



SANの概念

ONTAP 9

NetApp
February 12, 2026

目次

SANの概念	1
iSCSIを使用したSANプロビジョニング	1
iSCSIターゲット ノードのネットワーク接続と名前	1
ストレージ システムのノード名	1
iSCSIのTCPポート	2
iSCSIサービス管理	2
iSCSIサービス管理	2
iSCSI認証の仕組み	2
iSCSIイニシエータのセキュリティ管理	3
iSCSIエンドポイントの分離	3
ONTAPのiSCSIイニシエータのCHAP認証について説明します	4
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	6
リストの使用によるパフォーマンスとセキュリティの向上	
ONTAPのInternet Storage Name Service (iSNS)	6
FCを使用したSANプロビジョニング	9
FCターゲット ノードをネットワークに接続する方法	9
FCノードの識別方法	9
WWPNの使用方法	9
World Wide Name (WWN) の割り当ての仕組み	10
FCスイッチの識別方法	10
NVMeを使用したSANプロビジョニング	11
SANボリューム	11
SANボリュームの概要	11
ボリューム プロビジョニング オプションの設定	13
SANボリュームの構成オプション	14
SAN環境でのボリューム移動に関する要件	15
フラクショナル リザーブの設定に関する考慮事項	15
SANホスト側のスペース管理	17
SnapCenterによるホスト管理の簡易化	17
igroupについて	18
igroupによるLUNアクセスの提供例	18
igroupのイニシエータのWWPNとiSCSIノード名の指定	19
仮想SAN環境を使用する利点	19
ESXホストのVMware VAAIパフォーマンスの向上	20
VAAI環境を使用するための要件	20
VAAI機能がESXでサポートされているかどうかの確認	21
SANコピー オフロード	21
Microsoftオフロード データ転送 (ODX)	21
NVMeコピー オフロードについて	24

SANの概念

iSCSIを使用したSANプロビジョニング

SAN環境においては、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）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 HBA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 インターフェイスを介して接続する。iSCSIに使用されるインターフェイスで、SMBやNFSなど、別のプロトコルのトラフィックも送信できます。
- ユニファイド ターゲット アダプタ（UTA）またはコンバージド ネットワーク アダプタ（CNA）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ノード名には、_iqn_と_eui_という2つの形式（タイプ指定子）があります。SVM iSCSI targetは常にiqnタイプ指定子を使用します。イニシエータはiqnタイプまたはeuiタイプ指定子のいずれかを使用できます。

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、その他のアプリケーションやサーバでは使用できません。

関連情報

["NetAppのマニュアル：ONTAP SANホスト構成"](#)

iSCSIサービス管理

iSCSIサービス管理

```
`vserver iscsi interface enable`または `vserver iscsi interface  
disable` コマンドを使用して、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できます。
```

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。

ホストで**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 ホスト バス アダプタ (HBA) 経由：iSCSI HBA は、ホスト オペレーティング システムに対して、ローカル ディスクを持つ SCSI ディスク アダプタとして表示されます。
- TCP / IP処理をオフロードするTCPオフロード エンジン (TOE) 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セッションの第一段階では、イニシエータはストレージ 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 システムでは、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、または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ーを認証します。

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：これは、イニシエーターがストレージ システムを認証できるようにするための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限って、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 - ストレージ システムはイニシエータに対する認証を必要としません。

イニシエータとその認証方法の一覧を定義できます。この一覧にないイニシエータに適用するデフォルトの認証方法も定義できます。

関連情報

["Data ONTAPを使用したWindowsマルチパス オプション：Fibre Channelと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提供します。iSCSIイニシエータのリストとそれぞれの認証方法を定義したり、認証リストにイニシエータとそれに関連付けられた認証方式を表示したり、認証リストにイニシエータを追加または削除したり、リストにないイニシエータのデフォルトのiSCSIイニシエータ認証方法を定義したりできます。

iSCSIエンドポイントの分離

既存の iSCSI セキュリティ コマンドは、IP アドレス範囲または複数の IP アドレスを受け入れることができます。

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。これは、発信元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をログインできないようにするための、新しい独自の識別機能です。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。

