



# **NetApp SnapMirror Active Syncと Microsoft ストレッチクラスタを使用して同期 レプリケーションを設定する**

NetApp virtualization solutions

NetApp  
August 18, 2025

# 目次

|                                           |    |
|-------------------------------------------|----|
| NetApp SnapMirror Active Syncと            |    |
| Microsoft ストレッチ クラスターを使用して同期レプリケーションを設定する | 1  |
| はじめに                                      | 1  |
| ユースケース                                    | 1  |
| ソリューション アーキテクチャ                           | 2  |
| Microsoft ストレッチ フェールオーバー クラスターをインストールする   | 3  |
| クラスター間ピアリングの作成                            | 5  |
| ONTAPでメディアエーターを構成する                       | 6  |
| 対称アクティブ/アクティブ保護を構成する                      | 8  |
| クラスターフェイルオーバー検証テストを実行する                   | 9  |
| まとめ                                       | 11 |

# NetApp SnapMirror Active SyncとMicrosoft ストレッチ クラスタを使用して同期レプリケーションを設定する

SnapMirror Active Sync を使用して、Microsoft ストレッチ フェイルオーバー クラスタ間の同期の双方向レプリケーションを構成します。この手順には、ストレッチ フェイルオーバー クラスタのインストール、クラスタ間ピアリングの作成、ONTAPを使用したメディエーターの構成、対称アクティブ/アクティブ保護の有効化、およびクラスタ フェイルオーバー検証テストの実行が含まれます。

## はじめに

ONTAP 9.15.1 以降、SnapMirrorアクティブ同期は対称アクティブ/アクティブ展開をサポートし、双方向同期レプリケーションを使用して保護された LUN の両方のコピーからの読み取りおよび書き込み I/O 操作を可能にします。Windows ストレッチ クラスタは、複数の地理的な場所にまたがって高可用性と災害復旧を提供する Windows フェイルオーバー クラスタ機能の拡張機能です。SnapMirrorアクティブ同期対称アクティブ/アクティブと、Windows フェイルオーバー クラスタリングなどのクラスタ化されたアプリケーションを使用すると、Microsoft Hyper-V のビジネス クリティカルなアプリケーションの継続的な可用性を実現し、予期しないインシデント発生時に RTO と RPO をゼロにすることができます。このソリューションには次の利点があります。

- データ損失ゼロ: データが同期的に複製され、リカバリポイント目標 (RPO) がゼロになることを保証します。
- 高可用性と負荷分散: 両方のサイトがリクエストをアクティブに処理し、負荷分散と高可用性を実現します。
- ビジネス継続性: 対称型のアクティブ/アクティブ構成を実装して、両方のデータセンターがアプリケーションをアクティブに提供し、障害発生時にシームレスに引き継ぐことができますようにします。
- パフォーマンスの向上: 対称アクティブ/アクティブ構成を使用して、複数のストレージ システムに負荷を分散し、応答時間と全体的なシステム パフォーマンスを向上させます。

このホワイト ペーパーでは、Microsoft ストレッチ フェイルオーバー クラスタ間のSnapMirrorアクティブ同期テクノロジーによる同期双方向レプリケーションについて説明します。これにより、MSSQL や Oracle などのマルチサイト アプリケーション データが両方のサイトでアクティブにアクセス可能になり、同期されます。障害が発生した場合、アプリケーションはデータの損失やアクセスの損失なく、残りのアクティブ サイトに直ちにリダイレクトされ、高可用性、災害復旧、地理的な冗長性が実現されます。

## ユースケース

サイバー攻撃、停電、自然災害などの障害が発生した場合、グローバルに接続されたビジネス環境では、データ損失ゼロでビジネスクリティカルなアプリケーション データを迅速に回復することが求められます。こうした要求は、金融業界や、一般データ保護規則 (GDPR) などの規制要件を遵守する業界では高まっています。対称型のアクティブ/アクティブ構成を導入して、地理的に分散した場所間でデータを複製し、データへのローカル アクセスを提供し、地域的な停止が発生した場合でも継続性を確保します。

SnapMirrorアクティブ同期のユース ケースは次のとおりです。

アプリケーションの導入による目標復旧時間 (RTO) ゼロの実現

SnapMirrorアクティブ同期の展開では、プライマリ クラスターとミラー クラスターが存在します。プライマリ クラスター内の LUN (L1P) にはセカンダリ上にミラー (L1S) があり、読み取りと書き込みはホット プロキシミティ設定に基づいてホストのローカル サイトによって提供されます。

