# データストアと仮想マシンを保護
## ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

# 目次

# データストアと仮想マシンを保護

## ONTAP toolsでホストクラスタを保護する

ONTAP tools for VMware vSphereは、ホストクラスタの保護を管理します。選択したSVMに属し、クラスタの1つ以上のホストにマウントされているすべてのデータストアが、ホストクラスタで保護されます。

作業を開始する前に

ホスト クラスターを保護する前に、次の要件を満たしていることを確認してください。

- ホスト クラスタには、単一の SVM のデータストアのみが含まれます。
- ホスト クラスター上のデータストアは、クラスター外部のホストにはマウントされません。
- ホスト クラスタにマウントされるデータストアは、iSCSI または FC プロトコルを使用した VMFS データストアです。 NVMe/FC および NVMe/TCP プロトコルでは、 vVols、NFS、または VMFS データストアは使用できません。
- ホストにマウントされたFlexVol/LUN ボリュームに基づくデータストアは、どの整合性グループにも属しません。
- ホストにマウントされたFlexVol/LUN ボリュームに基づくデータストアは、 SnapMirror関係の一部ではありません。
- ホスト クラスターには少なくとも 1 つのデータストアが含まれています。

手順

1. vSphere Clientにログインします。
2. ホスト クラスターを右クリックし、* NetApp ONTAPツール* > クラスターの保護 を選択します。
3. 保護クラスタウィンドウでは、データストアの種類とソース ストレージ仮想マシン (VM) の詳細がシステムによって自動的に入力されます。保護されたデータストアを表示するには、データストア リンクを選択します。
4. [関係の追加]*を選択します。
5. ウィンドウで、[ターゲットStorage VM]と[ポリシー]*タイプを選択します。

   ポリシータイプはAsynchronousまたはAutomatedFailOverDuplexのいずれかです。

   SnapMirror関係をAutomatedFailOverDuplexタイプのポリシーとして追加する場合は、ONTAP tools for VMware vSphereが導入されているvCenterに、ストレージバックエンドとしてターゲットStorage VMを追加する必要があります。

   AutomatedFailOverDuplex ポリシー タイプには、均一なホスト構成と非均一なホスト構成があります。 *均一ホスト構成*トグル ボタンを選択すると、ホスト イニシエーター グループ構成がターゲット サイトに暗黙的に複製されます。詳細については、 "主要な概念と用語" 。
6. 不均一なホスト構成を選択した場合は、そのクラスタ内の各ホストのホストアクセス（ソース/ターゲット）を選択します。
7. 「 * 追加」を選択します。

8. ホスト クラスター保護の変更 操作を使用して、ホスト クラスター保護を編集できます。省略記号メニュー オプションを使用して、関係を編集または削除できます。
9. [保護]*ボタンを選択します。

   システムはジョブ ID の詳細を含む vCenter タスクを作成し、最近のタスク パネルにその進行状況を表示します。これは非同期タスクです。ユーザー インターフェイスにはリクエストの送信ステータスのみが表示され、タスクが完了するまで待機しません。

10. 保護されたホスト クラスターを表示するには、* NetApp ONTAPツール* > 保護 > ホスト クラスター リレーションシップ に移動します。整合性グループを選択すると、その容量、関連付けられているデータストア、および子整合性グループが表示されます。

作成後 1 時間以内に保護を解除する必要がある場合は、まずストレージの検出を実行してください。

関連情報

"VMware vSphere メトロ ストレージ クラスタ (vMSC)"

# SRAによる保護を使用して保護する

## データストアを保護するために **ONTAP tools** で **SRA** を設定する

## ONTAP tools for VMware vSphereには、SRA機能を有効にしてディザスタリカバリを設定するためのオプションがあります。

作業を開始する前に

- vCenter Serverインスタンスのセットアップと ESXiホストの設定が完了している必要があります。
- ONTAP Tools for VMware vSphereを導入しておく必要があります。
- `.tar.gz`からSRAアダプタファイルをダウンロードしておく必要があります "NetApp Support Site"。
- SRA ワークフローを実行する前に、ソースと宛先の両方のONTAPクラスタで同じカスタムSnapMirrorスケジュールを設定する必要があります。
- "ONTAP Tools for VMware vSphereサービスを有効にする" SRA 機能を有効にします。

手順

1. URL：を使用してVMware Live Site Recoveryアプライアンスの管理インターフェイスにログインし `https://:<srm_ip>:5480`、VMware Live Site Recoveryアプライアンスの管理インターフェイスで[Storage Replication Adapters]に移動します。
2. [New Adapter]*を選択します。
3. SRAプラグインの_.tar.gz_installerをVMware Live Site Recoveryにアップロードします。
4. アダプタを再スキャンして、[VMware Live Site Recovery][Storage Replication Adapters]ページで詳細が更新されたことを確認します。