この新しい機能では、2つの新しいコマンドを使用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

`vserver iscsi security add-initiator-address-range` コマンドを使用して IP アドレス範囲または複数の IP アドレスを追加することで、iSCSI イニシエータのセキュリティ管理を改善します。

```
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

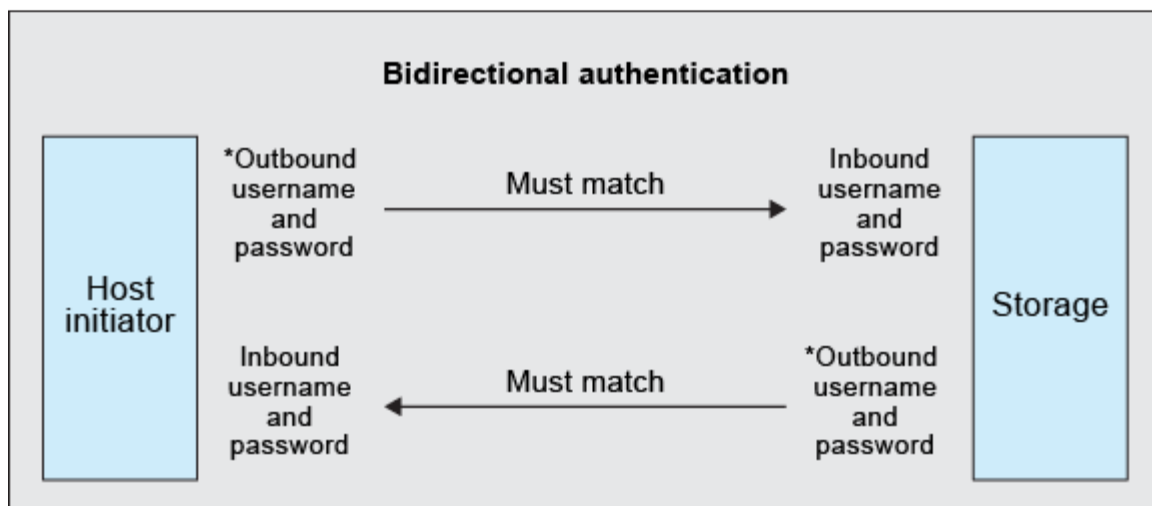
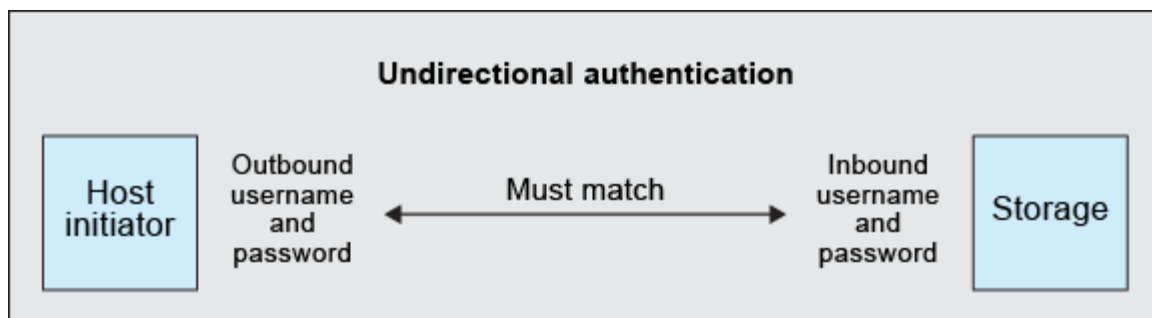
`vserver iscsi security remove-initiator-address-range` コマンドを使用して、IP アドレス範囲または複数の IP アドレスを削除します。

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

ONTAP の iSCSI イニシエータの CHAP 認証について説明します

Challenge Handshake Authentication Protocol (CHAP) は、iSCSI イニシエータとターゲットの間で認証に基づいた通信を可能にします。CHAP 認証を使用する場合、イニシエータとストレージ システムの両方で CHAP ユーザ名とパスワードを定義します。

iSCSI セッションの第一段階では、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 ユーザ名と CHAP アルゴリズムが含まれています。これに対し、ストレージ システムは CHAP チャレンジで応答します。CHAP 応答はイニシエータが提供します。ストレージ システムは CHAP 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。



*The outbound username and password for the host initiator must be different from the outbound username and password for the storage.

認証	アウトバウンド	インバウンド	一致？
一方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ホストイニシエーターのユーザー名とパスワード	ストレージのユーザー名とパスワード	一致する必要があります
双方向	ストレージのユーザー名とパスワード	ホストイニシエーターのユーザー名とパスワード	一致する必要があります

ホスト イニシエーターのアウトバウンド ユーザー名とパスワードは、ストレージ システムのアウトバウンド ユーザー名とパスワードとは異なる必要があります。

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、次のガイドラインに従ってください。

- インバウンド ユーザー名と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、イニシエーターのアウトバウンド CHAP 設定にも同じユーザー名と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 ユーザー名と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、イニシエーターのインバウンド CHAP 設定にも同じユーザー名と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、同じユーザー名とパスワードを使用できません。

- CHAPユーザ名は1～128バイトで指定できます。

システムでは null ユーザー名は許可されません。

- CHAPパスワード（シークレット）は1～512バイトで指定できます。

パスワードは16進数値または文字列で入力できます。16進数値の場合は、先頭に「0x」または「0X」を付けて入力してください。

システムでは null パスワードは許可されません。

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、スペースを使用できます。ただし、ホストでの制限の対象にはなりません。これらの文字が許可されていないホストでは、使用することはできません。



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に、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かかわらず16バイトです。

追加の制限については、イニシエータのドキュメント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 リストの使用によるパフォーマンスとセキュリティの向上

iSCSIインターフェイス 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の数を制限できるため、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 `SendTargets` コマンドを使用して検出セッションを開始すると、アクセスリストに登録されているLIF（ネットワークインターフェイス）に関連付けられたIPアドレスを受け取ります。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ことで、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。

