



VMware Site Recovery ManagerとONTAP

Enterprise applications

NetApp
February 10, 2026

This PDF was generated from <https://docs.netapp.com/ja-jp/ontap-apps-dbs/vmware/vmware-srm-overview.html> on February 10, 2026. Always check docs.netapp.com for the latest.

目次

VMware Site Recovery Manager と ONTAP	1
ONTAP を使用した VMware ライブサイトリカバリ	1
VLSR または SRM で ONTAP を使用する理由	1
VLSR での ONTAP 9 の活用方法	2
VLSR と ONTAP などのユースケース：ハイブリッドクラウドと移行	2
導入のベストプラクティス	3
最新バージョンの ONTAP tools を使用する	3
SMT の SVM のレイアウトとセグメント化	3
ONTAP 9 システムの管理に関するベストプラクティス	3
運用上のベストプラクティス	4
データストアおよびプロトコル	4
アレイペアについて	5
複製グループについて	6
保護グループについて	6
リカバリ・プランについて	6
テストフェイルオーバー	7
フェイルオーバーに関する考慮事項	7
再保護	7
フェイルバック	8
元のサイトを再保護する	8
レプリケーショントポロジ	8
サポートされる SnapMirror レイアウト	8
SnapMirror Active Sync による VMFS サポート	10
サポートされている Array Manager レイアウト	11
サポートされないレイアウトです	12
SnapMirror カスケード	13
SnapMirror と SnapVault	14
Site Recovery Manager 環境での qtree の使用	16
FC と iSCSI の混在環境	16
vVol レプリケーション使用時の VLSRM / SRM のトラブルシューティング	17
追加情報	18

VMware Site Recovery ManagerとONTAP

ONTAPを使用したVMwareライブサイトリカバリ

20年以上前に ESX が最新のデータセンターに導入されて以来、ONTAP はVMware vSphere、そして最近では Cloud Foundation の主要なストレージソリューションとなっています。NetApp は、SnapMirrorアクティブシンクなどの機能とともに、最新世代のASAAシリーズなどの革新的なシステムを継続的に導入しています。これらの進歩により、管理が簡素化され、回復力が強化され、ITインフラストラクチャの総所有コスト(TCO)が削減されます。

このドキュメントでは、VMware の業界をリードする災害復旧(DR)ソフトウェアである VMware Live Site Recovery (VLSR) (旧称 Site Recovery Manager (SRM)) のONTAPソリューションについて紹介します。これには、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するための最新の製品情報とベスト プラクティスが含まれます。



このドキュメントは、以前に公開された技術レポート _TR-4900: VMware Site Recovery Manager with ONTAP_ に代わるものです。

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 10.4 (NetApp Storage Replication Adapter[SRA]およびVASA Provider[VP]を含む) およびVMware Live Site Recovery 9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について説明します。

VLSRまたはSRMでONTAPを使用する理由

ONTAPを搭載したNetAppデータ管理プラットフォームは、VLSR で最も広く採用されているストレージソリューションの1つです。理由はたくさんあります。業界をリードするストレージ効率、マルチテナント、サービス品質の制御、スペース効率の高いスナップショットによるデータ保護、SnapMirrorによるレプリケーションを提供する、安全で高性能な統合プロトコル (NASとSANの組み合わせ) のデータ管理プラットフォームです。これらすべては、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て VMware ワークロードを保護し、豊富な自動化およびオーケストレーションツールを簡単に利用できるようにします。

アレイベースのレプリケーションにSnapMirrorを使用すると、ONTAPの最も実績があり成熟したテクノロジの1つを活用できます。SnapMirrorを使用すると、VM全体または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することで、安全で効率の高いデータ転送が可能になります。これらのブロックでも、重複排除、圧縮、コンパクト化などのスペース節約が活用されます。最新のONTAPシステムではバージョンに依存しないSnapMirrorが使用されるようになり、ソースクラスターと宛先クラスターを柔軟に選択できるようになりました。SnapMirrorは、災害復旧に利用できる最も強力なツールの1つになりました。

従来のNFS、iSCSI、またはファイバチャネル接続データストア(vVolsデータストアもサポートされるようになりました)を使用している場合でも、VLSRは、災害復旧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の機能を最大限に活用する強力なファーストパーティ製品を提供します。

