VMware Site Recovery ManagerとONTAP

Enterprise applications

NetApp
May 09, 2024

目次

VMware Site Recovery ManagerとONTAP

VMware Site Recovery ManagerとONTAP

ONTAPは、2002年に最新のデータセンターに導入されて以来、VMware vSphere環境向けストレージ解決策として業界をリードしてきました。また、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。

このドキュメントでは、業界をリードするVMwareのディザスタリカバリ（DR）ソフトウェアであるONTAP解決策for VMware Site Recovery Manager（SRM）について説明します。最新の製品情報とベストプラクティスを紹介し、導入の合理化、リスクの軽減、継続的な管理の簡素化を実現します。

> このドキュメントは、以前に公開されていたテクニカルレポート「TR-4900：VMware Site Recovery Manager」をONTAPに置き換えます。

ベストプラクティスは、ガイドや互換性ツールなどの他のドキュメントを補うものです。ラボテストに基づいて開発されており、ネットアップのエンジニアやお客様は広範な現場経験を積んでいます。推奨されるベストプラクティスがお客様の環境に適していない場合もありますが、一般に最もシンプルなソリューションであり、ほとんどのお客様のニーズに対応できます。

本ドキュメントでは、ONTAP Tools for VMware vSphere 9.12（NetApp Storage Replication Adapter[SRA]およびVASA Provider[VP]を含む）およびVMware Site Recovery Manager 8.7と組み合わせて使用した場合の、ONTAP 9の最近のリリースの機能を中心に説明します。

SRM で ONTAP を使用する理由

ONTAP ソフトウェアを基盤とするネットアップのデータ管理プラットフォームは、 SRM に最も広く採用されているストレージソリューションの一部です。理由はそれだけではありません。セキュアでハイパフォーマンスなユニファイドプロトコル（NASとSANを併用）データ管理プラットフォームで、業界を定義するストレージ効率、マルチテナンシー、サービス品質管理、スペース効率に優れたSnapshotによるデータ保護、SnapMirrorによるレプリケーションを実現します。VMware ワークロードを保護するためにネイティブのハイブリッドマルチクラウド統合を活用し、多数の自動化ツールやオーケストレーションツールを簡単に利用できます。

SnapMirrorをアレイベースのレプリケーションに使用すると、実績のある成熟したONTAPのテクノロジを活用できます。SnapMirror を使用すると、 VM やデータストア全体ではなく、変更されたファイルシステムブロックのみをコピーして、データを安全かつ効率的に転送できます。重複排除、圧縮、コンパクションなどのスペース削減効果を活用できます。最新の ONTAP システムで、バージョンに依存しない SnapMirror が使用されるようになり、ソースとデスティネーションのクラスタを柔軟に選択できるようになりました。SnapMirror は、災害復旧のための最も強力なツールの 1 つとなりました。

従来の NFS 、 iSCSI 、ファイバチャネル接続データストア（現在は VVOL データストアをサポート）のいずれを使用している場合でも、 SRM は、ディザスタリカバリやデータセンター移行の計画とオーケストレーションに ONTAP の機能のメリットを活用する堅牢なファーストパーティ製品を提供します。

SRM での ONTAP 9 の活用方法

SRM は、 ONTAP システムの高度なデータ管理テクノロジを活用して、 3 つの主要コンポーネントで構成される仮想アプライアンスである VMware vSphere 用 ONTAP ツールと統合します。

- vCenter プラグイン（旧 Virtual Storage Console （ VSC ））は、 SAN と NAS のどちらを使用している場合でも、ストレージ管理と効率化機能の簡易化、可用性の向上、ストレージコストと運用オーバーヘッドの削減を実現します。データストアのプロビジョニングのベストプラクティスを使用して、 NFS 環境およびブロックストレージ環境用の ESXi ホスト設定を最適化します。以上のメリットのために、 ONTAP ソフトウェアを実行するシステムで vSphere を使用する場合はこのプラグインを推奨します。
- VASA Provider for ONTAP は、 VMware vStorage APIs for Storage Awareness （ VASA ）フレームワークをサポートしています。VASA Provider では、 VM ストレージのプロビジョニングと監視に役立つように vCenter Server と ONTAP を接続します。VMware Virtual Volumes （ VVol ）のサポートと、ストレージ機能プロファイル（ VVol レプリケーション機能を含む）の管理、および個々の VM VVol のパフォーマンスの管理が可能になります。また、容量の監視やプロファイルへの準拠に関するアラームも生成されます。SRM と一緒に使用すると、 VASA Provider for ONTAP で VVOL ベースの仮想マシンをサポートできます。 SRM サーバに SRA アダプタをインストールする必要はありません。
- SRA は SRM と一緒に使用され、従来の VMFS データストアと NFS データストアの本番サイトとディザスタリカバリサイト間での VM データのレプリケーションを管理します。また、 DR レプリカの無停止テストにも使用できます。検出、リカバリ、再保護のタスクを自動化します。Windows SRM サーバおよび SRM アプライアンス用の SRA サーバアプライアンスと SRA アダプタの両方が含まれています。

SRM サーバに SRA アダプタをインストールして設定し、 VASA Provider で VVol 以外のデータストアを保護したり VVOL のレプリケーションを有効にしたりしたあとで、ディザスタリカバリ用に vSphere 環境を設定する作業を開始できます。

SRA と VASA Provider には、 SRM サーバ用のコマンド / 制御インターフェイスが用意されており、 VMware 仮想マシン（ VM ）を含む ONTAP FlexVol や、 SRA を保護する SnapMirror レプリケーションを管理できます。

SRM 8.3 以降では、 SRM サーバへの新しい SRM VVol Provider 制御パスが導入され、 SRA を使用せずに vCenter サーバおよびその経由で VASA Provider に通信できるようになりました。これにより、 SRM サーバは緊密に統合するための完全な API を提供するため、以前よりもはるかに ONTAP クラスタの制御を活用できました。

SRMでは、ネットアップ独自のFlexCloneテクノロジを使用して、システムを停止することなくDR計画をテストし、保護されたデータストアのクローンをDRサイトにほぼ瞬時に作成できます。SRM はサンドボックスを作成して安全にテストし、真の災害が発生した場合に組織とお客様を保護します。そのため、組織は災害時にフェイルオーバーを実行できます。

実際に災害が発生した場合や、計画的な移行の場合でも、 SRM では、最終的な SnapMirror 更新（必要な場合）を使用して、データセットに最新の変更を送信できます。その後、ミラーを解除し、 DR ホストにデータストアをマウントします。この時点で、計画済みの戦略に基づいて、 VM の電源を任意の順序で自動的にオンにすることができます。

SRM と ONTAP などのユースケース：ハイブリッドクラウドと移行

SRM 環境に ONTAP の高度なデータ管理機能を統合することで、ローカルストレージオプションに比べて、拡張性とパフォーマンスが大幅に向上します。それだけではありませんが、ハイブリッドクラウドの柔軟性を備えています。ハイブリッドクラウドを使用すると、 FabricPool を使用して、未使用のデータブロックをハイパフォーマンスアレイから希望するハイパースケーラに階層化してコストを削減できます。これは、 NetApp StorageGRID などのオンプレミスの S3 ストアである可能性があります。また、 ONTAP Select （ CVO ）やを使用して、ソフトウェアで定義される Cloud Volumes ONTAP やクラウドベースの DR でエッジベースのシステムに SnapMirror を使用することもできます "Equinix 内の NetApp Private Storage" Amazon Web Services （ AWS ）、 Microsoft Azure 、 Google Cloud Platform （ GCP ）で、クラウド内に完全に統合されたストレージ、ネットワーク、コンピューティングサービスのスタックを構築できます。

その後、FlexCloneを使用すれば、ストレージの設置面積をほぼゼロに抑えながら、クラウドサービスプロバイダのデータセンター内でテストフェイルオーバーを実行できます。組織を保護することで、かつてないほどコストを削減できます。

SRM は、 SnapMirror を使用して、計画的な移行を実行することもできます。これにより、 VM を 1 つのデータセンターから別のデータセンターに効率的に転送したり、独自のデータセンターや、任意の数のネットアップパートナーサービスプロバイダを介して VM を転送したりできます。

導入のベストプラクティス

次のセクションでは、ONTAPとVMware SRMを使用した導入のベストプラクティスについて説明します。

SMT の SVM のレイアウトとセグメント化

ONTAP では、 Storage Virtual Machine （ SVM ）の概念を採用して、セキュアなマルチテナント環境で厳密にセグメント化します。ある SVM の SVM ユーザは、別の SVM のリソースにアクセスしたりリソースを管理したりすることはできませんこれにより、 ONTAP テクノロジを活用できます。ビジネスユニットごとに別々の SVM を作成して、同じクラスタ上で独自の SRM ワークフローを管理することで、全体的なストレージ効率を高めることができます。

SVM を対象としたアカウントと SVM 管理 LIF を使用して ONTAP を管理することを検討し、セキュリティ制御を強化するだけでなく、パフォーマンスも向上させます。SRA は、物理リソースを含むクラスタ全体のすべてのリソースを処理する必要がないため、 SVM を対象とした接続を使用する場合は本質的にパフォーマンスが向上します。その代わり、特定の SVM に抽象化された論理資産だけを認識する必要があります。

NAS プロトコルのみを使用する（ SAN アクセスなし）場合は、次のパラメータを設定することで、 NAS 向けに最適化された新しいモードを利用することもできます（ SRA と VASA は、アプライアンスで同じバックエンドサービスを使用するため）。

1. コントロールパネルにログインします。 `https://<IP address>:9083` [Web based CLI interface]をクリックします。
2. コマンドを実行します `vp updateconfig -key=enable.qtree.discovery -value=true`。
3. コマンドを実行します `vp updateconfig -key=enable.optimised.sra -value=true`。
4. コマンドを実行します `vp reloadconfig`。

