



データストアと仮想マシンの保護 ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

データストアと仮想マシンの保護	1
ONTAP toolsでホストクラスタを保護する	1
SRA保護を使用して保護する	2
データストアを保護するために ONTAP tools で SRA を設定する	2
SAN および NAS 環境向けの ONTAP tools で SRA を構成する	3
大規模環境向けに ONTAP tools で SRA を構成する	4
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	5
ONTAP toolsでSRA認証情報を更新する	6
ONTAP toolsで保護サイトとリカバリサイトを構成する	7
保護対象サイトとリカバリ サイトのリソースの設定	9
ONTAP toolsで複製されたストレージシステムを検証する	13
ONTAP toolsのファンアウト保護	13

データストアと仮想マシンの保護

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、クラスタ内の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は、ホスト クラスタで保護されます。

開始する前に

ホストクラスタを保護する前に、以下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からのデータストアのみが含まれています。
- ホストクラスタ上のデータストアは、クラスタ外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プロトコルを使用するVMFSデータストアです。vVols、NFS、またはNVMe/FCおよびNVMe/TCPプロトコルを使用したVMFSデータストアは使用できません。
- ホスト上にマウントされたFlexVol/LUN ボリュームに基づくデータストアは、いずれ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 クライアントにログインします。
2. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. クラスタ保護ウィンドウでは、システムが自動的にデータストアの種類とソースストレージ仮想マシン (VM) の詳細を入力します。保護されているデータストアを表示するには、「データストア」リンクを選択してください。
4. 「関係を追加」を選択します。
5. 「**SnapMirror** 関係の追加」*ウィンドウで、「ターゲットストレージVM」と「ポリシー」*タイプを選択します。

ポリシータイプは非同期または AutomatedFailOverDuplex です。

SnapMirror関係をAutomatedFailOverDuplexタイプのポリシーとして追加する場合、ONTAP tools for VMware vSphereが導入されているのと同じvCenterに、ターゲットのstorage VMをストレージバックエンドとして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。*Uniform host configuration*トグルボタンを選択すると、ホストイニシエータ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](#)"を参照してください。

6. ホスト構成を統一しない場合は、そのクラスタ内の各ホストに対してホストアクセス（送信元/宛先）を選択してください。

7. *追加*を選択します。
8. **Modify host cluster protection** 操作を使用して、ホストクラスタ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捗状況を表示します。これは非同期タスクです。ユーザーインターフェースにはリクエストの送信状況のみが表示され、タスクの完了を待つことはありません。

10. 保護対象のホストクラスタを表示するには、* NetApp ONTAP tools* > 保護 > *ホストクラスタ関係*に移動します。整合性グループを選択すると、その容量、関連するデータストア、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ー \(vMSC\) "](#)

SRA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は、ディザスタリカバリを設定するためのSRA機能を有効にするオプションを提供します。

開始する前に

- vCenter Server インスタンスをセットアップし、ESXi ホストを設定しておく必要があります。
- ONTAP tools for VMware vSphere を導入しておく必要があります。
- SRA Adapter `tar.gz` ファイルを ["NetAppサポート サイト"](#) からダウンロードしておく必要があります。
- 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クラスターに同じカスタムSnapMirrorスケジュールが設定されている必要があります。
- ["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 : `https://<srm\_ip>:5480` を使用してVMware Live Site Recoveryアプライアンス管理インターフェイスにログインし、VMware Live Site Recoveryアプライアンス管理インターフェイスでStorage Replication Adaptersに移動します。
2. 「新しいアダプター」を選択します。
3. SRA プラグイン用の .tar.gz インストーラーを VMware Live Site Recovery にアップロードします。
4. 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で詳細が更新されていることを確認するために、アダプタを再スキャンしてください。



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、削除などの操作が利用できなくなる場合があります。データストアの検出を実行して、適切なコンテキストメニューアクションを更新および表示します。



各再保護操作の後には、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保護機能を備えた新しいシステムでは、必ずテストフェイルオーバーを実行してください。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。

ファンアウト構成において、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 フェイルオーバーの後、サイト B とサイト C の間でテストフェイルオーバーを実行してください。この手順を省略すると、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 用の 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環境向けにSRAを構成する



SRAワークフローの整合性グループは、UnifiedとASA r2ストレージシステムの両方で、SANプロトコル (iSCSIとファイバーチャネル) でのみサポートされています。

