



テクニカル レポート

SnapMirror[®] ビジネス継続性 (SM-BC) ONTAP 9.12.1

NetApp
Stephen Galla
2022年11月 | TR-4878

概要

NetApp[®] SnapMirror[®] ビジネス継続性 (SM-BC) は、アプリケーションレベルのきめ細かさを備えた継続的可用性を備えたストレージ解決策で、NetApp AFFまたはNetAppオールSANアレイ (ASA) ストレージシステムで実行されるNetApp ONTAP[®]で利用できます。最も重要なビジネスアプリケーションのRPO 0とRTO 0のニーズを満たすため。

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

目次

エグゼクティブサマリー	4
解決策の概要	4
メリット.....	5
主な用語と概念.....	5
アーキテクチャ	6
ユースケース.....	7
アプリケーションの設定	9
アプリケーションホスト.....	9
プロトコル	9
ホスト接続.....	9
ホストアクセスタイプ	9
マルチパス.....	9
データレイアウト	10
ビジネス継続性のための保護の設定	11
前提条件.....	11
ONTAPメディアエーターのインストール.....	13
ONTAPメディアエーターの設定	13
ビジネス継続性のための保護.....	14
問題.....	17
解決策	17
フェイルオーバー手順.....	17
計画的フェイルオーバー.....	18
整合グループへのボリュームの追加と削除	20
Single File SnapRestore	20
パーシャル・シングル・ファイルSnapRestore	21
既存のSnapMirror Synchronous関係を変換してビジネス継続性を確保.....	21
SM-BC関係があるONTAPバージョンのアップグレードとリバート.....	21
トラブルシューティング	21
追加情報の入手方法.....	21
バージョン履歴.....	21

図一覧

図1) ビジネス継続性とは.....	4
図2) SM-BC解決策.....	5
図3) SM-BCのアーキテクチャ.....	7
図4) SM-BCでALUAパスを使用.....	8
図5) 災害発生時に変更されたALUAパス.....	9
図6) ALUAを使用するSM-BC.....	10
図7) エンタープライズアプリケーション向けSVM内のデータレイアウト.....	11
図8) Caution/MustRead文.....	13
図9) ファンアウトトポロジ.....	19

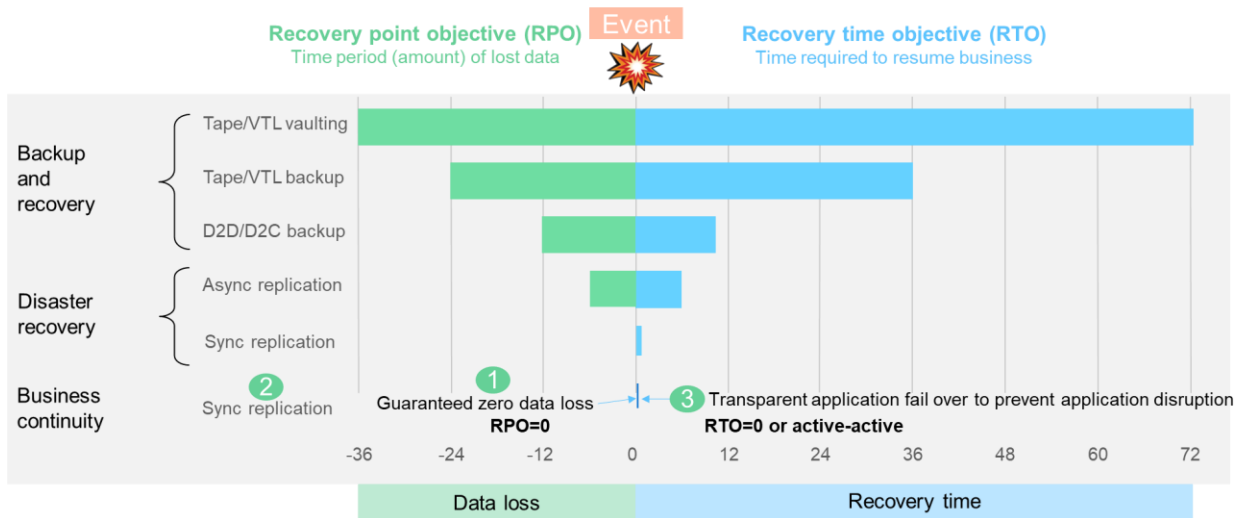
エグゼクティブ サマリー

絶えず接続されている今日のグローバルなビジネス環境では、サイバー攻撃、停電、自然災害による機器の障害などのシステム停止後に、ビジネスクリティカルなアプリケーションデータをデータ損失ゼロで迅速にリカバリしたいと考えています。特に、金融機関はデータ損失やアプリケーションの使用不能を一切許容しないため、一般データ保護規則（GDPR）やその他の規制要件を遵守する必要があります。図1は、ビジネス継続性の高レベル概要を示しています。

図1) ビジネス継続性とは

What is business continuity?

Ability for application to fail over to secondary copy in storage, without application reconnect or user disruption



組織は、次の要件を優先的に考慮して、効果的なビジネス継続性およびディザスタリカバリ（BCDR）計画を策定できます。

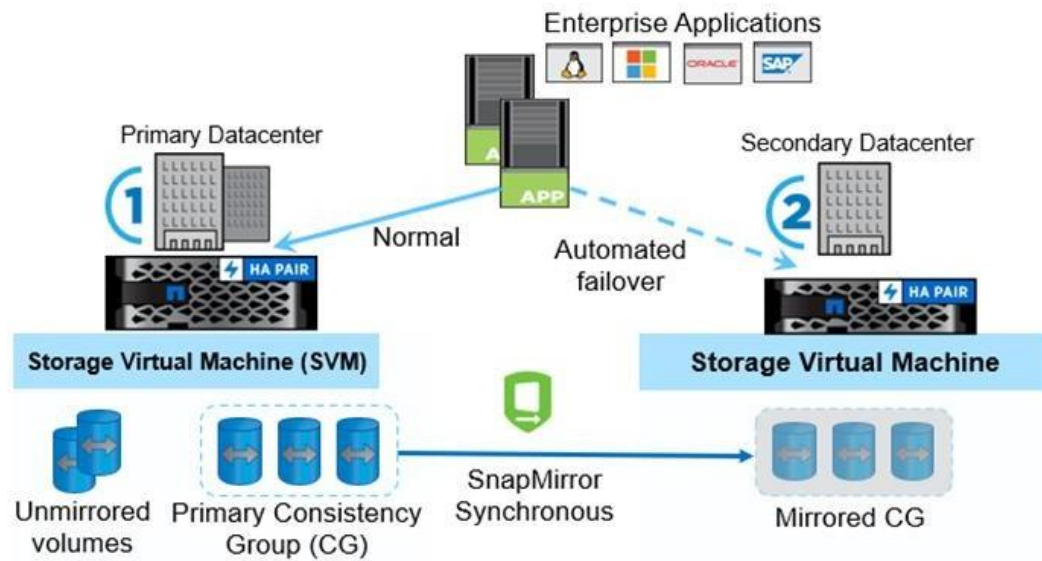
- ゼロ目標復旧時点（RPO）：同期レプリケーションによってデータ損失ゼロを達成
- 透過的アプリケーションフェイルオーバー（TAF）による目標復旧時間（RTO）ゼロ。災害発生時にビジネスクリティカルなアプリケーションの停止を防止