VVOL に ONTAP ツールを導入する際の考慮事項について説明します

SRM で VVol を使用する場合は、クラスタを対象としたクレデンシャルとクラスタ管理 LIF を使用してストレージを管理する必要があります。これは、 VM ストレージポリシーに必要なポリシーを満たすためには、 VASA Provider で基盤となる物理アーキテクチャを理解しておく必要があるためです。たとえば、オールフラッシュストレージを必要とするポリシーが設定されている場合、 VASA Provider では、どのシステムがオールフラッシュであるかを認識できる必要があります。

ONTAP Tools アプライアンスを管理している VVOL データストアに格納しないことを推奨します。その結果、アプライアンスがオフラインのためにアプライアンスのスワップ VVOL を作成できず、 VASA Provider の電源をオンにできなくなることがあります。

ONTAP 9 システムの管理に関するベストプラクティス

前述したように、クラスタまたは SVM を対象としたクレデンシャルと管理 LIF を使用して ONTAP クラスタを管理できます。パフォーマンスを最適化するには、VVOLを使用しないときは常にSVMを対象としたクレデンシャルの使用を検討してください。ただし、その場合は、いくつかの要件について確認しておく必要があります。また、機能の一部は失われます。

- デフォルトの vsadmin SVM アカウントには、 ONTAP ツールのタスクを実行するために必要なアクセスレベルがありません。そのため、新しい SVM アカウントを作成する必要があります。
- ONTAP 9.8以降を使用している場合はNetApp、ONTAP System Managerの[Users]メニューとONTAP toolsアプライアンスにあるjsonファイルを使用して、RBACの最小権限を持つユーザアカウントを作成することを推奨します。 `https://<IP address>:9083/vsc/config/`。管理者パスワードを使用して JSON ファイルをダウンロードしてください。これは SVM またはクラスタを対象としたアカウントに使用できます。

  ONTAP 9.6 以前を使用している場合は、で使用可能な RBAC User Creator （ RUC ）ツールを使用する必要があります "NetApp Support Siteの Toolchest"。

- vCenter UI プラグイン、 VASA Provider 、 SRA サーバはすべて完全に統合されたサービスであるため、vCenter UI で ONTAP ツール用のストレージを追加する場合と同じ方法で、 SRM で SRA アダプタにストレージを追加する必要があります。そうしないと、 SRA サーバが SRA アダプタ経由で SRM から送信された要求を認識しない可能性があります。
- SVM を対象としたクレデンシャルを使用している場合、 NFS パスのチェックは実行されませんこれは、物理的な場所が SVM から論理的に抽象化されているためです。ただしこれは原因の問題ではありません。最新の ONTAP システムで間接パスを使用してもパフォーマンスが著しく低下することはなくなりました。
- Storage Efficiency によるアグリゲートのスペース削減量が報告されないことがあります。
- サポートされている場合、負荷共有ミラーを更新することはできません。
- SVM を対象としたクレデンシャルで管理されている ONTAP システムでは、 EMS ロギングが実行されない場合があり

運用上のベストプラクティス

以降のセクションでは、VMware SRMとONTAPストレージの運用に関するベストプラクティスについて説明します。

データストアおよびプロトコル

- 可能であれば、必ず ONTAP ツールを使用してデータストアとボリュームをプロビジョニングしてください。ボリューム、ジャンクションパス、 LUN 、 igroup 、エクスポートポリシーが その他の設定は互換性のある方法で構成されます。
- SRM では、 ONTAP 9 で iSCSI 、ファイバチャネル、および NFS バージョン 3 をサポートしているのは、 SRA 経由のアレイベースのレプリケーションを使用している場合です。SRM は、従来のデータストアまたは VVOL データストアでの NFS バージョン 4.1 のアレイベースのレプリケーションをサポートしていません。
- 接続を確認するために、 DR サイトの新しいテスト用データストアをデスティネーション ONTAP クラスタからマウントしてアンマウントできることを必ず確認してください。データストアの接続に使用する各プロトコルをテストします。テスト用データストアは SRM の指示に従ってすべてのデータストアの自動

化を実行するため、 ONTAP ツールを使用して作成することを推奨します。

- SAN プロトコルは各サイトで同機種にする必要があります。NFS と SAN を混在させることはできますが、 SAN プロトコルを 1 つのサイト内に混在させないでください。たとえば、サイト A では FCP を、サイト B では iSCSI を使用できますサイト A では、 FCP と iSCSI の両方を使用しないでくださいその理由は、 SRA がリカバリサイトに混在する igroup を作成しないため、 SRM が SRA に指定されたイニシエータリストをフィルタリングしないためです。
- 以前のガイドでは、データの局所性にLIFを作成することを推奨つまり、必ず、ボリュームを物理的に所有するノード上の LIF を使用してデータストアをマウントします。これは、 ONTAP 9 の最新バージョンでは必須ではなくなりました。可能なかぎり、クラスタを対象としたクレデンシャルを指定した場合でも、ONTAPツールではデータに対してローカルなLIF間で負荷を分散するように選択されますが、高可用性やパフォーマンスを確保するための必須要件ではありません。
- ONTAP 9では、オートサイズが緊急時に十分な容量を提供できない場合に、スペース不足が発生したときにSnapshotを自動的に削除してアップタイムを維持するように設定できます。この機能のデフォルト設定では、SnapMirrorで作成されたSnapshotは自動的に削除されません。SnapMirror Snapshotが削除されると、NetApp SRAは影響を受けたボリュームのレプリケーションを反転および再同期できません。ONTAPがSnapMirror Snapshotを削除しないようにするには、Snapshotの自動削除機能をtryに設定します。

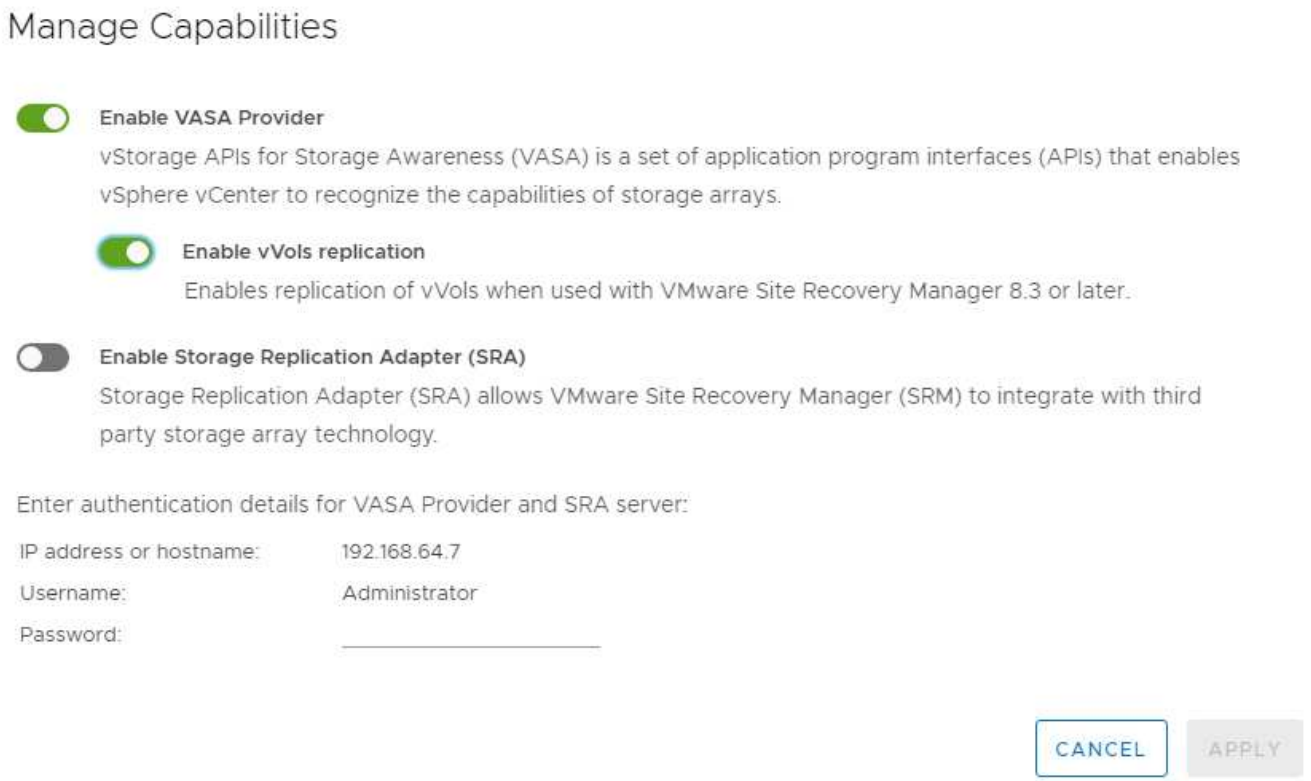
```
snap autodelete modify -volume -commitment try
```

- ボリュームのオートサイズの設定： `grow` SANデータストアヲフクムボリューム `grow_shrink` （NFSデータストアの場合）。の詳細を確認してください "ボリュームを自動的に拡張または縮小するための設定"。
- SRMは、データストアの数が少なく、保護グループがリカバリプランで最小化されている場合に最適なパフォーマンスを発揮します。したがって、RTOが重要なSRMで保護された環境では、VM密度の最適化を検討する必要があります。
- Distributed Resource Scheduler（DRS）を使用して、保護対象のESXiクラスタとリカバリESXiクラスタの負荷を分散します。フェイルバックを計画している場合、再保護を実行すると、以前に保護されていたクラスタが新しいリカバリクラスタになります。DRSは、両方向への配置のバランスをとるのに役立ちます。
- SRMでIPカスタマイズを使用するとRTOが増加する可能性があるため、可能な場合は使用しないでください。