アプリケーションの導入による**RTO**ゼロまたは**TAF**の実現

透過的アプリケーション フェイルオーバー (TAF) は、ホスト MPIO ソフトウェア ベースのパス フェイルオーバーに基づいており、ストレージへの中断のないアクセスを実現します。両方の LUN コピー (たとえば、プライマリ (L1P) とミラー コピー (L1S)) は同じ ID (シリアル番号) を持ち、ホストに対して読み取り/書き込み可能として報告されます。

クラスタ アプリケーション

VMware vSphere Metro Storage Cluster (vMSC)、Oracle RAC、SQL を使用した Windows フェールオーバー クラスターリングなどのクラスター化されたアプリケーションでは、パフォーマンスのオーバーヘッドなしで VM が他のサイトにフェールオーバーできるように、同時アクセスが必要です。SnapMirrorアクティブ同期の対称アクティブ / アクティブは、双方向レプリケーションによってローカルでIOを処理することで、クラスタアプリケーションの要件を満たします。

災害シナリオ

地理的に分散したサイト間で、アプリケーション用の複数のボリュームを同期的にレプリケートします。プライマリで中断が発生した場合には、セカンダリ コピーに自動的にフェールオーバーできるため、Tier 1 アプリケーションのビジネス継続性が確保されます。

**Windows** フェイルオーバー

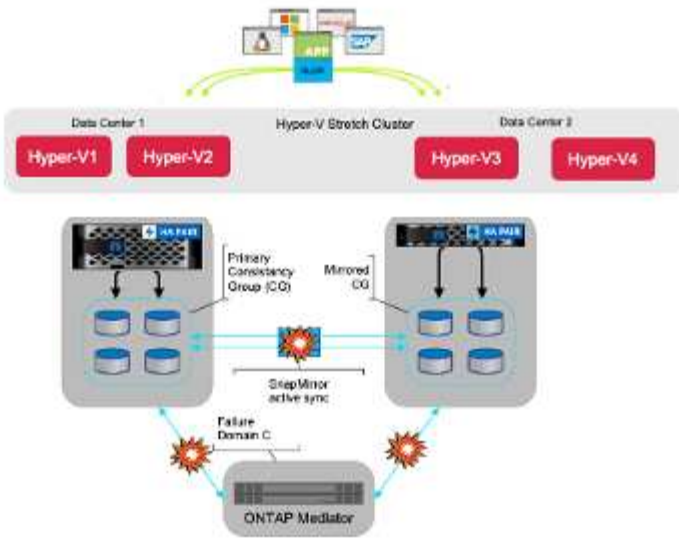
SnapMirrorアクティブ シンクは、使いやすいアプリケーション レベルの粒度と自動フェールオーバーによる柔軟性を提供し、仮想環境と物理環境の両方で、Oracle、Microsoft SQL Server などのビジネス クリティカルなアプリケーションの高いデータ可用性と高速なデータ レプリケーションを実現します。

## ソリューション アーキテクチャ

Microsoft ストレッチ クラスターには、各サイトに 2 つの Hyper-V ノードがあります。これら 2 つのノードはNetAppストレージを共有し、SnapMirrorアクティブ同期対称アクティブ/アクティブを使用して 2 つのサイト間でボリュームを複製します。整合性グループにより、データセットのすべてのボリュームが休止され、同じ時点でのSnapshotが作成されます。そのため、そのデータセットをサポートするボリューム間でデータ整合性のあるリストア ポイントが得られます。ONTAPメディエーターは、ピアリングされたONTAPクラスタとノードに関するヘルス情報を受信し、両者の間でオーケストレーションを行い、各ノード/クラスタが正常で実行中かどうかを判断します。

ソリューションコンポーネント:

- 2つのNetAppストレージシステムONTAP 9.15.1: 第1および第2の障害ドメイン
- ONTAPメディエーター用のRedhat 8.7 VM
- Windows 2022 上の 3 つの Hyper-V フェールオーバー クラスター:
  - アプリケーション用のサイト1、サイト2
  - 仲介者のためのサイト3
- Hyper-V 上の VM: Microsoft ドメイン コントローラ、MSSQL Always On フェールオーバー クラスタ インスタンス、ONTAP Mediator



## Microsoft ストレッチ フェールオーバー クラスターをインストールする

Windows Admin Center、PowerShell、または Server Manager コンソールを使用して、フェールオーバー クラスタリング機能とそれに関連する PowerShell コマンドレットをインストールできます。前提条件と手順の詳細については、「フェールオーバー クラスタの作成」を参照してください。