ONTAPのInternet Storage Name Service (iSNS)

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サーバでは、ネットワークでアクティブなiSCSIデバイスに関する情報（IPアドレス、iSCSIノード名（IQN）、ポータルグループなど）が維持されます。

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、使用するStorage Virtual Machine (SVM) がInternet Storage Name Service (iSNS) サーバに正しく登録されていることを確認してください。

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サーバではInternet Storage Name Service (iSNS) プロトコルが使用され、ネットワークでアクティブなiSCSIデバイスに関する情報 (IPアドレス、iSCSIノード名[IQN]、ポータル グループなど) が維持されます。

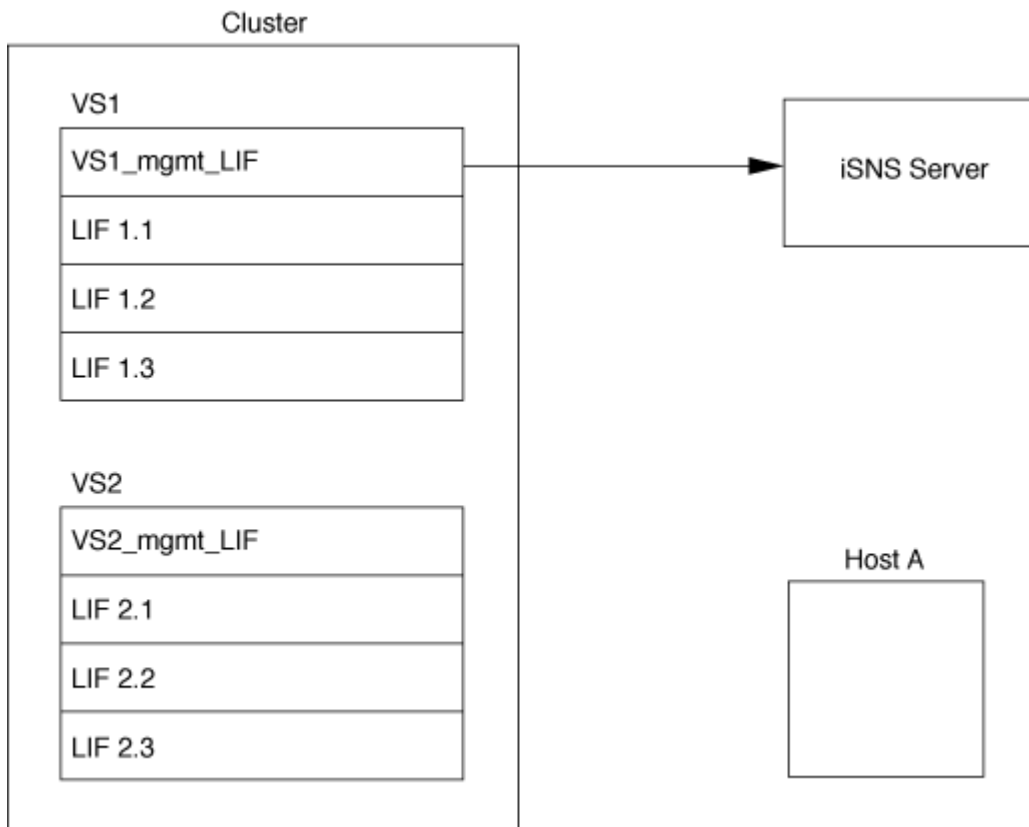
iSNSプロトコルを使用すると、IPストレージ ネットワークでiSCSIデバイスを自動的に検出し、管理できるようになります。iSCSIイニシエータが、iSNSサーバに照会することにより、iSCSIターゲット デバイスを検出します。

NetApp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、NetAppがサポートするベンダーから取得できます。

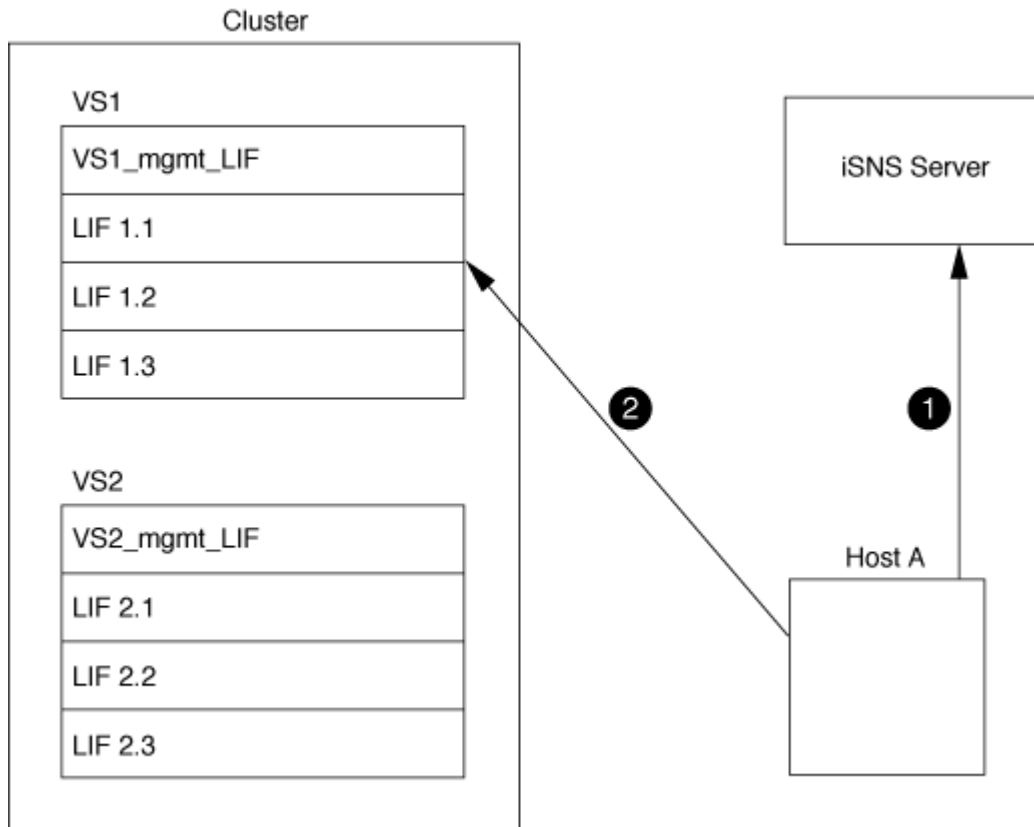
SVMとiSNSサーバの連動

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サーバに登録します。iSNS登録中、SVMはすべてのiSCSI LIFをSVM管理LIF経由でiSNSサーバに送信します。iSNS登録が完了すると、iSNSサーバは「VS1」でiSCSIサービスを提供しているすべてのLIFのリストを取得します。クラスタに複数のSVMが含まれている場合、iSNSサービスを利用するには、各SVMを個別にiSNSサーバに登録する必要があります。



次の例では、iSNSサーバがターゲットへの登録を完了すると、ステップ1に示すように、ホストAはiSNSサーバを介して「VS1」のすべてのLIFを検出できます。ホストAが「VS1」のLIFの検出を完了すると、ステップ2に示すように、ホストAは「VS1」内の任意のLIFとの接続を確立できます。「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」内のどのLIFも認識しません。



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のみとなります。

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。

設定変更を行ってからONTAPがiSNSサーバに更新を送信するまでの間に、数分間の遅延が発生する場合があります。iSNSサーバ上のiSNS情報を強制的に即時更新するには、次の手順を実行します：`vserver iscsi isns update`。詳細については、"[ONTAPコマンド リファレンス](#)"の`vserver iscsi isns update`を参照してください。

iSNSの管理用コマンド

ONTAPには、iSNSサービスを管理するための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	<code>vserver iscsi isns create</code>
iSNSサービスを開始する	<code>vserver iscsi isns start</code>
iSNSサービスを変更する	<code>vserver iscsi isns modify</code>
iSNSサービスの設定を表示する	<code>vserver iscsi isns show</code>

登録済みのiSNS情報を強制的に更新する	<code>vserver iscsi isns update</code>
iSNSサービスを停止する	<code>vserver iscsi isns stop</code>
iSNSサービスを削除する	<code>vserver iscsi isns delete</code>
コマンドのマニュアル ページを表示する	<code>man command name</code>