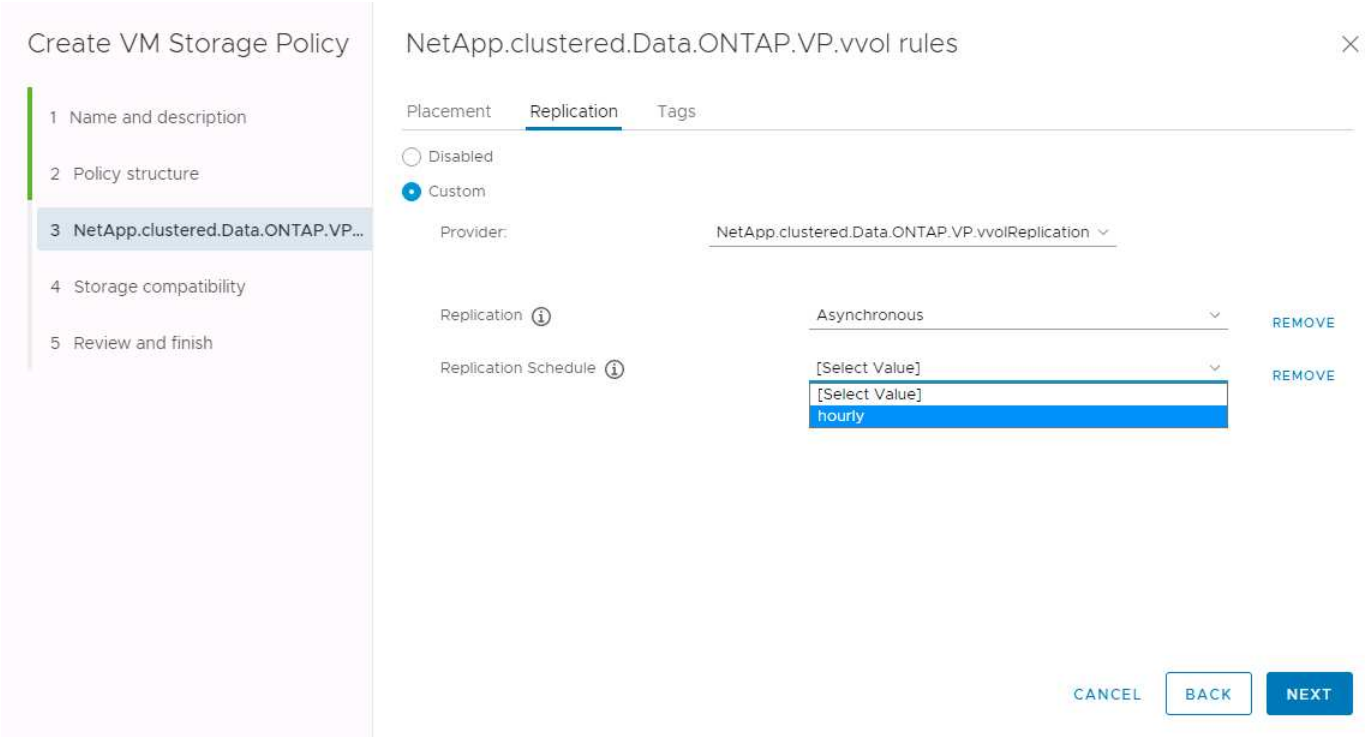
Storage Policy Based Management（SPBM；ストレージポリシーベースの管理）とVVOL

SRM 8.3以降では、vVolデータストアを使用したVMの保護がサポートされます。SnapMirror スケジュールは、次のスクリーンショットに示すように、 ONTAP のツール設定メニューで VVOL のレプリケーションが有効になっている場合、 VASA Provider によって VM ストレージポリシーに公開されます。

次の例は、vVolレプリケーションを有効にする方法を示しています。

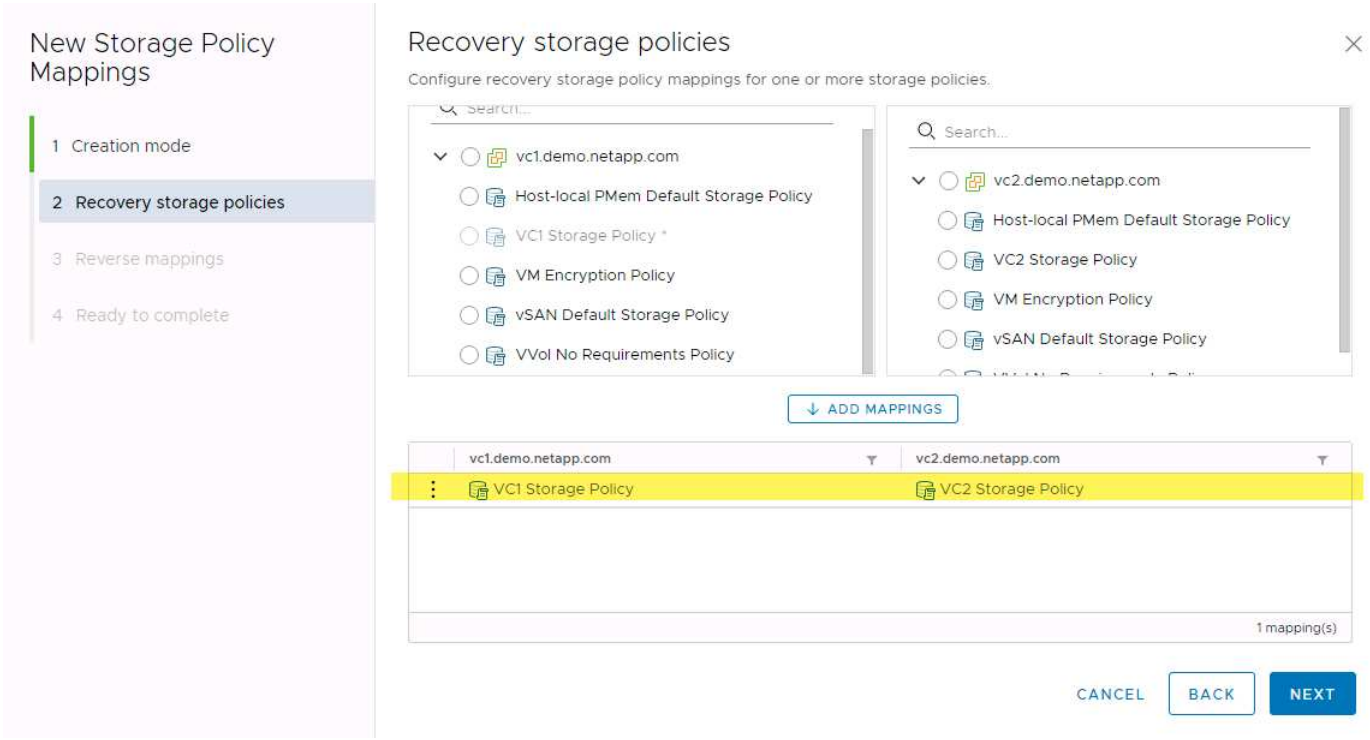


次のスクリーンショットは、 VM ストレージポリシーの作成ウィザードに表示される SnapMirror スケジュールの例を示しています。



ONTAP VASA プロバイダでは、異なるストレージへのフェイルオーバーがサポートされます。たとえば、システムは、エッジの場所にある ONTAP Select からコアデータセンターの AFF システムにフェイルオーバーできます。ストレージの類似性に関係なく、レプリケーションが有効な VM ストレージポリシーのストレージポリシーマッピングとリバースマッピングを常に設定して、リカバリサイトで提供されるサービスが期待され

る要件を満たしていることを確認する必要があります。次のスクリーンショットは、ポリシーマッピングの例を示しています。



VVOL データストア用にレプリケートされたボリュームを作成します

以前の VVOL データストアとは異なり、レプリケートされた VVOL データストアはレプリケーションを有効にして最初から作成する必要があります。また、 SnapMirror 関係を持つ ONTAP システムで事前に作成されたボリュームを使用する必要があります。そのためには、クラスタピアリングや SVM ピアリングなどの設定を事前に行う必要があります。これらのアクティビティはONTAP管理者が実行する必要があります。これにより、複数のサイトでONTAPシステムを管理する担当者とvSphereの運用を主に担当する担当者が厳密に分離されます。

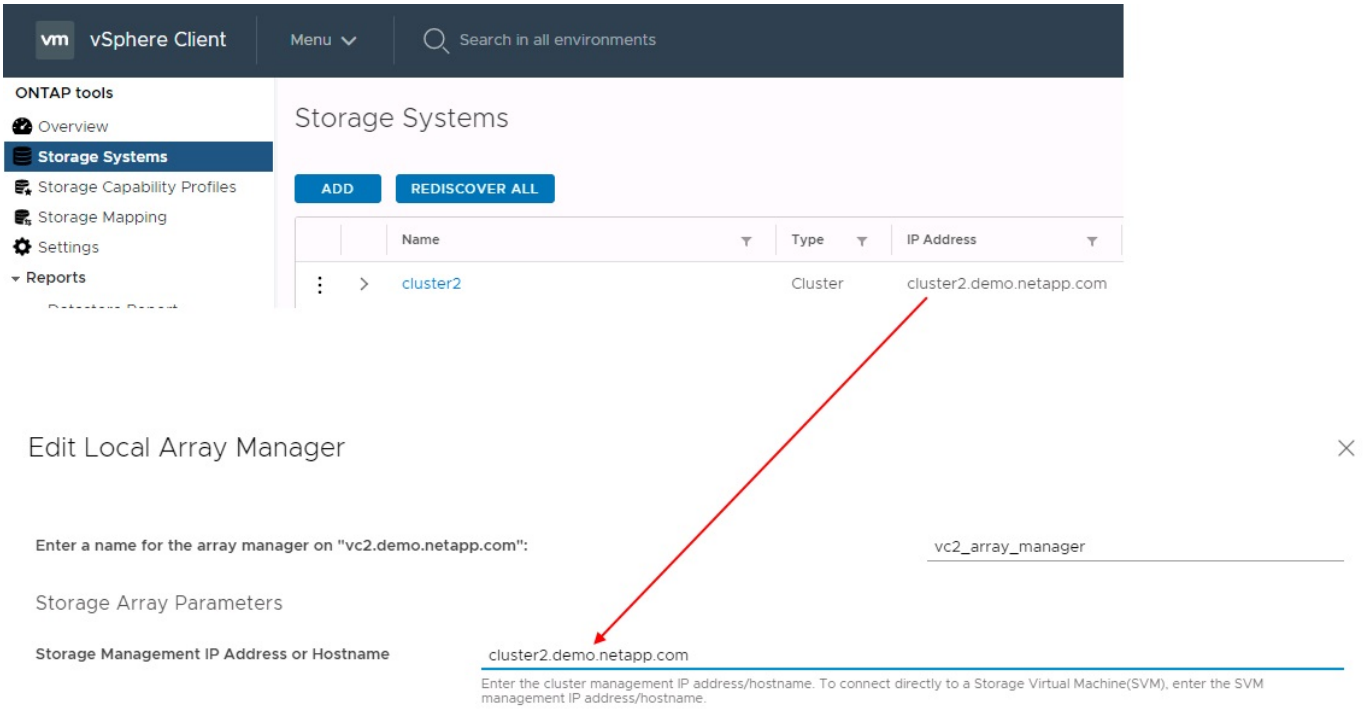
これは、 vSphere 管理者の代わりに新たな要件となります。ボリュームは ONTAP ツールの範囲外に作成されるため、定期的な再検出スケジュール期間が設定されるまで ONTAP 管理者が行った変更を認識することはありません。そのため、 VVOL で使用するボリュームまたは SnapMirror 関係を作成したときは常に再検出を実行することを推奨します。次のスクリーンショットに示すように、ホストまたはクラスタを右クリックし、ONTAP tools]>[Update Host and Storage Data]を選択します。