ONTAP 9.8で導入されたNetApp SM-BCは、ゼロRPOとほぼゼロRTOを実現する新しいビジネス継続性解決策です。SM-BCは、使いやすいアプリケーションレベルのきめ細かさや自動フェイルオーバー機能を備えた柔軟性を提供します。SM-BCでは、実績のあるIPネットワーク経由のSnapMirror Synchronous（SM-S）レプリケーションを使用して、LANまたはWAN経由でデータを高速でレプリケートします。仮想環境と物理環境の両方で、Oracleや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データ可用性を高め、データレプリケーションを高速化します。SM-BCを使用すると、TAFを使用してセカンダリコピーを作成し、サイト全体に障害が発生してもミッションクリティカルなビジネスサービスの運用を継続できます。このフェイルオーバーをトリガーするための手動操作や追加のスクリプト作成は必要ありません。

ソリューションの概要

SM-BCを使用すると、データLUNを保護できます。これにより、災害発生時にビジネス継続性を確保するために、アプリケーションを透過的にフェイルオーバーできます。図2はSM-BC解決策の図です。

図2) SM-BC解決策



SM-BCの主な機能は次のとおりです。

- SANアプリケーション（iSCSIまたはFC）のビジネス継続性と、地理的に離れた2つの場所での保護
- Oracle、Microsoft SQL Server、VMware vSphere Metro Storage Cluster（vMSC）解決策などのエンタープライズアプリケーション向けTAF。手動操作なし（ストレージへの再接続やアプリケーションユーザへの中断なし）
- 整合グループ（CG）は、アプリケーションデータ用の一連のボリュームについて、従属書き込み順序の整合性を維持します。
- ONTAPとの緊密な統合により、堅牢なNetAppテクノロジーを活用し、拡張性に優れたエンタープライズレベルのデータ保護を実現
- ストレージプロビジョニング、ホスト接続、両方のサイトでのNetApp Snapshot™ コピーとクローンの作成に関するデータ管理の簡素化

ビジネス上の主な利点

SM-BCには次のようなメリットがあります。

- きめ細かなアプリケーションでビジネス継続性を実現
- 自動フェイルオーバー：各アプリケーションのフェイルオーバーを評価
- LUN IDは変更されないため、アプリケーションはLUN IDを共有仮想デバイスとして認識
- セカンダリを柔軟に再利用できるため、アプリケーションのパフォーマンスや可用性に影響を与えることなく、開発/テスト、UAT、レポート作成の目的でアプリケーションに使用するクローンを瞬時に作成できます。
- 整合グループを使用して従属書き込み順序の整合性を維持し、アプリケーション管理を簡易化

主な用語と概念

ONTAP SM-BC解決策の詳細を確認し、導入を計画するにあたっては、主な用語と概念を理解しておくことが重要です。

SM-BCの略。 ONTAP 9.8以降で使用可能なソリューション、SnapMirror Business Continuity（SnapMirrorビジネス継続性）の略語。

Consistency Group (CG ; 整合グループ) の略。CGは複数のボリュームを格納するコンテナであり、Snapshotイメージの作成、スケジュール設定、ロールバックなどの処理を実行できます。たとえば、ホストでアプリケーションデータが複数のボリュームに分散している場合（たとえば、複数のVMディスクファイルを持つ仮想マシン[VM]や、データ、ログ、その他のファイルを分離したデータベースサーバなど）、保護およびレプリケートされたデータのスナップショットの整合性を確保することが重要になります。CGはNetApp FlexVol®ボリュームの集まりであり、ビジネス継続性のために保護する必要があるアプリケーションワークロードの整合性を保証します。CGの目的は、複数のボリュームのSnapshotイメージを同時に作成し、特定の時点（PIT）で一連のボリュームのcrash-consistentコピーを作成することです。CGを使用すると、データセットのすべてのボリュームが休止され、正確に同じピットにスナップされます。これにより、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提供されます。これにより、CGは従属書き込み順序の整合性を維持します。アプリケーションをビジネス継続性のために保護する場合は、このアプリケーションに対応するボリュームグループをCGに追加してから、ソースCGとデスティネーションCGの間にデータ保護関係を確立する必要があります。ソースとデスティネーションのCGには、同じ数とタイプのボリュームが含まれる必要があります。

構成要素 : CGに属する個々のFlexVol。

RPOゼロ。 目標復旧時点（RPO）ゼロ。災害やシステム停止からデータ損失なしでリカバリできます。

RTOゼロ。 ホストのマルチパスI/O（MPIO）を使用してストレージへの無停止アクセスを実現する、目標復旧時間（TAF）ゼロ。

Transparent Application Failover (TAF ; 透過的アプリケーションフェイルオーバー)。 アプリケーションに依存せずにオンサイトのストレージを停止できる機能。サイト障害やストレージの停止後に再設定する必要はありません。つまり、サイト障害やサイトのストレージ停止が発生した場合、ホストからストレージへのアクセスは無停止で行われます。SANの場合は、ホストMPIOを使用して、ストレージフェイルオーバーをアプリケーションに対して透過的に実行する必要があります。

同期していません。 アプリケーションI/Oがセカンダリストレージシステムにレプリケートされていない状態です。SnapMirrorレプリケーションが実行されておらず、サポートされていない操作による転送の失敗または失敗を示すため、デスティネーションボリュームはソースボリュームと同期していません。

ONTAPメディエーター。 ONTAPメディエーターは、ONTAPのクラスタ/ノードがハートビート情報を定期的に報告し、ピアが稼働しているかどうかを確認するツールです。ONTAPメディエーターは次の健全性情報を提供します。

- ピアONTAPクラスタ
- ピアONTAPクラスタノード
- CG（フェイルオーバーユニット）。各CGについて、次の情報が提供されます。
 - レプリケーションの状態：Uninitialized、In Sync、またはOut of Sync
 - プライマリコピーをホストするクラスタ
 - 操作コンテキスト（計画的フェイルオーバーに使用）

このONTAPメディエーターの健全性情報を使用すると、クラスタで障害のタイプを区別し、自動フェイルオーバーを実行するかどうかを判断できます。ONTAPメディエーターは、両方のONTAPクラスタ（プライマリおよびセカンダリ）とともにSM-BCクォーラムを構成する3つのメンバーの1つです。合意に達するには、クォーラムの少なくとも2つの当事者が特定の処理に同意する必要があります。

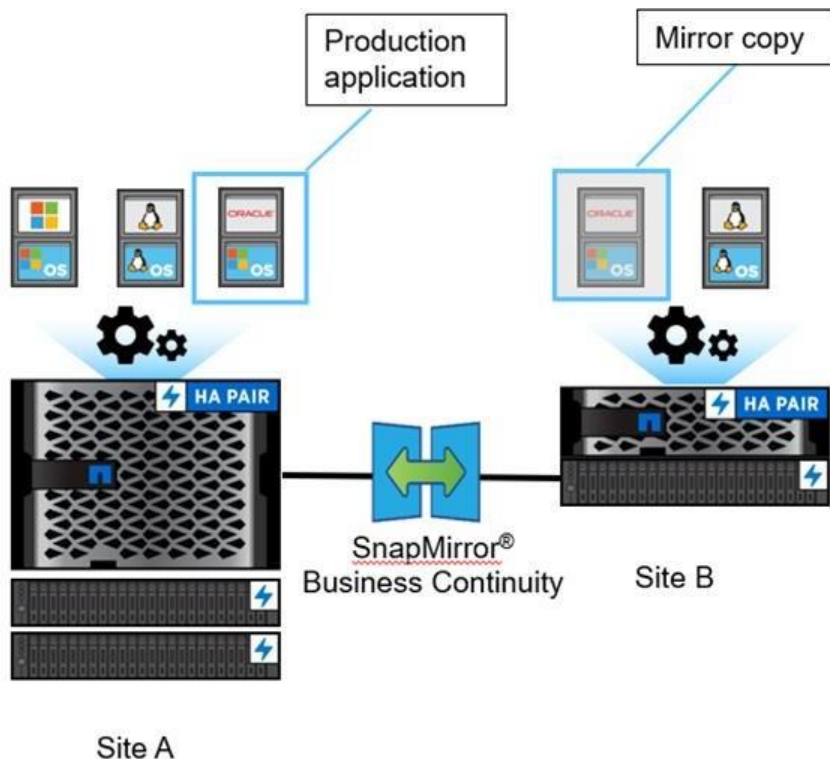
アーキテクチャ

図3は、両方のクラスタのアクティブワークロードに対応するSM-BCアーキテクチャを示しています。このアーキテクチャでは、両方のクラスタからプライマリワークロードを同時に処理できます。一部の国の金融機関の規制では、SM-BCが可能にする「Tick-Tock」導入と呼ばれるセカンダリデータセンターから定期的にサービスを提供することも義務付けられています。

