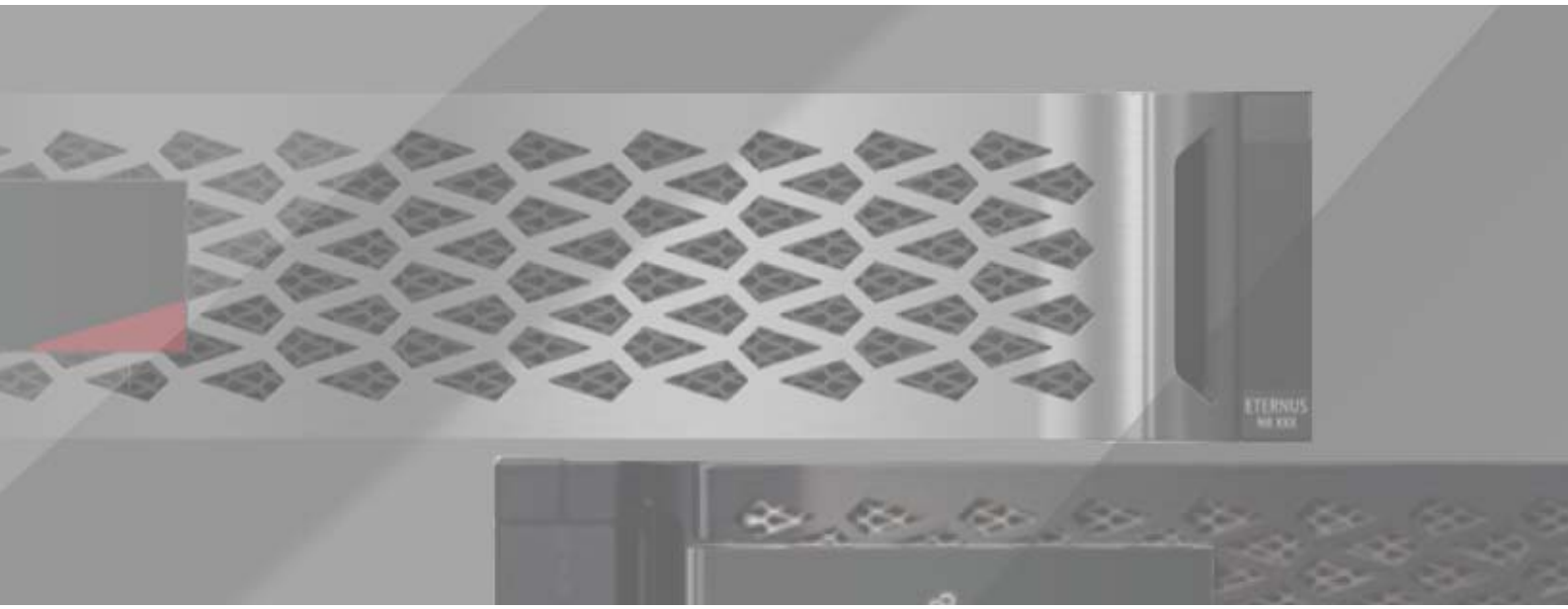
P3AG-5642-04Z0

# Fujitsu Storage
# ETERNUS AX series オールフラッシュアレイ，
# ETERNUS HX series ハイブリッドアレイ

## ONTAP 9.11.1 用
## SnapMirror 構成およびベストプラクティスガイド




FUJITSU

# 目次

# 図目次

# 表目次

# はじめに

本書では、ONTAP 9.11.1 でのレプリケーション設定に関する情報とベストプラクティスについて説明します。



第 3 版
2022 年 12 月

## 登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/

本書では、本文中の ™、® などの記号は省略しています。

## 本書の読み方

### 対象読者

本書は、ETERNUS AX/HX の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

### 関連マニュアル

ETERNUS AX/HX に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

# 本書の表記について

## ■ 本文中の記号

本文中では、以下の記号を使用しています。

| | |
|---|---|
| 注 意 | お使いになるときに注意していただきたいことを記述しています。必ずお読みください。 |
| 備 考 | 本文を補足する内容や、参考情報を記述しています。 |

