iSCSIサービスの管理

ONTAP 9

NetApp
December 20, 2024

目次

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

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

ホストでの**iSCSI**の実装方法

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）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、ログイン要求を許可または拒否するか、ログインが不要であると判断します。

iSCSI認証方式は次のとおりです。

- Challenge Handshake Authentication Protocol（CHAP）--イニシエータはCHAPユーザ名と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 --ストレージシステムはイニシエータの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。このリストにないイニシエータに適用される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アドレスの範囲または複数のIPアドレスを指定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際に、発信元IPアドレスを提供する必要があります。この新機能は、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がクラスタにログインできないようにすることで、一意の識別方式を提供します。サポート対象外または不明なIPアドレスから発信されたイニシエータではログインがiSCSIセッションレイヤで拒否されるため、イニシエータはクラスタ内のLUNまたはボリュームにアクセスできません。

既存のエントリの管理に役立つ2つの新しいコマンドを使用して、この新機能を実装します。

イニシエータのアドレス範囲を追加する

iSCSIイニシエータのセキュリティ管理を改善するには、IPアドレスの範囲を追加するか、コマンドを使用して複数のIPアドレスを追加し `vserver iscsi security add-initiator-address-range`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

IPアドレスの範囲または複数のIPアドレスを削除するには、コマンドを使用し `vserver iscsi security remove-initiator-address-range`ます。

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

CHAP認証とは

Challenge Handshake Authentication Protocol（CHAP）を使用すると、iSCSIイニシエ

ータとターゲット間の認証された通信が可能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ユーザ名と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ユーザ名とCHAPアルゴリズムが含まれます。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応答を提供します。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認証の使用に関するガイドライン

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とパスワードをストレージシステムで定義する場合は、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名とパスワードも定義して双方向認証を有効にする場合は、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、同じユーザ名とパスワードを使用できません。
- CHAPユーザ名には1~128バイトを指定できます。

  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バイトを指定できます。

  パスワードには、16進数の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、これはホストの制限の対象となります。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、それらを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、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が使用されてい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。

iSCSIインターフェイスアクセスリストを使用したイニシエータインターフェイスの制限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、アクセスリストにあるLIF（ネットワークインターフェイス）に関連付けられたIPアドレスがイニシエータ `SendTargets`に渡されます。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上のiSCSIデバイスの自動検出と管理を可能にするプロトコルです。iSNSサーバでは、ネットワーク上でアクティブな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。

ネットワークにiSNSサーバがない場合は、各ターゲットがホストから認識できるように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、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（IPアドレス、iSCSIノード名（IQN）、ポータルグループなど）を維持します。

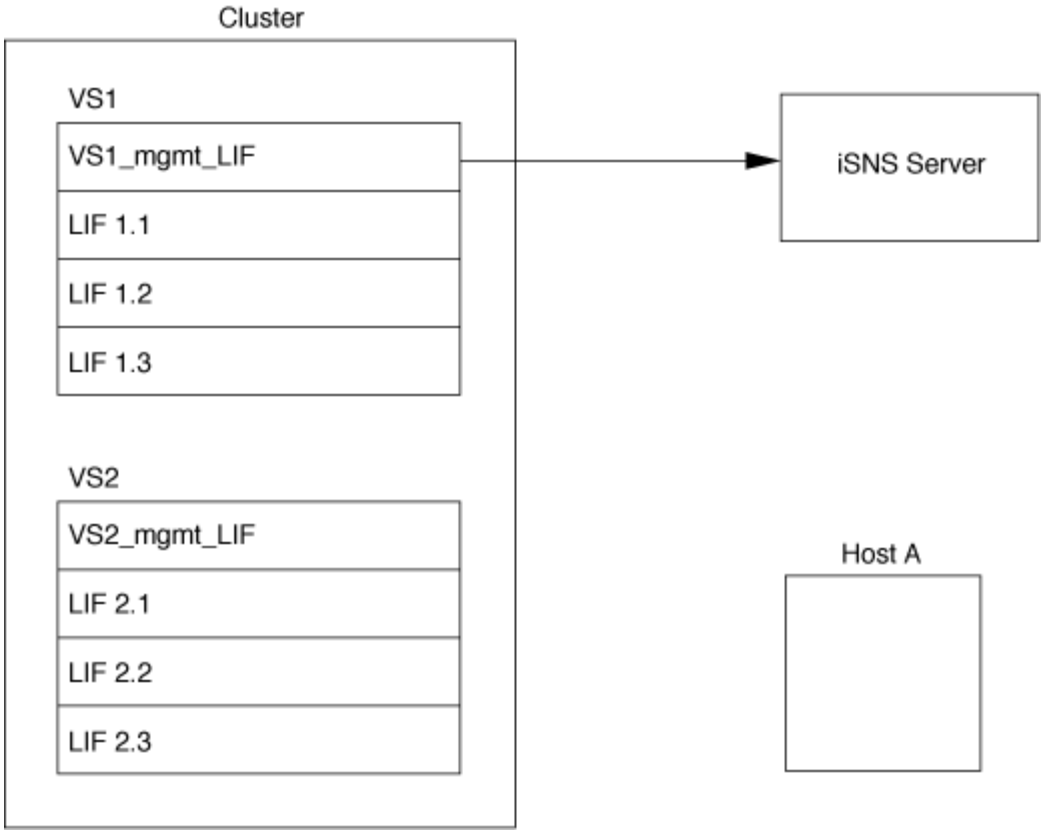
iSNSプロトコルを使用すると、IPストレージネットワーク上のiSCSIデバイスの自動検出と管理が可能になります。iSCSIイニシエータは、iSNSサーバに照会してiSCSIターゲットデバイスを検出できます。