ビジネス継続性を確保するためのデータ保護関係は、Storage Virtual Machine（SVM）内の異なるボリュームのアプリケーション固有のLUNを整合グループに追加することで、ソースストレージシステムとデスティネーション

ストレージシステムの間で作成されます。通常の運用では、エンタープライズアプリケーションからプライマリ整合グループに書き込みが行われ、プライマリ整合グループがこのI/Oをミラー整合グループに同期的にレプリケートします。

図3) SM-BCのアーキテクチャ



データ保護関係には2つの個別のコピーが存在しますが、SM-BCでは同じLUN IDが維持されるため、アプリケーションホストはこれを複数のパスを持つ共有仮想デバイスと見なします。ただし、一度に書き込まれるLUNコピーは1つだけです。障害が発生してプライマリストレージシステムがオフラインになると、ONTAP Mediatorによってその障害が検出され、アプリケーションがミラー整合性グループにシームレスにフェイルオーバーされます。このプロセスにより、特定のアプリケーションのみがフェイルオーバーされ、以前はフェイルオーバーのために必要だった手動操作やスクリプト作成は不要になります。

その他の考慮事項：

- ビジネス継続性を目的とした保護の対象外のミラーされていないボリュームもサポートされます。
- ビジネス継続性を目的として保護されているボリュームでは、他のSnapMirror非同期関係は1つだけサポートされます。
- ビジネス継続性を目的とした保護では、カスケードトポロジはサポートされていません。

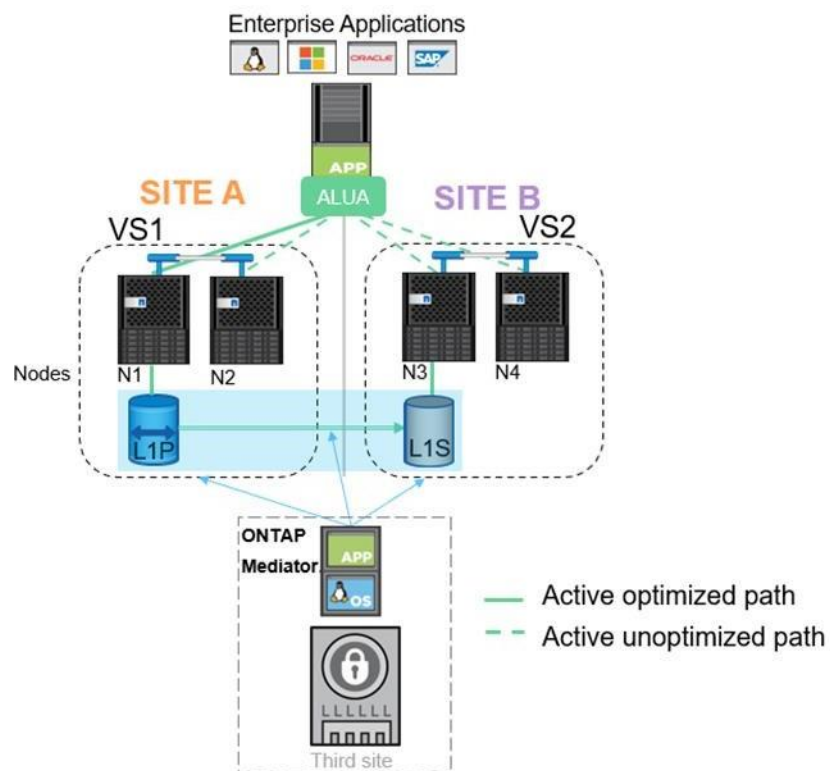
ユースケース

RTO（目標復旧時間）またはTAF（目標復旧時間）ゼロのためのアプリケーション導入

TAFは、ストレージへの無停止アクセスを実現するために、ホストの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います。プライマリ（L1P）とミラーコピー（L1S）などの両方のLUNコピーのID（シリアル番号）が同じで、読み取り/書き込み可能としてホストに報告されます。ただし、実際に読み取りと書き込みを処理するのはプライマリ ボリュームのみです。ミラー コピーへのI/Oはプライマリ コピーにプロキシされます。ホストからL1への優先パスはVS1：N1です。これは、Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）のアクセス状態がActive Optimized（A/O；アクティブ最適化）に基づいています。ONTAP Mediatorは、環境の一部として必要です。主に、プライマリでストレージが停止した

場合に（計画的または計画外の）フェイルオーバーを実行するために必要です。

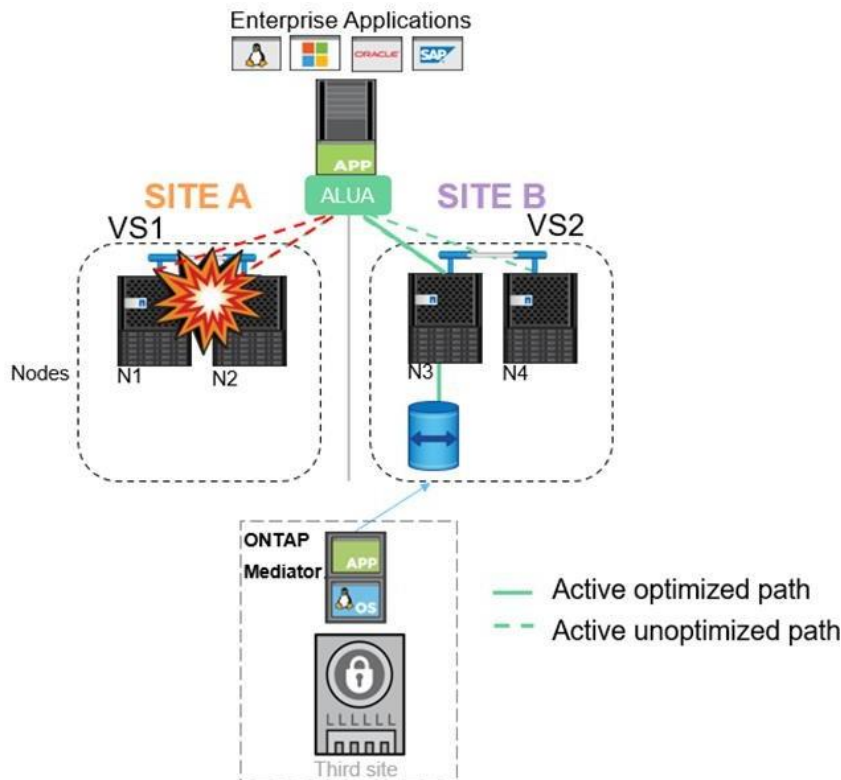
図4) SM-BCでALUAパスを使用



災害シナリオ

プライマリクラスタをホストしているサイトで災害が発生すると、ホストのマルチパスソフトウェアはクラスタを経由するすべてのパスを停止とマークし、セカンダリクラスタからのパスを使用します。その結果、ONTAP Mediatorによって無停止フェイルオーバーが有効になり、L1Sを使用するLUN L1のミラーコピーが VS2 : N3を経由するホスト優先パスを使用するアクティブコピーに変換されます。