VLSR での ONTAP 9 の活用方法

VLSR 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。

- ONTAP tools vCenter プラグイン（旧称 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を簡易化し、可用性を高め、ストレージコストと運用オーバーヘッドを削減します。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。NetApp では、ONTAP を実行しているシステムで vSphere を使用する際に、これらのメリットをすべて考慮してこのプラグインを推奨しています。
- ONTAP tools VASA Provider は、VMware vStorage APIs for Storage Awareness (VASA) フレームワークをサポートします。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。これにより、VMware Virtual Volumes (vVol) のサポート、VM ストレージポリシーの管理、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した。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。
- SRA は VLSR 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。SRA サーバアプライアンスと、Windows SRM サーバおよび VLSR アプライアンス用の SRA アダプタの両方が含まれています。

非 vVols データストアを保護するために VLSR サーバに SRA アダプタをインストールして構成したら、災害復旧用に vSphere 環境を構成するタスクを開始できます。

SRA は、VMware 仮想マシン (VM) を含む ONTAP FlexVol ボリュームおよびそれらを保護する SnapMirror レプリケーションを管理するための VLSR サーバ用のコマンドおよび制御インターフェイスを提供します。

VLSR は、NetApp 独自の FlexClone テクノロジーを使用して DR サイトの保護されたデータストアのクローンをほぼ瞬時に作成し、中断なく DR プランをテストできます。VLSR は、実際の災害発生時に組織と顧客が保護されるように安全にテストするためのサンドボックスを作成し、災害時に組織がフェールオーバーを実行できることに自信を持たせます。

実際に災害が発生した場合や、計画的な移行の場合でも、VLSR 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。



ONTAP システムでは SnapMirror レプリケーション用に同じクラスタ内の SVM をペアリングできますが、このシナリオのテストおよび認定は VLSR では行われていません。したがって、VLSR を使用する場合は、異なるクラスタの SVM のみを使用することを推奨します。

VLSR と ONTAP などのユースケース：ハイブリッドクラウドと移行

VLSR 展開を ONTAP の高度なデータ管理機能と統合すると、ローカルストレージ オプションと比較して、スケールとパフォーマンスが大幅に向上します。しかし、それ以上に、ハイブリッド クラウドの柔軟性がもたらされます。ハイブリッド クラウドでは、FabricPool を使用して、高性能アレイから使用されていないデータ ブロックを優先ハイパースケーラー (NetApp StorageGRID などのオンプレミスの S3 ストアなど) に階層化することでコストを節約できます。また、ソフトウェア定義の ONTAP Select またはクラウドベースの DR を備えたエッジベースのシステムにも SnapMirror を使用できます。 "Equinix Metal 上の NetApp ストレージ"、またはその他のホストされた ONTAP サービス。

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。

VLSR 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。

最新バージョンのONTAP toolsを使用する10

ONTAP tools 10では、以前のバージョンに比べて次の点が大幅に改善されています。

- ・ テストフェイルオーバーが8倍高速*
- ・ クリーンアップと再保護が2倍高速*
- ・ フェイルオーバーが32%高速*
- ・ 拡張性の向上
- ・ 共有サイトレイアウトのネイティブサポート

*これらの改善点は内部テストに基づいており、環境によって異なる場合があります。

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。

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ユーザのロールと権限の設定](#)"含まれているJSONファイルを使用します。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。

- 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マイクロサービスであるため、ONTAP tools の vCenter UI で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、最初に ONTAP tools Manager を使用して vCenter に関連付けないかぎり、NFS パスのチェックは実行されませ ["オンホオトクラスタ"](#) 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、キャッシングパス、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 を使用し、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。
- 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。これは今でもベストプラクティスですが、最新バージョンの ONTAP 9 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 で SnapMirror スナップショットが削除され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は、SANデータストアを含むボリュームの場合は `grow_shrink` に設定し、NFSデータストアの場合はに設定する必要があります `grow`。このトピックの詳細については、を"ボリュームのサイズを自動的に拡張および縮小するように設定する"参照してください。
- 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。

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。

The screenshot shows the vSphere Client interface. On the left, a sidebar menu includes 'ONTAP tools', 'Overview', 'Storage Systems' (which is selected and highlighted in blue), 'Storage Capability Profiles', 'Storage Mapping', 'Settings', and 'Reports'. The main pane is titled 'Storage Systems' and shows a table with one entry: 'cluster2' under 'Name', 'Cluster' under 'Type', and 'cluster2.demo.netapp.com' under 'IP Address'. Below this, there are 'ADD' and 'REDISCOVER ALL' buttons. A red arrow points from the 'cluster2.demo.netapp.com' text in the table to the 'cluster2.demo.netapp.com' text in the 'Storage Management IP Address or Hostname' field of the 'Edit Local Array Manager' dialog box. The dialog box also contains fields for 'Name' (containing 'vc2_array_manager') and 'Storage Array Parameters'.