開始する前に

保護サイトと復旧サイトには、以下のプログラムをインストールしておく必要があります。

- VMware Live Site Recovery : VMware のサイトには、VMware Live Site Recovery のインストールドキュメントが掲載されています。

["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。

iSCSIプロトコル構成については、SRAワークフローを実行する前に以下の点に注意してください：

- 保護されたサイト：iSCSI ストレージアダプタとデータ LIF の詳細は、データストアをプロビジョニングする際に自動的に構成されます。手動設定は不要です。
- リカバリサイト：iSCSIストレージアダプタは、ディザスタリカバリのリソースマッピングに含まれる各ESXiホストで手動で設定する必要があります。各ホストでアダプタを個別に設定しないようにするには、SRAワークフローが設定されているSVMを使用して、リカバリサイトにiSCSIタイプのプレースホルダデータストアを作成します。これにより、iSCSIアダプタと必要なデータLIF IPアドレスがマッピングされたすべてのESXiホストに自動的に追加されます。詳細については、["ONTAP toolsでプレースホルダデータストアを設定する"](#)を参照してください。

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. プライマリ ストレージ システムで、LUN が `ostype` オプションを `_VMware_` に設定した igroup に属していることを確認してください。
3. 復旧サイトのESXiホストが、ストレージ仮想マシン (SVM) に対して適切なiSCSIおよびファイバーチャネル接続を確立していることを確認してください。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ます、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。

これは、ESXi ホストに SVM 上にローカル LUN が接続されていることを確認するか、SVM に対して `iscsi show initiators` コマンドを使用することで実行できます。ESXi ホストでマッピングされた LUN への LUN アクセスを確認し、iSCSI 接続を検証してください。

NAS環境向けにSRAを設定する



SRAワークフローでは、NFSの整合性グループはサポートされていません。NFSデータストアボリュームが整合性グループの下に配置され、保護されている場合、デバイスの検出操作は失敗します。SRAを使用してNFSデータストアを保護する場合、整合性グループを使用しないでください。

開始する前に

保護サイトと復旧サイトには、以下のプログラムをインストールしておく必要があります。

- VMware Live Site Recovery : VMware Live Site Recovery のインストール手順書は、VMware サイトで入手できます - ["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ホストが、Storage Virtual Machine (SVM) からのNFSエクスポートボリュームをマウントしていることを確認してください。
3. VMware Live Site Recoveryにアレイを追加するためにArray Managerウィザードを使用する場合、NFSエクスポートが存在する有効なIPアドレスが*NFSアドレス*フィールドに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ホスト名またはFQDNを使用しないでください。
4. 復旧サイトにある各ESXiホストで `ping` コマンドを使用して、ホストにSVMからNFSエクスポートを提供するために使用されるIPアドレスにアクセスできるVMkernelポートがあ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

大規模環境で最適なパフォーマンスを発揮させるには、ストレージレプリケーションアダプタ (SRA) の推奨設定に従って、ストレージ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

大規模環境向けのVMware Live Site Recoveryでは、以下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
<code>StorageProvider.resignatureTimeout</code>	値を900秒から12000秒に引き上げます。
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	高い値を設定します（例：99999）

また、`StorageProvider.autoResignatureMode` オプションも有効にしてください。

ストレージプロバイダーの設定変更に関する詳細については、["Change Storage Provider Settings"](#)を参照してください。

ストレージ設定

タイムアウトが発生した場合は、`storage.commandTimeout` および `storage.maxConcurrentCommandCnt` の値をより大きな値に増やしてください。



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ことはありません。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 プロバイダの設定を変更するには、["Change Storage Settings"](#)を参照してください。

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アプライアンスをデプロイした後、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を設定すると、ONTAP tools for VMware vSphereの認証情報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。

開始する前に

- .tar.gz ファイルを ["NetAppサポート サイト"](#) からダウンロードしてください。
- ONTAP tools Manager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"](#) セクションを参照してください。
- vCenter Server を ONTAP tools for VMware vSphere アプライアンスに追加します。詳細については、["vCenter サーバーの追加"](#) セクションを参照してください。
- 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"](#) セクションを参照してください。



ONTAP tools 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 構成を更新してください。手順については、["Site Recovery Managerアプライアンスを再構成する"](#)を参照してください。