フェイルオーバー後、データストアに対して拡張、マウント、削除などのアクションが使用できなくなる可能性があります。データストアの検出を実行して更新し、適切なコンテキスト メニュー アクションを表示します。

再保護操作を実行するたびに、両方のサイトでストレージ検出を実行する必要があります。

SRA 保護を備えた新しいセットアップでは、常にテストフェイルオーバーを実行します。テストフェイルオーバーをスキップすると、再保護操作が失敗する可能性があります。

ファンアウト構成では、自動フェイルオーバーデュプレックスおよび非同期SnapMirrorの SnapMirrorソースがサイト B に変更されるSnapMirror Active Sync フェイルオーバー後に、サイト B と C の間でテストフェイルオーバーを実行します。この手順をスキップすると、再保護操作が失敗する可能性があります。

関連情報

"VMware Site Recovery Manager を使用して NFS データストアの災害復旧を構成する"

## SAN および NAS 環境向けの ONTAP tools で SRA を構成する

VMware Live Site Recovery用Storage Replication Adapter（SRA）を実行する前に、ストレージシステムをセットアップする必要があります。

### SAN環境用のSRAの設定

作業を開始する前に

保護対象サイトとリカバリサイトには、次のプログラムがインストールされている必要があります。

- VMware Live Site Recovery: VMware サイトでは、VMware Live Site Recovery のインストール ドキュメントが提供されています。

  "VMware Live Site Recoveryについて"

- SRA: VMware Live Site Recovery にアダプタをインストールします。

手順

1. 保護対象サイトで、プライマリ ESXi ホストがプライマリストレージシステムの LUN に接続されていることを確認します。
2. LUNが含まれているigroupにが含まれていることを確認します `ostype` プライマリストレージシステムでオプションを_vmware_に設定します。
3. リカバリ サイトの ESXi ホストに、ストレージ仮想マシン (SVM) への適切な iSCSI およびファイバ チャネル接続があることを確認します。セカンダリ サイトの ESXi ホストはセカンダリ サイトのストレージにアクセスできる必要があり、プライマリ サイトの ESXi ホストはプライマリ サイトのストレージにアクセスできる必要があります。

   そのためには、ESXiホストのSVMでローカルLUNが接続されていることを確認するか、または `iscsi show initiators` SVMでコマンドを実行します。 ESXiホストでマッピングされたLUNへのLUNアクセスをチェックして、iSCSI接続を確認します。

### NAS環境向けのSRAの設定

作業を開始する前に

保護対象サイトとリカバリサイトには、次のプログラムがインストールされている必要があります。

- VMware Live Site Recovery: VMware Live Site Recovery のインストール ドキュメントは、VMware のサイトにあります - "VMware Live Site Recoveryについて"
- SRA: VMware Live Site Recovery と SRA サーバーにアダプタをインストールします。

手順

1. 保護対象サイトのデータストアに、 vCenter Server に登録された仮想マシンがあることを確認します。
2. 保護対象サイトの ESXi ホストに、 Storage Virtual Machine （ SVM ）の NFS エクスポートボリュームがマウントされていることを確認します。
3. アレイマネージャウィザードを使用してVMware Live Site Recoveryにアレイを追加する際は、*NFSアドレス*フィールドにNFSエクスポートが存在するIPアドレスやFQDNなどの有効なアドレスが指定されていることを確認してください。*NFSアドレス*フィールドにはNFSホスト名を使用しないでください。
4. を使用します `ping` リカバリサイトの各ESXiホストでコマンドを実行し、SVMのNFSエクスポートへの接続に使用されるIPアドレスにホストのVMkernelポートからアクセスできることを確認します。

## 大規模環境向けに **ONTAP tools** で **SRA** を構成する

### 大規模な環境で最適なパフォーマンスを実現するには、Storage Replication Adapter（SRA）の推奨設定に従ってストレージのタイムアウト間隔を設定する必要があります。

ストレージプロバイダの設定

大規模な環境では、VMware Live Site Recoveryで次のタイムアウト値を設定する必要があります。

| * 詳細設定 * | * タイムアウト値 * |
|---|---|
| `StorageProvider.resignatureTimeout` | 設定の値を 900 秒から 12000 秒に増やします。 |
| `storageProvider.hostRescanDelaySec` | 60ドルだ |
| `storageProvider.hostRescanRepeatCnt` | 20 |
| `storageProvider.hostRescanTimeoutSec` | 高い値を設定します（例：99999）。 |