Windows ストレッチ クラスタをセットアップするための手順ガイドは次のとおりです。

1. 4台のサーバーすべて (hyperv1、hyperv2、hyperv3、hyperv4) にWindows 2022をインストールする
2. 4 台のサーバーすべてを同じ Active Directory ドメイン (hyperv.local) に参加させます。
3. 各サーバーに、Windows のフェールオーバー クラスタリング、Hyper-V、Hyper-V\_Powershell、および MPIO 機能をインストールします。

```
Install-WindowsFeature -Name "Failover-Clustering", "Hyper-V", "Hyper-V-Powershell", "MPIO" -IncludeManagementTools
```

4. MPIO を構成し、iSCSI デバイスのサポートを追加します。



5. サイト 1 とサイト 2 のONTAPストレージで、2 つの iSCSI LUN (SQLdata と SQLlog) を作成

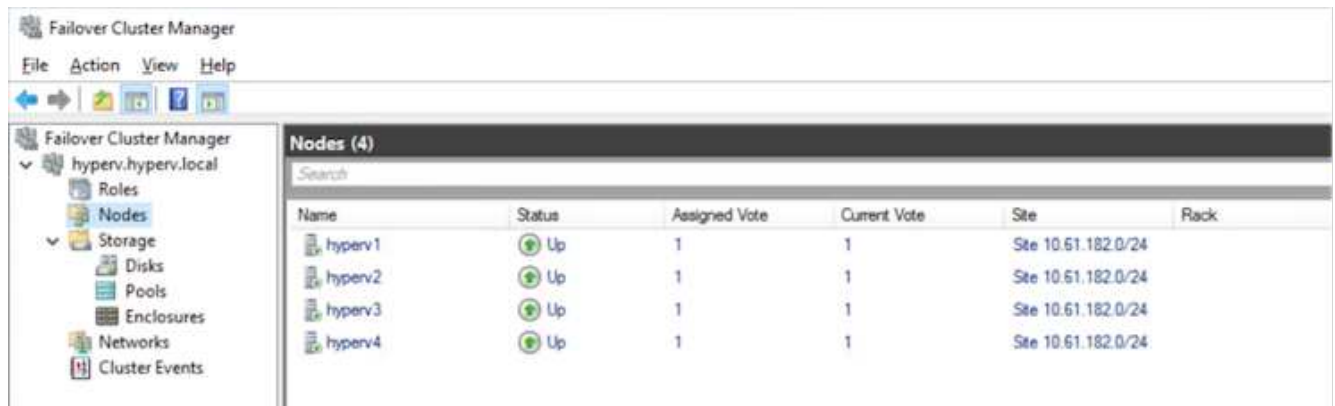
し、Windows サーバー IQN グループにマップします。Microsoft iSCSI ソフトウェア イニシエーターを使用して LUN を接続します。詳細については、"[Windows向けのiSCSIの設定](#)"。

6. エラーや警告がないか、クラスター検証レポートを実行します。

```
Test-Cluster -Node hyperv1, hyperv2, hyperv3, hyperv4
```