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。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。しかし、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むことができるため、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、SnapMirrorではアグリゲートの重複排除が考慮されていないため、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は、アプリケーションサーバの前にオンラインである必要があるMicrosoft SQL Serverよりも先に起動する必要があります。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した場合は、必ずテストフェイルオーバーを実行することを推奨します。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とも、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。

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できます。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。

各 NetApp SVM は、Site Recovery Manager では一意のアレイとして扱われます。VLSR は、特定のアレイ間（または SVM 間）のレプリケーション レイアウトをサポートします。

1 つの VM が、次の理由から、複数の VLSR 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。

- VLSR 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。VLSR 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、VLSR 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 VLSR アレイ（SVM）上のデータのみを所有します。

SnapMirror Replication



Protected Site

SVM-A1

VM1

Recovery Site

SVM-B1

VM1

SVM-A2

VM2

SVM-B2

VM2

SnapMirror Replication



Protected Site

SVM-A1

VM2

VM1

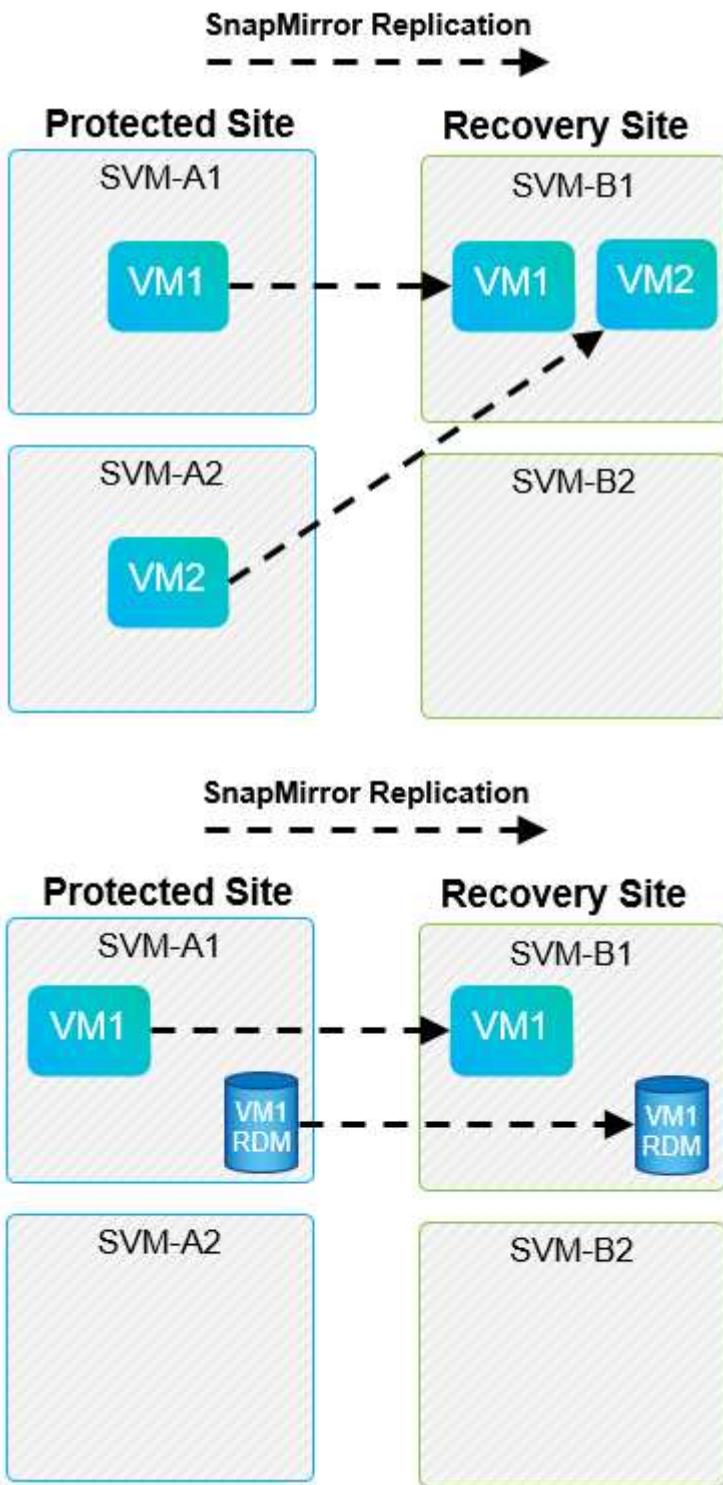
Recovery Site

SVM-B1

VM1

SVM-B2

VM2



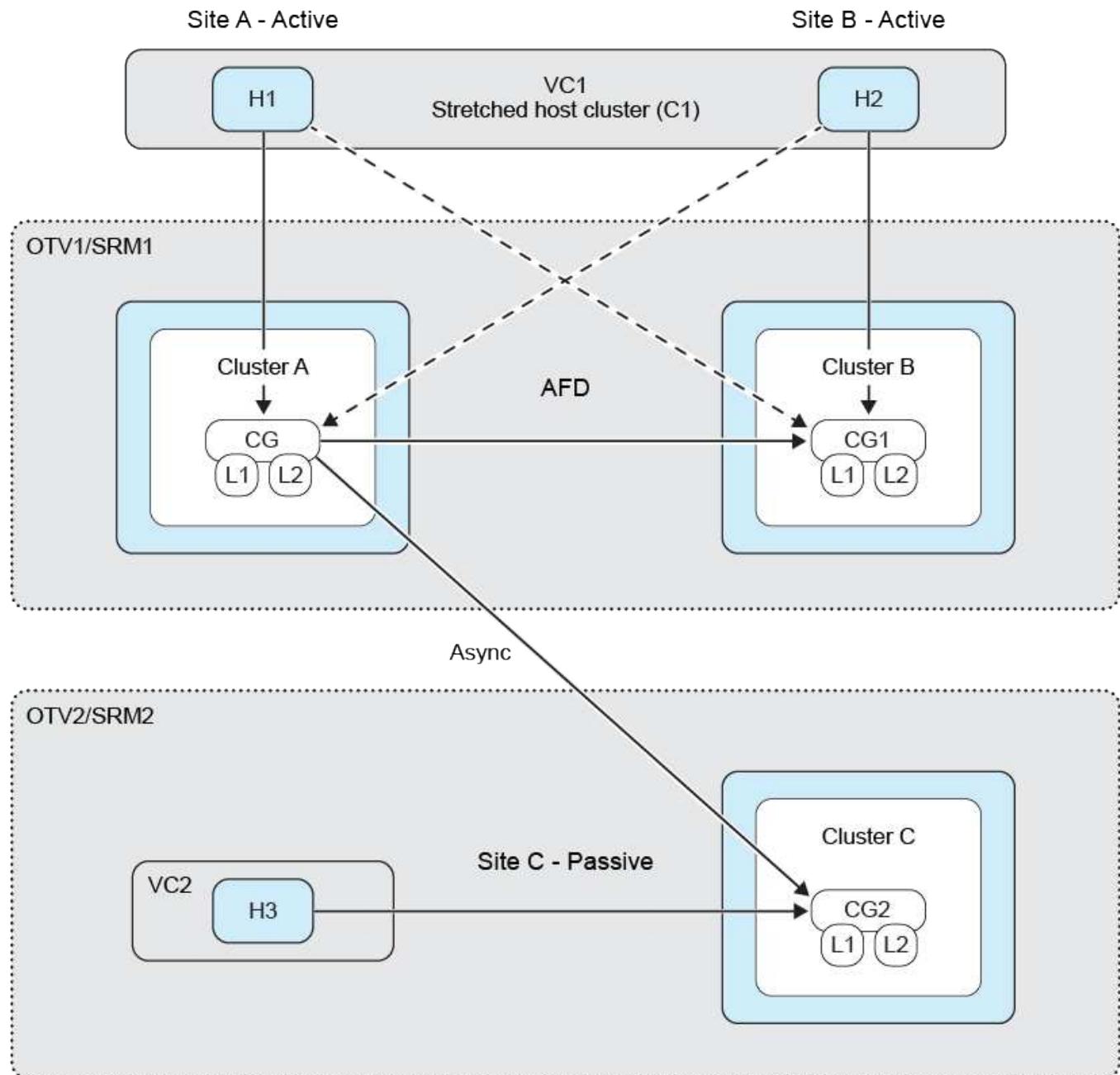
SnapMirror Active Sync による VMFS サポート

ONTAPツール 10.3 以降では、SnapMirror Active Sync (SMAs) を使用した VMFS データストアの保護もサポートされています。これにより、比較的近接する 2 つのデータセンター (障害ドメインと呼ばれる) 間でのビジネス継続性のための透過的なフェイルオーバーが可能になります。その後、ONTAPツール SRA と VLSR を介してSnapMirror非同期を使用して、長距離災害復旧を調整できます。