`vserver iscsi isns`の詳細については、link:<https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+iscsi+isns>["ONTAPコマンド リファレンス"]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いるので、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、スイッチのファブリック ネーム サービスに各SVMのLIFのWorld Wide Port Name (WWPN) が登録されます。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を使用したホストからノードへの直接接続はサポートされていません。接続にはNPIVが必要なため、スイッチを使用する必要があります。iSCSIセッションの場合、ネットワーク経由の接続または直接接続がサポートされます。ONTAPはこれら両方の方法をサポートしています。

FCノードの識別方法

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

WWPNの使用方法

WWPNは、FCをサポートするように設定されたSVM内の各LIFを識別します。これらのLIFは、クラスタ内の各ノードの物理FCポート（ノードでFCまたはFCoEとして設定されたFCターゲット カード、UTA、またはUTA2）を使用します。

- イニシエータ グループの作成

ホストのHBAのWWPNは、イニシエータ グループ (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 システムのLUNをigroupにマッピングすると、このグループ内のす

すべてのイニシエータに対し、この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、そのLUNがディスクとして表示されません。

また、ポートセットを作成することで、特定のターゲット ポートに関してだけ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

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を組み合わせ使用し、SVMおよびFC LIFを識別します。一部のOSでは、パーシスタント バインディングがないと、ホストにおいて同じターゲットIDでLUNが表示されません。

World Wide Name (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

Fibre Channelスイッチには、デバイス自体に1つ、デバイスの各ポートに1つ、Worldwide Port Name (WWPN) が割り当てられています。

たとえば次の図では、16ポートのBrocadeスイッチの各ポートにWWPNが割り当てられています。特定のスイッチのポート番号のレイアウトについては、ベンダーが提供しているそのスイッチのドキュメント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

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じように、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と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ません。

ONTAP 9.5以降、NVMeを使用したホスト側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、ライセンスを取得するための90日間の猶予期間が与えられます。["ONTAP One"](#)をお持ちの場合は、NVMeライセンスも含まれています。ライセンスは次のコマンドで有効化できます：

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

関連情報

["NetAppテクニカル レポート4684：『Implementing and Configuring Modern SANs with NVMe/FC』"](#)

SANボリューム

SANボリュームの概要

ONTAPでは、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つを提供しています。ボリューム スペースおよびONTAPブロック共有テクノロジのスペース要件が、オプションごとに異なる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NAS共有それぞれに専用のFlexVol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素化され、Active IQ Unified Manager (旧OnCommand Unified Manager) でのFlexVol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、作成時に追加のスペースが確保されません。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。

す。

FlexVolボリュームの`-space-guarantee`オプションを`none`に設定して、シンプロビジョニング ボリュームを作成します。

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は、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、作成時にアグリゲートから十分なストレージが確保されます。シックプロビジョニングを利用するようにボリュームを設定した場合は、ONTAPの任意のStorage Efficiency機能（圧縮や重複排除など）を使用して、さらに大容量のストレージ要件にも事前に対応できます。