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クライアントを使用して、管理者アカウントでVMware Live Site Recoveryアプライアンスにログインします。
4. 以下のコマンドを使用してrootユーザーに切り替えます：`su root`
5. コマンド ``cd /var/log/vmware/srm`` を実行して、ログディレクトリに移動します。
6. ログの保存場所で、SRAが使用する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てください：`docker exec -it -u srm <container id> sh`
8. 以下のコマンドを使用して、ONTAP tools for VMware vSphere の 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>`
 - Perlスクリプトが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うように、パスワードをシングルクォーテーションで囲ってください。
 - 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。これらの認証情報を使用して、SRA を VMware Live Site Recovery に登録してください。
 - vCenter の GUID を確認するには、vCenter インスタンスを追加した後、ONTAP tools Manager の vCenter Server ページに移動してください。["vCenter サーバーの追加"](#) セクションを参照してください。
9. アダプタを再スキャンして、更新された詳細情報がVMware Live Site Recovery Storage Replication Adaptersページに表示されていることを確認してください。

結果 ストレージ認証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、および認証情報を使用して、SRA で 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と通信するには、認証情報を変更した場合は、VMware Live Site Recoveryサーバー上でSRAの認証情報を更新する必要があります。

開始する前に

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

手順

1. VMware Live Site Recovery マシンからキャッシュされた ONTAP tools のクレデンシャルを削除するには、次のコマンドを実行します：
 - 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、新しい認証情報でSRAを設定します：

- a. `cd ..`
- b. ``perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`` パスワードの値はシングルクォーテーション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、および認証情報を使用してSRAサーバーと通信できます。

証明書の変更後に**VMware Live Site Recovery** アプライアンスで**vCenter**を再構成する

vCenter証明書が変更された場合（たとえば、vCenterのアップグレード後）、Site Recovery拡張機能でサムプリントの不一致エラーが発生する可能性があります。この問題を解決するには、次の手順を実行します。

手順

1. VMware Live Site Recovery アプライアンスで vCenter を再構成
 - a. ブラウザでVMware Live Site Recoveryアプライアンスの管理インターフェイスを開きます：
`https://<SRM_IP>:5480`
 - b. *** Summary *** タブを選択します。
 - c. vCenter Server 接続の **Reconfigure** を選択します。

これにより、vCenterから最新の証明書のサムプリントが取得され、受け入れられます。

2. サイトペアリングを再接続してください（エラーが続く場合）

再設定後も指紋不一致エラーが解消されない場合：

- a. vCenterユーザーインターフェイスにログインします。
- b. **Site Recovery** 拡張機能に移動します。
- c. **Site Pairing** セクションを探してください。
- d. ***再接続***を選択して、更新された証明書でサイトペアリングを再確立します。

ONTAP toolsで保護サイトとリカバリサイトを構成する

保護対象サイト上の仮想マシン群を保護するには、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場合、既存のデータストアグループに含めることも、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整合性グループを作成することもできます。保護された整合性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後、SnapMirror を更新し、保護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が確実に検出され、保護されるように、検出を手動で実行することも、スケジュールに基づいて実行することもできます。

保護対象サイトとリカバリ サイトのペアリング

vSphere Client を使用して作成した保護サイトとリカバリサイトをペアリングすることで、Storage Replication Adapter (SRA) がストレージシステムを検出できるようにする必要があります。



Storage Replication Adapter (SRA) は、Automated Failover Duplexタイプの同期関係が1つと、整合性グループ上の非同期SnapMirror関係が1つの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関係によるファンアウト、またはボリューム上のSnapMirror関係によるファンアウト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の対象外です。SRAでの整合性グループのサポートは、UnifiedおよびASA r2ストレージシステムのSANプロトコル (iSCSIおよびファイバーチャネル) に限定されています。NFSでは整合性グループはサポートされていません。NFSデータストアボリュームが整合性グループ下に配置されている場合、デバイス検出操作は失敗します。

開始する前に

- 保護対象サイトと復旧対象サイトの両方に、VMware Live Site Recoveryをインストールしておく必要があります。
- 保護サイトと復旧サイトの両方にSRAをインストールする必要があります。