# 第 1 章
# ソリューションの概要

企業は、ハードウェア、ソフトウェア、またはサイトの障害に直面した場合に、複数のアプローチを使用してデータの可用性を向上させることができます。データ保護 (DP) は最も重要な側面の 1 つです。これは、データが失われると、コストと時間の損失に直結するためです。データ保護とは、1 つの場所にあるデータを別の場所にコピーして、次の 2 つの用途に使用するプロセスです。

- **バックアップ**
  目的は、セカンダリからプライマリにリストアすることであり、セカンダリにフェイルオーバーすることはありません。これは、セカンダリの主な目的がアーカイブストレージであることを意味します。そのため、プライマリよりもセカンダリの方が多くのデータを保持できます。
- **災害復旧 (DR)**
  正確なレプリカまたはコピーがセカンダリに保持され、プライマリサイトで障害が発生した場合にプライマリからセカンダリへのフェイルオーバーに使用されます。

バックアップによって、消失したデータをアーカイブメディア ( テープ、ドライブ、クラウド ) からリカバリできますが、ミラーリングは、特にダウンタイムを最小限に抑えたい場合に、ビジネス継続性と DR のための最も一般的なデータ可用性メカニズムです。SnapMirror テクノロジーは、LAN および WAN 経由でデータのミラーリングまたはレプリケーションを行う、高速で柔軟性のあるエンタープライズソリューションです。SnapMirror を使用する主な利点は次のとおりです。

- **堅牢なエンタープライズテクノロジー**
  SnapMirror は、ONTAP ストレージシステムの成熟した機能であり、時間の経過とともに拡張および改善されてきました。SnapMirror では、更新の失敗からのリカバリ、レプリケーション処理の同時プロセスの使用、転送処理に使用されるネットワーク帯域幅の抑制などが可能です。
- **スピードと効率性**
  ブロックレベルの論理増分データ転送では、変更されたデータのみがデスティネーションレプリカに送信されます。SnapMirror を使用すると、ネットワーク圧縮などのさまざまなストレージ効率によってデータ量をさらに削減できます。ネットワーク圧縮により、データがソースから離れたときにデータを圧縮し、デスティネーションでデータを解凍することで、転送パフォーマンスを向上させることができます。
- **柔軟性**
  SnapMirror を使用すると、システムのニーズに合わせて異なる同期スケジュールを定義できます。また、プライマリリポジトリに問題がある場合は、SnapMirror を使用して同期の方向を変更することもできます。SnapMirror は、さまざまなレプリケーショントポロジーの作成にも使用できます。オプションには、1 つのボリュームを複数のセカンダリシステムにレプリケートするファンアウトと、デスティネーションボリューム自体をターシャリシステムに同期させるカスケードがあります。
- **テスト容易性**
  SnapMirror デスティネーションボリュームは、FlexClone テクノロジーを使用して、サイズに関係なく、スペース効率に優れた方法で書き込み可能なボリュームとして瞬時にクローン化できます。ソースからのデータのレプリケーションを停止する必要はありません。これは、たとえば DR テストの実行に非常に役立ちます。

- **フェイルオーバーとフェイルバック**
  ミラー先システムで運用する必要がある場合、SnapMirror 関係を一時的に停止します。これにより、デスティネーションボリュームが読み取り / 書き込み可能になり、使用できる状態になります。SnapMirror を使用すると、元のソースとデスティネーションで行われた変更を再同期してから、元の SnapMirror 関係を再確立できます。
- **使いやすさ**
  ONTAP System Manager を使用すると、簡素化されたワークフローとウィザードによるウォークスルーで操作を実行できます。また、すべての SnapMirror レプリケーション関係を 1 か所で監視および管理することもできます。
- **安全**
  ONTAP 9.x 以降では、SnapMirror 関係をネイティブのエンドツーエンドで暗号化できます。
- **クラウド対応**
  SnapMirror は、大手クラウドプロバイダーが提供している Amazon FSx for ONTAP や Cloud Volumes ONTAP などのクラウド上にある富士通のソリューションへの、ボリュームおよびストレージ仮想マシン (SVM) のレプリケーションをサポートしています。

# 1.1　目的と対象読者

このドキュメントは、ONTAP システムを管理、インストール、またはサポートする担当者、およびデータレプリケーション用にSnapMirror技術を設定および使用する予定のある担当者を対象としています。