VVOL と SRM については、 1 つ注意が必要です。保護された VM と保護されていない VM を同じ VVOL データストアに混在させないでください。これは、 SRM を使用して DR サイトにフェイルオーバーする場合、保護グループに属する VM のみが DR でオンラインになるためです。そのため、再保護（ SnapMirror を DR から本番環境に戻して再保護）する際に、フェイルオーバーされなかった VM が上書きされて、貴重なデータが含まれる可能性があります。

アレイペアについて

アレイペアごとにアレイマネージャが作成されます。SRM ツールと ONTAP ツールでは、クラスタクレデンシャルを使用している場合でも、各アレイペアリングを SVM の範囲で実行します。これにより、管理対象に割り当てられている SVM を基に、各テナント間で DR ワークフローを分割できます。特定のクラスタに対して複数のアレイマネージャを作成し、非対称にすることができます。異なる ONTAP 9 クラスタ間でファンアウトまたはファンインを実行できます。たとえば、クラスタ 1 の SVM A と SVM B をクラスタ 2 の SVM C に、クラスタ 3 の SVM D に、またはその逆にレプリケートできます。

SRM でアレイペアを設定する場合は、 ONTAP ツールに追加するのと同じ方法でアレイペアを SRM に追加する必要があります。つまり、アレイペアは同じユーザ名、パスワード、および管理 LIF を使用する必要があります。これは、 SRA がアレイと正しく通信するための要件です。次のスクリーンショットは、 ONTAP ツールでのクラスタの表示方法と、アレイマネージャへのクラスタの追加方法を示しています。



複製グループについて

レプリケーショングループには、同時にリカバリされる仮想マシンの論理集合が含まれます。レプリケーショングループは、 ONTAP ツール VASA Provider で自動的に作成されます。ONTAP の SnapMirror レプリケーションはボリュームレベルで実行されるため、ボリューム内のすべての VM が同じレプリケーショングループに属します。

レプリケーショングループについて考慮する必要がある要素と、 FlexVol ボリュームに VM を分散する方法にはいくつかの要素があります。類似するVMを同じボリュームにグループ化すると、アグリゲートレベルの重複排除機能がない古いONTAPシステムでストレージ効率を高めることができますが、グループ化するとボリュームのサイズが大きくなり、ボリュームのI/Oの同時実行数が少なくなります。最新のONTAPシステムでは、同じアグリゲート内のFlexVolボリュームにVMを分散することで、パフォーマンスとストレージ効率の最適なバランスを実現できます。その結果、アグリゲートレベルの重複排除が活用され、複数のボリューム間でI/Oの並列化が促進されます。保護グループ（以下で説明）には複数のレプリケーショングループを含めることができるため、ボリューム内の VM を 1 つにまとめてリカバリできます。このレイアウトの欠点は、Volume SnapMirrorではアグリゲートの重複排除が考慮されないため、ブロックがネットワーク経由で複数回送信される可能性があることです。

レプリケーショングループの最後の考慮事項の 1 つは、各グループがその性質によって論理整合グループになることです（ SRM 整合グループと混同しないようにしてください）。これは、ボリューム内のすべての VM が同じ Snapshot を使用して同時に転送されるためです。したがって、相互に整合性が必要な VM がある場合は、同じ FlexVol に格納することを検討してください。

保護グループについて

保護グループでは、 VM とデータストアをグループ単位で定義し、グループをまとめて保護サイトからリカバリします。保護対象サイトとは、通常の安定状態での運用中、保護グループで構成された VM が存在する場所です。SRM には保護グループの複数のアレイマネージャが表示される場合がありますが、保護グループは複数のアレイマネージャにまたがることはできません。このため、異なる SVM 上の複数のデータストアに VM ファイルをまたがって配置することはできません。

リカバリ・プランについて

リカバリプランでは、同じプロセスでリカバリする保護グループを定義します。同じリカバリプランに複数の保護グループを設定できます。また、リカバリプランの実行オプションを増やすには、 1 つの保護グループを複数のリカバリプランに含めることもできます。

リカバリプランを使用すると、 SRM 管理者は、 VM を優先グループ 1 （最大）から 5 （最小）に割り当てて、リカバリワークフローを定義できます。デフォルトは 3 （中）です。優先度グループ内で、 VM に依存関係を設定できます。

たとえば、データベースにMicrosoft SQL Serverを使用するティア1のビジネスクリティカルなアプリケーションがあるとします。したがって、優先度グループ 1 に VM を配置することにします。優先度グループ 1 では、サービスの提供順序の計画を開始します。Microsoft Windows ドメイン・コントローラを起動してから Microsoft SQL Server を起動してください。アプリケーション・サーバの前にオンラインになっている必要があります。依存関係は特定の優先度グループ内でのみ適用されるため、これらすべてのVMを優先度グループに追加してから依存関係を設定します。

アプリケーションチームと連携してフェイルオーバーシナリオに必要な処理の順序を把握し、それに応じてリカバリ計画を作成することを強く推奨します。

テストフェイルオーバー

ベストプラクティスとして、保護対象の VM ストレージの構成を変更する場合は、必ずテストフェイルオーバーを実行してください。これにより、災害が発生した場合に、Site Recovery Managerが予想されるRTOターゲット内でサービスをリストアできると信頼できます。

特に VM ストレージの再設定後にゲストアプリケーションの機能を確認することを推奨します。

テストリカバリ処理を実行すると、 VM 用の ESXi ホストにプライベートテスト用のバブルネットワークが作成されます。ただし、このネットワークは物理ネットワークアダプタに自動的には接続されないため、 ESXi ホスト間の接続は提供されません。DR テスト時に異なる ESXi ホストで実行されている VM 間の通信を可能にするために、 DR サイトの ESXi ホスト間に物理プライベートネットワークを作成します。テスト用ネットワークがプライベートであることを確認するために、テスト用のバブルネットワークを物理的に分離するか、 VLAN や VLAN タギングを使用して分離します。このネットワークは本番用ネットワークから分離する必要があります。 VM がリカバリされると、実際の本番用システムと競合する可能性のある IP アドレスを持つ本番用ネットワークに配置することはできなくなります。SRM でリカバリプランを作成する際、テスト中に VM を接続するためのプライベートネットワークとして、作成したテストネットワークを選択できます。

テストが検証されて不要になったら、クリーンアップ処理を実行します。クリーンアップを実行すると、保護

されている VM が初期状態に戻り、リカバリプランが Ready 状態にリセットされます。

フェイルオーバーに関する考慮事項

サイトのフェイルオーバーに関しては、このガイドに記載されている処理の順序に加えて、その他にもいくつかの考慮事項があります。

競合する問題の 1 つに、サイト間のネットワークの違いがあります。環境によっては、プライマリサイトと DR サイトで同じネットワーク IP アドレスを使用できる場合があります。この機能は、拡張仮想 LAN （ VLAN ）または拡張ネットワークセットアップと呼ばれます。それ以外の環境では、プライマリサイトと DR サイトで別々のネットワーク IP アドレス（異なる VLAN など）を使用する必要があります。

VMware では、この問題を解決する方法をいくつか提供しています。1 つは、 VMware NSX -T Data Center のようなネットワーク仮想化テクノロジーです。ネットワークスタック全体を運用環境からレイヤ 2 ～ 7 に抽象化し、より移植性の高いソリューションを実現します。の詳細を確認してください "SRMでのNSX-Tオプション"。

SRM では、リカバリ時に VM のネットワーク設定を変更することもできます。この再設定には、IPアドレス、ゲートウェイアドレス、DNSサーバ設定などの設定が含まれます。リカバリ時に個 々 のVMに適用されるさまざまなネットワーク設定は、リカバリプランのVMのプロパティ設定で指定できます。

VMware の dr-ip-customizer というツールを使用すると、リカバリプランで複数の VM のプロパティを個別に編集しなくても、 SRM で VM ごとに異なるネットワーク設定を適用できます。このユーティリティの使用方法については、を参照してください。 "VMwareのドキュメント"。

再保護

リカバリ後、リカバリサイトが新しい本番用サイトになります。リカバリ処理によって SnapMirror レプリケーションが解除されたため、新しい本番用サイトは今後の災害から保護されません。新しい本番用サイトは、リカバリ後すぐに別のサイトで保護することを推奨します。元の本番サイトが運用されている場合、 VMware 管理者は、元の本番サイトを新しいリカバリサイトとして使用して新しい本番サイトを保護できるため、保護の方向を実質的に変えることができます。再保護は、致命的でない障害でのみ使用できます。そのため、元の vCenter Server 、 ESXi サーバ、 SRM サーバ、および対応するデータベースを最終的にリカバリ可能な状態にする必要があります。使用できない場合は、新しい保護グループと新しいリカバリプランを作成する必要があります。