["ONTAP SnapMirrorアクティブ同期について学ぶ"](#)

データストアは整合性グループ (CG) に集められ、すべてのデータストアにわたる VM は同じ CG のメンバーとして書き込み順序の一貫性を維持します。

たとえば、ベルリンとハンブルクのサイトを SMas で保護し、3 番目のサイトのレプリカを SnapMirror 非同期を使用して VLSR で保護することが考えられます。もう 1 つの例としては、SMas を使用してニューヨークとニュージャージーのサイトを保護し、3 番目のサイトをシカゴに置くことが挙げられます。



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、VLSR 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`、`SVM2`、リカバリサイトである `SVM4` のピア関係が設定されて `SVM3` です。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

アは2つのうちの1つだけです。

New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Type

Select the type of protection group you want to create:

Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

Storage policies (array-based replication)
Protect virtual machines with specific storage policies.

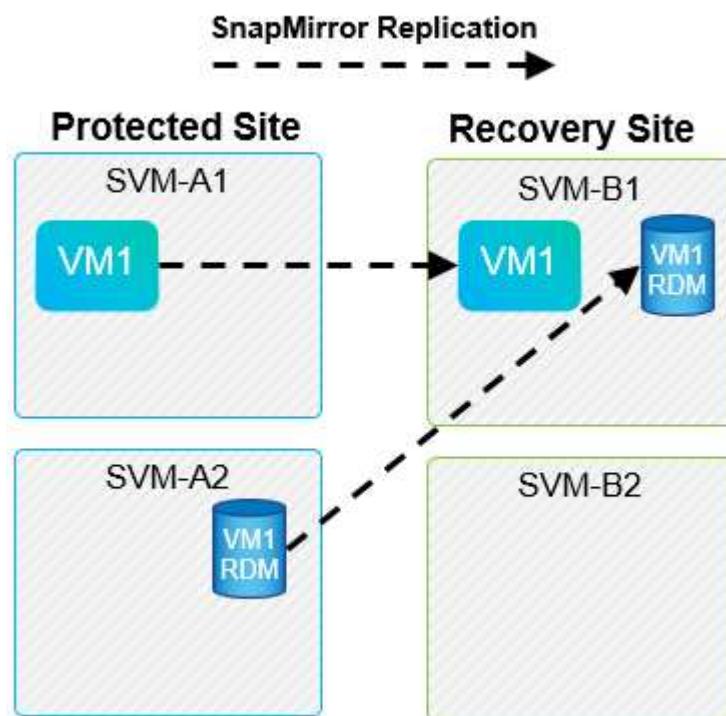
Select array pair

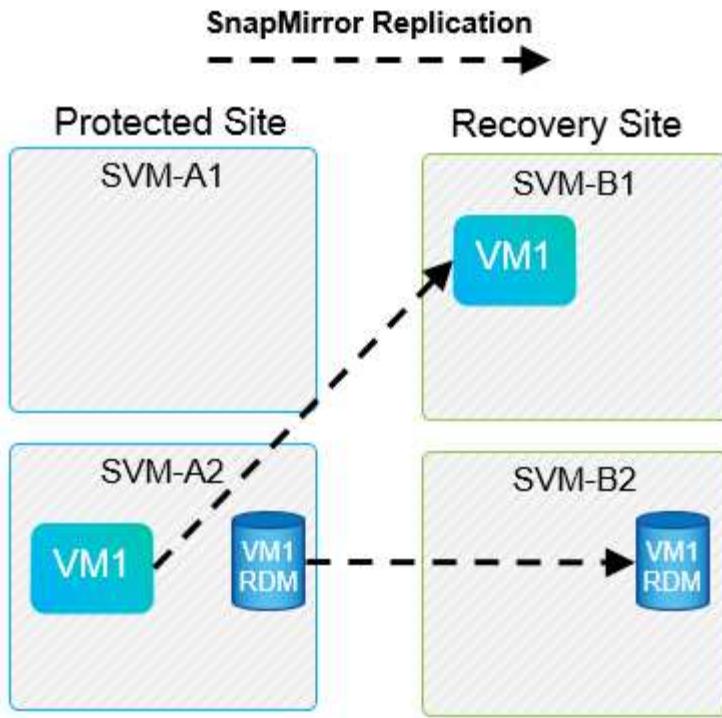
Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