このドキュメントでは、読者が次のプロセスとテクノロジーを理解していることを前提としています。

- ONTAP の操作に関する実用的な知識
- Snapshot テクノロジー、FlexVol、FlexGroup ボリューム、FlexClone テクノロジーなどの機能に関する実用的な知識
- DR およびデータレプリケーションソリューションに関する一般的な知識
- 富士通マニュアルサイトの「FUJITSU Storage ETERNUS AX/HX series データ保護パワーガイド」に精通していること

# 1.2　SnapMirror の新機能

表 1.1 に、このマニュアルの以前の版以降に導入された主な変更を示します。

表 1.1　SnapMirror の新機能

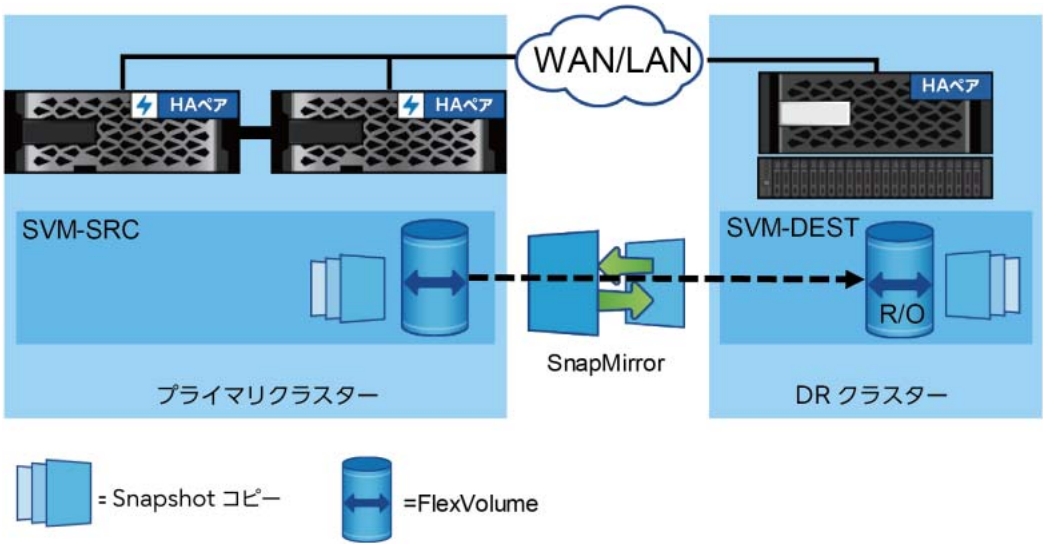
| 機能領域 | 変更内容 |
|---|---|
| SVM ディザスタリカバリ (SVM DR) とデータ移動 | • ONTAP 9.10.1 以降、SnapMirror は SVM 移行と呼ばれるデータ移動機能を提供しています。SVM 移行では、SnapMirror Asynchronous と SnapMirror Synchronous (SM-S) の両方を使用して、ボリュームデータと SVM 設定情報を移行します。<br>• ONTAP 9.11.1 以降、最大 6 つのノードを含むクラスタにホストされる SVM の移行がサポートされるようになりました。<br>• クラスタあたりの SVM DR 関係の数は、次のように増加しました。<br>- 9.10.1 では、FlexVol ボリュームのみホストする SVM の場合の SVM DR 関係の数は、クラスタあたり 32 から 64 です。<br>- 9.11.1 では、FlexVol ボリュームのみホストする SVM の場合の SVM DR 関係の数は、クラスタあたり 64 から 128 です。<br>- FlexGroup ボリュームをホストする SVM では、クラスタあたりの SVM DR 関係の数は、32 に制限されます。 |
| アーキテクチャ / 構造 | ONTAP 9.9.1 以降、SnapMirror は FlexGroup ボリュームのカスケード構成とファンアウト構成をサポートしています。これには、デスティネーションがオンプレミスまたは Cloud Volumes ONTAP の場合も含まれます。 |
| プロトコル | ONTAP 9.10.1 以降、SnapMirror は ONTAP S3 バケットを保護します。S3 SnapMirror は、ONTAP 以外のデスティネーションを持つことができます。 |