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

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使用するボリュームが作成されると、ONTAPはボリュームサイズに合わせてアグリゲートからストレージスペースを確保します。ブロック共有テクノロジーによって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ている場合、ONTAPは保護データオブジェクト（スナップショット、FlexCloneファイル、LUN）を削除して、それらが保持しているスペースを解放しようとし、ONTAPが保護データオブジェクトを上書きに必要なスペースに追いつくだけの速度で削除できる限り、書き込み処理は継続して成功します。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ません：

- 重複排除、圧縮、コンパクションなどのストレージ効率化テクノロジー
- Microsoftオフロード データ転送（ODX）

FlexVolボリュームの`-space-slo`（サービス レベル目標）オプションを`semi-thick`に設定して、セミシック プロビジョニング ボリュームを作成します。

スペース リザーブ ファイルおよびスペース リザーブLUNでの使用

スペース予約ファイル（LUN）とは、作成時にストレージが割り当てられるファイルです。従来、NetAppでは、スペース リザーベーションが無効になっているLUN（スペース予約されていないLUN）を指すために「シンプロビジョニングLUN」という用語が使用されてきました。

*注：*スペース予約されていないファイルは、通常、「thin-provisioned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/ファイルのスペース リザーベーション	上書き	保護データ ²	ストレージ効率 ³
シック	サポート	保証済み ¹	保証	サポート
シン	効果なし	なし	保証	サポート
セミシック	サポート	ベストエフォート ¹	ベスト エフォート	サポート対象外

注記

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 リザー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、スナップショット、および自動削除対象としてマークされたFlexCloneファイルと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、NetApp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により、ホスト アプリケーションはSCSI機能（ブロック環境でのLUNのスペース再生機能やスペース監視機能など）をサポートできるようになります。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 `space-allocation` 設定を使用して、LUN上でT10シンプロビジョニングのサポートを有効化または無効化します。ONTAP `space-allocation enable` 設定を使用して、LUN上でT10 SCSIシンプロビジョニングを有効にします。

"[ONTAP コマンド リファレンス](#)"の `[-space-allocation {enabled|disabled}]` コマンドには、T10 シン プロビジョニングのサポートを有効/無効にする方法と、LUNでT10 SCSIシン プロビジョニングを有効にする方法の詳細情報が含まれています。

ボリューム プロビジョニング オプションの設定

ボリュームを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用に設定できます。

タスク概要

``-space-slo`` オプションを ``thick`` に設定すると、次のことが保証されます：

- ボリューム全体がアグリゲートに事前割り当てされています。`volume create` コマンドまたは `volume modify` コマンドを使用して、ボリュームの ``-space-guarantee`` オプションを設定することはできません。
- 上書きに必要なスペースの100%が予約されています。`volume modify` コマンドを使用してボリュームの ``-fractional-reserve`` オプションを設定することはできません。

``-space-slo`` オプションを ``semi-thick`` に設定すると、次のことが保証されます：

- ボリューム全体がアグリゲートに事前割り当てされています。`volume create` コマンドまたは `volume modify` コマンドを使用して、ボリュームの ``-space-guarantee`` オプションを設定することはできません。
- 上書き用のスペースは予約されていません。`volume modify` コマンドを使用して、ボリュームの ``-fractional-reserve`` オプションを設定できます。
- Snapshotの自動削除が有効になっています。

手順

1. ボリューム プロビジョニング オプションを設定します。