CANCEL BACK NEXT

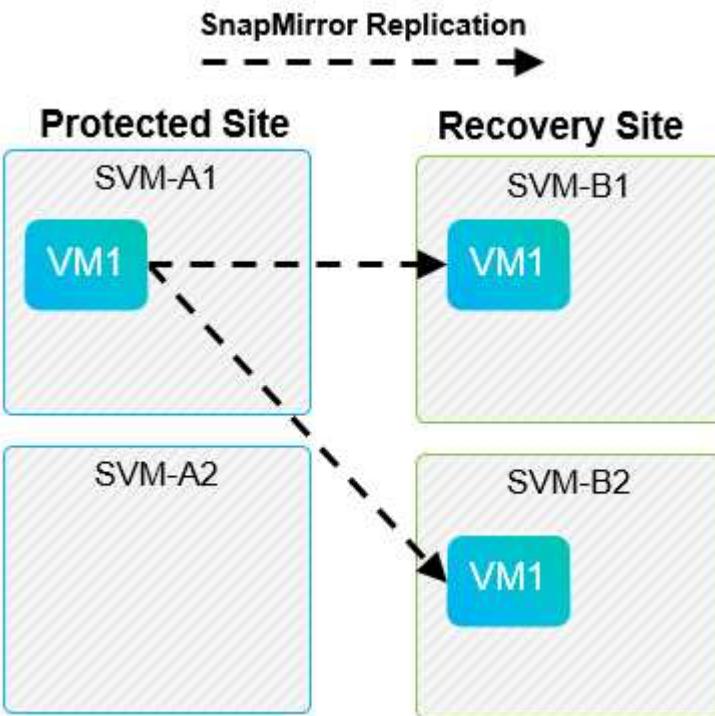
サポートされないレイアウトです

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。次の図の例では、が2つのSVM上にあるため、を VM1 `VLSRで保護するように設定することはできません。





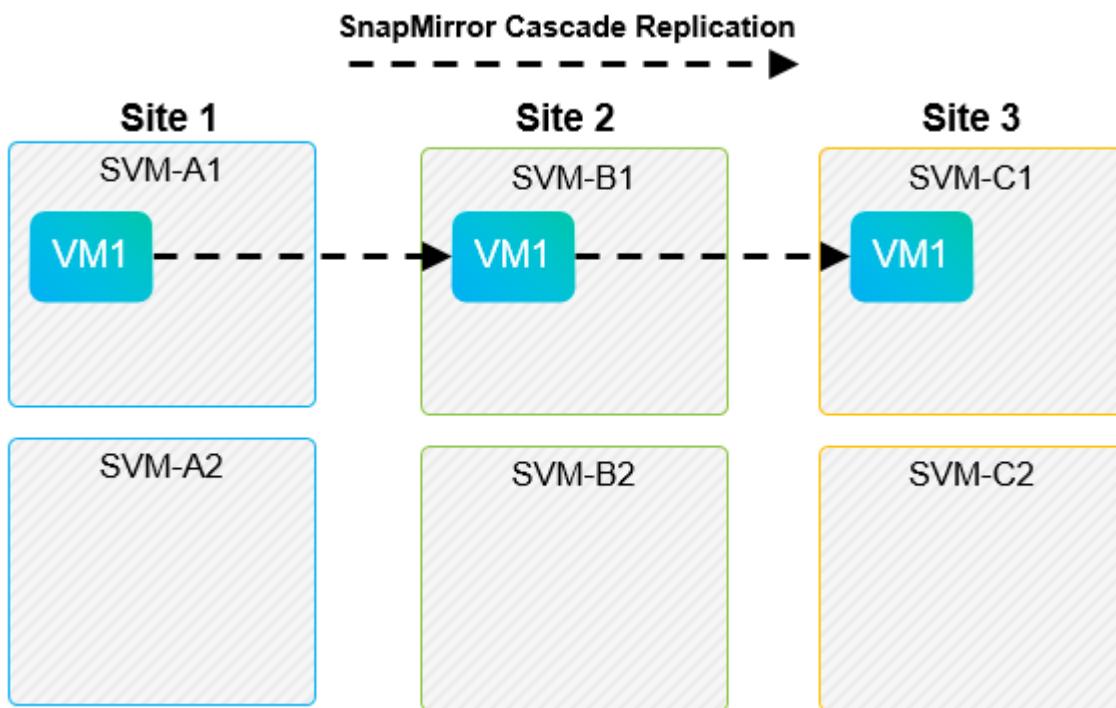
1つのネットアップボリュームを1つのソース SVM から同じ SVM または異なる SVM の複数のデスティネーションにレプリケートするレプリケーション関係は、SnapMirror ファンアウトと呼ばれます。VLSR ではファンアウトはサポートされていません。次の図の例では、`VM1` SnapMirror を使用して2つの異なる場所にレプリケートされるため、VLSR で保護を設定できません。