手順

- 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。
- オブジェクト > アクション > サイトのペアリング を選択します。
- 「Pair Site Recovery Manager Servers」ダイアログボックスで、保護対象サイトのPlatform Services Controllerのアドレスを入力し、「Next」を選択します。
- [Select vCenter Server]セクションで、次の手順を実行します。
 - 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。
 - SSO管理者認証情報を入力し、*完了*を選択します。
- 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承認してください。

結果

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

保護グループの設定

開始する前に

ソース サイトとターゲット サイトの両方で以下が設定されていることを確認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ます
- 仮想マシン
- 保護対象サイトとリカバリ サイトがペアリングされている
- ソースとデスティネーションのデータストアがそれぞれのサイトにマウントされている

手順

- vCenter Server にログインし、「Site Recovery」>「Protection Groups」を選択します。

2. 「Protection Groups」 ペインで、「New」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、*次へ*を選択します。
4. *Type*フィールドで、NFSおよびVMFSデータストアの*Type field option...*としてデータストアグループ（アレイベースのレプリケーション）を選択します。障害領域は、レプリケーションが有効になっているSVMで構成されます。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」タブで、有効になっているアレイペア、または構成した仮想マシンを含むレプリケーショングループのいずれかを選択し、*Next*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. 既存の復旧プランを選択するか、新しい復旧プランに追加を選択して新しい復旧プランを作成できます。
7. 「完了の準備」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 サイトのリソースの設定

ONTAP toolsでネットワーク マッピングを設定する

保護サイトから復旧サイトの適切なリソースへ各リソースをマッピングできるように、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両方のサイトで構成する必要があります。

以下のリソース設定を完了してください。

- 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

開始する前に

保護サイトと復旧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、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいネットワークマッピングを作成するには、管理タブで*Network Mappings* > *New*を選択します。
4. ネットワークマッピング作成ウィザードで、以下の操作を行います。
 - a. 「名前が一致するネットワークのマッピングを自動的に準備する」を選択し、「次へ」を選択します。
 - b. 保護サイトと復旧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. マッピングが正常に作成されたら、*次へ*を選択してください。
 - d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

[Network Mappings]ページに、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

保護サイトと復旧サイト間で通信を可能にするには、それぞれのフォルダをマッピングする必要があります。

開始する前に

保護サイトと復旧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、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいフォルダマッピングを作成するには、「管理」タブで*フォルダマッピング*>*フォルダー*アイコンを選択します。
4. Create Folder Mappingウィザードで、次の手順を実行します。
 - a. 「名前が一致するフォルダーのマッピングを自動的に準備する」を選択し、「次へ」を選択します。
 - b. 保護サイトと復旧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. マッピングが正常に作成されたら、*次へ*を選択してください。
 - d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

[Folder Mappings]ページに、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。環境内の他のフォルダについても、同様の手順で操作できます。

ONTAP toolsでリソースマッピングを設定する

保護サイトとリカバリサイトのリソースをマッピングして、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設定する必要があります。

開始する前に

保護サイトと復旧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、またはvSphere クラスターにすることができます。

手順

1. vCenter Server にログインし、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいリソースマッピングを作成するには、管理タブで*リソースマッピング*>*新規*を選択します。
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 Resources with Matching Names*を選択し、*Next*を選択します。
- b. 保護サイトと復旧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. マッピングが正常に作成されたら、*次へ*を選択してください。
- d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

リソースマッピングページには、保護対象サイトのリソースと復旧対象サイトのリソースが表示されます。環境内の他のリソースについても、同様の手順で操作できます。

ONTAP toolsでブレースホルダーデータストアを設定する

ブレースホルダーデータストアを構成して、保護対象の仮想マシン（VM）の復旧サイトにおけるvCenterインベントリのスペースを予約します。ブレースホルダーVMは小さく、通常は数百キロバイトしか使用しないため、ブレースホルダーデータストアに必要な容量は最小限です。

開始する前に

- 保護サイトと復旧サイトが接続されていることを確認してください。
- リソースマッピングが正しく設定されていることを確認してください。

手順

1. vCenter Server にログインし、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいブレースホルダーデータストアを作成するには、管理タブで「ブレースホルダーデータストア」>「新規」を選択します。
4. 適切なデータストアを選択し、**OK** をクリックしてください。



ブレースホルダー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に配置できますが、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ブレースホルダー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 のアレイマネージャウィザードを使用してストレージレプリケーションアダプタ（SRA）を構成することで、VMware Live Site Recovery とストレージ仮想マシン（SVM）間の連携を有効にできます。