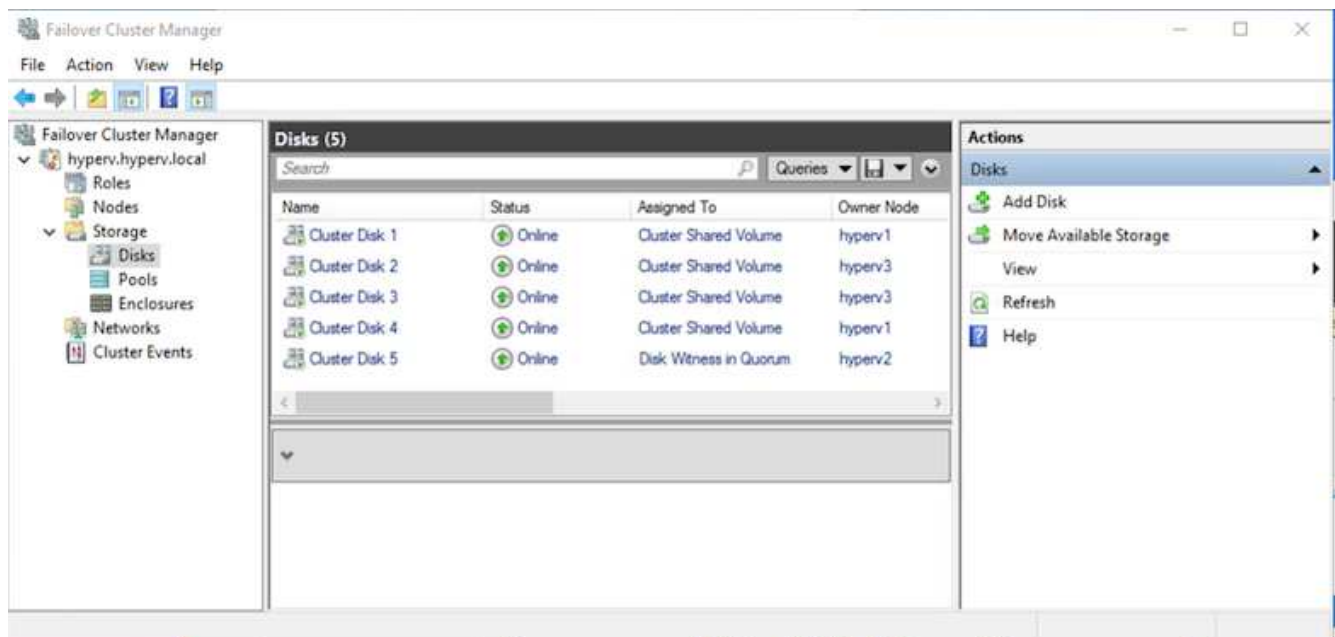
7. フェイルオーバークラスターを作成し、静的IPアドレスを割り当て、

```
New-Cluster -Name <clustername> -Node hyperv1, hyperv2, hyperv3, hyperv4, StaticAddress <IPaddress>
```



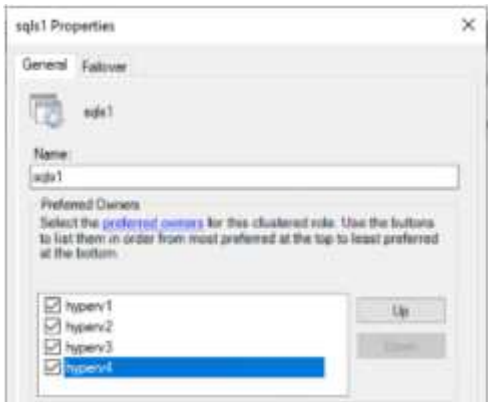
8. マップされた iSCSI ストレージをフェールオーバー クラスターに追加します。
9. クォーラムの監視を構成するには、クラスターを右クリック → [その他のアクション] → [クラスター クォーラム設定の構成] をクリックし、ディスク監視を選択します。

下の図は、クラスター化された共有 LUN が 4 つ (sqldata と sqllog の 2 つのサイトと、クォーラム内のディスク監視が 1 つ) 示されています。



## Always On フェールオーバー クラスタ インスタンス

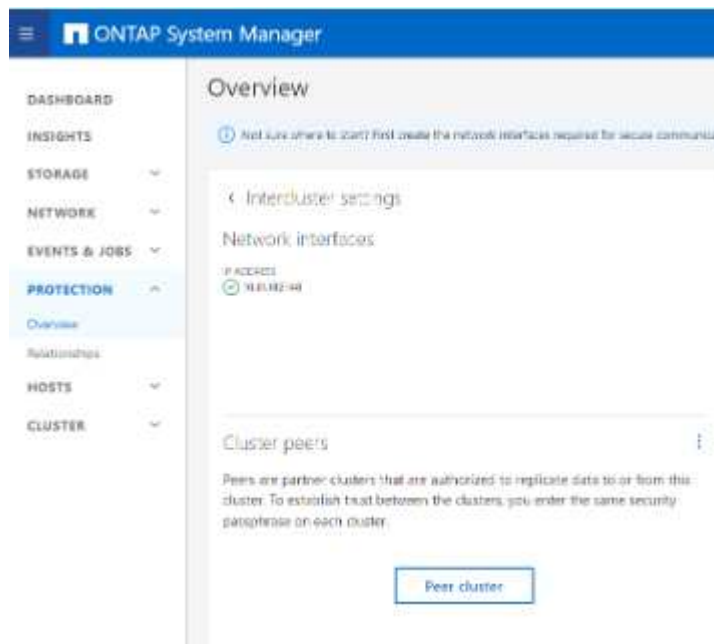
Always On フェールオーバー クラスタ インスタンス (FCI) は、WSFC 内の SAN 共有ディスク ストレージを持つノード全体にインストールされる SQL Server インスタンスです。フェールオーバー中、WSFC サービスはインスタンスのリソースの所有権を指定されたフェールオーバー ノードに転送します。その後、フェールオーバー ノードで SQL Server インスタンスが再起動され、データベースは通常どおりに回復されます。セットアップの詳細については、「SQL を使用した Windows フェールオーバー クラスタリング」を参照してください。各サイトに 2 つの Hyper-V SQL FCI VM を作成し、優先順位を設定します。サイト 1 の VM の優先所有者として hyperv1 と hyperv2 を使用し、サイト 2 の VM の優先所有者として hyperv3 と hyperv4 を使用します。



