードまたはポートからHAパートナーノードまたはポートに自動的に移行され、フェイルオーバーの完了後に再び移行されます。 または、iSCSI LIFのポートが正常な状態でなくなった場合、そのLIFは現在のホームノードの正常なポートに自動的に移行され、ポートが正常な状態に戻った時点で元のポートに戻ります。 を使用すると、iSCSIで実行されているSANワークロードは、フェイルオーバー後にI/Oサービスを迅速に再開できます。

ONTAP 9.11.1以降では、次のいずれかの条件に該当する場合、新しく作成したiSCSI LIFでLIFの自動フェイルオーバーがデフォルトで有効になります。

- SVMにiSCSI LIFがありません
- LIFの自動フェイルオーバーがSVMのすべてのiSCSI LIFで有効になっている

iSCSI LIFの自動フェイルオーバーを有効にする

デフォルトでは、ONTAP 9.10.1以前で作成したiSCSI LIFでは、LIFの自動フェイルオーバーは有効になりません。 SVM上にLIFの自動フェイルオーバーが有効になっていないiSCSI LIFがある場合、新しく作成したLIFでもLIFの自動フェイルオーバーは有効になりません。 LIFの自動フェイルオーバーが有効になっておらず、

フェイルオーバーが発生するとiSCSI LIFは移行されません。

の詳細を確認してください "LIFのフェイルオーバーとギブバック"。

ステップ

1. iSCSI LIFの自動フェイルオーバーを有効にします。

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-
policy sfo-partner-only -auto-revert true
```

SVMのすべてのiSCSI LIFを更新するには、 `-lif*` ではなく `lif`。

iSCSI LIFの自動フェイルオーバーを無効にする

ONTAP 9.10.1以前で作成したiSCSI LIFに対するiSCSI LIFの自動フェイルオーバーを以前に有効にしていた場合は、無効にすることもできます。

ステップ

1. iSCSI LIFの自動フェイルオーバーを無効にします。

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-
policy disabled -auto-revert false
```

SVMのすべてのiSCSI LIFを更新するには、 `-lif*` ではなく `lif`。

関連情報

- "LIF を作成"
- 手動で実行する "LIFを移行する"
- 手動で実行する "LIFをホームポートにリバートします。"
- "LIF のフェイルオーバーを設定する"

FC プロトコルを管理する

FC 用に SVM を設定

FC 用に Storage Virtual Machine （ SVM ）を設定するには、 SVM 用の LIF を作成し、それらの LIF に FC プロトコルを割り当てる必要があります。

作業を開始する前に

FCライセンス（"ONTAP Oneに付属"）を使用し、有効にする必要があります。FCライセンスが有効になっていない場合、LIFとSVMはオンラインとして表示されますが、動作ステータスはになります `down`。LIF と SVM を動作状態にするには、 FC サービスを有効にする必要があります。イニシエータをホストするには、SVM 内のすべての FC LIF で単一イニシエータゾーニングを使用する必要があります。

このタスクについて

ネットアップでは、 FC プロトコルを使用してデータを提供するそれぞれの SVM について、各ノードに少なくとも 1 つの FC LIF をサポートしています。 ノードごとに 1 つの LIF を接続した構成では、ノードごとに 2 つの LIF と 2 つのファブリックを使用する必要があります。これにより、ノードレイヤとファブリックで冗長性が確保されます。

例 **8.** 手順

System Manager の略

ONTAP System Manager（9.7以降）でiSCSI用のStorage VMを設定します。

をクリックして新しい**Storage VM**に**FC**を設定してください	既存の**Storage VM**に**FC**を設定
1. System Managerで、* Storage > Storage VM* をクリックし、* Add *をクリックします。 2. Storage VMの名前を入力してください。 3. アクセスプロトコル*として「* FC」を選択します。 4. [FCを有効にする]をクリックします。 + FCポートが自動的に割り当てられます。 5. [保存（ Save ）] をクリックします。	1. System Manager で、 * Storage > Storage VM* をクリックします。 2. 設定するStorage VMをクリックします。 3. [設定]タブをクリックし、をクリックします ⚙ をクリックします。 4. Enable FC（FCを有効にする）をクリックし、ネットワークインタフェースのIPアドレスとサブネットマスクを入力します。 + FCポートが自動的に割り当てられます。 5. [保存（ Save ）] をクリックします。

CLI の使用

1. SVM で FC サービスを有効にします。

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. FC を提供する各ノードの SVM 用に 2 つの LIF を作成します。
   - ONTAP 9.6以降：

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - ONTAP 9.5以前：

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. LIFが作成され、動作ステータスがになっていることを確認します `online`：

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

関連情報

"ネットアップサポート"

"NetApp Interoperability Matrix Tool で確認できます"

クラスタ SAN 環境での LIF に関する注意事項

SVM の FC サービスを削除する

Storage Virtual Machine （ SVM ）の不要になった FC サービスは削除できます。

必要なもの

SVM の FC サービスを削除するには、事前に管理ステータスを「所有」にする必要があります。管理ステータスをdownに設定するには、を使用します `vserver fcp modify` コマンドまたはを実行します `vserver fcp stop` コマンドを実行します

手順

1. を使用します `vserver fcp stop` コマンドを使用してLUNへのI/Oを停止します。

   ```
   vserver fcp stop -vserver vs_1
   ```

2. を使用します `vserver fcp delete` SVMからサービスを削除するコマンド。

   ```
   vserver fcp delete -vserver vs_1
   ```

3. を使用します `vserver fcp show` SVMからFCサービスが削除されたことを確認します。

   ```
   vserver fcp show -vserver vs_1
   ```

FCoE ジャンボフレーム用の MTU の推奨設定

Fibre Channel over Ethernet （ FCoE ）の場合、 CNA のイーサネットアダプタ部分については、ジャンボフレームを 9000 MTU で設定する必要があります。CNA の FCoE アダプタ部分については、ジャンボフレームを 1500 以上の MTU で設定する必要があります。イニシエータ、ターゲット、および介在するすべてのスイッチがジャンボフレームをサポートしており、ジャンボフレーム用に設定されている場合にのみ、ジャンボフレームを設定します。

NVMe プロトコルを管理します

SVM の NVMe サービスを開始します

Storage Virtual Machine （ SVM ）で NVMe プロトコルを使用する前に、 SVM で NVMe サービスを開始しておく必要があります。

作業を開始する前に

システムで NVMe プロトコルが許可されている必要があります。

サポートされる NVMe プロトコルは次のとおりです。

プロトコル	先頭のドキュメント	許可者
TCP	ONTAP 9.10.1	デフォルト
FCP	ONTAP 9.4	デフォルト

手順

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. NVMe プロトコルが許可されていることを確認します。

   ```
   vserver nvme show
   ```

3. NVMe プロトコルサービスを作成します。

   ```
   vserver nvme create
   ```

4. SVM で NVMe プロトコルサービスを開始します。

   ```
   vserver nvme modify -status -admin up
   ```

SVM から **NVMe** サービスを削除します

必要に応じて、 Storage Virtual Machine （ SVM ）から NVMe サービスを削除できます。

手順

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. SVM で NVMe サービスを停止します。

   ```
   vserver nvme modify -status -admin down
   ```

3. NVMe サービスを削除します。

   ```
   vserver nvme delete
   ```

ネームスペースのサイズを変更する

ONTAP 9.10.1 以降では、 ONTAP CLI を使用して NVMe ネームスペースのサイズを拡張または縮小できます。System Manager を使用して、 NVMe ネームスペースのサイズを拡張できます。

ネームスペースのサイズを拡張する

System Manager の略

1. Storage > NVMe Namespaces * をクリックします。
2. 拡張するネームスペースの上にあるをクリックします ⋮をクリックし、 * 編集 * をクリックします。
3. 容量 * で、ネームスペースのサイズを変更します。

CLI の使用

1. 次のコマンドを入力します。 `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

ネームスペースのサイズを縮小します

NVMe ネームスペースのサイズを縮小するには、 ONTAP CLI を使用する必要があります。

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. ネームスペースのサイズを縮小します。

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

ネームスペースを**LUN**に変換する

ONTAP 9.11.1以降では、ONTAP CLIを使用して、既存のNVMeネームスペースをインプレースでLUNに変換できます。

を開始する前に

- 指定したNVMeネームスペースにはサブシステムへの既存のマッピングがありません。
- ネームスペースをSnapshotコピーの一部にしたり、SnapMirror関係のデスティネーション側で読み取り専用ネームスペースとして使用したりすることはできません。
- NVMeネームスペースは特定のプラットフォームとネットワークカードでのみサポートされるため、この機能は特定のハードウェアでのみ機能します。

手順

1. 次のコマンドを入力して、NVMeネームスペースをLUNに変換します。

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

NVMe経由のインバンド認証の設定

ONTAP 9.12.1以降では、ONTAPコマンドラインインターフェイス（CLI）を使用して、DH-HMAC-CHAP認証を使用して、NVMe/TCPおよびNVMe/FCプロトコルを介し

たNVMeホストとコントローラ間のインバンド（セキュア）双方向および単方向認証を設定できます。 ONTAP 9.14.1以降では、インバンド認証をSystem Managerで設定できます。

インバンド認証を設定するには、各ホストまたはコントローラにDH-HMAC-CHAPキーを関連付ける必要があります。DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。 NVMeホストまたはコントローラがピアを認証するには、ピアに関連付けられたキーを認識している必要があります。

単方向認証では、コントローラではなくホストにシークレットキーが設定されます。 双方向認証では、ホストとコントローラの両方にシークレットキーが設定されます。

SHA-256がデフォルトのハッシュ関数で、2048ビットがデフォルトのDHグループです。

System Manager の略

ONTAP 9.14.1以降では、NVMeサブシステムの作成または更新、NVMeネームスペースの作成またはクローニング、新しいNVMeネームスペースを使用した整合グループの追加時に、System Managerを使用してインバンド認証を設定できます。

手順

1. System Managerで、**[**ホスト**]>[NVMe**サブシステム**]***をクリックし、[追加]*をクリックします。
2. NVMeサブシステム名を追加し、Storage VMとホストオペレーティングシステムを選択します。
3. ホストのNQNを入力します。
4. [Host NQN]の横にある*[Use in-band authentication]*を選択します。
5. ホストシークレットとコントローラシークレットを指定します。

   DH-HMAC-CHAPキーは、NVMeホストまたはコントローラのNQNと管理者が設定した認証シークレットを組み合わせたものです。

6. ホストごとに使用するハッシュ関数とDHグループを選択します。

   ハッシュ関数とDHグループを選択しない場合、SHA-256がデフォルトのハッシュ関数として割り当てられ、2048ビットがデフォルトのDHグループとして割り当てられます。

7. 必要に応じて、*[追加]*をクリックし、必要に応じて手順を繰り返してホストを追加します。
8. [保存（ Save ）] をクリックします。
9. インバンド認証が有効になっていることを確認するには、*[システムマネージャ]>[ホスト]>[NVMeサブシステム]>[グリッド]>[ピークビュー]*をクリックします。

   ホスト名の横にあるトランスペアレントキーアイコンは、単方向モードがイネーブルであることを示します。 ホスト名の横にある不透明キーは、双方向モードが有効であることを示します。

CLI の使用

手順

1. NVMeサブシステムにDH-MHMAC-CHAP認証を追加します。

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. DH-MHMAC CHAP認証プロトコルがホストに追加されていることを確認します。

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

3. NVMeコントローラの作成時にDH-MHMAC CHAP認証が実行されたことを確認します。

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

NVMe経由のインバンド認証を無効にする

DH-HMAC-CHAPを使用してNVMe経由のインバンド認証を設定している場合は、いつでも無効にすることができます。

ONTAP 9.12.1以降からONTAP 9.12.0以前にリバートする場合は、リバート前にインバンド認証を無効にする必要があります。 DH-HMAC-CHAPを使用するインバンド認証が無効になっていない場合、リバートは失敗します。

手順

1. サブシステムからホストを削除して、DH-MHMAC-CHAP認証を無効にします。

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. DH-MHMAC-CHAP認証プロトコルがホストから削除されたことを確認します。

```
vserver nvme subsystem host show
```

3. 認証を行わずにホストをサブシステムに再度追加します。

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

NVMeホスト優先度の変更

ONTAP 9.14.1以降では、特定のホストに対するリソース割り当ての優先順位を設定するようにNVMeサブシステムを設定できます。デフォルトでは、ホストがサブシステムに追加されると、通常の優先度が割り当てられます。高い優先度を割り当てられたホストには、より多くのI/Oキュー数とキュー深度が割り当てられます。

ONTAPのコマンドラインインターフェイス（CLI）を使用して、デフォルト優先度を手動で標準から高に変更できます。 ホストに割り当てられている優先度を変更するには、サブシステムからホストを削除してから再度追加する必要があります。

手順

1. ホストプライオリティがRegularに設定されていることを確認します。

```
vserver nvme show-host-priority
```

2. サブシステムからホストを削除します。

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

3. ホストがサブシステムから削除されたことを確認します。

```
vserver nvme subsystem host show
```

4. 優先度が高いサブシステムにホストを再度追加します。

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

NVMe / TCPコントローラのホストの自動検出を管理します。

ONTAP 9.14.1以降、IPベースのファブリックでは、NVMe/TCPプロトコルを使用するコントローラのホスト検出がデフォルトで自動化されます。

NVMe / TCPコントローラのホスト検出を自動化

以前に自動ホスト検出を無効にしていたが、ニーズが変わった場合は、再度有効にすることができます。

手順

1. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を有効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. NVMe/TCPコントローラの自動検出が有効になっていることを確認します。

```
vserver nvme show
```

NVMe / TCPコントローラのホストの自動検出を無効にする

NVMe / TCPコントローラをホストで自動的に検出する必要がなく、ネットワークで不要なマルチキャストトラフィックが検出された場合は、この機能を無効にする必要があります。

手順

1. advanced 権限モードに切り替えます。

```
set -privilege advanced
```

2. 自動検出を無効にします。

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. NVMe/TCPコントローラの自動検出が無効になっていることを確認します。

```
vserver nvme show
```

NVMeホスト仮想マシン識別子の無効化

ONTAP 9.14.1以降では、デフォルトで、ONTAPでNVMe/FCホストが一意の識別子で仮想マシンを識別し、NVMe/FCホストが仮想マシンのリソース利用率を監視する機能がサポートされます。 これにより、ホスト側のレポート作成とトラブルシューティングが強化されます。

この機能は、bootargを使用して無効にできます。

ステップ

1. 仮想マシンIDを無効にします。

```
bootargs set fct_sli_appid_off <port>, <port>
```

次の例は、ポート0gとポート0iのVMIDを無効にします。

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

FC アダプタを搭載したシステムを管理する

FC アダプタを搭載したシステムを管理する

オンボード FC アダプタと FC アダプタカードの管理に使用できるコマンドが用意されています。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボード FC アダプタが搭載されています。イニシエータまたはターゲットとして設定された FC アダプタカードを使用することもできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（ FlexArray ）にも接続します。ターゲットは FC スイッチのみに接続します。 FC ターゲットの HBA ポートとスイッチポートの速度は、両方とも同じ値に設定し、 auto には設定しないでください。

関連情報

"SAN構成"

FC アダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。を使用する必要があります `run -node` *`node_name`* FCイニシエータアダプタのコマンドを使用する前のコマンド。

FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	`network fcp adapter show`
FC ターゲットアダプタのパラメータを変更する	`network fcp adapter modify`
FC プロトコルトラフィック情報を表示します	`run -node node_name sysstat -f`
FC プロトコルの実行時間を表示します	`run -node node_name uptime`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`
コマンドのマニュアルページを表示します	`man command_name`

FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	`run -node node_name storage show adapter`
アダプタの設定とステータスを表示します	`run -node node_name sysconfig -v adapter`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node node_name sysconfig -ac`

オンボード **FC** アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	`run -node node_name system hardware unified-connect show`

FCアダプタを設定

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、で確認できます

"NetApp Hardware Universe の略"。

ターゲットモードは、ポートを FC イニシエータに接続するために使用します。イニシエータモードは、テープドライブやテープライブラリへのポートの接続、または FlexArray 仮想化や Foreign LUN Import （ FLI ）を使用するサードパーティストレージへのポートの接続に使用されます。

FC アダプタを構成する手順は、 FC プロトコルでも FC-NVMe プロトコルでも同じです。ただし、 FC-NVMe をサポートする FC アダプタは限られています。を参照してください "NetApp Hardware Universe の略" FC-NVMe プロトコルをサポートするアダプタの一覧が表示されます。

FC アダプタをターゲットモードに設定します

手順

1. アダプタをオフラインにします。

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

   ```
   network fcp adapter show -node node_name
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

FC アダプタをイニシエータモードに設定します

必要なもの

- アダプタの LIF を、メンバーとして属するすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更する物理ポートを使用するすべての Storage Virtual Machine （ SVM ）のすべての LIF を、移行するか破棄する必要があります。

> NVMe/FC ではイニシエータモードがサポートされます。

手順

1. アダプタからすべての LIF を削除します。

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

2. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin
down
```

アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

```
system hardware unified-connect modify -t initiator adapter_port
```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対して FC ポートが正しい状態で設定されていることを確認します。

```
system hardware unified-connect show
```

6. アダプタをオンラインに戻します。

```
node run -node node_name storage enable adapter adapter_port
```

アダプタの設定を確認します

特定のコマンドを使用して、FC / UTAアダプタに関する情報を表示できます。

FCターゲットアダプタ

ステップ

1. を使用します `network fcp adapter show` アダプタ情報を表示するコマンド： `network fcp adapter show -instance -node node1 -adapter 0a`

   使用されている各スロットのシステム設定情報とアダプタ情報が出力に表示されます。

ユニファイドターゲットアダプタ（**UTA**）の**X1143A-R6**

手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. を実行します `system hardware unified-connect show` コマンドを使用して、ポートの設定とモジュールを確認します。
3. ポート情報を確認してから、 CNA とポートを設定します。

UTA2 ポートを **CNA** モードから **FC** モードに変更します

Fibre Channel （ FC ；ファイバチャネル）イニシエータモードと FC ターゲットモードをサポートするには、 UTA2 ポートを Converged Network Adapter （ CNA ；統合ネットワークアダプタ）モードから FC モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

手順

1. アダプタをオフラインにします。

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. ポートのモードを変更します。

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. ノードをリブートし、アダプタをオンラインにします。

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。

   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

     i. LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。

     ii. を実行して、ポートを手動で削除します `network port delete` コマンドを実行します

     状況に応じて `network port delete` コマンドが失敗した場合は、エラーに対処してからもう一度コマンドを実行する必要があります。

   - ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

     VIFマネージャでポートが削除されない場合は、管理者がリブート後にを使用してポートを手動で削除する必要があります `network port delete` コマンドを実行します

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
```

```
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、 10Gb イーサネット SFP を使用します。FC の場合は、ノードで構成を変更する前に、8Gb SFP または 16Gb SFP を使用します。

CNA / UTA2 ターゲットアダプタの光モジュールを変更します

ユニファイドターゲットアダプタ（ CNA / UTA2 ）用に選択したパーソナリティモードをサポートするには、そのアダプタで光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6 アダプタから現在の光モジュールを取り外します。
3. 優先して使用するパーソナリティモード（ FC または CNA ）の光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   サポートされている SFP+ モジュールと Cisco ブランドの銅線（ Twinax ）ケーブルについては、Hardware Universe を参照してください。

関連情報

"NetApp Hardware Universe の略"

X1143A-R6 アダプタでサポートされるポート設定

FC ターゲットモードは、 X1143A-R6 アダプタポートのデフォルト設定です。ただし、このアダプタのポートは、 10Gb イーサネットおよび FCoE ポートまたは 16Gb FC ポートとして設定できます。

イーサネットおよび FCoE 用に設定した場合、 X1143A-R6 アダプタは、同じ 10GbE ポートの NIC および FCoE のターゲットトラフィックを同時にサポートします。FC 用に設定した場合、同じ ASIC を共有する 2 ポートの各ペアを FC ターゲットまたは FC イニシエータモード用に個別に設定できます。つまり、単一の X1143A-R6 アダプタが、 1 つの 2 ポートペアで FC ターゲットモードをサポートし、もう 1 つの 2 ポートペアで FC イニシエータモードをサポートできます。

関連情報

"NetApp Hardware Universe の略"

"SAN構成"

ポートを設定します

ユニファイドターゲットアダプタ（ X1143A-R6 ）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. を使用して、必要に応じてFibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します `system node hardware unified-connect modify` コマンドを実行します
2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   CNA の場合は、 10Gb イーサネット SFP を使用します。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

X1133A-R6 アダプタ使用時の接続の切断を回避します

別の X1133A-R6 HBA への冗長パスを構成することにより、ポート障害時に接続が切断されないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一の ASIC の両方のポートを、ターゲットモードまたはイニシエータモードのどちらかで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

すべての **SAN** プロトコルの **LIF** を管理します

すべての **SAN** プロトコルの **LIF** を管理します

SAN環境でクラスタのフェイルオーバー機能を利用するには、イニシエータでMultipath I/O（MPIO；マルチパスI/O）とAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）を使用する必要があります。ノードで障害が発生した場合、 LIF は障害が発生したパートナーノードの IP アドレスを引き継ぎません。代わりに、 MPIO ソフトウェアが、ホストの ALUA を使用して、 LIF 経由で LUN にアクセスするための適切なパスを選択します。