```
volume create -vserver vs1 -volume vol1 -aggregate  
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

この `space-guarantee` オプションは、AFFシステムおよび非AFF DPボリュームの場合はデフォルトで `none` になります。それ以外の場合は、デフォルトで `volume` になります。既存のFlexVolボリュームの場合は、`volume modify` コマンドを使用してプロビジョニングオプションを設定してください。

次のコマンドは、SVM vs1のvol1をシンプロビジョニング用に設定します。

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

次のコマンドは、SVM vs1のvol1をシックプロビジョニング用に設定します。

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

次のコマンドは、SVM vs1のvol1をセミシックプロビジョニング用に設定します。

```
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、ボリュームのサイズを事前設定した最大サイズまでONTAP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。

ボリュームの自動拡張は、Snapshot作成をサポートするためにトリガーできません。Snapshotを作成しようとした際にボリュームに十分なスペースがない場合は、ボリュームの自動拡張が有効であっても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、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、ONTAPで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の自動削除は、次のいずれかの状況が発生すると、Snapshotを自動的に削除します。

- ボリュームがフルに近い状態の場合
- Snapshotリザーブ スペースがほぼいっぱいです。
- オーバーライト リザーブ スペースがフルの場合

スナップショットの自動削除を設定すると、古いものから新しいものへ、または新しいものから古いものの順にスナップショットを削除できます。スナップショットの自動削除では、クローンボリュームまたはLUN内のスナップショットにリンクされているスナップショットは削除されません。

ボリュームに追加のスペースが必要で、自動拡張とスナップショットの自動削除の両方を有効にしている場合、デフォルトでONTAPはまず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が確保できない場合は、スナップショット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、ボリューム内でスナップショット用に予約される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は、他の目的には使用できません。Snapshotリザーブに割り当てられたスペースがすべて使用されると、スナップショットはボリューム上の追加のスペースを消費し始めます。

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前に、特定の要件を満たす必要があります。

- ボリュームにLUNが含まれている場合は、クラスタの各ノードに接続するパス（LIF）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（Single Point of Failure）が排除され、コンポーネント障害からシステムを保護できます。

- 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（_LUN オーバーライト リザーブ_とも呼ばれます）を使用すると、FlexVolボリューム内のスペース リザーベーションされたLUNとファイルに対するオーバーライト リザーブを無効にすることができます。これによりストレージ使用率を最

大化できますが、スペース不足による書き込み操作の失敗によって環境に悪影響が出る場合は、この構成に課される要件を理解する必要があります。

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ます。有効な値は`0`と`100`パーセントのみです。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`0`に設定すると、ストレージ使用率が向上します。ただし、ボリュームギャランティを`volume`に設定していても、ボリューム内のデータにアクセスするアプリケーションで、ボリュームの空き容量が不足している場合、データ障害が発生する可能性があります。ただし、ボリュームを適切に設定し、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は、フラクショナルリザーブを`0`に設定したボリュームに対して、以下の_すべて_の要件が満たされている場合に「ベストエフォート」の書き込み保証を提供します：

- 重複排除を使用していない
- 圧縮を使用していない
- FlexCloneサブファイルを使用していない
- 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る

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 オフロードを使用していない
- ボリューム保証が`volume`に設定されています
- ファイルまたはLUNのスペース リザーベーションは `enabled`
- ボリュームSnapshotリザーブは`0`に設定されています
- ボリュームスナップショットの自動削除は、`enabled`コミットメントレベルが`destroy、破棄リストが`lun_clone,vol_clone,cifs_share,file_clone,sfsr、トリガーが`volume`で実行されます。`

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。

変更率が高い場合、上記の必要な構成設定をすべて使用していても、まれにSnapshotの自動削除が遅れてボリュームの容量が不足する可能性があることに注意してください。

さらに、ボリュームの自動拡張機能をオプションで使用して、ボリュームのスナップショットを自動的に削除する必要が生じる可能性を減らすことができます。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容量を監視する必要があります。アグリゲートがいっぱいになり、ボリュームの拡張ができなくなると、ボリュームの空き容量が枯渇するにつれて、より多くのスナップショットが削除される可能性があります。

上記の構成要件をすべて満たすことができず、ボリュームの容量不足を回避する必要がある場合は、ボリュームのフラクショナルリザーブ設定を`100`に設定する必要があります。これにより、事前により多くの空き容量が必要になりますが、上記のテクノロジーが使用されている場合でもデータ変更操作が成功することが保証されます。

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	デフォルトの部分リザーブ	有効な値
Volume	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利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かネームスペースに格納されています。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。一方、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。この場合、ホストとストレージ システムの双方で、200GBの空きスペースが報告されます。ここでホストに100GBのデータが書き込まれた場合、この時点では、ホストもストレージ システムも、使用済みスペースが100GB、未使用スペースが100GBと報告します。

次に、ホストから50GBのデータが削除されました。このとき、ホスト側では使用済みスペースが50GB、未使用スペースが150GBであると報告されます。一方、ストレージ システム側で報告される数値は、依然として使用済みスペース100GB、未使用スペース100GBとなります。

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、複数のストレージ システム間に分散できるストレージ プールから仮想ディスクを簡単に作成し、ストレージ プロビジョニング タスクを自動化して、ホスト データと一致するスナップショットからスナップショットとクローンを作成するプロセスを簡素化できます。

NetApp製品ドキュメントで ["SnapCenter"](#)の詳細を参照してください。

関連リンク

["SANプロトコルのONTAPスペース割り当ての有効化"](#)

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にマッピングするためには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は、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。