また、を有効にする必要があります `StorageProvider.autoResignatureMode` オプション

ストレージプロバイダの設定の変更の詳細については、を参照してください "Change Storage Provider Settings"。

ストレージ設定

タイムアウトに達した場合は、 `storage.commandTimeout` および `storage.maxConcurrentCommandCnt` 値を大きくします。

このタイムアウト間隔は最大値です。最大タイムアウトに達するまで待つ必要はありません。ほとんどのコマンドは、設定された最大タイムアウト間隔以内に終了します。

SANプロバイダ設定の変更については、を参照してください "Change Storage Settings"。

## ONTAP tools を使用して VMware Live Site Recovery アプライアンスで SRA を構成する

VMware Live Site Recovery アプライアンスを展開した後、ストレージ レプリケーション アダプタ (SRA) を構成して、災害復旧管理を有効にします。

VMware Live Site Recovery アプライアンスで SRA を構成すると、ONTAP tools for VMware vSphereがアプライアンス内に保存され、VMware Live Site Recovery と SRA 間の通信が可能になります。

作業を開始する前に

- _.tar.gz_ファイルを "NetApp Support Site"。
- ONTAPツール マネージャーで SRA サービスを有効にします。詳細については、 "サービスを有効にする" セクション。
- VMware vSphere アプライアンスの ONTATP ツールに vCenter Server を追加します。詳細については、"vCenter Server を追加する"セクション。
- ONTAP tools for VMware vSphereにストレージ バックエンドを追加します。詳細については、 "ストレージバックエンドを追加する"セクション。

> ONTAPツールから vCenter 証明書パッチを適用した場合は、(:5480) ポートを使用して VMware Live Site Recovery アプライアンスの vCenter 構成を更新します。手順については、"Site Recovery Manager アプライアンスを再構成する" 。

手順

1. VMware Live Site Recoveryアプライアンスの画面で、* Storage Replication Adapter > New Adapter *を選択します。
2. _.tar.gz_ファイルをVMware Live Site Recoveryにアップロードします。
3. PuTTY などの SSH クライアントを介して管理者アカウントを使用して VMware Live Site Recovery アプライアンスにログインします。
4. 次のコマンドを使用してrootユーザに切り替えます。 `su root`
5. コマンドを実行する `cd /var/log/vmware/srm`ログディレクトリに移動します。
6. ログの場所で、SRA で使用される Docker ID を取得するコマンドを入力します。 `docker ps -l`
7. コンテナIDにログインするには、次のコマンドを入力します。 `docker exec -it -u srm <container id> sh`
8. 次のコマンドを使用して、 ONTAP tools for VMware vSphere IP アドレスとパスワードで VMware Live Site Recovery を構成します。 `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - パスワードを一重引用符で囲んで指定すると、Perl スクリプトは特殊文字を区切り文字としてではなく、パスワードの一部として扱います。
   - アプリケーション（VASA Provider/SRA）のユーザー名とパスワードは、これらのサービスを初めて有効にする際に、 ONTAP Tools Manager で設定できます。これらの資格情報を使用して、SRA を VMware Live Site Recovery に登録します。

- vCenter GUID を見つけるには、vCenter インスタンスを追加した後、 ONTAPツール マネージャの vCenter Server ページに移動します。参照"vCenter Server を追加する"セクション。

9. アダプタを再スキャンして、更新された詳細が VMware Live Site Recovery のストレージ レプリケーション アダプタ ページに表示されることを確認します。

結果 ストレージ資格情報が保存されたことを示す確認メッセージが表示されます。これで、指定された IP アドレス、ポート、および資格情報を使用して SRA サーバーと通信できるようになりました。

## ONTAP toolsでSRA認証情報を更新する

### VMware Live Site RecoveryがSRAと通信するために、クレデンシャルを変更した場合は、VMware Live Site RecoveryサーバのSRAクレデンシャルを更新する必要があります。

作業を開始する前に

トピックに記載されている手順を実行しておく必要があります "VMware Live Site RecoveryアプライアンスでのSRAの設定"。

手順

1. 次のコマンドを実行して、VMware Live Site Recoveryマシンフォルダのキャッシュされ たONTAP toolsユーザ名パスワードを削除します。
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Perlコマンドを実行して、SRAに新しいクレデンシャルを設定します。
   a. `cd ..`
   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` パスワードの値は一重引用符で囲む必要があります。

      ストレージクレデンシャルが保存されたことを示す成功メッセージが表示されます。SRA は、指定された IP アドレス、ポート、およびクレデンシャルを使用して SRA サーバと通信できます。