# 1.3　SnapMirror の概要

SnapMirror は、ONTAP に組み込まれたレプリケーションソリューションで、ビジネス継続性と DR を目的としています。SnapMirror は、プライマリおよびセカンダリストレージシステム上のデータボリューム (FlexVol または FlexGroup) 間のデータ保護関係によって設定されます。SnapMirror は、定期的にレプリカを更新して、プライマリに書き込まれた変更によって最新の状態に保ちます。

このエンタープライズデータのレプリカまたはミラーは、地理的に離れたサイトまたはクラウドのセカンダリストレージシステムに作成されます。プライマリサイトで災害が発生した場合は、フェイルオーバーしてセカンダリからデータを提供できます。プライマリサイトのエラー状態が修正されたら、変更をプライマリサイトにレプリケートし直して、プライマリサイトからクライアントへのサービスを再開できます。SnapMirror を使用すると、総所有コスト (TCO) を削減でき、DR サイトを積極的にビジネスで使用することによって DR への投資を容易に正当化できます。SnapMirror レプリケーションの概要については、図 1.1 を参照してください。

図 1.1　SnapMirror レプリケーションの概要




ONTAP にはデータ保護機能が不可欠です。SnapMirror は Snapshot テクノロジーと緊密に統合されており、ドライブ上のレプリカやスペース効率に優れたデータのポイントインタイムコピーを迅速かつ効率的に作成します。

富士通統合データ保護を使用すると、すばやくアクセス可能でアプリケーションコンシステントな Snapshot コピーの履歴をドライブ上に作成でき、従来のバックアップウィンドウの概念を排除できます。その後、SnapMirror は Snapshot コピーの履歴をデスティネーションにレプリケートし、バックアップ、DR、またはテストおよび開発に使用できます。

SnapMirror レプリケーションは、前回の更新以降に変更または追加されたネイティブ 4K ブロックのみをレプリケートするため、効率的です。SnapMirror を富士通のストレージ効率化テクノロジーと組み合わせると、さらなる効率性が得られます。圧縮およびデータ重複排除テクノロジーにより、通信およびストレージ容量を大幅に節約できます。

# 1.4　使用例の概要

## 1.4.1　ニアラインバックアップ

SnapMirror の主な使用例の 1 つは、データバックアップです。企業向けデータストレージの黎明期から、データバックアップはテープの領域でした。テープバックアップでは、迅速なデータリカバリにいくつかの課題がありました。その 1 つは、多くの場合、テープバックアップが機能せず、災害シナリオからのリカバリには最短でも数時間かかるということです。

SnapMirrorは、同じクラスタ内またはリモートターゲットにデータをレプリケートすることによって、プライマリバックアップツールとして使用できます。SnapMirror を使用すると、ストレージ管理者は単一のファイルまたはストレージ構成全体を迅速にリストアできます。

## 1.4.2　DR

SnapMirror の技術は DR プランの一部としても使用されています。重要なデータが別の物理的な場所にレプリケートされる場合、重大な災害が発生しても、ビジネスクリティカルなアプリケーションのデータが長期間使用できなくなることはありません。クライアントは、破損、誤った削除、自然災害などから本番サイトを復旧するまで、ネットワークを介してレプリケートされたデータにアクセスできます。

プライマリサイトへのフェイルバックの場合、SnapMirror は、DR サイトをプライマリサイトと再同期し、変更されたデータまたは新しいデータのみを DR サイトからプライマリサイトに転送するための効率的な手段を提供します。これは、単に SnapMirror 関係を逆にすることによって行われます。プライマリ本番サイトが通常のアプリケーション運用を再開した後、SnapMirror は別のベースライン転送を必要とせずに DR サイトへの転送を続行します。

## 1.4.3　DR テストとアプリケーションのテスト、および開発

FlexClone テクノロジーを使用すると、すべての本番データが使用可能かどうかを確認するためにセカンダリコピーの読み取り / 書き込みアクセス権を必要とする場合に、SnapMirror デスティネーション FlexVol ボリュームの読み取り / 書き込み可能コピーをすばやく作成できます。

## 1.4.4　データ分散とリモートデータアクセス

SnapMirror テクノロジーを使用すると、企業全体に大量のデータを分散して、リモートサイトのデータにアクセスできます。リモートデータアクセスにより、リモートサイトのクライアントによるアクセスが高速化されます。また、事前に設定されたレプリケーション時間に WAN の使用が発生するため、高コストのネットワークおよびサーバリソースをより効率的かつ予測可能な方法で使用できます。ストレージ管理者は、特定の時間に本番データをレプリケートして、ネットワーク全体の使用率を最小限に抑えることができます。