## クラスタ間ピアリングの作成

SnapMirrorを使用して Snapshot コピーを複製する前に、ソース クラスタと宛先クラスタの間にピア関係を作成する必要があります。

1. 両方のクラスタにクラスタ間ネットワーク インターフェイスを追加



2. cluster peer create コマンドを使用すると、ローカル クラスタとリモート クラスタ間にピア関係を作成できます。ピア関係が作成されたあとで、cluster peer create をリモート クラスタで実行して、ローカル クラスタに対してピア関係を認証できます。

## ONTAPでメディエーターを構成する

ONTAPメディエーターは、ピアリングされたONTAPクラスタとノードに関するヘルス情報を受信し、両者の間でオーケストレーションを行い、各ノード/クラスタが正常で実行中かどうかを判断します。SM-asを使用すると、データがソース ボリュームに書き込まれるとすぐにターゲットに複製されます。メディエーターは、3 番目の障害ドメインに展開する必要があります。前提条件

- ハードウェア仕様: 8GB RAM、2x2GHz CPU、1Gb ネットワーク (<125ms RTT)
- Red Hat 8.7 OSをインストールし、チェック"[ONTAP MediatorのバージョンとサポートされているLinuxのバージョン](#)"。
- Mediator Linuxホストを構成する: ネットワーク設定とファイアウォールポート31784および3260
- yum-utilsパッケージをインストールする
- "[UEFIセキュア ブートが有効になっている場合のセキュリティ キーの登録](#)"

### 手順

1. Mediatorインストールパッケージを以下からダウンロードします。"[ONTAPメディエーターのダウンロードページ](#)"。
2. ONTAP Mediator のコード署名を確認します。
3. インストーラを実行し、必要に応じてプロンプトに応答します。

```
./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

4. セキュア ブートが有効な場合、インストール後に追加の手順を実行してセキュリティ キーを登録する必要があります。
  - a. README ファイルの指示に従って、SCST カーネル モジュールに署名します。



```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing
```

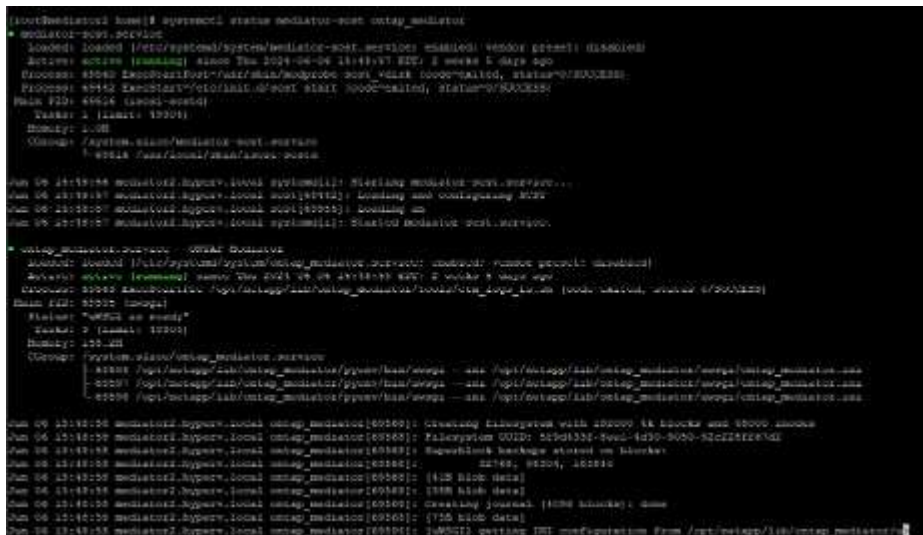
- b. 必要なキーを特定します。

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

## 5. インストールの確認

- a. プロセスを確認します。

```
systemctl status ontap_mediator mediator-scst
```



- b. ONTAP Mediatorサービスで使用されているポートを確認します。