## ONTAP toolsで保護サイトとリカバリサイトを構成する

### 保護対象サイトで仮想マシンのグループを保護するには、保護グループを作成する必要があります。

新しいデータストアを追加する際は、既存のデータストアグループに含めるか、新しいデータストアを追加して保護用の新しいボリュームまたはコンシステンシグループを作成することができます。保護対象のコンシステンシグループまたはボリュームに新しいデータストアを追加したら、 SnapMirrorを更新し、保護対象サイトとリカバリサイトの両方でストレージ検出を実行します。新しいデータストアを確実に検出・保護するために、検出を手動で実行することも、スケジュールに従って実行することもできます。

保護対象サイトとリカバリサイトをペアリング

Storage Replication Adapter（SRA）でストレージシステムを検出できるようにするには、作成された保護対象サイトとリカバリサイトをvSphere Clientを使用してペアリングする必要があります。

ストレージ レプリケーション アダプタ (SRA) は、整合性グループ上の自動フェイルオーバー デュプレックス タイプの 1 つの同期関係と非同期関係SnapMirrorによるファンアウトをサポートします。ただし、整合性グループ上の 2 つの非同期SnapMirrorを使用したファンアウト、またはボリューム上のファンアウト SnapMirror はサポートされていません。Vault タイプのSnapMirror関係は、これらのファンアウト制限内では考慮されません。

作業を開始する前に

- 保護対象サイトとリカバリサイトにVMware Live Site Recoveryがインストールされている必要があります。
- 保護対象サイトとリカバリサイトにSRAをインストールしておく必要があります。

手順

1. vSphere Client のホームページで、**Site Recovery** アイコンをダブルクリックし、**Sites** を選択します。
2. **>**[アクション]**>**[サイトのペアリング]*を選択します。
3. [Site Recovery Managerサーバのペアリング]ダイアログボックスで、保護対象サイトのプラットフォームサービスコントローラのアドレスを入力し、*[次へ]*を選択します。
4. Select vCenter Server セクションで、次の手順を実行します。
   a. 保護対象サイトの vCenter Server が対応するペア候補として表示されていることを確認します。
   b. SSO管理クレデンシャルを入力し、*[終了]*を選択します。
5. プロンプトが表示されたら、*[はい]*を選択してセキュリティ証明書を受け入れます。

結果

オブジェクト ダイアログ ボックスには、保護されたサイトと回復サイトの両方が表示されます。

保護グループを設定します

作業を開始する前に

ソースとターゲットの両方のサイトで以下を設定する必要があります。

- 同じバージョンのVMware Live Site Recoveryがインストールされている
- 仮想マシン
- 保護対象サイトとリカバリサイトのペアリング
- ソースとデスティネーションのデータストアをそれぞれのサイトにマウントする必要があります

手順

1. vCenter Server にログインし、**Site Recovery** > **Protection Groups** を選択します。
2. ペインで[新規]*を選択します。
3. 保護グループの名前と説明、方向を指定し、* Next *を選択します。
4. *タイプ*フィールドで、*タイプフィールドオプション…*として、NFSおよびVMFSデータストアのデータ

ストアグループ（アレイベースレプリケーション）を選択します。フォールト ドメインは、実際には、レプリケーションが有効になっているSVMです。ピアリングのみが実装されており、問題のないSVMが表示されます。

5. Replication groups（レプリケーショングループ）タブで、有効なアレイペアまたは設定した仮想マシンがあるレプリケーショングループのいずれかを選択し、* Next（次へ）*を選択します。

   レプリケーショングループ上のすべての仮想マシンが保護グループに追加されます。

6. 既存のリカバリ プランを選択するか、[新しいリカバリ プランに追加] を選択して新しいリカバリ プランを作成することもできます。
7. [Ready to Complete]タブで、作成した保護グループの詳細を確認し、*[Finish]*を選択します。

## 保護対象サイトとリカバリサイトのリソースを設定

**ONTAP tools**でネットワーク マッピングを設定する

### 保護対象サイトの各リソースがリカバリサイトの適切なリソースにマッピングされるように、両方のサイトでVMネットワーク、ESXiホスト、フォルダなどのリソースマッピングを設定する必要があります。

次のリソース設定を完了する必要があります。

- ネットワークマッピング
- フォルダマッピング
- リソースマッピング
- プレースホルダデータストア

作業を開始する前に

保護対象サイトとリカバリサイトを接続しておく必要があります。

手順

1. vCenter Serverにログインし、* Site Recovery **>** Sites *を選択します。
2. 保護対象サイトを選択し、*[管理]*を選択します。
3. [管理]タブで*>[新規]*を選択して、新しいネットワークマッピングを作成します。
4. Create Network Mappingウィザードで、次の手順を実行します。
   a. [Automatically Prepare Mappings for Networks with Matching Names]*を選択し、[次へ]*を選択します。
   b. 保護対象サイトとリカバリサイトに必要なデータセンターオブジェクトを選択し、*[マッピングの追加]*を選択します。
   c. マッピングが作成されたら、*[次へ]*を選択します。
   d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*を選択します。