HA ペアの各ノードから 1 つ以上の iSCSI パスを作成し、 HA ペアで処理する LUN に論理インターフェイス（ LIF ）を使用してアクセスできるようにする必要があります。 SAN をサポートする Storage Virtual Machine （ SVM ）ごとに管理 LIF を 1 つ設定する必要があります。

直接接続またはイーサネットスイッチの使用がサポートされています。両方のタイプの接続用にLIFを作成する必要があります。

- SAN をサポートする Storage Virtual Machine （ SVM ）ごとに管理 LIF を 1 つ設定する必要があります。ノードごとに 2 つの LIF を設定できます。 LIF は、 iSCSI 用のイーサネットネットワークを分離するために、 FC で使用するファブリックごとに 1 つずつ使用します。

作成したLIFは、ポートセットから削除したり、Storage Virtual Machine（SVM）内の別のノードに移動したり、LIFを削除したりできます。

関連情報

- "LIFを上書き設定"
- "LIF を作成"

NVMe LIF を設定します

NVMe LIF を設定するときは、特定の要件を満たす必要があります。

作業を開始する前に

LIF を作成する FC アダプタで NVMe がサポートされている必要があります。サポートされているアダプタについては、 "Hardware Universe"。

このタスクについて

ONTAP 9.12.1以降では、ノードごとに最大12ノードのNVMe LIFを2つ設定できます。 ONTAP 9.11.1以前では、ノードあたり2つのNVMe LIFを、最大2つのノードで設定できます。

NVMe LIF を作成するときのルールは次のとおりです。

- データ LIF で使用できるデータプロトコルは NVMe のみです。
- SAN をサポートする SVM ごとに管理 LIF を 1 つ設定する必要があります。
- ONTAP 9.5以降では、ネームスペースを含むノードとそのHAパートナーにNVMe LIFを設定する必要があります。
- ONTAP 9.4 のみ：
  - NVMe の LIF とネームスペースは、同じノードでホストする必要があります。
  - 設定できる NVMe データ LIF は SVM ごとに 1 つだけです。

手順

1. LIF を作成します。

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

> NVMe/TCPはONTAP 9.10.1以降で使用できます。

2. LIF が作成されたことを確認します。

```
network interface show -vserver <SVM_name>
```

作成後、NVMe/TCP LIFはポート8009で検出をリスンします。

SAN LIFを移動する前に理解しておくべきこと

クラスタにノードを追加したりクラスタからノードを削除するなど、クラスタの構成を変更する場合は、 LIF を移動するだけで済みます。LIF を移動すれば、 FC ファブリックを再ゾーニングしたり、クラスタに接続されたホストとその新しいターゲットインターフェイスとの間に新しい iSCSI セッションを作成したりする必要がありません。

を使用してSAN LIFを移動することはできません `network interface move` コマンドを実行しますSAN LIF を移動するには、まず目的の LIF をオフラインにし、別のホームノードやポートに移動させてから、移動先の新しい場所で LIF をオンラインに戻します。Asymmetric Logical Unit Access （ ALUA ；非対称論理ユニットアクセス）は、任意の ONTAP 解決策の一部として冗長パスと自動選択を提供します。このため、移動時に LIF がオフライン状態になっても、 I/O の中断は生じません。ホストは再試行してから、 I/O を別の LIF に移動するだけです。

LIF の移動を使用すると、システムを停止することなく次の操作を実行できます。

- クラスタの 1 つの HA ペアを、 LUN データにアクセスするホストにはまったく支障のない形で、アップグレードした HA ペアに置き換えます
- ターゲットインターフェイスカードをアップグレードします
- Storage Virtual Machine （ SVM ）のリソースをクラスタ内のノードセットから別のノードセットに移行する

ポートセットから **SAN LIF** を削除する

削除または移動する LIF がポートセットに含まれている場合、 LIF を削除または移動する前に、ポートセットから LIF を削除する必要があります。

このタスクについて

次の手順の手順 1 は、 LIF が 1 つだけポートセットにある場合にのみ実行する必要があります。ポートセットがイニシエータグループにバインドされている場合、そのポートセット内の最後の LIF は削除できません。複数の LIF がポートセットにある場合は、手順 2 から開始できます。

手順

1. ポートセットにLIFが1つしかない場合は、を使用します `lun igroup unbind` イニシエータグループからポートセットのバインドを解除するコマンド。

   > イニシエータグループとポートセットのバインドを解除すると、イニシエータグループ内のすべてのイニシエータは、すべてのネットワークインターフェイス上の、そのイニシエータグループにマッピングされたすべてのターゲット LUN にアクセスできるようになります。

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

2. を使用します `lun portset remove` コマンドを使用してポートセットからLIFを削除します。

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

SAN LIF を移動します

ノードをオフラインにする必要がある場合、 SAN LIF を移動して WWPN などの設定情報を保持しておけば、スイッチファブリックの再ゾーニングを行わずに済みます。SAN LIF は移動前にオフラインにする必要があるため、ホストトラフィックについては、ホストマルチパスソフトウェアを使用して、 LUN への無停止アクセスを確保する必要があります。SAN LIF はクラスタ内の任意のノードに移動できますが、 SAN LIF を別の Storage Virtual Machine （ SVM ）に移動することはできません。

必要なもの

LIF がポートセットのメンバーである場合、 LIF を別のノードに移動する前に、その LIF をポートセットから削除しておく必要があります。

このタスクについて

移動する LIF のデスティネーションノードおよび物理ポートは、同じ FC ファブリック上またはイーサネットネットワーク上に存在する必要があります。適切にゾーニングされていない別のファブリック上に LIF を移動したり、 iSCSI イニシエータとターゲットを接続していないイーサネットネットワーク上に LIF を移動したりすると、その LIF をオンラインに戻しても接続できなくなります。

手順

1. LIF の管理ステータスと動作ステータスを表示します。

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

2. LIFのステータスをに変更します `down` （オフライン）：

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin
   down
   ```

3. LIF を新しいノードとポートに割り当てます。

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

4. LIFのステータスをに変更します `up` （オンライン）：

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin up
   ```

5. 変更内容を確認します。

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

SAN 環境の LIF を削除する

LIF を削除する前に、 LIF に接続しているホストが、別のパスを介して LUN にアクセスできることを確認してください。

必要なもの

削除する LIF がポートセットのメンバーである場合、 LIF を削除する前に、まずポートセットから LIF を削除

する必要があります。

System Manager の略

ONTAP System Manager（9.7以降）を使用してLIFを削除します。

手順

1. System Managerで、* Network > Overview をクリックし、 Network Interfaces *を選択します。
2. LIFを削除するStorage VMを選択します。
3. をクリックします ⋮ をクリックし、 * Delete * を選択します。

CLI の使用

ONTAP CLIを使用してLIFを削除する

手順

1. 削除する LIF の名前と現在のポートを確認します。

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

2. LIF を削除します。

   ```
   network interface delete

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

3. LIF が削除されたことを確認します。

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                     Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

クラスタにノードを追加するための**SAN LIF**の要件

クラスタにノードを追加する場合は、一定の考慮事項について理解しておく必要があります。

- 新しいノードに LUN を作成する前に、必要に応じてそれらのノードに LIF を作成する必要があります。
- ホストスタックとプロトコルの指示に従って、作成した LIF をホストから検出する必要があります。
- クラスタインターコネクトネットワークを使用しないでも LUN やボリュームを移動できるようにするには、新しいノード上に LIF を作成する必要があります。

ホストによる **iSCSI SendTargets** 検出処理に対して **FQDN** を返すように **iSCSI LIF** を設定します

ONTAP 9 以降では、ホスト OS から送信された iSCSI SendTargets 検出処理に対して Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を返すように iSCSI LIF を設定できます。FQDN を返すように設定すると、ホスト OS とストレージサービスの間にネットワークアドレス変換（ NAT ）デバイスがある場合に便利です。

このタスクについて

IP アドレスは NAT デバイスを挟んだ反対側では認識されませんが、 FQDN であれば両方で認識されます。

> FQDN 値の互換性のある最大文字数は、すべてのホスト OS で 128 文字です。

手順

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. FQDN を返すように iSCSI LIF を設定します。

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   次の例では、 FQDN として storagehost-005.example.com を返すように iSCSI LIF を設定しています。

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. sendtargets が FQDN になっていることを確認します。

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   この例では、 sendtargets-fqdn 出力フィールドに storagehost-005.example.com が表示されています。

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif        sendtargets-fqdn
   ------- ---------- ---------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

関連情報

"ONTAP 9コマンド"

推奨されるボリュームとファイルまたは **LUN** の設定の組み合わせ

推奨されるボリュームとファイルまたは **LUN** の設定の組み合わせの概要

使用可能な FlexVol の設定とファイルまたは LUN の設定の組み合わせは、使用するアプリケーションと管理要件によって異なります。これらの組み合わせのメリットとデメリットを理解しておくと、環境に適したボリュームと LUN の設定の組み合わせを決定する際に役立ちます。

推奨されるボリュームと LUN の設定の組み合わせは次のとおりです。

- スペースリザーブファイルまたはスペースリザーブ LUN とシックボリュームプロビジョニング
- スペースリザーブなしのファイルまたはスペースリザーブなしの LUN とシンボリュームプロビジョニング
- スペースリザーブファイルまたはスペースリザーブ LUN とセミシックボリュームプロビジョニング

これらのいずれかの設定の組み合わせとともに、 LUN で SCSI シンプロビジョニングを使用できます。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックボリュームプロビジョニング

- 利点 :*
- スペースリザーブファイルでのすべての書き込み処理が保証されます。スペース不足のために失敗することはありません。
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- コストと制限： *
- シックプロビジョニングボリュームをサポートするための十分なスペースをアグリゲートから事前に確保しておく必要があります。
- LUN 作成時に、 LUN の 2 倍のサイズのスペースがボリュームから割り当てられます。

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンボリュームプロビジョニング

- 利点 :*
- ボリュームでの Storage Efficiency テクノロジとデータ保護テクノロジに関する制限はありません。
- スペースは使用時に初めて割り当てられます。
- 費用および制限 :*
- 書き込み処理は保証されず、ボリュームの空きスペースが不足すると失敗する場合があります。
- アグリゲートの空きスペースを効果的に管理して、空きスペースが不足しないようにする必要があります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニング

- 利点 :*

事前に確保されるスペースがシックボリュームプロビジョニングの場合よりも少なく、ベストエフォートの書き込み保証も提供されます。

- 費用および制限 :*
- このオプションを指定すると、書き込み処理が失敗することがあります。

  このリスクは、ボリュームの空きスペースとデータの揮発性の適切なバランスを維持することで軽減できます。

- Snapshot コピー、 FlexClone ファイル、 FlexClone LUN などのデータ保護オブジェクトは保持できません。
- 重複排除、圧縮、 ODX / コピーオフロードなど、自動で削除できない ONTAP のブロック共有ストレージ効率化機能は使用できません。

環境に適したボリュームと **LUN** の構成の組み合わせを決定します

環境に関するいくつかの基本的な質問に答えることで、環境に最も適した FlexVol ボリュームと LUN の設定を決定できます。

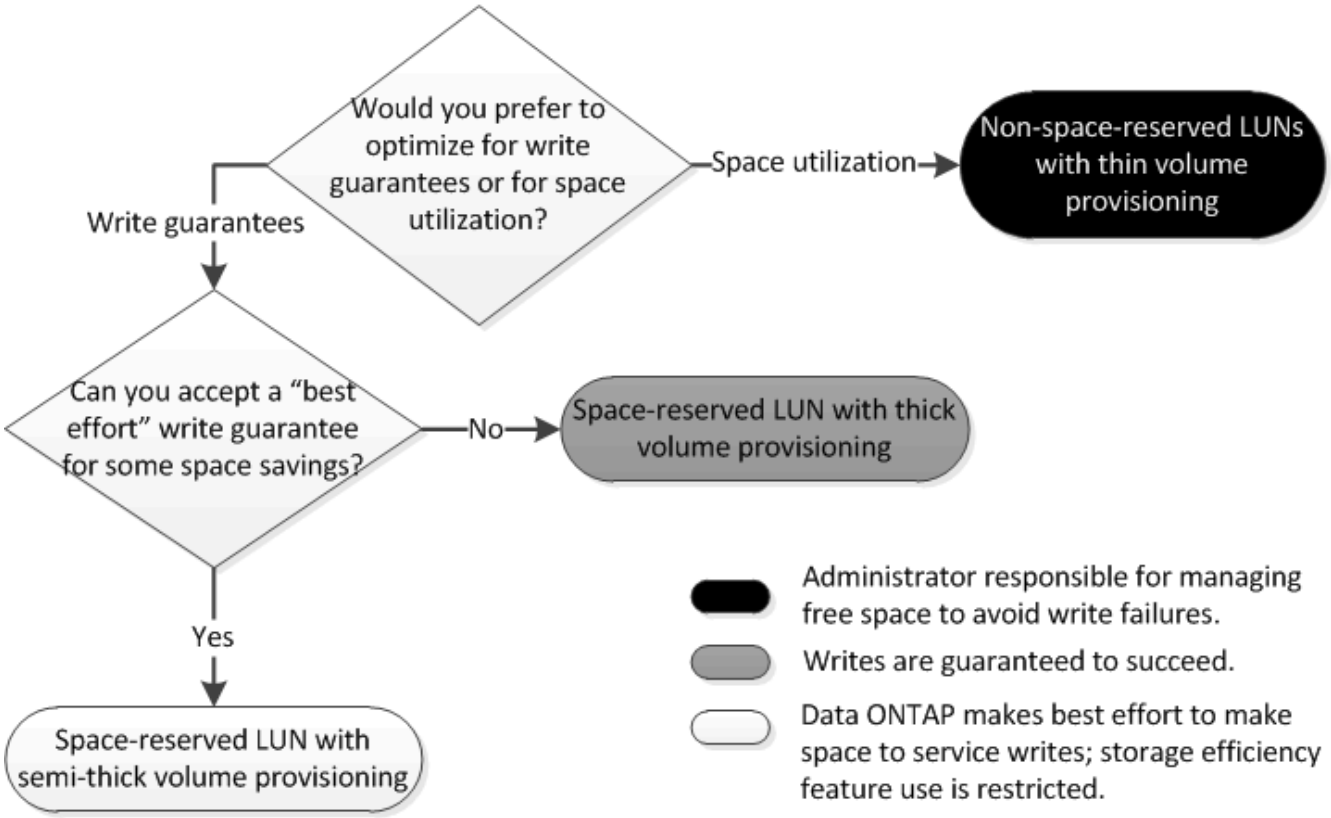
このタスクについて

LUN とボリュームの設定は、ストレージ利用率を最大限に高めるため、または書き込みを確実に保証するために最適化することができます。ストレージの利用要件と、空きスペースを監視し迅速に補充するための要件に基づいて、ご使用の環境に適した FlexVol ボリュームと LUN ボリュームを決める必要があります。

LUN ごとに個別のボリュームを設定する必要はありません。

ステップ

1. 次のデシジョンツリーを使用して、環境に最も適したボリュームと LUN の設定の組み合わせを決定してください。



LUN のデータの増加率を計算します

スペースリザーブ LUN とスペースリザーブなしの LUN のどちらが適切かを判断するには、時間の経過に伴う LUN データの増加率を把握する必要があります。

このタスクについて

データの増加率が一定して高い場合、スペースリザーブ LUN の使用が適しています。データの増加率が低い場合は、スペースリザーブなしの LUN を検討してください。

OnCommand Insight などのツールを使用してデータの増加率を計算することも、手動で計算することもできます。手動計算の手順を次に示します。

手順

1. スペースリザーブ LUN をセットアップします。
2. 一定期間、たとえば 1 週間、 LUN 上のデータを監視します。

   データの増加が定期的に発生する代表的なサンプルを形成するために、十分な監視期間を確保してください。たとえば、毎月末には大量のデータが常に増加する可能性があります。

3. 毎日、増加したデータの量を GB 単位で記録します。
4. 監視期間の最後に、 1 日ごとの合計を合算し、監視期間中の総日数で割ります。

   この計算で、平均増加率が導かれます。

例

この例では、 200GB の LUN が必要です。1 週間 LUN を監視し、毎日のデータの変更を記録しました。記録は次のとおりです。

- 日曜日： 20GB
- 月曜日： 18GB
- 火曜日： 17GB
- 水曜日： 20GB
- 木曜日： 20GB
- 金曜日： 23GB
- 土曜日： 22GB

この例では、増加率は（ 20+18+17+20+20+23+22 ） / 7 で求めることができ、 1 日あたり 20GB となります。

スペースリザーブファイルまたはスペースリザーブ **LUN** とシックプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、 Storage Efficiency テクノロジを使用できます。また、事前に十分なスペースが割り当てられるため、空きスペースを能動的に監視する必要がありません。

シックプロビジョニングを使用するボリュームでスペースリザーブファイルまたはスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	ボリューム
フラクショナルリザーブ	100
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	価値
スペースリザベーション	有効

スペースリザーブなしのファイルまたはスペースリザーブなしの **LUN** とシンプロビジョニングボリュームを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、事前に割り当てられるス

トレージの量が最小になりますが、スペース不足によるエラーを回避するために空きスペースを能動的に管理する必要があります。

シンプロビジョニングボリュームでスペースリザーブなしのファイルまたはスペースリザーブなしの LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	なし
フラクショナルリザーブ	0
Snapshot リザーブ	任意
Snapshot の自動削除	任意。
自動拡張	任意。

ファイルまたは **LUN** の設定	価値
スペースリザベーション	無効

その他の考慮事項については

ボリュームまたはアグリゲートのスペースが不足すると、ファイルまたは LUN への書き込み処理が失敗する場合があります。

ボリュームとアグリゲートの両方の空きスペースを能動的に監視しない場合は、ボリュームの自動拡張を有効にして、ボリュームの最大サイズをアグリゲートのサイズに設定してください。この設定では、アグリゲートの空きスペースを能動的に監視する必要がありますが、ボリュームの空きスペースを監視する必要はありません。

スペースリザーブファイルまたはスペースリザーブ **LUN** とセミシックボリュームプロビジョニングを組み合わせた場合の構成設定

この FlexVol とファイルまたは LUN の設定の組み合わせでは、フルプロビジョニングとの組み合わせに比べて事前に割り当てるストレージが少なくて済みますが、ボリュームに使用できる効率化テクノロジが制限されます。この設定の組み合わせでは、上書きがベストエフォートベースで行われます。

セミシックプロビジョニングを使用するボリュームでスペースリザーブ LUN を設定するには、次の設定が必要です。

音量設定	価値
保証	ボリューム

音量設定	価値
フラクショナルリザーブ	0
Snapshot リザーブ	0
Snapshot の自動削除	オン。この場合、コミットメントレベルを destroy に設定し、削除リストにすべてのオブジェクトを追加し、トリガーを volume に設定し、すべての FlexClone LUN と FlexClone ファイルの自動削除を有効にします。
自動拡張	オプション。有効にした場合は、アグリゲートの空きスペースを能動的に監視する必要があります。

ファイルまたは **LUN** の設定	価値
スペースリザベーション	有効

テクノロジの制限事項

この設定の組み合わせでは、次のボリュームの Storage Efficiency テクノロジを使用できません。

- 圧縮
- 重複排除
- ODX コピーオフロードと FlexClone コピーオフロード
- 自動削除の対象としてマークされていない FlexClone LUN と FlexClone ファイル（アクティブクローン）
- FlexClone サブファイル
- ODX / コピーオフロード

その他の考慮事項については

この設定の組み合わせを使用する場合は、次の点を考慮する必要があります。

- 対象の LUN をサポートするボリュームのスペースが不足した場合は、保護データ（ FlexClone LUN 、FlexClone ファイル、および Snapshot コピー）が削除されます。
- ボリュームの空きスペースが不足すると、書き込み処理がタイムアウトして失敗することがあります。

AFF プラットフォームではデフォルトで圧縮が有効になります。AFF プラットフォームのセミシックプロビジョニングを使用するボリュームに対しては、明示的に圧縮を無効にする必要があります。

SANのデータ保護

SAN 環境でのデータ保護方法の概要

データを保護するには、データのコピーを作成して、誤ってデータを削除した場合、アプリケーションがクラッシュした場合、データが破損した場合、災害が発生した場合にそのコピーをリストアできるようにします。データ保護およびバックアップのニーズに応じて、 ONTAP では、データを保護するためのさまざまな方法を提供しています。

SnapMirror のビジネス継続性（ **SM-BC** ）

ONTAP 9.9.1の一般提供開始以降では、目標復旧時間ゼロ（ゼロRTO）または透過的アプリケーションフェイルオーバー（TAF）によって、SAN環境でビジネスクリティカルなアプリケーションを自動的にフェイルオーバーできます。SM-BCを使用するには、2つのAFFクラスタまたは2つのオールフラッシュSANアレイ（ASA）クラスタを使用する構成にONTAPメディエーター1.2がインストールされている必要があります。

"ネットアップのマニュアル： SnapMirror Business Continuity"

Snapshot コピー

LUN の複数のバックアップを手動または自動で作成、スケジュール、および保守できます。Snapshot コピーは、最小限のボリュームスペースしか使用せず、パフォーマンスコストもかかりません。LUN データを誤って変更または削除した場合は、最新のいずれかの Snapshot コピーからデータをすばやく簡単にリストアできます。

FlexClone LUN （ **FlexClone** のライセンスが必要）

アクティブボリューム内や Snapshot コピー内にある別の LUN の書き込み可能なポイントインタイムコピーを提供します。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

SnapRestore （ライセンスが必要）

ボリューム全体の Snapshot コピーから高速かつスペース効率に優れたデータリカバリを必要に応じて実行できます。SnapRestore を使用すると、ストレージシステムをリブートしなくても、 LUN を以前保存した状態にリストアできます。

データ保護ミラーコピー（ **SnapMirror** のライセンスが必要）

非同期のディザスタリカバリを提供します。そのために、ボリューム上にあるデータの Snapshot コピーを定期的に作成し、それらの Snapshot コピーを通常は別のクラスタ上にあるパートナーボリュームにローカルエリアネットワークまたはワイドエリアネットワーク経由でコピーして保持します。ソースボリューム上のデータが破損した場合や失われた場合には、パートナーボリューム上のミラーコピーにより、最新の Snapshot コピーの時点におけるデータをすぐに使用およびリストアすることができます。

SnapVault バックアップ（ **SnapMirror** のライセンスが必要）

ストレージ効率に優れた、長期間保持できるバックアップを提供します。SnapVault 関係により、ボリュームの選択した Snapshot コピーをデスティネーションボリュームにバックアップし、保持することができます。

テープバックアップおよびアーカイブ処理を行っている場合は、 SnapVault セカンダリボリュームにすでにバックアップされているデータに対してそれらの処理を実行できます。

SnapDrive for Windows または **UNIX** （ **SnapDrive** ライセンスが必要）

LUN へのアクセスを設定し、 LUN を管理し、ストレージシステムの Snapshot コピーを Windows ホストまたは UNIX ホストから直接管理します。

ネイティブテープバックアップ / リカバリ

ONTAP はほとんどの既存のテープドライブに対応しており、テープベンダーが新しいデバイスのサポートを動的に追加するための方策も用意されています。ONTAP は Remote Magnetic Tape （ RMT ）プロトコルもサポートしているため、 RMT 対応システムへのバックアップやリカバリも可能です。

関連情報

"ネットアップのマニュアル： SnapDrive for UNIX"

"ネットアップのマニュアル： SnapDrive for Windows （現在のリリース）"

"テープバックアップによるデータ保護"

LUN の移動またはコピーが Snapshot コピーに及ぼす影響

LUN の移動またはコピーが **Snapshot** コピーに及ぼす影響の概要

Snapshot コピーはボリュームレベルで作成します。 LUN を別のボリュームにコピーまたは移動すると、デスティネーションボリュームの Snapshot コピーポリシーがコピーまたは移動されたボリュームに適用されます。デスティネーションボリュームの Snapshot コピーが確立されていない場合、移動またはコピーされた LUN の Snapshot コピーは作成されません。

Snapshot コピーから単一の **LUN** をリストアします

ボリューム全体をリストアすることなく、ボリューム内の単一 LUN のみを Snapshot コピーからリストアできます。LUN は、元の場所またはボリューム内の新しいパスにリストアできます。この処理では、ボリューム内の他のファイルまたは LUN に影響を与えることなく、単一の LUN だけがリストアされます。ファイルは、ストリームを使用してリストアすることもできます。

必要なもの

- リストア処理を完了するには、ボリュームに十分なスペースが必要です。
  - フラクショナルリザーブが 0% のスペースリザーブ LUN をリストアする場合、リストアする LUN と同じサイズのスペースが必要です。
  - フラクショナルリザーブが 100% のスペースリザーブ LUN をリストアする場合、リストアする LUN の 2 倍のサイズのスペースが必要です。
  - スペースリザーブなしの LUN をリストアする場合、リストアする LUN が実際に使用しているスペースのみが必要です。
- デスティネーション LUN の Snapshot コピーを作成しておく必要があります。

  リストア処理が失敗すると、デスティネーション LUN が切り捨てられる可能性があります。このような

場合は、 Snapshot コピーを使用してデータ損失を防ぐことができます。

- ソース LUN の Snapshot コピーを作成しておく必要があります。

  まれに、 LUN のリストアに失敗したときに、ソース LUN が使用不能になることがあります。この場合、Snapshot コピーを使用して、リストアを試みる直前の状態に LUN を復帰させることができます。

- デスティネーション LUN とソース LUN の OS タイプが同じである必要があります。

  デスティネーション LUN の OS タイプがソース LUN の OS タイプと異なる場合は、リストア処理後、ホストからデスティネーション LUN へのデータアクセスが失われる可能性があります。

手順

1. ホストから、 LUN へのホストアクセスをすべて停止します。
2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUN のマッピングを解除します。

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. LUN のリストア先にする Snapshot コピーを決定します。

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. LUN をリストアする前に、 LUN の Snapshot コピーを作成します。

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

6. ボリューム内の指定した LUN をリストアします。

   ```
   volume snapshot restore-file -vserver vserver_name -volume volume_name
   -snapshot snapshot_name -path lun_path
   ```

7. 画面の手順に従います。
8. 必要に応じて、 LUN をオンラインにします。

   ```
   lun modify -vserver vserver_name -path lun_path -state online
   ```

9. 必要に応じて、 LUN を再マッピングします。

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

10. ホストから、 LUN を再マウントします。
11. ホストから、 LUN へのアクセスを再開します。

Snapshot コピーからボリューム内のすべての **LUN** をリストアします

を使用できます `volume snapshot restore` 指定したボリューム内のすべてのLUNをSnapshotコピーからリストアするコマンド。

手順

1. ホストから、 LUN へのホストアクセスをすべて停止します。

   SnapRestore を使用している場合は、ボリューム内の LUN へのすべてのホストアクセスを停止しないと、原因によるデータの破損やシステムエラーが発生する可能性があります

2. ホスト上の LUN をアンマウントして、ホストが LUN にアクセスできないようにします。
3. LUN のマッピングを解除します。

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. ボリュームのリストア先にする Snapshot コピーを決定します。

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

6. データをリストアします。

   ```
   volume snapshot restore -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