次の表は、ストレージ システムにアクセスする4つのホストを、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ています。クラスタ化されたホスト (Host3およびHost4) は、どちらも同じ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を持つホスト	igroup	igroupに追加されたWWPN、IQN、EUI	igroupにマッピングされた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個) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	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を持つホスト	igroup	igroupに追加されたWWPN、IQN、EUI	igroupにマッピングされたLUN
Host3、マルチパス、Host4でクラスタ構成 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	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/qtrees1/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	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4 /vol/vol2/qtrees1/lun5

igroupのイニシエータのWWPNとiSCSIノード名の指定

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。

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内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のアクティブなiSCSI LIFまたはFC LIFから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、イニシエータがLUNへのアクセスに使用するLIFを制限できます。

ESXホストのVMware VAAIパフォーマンスの向上

ONTAPは、ESXホストがESX 4.1以降を実行している場合、特定のVMware vStorage APIs for Array Integration (VAAI) 機能をサポートします。これらの機能は、ESXホストからストレージシステムへの処理のオフロードとネットワークスループットの向上に役立ちます。ESXホストは、適切な環境でこれらの機能を自動的に有効化します。

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に関与することなく、LUN間またはLUN内でのデータ転送を開始できます。これにより、ESXのCPUサイクルが節約され、ネットワークスループットが向上します。拡張コピー機能（「コピー オフロード」とも呼ばれます）は、仮想マシンのクローン作成などのシナリオで使用されます。ESXホストによって呼び出されると、コピー オフロード機能は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をコピーします。コピー オフロードは、以下の方法でデータを転送します：

- LUN内
- ボリューム内のLUN間
- ストレージ仮想マシン（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 この機能呼び出すことができない場合は、ESXホストはコピー操作に標準のREADコマンドとWRITEコマンドを自動的に使用します。

- WRITE_SAME

この機能は、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作業をオフロードします。ESXホストは、ファイルのゼロフィルなどの操作でこの機能を使用します。

- COMPARE_AND_WRITE

この機能は、特定のファイルアクセスの同時実行制限をバイパスし、仮想マシンの起動などの操作を高速化します。

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、適切な環境を設定するとESXホストによって自動的に呼び出されます。

環境要件は次のとおりです：

- ESXホストはESX 4.1以降を実行している必要があります。
- VMwareデータストアをホストするNetApp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宛先は、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必要があります。



コピー オフロード機能は現在、異なるストレージシステムでホストされているVMwareデータストア間でのデータのコピーをサポートしていません。

VAAI機能がESXでサポートされているかどうかの確認

ESX オペレーティング システムが VAAI 機能をサポートしているかどうかを確認するには、vSphere Client を確認するか、ホストにアクセスする他の手段を使用します。ONTAP はデフォルトで SCSI コマンドをサポートしています。

ESXホスト詳細設定を確認することで、VAAI機能が有効になっているかどうかを確認できます。表は、ESX 制御名に対応するSCSIコマンドを示しています。

SCSIコマンド	ESXコントロール名 (VAAI機能)
EXTENDED_COPY	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARE_AND_WRITE	HardwareAcceleratedLocking

SANコピー オフロード

Microsoftオフロード データ転送 (ODX)

Microsoft Offloaded Data Transfer (ODX) は、*copy offload* と呼ばれ、ホスト コンピューター経由でデータを転送せずに、ストレージ デバイス内または互換性のあるストレージ デバイス間で直接データを転送することを可能にします。

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。コピー オフロード機能を使用するためには、VMwareとWindowsそれぞれのオペレーティング システム環境の要件を満たすようにシステムを構成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する可能性があります。["非整列LUNの詳細"](#)。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXをサポートしています。

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、コピーが同じボリューム内で行われるとパフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、同じボリュームで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またがってコピーを実行する場合は、ホストベースのコピーの場合ほど大幅にはパフォーマンスが向上しない可能性があります。

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の使用要件

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：2GB

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"](#)

- 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。

- 仮想ハードディスク（VHD）の作成と変換、スナップショットの管理、仮想マシン間のファイルのコピーなどのHyper-V管理操作
- エクスプローラ操作
- Windows PowerShellコピーコマンド
- Windows コマンド プロンプトのコピー コマンド Microsoft TechNet ライブラリには、Windows サーバーおよびクライアントでサポートされている ODX アプリケーションに関する詳細情報が含まれています。

- 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の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"](#)

特殊なシステム ファイルの要件

qtree内のODXファイルは削除できます。テクニカルサポートから指示がない限り、その他の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り、ODX転送中に使用されるデータのポイントインタイム表現が可能になります。以下のシステムファイルは、データがオフロードされたLUNまたはファイルを含む各ボリュームのルートレベルにあります：

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