フェイルバック

フェイルバック処理は、基本的に以前とは異なる方向のフェイルオーバーです。ベストプラクティスとして、フェイルバックを実行する前に、元のサイトが許容可能なレベルの機能に戻っていること、つまり元のサイトにフェイルオーバーしていることを確認することを推奨します。元のサイトが侵害されたままの場合は、障害が十分に修正されるまでフェイルバックを遅らせる必要があります。

フェイルバックのもう 1 つのベストプラクティスとして、再保護の完了後、および最終フェイルバックの実行前に、常にテストフェイルオーバーを実行することがあります。これにより、元のサイトに配置されたシステムで処理が完了できるかどうかを確認できます。

元のサイトを再保護する

フェイルバック後、再保護を再度実行する前に、すべての関係者にサービスが正常に戻ったことを確認する必要があります。

フェイルバック後の再保護を実行すると、基本的に環境は最初の状態に戻り、 SnapMirror レプリケーションが本番用サイトからリカバリサイトに再度実行されます。

レプリケーショントポロジ

ONTAP 9 では、クラスタの物理コンポーネントはクラスタ管理者には見えますが、クラスタを使用しているアプリケーションやホストからは直接見えません。物理コンポーネントは共有リソースのプールを提供し、このリソースプールから論理クラスタリソースが構築されます。アプリケーションとホストは、ボリュームと LIF を含む SVM 経由でのみデータにアクセスします。

VMware vCenter Site Recovery Manager では、各 NetApp SVM がアレイとして扱われます。SRM は、特定のアレイ間（または SVM から SVM ）のレプリケーションレイアウトをサポートしています。

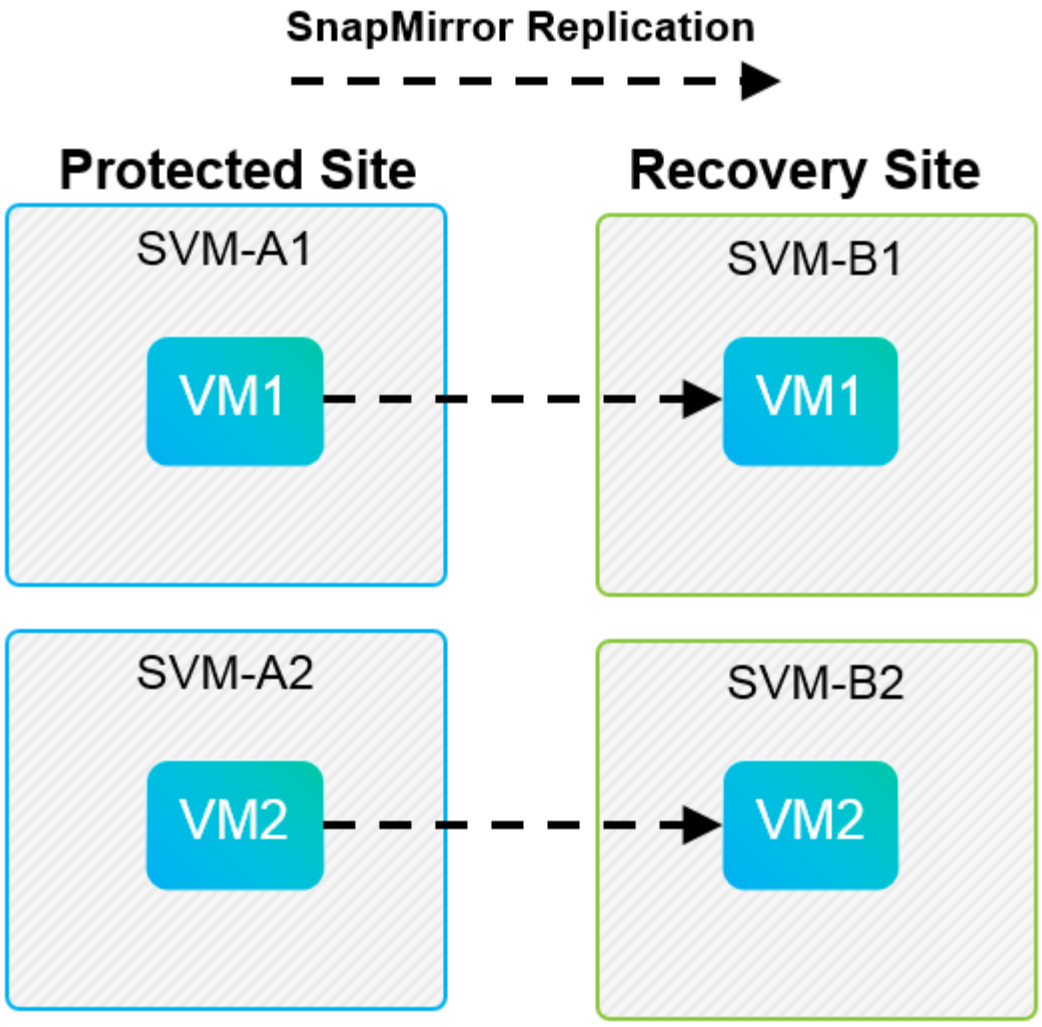
1 つの VM が、次の理由から、複数の SRM アレイ上で仮想マシンディスク（ VMDK ）または RDM を所有することはできません。

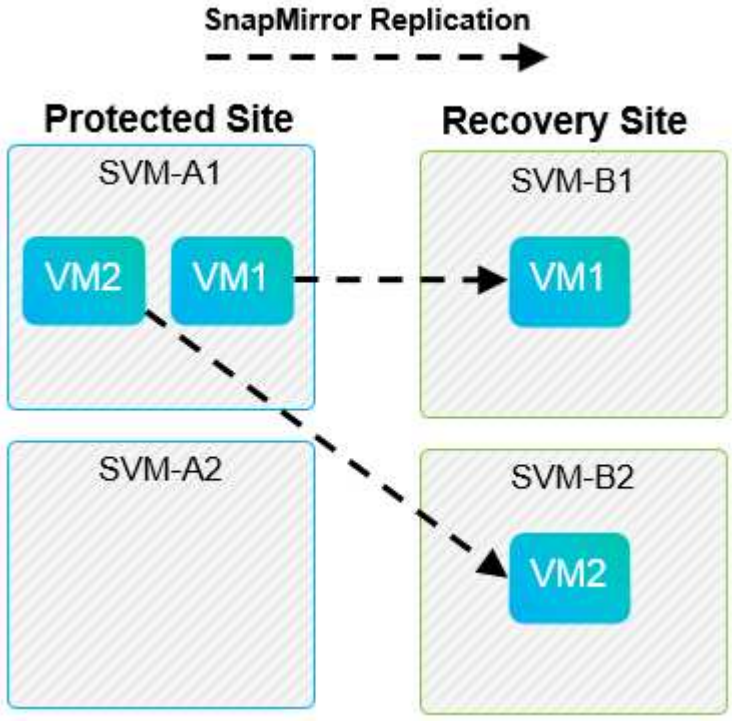
- SRM は SVM のみを認識し、個々の物理コントローラは認識しません。
- SVM は、クラスタ内の複数のノードにまたがる LUN とボリュームを制御できます。

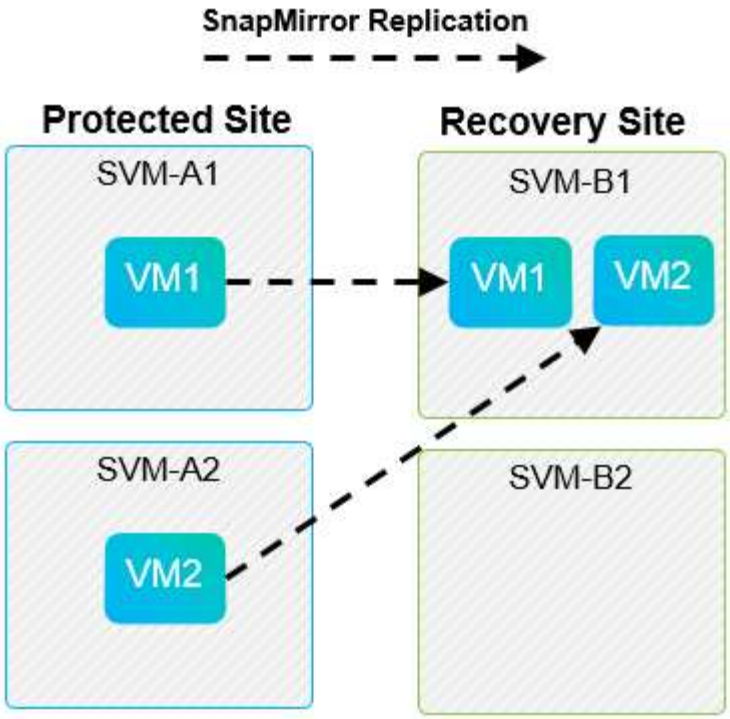
ベストプラクティス
サポートされるかどうかを判断するには、このルールに注意してください。 SRM と NetApp SRA を使用して VM を保護するには、 VM のすべての部分が 1 つの SVM 上にのみ存在する必要があります。このルールは、保護対象サイトとリカバリサイトの両方に適用されます。