図5) 災害発生時に変更されたALUAパス



アプリケーションの設定

アプリケーションホスト

サポートされるホストオペレーティングシステムは、スタンドアロンのMicrosoft Windows Server、スタンドアロンのRed Hat Enterprise Linux (RHEL)、およびVMware vMSCです。

プロトコル

SM-BCでは、iSCSIプロトコルとFCプロトコルを使用して、物理ホストまたはESXiホストからはディスクデバイスとして認識されるSAN環境のLUN（論理ユニット）を保護します。

ホスト接続

ホストとストレージのネットワーク接続では、FC接続またはイーサネット（iSCSI）接続のいずれかを使用できます。

ホストアクセスタイプ

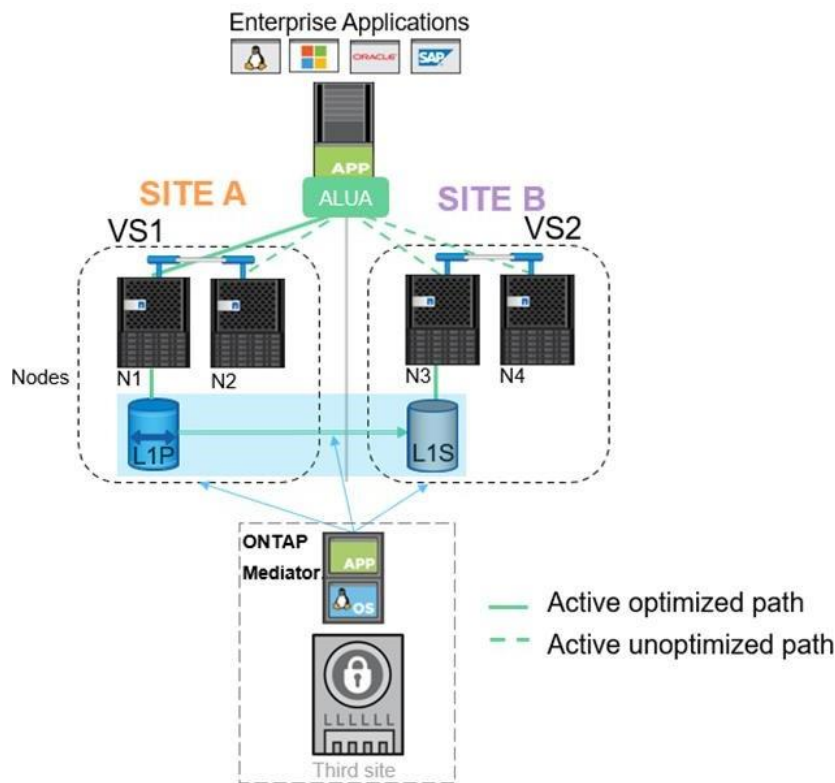
CGボリュームには、均一または非均一のSAN接続を使用して、アプリケーションホストからアクセスできます。統一されたストレージアクセス構成では、各ホストから両方のONTAPクラスタへの接続が可能です。一方、ストレージ構成が統一されていない場合は、ホストからローカルストレージレイへの接続のみが可能です。

マルチパス

図6に示すように、SM-BCではALUAが使用されます。ALUAは、アプリケーションホストのマルチパスソフトウェアに優先順位とアクセス可用性を設定してアドバタイズされたパスを使用して、アプリケーションホストとストレージレイ間の通信を可能にする標準のSCSIメカニズムです。ALUAは、LUNを所有するコントローラへの

アクティブな最適パスおよびその他のパスをアクティブな非最適パスとしてマークします。このパスは、プライマリパスで障害が発生した場合にのみ使用されます。

図6) ALUAを使用するSM-BC

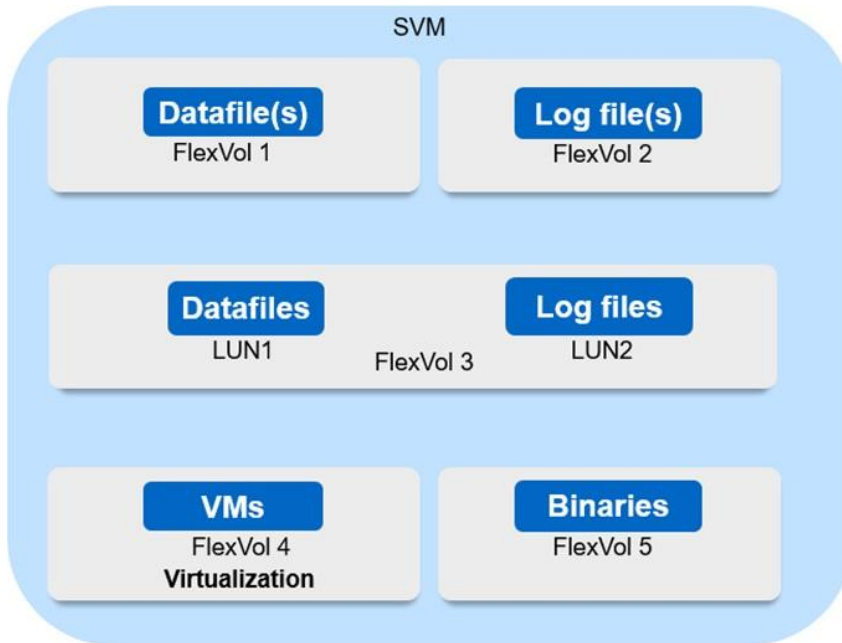


データレイアウト

ビジネス継続性のために保護が必要なワークロードを特定し、データ保護戦略で明確に定義することが重要です。データ保護戦略で最も重要なステップは、エンタープライズアプリケーションのデータレイアウトを明確にして、ボリュームの分散方法やビジネス継続性の保護方法を決定できるようにすることです。シームレスなフェイルオーバーはアプリケーションごとにCGで実行されるため、必要なデータボリュームを必ずCGに追加してください。

図7は、エンタープライズアプリケーション用のSVM内のデータレイアウトを示しています。

図7) エンタープライズアプリケーション向けSVM内のデータレイアウト



- データ ボリューム：
 - ランダムリードのワークロードはシーケンシャルライトとは切り離されているため、データファイルとログファイルは通常、データベースのサイズによっては別々のボリュームに配置されます。
 - 重要な大規模データベースの場合、単一のデータファイルがFlexVol 1に、対応するログファイルがFlexVol 2にあります。
 - 統合を効率化するために、小規模から中規模の重要でないデータベースは、すべてのデータファイルがFlexVol 1に配置され、対応するログファイルがFlexVol 2に配置されるようにグループ化されます。ただし、このグループ化によって、アプリケーションレベルの細分性が失われます。
 - 別の方法としては、すべてのファイルを同じFlexVol 3に格納し、データファイルをLUN1に、ログファイルをLUN 2に格納する方法があります。
- 環境が仮想化されている場合は、さまざまなエンタープライズアプリケーションのすべてのVMを1つのデータストアで共有します。通常、VMとアプリケーションバイナリはSnapMirrorを使用して非同期でレプリケートされます。