結果

[ ネットワークマッピング ] ページには、保護対象サイトのリソースとリカバリサイトのリソースが表示されます。環境内の他のネットワークについても、同じ手順を実行します。

**ONTAP tools**でフォルダマッピングを設定する

## 保護対象サイトとリカバリサイトの間の通信を有効にするには、それらのサイトのフォルダをマッピングする必要があります。

作業を開始する前に

保護対象サイトとリカバリサイトを接続しておく必要があります。

手順

1. vCenter Serverにログインし、* Site Recovery **>** Sites *を選択します。
2. 保護対象サイトを選択し、*[管理]*を選択します。
3. [管理]タブで*>[フォルダ]*アイコンを選択して、新しいフォルダマッピングを作成します。
4. Create Folder Mapping ウィザードで、次の手順を実行します。
   a. [Automatically Prepare Mappings for Folders with Matching Names]*を選択し、[*Next]*を選択します。
   b. 保護対象サイトとリカバリサイトに必要なデータセンターオブジェクトを選択し、*[マッピングの追加]*を選択します。
   c. マッピングが作成されたら、*[次へ]*を選択します。
   d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*を選択します。

結果

[ フォルダマッピング ] ページには、保護対象サイトリソースとリカバリサイトリソースが表示されます。環境内の他のネットワークについても、同じ手順を実行します。

**ONTAP tools**でリソースマッピングを設定する

## 仮想マシンがどちらか一方のホストグループにフェイルオーバーするように構成されるように、保護対象サイトとリカバリサイトのリソースをマッピングする必要があります。

作業を開始する前に

保護対象サイトとリカバリサイトを接続しておく必要があります。

VMware Live Site Recoveryでは、リソースはリソースプール、ESXiホスト、vSphereクラスタのいずれかになります。

手順

1. vCenter Serverにログインし、* Site Recovery **>** Sites *を選択します。
2. 保護対象サイトを選択し、*[管理]*を選択します。
3. [管理]タブで*>[新規]*を選択して、新しいリソースマッピングを作成します。
4. Create Resource Mapping ウィザードで、次の手順を実行します。
   a. [Automatically Prepare Mappings for Resource with Matching Names]*を選択し、[次へ]*を選択します。
   b. 保護対象サイトとリカバリサイトに必要なデータセンターオブジェクトを選択し、*[マッピングの追

加]*を選択します。

c. マッピングが作成されたら、*[次へ]*を選択します。

d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*を選択します。

結果

リソースマッピングページには、保護対象サイトリソースとリカバリサイトリソースが表示されます。環境内の他のネットワークについても、同じ手順を実行します。

### **ONTAP tools**でプレースホルダデータストアを設定する

保護された仮想マシン (VM) 用にリカバリ サイトの vCenter インベントリ内のスペースを予約するようにプレースホルダー データストアを構成します。プレースホルダ VM は小さく、通常は数百キロバイトしか使用しないため、プレースホルダ データストアに必要な容量は最小限です。

作業を開始する前に

- 保護されたサイトとリカバリ サイトが接続されていることを確認します。
- リソース マッピングが構成されていることを確認します。

手順

1. vCenter Serverにログインし、* Site Recovery **>** Sites *を選択します。
2. 保護対象サイトを選択し、*[管理]*を選択します。
3. [管理]タブで*>[新規]*を選択して、新しいプレースホルダデータストアを作成します。
4. 適切なデータストアを選択し、* OK *を選択します。

> プレースホルダ データストアはローカル ストレージまたはリモート ストレージ上に存在できますが、レプリケーションは必要ありません。

5. 手順3~5を繰り返して、リカバリサイト用のプレースホルダデータストアを設定します。

### **ONTAP tools**のアレイマネージャを使用して**SRA**を設定する

VMware Live Site RecoveryのArray Managerウィザードを使用してStorage Replication Adapter（SRA）を設定し、VMware Live Site RecoveryとStorage Virtual Machine（SVM）の間のやり取りを有効にすることができます。

作業を開始する前に

- VMware Live Site Recoveryで保護対象サイトとリカバリサイトをペアリングしておく必要があります。
- アレイマネージャを設定する前に、オンボードストレージを設定しておく必要があります。
- 保護対象サイトとリカバリサイト間のSnapMirror関係を設定し、レプリケートしておく必要があります。
- マルチテナンシーを有効にするには、SVM管理LIFを有効にしておく必要があります。