7. 画面の指示に従います。
8. LUN を再マッピングします。

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

9. LUN がオンラインであることを確認します。

   ```
   lun show -vserver vserver_name -path lun_path -fields state
   ```

10. LUN がオンラインになっていない場合は、オンラインにします。

    ```
    lun modify -vserver vserver_name -path lun_path -state online
    ```

11. 権限の設定を admin に変更します。

    ```
    set -privilege admin
    ```

12. ホストから、 LUN を再マウントします。
13. ホストから、 LUN へのアクセスを再開します。

ボリュームから既存の **Snapshot** コピーを削除します

ボリュームから既存の Snapshot コピーを手動で削除できます。この処理は、ボリュームのスペースを増やす必要がある場合などに実行します。

手順

1. を使用します `volume snapshot show` コマンドを使用して、削除するSnapshotコピーを確認します。

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                Size   Total% Used%
-------- ------- ----------------------- -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB   0%    32%
                 snap2.2013-05-09_0010   76KB   0%    32%
                 snap2.2013-05-10_0010   76KB   0%    32%
                 snap3.2013-05-10_1005   72KB   0%    31%
                 snap3.2013-05-10_1105   72KB   0%    31%
                 snap3.2013-05-10_1205   72KB   0%    31%
                 snap3.2013-05-10_1305   72KB   0%    31%
                 snap3.2013-05-10_1405   72KB   0%    31%
                 snap3.2013-05-10_1505   72KB   0%    31%
10 entries were displayed.
```

2. を使用します `volume snapshot delete` Snapshotコピーを削除するコマンド。

状況	入力するコマンド
1 つの Snapshot コピーを削除します	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name`*
複数の Snapshot コピーを削除する	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name1`*`[,`*`snapshot_name2`*`,…]`
すべての Snapshot コピーを削除します	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot *`

次の例は、ボリューム vol3 上のすべての Snapshot コピーを削除します。

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *

10 entries were acted on.
```

FlexClone LUN を使用してデータを保護します

FlexClone LUN を使用してデータの概要を保護します

FlexClone LUN は、アクティブボリューム内や Snapshot コピー内にある別の LUN の書き込み可能なポイントインタイムコピーです。クローンとその親は、相互に影響を及ぼさずに個別に変更できます。

FlexClone LUN は、最初は親 LUN とスペースを共有します。デフォルトでは、 FlexClone LUN は親 LUN のスペースリザーブ属性を継承します。たとえば、親 LUN がスペースリザーブなしの場合は、 FlexClone LUN もデフォルトでスペースリザーブなしになります。ただし、スペースリザーブ LUN である親から、スペースリザーブなしの FlexClone LUN を作成することもできます。

LUN クローンの作成時にはバックグラウンドでブロック共有が発生し、ブロック共有が終了するまでボリュームの Snapshot コピーは作成できません。

でFlexClone LUNの自動削除機能を有効にするには、ボリュームを設定する必要があります `volume snapshot autodelete modify` コマンドを実行します有効にしない場合、 FlexClone LUN を自動削除したくても、ボリュームで FlexClone の自動削除が有効になっていないため、 FlexClone LUN は削除されません。

FlexClone LUN を作成すると、 FlexClone LUN の自動削除機能がデフォルトで無効になります。FlexClone LUN を自動削除できるようにするには、 FlexClone LUN ごとに FlexClone LUN を手動で有効にする必要があります。ボリュームのセミシックプロビジョニングを使用している場合に、このオプションが提供する「ベストエフォート」の書き込み保証が必要な場合は、 _ALL_FlexClone LUN を自動削除できるようにする必要があります。

> Snapshot コピーから FlexClone LUN を作成すると、スペース効率に優れたバックグラウンドプロセスを使用して、 LUN が自動的に Snapshot コピーからスプリットされます。そのため、LUN が Snapshot コピーに依存したり、追加スペースを消費したりすることはなくなります。このバックグラウンドスプリットが終了する前に Snapshot コピーが自動的に削除された場合、その FlexClone LUN は、 FlexClone LUN の自動削除機能が無効になっていても削除されます。バックグラウンドスプリットが完了したあとは、 Snapshot コピーが削除されても、FlexClone LUN は削除されません。

関連情報

"論理ストレージ管理"

FlexClone LUN を使用する理由

FlexClone LUN を使用すると、 LUN の読み書き可能なコピーを複数作成できます。

これは、次のような場合に行います。

- テストを目的として LUN の一時的なコピーを作成する必要があります。

- 本番環境のデータへのアクセスを許可することなく、追加のユーザがデータのコピーを利用できるようにする必要があります。
- 変更および開発作業用にデータベースのクローンを作成し、元のデータを未変更のまま残す場合
- LUN データの特定のサブセット（ボリュームグループ内の特定の論理ボリュームまたはファイルシステム）にアクセスする場合。 またはファイルシステム内の特定のファイルまたはファイルセット）を選択し、元の LUN の残りのデータをリストアせずに、元の LUN にコピーします。これは、 LUN とその LUN クローンを同時にマウントできるオペレーティングシステムで機能します。SnapDrive for UNIXはでこれをサポートしています `snap connect` コマンドを実行します
- 同じオペレーティングシステム上に複数の SAN ブートホストが必要な場合。

自動削除設定を使用して **FlexVol** ボリュームの空きスペースを再生する方法

FlexVol の自動削除設定を有効にすると、 FlexClone ファイルおよび FlexClone LUN を自動的に削除できます。自動削除を有効にすると、ボリュームがフルに近くなったときに、指定した量の空きスペースをボリューム内に再生できます。

ボリュームの空きスペースが一定のしきい値を下回ったときに FlexClone ファイルおよび FlexClone LUN の削除を自動的に開始し、ボリュームの空きスペースを指定の量だけ再生したらクローンの削除を自動的に中止するように設定できます。クローンの自動削除を開始するしきい値を指定することはできませんが、それぞれのクローンを削除対象に含めるかどうかと、ボリュームの空きスペースの目標量を指定することができます。

ボリュームの空きスペースが一定のしきい値を下回ったとき、および次の要件の両方に達したときに、FlexClone ファイルおよび FlexClone LUN が自動的に削除されます。

- FlexClone ファイルおよび FlexClone LUN が格納されているボリュームに対して自動削除機能が有効になっている。

  FlexVol に対して自動削除機能を有効にするには、を使用します `volume snapshot autodelete modify` コマンドを実行しますを設定する必要があります `-trigger` パラメータの値 `volume` または `snap_reserve` ボリュームがFlexCloneファイルおよびFlexClone LUNを自動的に削除するように設定します。

- FlexClone ファイルおよび FlexClone LUN に対して自動削除機能が有効になっている。

  FlexCloneファイルまたはFlexClone LUNに対して自動削除を有効にするには、を使用します `file clone create` コマンドにを指定します `-autodelete` パラメータこのクローン設定はボリュームの他の設定よりも優先されるため、この設定で個別に自動削除を無効にすることで、特定の FlexClone ファイルや FlexClone LUN を保持することができます。

FlexClone ファイルおよび **FlexClone LUN** を自動的に削除するように **FlexVol** を設定する

ボリュームの空きスペースが特定のしきい値を下回った場合に、自動削除を有効にした FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定できます。

必要なもの

- FlexVol ボリュームに FlexClone ファイルおよび FlexClone LUN が含まれていて、オンラインになっている必要があります。

- FlexVol ボリュームを読み取り専用ボリュームにすることはできません。

手順

1. を使用して、FlexVol ボリューム内のFlexCloneファイルおよびFlexClone LUNの自動削除を有効にします `volume snapshot autodelete modify` コマンドを実行します
   - をクリックします `-trigger` パラメータを指定することもできます `volume` または `snap_reserve`。
   - をクリックします `-destroy-list` パラメータは常に指定する必要があります `lun_clone,file_clone` 削除するクローンのタイプが1つだけであるかどうかは関係ありません。[+]
     次の例は、ボリューム vol1 で FlexClone ファイルおよび FlexClone LUN の自動削除を有効にし、ボリュームの 25% が空きスペースになるまでスペースが再生されるようにします。

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

> FlexVol ボリュームの自動削除を有効にする際に、の値を設定した場合 `-commitment` パラメータの値 `destroy`を使用して、すべての`FlexClone`ファイルおよび`FlexClone LUN`を削除します `-autodelete` パラメータをに設定します `true` ボリュームの空きスペースが指定したしきい値を下回った場合に削除されることがあります。ただし、FlexCloneファイルとFlexClone LUNはを使用します `-autodelete` パラメータをに設定します `false` は削除されません。

2. を使用して、FlexVol ボリュームでFlexCloneファイルおよびFlexClone LUNの自動削除が有効になっていることを確認します `volume snapshot autodelete show` コマンドを実行します

   次の例では、ボリューム vol1 で FlexClone ファイルおよび FlexClone LUN の自動削除が有効になっています。

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)*
    Target Free Space: 25%
              Trigger: volume
     Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. 次の手順を実行して、ボリューム内の削除対象とする FlexClone ファイルおよび FlexClone LUN の自動削除を有効にします。

   a. を使用して、特定のFlexCloneファイルまたはFlexClone LUNの自動削除を有効にします `volume file clone autodelete` コマンドを実行します

      を使用して、特定のFlexCloneファイルまたはFlexClone LUNを強制的に自動削除することができます `volume file clone autodelete` コマンドにを指定します `-force` パラメータ

      次の例は、ボリューム vol1 に含まれる FlexClone LUN lun1_clone の自動削除が有効になっていることを示します。

      ```
      cluster1::> volume file clone autodelete -vserver vs1 -clone-path
      /vol/vol1/lun1_clone -enabled true
      ```

      FlexClone ファイルおよび FlexClone LUN の作成時に自動削除を有効にすることができます。

   b. を使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が有効になっていることを確認します `volume file clone show-autodelete` コマンドを実行します

      次の例は、 FlexClone LUN lun1_clone で自動削除が有効になっていることを示します。

      ```
      cluster1::> volume file clone show-autodelete -vserver vs1 -clone
      -path vol/vol1/lun1_clone
                                                                Vserver
      Name: vs1
                                                                Clone
      Path: vol/vol1/lun1_clone

      **Autodelete Enabled: true**
      ```

コマンドの使用の詳細については、該当するマニュアルページを参照してください。

アクティブボリュームから **LUN** のクローンを作成します

アクティブボリュームの LUN をクローニングして、 LUN のコピーを作成できます。こうして作成された FlexClone LUN は、アクティブボリューム内の元の LUN の読み書き可能なコピーです。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスには、 "ONTAP One"。

このタスクについて

スペースリザーブされた FlexClone LUN には、親のスペースリザーブ LUN と同量のスペースが必要です。FlexClone LUN のスペースをリザーブしない場合は、 FlexClone LUN に対する変更を保存するために十分なスペースがボリュームにあることを確認する必要があります。

手順

1. クローンを作成する前に、 LUN が igroup にマッピングされていないこと、またはに書き込まれていないことを確認する必要があります。
2. を使用します `lun show` コマンドを実行してLUNが存在することを確認します。

   `lun show -vserver vs1`

   ```
   Vserver   Path                State      Mapped     Type      Size
   -------- ------------------ --------- --------- -------- -------
   vs1       /vol/vol1/lun1     online    unmapped  windows  47.07MB
   ```

3. を使用します `volume file clone create` コマンドを使用してFlexClone LUNを作成します。

   `volume file clone create -vserver vs1 -volume vol1 -source-path lun1 -destination-path/lun1_clone`

   FlexClone LUNを自動削除に使用できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してこの FlexClone LUN をボリューム内に作成する場合は、すべての FlexClone LUN で自動削除を有効にする必要があります。

4. を使用します `lun show` コマンドを実行して、LUNが作成されたことを確認します。

   `lun show -vserver vs1`

   ```
   Vserver   Path                      State    Mapped   Type      Size
   -------- ------------------------ -------- -------- -------- ------
   vs1       /vol/volX/lun1           online   unmapped windows  47.07MB
   vs1       /vol/volX/lun1_clone     online   unmapped windows  47.07MB
   ```

ボリューム内の **Snapshot** コピーから **FlexClone LUN** を作成します

ボリューム内の Snapshot コピーを使用して、 LUN の FlexClone コピーを作成できます。LUN の FlexClone コピーは読み書き可能です。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスは、 "ONTAP One"。

このタスクについて

FlexClone LUN は、親 LUN のスペースリザベーション属性を継承します。スペースリザーブされた FlexClone LUN には、親のスペースリザーブ LUN と同量のスペースが必要です。FlexClone LUN のスペースをリザーブしない場合は、クローンに対する変更を保存するために十分なスペースがボリュームに必要です。

手順

1. LUN がマッピングされていないか、書き込まれていないことを確認します。
2. LUN が含まれているボリュームの Snapshot コピーを作成します。

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot
snapshot_name
```

クローニングする LUN の Snapshot コピー（元の Snapshot コピー）を作成する必要があります。

3. Snapshot コピーから FlexClone LUN を作成します。

```
file clone create -vserver vserver_name -volume volume_name -source-path
source_path -snapshot-name snapshot_name -destination-path destination_path
```

FlexClone LUNを自動削除に使用できるようにする必要がある場合は、を含めます `-autodelete true`。セミシックプロビジョニングを使用してこの FlexClone LUN をボリューム内に作成する場合は、すべての FlexClone LUN で自動削除を有効にする必要があります。

4. FlexClone LUN が正しいことを確認します。

```
lun show -vserver vserver_name
```

```
Vserver Path                        State    Mapped    Type     Size
------- ----------------------      -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone        online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

特定の **FlexClone** ファイルまたは **FlexClone LUN** を自動削除の対象から除外します

FlexClone ファイルおよび FlexClone LUN を自動的に削除するように FlexVol を設定すると、指定した条件を満たすすべてのクローンが削除される可能性があります。特定の FlexClone ファイルまたは FlexClone LUN を残したい場合は、それらを FlexClone の自動削除プロセスから除外できます。

必要なもの

FlexClone ライセンスがインストールされている必要があります。このライセンスは、 "ONTAP One"。

このタスクについて

FlexClone ファイルまたは FlexClone LUN を作成すると、クローンの自動削除設定がデフォルトで無効になります。自動削除を無効にした FlexClone ファイルと FlexClone LUN は、ボリュームのスペースを再生するためにクローンを自動的に削除するように FlexVol を設定しても保持されます。

> を設定した場合は `commitment` ボリュームのレベルをに設定します `try` または `disrupt``特定の`FlexClone`ファイルまたは`FlexClone LUN`を個別に保持するには、それらのクローンの自動削除を無効にします。ただし、を設定した場合 `commitment` ボリュームのレベルをに設定します `destroy` 削除リストには次のものが含まれます `lun_clone,file_clone`では、ボリューム設定はクローン設定よりも優先され、クローンの自動削除設定に関係なく、すべてのFlexCloneファイルとFlexClone LUNが削除されます。

手順

1. を使用して、特定のFlexCloneファイルまたはFlexClone LUNを自動的に削除しないように設定します

`volume file clone autodelete` コマンドを実行します

次の例は、 vol1 に含まれている FlexClone LUN lun1_clone の自動削除を無効にする方法を示しています。

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

自動削除を無効にした FlexClone ファイルまたは FlexClone LUN は、ボリュームのスペース再生を目的とした自動削除の対象になりません。

2. を使用して、FlexCloneファイルまたはFlexClone LUNで自動削除が無効になっていることを確認します `volume file clone show-autodelete` コマンドを実行します