ビジネス継続性のための保護の設定

前提条件

ハードウェア

SM-BCでは、AFFモデルまたはASAモデルの2ノードのHAクラスタのみがサポートされます。プライマリクラスタとセカンダリクラスタの両方で、同じタイプ（AFFまたはASA）を使用する必要があります。FASモデルを含むビジネス継続性のための保護はサポートされていません。

注： ビジネス継続性の目的は、災害などサイトが動作不能になる可能性のある障害から保護し、システムを停止することなくビジネスの運用を継続できるようにすることです。そのため、同じクラスタ内でビジネス継続性を保護することはできません。ソースクラスタとデスティネーションクラスタが分離されている必要があります。

ライセンス

ソースとデスティネーションの両方のストレージクラスタにデータ保護バンドルまたはワнтаイムプレミアムバンドルがある場合は、**SM-BC**を使用できます。

ソフトウェア

- ストレージシステムは**ONTAP 9.8**以降である必要があります。
- ソースクラスタとデスティネーションクラスタのすべてのノードを**ONTAP 9.8**以降にインストールまたはアップグレードしておく必要があります。
- **RHEL**を実行する**Linux**サーバまたは**VM (7.6、7.7、7.8、7.9、8.1 ONTAP、8.2、8.3、8.4、8.5)** または **CentOS (7.6、7.7、7.8、7.9)**。

ネットワーク

ストレージレイバースのレプリケーションでは、**TCP / IP**ネットワークを介して転送されます。ソースストレージシステムとデスティネーションストレージシステム間の最大応答時間 (**RTT**) レイテンシは**10**ミリ秒未満です。

ONTAP クラスタ コウセイ

ソースクラスタとデスティネーションクラスタが適切に設定されていることを確認する。詳細については、「[ONTAP クラスタ構成の確認](#)」を参照してください。

ONTAP Mediator

ONTAP メディエーターは、**2**つのONTAP クラスタとは別の**第3**の障害ドメインにインストールされ、次の**3**者クォーラムでの合意を確立するために使用されます。

- **SM-BC**プライマリ**CG**をホストするプライマリONTAP クラスタ
- ミラー**CG**をホストしているセカンダリONTAP クラスタ
- **ONTAP Mediator**

ONTAPは、ストレージシステム間のレプリケーションのステータスとともに、ノード管理**LIF**とクラスタ管理**LIF**を介してノードとコントローラのハートビートを定期的に送信しますONTAP。サイト障害とスイッチ間リンク (**ISL**) 障害 (サイト間リンクが停止している場合) を区別するために、複数のパスを介した冗長接続が確立されます。**Mediator**の健全性情報を使用すると、クラスタ間**LIF**の障害やサイト障害などを区別できます。ONTAPでは、メディエーターから提供される情報とクラスタ間**LIF**の健全性チェックの情報を使用して、自動フェイルオーバーを実行するかどうかを判断できます。ONTAP メディエーターソフトウェアとクラスタ内のすべてのノード、およびクラスタ自体への接続が (イベントにより) 失われると、そのクラスタは到達不能と宣言されます。ONTAP メディエーターはこの処理を**3**秒おきに試行し、障害 (接続、サイトなど) の検出を**3**回試行します。その後、稼働しているクラスタ (到達可能な状態) がパートナークラスタへのすべてのリンクが切断されたことを示します。次に**ONTAP Mediator**がアラートをトリガーし、セカンダリサイトのミラー**CG**への自動フェイルオーバーを有効にして、クライアントへの**I/O**の中断をゼロにします。ネットワークの不具合やネットワークイベント (リンクのダウンなど) がこの**9**秒間のウィンドウ内で手動または自動で修正されない場合、使用可能な冗長パスがない限り、ハートビート障害が発生し、関係が同期しなくなる可能性があります (たとえば、別のポートへの**LIF**のフェイルオーバー)。ハートビートを維持できます。

また、ONTAP メディエーターは、クラスタ内の他のノードとのネットワークハートビートまたはディスクハートビートの障害が原因ですべてのノードがクラスタ内で唯一稼働しているメンバーであると見なし、自身をプライマリと宣言するスプリットブレインシナリオからの保護にも役立ちます。

要約すると、ONTAP メディエーターは次の目的で使用されます。

- クォーラムを確立する
- スプリットブレインシナリオを回避する

- 障害が検出されたときの自動フェイルオーバーを有効にする

注：ONTAP Mediator 1.5では、ビジネス継続性を確保するために10個のクラスタペアを管理できます。

注：ONTAPメディエーター1.5では、SM-BC構成に加えて、MetroCluster IP（MC IP）構成も管理できます。

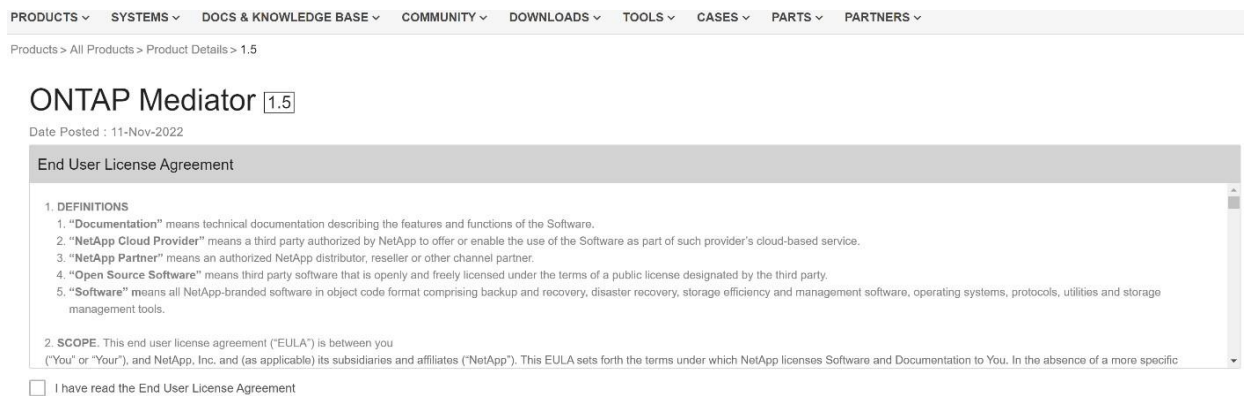
注：ONTAP Mediatorを使用できない場合は、計画的フェイルオーバーまたは自動フェイルオーバーを実行できません。アプリケーションデータは、中断することなく引き続き同期的にレプリケートされますが、データ損失はゼロです。

ONTAPメディエーターのインストール

SM-BC解決策を設定して使用するには、ONTAP Mediatorをインストールする必要があります。インストールする前に、ライセンス契約および図8に示す注意事項/必読事項に同意する必要があります。

詳細については、「[ONTAPメディエーターのインストール](#)」を参照してください。

図8) Caution/MustRead文



注：Mediatorをインストールする場合は、自己署名証明書を信頼できる主要なCAによって署名された有効な証明書に置き換える必要があります。

ONTAPメディエーターの設定

ビジネス継続性のための保護を開始する前に、ONTAPメディエーターを初期化する必要があります。これは、ONTAPシステムマネージャまたはONTAP CLIのグラフィカルユーザインターフェイスを使用して実行できます。

ONTAPシステムマネージャで、次の手順を実行します。

1. [保護] > [概要] > [メディエーター] > [設定]の順に選択します。
2. [追加]をクリックし、Mediatorサーバの次の情報を入力します。
 - IPv4 アドレス
 - ユーザ名
 - パスワード