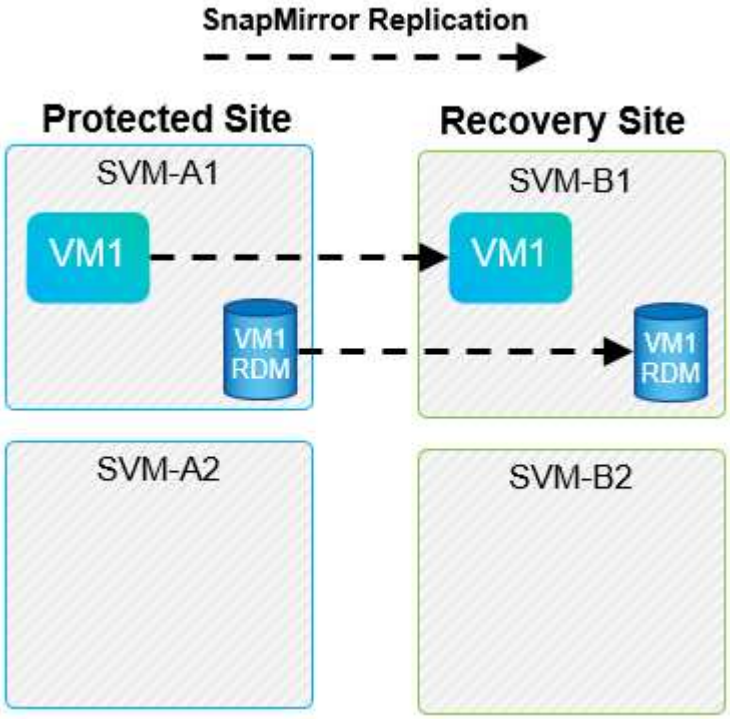
サポートされる **SnapMirror** レイアウト

次の図は、 SRM と SRA でサポートされる SnapMirror 関係のレイアウトシナリオを示しています。レプリケートされたボリューム内の各 VM は、各サイトの 1 つの SRM アレイ（ SVM ）上のデータのみを所有します。


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2

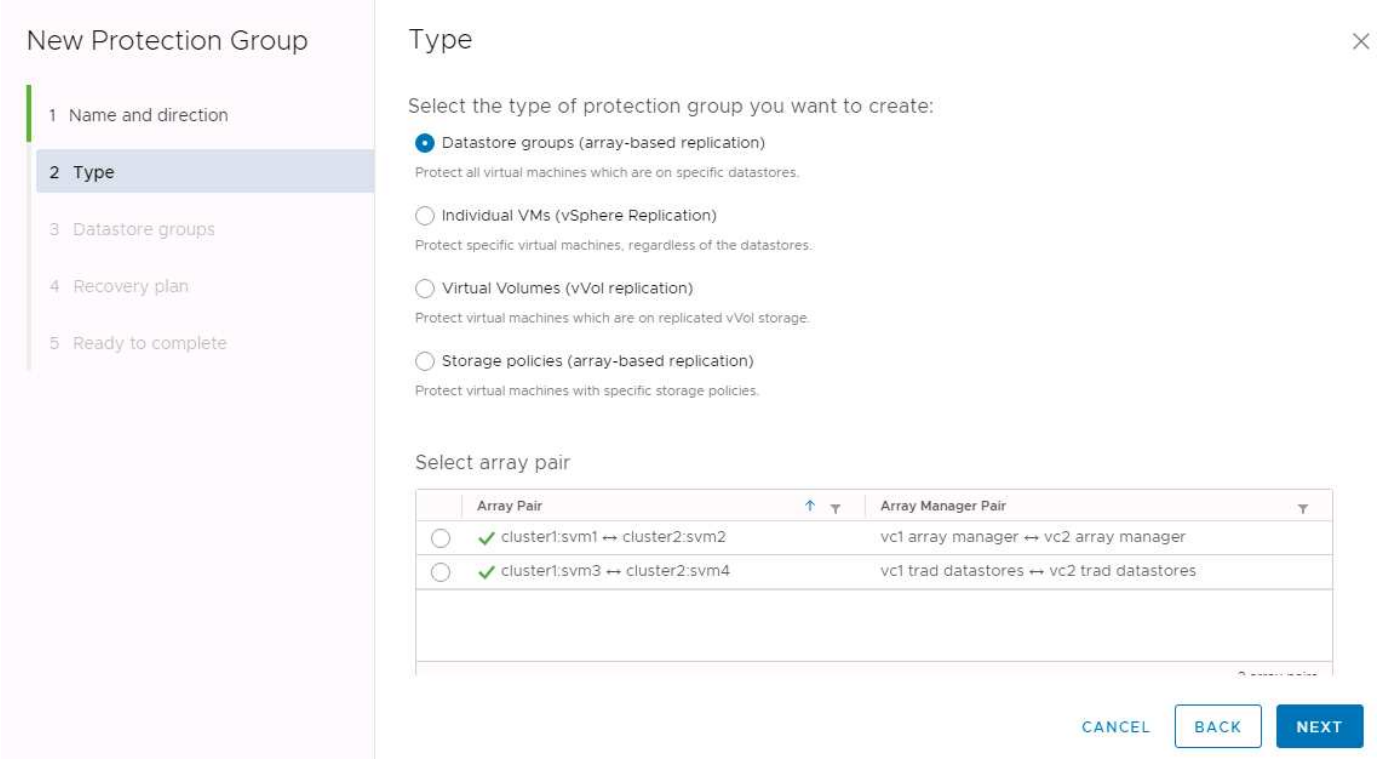

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





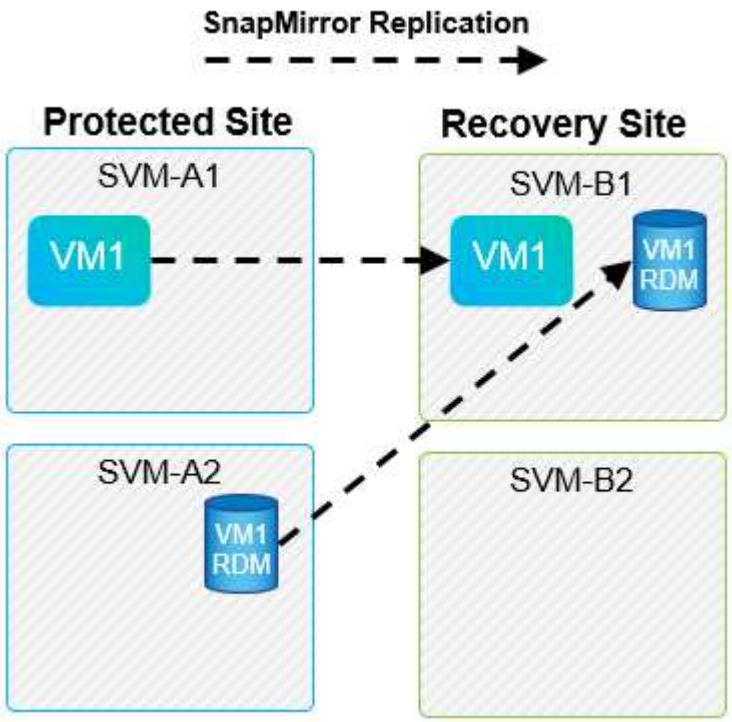
サポートされている **Array Manager** レイアウト

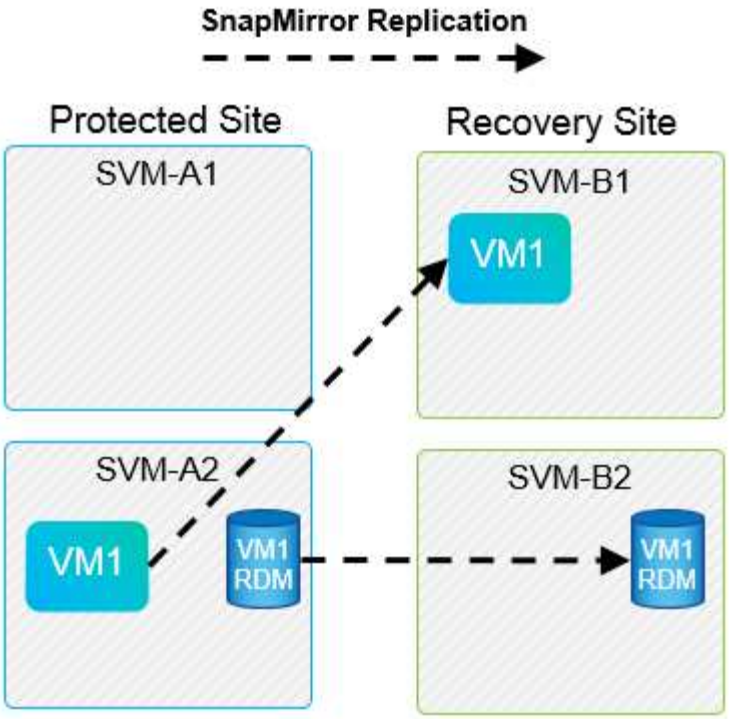
次のスクリーンショットに示すように、 SRM でアレイベースレプリケーション（ ABR ）を使用すると、保護グループは単一のアレイペアに分離されます。このシナリオでは、 SVM1 および SVM2 ピア関係を設定する SVM3 および SVM4 リカバリサイトで。ただし、保護グループを作成するときに選択できるアレイペアは 2 つのうちの 1 つだけです。



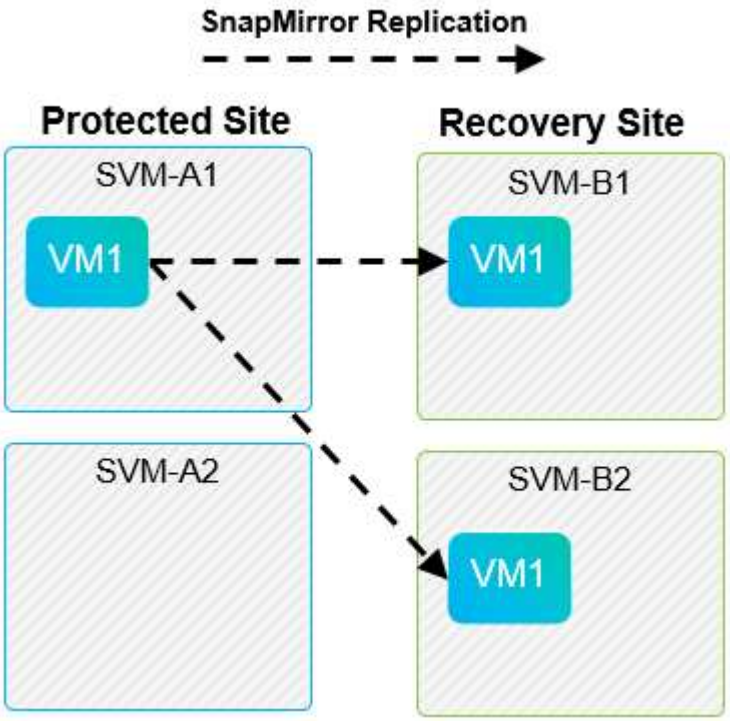
サポートされないレイアウトです

サポート対象外の構成では、個々の VM が所有する複数の SVM にデータ（ VMDK または RDM ）があります。次の図に示す例では、 `VM1` SRMで保護を設定できません。理由： `VM1` 2つのSVM上のデータがあります。