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、VLSR ではサポートしていません。次の図に示すシナリオでは、VLSR 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、VLSR 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、VLSR 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。

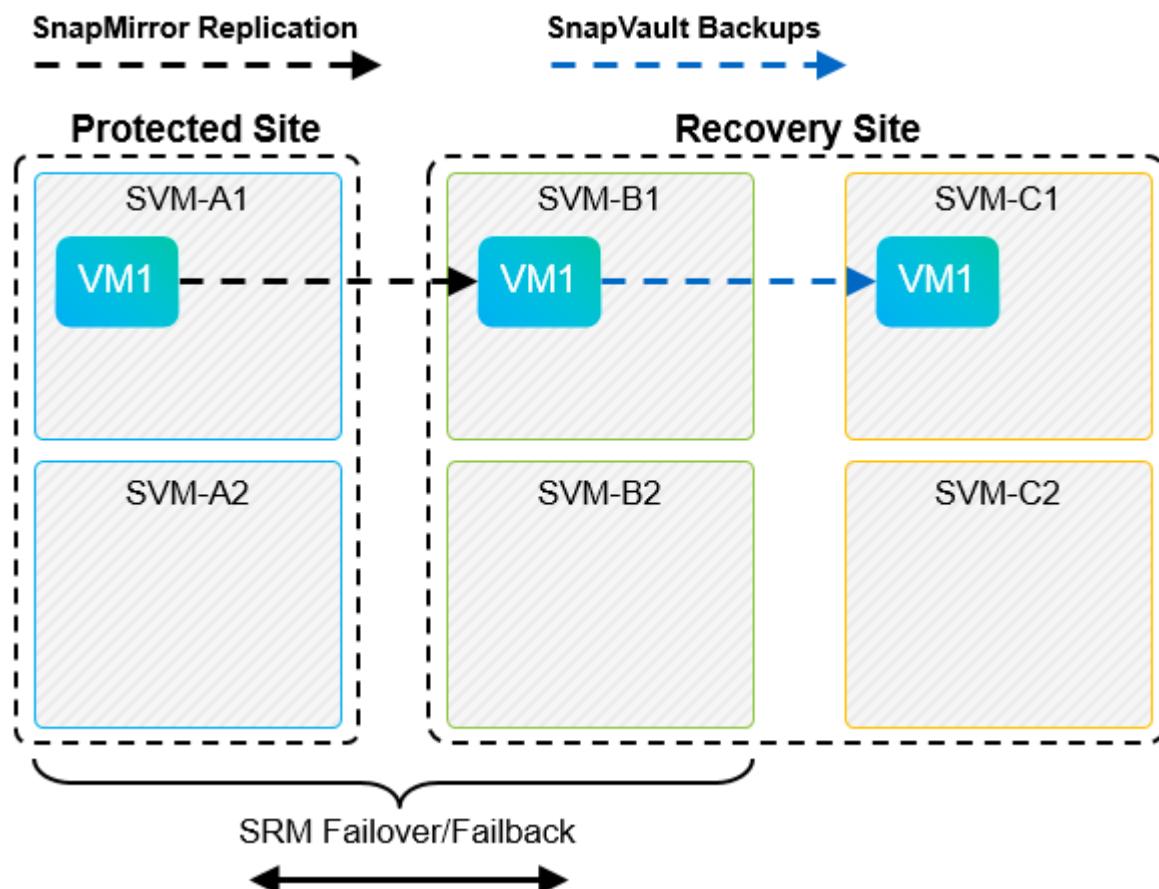
ONTAP 9のSnapMirrorとSnapVaultの最新情報については、以下を参照してください。『[TR-4015 : 『SnapMirror Configuration Best Practice Guide for ONTAP 9』](#)』