手順を使用して、[CLIを使用してONTAPメディエーターを初期化](#)します。

通常の動作中は、ONTAPメディエーターの状態は「connected」になります。それ以外の状態の場合はエラー状態を示している可能性があり、Event Management System（EMS；イベント管理システム）メッセージに表示して適切に対処できます。

ビジネス継続性のための保護

ビジネス継続性のための保護では、2つのONTAPストレージシステム間にデータ保護関係を作成し、アプリケーション固有のLUNを保護グループと呼ばれる整合グループに追加します。

注：LUNは同じSVM内に存在する必要があります。

ONTAPシステムマネージャで、次の手順を実行します。

1. [保護] > [概要] > [ビジネス継続性のための保護] > [LUNの保護]。
2. ソース クラスタで保護するLUNを1つ以上選択します。
3. デスティネーションのクラスタとSVMを選択します。
4. [関係の初期化]はデフォルトで選択されています。[Save]をクリックして保護を開始します。
5. デスティネーションクラスタでONTAP System Managerを使用します。ビジネス継続性のための保護が「同期されている」ことを確認するには、[Protection]>[Relationships]を選択します。

注：ONTAPの[System Manager]>[Applications]タブで作成された、AppDM（Oracle、Microsoft SQL Server、仮想サーバ、仮想デスクトップアプリケーション、汎用のSAN / NASコンテナとして使用する場合など）に関連付けられたボリュームはサポートされません。

注：ONTAP 9.12.1では、サポートされる整合グループは50個までです。

注：ビジネス継続性を目的として保護されているソースボリュームに対しても、非同期データ保護関係をあと1つだけ作成できます。

手順を使用したONTAP CLIからの保護 [整合性グループ関係の作成](#)と [整合性グループの初期化](#)

注：保護関係を設定したら、セカンダリクラスタ内のレプリケートされたLUNをホストにマッピングし、ホストの設定時にプライマリクラスタとセカンダリクラスタの両方のLUNへのI/Oパスを検出する必要があります。

ONTAPシステムマネージャで、次の手順を実行します。

1. [Storage]>[LUNs]>デスティネーションLUNが認識されていることを確認します。
2. 各LUNを編集して正しいホストマッピング>イニシエータグループにマッピングします。
3. ONTAP CLIの場合は、「[アプリケーションホストへのLUNのマッピング](#)」を参照してください。
4. アプリケーションホストで、ディスクを再スキャンし、（セカンダリストレージシステムから）デスティネーションLUNへのパスが検出され、ALUAがこれらのパスを正しくアダプタイズすることを確認する必要があります。

ストレージLIF

以下のシナリオに従ってSAN LIFのサービスポリシーを変更した場合、変更内容はピアクラスタに正確にレプリケートされません。snapmirror abort resync 変更内容が確実にレプリケートされるようにするには、のあとにを付ける必要があります。

シナリオ1

SAN LIFのサービスポリシーを default-data-blocks とに変更し default-data-files たり、元の状態に戻したりします。

```
C1_sti96-vsimg-ucs540a_cluster::*> net int show -vserver vs0 -fields data-protocol
(network interface show)
vserver lif data-protocol
-----
vs0      lif1 iscsi

C1_sti96-vsimg-ucs540a_cluster::*> iscsi interface show -fields relative-port-id
vserver lif relative-port-id
-----
```

```

vs0      lif1 2

C1_sti96-vsimg-ucs540a_cluster::*> net int modify -vserver vs0 -lif lif1 -service-policy default-
data-files
(network interface modify)

Warning: Assigning service policy "default-data-files" to LIF "lif1" on Vserver
"vs0" will impact the data services supported by this LIF, which
requires the LIF to be temporarily brought offline. Data service on
this LIF will be briefly interrupted while this change is applied, and
any existing network connections will be reset.
Do you want to continue? {y|n}: y

C1_sti96-vsimg-ucs540a_cluster::*> net int show -vserver vs0 -fields data-protocol
(network interface show)
vserver lif data-protocol
-----
vs0      lif1 nfs,cifs,fcache

C1_sti96-vsimg-ucs540a_cluster::*> iscsi interface show -fields relative-port-id
There are no entries matching your query.

C1_sti96-vsimg-ucs540a_cluster::*> net int modify -vserver vs0 -lif lif1 -service-policy default-
data-blocks
(network interface modify)

Warning: Assigning service policy "default-data-blocks" to LIF "lif1" on
Vserver "vs0" will impact the data services supported by this LIF,
which requires the LIF to be temporarily brought offline. Data service
on this LIF will be briefly interrupted while this change is applied,
and any existing network connections will be reset.
Do you want to continue? {y|n}: y

C1_sti96-vsimg-ucs540a_cluster::*> iscsi interface show -fields relative-port-id
vserver lif relative-port-id
-----
vs0      lif1 3

C1_sti96-vsimg-ucs540a_cluster::*> snapmirror abort *
Operation is queued: snapmirror abort for the relationship with destination
"vs1:/cg/smbc_dst_hard1".

Warning: It is recommended to quiesce the relationship using the "snapmirror
quiesce" command instead of aborting the SnapMirror Synchronous
transfer. For relationships with a policy of type "strict-sync-mirror"
this will fail client I/O on source volume if the status is InSync.
Do you want to continue? {y|n}: yes
Operation is queued: snapmirror abort for the relationship with destination "vs1:sync_dst_1".
1 entries were acted on.

C1_sti96-vsimg-ucs540a_cluster::*> snapmirror resync *
Operation is queued: snapmirror resync to destination "vs1:/cg/smbc_dst_hard1".

```

シナリオ2

クラスタ間LIFのサービスポリシーをnode-mgmtに変更します。

```

C1_sti96-vsimg-ucs540a_cluster::*> net int show -role intercluster -fields role,service-
policy,services
(network interface show)
vserver      lif service-policy      services      role
-----
C1_sti96-vsimg-ucs540a_cluster ic default-intercluster intercluster-core,management-https
intercluster
C1_sti96-vsimg-ucs540a_cluster sti96-vsimg-ucs540a_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
C1_sti96-vsimg-ucs540a_cluster sti96-vsimg-ucs540b_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
3 entries were displayed.

```

```

SMBC_A:.*> net int modify -vserver C1_sti96-vsim-ucs540a_cluster -lif ic -service-policy default-
management
(network interface modify)

C1_sti96-vsim-ucs540a_cluster:.*> net int show -role intercluster -fields role,service-
policy,services
(network interface show)
vserver          lif          service-policy
services          role
-----
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540a_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540b_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
2 entries were displayed.