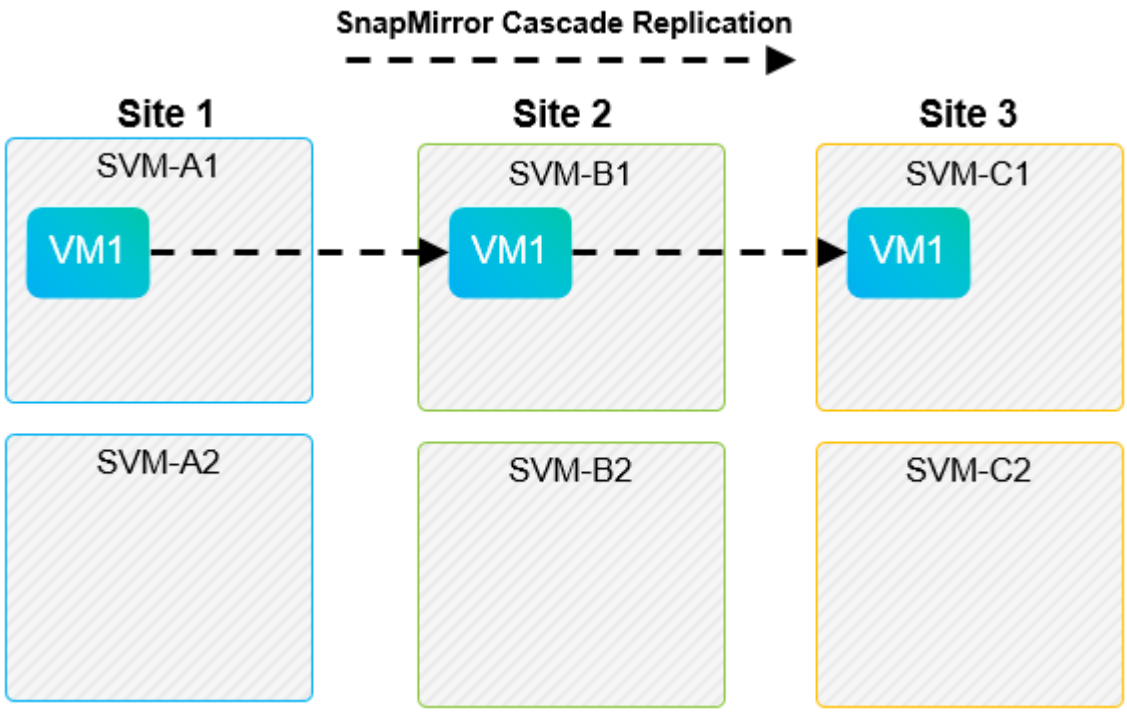
1 つのネットアップボリュームを 1 つのソース SVM から同じ SVM または異なる SVM の複数のデスティネーションにレプリケートするレプリケーション関係は、 SnapMirror ファンアウトと呼ばれます。SRM ではファンアウトはサポートされていません。次の図の例では、 `VM1` SnapMirrorを使用して2つの異なる場所にレプリケートされるため、SRMで保護を設定できません。



SnapMirror カスケード

SnapMirror でソースボリュームをデスティネーションボリュームにレプリケートし、そのデスティネーションボリュームを SnapMirror で別のデスティネーションボリュームにレプリケートする SnapMirror 関係のカス

ケードを、 SRM ではサポートしていません。次の図に示すシナリオでは、 SRM を使用してサイト間のフェイルオーバーを実行することはできません。



SnapMirror と SnapVault

NetApp SnapVault ソフトウェアを使用すると、ネットアップストレージシステム間でエンタープライズデータをディスクベースでバックアップできます。SnapVault と SnapMirror は同じ環境内に共存できますが、SRM でサポートされているのは、 SnapMirror 関係のフェイルオーバーだけです。

NetApp SRAは、 `mirror-vault` ポリシータイプ。

SnapVault は ONTAP 8.2 で一から再構築されました。以前の Data ONTAP 7-Mode で使用されていたユーザは共通点に注意する必要がありましたが、このバージョンの SnapVault では主に拡張機能が追加されています。大きな進歩の 1 つは、 SnapVault 転送時にプライマリデータの Storage Efficiency を維持できることです。

アーキテクチャの重要な変更点は、 7-Mode SnapVault の場合と同様に、 ONTAP 9 の SnapVault でも qtree レベルではなくボリュームレベルでレプリケートされる点です。つまり、 SnapVault 関係のソースはボリュームでなければならず、そのボリュームは SnapVault セカンダリシステム上の独自のボリュームにレプリケートされる必要があります。

SnapVaultを使用する環境では、プライマリストレージシステム上に特別な名前のスナップショットが作成されます。実装されている構成に応じて、SnapVaultスケジュールまたはNetApp Active IQ Unified Managerなどのアプリケーションを使用して、名前付きSnapshotをプライマリシステムに作成できます。プライマリシステムで作成された名前付きSnapshotがSnapMirrorデスティネーションにレプリケートされ、そこからSnapVaultデスティネーションに保存されます。

ソースボリュームは、ボリュームが DR サイトの SnapMirror デスティネーションにレプリケートされるカスケード構成で作成でき、そこから SnapVault デスティネーションに保存されます。ファンアウト関係では、一方のデスティネーションが SnapMirror デスティネーション、もう一方が SnapVault デスティネーションであるソースボリュームも作成できます。ただし、 SRM フェイルオーバーまたはレプリケーションの反転時に、

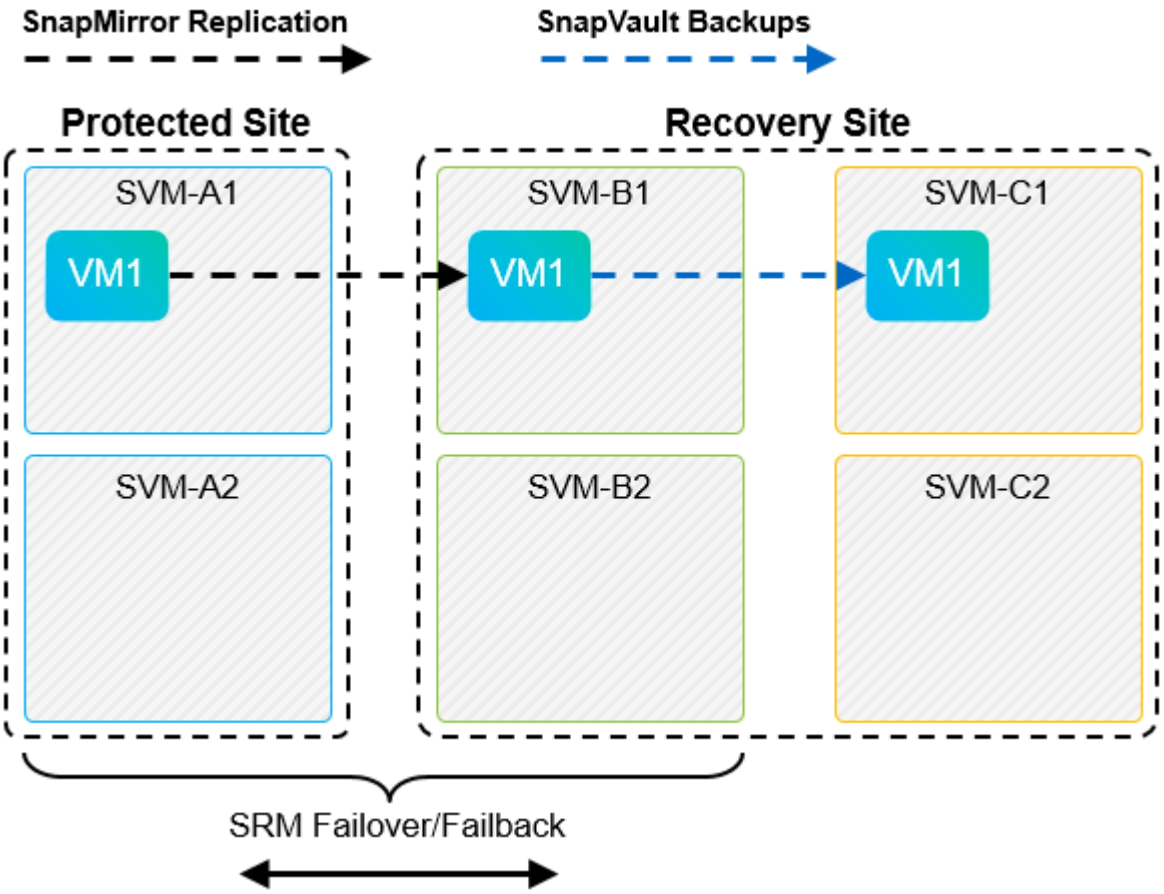
SRA は、 SnapMirror デスティネーションボリュームを SnapVault のソースとして使用するように SnapVault 関係を自動では再設定しません。

SnapMirror および SnapVault for ONTAP 9 の最新情報については、を参照してください "TR-4015 ： 『 SnapMirror Configuration Best Practice Guide for ONTAP 9 』"

ベストプラクティス
SnapVault と SRM を同じ環境で使用する場合、通常は DR サイトの SnapMirror デスティネーションから SnapVault バックアップを実行する、 SnapMirror から SnapVault へのカスケード構成を使用することを推奨します。災害が発生すると、この構成によってプライマリサイトにアクセスできなくなります。リカバリサイトに SnapVault デスティネーションを配置すると、フェイルオーバー後に SnapVault バックアップを再設定して、リカバリサイトで SnapVault バックアップを継続できるようになります。