   次の例では、 FlexClone LUN lun1_clone の自動削除が false になっています。

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone Path:
vol/vol1/lun1_clone
                                                                Autodelete
Enabled: false
```

SAN 環境で SnapVault バックアップを構成して使用する

SAN 環境での SnapVault バックアップの構成と使用の概要

SAN 環境で SnapVault を設定して使用する方法は、 NAS 環境の場合とほぼ同じですが、 SAN 環境で LUN をリストアする場合は、いくつか特別な手順を踏む必要があります。

SnapVault バックアップには、ソースボリュームの読み取り専用コピーのセットが含まれています。SAN 環境では、必ず、個々の LUN ではなくボリューム全体を SnapVault のセカンダリボリュームにバックアップします。

LUN を含むプライマリボリュームと、 SnapVault バックアップとして動作するセカンダリボリュームの間に SnapVault 関係を作成して初期化する手順は、ファイルプロトコルに使用される FlexVol ボリュームで使用される手順と同じです。この手順の詳細については、を参照してください "データ保護"。

Snapshot コピーを作成して SnapVault セカンダリボリュームにコピーする前に、 LUN がバックアップされ、一貫した状態であることを確認することが重要です。Snapshotコピーの作成をSnapCenter で自動化すると、バックアップされたLUNが確実に過不足なく、元のアプリケーションで使用可能な状態になります。

SnapVault セカンダリボリュームから LUN をリストアする場合には、 3 つの基本の選択肢があります。

- SnapVault セカンダリボリュームから LUN を直接マッピングし、ホストを LUN に接続して LUN の内容にアクセスできます。

  この LUN は読み取り専用であり、 SnapVault バックアップ内の最新の Snapshot コピーからのみマッピングできます。永続的予約およびその他の LUN のメタデータは失われます。必要に応じて、元の LUN に引き続きアクセス可能であれば、ホスト上でコピープログラムを使用して LUN の内容を元の LUN にコピーすることができます。

  LUN のシリアル番号がソース LUN のものと異なります。

- SnapVault セカンダリボリューム内の任意の Snapshot コピーを、新しい読み書き可能ボリュームにクローニングします。

  その後、ボリューム内の任意の LUN をマッピングし、ホストを LUN に接続して LUN の内容にアクセスできます。必要に応じて、元の LUN に引き続きアクセス可能であれば、ホスト上でコピープログラムを使用して LUN の内容を元の LUN にコピーすることができます。

- SnapVault セカンダリボリューム内の任意の Snapshot コピーから、 LUN が含まれているボリューム全体をリストアできます。

  ボリューム全体をリストアすると、ボリューム内のすべての LUN とすべてのファイルが置き換えられます。Snapshot コピーの作成後に作成された新しい LUN はすべて失われます。

  LUN では、マッピング、シリアル番号、 UUID 、永続的予約が維持されます。

SnapVault バックアップから読み取り専用の **LUN** コピーにアクセスする

LUN の読み取り専用コピーには、 SnapVault バックアップ内の最新の Snapshot コピーからアクセスできます。LUN の ID 、パス、およびシリアル番号はソース LUN のものとは異なり、あらかじめマッピングしておく必要があります。永続的予約、 LUN マッピング、および igroup は、 SnapVault セカンダリボリュームにレプリケートされません。

必要なもの

- SnapVault 関係が初期化されていて、 SnapVault セカンダリボリューム内の最新の Snapshot コピーに目的の LUN が含まれている必要があります。
- SnapVault バックアップがある Storage Virtual Machine （ SVM ）に、適切な SAN プロトコル対応の LIF が 1 個以上あり、 LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- SnapVault セカンダリボリュームから LUN コピーに直接アクセスする場合、 SnapVault SVM に事前に igroup を作成しておく必要があります。

  LUN には SnapVault セカンダリボリュームから直接アクセスできます。 LUN を含むボリュームのリストアやクローニングを行う必要はありません。

このタスクについて

SnapVault セカンダリボリュームに新しい Snapshot コピーが追加されたときに、以前の Snapshot コピーに LUN がマッピングされている場合、マッピングされた LUN の内容が変更されます。LUN は引き続き同じ ID でマッピングされますが、データは新しい Snapshot コピーから取得されます。LUN のサイズが変更された場合、一部のホストはサイズの変更を自動的に検出します。 Windows ホストでは、サイズ変更を検知するためにディスクの再スキャンが必要です。

手順

1. を実行します `lun show` コマンドを実行して、SnapVault セカンダリボリューム内の使用可能なLUNをリスト表示します。

   この例では、プライマリボリューム srcvolA 内の元の LUN と、 SnapVault セカンダリボリューム dstvolB 内のコピーされた LUN の両方が表示されています。

```
cluster::> lun show

Vserver   Path                  State   Mapped   Type          Size
--------  ------------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

2. 目的のホストのigroupが、SnapVault セカンダリボリュームがあるSVM内にまだ存在していない場合は、を実行します `igroup create` igroupを作成するコマンドです。

   このコマンドでは、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成します。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. を実行します `lun mapping create` コマンドを実行して、目的のLUNコピーをigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

4. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

SnapVault バックアップから単一の **LUN** をリストアする

単一の LUN を新しい場所または元の場所にリストアできます。SnapVault セカンダリボリューム内の任意の Snapshot コピーを使用してリストアできます。LUN を元の場所にリストアするには、まず新しい場所にリストアしてから、元の場所にコピーします。

必要なもの

- SnapVault 関係が初期化されていて、 SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。
- SnapVault セカンダリボリュームがある Storage Virtual Machine （ SVM ）に、適切な SAN プロトコル対応の LIF が 1 個以上あり、 LUN コピーへのアクセスに使用するホストからこの LIF にアクセスできることが必要です。
- igroup が SnapVault SVM 上にすでに存在している必要があります。

このタスクについて

このプロセスでは、 SnapVault セカンダリボリューム内の Snapshot コピーから、読み書き可能なボリュームクローンを作成します。このクローン内の LUN を直接使用することも、必要に応じて LUN の内容を元の LUN の場所にコピーすることもできます。

クローン内の LUN のパスとシリアル番号は、元の LUN のものとは異なります。永続的予約は維持されません。

手順

1. を実行します `snapmirror show` コマンドを使用して、SnapVault バックアップが含まれているセカンダリボリュームを検証します。

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

2. を実行します `volume snapshot show` コマンドを使用して、LUNのリストア元となるSnapshotコピーを特定します。

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                 State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. を実行します `volume clone create` 目的のSnapshotコピーから読み書き可能クローンを作成するコマンド。

   ボリュームクローンは、 SnapVault バックアップと同じアグリゲート内に作成されます。アグリゲート内

に、クローンを格納できるだけの十分なスペースが必要です。

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. を実行します `lun show` コマンドを実行して、ボリュームクローン内のLUNをリスト表示します。

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                        State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

5. 目的のホストのigroupがSnapVault バックアップがあるSVMにまだ存在していない場合は、を実行します `igroup create` igroupを作成するコマンドです。

   この例では、 iSCSI プロトコルを使用する Windows ホスト用の igroup を作成しています。

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. を実行します `lun mapping create` コマンドを実行して、目的のLUNコピーをigroupにマッピングします。

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. ホストを LUN に接続し、適宜 LUN の内容にアクセスします。

   この LUN は読み書き可能であり、元の LUN の代わりに使用できます。LUN のシリアル番号が異なるため、ホストはこの LUN が元の LUN とは別の LUN であると解釈します。

8. ホスト上でコピープログラムを使用して、 LUN の内容を元の LUN にコピーします。

ボリューム内のすべての **LUN** を **SnapVault** バックアップからリストアします

ボリューム内の 1 つ以上の LUN を SnapVault バックアップからリストアする必要があ

る場合は、ボリューム全体をリストアできます。ボリュームをリストアする場合は、ボリューム内のすべての LUN が対象になります。

必要なもの

SnapVault 関係が初期化されていて、 SnapVault セカンダリボリュームに、リストアに使用する適切な Snapshot コピーが含まれている必要があります。

このタスクについて

ボリューム全体をリストアすると、ボリュームの状態は、リストアに使用した Snapshot コピーが作成された時点の状態に戻ります。Snapshot コピーの作成後にボリュームに追加された LUN がある場合、その LUN はリストアの過程で削除されます。

ボリュームのリストア後も、 LUN と igroup とのマッピングはリストアの直前と同じ状態が維持されます。LUN のマッピングは、 Snapshot コピー作成時点のマッピングとは異なる場合があります。ホストクラスタによる LUN の永続的予約は維持されます。

手順

1. ボリューム内のすべての LUN に対する I/O を停止します。
2. を実行します `snapmirror show` コマンドを実行して、SnapVault セカンダリボリュームが含まれているセカンダリボリュームを確認します。

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

3. を実行します `volume snapshot show` コマンドを使用して、リストア元のSnapshotコピーを特定します。

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                 State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. を実行します `snapmirror restore` コマンドを入力し、を指定します `-source-snapshot` 使用するSnapshotコピーを指定するオプション。

リストア先として指定するのは、リストア先の元のボリュームです。

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. ホストクラスタ間で LUN を共有している場合は、影響を受けるホストから LUN に対する永続的予約をリストアします。

SnapVault バックアップからのボリュームのリストア

次の例では、 Snapshot コピーの作成後に lun_D という名前の LUN がボリュームに追加されています。Snapshot コピーからボリューム全体をリストアしたあと、 lun_D は表示されなくなります。

を参照してください `lun show` コマンドの出力では、プライマリボリュームsrcvolA内のLUNと、SnapVaultセカンダリボリュームdstvolB内のそれらのLUNの読み取り専用コピーを確認できます。SnapVault バックアップに lun_D のコピーはありません。

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------  ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------  ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

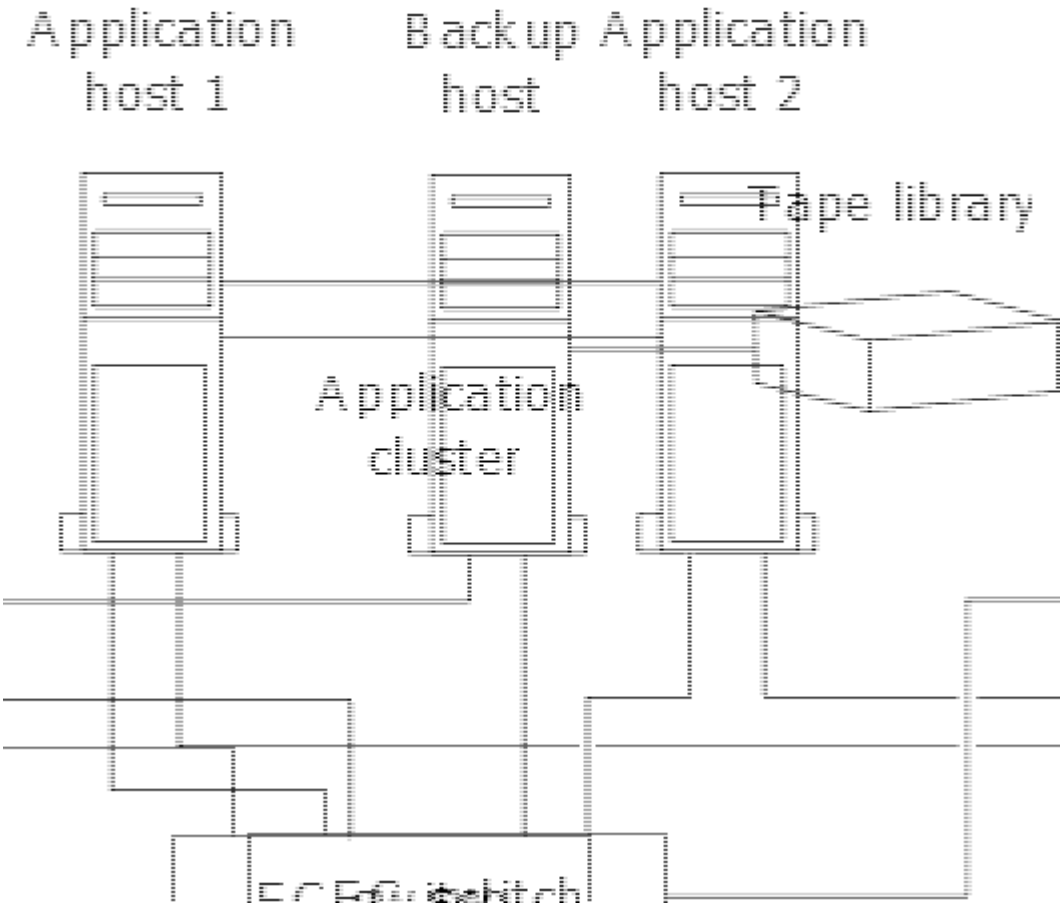
ボリュームが SnapVault セカンダリボリュームからリストアされると、ソースボリュームには lun_D が存在しなくなりますリストア後もソースボリューム内の LUN のマッピングは維持されるため、再マッピングする必要はありません。

ホストバックアップシステムをプライマリストレージシステムに接続する方法

テープへの SAN システムのバックアップは、アプリケーションホストのパフォーマンス低下を避けるため、別のバックアップホストで実行できます。

SAN と NAS のデータは、バックアップ目的で分けておくことが必須です。次の図に、プライマリストレージシステムに接続するホストバックアップシステムに推奨される物理構成を示します。ボリュームは SAN 専用

として設定する必要があります。LUN は単一のボリュームに限定することも、複数のボリュームまたはストレージシステムに分散して設定することもできます。



ホスト上のボリュームは、ストレージシステムからマッピングされた単一の LUN 、または HP-UX システム上の VxVM などのボリュームマネージャを使用して複数の LUN で構成できます。

ホストバックアップシステムを介して **LUN** をバックアップする

ホストバックアップシステムのソースデータとして、 Snapshot コピー内のクローン LUN を使用できます。

必要なもの

本番用 LUN が必要です。アプリケーションサーバの WWPN またはイニシエータノード名を含む igroup にマッピングされている必要があります。また、 LUN がフォーマット済みで、ホストにアクセスできる必要があります

手順

1. ホストファイルシステムバッファの内容をディスクに保存します。

   ホストオペレーティングシステムのコマンドを使用するか、 SnapDrive for Windows または SnapDrive for UNIX を使用できます。この手順を SAN バックアップのプリプロセススクリプトに含めることもできます。