```
[root@mediator2 server_config]# netstat -anlt | grep -E '3260|31784'
```

| Protocol | State | Recv-Q | Send-Q | Local Address       | Foreign Address     | State       |
|----------|-------|--------|--------|---------------------|---------------------|-------------|
| tcp      | 0     | 0      | 0      | 0.0.0.0:3260        | 0.0.0.0:*           | LISTEN      |
| tcp      | 0     | 0      | 0      | 0.0.0.0:31784       | 0.0.0.0:*           | LISTEN      |
| tcp      | 0     | 0      | 0      | 10.61.182.163:31784 | 10.61.182.148:26429 | ESTABLISHED |
| tcp      | 0     | 0      | 0      | 10.61.182.163:31784 | 10.61.182.148:24546 | FIN_WAIT2   |
| tcp6     | 0     | 0      | 0      | :::3260             | :::*                | LISTEN      |

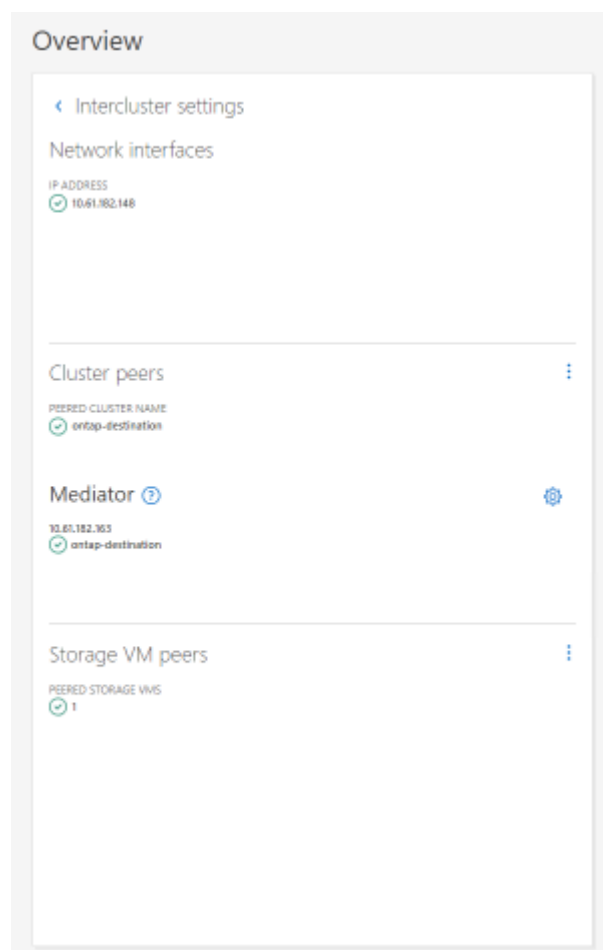
## 6. 自己署名証明書を使用したSnapMirrorアクティブ同期用のONTAP Mediatorの初期化

- a. ONTAP Mediator Linux VM/ホスト ソフトウェアのインストール場所 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` からONTAP Mediator CA 証明書を見つけてみます。
- b. ONTAP MediatorのCA証明書をONTAPクラスタに追加します。