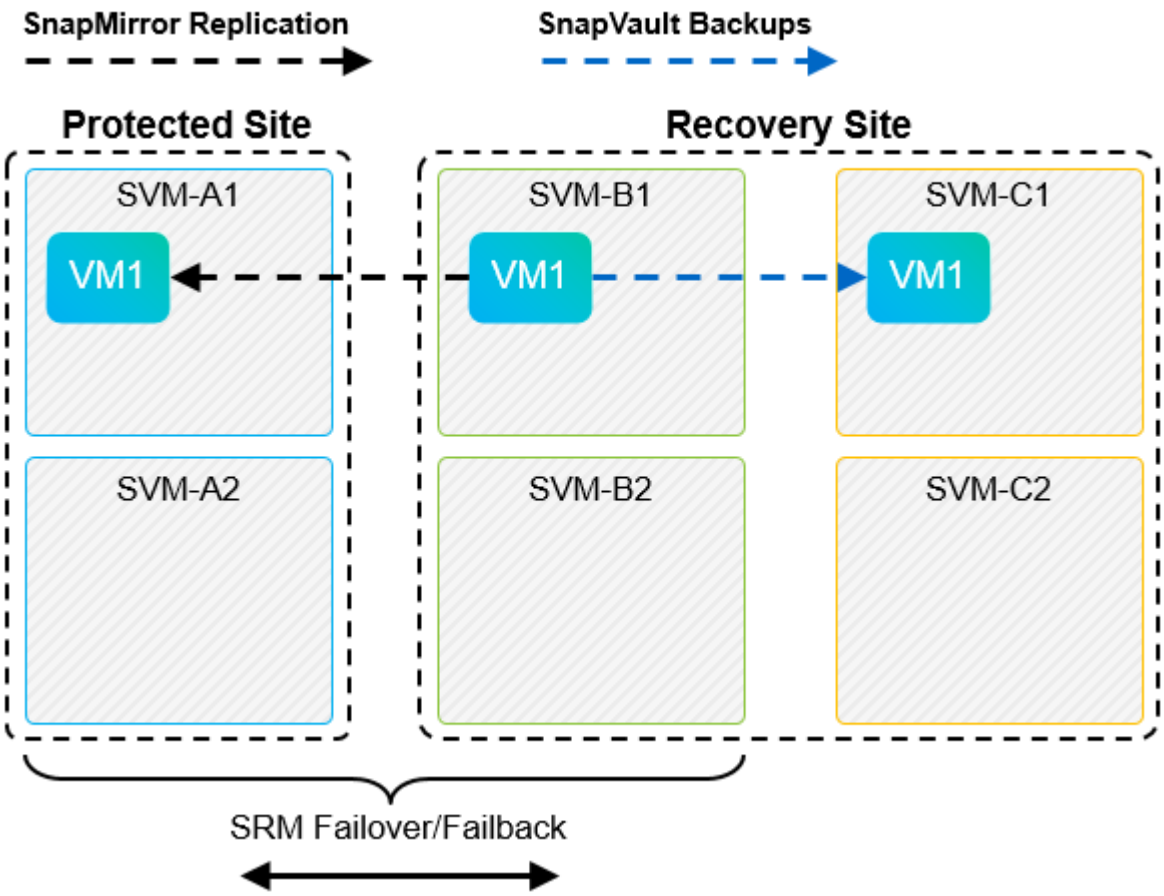
VMware 環境では、各データストアに Universal Unique Identifier （ UUID ）が割り当てられ、各 VM には一意の Managed Object ID （ MOID ）が割り当てられます。SRM は、フェイルオーバーやフェイルバックの実行時にこれらの ID を維持しません。SRM はフェイルオーバーでデータストア UUID と VM MOID を維持しないため、これらの ID に依存するアプリケーションは SRM フェイルオーバーのあとに再設定する必要があります。たとえば、 SnapVault レプリケーションを vSphere 環境と調整する NetApp Active IQ Unified Manager などがあります。

次の図に、 SnapMirror から SnapVault へのカスケード構成を示します。SnapVault デスティネーションがプライマリサイトの停止の影響を受けない DR サイトまたは第 3 のサイトにある場合、フェイルオーバー後にバックアップを続行できるように環境を再設定できます。



次の図は、 SRM を使用して SnapMirror レプリケーションをプライマリサイトに反転したあとの構成を示しています。SnapMirror ソースから SnapVault バックアップが実行されるように環境が再設定されている。こ

のセットアップは、 SnapMirror SnapVault のファンアウト構成です。



SRM でフェイルバックを実行し、 SnapMirror 関係が再度反転されると、本番環境のデータはプライマリサイトに戻ります。SnapMirror と SnapVault のバックアップにより、 DR サイトへのフェイルオーバー前と同じ方法でこのデータを保護できるようになりました。

Site Recovery Manager 環境での qtree の使用

qtree は、 NAS のファイルシステムクォータを適用可能な特殊なディレクトリです。ONTAP 9 では qtree を作成でき、 SnapMirror でレプリケートされたボリュームに配置できます。ただし、 SnapMirror では、個々の qtree のレプリケーションまたは qtree レベルのレプリケーションは実行できません。すべての SnapMirror レプリケーションは、ボリュームレベルで実行されます。このため、 SRM で qtree を使用することは推奨されません。

FC と iSCSI の混在環境

サポート対象の SAN プロトコル（ FC 、 FCoE 、 iSCSI ）の場合、 ONTAP 9 は LUN サービスを提供します。 LUN サービスの提供とは、 LUN を作成して、接続されているホストにマッピングする機能です。クラスタは複数のコントローラで構成されるため、個々の LUN へのマルチパス I/O で管理される論理パスが複数あります。ホスト上で Asymmetric Logical Unit Access （ ALUA ；非対称論理ユニットアクセス）が使用されるため、 LUN への最適なパスが選択され、データ転送用にアクティブになります。LUN への最適パスが変わった場合（格納先ボリュームが移動された場合など）、 ONTAP 9 は自動的にこの変更を認識し、システムを停止することなく調整します。最適パスが利用できなくなった場合、 ONTAP は無停止で他の利用可能なパスに切り替えることができます。

VMware SRM と NetApp SRA の環境では、一方のサイトで FC プロトコルを使用し、もう一方のサイトで

iSCSI プロトコルを使用できます。ただし、 FC 接続のデータストアと iSCSI 接続のデータストアを同じ ESXi ホストで混在させたり、同じクラスタ内の別のホストで使用したりすることはできません。この構成は SRM ではサポートされていません。 SRM フェイルオーバーまたはテストフェイルオーバーの実行中、 SRM は要求に応じて ESXi ホストのすべての FC イニシエータと iSCSI イニシエータを含めます。

ベストプラクティス
SRM と SRA では、保護サイトとリカバリサイト間での FC プロトコルと iSCSI プロトコルの混在をサポートしています。ただし、各サイトで FC または iSCSI のどちらかのプロトコルを 1 つだけ使用し、同じサイトで両方のプロトコルを使用することはできません。1 つのサイトに FC プロトコルと iSCSI プロトコル両方を設定する必要がある場合、一部のホストで iSCSI を使用し、他のホストで FC を使用することを推奨します。また、 VM がどちらか一方のホストグループまたは他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されるように、 SRM リソースマッピングを設定することも推奨します。

VVol レプリケーションを使用する場合の SRM のトラブルシューティング

SRM で VVOL レプリケーションを使用する場合、 SRA と従来のデータストアで使用するワークフローは大きく異なります。たとえば、アレイマネージャの概念はありません。そのため、 `discoverarrays` および `discoverdevices` コマンドは表示されません。

トラブルシューティングを行う場合は、以下に示す新しいワークフローについて理解しておくと役立ちます。

1. queryReplicationPeer ： 2 つのフォールトドメイン間のレプリケーション契約を検出します。
2. queryFaultDomain ：障害ドメインの階層を検出します。
3. queryReplicationGroup ：ソースドメインまたはターゲットドメインに存在するレプリケーショングループを検出します。
4. syncReplicationGroup ：ソースとターゲット間でデータを同期します。
5. queryPointInTimeReplica ：ターゲット上のポイントインタイムレプリカを検出します。
6. testFailoverReplicationGroupStart ：テストフェイルオーバーを開始します。
7. testFailoverReplicationGroupStop ：テストフェイルオーバーを終了します。
8. promoteReplicationGroup ：テスト中のグループを本番環境に昇格します。
9. prepareFailoverReplicationGroup ：災害復旧の準備をします。
10. FailoverReplicationGroup ：ディザスタリカバリを実行します。
11. revertReplicateGroup ：逆方向のレプリケーションを開始します。
12. queryMatchingContainer: 指定されたポリシーを使用したプロビジョニング要求を満たす可能性のあるコンテナを（ホストまたはレプリケーショングループとともに）検索します。
13. queryResourceMetadata ： VASA Provider からすべてのリソースのメタデータを検出し、リソース利用率を回答として queryMatchingContainer 関数に返すことができます。

VVOL レプリケーションの設定時に表示される最も一般的なエラーは、 SnapMirror 関係を検出できないエラーです。これは、ボリュームおよび SnapMirror 関係が ONTAP ツールを対象としたものではないためです。そのため、 SnapMirror 関係が常に完全に初期化されていることを確認し、レプリケートされた VVOL データストアを作成する前に両方のサイトの ONTAP ツールで再検出を実行することを推奨します。

追加情報

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- TR-4597 ：『 VMware vSphere for ONTAP 』
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400 ：『 VMware vSphere Virtual Volumes with ONTAP 』
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- TR-4015 ：『 SnapMirror Configuration Best Practice Guide for ONTAP 9 』
https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- RBAC User Creator for ONTAP の略
"https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- VMware vSphere リソース用の ONTAP ツール
"https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- VMware Site Recovery Manager のドキュメント
"https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

を参照してください "Interoperability Matrix Tool （ IMT ）" NetApp Support Siteで、本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかを確認してください。NetApp IMT には、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

著作権に関する情報

商標に関する情報