```
`copy-offload delete-tokens -path dir_path -node  
_node_name_` コマンドを使用して、ODXファイルを含むqtreeを削除できます。
```

ODXの使用事例

SVMでODXを使用する前にユースケースについて確認し、どのような場合にパフォーマンスが向上するかを判断できるように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サーバおよびクライアントで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、以下の事例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

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

- ボリュームとノードが異なり、SVMは同じ

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

- SVMが異なり、ノードは同じ

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

- SVMとノードが異なる

ソースとデスティネーションのファイルまたはLUNは、異なるノード上の異なるボリュームにあります。

データは異なるSVMに所有されます。

- クラスタ間

ソースとデスティネーションの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。

さらに、いくつかの特殊なユースケースがあります。

- ONTAPのODXの実装では、ODXを使用してSMB共有とFC / iSCSI接続の仮想ドライブとの間でファイルをコピーできます。

Windowsエクスプローラ、Windows CLI (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でODXコピー オフロードを使用すると、SMB共有と接続されたLUNが同じクラスタにある場合に、それらの間でシームレスにファイルを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。

NVMeコピー オフロードについて

NVMeコピー オフロードにより、NVMeホストはコピー処理をホストCPUからONTAPストレージ コントローラのCPUにオフロードできます。ホストは、CPUリソースをアプリケーション ワークロード用に確保しながら、あるNVMeネームスペースから別のNVMeネームスペースにデータをコピーできます。

例えば、パフォーマンス分散を改善するためにストレージワークロードの再バランス調整が必要だとします。これには、平均サイズがそれぞれ500 GBのNVMeネームスペースを45個含む10台の仮想マシン (VM) を移行する必要があります。つまり、約22.5 TBのデータをコピーする必要があるということです。ホストは、データ移行に自身のCPUを使用する代わりに、NVMeコピー オフロードで、データのコピー中にアプリケーションワークロード用のCPUリソースが減少することを防ぐことができます。

NVMeコピー オフロードのサポートと制限事項

NVMeコピー オフロードはONTAP 9.18.1以降でサポートされます。ONTAPはNVMeコピー オフロードを開始できません。ホストによってサポートされ、開始される必要があります。

ONTAPを使用したNVMeコピー オフロード処理には、次の制限事項があります：

- サポートされるコピー操作の最大サイズは16MBです。
- データは同じサブシステム内のNVMe名前空間間でのみ移行できます。
- データは同じ HA ペア内のノード間でのみ移行できます。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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