SRA では、クラスタレベルの管理と SVM レベルの管理がサポートされます。クラスタレベルでストレージを追加すると、クラスタ内のすべてのSVMを検出して処理を実行できます。SVM レベルでストレージを追加す

る場合は、特定の SVM だけを管理できます。

手順

1. VMware Live Site Recoveryで、* Array Managers **>** Add Array Manager *を選択します。
2. 次の情報を入力して、VMware Live Site Recoveryでアレイについて説明します。

   a. [**Display Name**] フィールドに、アレイマネージャを識別する名前を入力します。

   b. 「 * SRA Type * 」フィールドで、「 * ONTAP 向け NetApp Storage Replication Adapter 」を選択します。

   c. クラスタまたは SVM への接続情報を入力します。

      - クラスターに接続する場合は、クラスター管理 LIF を入力する必要があります。
      - SVM に直接接続する場合は、SVM 管理 LIF の IP アドレスを入力する必要があります。

      アレイマネージャを設定するときは、ONTAP tools for VMware vSphereでストレージシステムのオンボードに使用したのと同じ接続（IPアドレス）をストレージシステムに使用する必要があります。たとえば、アレイマネージャの設定範囲がSVMである場合は、ONTAP tools for VMware vSphereのストレージをSVMレベルで追加する必要があります。

   d. クラスターに接続する場合は、**SVM** 名 フィールドに SVM 名を指定するか、クラスター内のすべての SVM を管理するには空白のままにします。

   e. 検出するボリュームを * Volume include list * フィールドに入力します。

      保護対象サイトではソースボリュームを、リカバリサイトではレプリケートされたデスティネーションボリュームを入力できます。

      たとえば、ボリュームdst_vol1とSnapMirror関係にあるボリュームsrc_vol1を検出する場合は、保護対象サイトのフィールドでsrc_vol1を指定し、リカバリサイトのフィールドでdst_vol1を指定する必要があります。

   f. * （オプション） * Volume exclude list * フィールドに、検出対象から除外するボリュームを入力します。

      保護対象サイトではソースボリュームを、リカバリサイトではレプリケートされたデスティネーションボリュームを入力できます。

   たとえば、volume_dst_vol1_とSnapMirror関係にあるvolume_src_vol1_を除外する場合は、保護対象サイトのフィールドで_src_vol1_を指定し、リカバリサイトのフィールドで_dst_vol1_を指定する必要があります。

3. 「 * 次へ * 」を選択します。
4. アレイが検出され、[Add Array Manager]ウィンドウの下部に表示されていることを確認し、*[Finish]*を選択します。

適切な SVM 管理 IP アドレスとクレデンシャルを使用して、リカバリサイトでも同じ手順を実行します。アレイマネージャの追加ウィザードのアレイペアを有効にする画面で、正しいアレイペアが選択されていること、および有効にする準備ができたことを確認する必要があります。

## ONTAP toolsで複製されたストレージシステムを検証する

Storage Replication Adapter（SRA）を設定したら、保護対象サイトとリカバリサイトが正常にペアリングされていることを確認する必要があります。レプリケートされたストレージシステムは、保護対象サイトとリカバリサイトの両方から検出可能である必要があります。

作業を開始する前に

- ストレージシステムを設定しておく必要があります。
- VMware Live Site Recoveryアレイマネージャを使用して、保護対象サイトとリカバリサイトをペアリングしておく必要があります。
- SRAのテストフェイルオーバー処理とフェイルオーバー処理を実行する前に、FlexCloneライセンスとSnapMirrorライセンスを有効にしておく必要があります。
- ソースサイトとデスティネーションサイトで同じSnapMirrorポリシーとスケジュールを使用する必要があります。

手順

1. vCenter Server にログインします。
2. サイト回復 > アレイ ベースのレプリケーション に移動します。
3. 必要なアレイペアを選択し、対応する詳細を確認します。

   保護対象サイトとリカバリサイトで、ステータスが「有効」になっているストレージシステムが検出されている必要があります。

## ONTAP toolsのファンアウト保護

ファンアウト保護のシナリオでは、コンシステンシ グループは、最初の宛先ONTAPクラスタ上の同期関係と、2 番目の宛先ONTAPクラスタ上の非同期関係によって二重に保護されます。 SnapMirrorアクティブ同期保護の作成、編集、および削除ワークフローにより、同期保護が維持されます。 VMware Live Site Recovery アプライアンスのフェイルオーバーと再保護ワークフローは、非同期保護を維持します。