2. を使用します `volume snapshot create` コマンドを使用して本番用LUNのSnapshotコピーを作成します。

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
-comment "Single snapshot" -foreground false
```

3. を使用します `volume file clone create` 本番用LUNのクローンを作成するコマンド。

   ```
   volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot
   -name snap_vol3 -destination-path lun1_backup
   ```

4. を使用します `lun igroup create` バックアップサーバのWWPNを含むigroupを作成するコマンド。

   ```
   lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows
   -initiator 10:00:00:00:c9:73:5b:91
   ```

5. を使用します `lun mapping create` 手順3で作成したLUNクローンをバックアップホストにマッピングするコマンド。

   ```
   lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
   ```

   この手順を SAN バックアップアプリケーションのポストプロセススクリプトに含めることができます。

6. ホストから、新しい LUN を検出し、ファイルシステムをホストで使用できるようにします。

   この手順を SAN バックアップアプリケーションのポストプロセススクリプトに含めることができます。

7. SAN バックアップアプリケーションを使用して、バックアップホストの LUN クローン内のデータをテープにバックアップします。
8. を使用します `lun modify` LUNクローンをオフラインにするコマンド。

   ```
   lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
   ```

9. を使用します `lun delete` をクリックしてLUNクローンを削除します。

   ```
   lun delete -vserver vs3 -volume vol3 -lun lun1_backup
   ```

10. を使用します `volume snapshot delete` コマンドを実行してSnapshotコピーを削除します。

    ```
    volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
    ```

SAN 構成リファレンス

SANコウセイノカイヨウ

Storage Area Network（SAN；ストレージエリアネットワーク）は、iSCSIやFCなどのSAN転送プロトコルを使用してホストに接続されるストレージ解決策で構成されます。ストレージ解決策が1つ以上のスイッチを介してホストに接続されるようにSANを設定できます。 iSCSIを使用している場合は、スイッチを使用せずにストレージ解決策がホストに直接接続されるようにSANを設定することもできます。

SANでは、Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストからスト

レージ解決策に同時にアクセスできます。 を使用できます "選択的LUNマッピング" および "ポートセット" ホストとストレージの間のデータアクセスを制限します。

iSCSIの場合、ストレージ解決策とホスト間のネットワークトポロジをネットワークと呼びます。 FC、FC / NVMe、FCoEの場合、ストレージ解決策とホストの間のネットワークトポロジをファブリックと呼びます。 冗長性を確保してデータアクセスの中断からデータを保護するには、マルチネットワークまたはマルチファブリック構成のHAペアを使用してSANをセットアップする必要があります。 シングルノードまたはシングルネットワーク/ファブリックを使用する構成は完全な冗長性がないため、推奨されません。

SANの設定が完了したら、次の操作を実行できます。 "iSCSIまたはFC用のストレージのプロビジョニング"または、次の操作を実行できます "FC / NVMe用のストレージのプロビジョニング"。 その後、ホストに接続してデータの提供を開始できます。

SANプロトコルのサポートは、ONTAPのバージョン、プラットフォーム、構成によって異なります。具体的な構成の詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

関連情報

- "SAN の管理の概要"
- "NVMeの構成、サポート、制限事項"

iSCSIコウセイ

iSCSI SANホストの構成方法

iSCSI構成では、iSCSI SANホストに直接接続するか、1つ以上のIPスイッチを介してホストに接続するハイアベイラビリティ（HA）ペアを使用します。

"HA ペア" ホストがLUNへのアクセスに使用するアクティブ/最適化パスとアクティブ/非最適パスのレポートノードとして定義されます。Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから同時にストレージにアクセスできます。 ホストでは、ALUAをサポートするサポート対象のマルチパス解決策がインストールおよび設定されている必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、 "NetApp Interoperability Matrix Tool で確認できます"。

マルチネットワーク構成では、ホストをストレージシステムに接続するスイッチが複数あります。 完全な冗長性を備えたマルチネットワーク構成を推奨します。 シングルネットワーク構成では、1台のスイッチでホストをストレージシステムに接続します。 シングルネットワーク構成では完全な冗長性は確保されません。

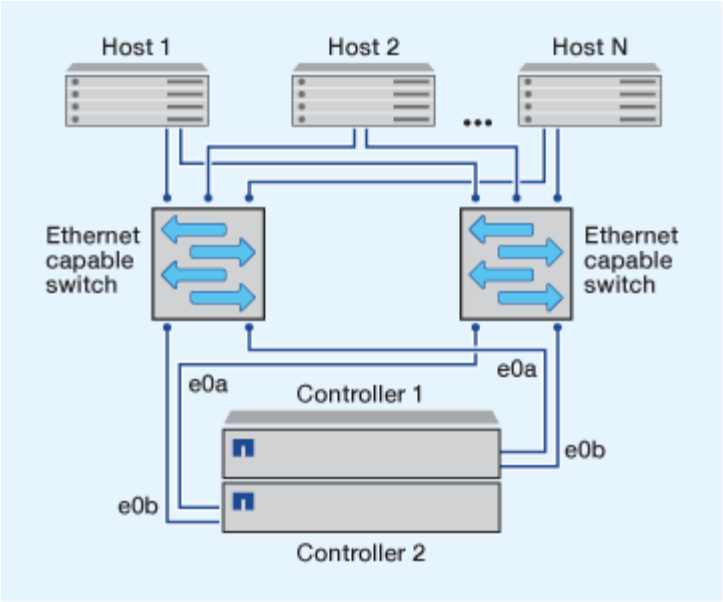
> "シングルノードコウセイ" は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- 詳細をご確認ください "選択的LUNマッピング（SLM）" HAペアが所有するLUNへのアクセスに使用するパスを制限します。
- 詳細はこちら "SAN LIF"。
- の詳細を確認してください "iSCSIにおけるVLANの利点"。

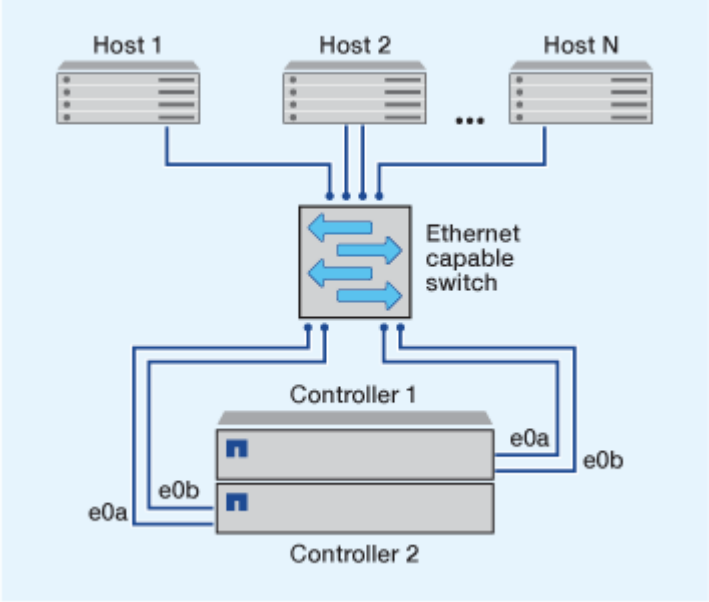
マルチネツトワアクiSCSIコウセイ

マルチネットワークの HA ペア構成では、 HA ペアを複数のスイッチで 1 つまたは複数のホストに接続します。スイッチが複数あるため、この構成では完全な冗長性が確保されます。



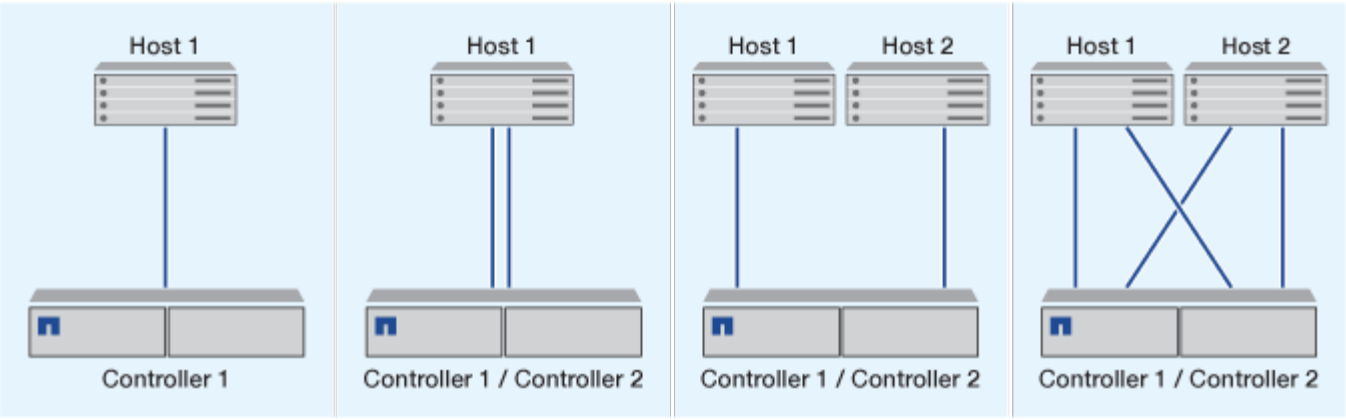
タンイチネツトワアクノ**iSCSI**コウセイ

単一ネットワークの HA ペア構成では、 HA ペアを 1 台のスイッチで 1 つまたは複数のホストに接続します。スイッチが 1 台しかないため、この構成では完全な冗長性は確保されません。



直接接続型**iSCSI**構成

直接接続型の構成では、 1 つ以上のホストをコントローラに直接接続します。



iSCSI 構成で **VLAN** を使用する利点

VLAN は、ブロードキャストドメインにグループ化されたスイッチポートのグループで構成されます。VLAN は、単一のスイッチに設定することも、複数のスイッチシャーシにまたがって設定することもできます。静的な VLAN と動的な VLAN を使用すると、 IP ネットワークインフラ内でのセキュリティの強化、問題の切り分け、および使用可能なパスの制限が可能になります。

大規模な IP ネットワークインフラに VLAN を実装する利点は次のとおりです。

- セキュリティの向上：

  VLAN を使用すると、イーサネットネットワークまたは IP SAN のノード間のアクセスが制限されるため、既存のインフラを利用しながらセキュリティを強化できます。

- 問題を切り分けることで、イーサネットネットワークや IP SAN の信頼性が高まります。
- 問題の範囲を制限することで、問題解決時間を短縮できます。
- 特定の iSCSI ターゲットポートへの使用可能なパスの数が削減されます。
- ホストで使用されるパスの最大数が削減されます。

  パスが多すぎると再接続の時間が遅くなります。ホストにマルチパス解決策がない場合は、 VLAN を使用して 1 つのパスのみを許可できます。

動的 **VLANs**

動的な VLAN は MAC アドレスに基づいています。VLAN は、 VLAN に含めるメンバーの MAC アドレスを指定して定義できます。

動的な VLAN は柔軟性に優れており、デバイスがスイッチに物理的に接続されている物理ポートにマッピングする必要はありません。ケーブルを別のポートに接続するときに VLAN を再構成する必要はありません。

静的な **VLAN**

静的な VLAN はポートベースです。スイッチポートとスイッチポートを使用して、 VLAN とそのメンバーを定義します。

静的な VLAN を使用すると、 MAC （メディアアクセス制御）のスプーフィングを使用した VLAN への不正

アクセスを防止できるため、セキュリティが向上します。ただし、第三者がスイッチに物理的にアクセスできる場合は、ケーブルを交換してネットワークアドレスを再設定することでアクセスが可能になります。

環境によっては、静的な VLAN は動的な VLAN よりも簡単に作成および管理できます。静的な VLAN では、48 ビットの MAC アドレスではなく、スイッチとポートの識別子のみを指定する必要があるからです。また、 VLAN の識別子をスイッチのポート範囲のラベルとして設定することもできます。

FCコウセイ

FCおよびFC-NVMe SANホストの構成方法

FCおよびFC-NVMe SANホストは、HAペアと少なくとも2つのスイッチを使用して設定することを推奨します。 これにより、ファブリックレイヤとストレージシステムレイヤで冗長性が確保され、フォールトトレランスとノンストップオペレーションがサポートされます。FC または FC-NVMe SAN ホストをスイッチを使用せずに HA ペアに直接接続することはできません。

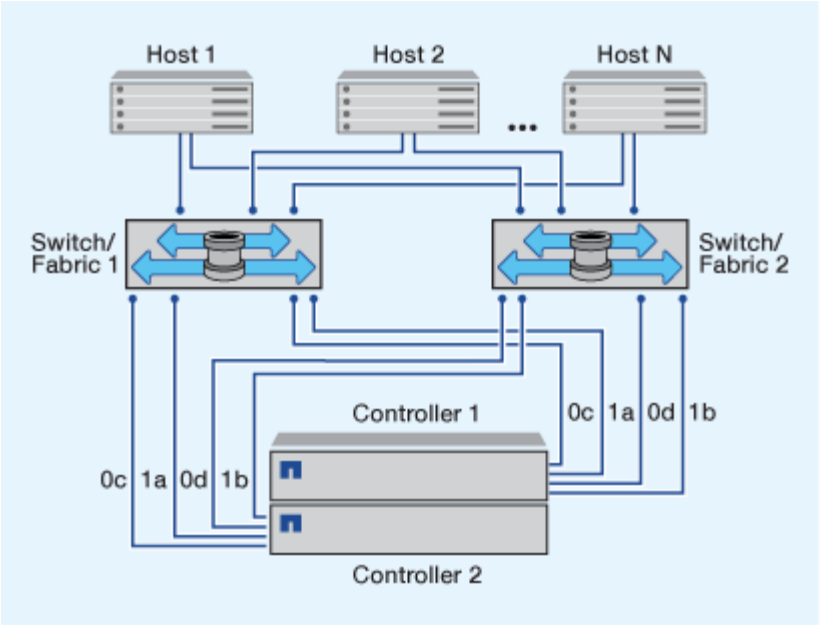
カスケードファブリック、部分メッシュファブリック、フルメッシュファブリック、コアエッジファブリック、およびディレクタファブリックは、 FC スイッチをファブリックに接続する業界標準の方法であり、いずれもサポートされます。 異機種混在の FC スイッチファブリックの使用は、組み込みのブレードスイッチ以外はサポートされていません。 特定の例外については、を参照してください "Interoperability Matrix Tool で確認してください"。 ファブリックは 1 つまたは複数のスイッチで構成できます。また、ストレージコントローラは複数のスイッチに接続することができます。

Windows、Linux、UNIXなど、異なるオペレーティングシステムを使用する複数のホストから、ストレージコントローラに同時にアクセスできます。 ホストには、サポートされるマルチパス解決策をインストールおよび設定する必要があります。サポートされるオペレーティングシステムとマルチパスソリューションは、Interoperability Matrix Toolで確認できます。

マルチファブリックノFCコウセイオヨビFC-NVMeコウセイ

マルチファブリックのHAペア構成では、HAペアを複数のスイッチで1つ以上のホストに接続します。次の図は、マルチファブリックのHAペアを示しています。わかりやすいように、この図ではファブリックが2つだけになっていますが、マルチファブリック構成は2つ以上の任意の数のファブリックで構成できます。

次の図のFCターゲットポート番号（0c、0d、1a、1b）は一例です。実際のポート番号は、使用しているストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

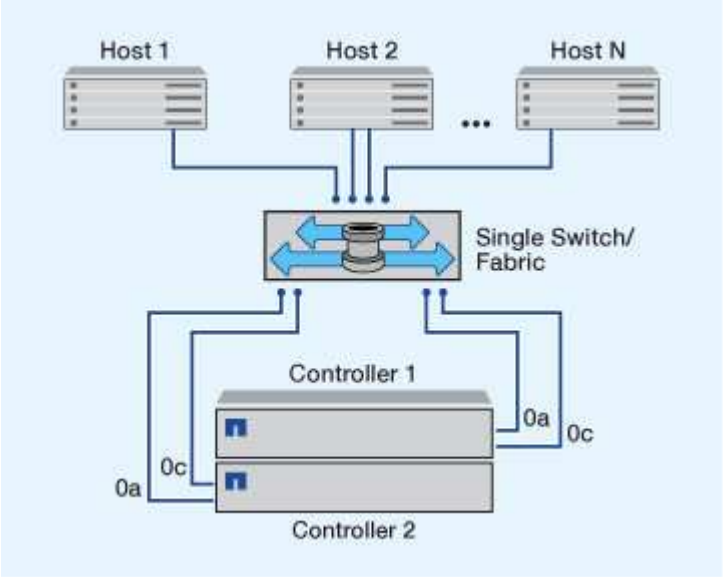


タンイツファブリックノ**FC**コウセイオヨビ**FC-NVMe**コウセイ

単一ファブリックの HA ペア構成では、 HA ペアの両方のコントローラを 1 つのファブリックで 1 つまたは複数のホストに接続します。ホストとコントローラは単一のスイッチを介して接続されるため、単一ファブリックのHAペア構成では完全な冗長性は確保されません。

次の図のFCターゲットポート番号（0a、0c）は一例です。実際のポート番号は、使用しているストレージノードのモデル、および拡張アダプタを使用しているかどうかによって異なります。

単一ファブリックのHAペア構成は、FC構成をサポートするすべてのプラットフォームでサポートされます。



"シングルノードコウセイ" は、フォールトトレランスやノンストップオペレーションのサポートに必要な冗長性が確保されないため、推奨されません。

関連情報

- 詳細をご確認ください "選択的LUNマッピング（SLM）" HAペアが所有するLUNへのアクセスに使用する

パスを制限します。

- 詳細はこちら "SAN LIF"。

FC スイッチ構成のベストプラクティス

FC スイッチを構成するときは、パフォーマンスを最大限に高めるために一定のベストプラクティスに従うことを推奨します。

FC スイッチの構成では、リンク速度を固定の値に設定すると効果的です。これは大規模なファブリックに特に適した方法で、ファブリックを再構築する際のパフォーマンスが最大限に高まり、時間を大幅に短縮することができます。自動ネゴシエーションは柔軟性に優れていますが、 FC スイッチの構成では期待したパフォーマンスを常に得られるとはかぎらないため、全体の構築時間は長くなります。

ファブリックに接続されているすべてのスイッチで、 N_Port ID Virtualization （ NPIV ）がサポートされていて有効になっている必要があります。ONTAP は、 NPIV を使用して FC ターゲットをファブリックに提示します。

サポートされている環境の詳細については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

FC および iSCSI のベストプラクティスについては、を参照してください "NetAppテクニカルレポート4080：『Best Practices for Modern SAN』"。

サポートされる **FC** ホップ数

ホストとストレージシステムの間でサポートされる FC の最大ホップ数は、スイッチベンダーとストレージシステムによる FC 構成のサポート内容によって異なります。

ホップ数とは、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチ数です。Cisco では、この値を「 SAN ファブリックの直径」とも呼びます。

スイッチベンダー	サポートされるホップ数
Brocade	FCでは7、FCoEでは5
シスコ	7 FCの場合、最大3つのスイッチをFCoEスイッチにすることができます。

関連情報

"ネットアップのダウンロード： Brocade 拡張性マトリックスのドキュメント"

"ネットアップのダウンロード： Cisco 拡張性マトリックスのドキュメント"

サポートされる **FC** ターゲットポートの速度

FC ターゲットポートは、さまざまな速度で実行するように構成できます。ターゲットポートの速度は接続先デバイスの速度と同じにする必要があります。同じホストで使用するターゲットポートは、すべて同じ速度に設定する必要があります。

FC-NVMe 構成の場合も、 FC 構成の場合とまったく同じ方法で FC ターゲットポートを使用できます。

ターゲットポートの速度は、自動ネゴシエーションを使わずに、接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

オンボードポートと拡張アダプタは、次の速度で実行するように構成できます。コントローラと拡張アダプタのポートは、必要に応じて、さまざまな速度で実行するように個別に構成することができます。

4Gb ポート	**8Gb** ポート	**16Gb** ポート	**32Gb** ポート
• 4 GB • 2 Gb • 1 Gb	• 8 Gb • 4 GB • 2 Gb	• 16Gb • 8 Gb • 4 GB	• 32Gb • 16Gb • 8 Gb

UTA2 ポートでは、必要に応じて、 8Gb の SFP+ アダプタを使用して 8Gb 、 4Gb 、 2Gb の速度をサポートできます。

FC のターゲットポート構成に関する推奨事項

最大のパフォーマンスと可用性を得るためには、推奨される FC ターゲットポート構成を使用します。

次の表に、オンボード FC および FC-NVMe ターゲットポートの使用優先順位を示します。拡張アダプタの場合は、接続に同じ ASIC を使用しないように FC ポートを分散させます。優先スロットの順序については、を参照してください "NetApp Hardware Universe の略" コントローラで使用する ONTAP ソフトウェアのバージョンに対応しています。

FC-NVMe は次のモデルでサポートされます。

- AFF A300

  AFF A300 オンボードポートでは FC-NVMe がサポートされません。

- AFF A700の略
- AFF A700s
- AFF A800

FAS2520システムにはオンボードのFCポートはなく、アドオンのアダプタもサポートされません。

コントローラ	**ASIC** を共有するポートペア	ターゲットポートの数：優先ポート
FAS9000 、 AFF A700 、 AFF A700s 、 AFF A800	なし	すべてのデータポートが拡張アダプタにあります。を参照してください "NetApp Hardware Universe の略" を参照してください。

コントローラ	**ASIC** を共有するポートペア	ターゲットポートの数：優先ポート
8080 、 8060 、 8040	0E+0f 0g+0h	1 ： 0e 2 ： 0e 、 0g 3 ： 0e 、 0g 、 0h 4 ： 0e 、 0g 、 0f 、 0h
FAS8200 と AFF A300	0g+0h	1：0g 2：0g、0h
8020	0c+0d	1：0c 2：0c、0d
62xx	0a+0b 0c+0d	1：0A 2：0a、0c 3：0a、0c、0b 4：0a、0c、0b、0d
32xx	0c+0d	1：0c 2：0c、0d
FAS2554 、 FAS2552 、 FAS2600 シリーズ、 FAS2720 、 FAS2750 、 AFF A200 、 AFF A220	0c+0d 0E+0f	1：0c 2：0c、0e 3：0c、0e、0d 4：0c、0e、0d、0f

FC アダプタを搭載したシステムを管理する

FC アダプタを搭載したシステムの管理の概要

オンボード FC アダプタと FC アダプタカードの管理に使用できるコマンドが用意されています。これらのコマンドを使用して、アダプタモードの設定、アダプタ情報の表示、および速度の変更を行うことができます。

ほとんどのストレージシステムには、イニシエータまたはターゲットとして設定できるオンボード FC アダプタが搭載されています。イニシエータまたはターゲットとして設定された FC アダプタカードを使用すること

もできます。イニシエータはバックエンドディスクシェルフに接続します。場合によっては、外部ストレージアレイ（ FlexArray ）にも接続します。ターゲットは FC スイッチのみに接続します。 FC ターゲットの HBA ポートとスイッチポートの速度は、両方とも同じ値に設定し、 auto には設定しないでください。

FC アダプタの管理用コマンド

FC コマンドを使用して、ストレージコントローラの FC ターゲットアダプタ、 FC イニシエータアダプタ、およびオンボード FC アダプタを管理できます。FC アダプタの管理に使用するコマンドは、 FC プロトコルと FC-NVMe プロトコルで同じです。

FC イニシエータアダプタのコマンドは、ノードレベルでのみ機能します。を使用する必要があります `run -node *node_name*` FCイニシエータアダプタのコマンドを使用する前のコマンド。

FC ターゲットアダプタの管理用コマンド

状況	使用するコマンド
ノードの FC アダプタ情報を表示する	`network fcp adapter show`
FC ターゲットアダプタのパラメータを変更する	`network fcp adapter modify`
FC プロトコルトラフィック情報を表示します	`run -node *node_name* sysstat -f`
FC プロトコルの実行時間を表示します	`run -node *node_name* uptime`
アダプタの設定とステータスを表示します	`run -node *node_name* sysconfig -v *adapter*`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node *node_name* sysconfig -ac`
コマンドのマニュアルページを表示します	`man command_name`

FC イニシエータアダプタの管理用コマンド

状況	使用するコマンド
ノードのすべてのイニシエータおよびそのアダプタの情報を表示する	`run -node *node_name* storage show adapter`
アダプタの設定とステータスを表示します	`run -node *node_name* sysconfig -v *adapter*`
拡張カードが取り付けられていること、および構成にエラーがないかどうかを確認します	`run -node *node_name* sysconfig -ac`

オンボード **FC** アダプタの管理用コマンド

状況	使用するコマンド
オンボード FC ポートのステータスを表示します	`system node hardware unified-connect show`

FC アダプタをイニシエータモードに設定します

オンボードアダプタの個々の FC ポートや特定の FC アダプタカードをイニシエータモードに設定することができます。イニシエータモードは、テープドライブやテープライブラリへのポートの接続、または FlexArray 仮想化や Foreign LUN Import （ FLI ）を使用するサードパーティストレージへのポートの接続に使用されます。

必要なもの

- アダプタの LIF を、メンバーとして属するすべてのポートセットから削除する必要があります。
- 物理ポートのパーソナリティをターゲットからイニシエータに変更する前に、変更する物理ポートを使用するすべての Storage Virtual Machine （ SVM ）のすべての LIF を、移行するか破棄する必要があります。

このタスクについて

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、で確認できます "NetApp Hardware Universe の略"。

NVMe/FC ではイニシエータモードがサポートされます。

手順

1. アダプタからすべての LIF を削除します。

   ```
   network interface delete -vserver SVM_name -lif lif_name,lif_name
   ```

2. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. アダプタをターゲットからイニシエータに変更します。

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. 変更したアダプタをホストしているノードをリブートします。
5. 構成に対して FC ポートが正しい状態で設定されていることを確認します。

   ```
   system hardware unified-connect show
   ```

6. アダプタをオンラインに戻します。

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

FC アダプタをターゲットモードに設定します

オンボードアダプタの個々の FC ポートや特定の FC アダプタカードをターゲットモードに設定できます。ターゲットモードは、ポートを FC イニシエータに接続するために使用します。

このタスクについて

オンボードの FC ポートは、それぞれイニシエータまたはターゲットとして個別に構成できます。一部の FC アダプタのポートについては、オンボードの FC ポートと同様に、それぞれターゲットポートまたはイニシエータポートとして個別に構成することもできます。ターゲットモードに設定できるアダプタのリストは、で確認できます "NetApp Hardware Universe の略"。

FC アダプタを構成する手順は、 FC プロトコルでも FC-NVMe プロトコルでも同じです。ただし、 FC-NVMe をサポートする FC アダプタは限られています。を参照してください "NetApp Hardware Universe の略" FC-NVMe プロトコルをサポートするアダプタの一覧が表示されます。

手順

1. アダプタをオフラインにします。

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

2. アダプタをイニシエータからターゲットに変更します。

   ```
   system node hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. 変更したアダプタをホストしているノードをリブートします。
4. ターゲットポートの設定が正しいことを確認します。

   ```
   network fcp adapter show -node node_name
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

FC ターゲットアダプタに関する情報を表示する

を使用できます `network fcp adapter show` コマンドを使用して、システム内のFCアダプタのシステム設定およびアダプタ情報を表示します。

ステップ

1. を使用して、FCアダプタに関する情報を表示します `network fcp adapter show` コマンドを実行しま

す

使用されている各スロットのシステム設定情報とアダプタ情報が出力に表示されます。

```
network fcp adapter show -instance -node node1 -adapter 0a
```

FC アダプタの速度を変更します

自動ネゴシエーションを使わずに、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにすることを推奨します。自動ネゴシエーションを設定したポートの方が、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

このタスクについて

このタスクではクラスタ内のすべてのStorage Virtual Machine（SVM）とLIFが対象となるため、を使用する必要があります `-home-port` および `-home-lif` この操作の範囲を制限するパラメータ。これらのパラメータを使用しないと、処理環境によってクラスタ内のすべての LIF が処理によって使用されなくなる可能性があります。

手順

1. アダプタのすべての LIF をオフラインにします。

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin down
   ```

2. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

   アダプタがオフラインにならない場合は、システムの該当するアダプタポートからケーブルを取り外すこともできます。

3. ポートアダプタの最大速度を確認します。

   ```
   fcp adapter show -instance
   ```

   アダプタ速度を最大速度よりも速くすることはできません。

4. アダプタ速度を変更します。

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. アダプタのすべての LIF をオンラインにします。

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
-status-admin up
```

サポートされる FC ポート

オンボードの FC ポートと FC 用の CNA / UTA2 ポートの数は、コントローラのモデルによって異なります。また、 FC ポートは、サポートされている FC ターゲット拡張アダプタのほか、 FC SFP+ アダプタ用の追加の UTA2 カードからも提供されます。

オンボードの FC 、 UTA 、および UTA2 ポートを使用できます

- オンボードポートは、ターゲットまたはイニシエータのどちらかの FC ポートとして個別に構成できます。
- オンボードの FC ポートの数はコントローラのモデルによって異なります。

  。 "NetApp Hardware Universe の略" に、各コントローラモデルのオンボード FC ポートの一覧を示します。

- FAS2520システムはFCをサポートしていません。

ターゲット拡張アダプタの FC ポート

- 使用可能なターゲット拡張アダプタは、コントローラのモデルによって異なります。

  。 "NetApp Hardware Universe の略" に、各コントローラモデルのターゲット拡張アダプタの一覧を示します。

- 一部の FC 拡張アダプタのポートは、工場出荷時にイニシエータまたはターゲットのどちらかとして構成されており、変更することはできません。

  その他のポートについては、オンボードの FC ポートと同様に、それぞれターゲットまたはイニシエータどちらかの FC ポートとして個別に構成できます。完全なリストは、で入手できます "NetApp Hardware Universe の略"。

X1133A-R6 アダプタ使用時の接続の切断を回避します

別の X1133A-R6 HBA への冗長パスを構成することにより、ポート障害時に接続が切断されないようにすることができます。

X1133A-R6 HBA は、 4 ポート 16Gb の FC アダプタで、 2 組の 2 ポートペアで構成されます。X1133A-R6 アダプタは、ターゲットモードまたはイニシエータモードとして設定できます。2 ポートペアはそれぞれ 1 つの ASIC でサポートされます（たとえば、ポート 1 とポート 2 は ASIC 1 、ポート 3 とポート 4 は ASIC 2 ）。単一の ASIC の両方のポートを、ターゲットモードまたはイニシエータモードのどちらかで動作するように設定する必要があります。ペアをサポートする ASIC でエラーが発生すると、そのペアの両方のポートがオフラインになります。

接続が切断されないようにするには、別の X1133A-R6 HBA への冗長パスか、 HBA の別の ASIC でサポートされるポートへの冗長パスを構成します。

X1143A-R6 アダプタでサポートされるポート設定の概要

X1143A-R6 アダプタのポートは、デフォルトでは FC ターゲットモードで構成されますが、 10Gb イーサネットポートおよび FCoE ポート（ CNA ポート）、あるいは 16Gb FC イニシエータポートまたはターゲットポートとして構成することもできます。 これには、 SFP+ アダプタが必要です。

イーサネットおよび FCoE 用に設定した場合、 X1143A-R6 アダプタは、同じ 10GbE ポートの NIC および FCoE のターゲットトラフィックを同時にサポートします。FC 用に設定した場合、同じ ASIC を共有する 2 ポートの各ペアを FC ターゲットまたは FC イニシエータモード用に個別に設定できます。つまり、単一の X1143A-R6 アダプタが、 1 つの 2 ポートペアで FC ターゲットモードをサポートし、もう 1 つの 2 ポートペアで FC イニシエータモードをサポートできます。 同じ ASIC に接続するポートペアは、同じモードで設定する必要があります。

X1143A-R6 アダプタは、 FC モードでは既存の FC デバイスと同じように動作し、最大速度は 16Gbps になります。X1143A-R6 アダプタを CNA モードで使用すると、同じ 10GbE ポートを共有する NIC および FCoE のトラフィックを同時に処理することができます。CNA モードでは、 FCoE の機能については FC ターゲットモードのみがサポートされます。

ポートを設定します

ユニファイドターゲットアダプタ（ X1143A-R6 ）を設定するには、同じチップ上の隣接する 2 個のポートを同じパーソナリティモードで設定する必要があります。

手順

1. を使用して、必要に応じてFibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します `system node hardware unified-connect modify` コマンドを実行します
2. FC または 10Gb イーサネットに適したケーブルを接続します。
3. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   CNA の場合は、 10Gb イーサネット SFP を使用します。FC の場合は、接続先の FC ファブリックに応じて 8Gb SFP または 16Gb SFP を使用します。

UTA2 ポートを **CNA** モードから **FC** モードに変更します

Fibre Channel （ FC ；ファイバチャネル）イニシエータモードと FC ターゲットモードをサポートするには、 UTA2 ポートを Converged Network Adapter （ CNA ；統合ネットワークアダプタ）モードから FC モードに変更する必要があります。ポートをネットワークに接続する物理メディアを変更する必要がある場合は、パーソナリティを CNA モードから FC モードに変更します。

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. ポートのモードを変更します。

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。

   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。

     i. LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。

     ii. を実行して、ポートを手動で削除します `network port delete` コマンドを実行します

     状況に応じて `network port delete` コマンドが失敗した場合は、エラーに対処してからもう一度コマンドを実行する必要があります。

   - ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。

     VIFマネージャでポートが削除されない場合は、管理者がリブート後にを使用してポートを手動で削除する必要があります `network port delete` コマンドを実行します

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                           Current  Current    Pending  Pending    Admin
    Node          Adapter  Mode     Type       Mode     Type
Status
    ------------  -------  -------  ---------  -------  ---------
-----------
    net-f8040-34-01
```

```
                    0e       cna      target     -        -
offline
    net-f8040-34-01
                    0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. 適切な SFP+ が取り付けられていることを確認します。