開始する前に

- VMware Live Site Recoveryで、保護対象サイトと復旧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、オンボーディング済みのストレージを設定しておく必要があります。
- 保護サイトとリカバリサイト間の SnapMirror 関係を設定および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を有効にする必要があります。

SRAは、クラスタレベルの管理とSVMレベルの管理をサポートします。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を検出して操作を実行できるようになります。SVMレベルでストレージを追加すると、その特定のSVMのみを管理できるようになります。

手順

1. VMware Live Site Recoveryで、「Array Managers」>「Add Array Manager」を選択します。
2. VMware Live Site Recovery でアレイを説明するために、以下の情報を入力してください。
 - a. **Display Name** フィールドに、アレイマネージャを識別するための名前を入力してください。
 - b. 「SRA タイプ」フィールドで、「NetApp Storage Replication Adapter for ONTAP」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。

- クラスタに接続する場合は、クラスタ管理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構成する際は、ONTAP tools for VMware vSphere でストレージシステムをオンボーディングする際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。例えば、アレイマネージャの構成がSVMスコープの場合、ONTAP tools for VMware vSphere 配下のストレージはSVMレベルで追加する必要があります。

- d. クラスタに接続する場合は、*SVM名*フィールドにSVM名を指定するか、クラスタ内のすべてのSVMを管理する場合は空白のままにしてください。
- e. 検出するボリュームを **Volume include list** フィールドに入力してください。

保護対象サイト側のソース ボリューム、およびリカバリ サイト側の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。

例えば、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、保護サイトフィールドに `src_vol1` を指定し、リカバリサイトフィールドに `dst_vol1` を指定する必要があります。

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

保護対象サイト側のソース ボリューム、およびリカバリ サイト側の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` を除外する場合は、保護サイトフィールドに `src_vol1` を指定し、リカバリサイトフィールドに `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、「アレイマネージャの追加」ウィンドウの下部に表示されていることを確認し、「完了」を選択します。

該当するSVMの管理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。Add Array Managerウィザードの[Enable Array Pairs]画面で、正しいアレイ ペアが選択されていて、有効化できる状態になっていることを確認します。

ONTAP toolsで複製されたストレージシステムを検証する

ストレージレプリケーションアダプタ（SRA）の設定後、保護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。複製されたストレージシステムは、保護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。

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操作およびフェイルオーバー操作を実行する前に、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。
- 送信元サイトと送信先サイトで同じSnapMirrorポリシーとスケジュールを設定する必要があります。
- カスタムスケジュールを設定したカスタムSnapMirrorポリシーを使用している場合は、保護サイトと復旧サイトの両方で同じスケジュールとポリシーを設定する必要があります。
- カスタムSnapMirrorポリシー（デフォルトまたはカスタムスケジュールのいずれか）を使用している場合は、新しいポリシーが認識されるように、ONTAP toolsからストレージ検出を実行する必要があります。これを行わないと、テストフェイルオーバーやフェイルオーバーを含むSRAワークフローが失敗します。次のポイントでストレージ検出を実行します：
 - 復旧サイトでカスタムポリシーを作成した後。
 - 保護対象サイトでポリシーを再作成する再保護処理の実行後。

手順

1. vCenter Serverにログインします。
2. 「Site Recovery」 > 「Array Based Replication」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てください。

ストレージシステムは、保護サイトとリカバリサイトで有効のステータスで検出される必要があります。

ONTAP toolsのファンアウト保護

ファンアウト保護シナリオでは、整合性グループは最初の宛先 ONTAP クラスターとの同期関係、および2番目の宛先 ONTAP クラスターとの非同期関係によって二重に保護されます。作成、編集、削除の SnapMirror アクティブ同期保護ワークフローは、同期保護を維持します。VMware Live Site Recovery アプライアンスのフェイルオーバーおよび再保護ワークフローは、非同期保護を維持します。