SVM ユーザーではファンアウトはサポートされません。

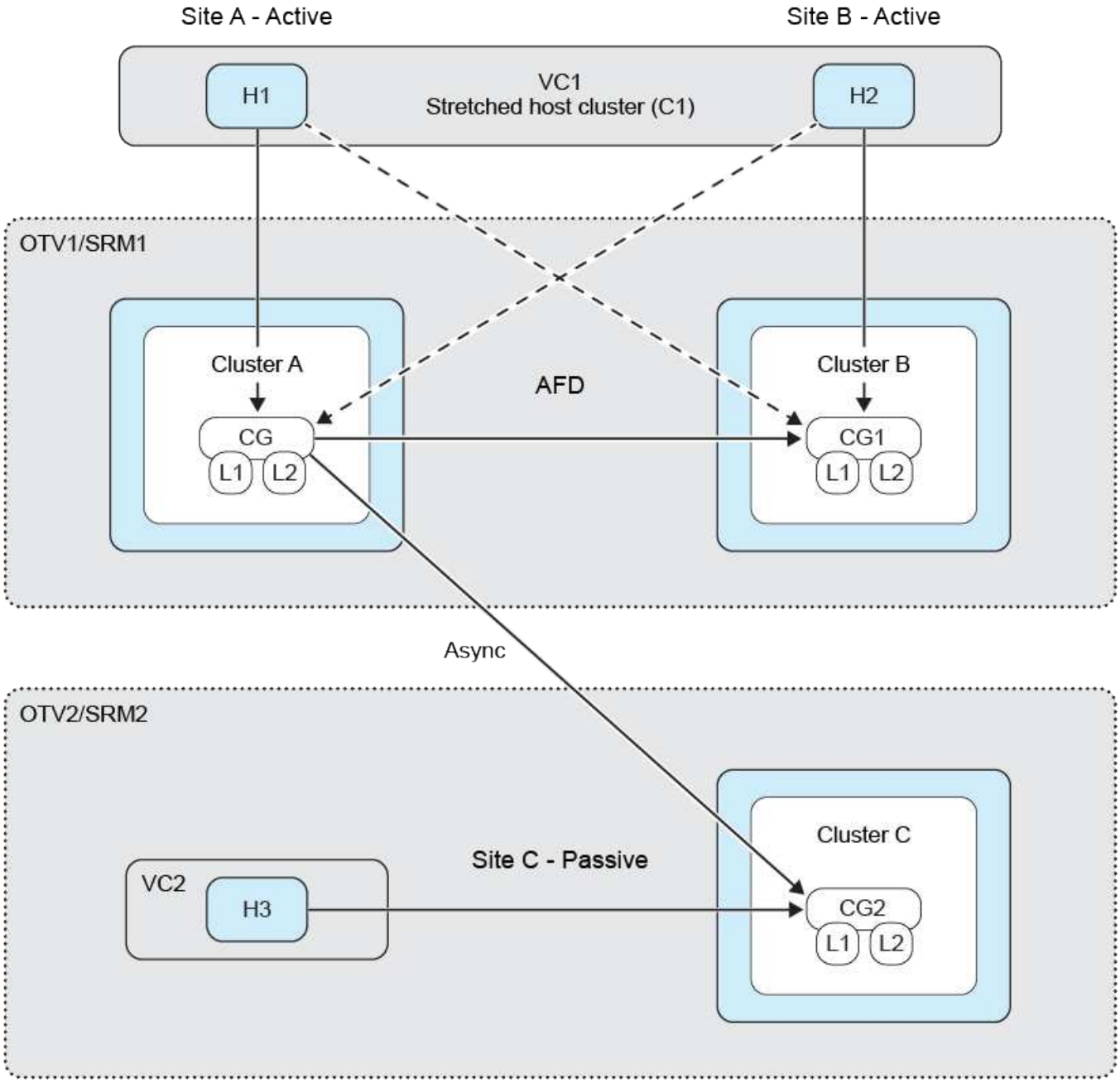
ファンアウト保護を設定するには、3 つのサイト クラスターと SVM をピアリングします。