```
network fcp adapter show -instance -node -adapter
```

CNA の場合は、 10Gb イーサネット SFP を使用します。FC の場合は、ノードで構成を変更する前に、8Gb SFP または 16Gb SFP を使用します。

CNA / UTA2 ターゲットアダプタの光モジュールを変更します

ユニファイドターゲットアダプタ（ CNA / UTA2 ）用に選択したパーソナリティモードをサポートするには、そのアダプタで光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6 アダプタから現在の光モジュールを取り外します。
3. 優先して使用するパーソナリティモード（ FC または CNA ）の光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

   ```
   network fcp adapter show -instance -node -adapter
   ```

   サポートされている SFP+ モジュールと Cisco ブランドの銅線（ Twinax ）ケーブルについては、を参照してください "NetApp Hardware Universe の略"。

アダプタの設定を確認します

ユニファイドターゲットアダプタ（X1143A-R6）の設定を確認するには、を実行する必要があります `system hardware unified-connect show` コマンドを使用してコントローラ上のすべてのモジュールを表示します。

手順

1. ケーブルを接続していない状態でコントローラをブートします。
2. を実行します `system hardware unified-connect show` コマンドを使用して、ポートの設定とモジュールを確認します。
3. ポート情報を確認してから、 CNA とポートを設定します。

FCoEコウセイ

FCoE の設定方法の概要

FCoE は、 FCoE スイッチを使用してさまざまな方法で構成できます。直接接続型の構成は FCoE ではサポートされません。

FCoE 構成はすべてデュアルファブリックです。完全な冗長性を提供し、ホスト側でマルチパスソフトウェアが必要です。すべての FCoE 構成で、イニシエータとターゲット間のパスには、最大ホップ数内であればいくつでも FCoE スイッチと FC スイッチを配置できます。スイッチ同士を接続するためには、イーサネット ISL をサポートするファームウェアバージョンがスイッチで実行されている必要があります。FCoE 構成の各ホストでオペレーティングシステムが同じである必要はありません。

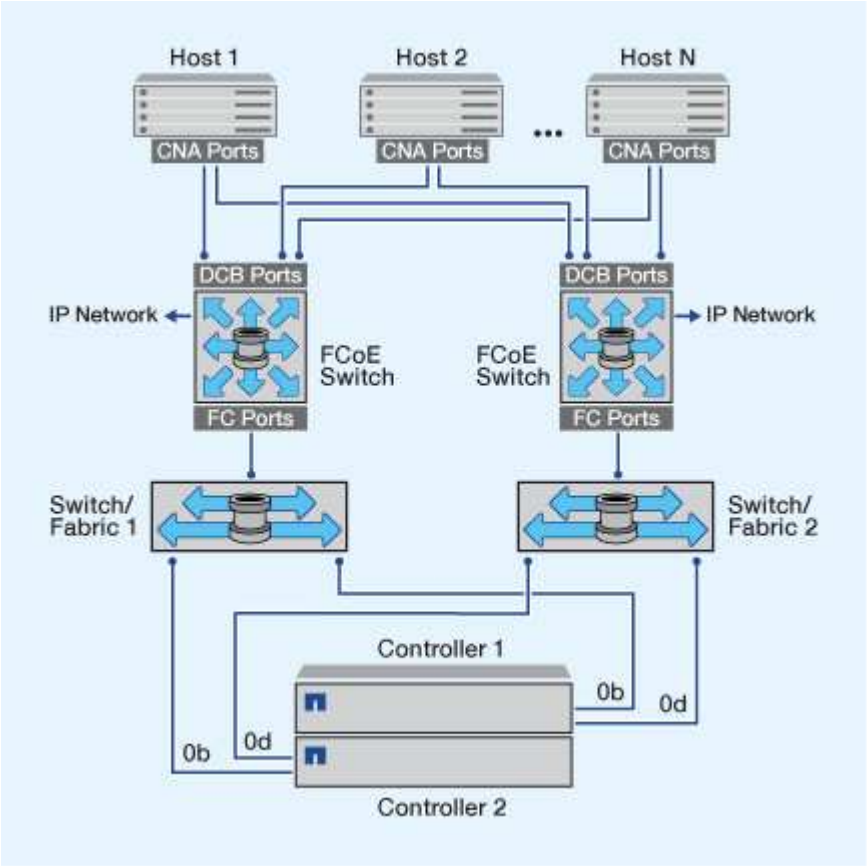
FCoE 構成では、 FCoE の機能を明示的にサポートするイーサネットスイッチが必要です。FCoE 構成は、FC スイッチと同じ相互運用性と品質管理プロセスに照らして検証されます。サポートされる構成の一覧については、 Interoperability Matrix を参照してください。これらのサポートされる構成には、スイッチモデル、単一ファブリックに導入可能なスイッチの数、サポートされるスイッチファームウェアのバージョンなどのパラメータが含まれています。

次の図の FC ターゲット拡張アダプタのポート番号は一例です。実際のポート番号は、 FCoE ターゲット拡張アダプタがインストールされている拡張スロットによって変わる場合があります。

FCoE イニシエータから **FC** ターゲット

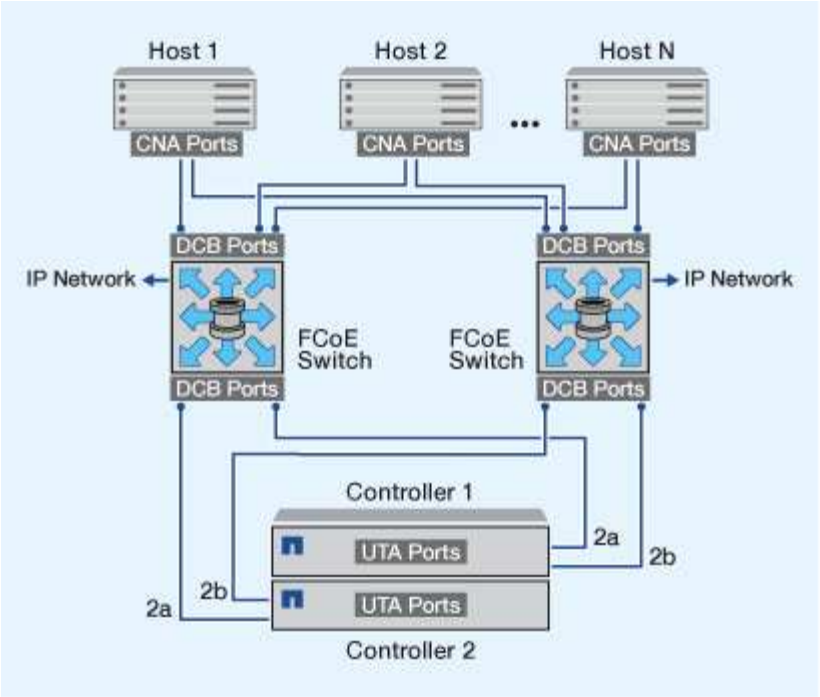
FCoE イニシエータ（ CNA ）を使用すると、 FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FC ターゲットポートに接続できます。FCoE スイッチには FC ポートも必要です。ホストの FCoE イニシエータは、常に FCoE スイッチに接続されます。FCoE スイッチは、 FC ターゲットに直接接続することも、 FC スイッチを介して FC ターゲットに接続することもできます。

次の図では、ホストの CNA を FCoE スイッチに接続し、 FC スイッチを HA ペアに接続しています。



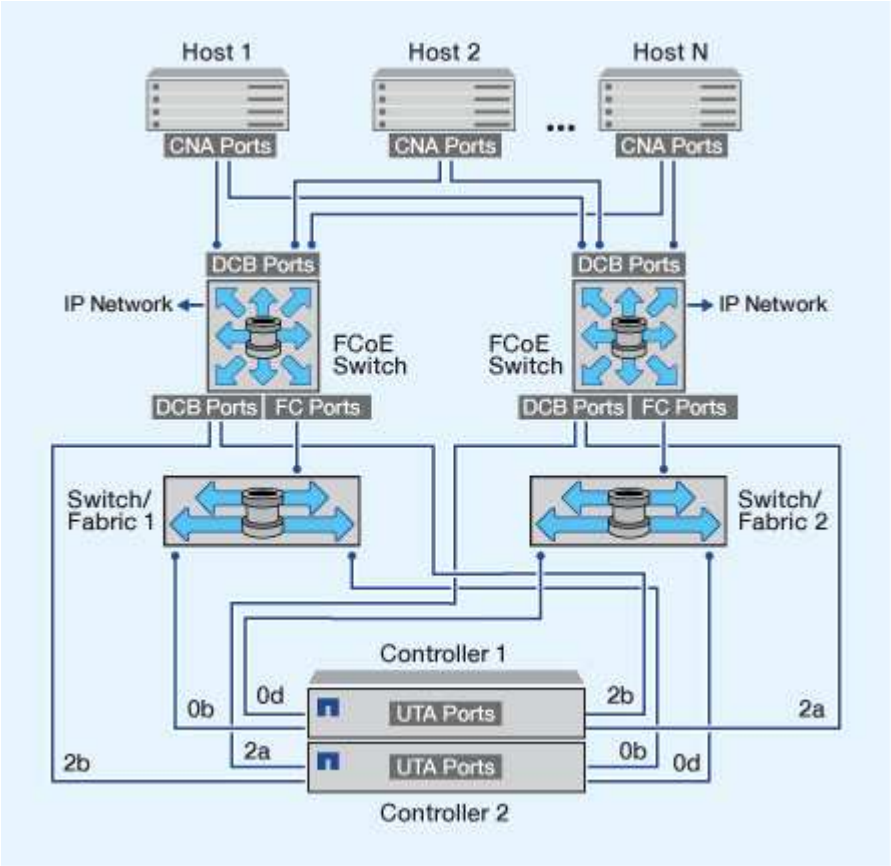
FCoE イニシエータから **FCoE** ターゲット

ホストの FCoE イニシエータ（ CNA ）を使用すると、 FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE ターゲットポート（ UTA または UTA2 とも呼ばれる）に接続できます。



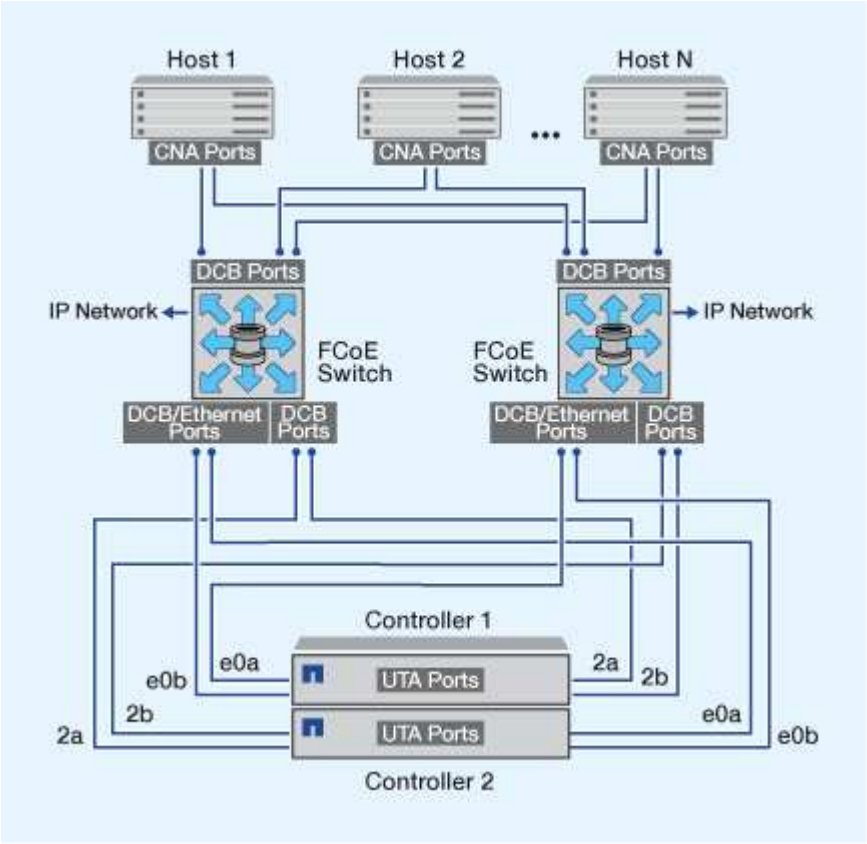
FCoE イニシエータから **FCoE** および **FC** ターゲット

ホストの FCoE イニシエータ（ CNA ）を使用すると、 FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE および FC ターゲットポート（ UTA または UTA2 とも呼ばれる）に接続できます。



FCoE と IP ストレージプロトコルの混在

ホストの FCoE イニシエータ（ CNA ）を使用すると、 FCoE スイッチを介して、ホストを HA ペアの両方のコントローラの FCoE ターゲットポート（ UTA または UTA2 とも呼ばれる）に接続できます。FCoE ポートでは、単一のスイッチへの従来のリンクアグリゲーションは使用できません。Cisco スイッチは、 FCoE をサポートする特別なタイプのリンクアグリゲーション（仮想ポートチャネル）をサポートします。仮想ポートチャネルは、 2 つのスイッチへの個別のリンクを集約します。仮想ポートチャネルは他のイーサネットトラフィックにも使用できます。NFS、SMB、iSCSI、およびその他のイーサネットトラフィックなど、FCoE以外のトラフィックに使用されるポートでは、FCoEスイッチの通常のイーサネットポートを使用できます。



FCoE イニシエータとターゲットの組み合わせ

FCoE および従来の FC のイニシエータとターゲットの特定の組み合わせがサポートされます。

FCoE イニシエータ

ホストコンピュータの FCoE イニシエータは、ストレージコントローラの FCoE ターゲットと従来の FC ターゲットの両方で使用できます。ホストの FCoE イニシエータは FCoE DCB （ Data Center Bridging ）スイッチに接続する必要があります。ターゲットに直接接続することはできません。

次の表に、サポートされる組み合わせを示します。

イニシエータ	ターゲット	サポートされます
FC	FC	はい。

イニシエータ	ターゲット	サポートされます
FC	FCoE	はい。
FCoE	FC	はい。
FCoE	FCoE	はい。

FCoE ターゲット

ストレージコントローラで FCoE ターゲットポートと 4Gb 、 8Gb 、 16Gb の FC ポートを混在させることができます。 FC ポートがアドインのターゲットアダプタであるかオンボードのポートであるかは関係ありません。FCoE と FC の両方のターゲットアダプタを同じストレージコントローラに搭載できます。

FC のオンボードポートと拡張ポートの組み合わせルールが引き続き適用されます。

FCoE でサポートされるホップ数

ホストとストレージシステムの間でサポートされる Fibre Channel over Ethernet （ FCoE ）の最大ホップ数は、スイッチベンダー、およびストレージシステムでの FCoE 構成のサポート内容によって異なります。

ホップ数とは、イニシエータ（ホスト）とターゲット（ストレージシステム）の間のパスにあるスイッチ数です。Cisco Systems のマニュアルでは、この値のことを「 SAN fabric_ の直径」とも呼んでいます。

FCoE では、 FCoE スイッチを FC スイッチに接続することができます。

エンドツーエンドの FCoE 接続では、イーサネットの Inter-Switch Link （ ISL ；スイッチ間リンク）に対応したバージョンのファームウェアが FCoE スイッチで実行されている必要があります。

次の表に、サポートされる最大ホップ数を示します。

スイッチベンダー	サポートされるホップ数
Brocade	FCの場合は7 FCoE の場合は 5
シスコ	7. FCoE スイッチは 3 台まで使用できます。

ファイバチャネルおよび **FCoE** のゾーニング

ファイバチャネルおよび **FCoE** のゾーニングの概要

FC ゾーン、 FC-NVMe ゾーン、または FCoE ゾーンは、ファブリック内の 1 つ以上のポートを論理的にグループ化したものです。デバイス同士が互いを認識し、接続し、相

互にセッションを確立して通信できるようにするには、両方のポートに共通のゾーンメンバーシップが必要です。シングルイニシエータのゾーニングを推奨します。

ゾーニングを行う理由

- イニシエータ HBA 間のクロストークを削減または解消できます。

  これは小規模な環境でも発生し、ゾーニングを実装する最大の理由の 1 つです。ゾーニングによってファブリックの論理サブセットを作成することで、クロストークの問題が解消されます。

- 特定の FC 、 FC-NVMe 、または FCoE ポートへの使用可能なパスの数と、ホストと特定の LUN の間に認識されるパスの数を減らすことができます。

  たとえば、一部のホスト OS のマルチパスソリューションには、管理できるパスの数に制限があります。ゾーニングを使用すると、 OS のマルチパスドライバで認識されるパスの数を減らすことができます。ホストにマルチパス解決策がインストールされていない場合は、ファブリックのゾーニングまたは SVM の選択的 LUN マッピング（ SLM ）とポートセットの組み合わせを使用して、認識される LUN へのパスが 1 つだけであることを確認する必要があります。

- ゾーンを共有するエンドポイントへのアクセスと接続を制限することで、セキュリティを強化します。

  共通のゾーンがないポート同士が通信することはできません。

- 発生する問題を切り離すことで SAN の信頼性が高まり、問題の範囲を限定することで解決時間を短縮する効果があります。

ゾーニングに関する推奨事項

- 1 つの SAN にホストを 4 つ以上接続する場合や SAN に接続されたノードで SLM が実装されていない場合は、常にゾーニングを実装してください。
- 一部のスイッチベンダーでは World Wide Node Name のゾーニングも使用できますが、特定のポートを正しく定義し、 NPIV を効果的に利用するには、 World Wide Port Name のゾーニングを使用する必要があります。
- 管理性を損なわない範囲でゾーンサイズを制限することを推奨します。

  複数のゾーンを重複させてサイズを制限することができます。ホストまたはホストクラスタごとにゾーンを定義することを推奨します。

- イニシエータ HBA 間のクロストークを解消するために、単一イニシエータのゾーニングを使用してください。

World Wide Name に基づくゾーニング

World Wide Name （ WWN ；ワールドワイド名）に基づくゾーニングでは、ゾーンに含めるメンバーの WWN を指定します。ONTAP でのゾーニングでは、 World Wide Port Name （ WWPN ）ゾーニングを使用する必要があります。

WWPN ゾーニングは柔軟性に優れており、デバイスをファブリックに接続する物理的な場所によってアクセスが制限されることがありません。ケーブルを別のポートに接続するときにゾーンを再設定する必要はありません。

ONTAP を実行するストレージコントローラへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（ LIF ）の WWPN を使用して FC スイッチをゾーニングしてください。LIF の詳細については、『 ONTAP ネットワーク管理ガイド』を参照してください。

"Network Management の略"

個々のゾーン

推奨されるゾーニング設定では、ゾーンごとに 1 つのホストイニシエータを配置します。ゾーンは、ホストイニシエータポートとストレージノード上の 1 つ以上のターゲット LIF で構成され、ターゲットあたりの希望する数のパスまで LUN へのアクセスを提供します。つまり、同じノードにアクセスする複数のホストはお互いのポートを認識できませんが、各イニシエータはすべてのノードにアクセスできます。

Storage Virtual Machine （ SVM ）のすべての LIF を、ホストイニシエータがあるゾーンに追加する必要があります。これにより、既存のゾーンを編集したり、新しいゾーンを作成したりせずに、ボリュームや LUN を移動できます。

ONTAP を実行するノードへのファイバチャネルパスでは、ノードの物理ポートの WWPN ではなく、ターゲットの論理インターフェイス（ LIF ）の WWPN を使用して FC スイッチをゾーニングしてください。物理ポートの WWPN は「 50 」で始まり、 LIF の WWPN は「 20 」で始まります。

単一ファブリックゾーニング

単一ファブリック構成でも、各ホストイニシエータを各ストレージノードに接続できます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。マルチパスで解決策の耐障害性を確保するには、各ホストに 2 つのイニシエータが必要です。

各イニシエータには、アクセス可能なノードの LIF を少なくとも 1 つ割り当てる必要があります。ホストイニシエータからクラスタ内の HA ペアのノードへのパスが少なくとも 1 つあるようにゾーニングを設定して、LUN 接続用のパスを提供する必要があります。つまり、ホスト上の各イニシエータには、そのゾーン構成内のノードごとにターゲット LIF が 1 つだけ割り当てられます。クラスタ内の同じノードまたは複数のノードへのパスが複数必要な場合は、ゾーン構成内の各ノードに複数の LIF を割り当てます。これにより、あるノードに障害が発生した場合や、 LUN を含むボリュームが別のノードに移動した場合も、ホストは引き続き LUN にアクセスできます。この場合、レポートノードを適切に設定する必要もあります。

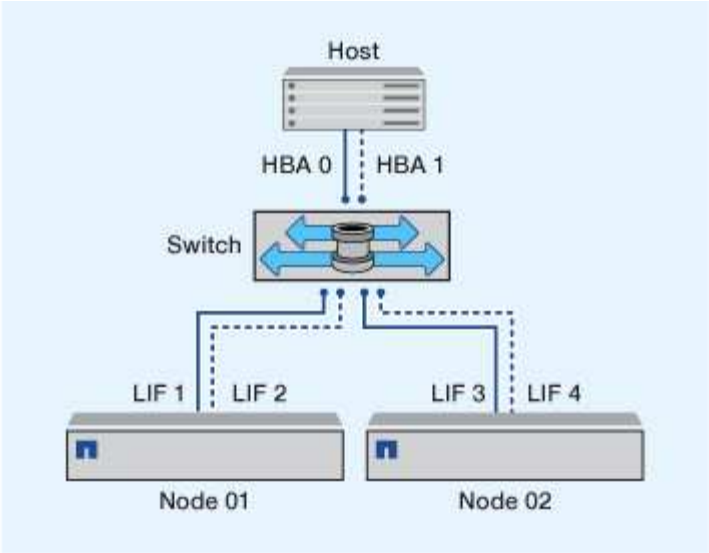
単一ファブリック構成はサポートされていますが、可用性に優れているとはみなされません。1 つのコンポーネントで障害が発生すると、原因によるデータアクセスが失われる可能性があります。

次の図では、ホストに 2 つのイニシエータがあり、マルチパスソフトウェアを実行しています。次の 2 つのゾーンがあります。

> この図で使用されている命名規則は、 ONTAP 解決策で使用できる一例です。

- ゾーン 1 ： HBA 0 、 LIF_1 、および LIF_3
- ゾーン2：HBA 1、LIF_2、およびLIF_4

これよりもノード数が多い構成では、追加のノードの LIF がこれらのゾーンに配置されます。



この例では、各ゾーンに 4 つの LIF をすべて配置することもできます。その場合のゾーンは次のようになります。

- ゾーン 1 ： HBA 0 、 LIF_1 、 LIF_2 、 LIF_3 、および LIF_4
- ゾーン2：HBA 1、LIF_1、LIF_2、LIF_3、およびLIF_4

> ホスト OS とマルチパスソフトウェアが、ノード上の LUN へのアクセスに使用される数のパスをサポートしている必要があります。ノードの LUN へのアクセスに使用するパスの数については、 SAN 構成の制限に関するセクションを参照してください。

関連情報

"NetApp Hardware Universe の略"

デュアルファブリックの **HA** ペアのゾーニング

デュアルファブリック構成では、各ホストイニシエータを各クラスタノードに接続できます。各ホストイニシエータは、異なるスイッチを使用してクラスタノードにアクセスできます。複数のパスを管理するには、ホストにマルチパスソフトウェアが必要です。

1 つのコンポーネントで障害が発生してもデータへのアクセスは維持されるため、デュアルファブリック構成はハイアベイラビリティとみなされます。

次の図では、ホストに 2 つのイニシエータがあり、マルチパスソフトウェアを実行しています。2 つのゾーンがあります。SLM では、すべてのノードがレポートノードとなるように設定されています。

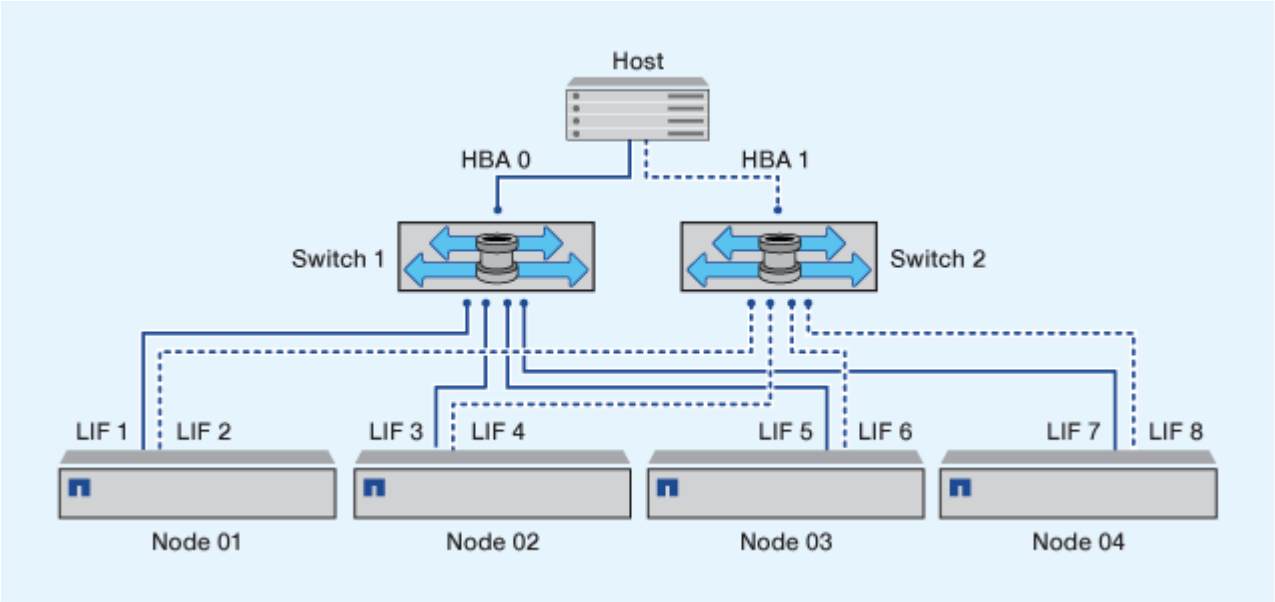
> この図で使用されている命名規則は、 ONTAP 解決策で使用できる一例です。

- ゾーン1：HBA 0、LIF_1、LIF_3、LIF_5、およびLIF_7
- ゾーン2：HBA 1、LIF_2、LIF_4、LIF_6、およびLIF_8

各ホストイニシエータは、異なるスイッチを使用してゾーニングされています。ゾーン 1 には、スイッチ 1 からアクセスします。ゾーン2にはスイッチ2からアクセスします。

各イニシエータは、すべてのノードの LIF にアクセスできます。これにより、あるノードで障害が発生しても、ホストは引き続き LUN にアクセスできます。SVM は、選択的 LUN マップ（ SLM ）とレポートノードの設定に基づいて、 clustered 解決策のすべてのノードのすべての iSCSI LIF と FC LIF にアクセスできます。SLM 、ポートセット、または FC スイッチゾーニングを使用することで、 SVM からホストへのパスの数と SVM から LUN へのパスの数を少なくすることができます。

これよりもノード数が多い構成では、追加のノードの LIF がこれらのゾーンに配置されます。



ホスト OS とマルチパスソフトウェアが、ノード上の LUN へのアクセスに使用される数のパスをサポートしている必要があります。

関連情報

"NetApp Hardware Universe の略"

Cisco FC および **FCoE** スイッチのゾーニング制限

Cisco FC スイッチおよび FCoE スイッチを使用する場合、 1 つのファブリックゾーンに同じ物理ポートのターゲット LIF を複数含めることはできません。同じポートの LIF を同じゾーンに複数配置すると、接続が失われた場合に LIF ポートがリカバリできなくなる可能性があります。

FC-NVMe プロトコルには、通常の FC スイッチが FC プロトコルとまったく同じ方法で使用されます。

- FC および FCoE プロトコルの複数の LIF は、ゾーンが同じでなければノード上の物理ポートを共有することができます。
- FC-NVMe と FCoE は、同じ物理ポートを共有できません。
- FC と FC-NVMe は、同じ 32Gb 物理ポートを共有できます。
- Cisco FC スイッチおよび FCoE スイッチでは、特定のポートの各 LIF をそのポートの他の LIF とは別のゾーンに配置する必要があります。
- 1 つのゾーンに FC と FCoE 両方の LIF を配置することができます。ゾーンにはクラスタ内のすべてのターゲットポートの LIF を配置することができますが、ホストのパス制限を超えないように注意し、 SLM

の設定を確認してください。

- 物理ポートが異なる LIF は、同じゾーンに配置することもできます。
- Cisco スイッチを使用する場合は、 LIF を分離する必要があります。

  必須ではありませんが、 LIF の分離はすべてのスイッチで推奨されます

共有 SAN 構成の要件

共有 SAN 構成とは、ホストを ONTAP ストレージシステムと他社のストレージシステムの両方に接続する構成です。単一のホストから ONTAP ストレージシステムと他社のストレージシステムにアクセスする場合は、いくつかの要件を満たす必要があります。

いずれのホストオペレーティングシステムでも、各ベンダーのストレージシステムへの接続には別々のアダプタを使用することを推奨します。別々のアダプタを使用すると、ドライバや設定が競合する可能性が低くなります。ONTAP ストレージシステムへの接続には、 NetApp Interoperability Matrix Tool にサポート対象として記載されたアダプタモデル、 BIOS 、ファームウェア、ドライバを使用する必要があります。

必須または推奨のタイムアウト値やホストのその他のストレージパラメータを設定します。ネットアップソフトウェアのインストールやネットアップ設定の適用は必ず最後に行ってください。

- AIX の場合、構成に対応する AIX Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- ESX の場合、 Virtual Storage Console for VMware vSphere を使用してホスト設定を適用します。
- HP-UX の場合、 HP-UX のデフォルトのストレージ設定を使用します。
- Linux の場合、構成に対応する Linux Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- Solaris の場合、構成に対応する Solaris Host Utilities バージョンの値を Interoperability Matrix Tool で確認して適用します。
- Windows の場合、構成に対応する Windows Host Utilities のバージョンを Interoperability Matrix Tool で確認してインストールします。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

MetroCluster 環境のSAN構成

MetroCluster 環境のSAN構成

MetroCluster 環境で SAN 構成を使用する際の注意事項は次のとおりです。

- MetroCluster 構成では ' フロントエンド FC ファブリックのルーテッド VSAN 構成はサポートされません
- ONTAP 9.12.1以降では、NVMe/FCで4ノードMetroCluster IP構成がサポートされます。MetroCluster構成はNVMe/TCPではサポートされません。MetroCluster 構成はONTAP 9.12.1よりも前のNVMeではサポートされません。
- MetroCluster 構成では、iSCSI、FC、FCoEなどの他のSANプロトコルがサポートされます。

- SANクライアント構成を使用している場合は、に記載されているメモにMetroCluster 構成に関する特別な考慮事項がないかどうかを確認する必要があります "NetApp Interoperability Matrix Tool で確認できます" IMT
- オペレーティングシステムとアプリケーションでは、MetroCluster の自動計画外スイッチオーバーとTiebreakerまたはメディエーターから開始されたスイッチオーバーをサポートするために、120秒のI/O耐障害性を提供する必要があります。
- フロントエンド SAN の両側で MetroCluster が同じ WWPN を使用している。

関連情報

- "MetroCluster のデータ保護とディザスタリカバリについて理解する"
- "技術情報アーティクル：「What are AIX Host support considerations in a MetroCluster configuration？」"
- "技術情報アーティクル：「Solaris host support considerations in a MetroCluster configuration」"

スイッチオーバーとスイッチバックの間でポートが重複しないようにする

SAN環境では、古いポートがオフラインになって新しいポートがオンラインになったときに重複しないように、フロントエンドスイッチを設定できます。

スイッチオーバーの実行中に、ディザスタサイトの FC ポートがオフラインで、このポートがネームサービスとディレクトリサービスから削除されたことをファブリックが検出するまで、サバイバーサイトの FC ポートがファブリックにログインすることがあります。

災害時に FC ポートがまだ削除されていないと、 WWPN の重複が原因で、サバイバーサイトでの FC ポートのファブリックログインが拒否される可能性があります。FC スイッチのこの動作は、既存のデバイスではなく、前のデバイスのログインに合わせて変更できます。この動作が他のファブリックデバイスに与える影響を確認してください。詳細については、スイッチベンダーにお問い合わせください。

スイッチのタイプに応じて、適切な手順 を選択します。

例 **9.** 手順

Cisco スイッチ

1. スイッチに接続してログインします。
2. コンフィギュレーションモードを開始します。