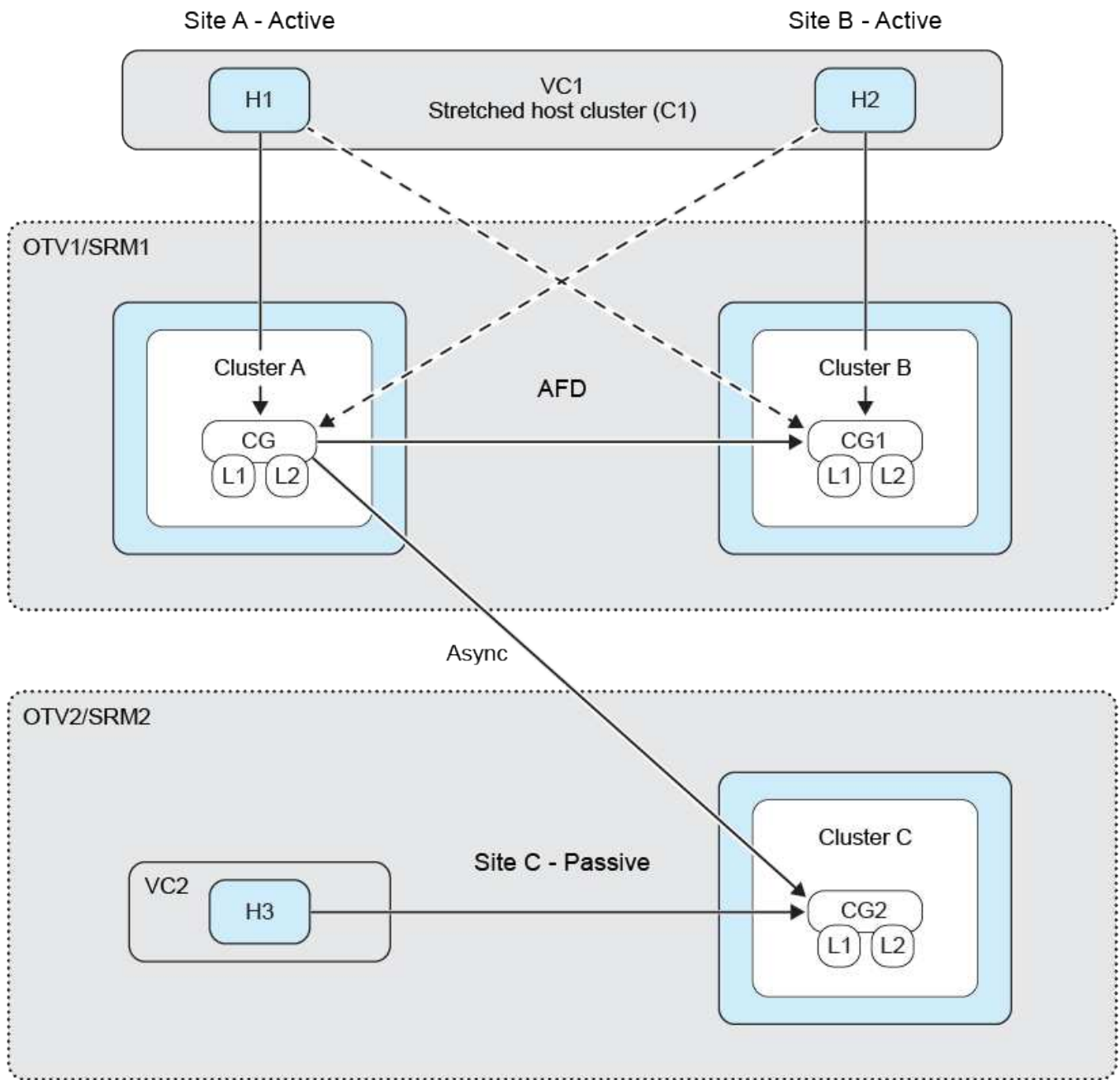
ファンアウトはSVMユーザーではサポートされていません。

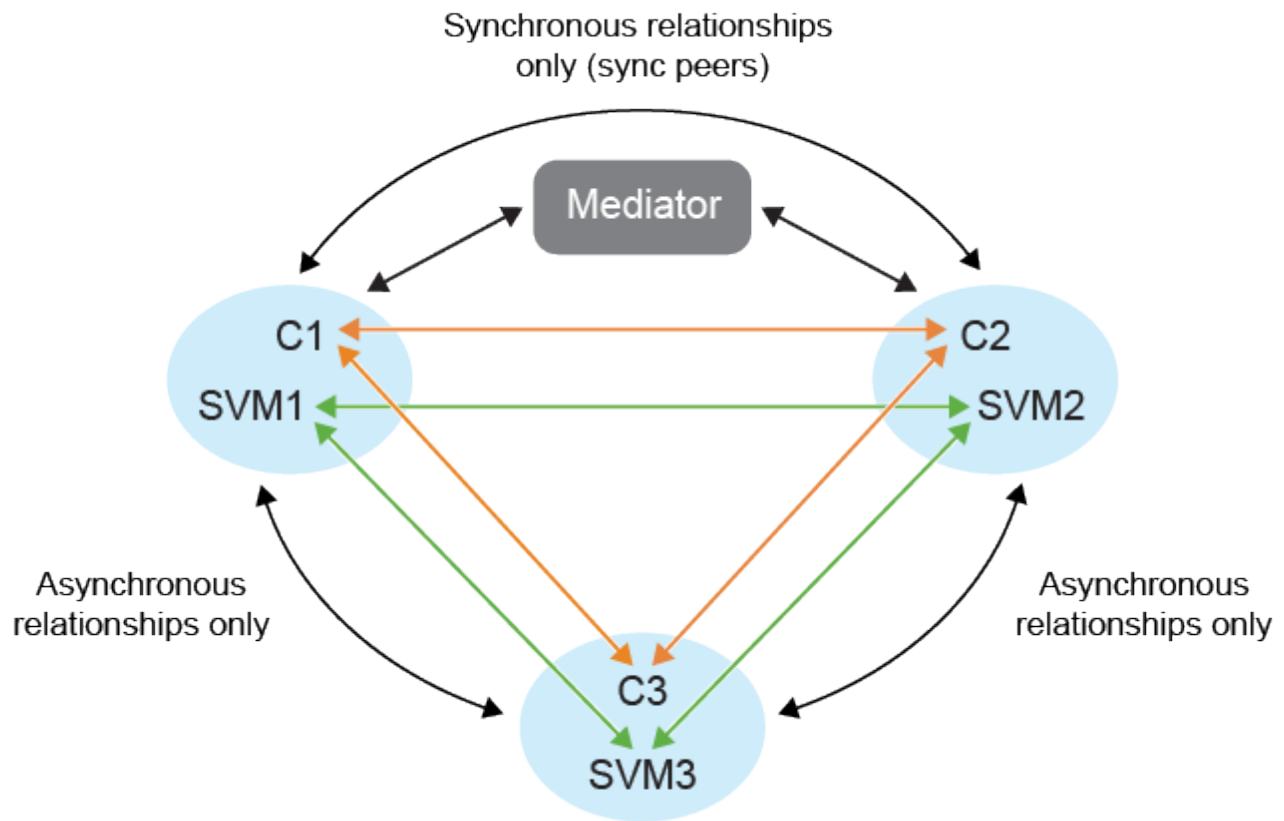
ファンアウト保護を設定するには、3つのサイトクラスターとSVMをピアリングします。

例：

実行している場合、	操作
• ソース整合性グループはクラスターc1とSVM svm1上にあります • 最初の宛先整合性グループはクラスター c2 と SVM svm2 上にあり、 • 2番目の宛先整合性グループはクラスター c3 と SVM svm3 上にあります	• ソース ONTAP クラスターのクラスタピアリングは（C1、C2）と（C1、C3）になります。 • 最初の宛先 ONTAP クラスターのクラスタピアリングは（C2、C1）と（C2、C3）となり、 • 2番目の宛先 ONTAP クラスターでのクラスタピアリングは（C3、C1）と（C3、C2）になります。 • ソースSVM上のSVMピアリングは（svm1, svm2）および（svm1, svm3）になります。 • 最初の宛先SVMでのSVMピアリングは（svm2, svm1）と（svm2, svm3）になり、 • 2番目の宛先SVMにおけるSVMピアリングは（svm3, svm1）および（svm3, svm2）となります。

次の図は、ファンアウト保護設定を示しています
：





手順

1. 新しいプレースホルダーデータストアを選択してください。段階的保護のためのプレースホルダーデータストア選択基準は以下のとおりです：
 - 保護対象のホストクラスタ内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、VMware Live Site Recovery アプライアンスに追加してください。この設定では、プレースホルダ データストアを保護対象から外すことができます。

詳細については、"[プレースホルダーデータストアを選択してください](#)"を参照してください。
2. "[保護されたホストクラスタを変更する](#)"に従って、データストアをホストクラスタ保護に追加します。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

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。