```
security certificate install -type server-ca -vserver <vserver_name>
```

7. メディエーターを追加するには、システム マネージャーの保護 > 概要 > メディエーターに移動し、メディエーターの IP アドレス、ユーザー名 (API ユーザーのデフォルトは mediatoradmin)、パスワード、およびポート 31784 を入力します。

次の図は、クラスター間ネットワーク インターフェイス、クラスター ピア、メディエーター、および SVM ピアがすべて設定されていることを示しています。



## 対称アクティブ/アクティブ保護を構成する

整合性グループは、アプリケーション ワークロードの管理に便利です。ローカルとリモートの保護ポリシーを簡単に設定できるほか、一連のボリュームの特定の時点のクラッシュ整合性またはアプリケーション整合性 Snapshot コピーを同時に作成できます。詳細については、["一貫性グループの概要"](#)。このセットアップでは均一な構成を使用します。

### 均一な構成の手順

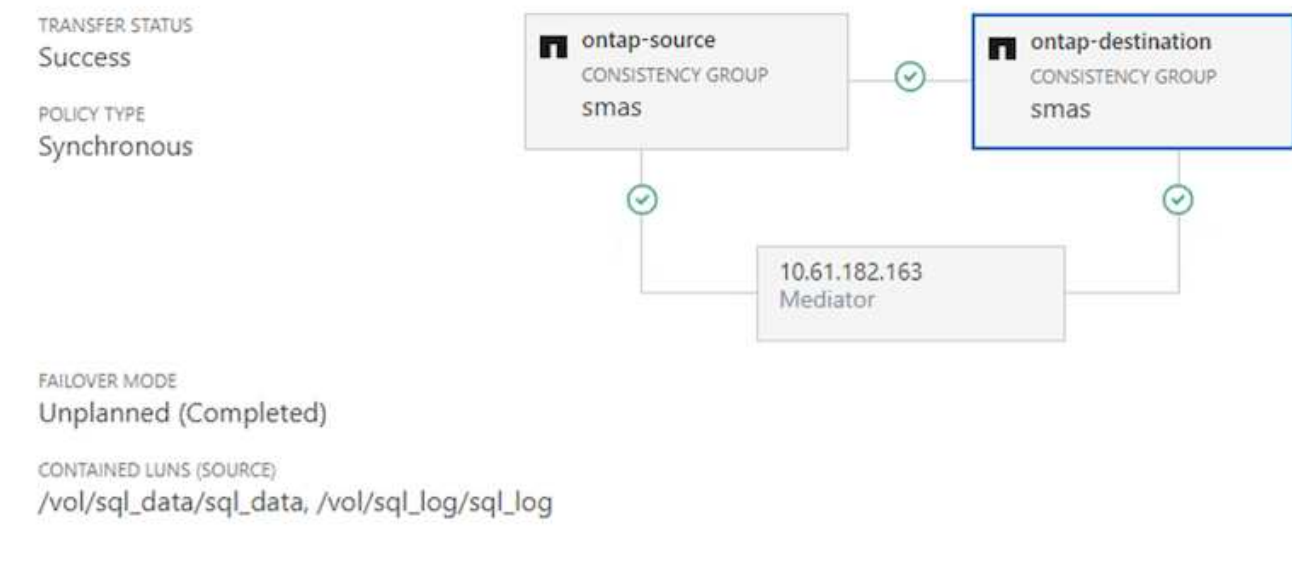
1. 整合性グループを作成する際は、igroupを作成するホスト イニシエータを指定します。
2. SnapMirrorを有効にするチェックボックスを選択し、AutomatedFailoverDuplex ポリシーを選択します。
3. 表示されるダイアログ ボックスで、[イニシエータ グループを複製] チェックボックスをオンにして igroup を複製します。「近接設定の編集」で、ホストの近接 SVM を設定します。

Proximity settings

| Initiator                                      | Initiator in proximity to |
|------------------------------------------------|---------------------------|
| Initiator group: hyperv<br>Mapped LUNs: 2      |                           |
| iqn.1991-05.com:microsoft:hyperv2.hyperv.local | Destination               |
| iqn.1991-05.com:microsoft:hyperv3.hyperv.local | Source                    |
| iqn.1991-05.com:microsoft:hyperv1.hyperv.local | Destination               |
| iqn.1991-05.com:microsoft:hyperv4.hyperv.local | Source                    |

#### 4. 保存を選択

保護関係はソースと宛先の間で確立されます。



### クラスタフェイルオーバー検証テストを実行する

計画されたフェイルオーバー テストを実行してクラスタ検証チェックを行うことをお勧めします。両方のサイトの SQL データベースまたはクラスター化されたソフトウェアでは、テスト中もプライマリ サイトまたはミラー サイトは引き続きアクセスする必要があります。

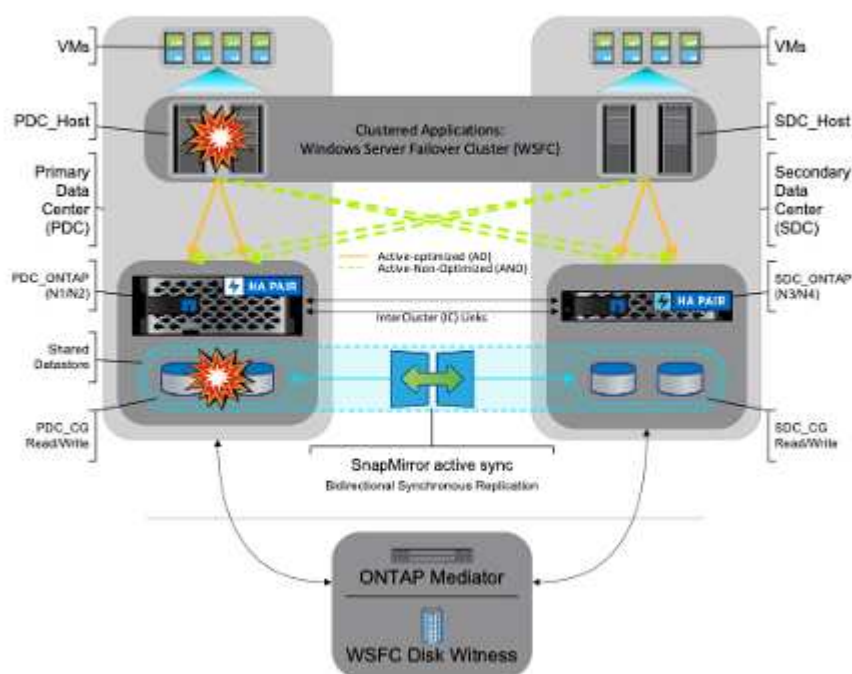
Hyper-V フェイルオーバー クラスターの要件は次のとおりです。

- SnapMirrorアクティブ同期関係が同期されている必要があります。
- 中断を伴わない操作が進行中の場合、計画されたフェイルオーバーを開始することはできません。中断を伴わない操作には、ボリュームの移動、アグリゲートの再配置、ストレージのフェイルオーバーが含まれます。