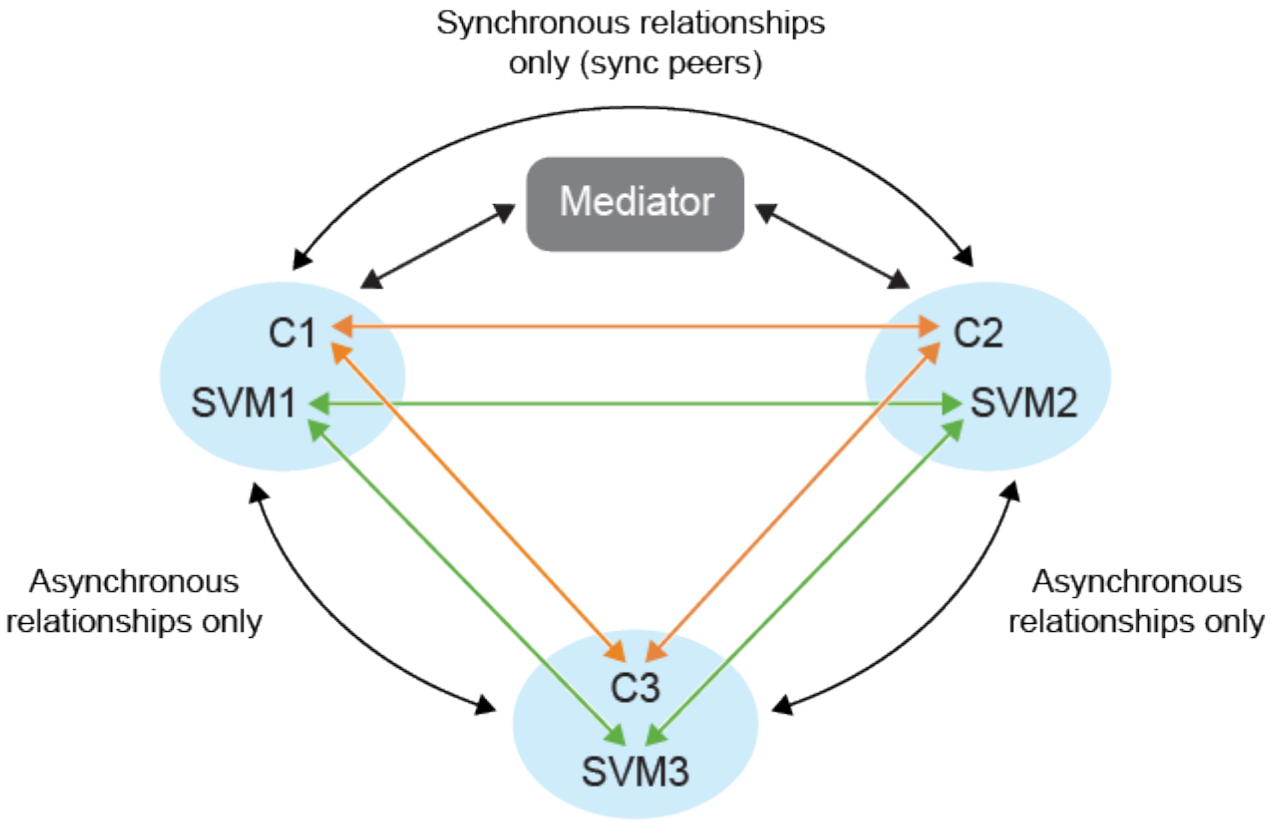
例

| 条件 | そうすると |
| --- | --- |

| | |
|---|---|
| • ソース整合性グループはクラスタc1とSVM svm1にあります<br>• 1つ目のデスティネーション整合性グループがクラスタc2およびSVM svm2上にあり、<br>• 2つ目のデスティネーション整合性グループはクラスタc3とSVM svm3にあります。 | • ソースONTAPクラスタのクラスタピアリングは、（c1、c2）および（c1、c3）になります。<br>• 最初のデスティネーションONTAPクラスタのクラスタピアリングは、（c2、c1）および（c2、c3）と<br>• 2番目のデスティネーションONTAPクラスタのクラスタピアリングは、（c3、c1）および（c3、c2）になります。<br>• ソースSVMのSVMピアリングは（svm1、svm2）と（svm1、svm3）になります。<br>• 1つ目のデスティネーションSVMでのSVMピアリングは、（svm2、svm1）と（svm2、svm3）と<br>• 2つ目のデスティネーションSVMのSVMピアリングは、（svm3、svm1）と（svm3、svm2）になります。 |

次の図は、ファンアウト保護構成を示しています。


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2




手順

1. 新しいプレースホルダー データストアを選択します。段階的保護のプレースホルダ データストアの選択基準は次のとおりです。
   - 保護しているホスト クラスターにプレースホルダー データストアを配置しないでください。
   - ホスト クラスタにプレースホルダ データストアを含める必要がある場合は、 SnapMirrorアクティブ同期保護を設定する前に、それを VMware Live Site Recovery アプライアンスに追加します。この設定により、プレースホルダー データストアを保護から除外することができます。

     詳細については、 "プレースホルダデータストアの選択"

2. 次のようにホストクラスタ保護にデータストアを追加します。"保護されているホストクラスタを変更" 。非同期ポリシー タイプと同期ポリシー タイプの両方を追加します。

## 著作権に関する情報



## 商標に関する情報