ベストプラクティス

SnapVault と VLSR 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。

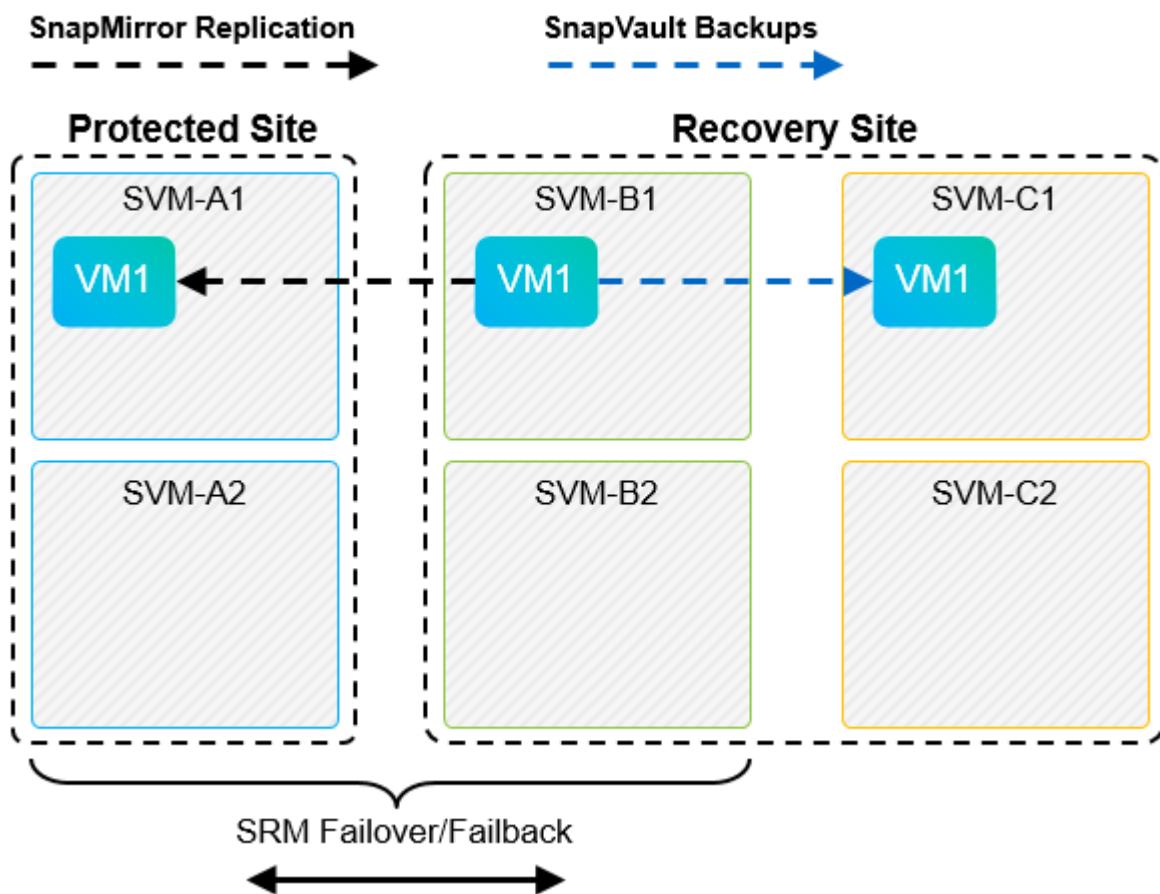
VMware 環境では、各データストアに Universal Unique Identifier (UUID) が割り当てられ、各 VM には一意の Managed Object ID (MOID) が割り当てられます。VLSR は、フェイルオーバーやフェイルバックの実行時にこれらの ID を維持しません。VLSR はフェイルオーバーでデータストア UUID と VM MOID を維持しないため、これらの ID に依存するアプリケーションは VLSR フェイルオーバーのあとに再設定する必要があります。たとえば、SnapVault レプリケーションを vSphere 環境と調整する NetApp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



VSRMがフェイルバックおよびSnapMirror関係の2回目の反転を実行すると、本番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オータを適用できる特別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、のSnapMirrorでは、個々のqtreeのレプリケーションや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、VLSR 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 VLSR 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 VLSR ではサポートされていません。VLSR 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、VLSR 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

VLSR 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、VLSR リソースマッピングを設定することも推奨します。

vVolレプリケーション使用時のVLSRM / SRMのトラブルシューティング

ONTAP tools 9.13P2を使用している場合、vVolレプリケーションを使用している場合は、SRAおよび従来のデータストアで使用される場合とは、VLSRおよびSRMでのワークフローが大きく異なります。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`コマンドや`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。

- ONTAP Tools for VMware vSphere 10.x のリソース "<https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab>"
- ONTAP Tools for VMware vSphere 9.x のリソース "<https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab>"
- 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 ONTAP 9 向け SnapMirror 構成ベストプラクティスガイド <https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- VMware Live Site Recovery のドキュメント "<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html>"

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については、NetAppサポートサイトのを参照して "[Interoperability Matrix Tool \(IMT\)](#)" ください。NetApp IMTでは、NetAppでサポートされ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と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

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隨時、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 5225.227-19（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権を有し、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権については、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。