- ONTAP Mediatorが設定されて接続され、クォーラムを構成している必要があります。

- VM 移行のプロセスを最適化するために、各サイトには同じ CPU ファミリに属する CPU プロセッサを搭載した少なくとも 2 つの Hyper-V クラスター ノードが必要です。CPU は、ハードウェア支援による仮想化とハードウェアベースのデータ実行防止 (DEP) をサポートする CPU である必要があります。
- 回復力を確保するには、Hyper-V クラスター ノードは同じ Active Directory ドメイン メンバーである必要があります。
- 単一障害点を回避するために、Hyper-V クラスター ノードと NetApp ストレージ ノードは冗長ネットワークで接続する必要があります。
- すべてのクラスター ノードから iSCSI、ファイバー チャネル、または SMB 3.0 プロトコル経由でアクセスできる共有ストレージ。

## テストシナリオ

ホスト、ストレージ、またはネットワークでフェイルオーバーをトリガーする方法は多数あります。



## Hyper-V のノードまたはサイトに障害が発生した

- ノード障害 フェールオーバー クラスター ノードは、障害が発生したノードのワークロードを引き継ぐことができます。このプロセスはフェールオーバーと呼ばれます。アクション: Hyper-V ノードの電源をオフにします。期待される結果: クラスター内の他のノードがワークロードを引き継ぎます。VM は他のノードに移行されます。
- 1 つのサイト障害 サイト全体を障害状態にして、プライマリ サイトのミラー サイトへのフェールオーバーをトリガーすることもできます。アクション: 1 つのサイトの両方の Hyper-V ノードをオフにします。期待される結果: SnapMirrorアクティブ同期対称アクティブ/アクティブは双方向レプリケーションを使用して IO をローカルに提供し、RPO と RTO がゼロでワークロードに影響を与えないため、プライマリ サイトの VM はミラー サイトの Hyper-V クラスターに移行されます。

## 1つのサイトでのストレージ障害

- プライマリ サイトの SVM を停止します。アクション: iSCSI SVM を停止します。期待される結果: Hyper-

V プライマリ クラスターはすでにミラー サイトに接続されており、SnapMirrorアクティブ同期対称アクティブ/アクティブにより、RPO と RTO がゼロでワークロードに影響はありません。

#### 成功基準

テスト中は、次の点に注意してください。

- クラスターの動作を観察し、サービスが残りのノードに転送されていることを確認します。
- エラーやサービスの中断がないか確認してください。
- クラスターがストレージ障害を処理して動作を継続できることを確認します。
- データベース データに引き続きアクセスでき、サービスが継続して動作していることを確認します。
- データベースのデータの整合性が維持されていることを確認します。
- 特定のアプリケーションがユーザーに影響を与えずに別のノードにフェールオーバーできることを検証します。
- フェイルオーバー中およびフェイルオーバー後にクラスターが負荷を分散し、パフォーマンスを維持できることを確認します。

## まとめ

SnapMirrorアクティブ同期は、MSSQL や Oracle などのマルチサイト アプリケーション データを両方のサイトでアクティブにアクセスし、同期するのに役立ちます。障害が発生した場合、アプリケーションはデータの損失やアクセスの損失なく、残りのアクティブ サイトに直ちにリダイレクトされます。

## 著作権に関する情報

Copyright © 2025 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。