```
switch# config t
switch(config)#
```

3. ネームサーバデータベースの最初のデバイスエントリを新しいデバイスで上書きします。

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. NX-OS 8.x を実行しているスイッチで、 flogi quiesce タイムアウトが 0 に設定されていることを確認します。

   a. 休止期間を表示します。

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 前の手順の出力で時刻がゼロであることが示されない場合は、 0 に設定します。

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Brocade スイッチ

1. スイッチに接続してログインします。
2. を入力します `switchDisable` コマンドを実行します
3. を入力します `configure` コマンドを入力し、を押します `y` をクリックします。

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. 設定 1 を選択：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 残りのプロンプトに応答するか、 * Ctrl+D* を押します。
6. を入力します `switchEnable` コマンドを実行します

関連情報

"テストまたはメンテナンスのためのスイッチオーバーの実行"

ホストでのマルチパスのサポート

ホストでのマルチパスのサポートの概要

ONTAP では、 FC と iSCSI のどちらのパスにも必ず Asymmetric Logical Unit Access （ALUA ；非対称論理ユニットアクセス）が使用されます。FC プロトコルと iSCSI プロトコルに対して ALUA をサポートするホスト構成を使用してください。

ONTAP 9.5 以降では、 Asynchronous Namespace Access （ANA）を使用する NVMe 構成で、マルチパス HA ペアのフェイルオーバー / ギブバックがサポートされます。ONTAP 9.4 では、 NVMe でサポートされるホストからターゲットへのパスは 1 つだけです。アプリケーションホストは、ハイアベイラビリティ（HA）パートナーへのパスのフェイルオーバーを管理する必要があります。

ALUA または ANA をサポートする具体的なホスト設定については、を参照してください "NetApp Interoperability Matrix Tool で確認できます" および "ONTAP SAN ホスト構成" ホストオペレーティングシステムに応じて異なります。

ホストのマルチパスソフトウェアが必要になる状況

Storage Virtual Machine （SVM）の論理インターフェイス（LIF）からファブリックへのパスが複数ある場合、マルチパスソフトウェアが必要です。ホストが複数のパスで LUN にアクセスできる場合は、ホストにマルチパスソフトウェアが必要です。

マルチパスソフトウェアは、 LUN へのすべてのパスを単一のディスクとしてオペレーティングシステムに表示します。マルチパスソフトウェアがない場合、各パスが別々のディスクとしてオペレーティングシステムに認識されるため、データの破損を招くことがあります。

次のいずれかに該当する場合、解決策に複数のパスがあるとみなされます。

- ホストの 1 つのイニシエータポートを SVM の複数の SAN LIF に接続している場合
- 複数のイニシエータポートを SVM の単一の SAN LIF に接続しています
- 複数のイニシエータポートを SVM の複数の SAN LIF に接続しています

HA 構成では、マルチパスソフトウェアの使用を推奨します。選択的 LUN マップに加え、 FC スイッチのゾーニングまたはポートセットを使用して、 LUN へのアクセスに使用するパスを制限することを推奨します。

マルチパスソフトウェアは、マルチパス I/O （ MPIO ）ソフトウェアとも呼ばれます。

ホストからクラスタ内のノードへの推奨されるパス数

ホストからクラスタ内の各ノードへのパスは 8 個までにすることを推奨します。ホスト OS やホストで使用されるマルチパスでサポートされるパスの総数に注意が必要です。

選択的 LUN マップ（ SLM ）を使用して、クラスタ内の Storage Virtual Machine （ SVM ）で使用される各レポートノードへのパスを LUN ごとに少なくとも 2 つ確保します。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。

クラスタにノードが 4 つ以上ある場合、またはいずれかのノードの SVM で 5 つ以上のターゲットポートを使用している場合は、 ノード上の LUN へのアクセスに使用できるパスの数を制限し、推奨される最大数である 8 個以内にするには、次の方法を使用します。

- SLM

  SLM は、ホストから LUN へのパスを、 LUN を所有するノード上のパスと所有者ノードの HA パートナーのパスだけに制限します。SLM はデフォルトでは有効になっています。

- iSCSI のポートセット
- ホストの FC igroup マッピング
- FC スイッチゾーニング

関連情報

"SAN 管理"

構成の制限

SAN 構成でサポートされるノード数を確認

ONTAP でサポートされるクラスタあたりのノード数は、 ONTAP のバージョン、クラスタ内のストレージコントローラのモデル、およびクラスタノードのプロトコルによって異なります。

このタスクについて

FC 、 FC-NVMe 、 FCoE 、または iSCSI が設定されたノードがクラスタにある場合、そのクラスタには SAN ノードの制限が適用されます。クラスタ内のコントローラに基づくノードの制限については、 _ Hardware Universe _ を参照してください。

手順

1. に進みます "NetApp Hardware Universe の略"。
2. 左上の [* ホーム] ボタンの横にある [* プラットフォーム] をクリックし、プラットフォームの種類を選択します。
3. 使用している ONTAP のバージョンの横にあるチェックボックスをオンにします。

   プラットフォームを選択するための新しい列が表示されます。

4. 解決策で使用しているプラットフォームの横にあるチェックボックスをオンにします。
5. [仕様を選択] 列の [すべて選択 *] チェックボックスをオフにします。
6. [クラスタあたりの最大ノード数（ NAS / SAN ） *] チェックボックスをオンにします。
7. [結果を表示（ Show Results ）] をクリックする。

関連情報

"NetApp Hardware Universe の略"

FC 構成および **FC-NVMe** 構成におけるクラスタあたりのサポートされるホスト数を確認します

クラスタに接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのセッション数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

このタスクについて

FC 構成および FC-NVMe 構成では、システムの Initiator-Target Nexus （ ITN ；イニシエータ - ターゲット接続）の数に基づいて、クラスタにホストを追加できるかどうかを判断します。

1 つの ITN は、ホストのイニシエータからストレージシステムのターゲットへの 1 つのパスに該当します。FC 構成および FC-NVMe 構成のノードあたりの最大 ITN 数は 2 、 048 です。ITN がこの最大数を超えない限り、クラスタにホストを追加することができます。

クラスタで使用されている ITN の数を確認するには、クラスタの各ノードで次の手順を実行します。

手順

1. ノードの LIF をすべて特定します。
2. ノードのすべての LIF に対して次のコマンドを実行します。

   ```
   fcp initiator show -fields wwpn, lif
   ```

   コマンド出力の一番下に表示されたエントリ数が、その LIF の ITN 数です。
3. それぞれの LIF について、表示された ITN 数を記録します。
4. クラスタのすべてのノードの各 LIF の ITN 数を合計します。

   この値がクラスタの ITN の総数になります。

iSCSI 構成でサポートされるホスト数を確認します

iSCSI 構成で接続できる SAN ホストの最大数は、クラスタの各ノードに接続されるホストの数、ホストあたりのイニシエータ数、ホストあたりのログイン数、クラスタ内のノード数など、クラスタのさまざまな属性の組み合わせによって大きく異なります。

このタスクについて

ノードに直接または 1 つ以上のスイッチを介して接続できるホストの数は、使用可能なイーサネットポートの数で決まります。使用可能なイーサネットポートの数は、コントローラのモデル、およびコントローラにインストールされているアダプタの数とタイプによって決まります。コントローラおよびアダプタでサポートさ

れるイーサネットポートの数は、 _ Hardware Universe _ で確認できます。

マルチノードクラスタ構成の場合は、ノードあたりの iSCSI セッションの数に基づいて、クラスタにホストを追加できるかどうかを判断する必要があります。ノードあたりの iSCSI セッションの最大数をクラスタが下回っている場合は、引き続きクラスタにホストを追加できます。ノードあたりの iSCSI セッションの最大数は、クラスタ内のコントローラのタイプによって異なります。

手順

1. ノードのターゲットポータルグループをすべて特定します。
2. ノードのすべてのターゲットポータルグループについて、それぞれ iSCSI セッションの数を確認します。

   ```
   iscsi session show -tpgroup tpgroup
   ```

   コマンド出力の一番下に表示されたエントリ数が、そのターゲットポータルグループの iSCSI セッション数です。

3. 各ターゲットポータルグループについて、表示された iSCSI セッション数を記録します。
4. ノードの各ターゲットポータルグループの iSCSI セッション数を追加します。

   この値がノードの iSCSI セッションの総数になります。

FC スイッチの構成の制限

ファイバチャネルスイッチには、ポート、ポートグループ、ブレード、およびスイッチごとにサポートされるログイン数など、最大構成制限があります。サポートされる制限については、スイッチベンダーから文書化されています

各 FC の Logical Interface （ LIF ；論理インターフェイス）が FC のスイッチポートにログインします。ノードの 1 つのターゲットからのログインの総数は、 LIF の数に、基盤となる物理ポートへのログイン数として 1 を足した数です。スイッチベンダーが設定しているログインやその他の構成値の制限を超えないようにしてください。これは、 NPIV が有効な仮想環境のホスト側で使用されているイニシエータにも当てはまります。解決策で使用されているターゲットまたはイニシエータのログインについては、スイッチベンダーが設定している制限を超えないようにしてください。

Brocade スイッチの最大数

Brocade スイッチの最大構成数は、 _Brocade 拡張性ガイドライン _ で確認できます。

Cisco Systems スイッチの最大数

Cisco スイッチの構成の制限については、を参照してください "Cisco の設定の制限" 使用している Cisco スイッチソフトウェアのバージョンに対応したガイドです。

キュー深度の算出の概要

ノードあたりおよび FC ポートのファンインあたりの ITN 数を最大にするために、ホストの FC キュー深度の調整が必要になる場合があります。LUN の最大数と 1 つの FC ポートに接続できる HBA の数は、 FC ターゲットポートで使用可能なキューの深さによって制限されます。

このタスクについて

キュー深度は、ストレージコントローラで一度にキューに格納することができる、 I/O 要求（ SCSI コマンド）の数です。ホストのイニシエータ HBA からストレージコントローラのターゲットアダプタへの I/O 要求ごとに、キューエントリが 1 つ作成されます。一般に、キュー深度を大きくするとパフォーマンスが向上します。ただし、ストレージコントローラの最大キュー深度に達すると、ストレージコントローラは QFULL 応答を返して受け取ったコマンドを拒否します。QFULL 状態はシステムパフォーマンスの大幅な低下を招き、一部のシステムではエラーを引き起こすこともあります。そのため、 1 台のストレージコントローラに多数のホストがアクセスしている環境では、 QFULL が発生しないように慎重に計画してください。

複数のイニシエータ（ホスト）を含む構成では、すべてのホストでキュー深度を同程度に設定する必要があります。同じターゲットポートを介してストレージコントローラに接続されたホスト間では、キュー深度に応じてリソースへのアクセスに差があり、キュー深度が小さいホストよりもキュー深度の大きいホストのアクセスが優先されます。

キュー深度を「チューニング」する場合は、次の一般的な推奨事項を考慮してください。

- 小規模から中規模のシステムでは、 HBA キュー深度を 32 にする。
- 大規模のシステムでは、 HBA キュー深度を 128 にする。
- 例外的なケースまたはパフォーマンステストでは、キュー深度を 256 にしてキュー関連の問題の発生を回避します。
- すべてのホストにアクセスが均等になるように、すべてのホストでキュー深度を同程度に設定する必要があります。
- パフォーマンスの低下やエラーを回避するために、ストレージコントローラのターゲット FC ポートのキュー深度を超えないようにする。

手順

1. 1 つの FC ターゲットポートに接続しているすべてのホストの FC イニシエータの数を数えます。
2. 128 をかけます。
   - 2 、 048 より小さい場合は、すべてのイニシエータのキュー深度を 128 に設定します。
     15 台のホストがあり、 1 つのイニシエータがストレージコントローラ上の 2 つのターゲットポートのそれぞれに接続されています。15 × 128 = 1 、 920 。これは合計最大キュー深度の 2 、 048 より少ないため、すべてのイニシエータのキュー深度を 128 に設定できます。
   - この値が 2 、 048 よりも大きい場合は、手順 3 に進みます。
     30台のホストがあり、1つのイニシエータがストレージコントローラ上の2つのターゲットポートのそれぞれに接続されています。30 × 128 = 3 、 840 。これは合計最大キュー深度の 2 、 048 より大きいため、手順 3 に記載されているいずれかのオプションを実行して調整します。
3. 次のいずれかのオプションを選択して、ストレージコントローラにホストを追加します。
   - オプション 1 ：
     i. FC ターゲットポートを追加します。
     ii. FC イニシエータを再配分します。
     iii. 手順 1 と 2. を繰り返します。
     [+]
     必要とされるキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。この状態を解決するために、各コントローラに 2 ポートの FC ターゲットアダプタを追加し、 30 台のホストのうち 15 台が 1 つのポートセットに接続され、残りの 15 台のホストが 2 つ目のポートセットに接続されるように FC スイッチをゾーニングし直します。これで、ポートあたりのキュー

深度は 15 × 128 = 1 、 920 となります。

- オプション2：
  i. 各ホストを「ラージ」または「モール」として指定します。これは、予想される I/O ニーズに基づいています。
  ii. 大規模イニシエータの台数に 128 をかけます。
  iii. 小規模イニシエータの台数に 32 をかけます。
  iv. 2 つの結果をまとめて追加します。
  v. 2 、 048 より小さい場合は、大規模ホストのキュー深度を 128 に、小規模ホストのキュー深度を 32 に設定します。
  vi. 2 、 048 よりも大きい場合は、合計キュー深度が 2 、 048 以下になるまで各イニシエータのキュー深度を下げます。

> 特定の 1 秒あたりの I/O スループットに必要なキュー深度を算出するには、次の式を使用します。
>
> 必要なキュー深度 = （ IOPS ） ×（応答時間）
>
> たとえば、応答時間 3 ミリ秒で 40 、 000 IOPS のスループットに必要なキュー深度は、 40 、 000 ×（ .003 ） = 120 です。

基本的な推奨構成である 32 個にキュー深度を制限した場合、ターゲットポートに接続できるホストの最大数は 64 です。ただし、キュー深度を 128 にした場合は、 1 つのターゲットポートに接続できるホストの最大数は 16 になります。キュー深度が大きいほど、 1 つのターゲットポートでサポートできるホストの数は少なくなります。キュー深度を小さくできないような要件がある場合は、ターゲットポートを増やしてください。

必要とされるキュー深度 3 、 840 は、ポートあたりの使用可能なキュー深度を超えています。ストレージ I/O のニーズが高い「大規模」ホストが 10 台あり、 I/O のニーズが低い「モール」ホストが 20 台あります。大規模ホストのイニシエータのキュー深度を 128 に、小規模ホストのイニシエータのキュー深度を 32 に設定します。

その結果、合計キュー深度は（ 10 × 128 ） + （ 20 × 32 ） = 1 、 920 になります。

使用可能なキュー深度を、各イニシエータに均等に分配できます。

そのため、イニシエータあたりのキュー深度は 2 、 048 ÷ 30 = 68 となります。

SAN ホストでキュー深度を設定します

ノードあたりおよび FC ポートのファンインあたりの ITN 数を最大にするために、ホストのキュー深度の変更が必要になる場合があります。

AIX ホスト

を使用して、AIXホストのキュー深度を変更できます `chdev` コマンドを実行しますを使用して行った変更 `chdev` コマンドはリブート後も維持されます。

例

- hdisk7 デバイスのキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- fcs0 HBA のキュー深度を変更するには、次のコマンドを使用します。

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  のデフォルト値 `num_cmd_elems` 200です最大値は 2 、 048 です。

  > 変更するには、必要に応じてHBAをオフラインにします `num_cmd_elems` を使用してオンラインに戻します `rmdev -l fcs0 -R` および `makdev -l fcs0 -P` コマンド

HP-UX ホスト

HP-UXホストのLUNまたはデバイスのキュー深度は、kernelパラメータを使用して変更できます `scsi_max_qdepth`。HBAのキュー深度は、カーネルパラメータを使用して変更できます `max_fcp_reqs`。

- のデフォルト値 `scsi_max_qdepth` 8です最大値は255です。

  `scsi_max_qdepth` を使用して、実行中のシステムで動的に変更できます `-u` オプションを選択します `kmtune` コマンドを実行します変更は、システム上のすべてのデバイスに有効です。たとえば、 LUN のキュー深度を 64 に増やすには、次のコマンドを使用します。

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  を使用して、個 々 のデバイスファイルのキュー深度を変更できます `scsictl` コマンドを実行しますを使用して変更を行います `scsictl` コマンドの設定は、システムのリブート後は維持されません。特定のデバイスファイルのキュー深度を表示および変更するには、次のコマンドを実行します。

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- のデフォルト値 `max_fcp_reqs` 512です最大値は 1024 です。

  を変更するには、カーネルを再構築し、システムを再起動する必要があります `max_fcp_reqs` 有効にします。たとえば、 HBA のキュー深度を 256 に変更するには、次のコマンドを使用します。

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris ホストの場合

Solaris ホストの LUN および HBA のキュー深度を設定できます。

- LUN のキュー深度の場合：ホストで使用中の LUN の数に LUN あたりのスロットル（ lun-queue-depth ）をかけた値が、ホストの tgt-queue-depth の値以下になる必要があります。
- Sunスタックのキュー深度の場合：標準ドライバでは、LUN単位またはターゲット単位ではサポートされていません `max_throttle` HBAレベルの設定。を設定するための推奨方法 `max_throttle` ネイティブドライバの値は、のデバイスタイプごと（VID_PID）レベルです `/kernel/drv/sd.conf` および

`/kernel/drv/ssd.conf` ファイル。ホストユーティリティでは、この値が MPxIO 構成では 64 、Veritas DMP 構成では 8 に設定されます。

手順

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. を検索します `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   デフォルト値はインストール時に 32 に設定されています。

4. 環境の構成に基づいて目的の値を設定します。
5. ファイルを保存します。
6. を使用してホストをリブートします `sync; sync; sync; reboot -- -r` コマンドを実行します

QLogic HBA の VMware ホスト

を使用します `esxcfg-module` HBAタイムアウト設定を変更するコマンド。を手動で更新します `esx.conf` ファイルは推奨されません。

手順

1. root ユーザとしてサービスコンソールにログオンします。
2. を使用します `#vmkload_mod -l` 現在ロードされているQlogic HBAモジュールを確認するコマンド。
3. Qlogic HBA の単一インスタンスの場合は、次のコマンドを実行します。

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   この例では qla2300_707 が使用されています。の出力に基づいて、適切なモジュールを使用します `vmkload_mod -l`。

4. 次のコマンドを使用して変更を保存します。

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. 次のコマンドを使用してサーバをリブートします。

   ```
   #reboot
   ```

6. 次のコマンドを使用して変更を確認します。
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Emulex HBA の VMware ホスト

を使用します `esxcfg-module` HBAタイムアウト設定を変更するコマンド。を手動で更新します `esx.conf`

ファイルは推奨されません。

手順

1. root ユーザとしてサービスコンソールにログオンします。
2. を使用します `#vmkload_mod -l grep lpfc` コマンドを実行して、どのEmulex HBAが現在ロードされているかを確認します。
3. Emulex HBA の単一インスタンスの場合は、次のコマンドを入力します。

   ```
   #esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
   ```

   > HBA のモジュールに応じて、最後の部分には lpfcdd_7xx または lpfcdd_732 を指定します。このコマンドでは lpfcdd_7xx モジュールを指定しています。の結果に基づいて、適切なモジュールを使用する必要があります `vmkload_mod -l`。

   このコマンドを実行すると、 lpfc0 で表される HBA に対して LUN のキュー深度を 16 に設定します。

4. Emulex HBA の複数のインスタンスの場合は、次のコマンドを実行します。

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   lpfc0 に対する LUN のキュー深度と lpfc1 に対する LUN のキュー深度が 16 に設定されます。

5. 次のコマンドを入力します。

   ```
   #esxcfg-boot -b
   ```

6. を使用してリブートします `#reboot`。

Emulex HBA の Windows ホスト

Windowsホストでは、を使用できます `LPUTILNT` Emulex HBAのキュー深度を更新するユーティリティ。

手順

1. を実行します `LPUTILNT` にあるユーティリティ `C:\WINNT\system32` ディレクトリ。
2. 右側のメニューから * Drive Parameters * （ドライブパラメータ）を選択します。
3. スクロールダウンして、 [**QueueDepth**] をダブルクリックします。

   > 150 より大きい * QueueDepth * を設定する場合は、次の Windows レジストリ値も適切に増やす必要があります。
   >
   > `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Qlogic HBA の Windows ホスト

Windowsホストでは、およびを使用できます `SANsurfer` Qlogic HBAのキュー深度を更新するHBAマネージャユーティリティ。

手順

1. を実行します `SANsurfer` HBAマネージャユーティリティ。
2. [* HBA ポート **>** 設定] をクリックします。
3. リスト・ボックスの * HBA ポートの詳細設定 * をクリックします。
4. を更新します `Execution Throttle` パラメータ

Emulex HBA の Linux ホスト

Linux ホストでは Emulex HBA のキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。

手順

1. 変更するキュー深度パラメータを特定します。

   ```
   modinfo lpfc|grep queue_depth
   ```

   キュー深度パラメータとその概要のリストが表示されます。使用しているオペレーティングシステムのバージョンに応じて、次のキュー深度パラメータを 1 つ以上変更できます。

   - `lpfc_lun_queue_depth`：特定のLUNのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_hba_queue_depth`：lpfc HBAのキューに格納できるFCコマンドの最大数（uint）
   - `lpfc_tgt_queue_depth`：特定のターゲットポートのキューに格納できるFCコマンドの最大数（uint）

     - `lpfc_tgt_queue_depth` パラメータは、Red Hat Enterprise Linux 7.xシステム、SUSE Linux Enterprise Server 11 SP4システム、および12.xシステムにのみ適用されます。

2. にキュー深度パラメータを追加して、キュー深度を更新します `/etc/modprobe.conf` ファイル（Red Hat Enterprise Linux 5.xシステム用）を参照してください `/etc/modprobe.d/scsi.conf` ファイル（Red Hat Enterprise Linux 6.xまたは7.xシステム、またはSUSE Linux Enterprise Server 11.xまたは12.xシステム用）

   使用しているオペレーティングシステムのバージョンに応じて、次のコマンドを 1 つ以上追加できます。

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

   詳細については、を参照してください "システム管理" を参照してください。

4. 変更したキュー深度パラメータの値が更新されていることを確認します。

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

キュー深度の現在の値が表示されます。

QLogic HBA の Linux ホスト

Linux ホストでは QLogic ドライバのデバイスキュー深度を更新できます。更新をリブート後も維持するには、新しい RAM ディスクイメージを作成してホストをリブートする必要があります。QLogic HBA のキュー深度を変更するには、 QLogic HBA の管理 GUI またはコマンドラインインターフェイス（ CLI ）を使用します。

このタスクでは、 QLogic HBA の CLI を使用して QLogic HBA のキュー深度を変更する方法を示します

手順

1. 変更するデバイスキュー深度パラメータを確認します。

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   変更できるのはのみです `ql2xmaxqdepth` キュー深度パラメータ。各LUNに設定できる最大キュー深度を指定します。RHEL 7.5 以降のデフォルト値は 64 です。RHEL 7.4 以前のデフォルト値は 32 です。

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. デバイスのキュー深度の値を更新します。

   - 永続的に変更する場合は、次の手順を実行します。

     i. にキュー深度パラメータを追加して、キュー深度を更新します `/etc/modprobe.conf` ファイル（Red Hat Enterprise Linux 5.xシステム用）を参照してください `/etc/modprobe.d/scsi.conf` Red Hat Enterprise Linux 6.xまたは7.xシステム、またはSUSE Linux Enterprise Server 11.xまたは12.xシステムのファイル： `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. 新しい RAM ディスクイメージを作成し、ホストをリブートして、リブート後も更新内容を維持します。

     詳細については、を参照してください "システム管理" を参照してください。

   - 現在のセッションだけでパラメータを変更する場合は、次のコマンドを実行します。

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     次の例では、キュー深度を 128 に設定します。

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. キュー深度の値が更新されたことを確認します。

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

キュー深度の現在の値が表示されます。

4. ファームウェアパラメータを更新してQLogic HBAのキュー深度を変更します `Execution Throttle` QLogic HBA BIOSからアクセスします。

   a. QLogic HBA の管理 CLI にログインします。

      ```
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      ```

   b. メインメニューからを選択します `Adapter Configuration` オプション

      ```
      [root@localhost ~]#
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      Using config file:
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
      Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
      Working dir: /root

      QConvergeConsole

              CLI - Version 2.2.0 (Build 15)

          Main Menu

          1:  Adapter Information
          **2:  Adapter Configuration**
          3:  Adapter Updates
          4:  Adapter Diagnostics
          5:  Monitoring
          6:  FabricCache CLI
          7:  Refresh
          8:  Help
          9:  Exit


              Please Enter Selection: 2
      ```

   c. アダプタ設定パラメータのリストからを選択します `HBA Parameters` オプション

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. HBA ポートのリストから、必要な HBA ポートを選択します。

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

HBA ポートの詳細が表示されます。

e. [HBA Parameters]メニューからを選択します `Display HBA Parameters` オプションを選択すると、の現在の値が表示されます `Execution Throttle` オプション

のデフォルト値 `Execution Throttle` オプションは65535です。

```
HBA Parameters Menu

=========================================================
HBA            : 2 Port: 1
SN             : BFD1524C78510
HBA Model      : QLE2562
HBA Desc.      : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version     : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=========================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
---------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
---------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Enter * を押して続行します。

b. [HBA Parameters]メニューからを選択します `Configure HBA Parameters` HBAパラメータを変更するオプション。

c. [Configure Parameters]メニューからを選択します `Execute Throttle` オプションを選択し、このパラメータの値を更新します。

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Enter * を押して続行します。

e. [Configure Parameters]メニューからを選択します `Commit Changes` 変更を保存するオプション。

f. メニューを終了します。