```

シナリオ3

サービスポリシーを管理からクラスタ間に変更します。

```

C1_sti96-vsim-ucs540a_cluster:.*> net int show -role node-mgmt -fields role,service-
policy,services
(network interface show)
vserver          lif service-policy    services
role
-----
C1_sti96-vsim-ucs540a_cluster ic default-management management-core,management-
autosupport,management-ssh,management-https node-mgmt
C1_sti96-vsim-ucs540a_cluster ic2 default-management management-core,management-
autosupport,management-ssh,management-https node-mgmt
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540a_mgmt1 default-management management-
core,management-autosupport,management-ssh,management-https node-mgmt
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540b_mgmt1 default-management management-
core,management-autosupport,management-ssh,management-https node-mgmt
4 entries were displayed.

C1_sti96-vsim-ucs540a_cluster:.*> net int show -role intercluster -fields role,service-
policy,services
(network interface show)
vserver          lif          service-policy
services          role
-----
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540a_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
C1_sti96-vsim-ucs540a_cluster sti96-vsim-ucs540b_inet4_intercluster1 default-intercluster
intercluster-core,management-https intercluster
2 entries were displayed.

C1_sti96-vsim-ucs540a_cluster:.*> net int modify -vserver C1_sti96-vsim-ucs540a_cluster -lif ic2
-service-policy default-intercluster
(network interface modify)

```

SM-BCの可用性

SM-BC関係の可用性は、プライマリクラスタ、セカンダリクラスタ、またはその両方で一連のコマンドを使用して確認できます。例：

```

SMBC_A:.*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86  SMBC_B      connected      true

SMBC_B:.*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status

```



```

-----
10.236.172.86    SMBC_A          connected      true

SMBC_B:::> snapmirror show -expand

Source          Destination Mirror Relationship    Total          Progress
Path           Type Path      State  Status            Progress  Healthy  Last
-----
vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored InSync -          true    -
vs0:voll1    XDP vs1:voll_dp Snapmirrored InSync -          true    -
2 entries were displayed.

SMBC_A:::> volume show -fields is-smbc-master,smbc-consensus,is-smbc-failover-capable -volume
voll1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs0      voll      true          false          Consensus

SMBC_B:::> volume show -fields is-smbc-master,smbc-consensus,is-smbc-failover-capable -volume
voll_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs1      voll_dp false          true           No-consensus

```

クラスタ間LIFをホストするポートが停止した（管理停止またはリンク停止）場合は、SM-BC関係が「非同期」になり、RPOゼロとRTOゼロの停止が発生します。

問題

たとえば、Cisco Application Centric Infrastructure (ACI) で設定されたブリッジドメインを使用するニッチなユースケースです。デフォルトでは、これらのスイッチは、L2不明ユニキャストアドレスを解決するためにハードウェアプロキシモードを使用します。宛先MACアドレスが不明な場合、パケットはスパインプロキシに転送されます。また、スパインプロキシのデータベースに宛先MACアドレス情報がない場合、パケットはドロップされます。これにより、ACIスイッチの背後にあるONTAPのL2到達可能性の問題が発生します。

たとえば、2つの2ノードONTAPクラスタ（プライマリとセカンダリ）がクラスタ間ネットワークインターフェイス（LIF）を使用してクラスタピア関係を形成しており、すべてのノードのクラスタ間LIFがACIコードを実行しているCisco Nexusスイッチに接続されているとします。プライマリクラスタのノード1には、ポートe0cとポートe0dがあり、それぞれIC LIF ic1とic2をホストしています。ポートe0cとe0dはIC LIFフェイルオーバーグループに属しています。

ポートe0cが管理上停止になった場合は、LIF IC1がポートe0dにフェイルオーバーします。ノード1で実行されているONTAPから、LIF IC1がポートe0dでホストされるようになり、関連するMACアドレスが更新されたことがACIスイッチに通知されます。ただし、このACIスイッチが、ハードウェアプロキシモードを使用してL2不明ユニキャストアドレスを解決するように設定されたCisco Application Policy Infrastructure Controller (APIC) によって駆動されている場合、ノード1からのMACアドレス更新がファブリック内でさらに伝播されない可能性があります。これにより、LIF IC1にセカンダリクラスタから到達できなくなります。

解決策

Cisco APICのL2不明ユニキャストポリシーをデフォルトのハードウェアプロキシモードから、影響を受けるVLANのフラッドイングアルゴリズムを使用するように変更します。

フェイルオーバー手順

フェイルオーバーおよびフェイルバック操作は、BCDR計画の成功に不可欠です。災害が発生した場合、フェイルオーバーとは、ミッションクリティカルなワークロードをプライマリストレージシステムからディザスタリカバリサイトのセカンダリストレージシステムに移行するプロセスのことです。計画的フェイルオーバーを使用して、ディザスタリカバリ構成を評価したり、プライマリクラスタのメンテナンスを実施したりすること

ができます。一部の国の金融機関に対する規制では、企業がセカンダリデータセンターから定期的にサービスを提供できるようにすることが求められています。

計画的フェイルオーバー

計画的フェイルオーバーを実行して、ディザスタリカバリ設定を評価したり、セカンダリクラスタの管理者が開始したプライマリクラスタのメンテナンスを実行したりできます。この処理では、セカンダリクラスタがプライマリクラスタからテイクオーバーするように、プライマリロールとセカンダリロールを切り替える必要があります。新しいプライマリクラスタがローカルで入出力要求の処理を開始できるようになり、クライアントの処理は中断されません。ALUAはそれに応じてパスを更新します。

ONTAPシステムマネージャで、次の手順を実行します。

1. [保護]>[概要]>[関係]を選択します。
2. 関係にカーソルを合わせ、楕円を選択して[Failover]をクリックします。

詳細については、「[ONTAP CLIを使用した計画的フェイルオーバーの実行](#)」を参照してください。

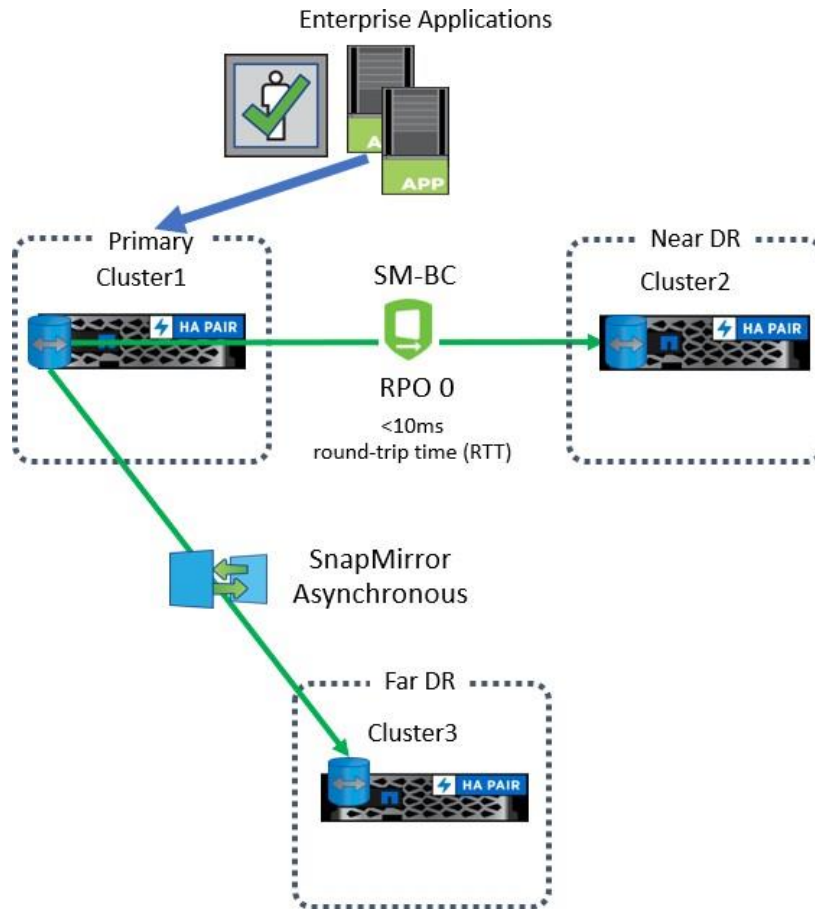
計画的フェイルオーバー処理のステータスと進捗状況は `snapmirror failover show`、コマンドを使用して監視できます。フェイルオーバー処理が完了したら、`snapmirror show` コマンドを使用して、新しいデスティネーションクラスタから同期レプリケーションの保護ステータスを監視できます。