NetAppでは、iSNSサーバの提供や再販は行われません。これらのサーバは、NetAppでサポートされているベンダーから入手できます。

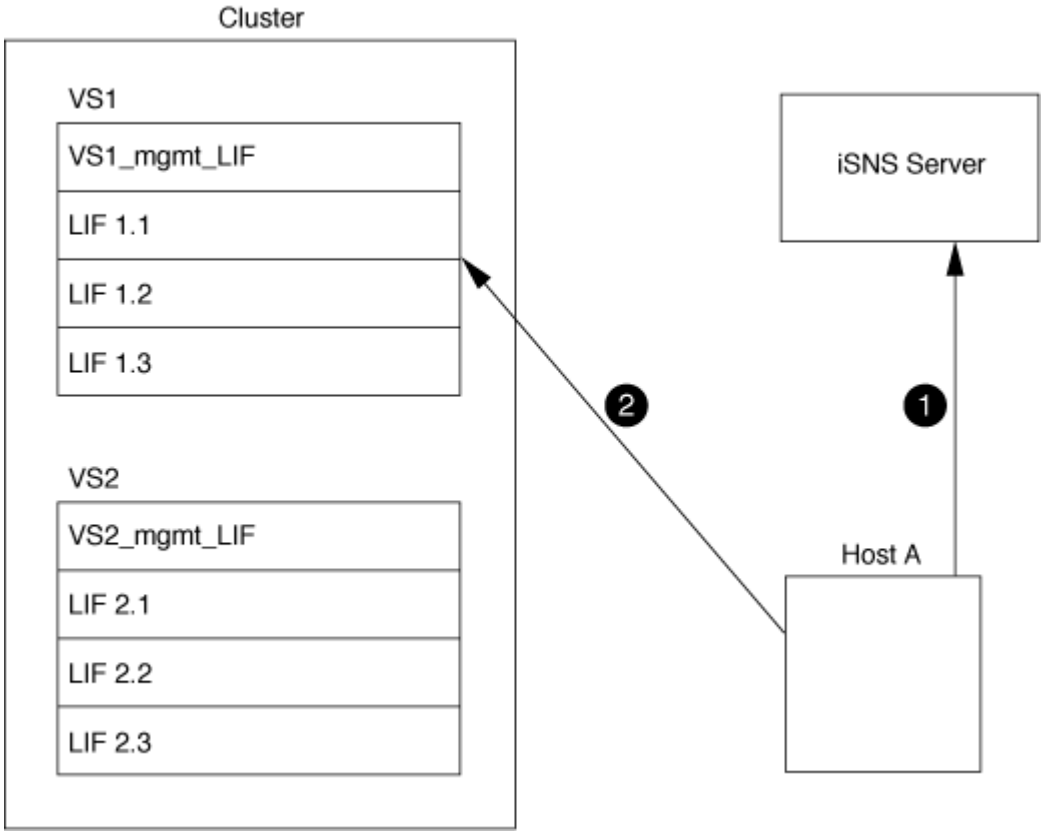
SVMとiSNSサーバの連動

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。クラスタに複数のSVMが含まれている場合は、iSNSサービスを使用するために、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した場合、ホストはインターフェイスアクセスリストに定義されているLIFのみを使用してターゲットにアクセスできます。

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	`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サービスを停止する	`vserver iscsi isns stop`
iSNSサービスを削除する	`vserver iscsi isns delete`
コマンドのマニュアルページを表示する	`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。

著作権に関する情報

商標に関する情報