注： ボリューム移動、アグリゲートの再配置、ストレージフェイルオーバーなどの無停止操作の実行中は、計画的フェイルオーバーを開始できません。

3ウェイポロジ

図9は、3ウェイのファンアウトポロジを示しています。

図9) ファンアウトトポロジ



近いDRサイトへの計画的フェイルオーバーで、近いDRサイトから遠いDRサイトへの新しいSnapMirror関係を作成すると、「Last Transfer Error : No common Snapshot copy found between SVM2 : smbc_dest and SVM3 : async」というエラーが表示され、ベースラインの再実行が必要になります。この問題に対処し、この再ベースラインを回避するには、diag privilege set diag計画的フェイルオーバーまたはネゴシエートフェイルオーバーを実行する前に、Cluster1で () の次のコマンドを実行します。

```
Cluster1::> set diag
Cluster1*::> run -node * setflag skip_cg_css_post_init_resync 1
Cluster1*::> run -node * sm_disable_cg_css_sched 1
```

新しいセカンダリストレージで（フェイルオーバー後に）上記のコマンドを無効にして、Cluster1で共通のSnapshotが引き続き作成されるようにすることが重要です。

```
Cluster1::> set diag
Cluster1*::> run -node * setflag skip_cg_css_post_init_resync 0
Cluster1*::> run -node * sm_disable_cg_css_sched 0
```

自動計画外フェイルオーバー

自動計画外フェイルオーバー（AUFO）処理は、ONTAP Mediatorを使用してのみ実行されます。この処理は、プライマリクラスタが停止したか分離され、セカンダリクラスタがプライマリに変換されてクライアントへのサービス提供が開始されたときに実行されます。

注： 自動計画外フェイルオーバーまたは非同期イベントが80秒を超えた場合は、ホストのLUN I/Oパスを再スキャンしてI/Oパスが失われないようにすることが重要です。詳細については、各ホストOSベンダーのLUN I/Oパスの再スキャンに関するドキュメントを参照してください。

自動計画外フェイルオーバーの実行中は `snapmirror failover show`、コマンドを使用して処理のステータスを監視できます。

```
ClusterB::> snapmirror failover show -instance

      Start Time: 9/23/2020 22:03:29
      Source Path: vs1:/cg/scg3
      Destination Path: vs3:/cg/dcg3
      Failover Status: completed
      Error Reason:
        End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
      Failover Type: unplanned
      Error Reason codes: -
```

注： サイト間リンクが停止し、原因プライマリ分離によってプライマリCGをホストしているONTAPクラスタがピアクラスタとメディアーターにアクセスできない場合、以降のストレージフェイルオーバーは停止します。この場合、NetAppでは、分離されたプライマリから既存のLUNマップを削除し、ディザスタリカバリが再確立されたときに再マッピングすることを推奨しています。

注： ボリューム移動が実行中でAUFOがトリガーされた場合は、このジョブが停止し、カットオーバー保留状態で無期限に待機するために、実行中のボリューム移動を中止する必要があります。回避策がボリューム移動インスタンスを中止し、ボリューム移動ジョブを再開します。

```
# Abort the stuck volume move job
Cluster::> volume move abort -volume <volume name>
# Restart the volume move job
Cluster::> volume move start -volume <volume name> -destination-aggregate <destination aggregate name>
```

整合性グループへのボリュームの追加と削除

CGの構成の変更は、ONTAP 9.12.1ではサポートされていません。そのため、構成を変更する唯一の方法は、元の関係を削除してから、CGの新しい構成との新しいSM-BC関係を作成することです。詳細については、「[整合グループ内のボリュームの追加と削除](#)」を参照してください。

注： CGを拡張するために追加する新しいボリュームには、ソースボリュームとデスティネーションボリュームに共通のSnapshotコピーのペアが必要です。詳細については、[共通のSnapshotコピーの作成](#)を参照してください。

単一ファイル対応のSnapRestore

ONTAP 9.11.1以降では、Single File SnapRestoreがサポートされます。この機能を使用すると、アプリケーションで作成されたSnapshotコピーから、SM-BCのソース（ボリューム）ボリュームとデスティネーション（Snapshotコピー）ボリュームの間でレプリケートされた単一ファイル/LUNのリストアを実行できます。ボリュームには1つ以上のLUNを含めることができるため、ボリューム内の他のLUNを中断せずに、1つのLUNをきめ細かくリストアする必要があります。Single File SnapRestoreには、インプレースとアウトオブプレースの2つのオプションがあります。In Placeオプションは、フルリストアを実行し、元のファイルまたはLUNを上書きします。Out-of-Placeオプションは、フルリストアを実行し、データを新しいファイルに書き込み、新しいLUNを作成します。詳細については、「[Snapshotコピーから単一ファイルをリストアする](#)」を参照してください。

パーシャル・シングル・ファイルSnapRestore

Partial Single File SnapRestoreはONTAP 9.12.1以降でサポートされます。この機能を使用すると、アプリケーションで作成されたSnapshotコピーから、SM-BCのソース（ボリューム）ボリュームとデスティネーション（Snapshotコピー）ボリュームの間でレプリケートされた一連のデータをリストアできます。想定されるユースケースとしては、同じLUNに複数のデータベースが格納されているホストにデータベースをリストアする方法があります。この機能を使用するには、データの開始バイトオフセットとバイトカウントを知る必要があります。詳細については、「[Snapshotコピーからファイルの一部をリストアする](#)」を参照してください。

ビジネス継続性のために既存のSnapMirror Synchronous関係を変換して保護

デスティネーションボリュームのすべてのLUNがアプリケーションホストからマッピングされていない場合は、既存のSM-S関係をSM-BCに変換できます。そうしないと、SM-BC保護関係の作成がエラーで失敗します。詳細については、「[既存の関係からSM-BC関係への変換](#)」を参照してください。

SM-BC関係があるONTAPのバージョンのアップグレードとリバート

状況によっては、SM-BC関係を含むONTAPのインストールを以前のバージョンにリバートできます。ただし、続行する前に慎重に検討する必要があります。ほとんどの場合、リバート前に既存のSM-BC関係を削除する必要があります。

詳細については、「[SM-BCのアップグレードとリバートに関する考慮事項](#)」を参照してください。

トラブルシューティング

オンラインの[トラブルシューティングマニュアル](#)を参照してください。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細は、以下のドキュメントやウェブサイトをご参照ください。

- SnapMirrorビジネス継続性ソリューションのドキュメント
<https://docs.netapp.com/us-en/ontap/smbc/index.html>
SM-BCには、ONTAPシステムマネージャ、CLI、またはONTAP REST APIを使用してアクセスおよび設定できます。

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2021年1月	ONTAP 9.8用のリリース。
バージョン2.0	2022年8月	ONTAP 9.11.1リリース
バージョン3.0	2022年11月	ONTAP 9.12.1リリース

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 サイトで [Interoperability Matrix Tool \(IMT\)](#) を参照してください。NetApp IMT には、NetApp 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。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

Copyright © 2024 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。

NetApp 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、NetApp によって「現状のまま」提供されています。NetApp 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。NetApp 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。

NetApp 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。NetApp 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、NetApp は責任を負いません。この製品の使用または購入は、NetApp 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り保護されている場合があります。

本書に含まれるデータは市販の製品および/またはサービス（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。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、<https://www.netapp.com/company/legal/trademarks/> 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。

TR-4878-1122-JP