### 1.4.5　バックアップのオフロードとリモートテープアーカイブ

SnapMirror テクノロジーは、バックアップの統合や、本番サーバのテープバックアップのオーバーヘッドの軽減にも使用できます。このアプローチにより、バックアップオペレーションの一元化が容易になり、リモートサイトでのバックアップ管理要件が軽減されます。Snapshot テクノロジーでは、プライマリストレージシステムの従来のバックアップウィンドウを排除できます。したがって、テープバックアップの SnapMirror デスティネーションへのオフロードにより、本番ストレージシステムでのバックアップオペレーションのオーバーヘッドが大幅に削減されます。

## 1.5　統合アーキテクチャの柔軟性

SnapMirror は、幅広いユーザー要件に対応するために、幅広いプラットフォームにデータ保護を提供します。SnapMirror は、データセンター環境用の ONTAP のネイティブ機能としてスタートしましたが、最近のアップデートでは新しいクラウド中心プラットフォームを採用した機能拡張を実施しており、図 1.2 に示す通りに、プライベートクラウド、ハイブリッドクラウド、およびパブリッククラウドの導入に対応しています。

### 1.5.1　データセンターへの導入

SnapMirror は、データセンターの任意の ONTAP プラットフォームで使用でき、ONTAP を導入したストレージにパフォーマンスと拡張性に関する幅広いニーズに対応します。これらの導入は、CLI、REST API、または Web ベースの ONTAP System Manager UI を使用して管理できます。

### 1.5.2　プライベートクラウドへの導入

SnapMirror プライベートクラウドへの導入は、データセンターへの導入と同様に設計されており、プラットフォームの柔軟性はすべて同じで、REST API によって提供される管理の柔軟性によって、クラウド中心の管理と、Kubernetes、VMware vRealize などの運用プラットフォームをサポートします。

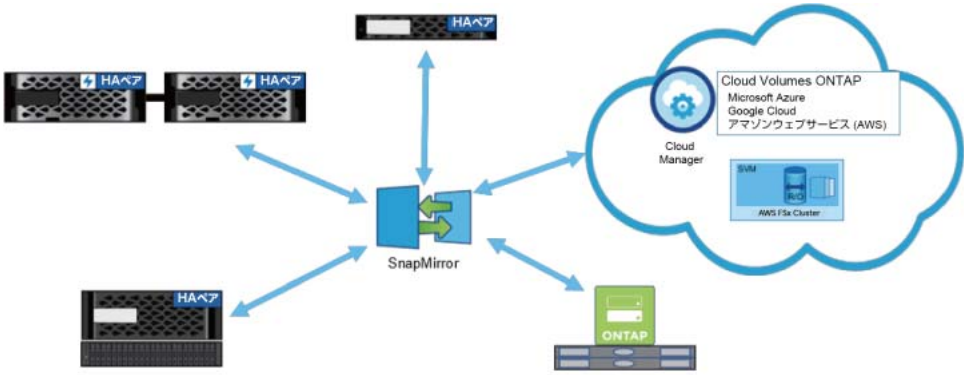
### 1.5.3　ハイブリッドクラウドへの導入

SnapMirror は、クラウド環境で動作する Cloud Manager を介した Cloud Volumes ONTAP、および Amazon FSx for ONTAP と、ONTAP オンプレミス間のデータレプリケーションをサポートします。

## 1.5.4　パブリッククラウドへの導入

ハイブリッドクラウドへの導入と同様に、Cloud Volumes ONTAP や Amazon FSx for ONTAP などのソリューションを通じて、ONTAP はクラウドで完全にホストすることができます。どちらのソリューションも、プライマリおよび DR クラウドベースの導入をサポートする SnapMirror 機能へのアクセスを提供し、ONTAP System Manager、CLI、または REST API を使用して管理ができます。さらに、Cloud Manager を使用して、ONTAP クラスタの Cloud Volume 間でデータをレプリケートするように SnapMirror を設定できます。

図 1.2　統合アーキテクチャの柔軟性



# 第 2 章
# ネットワークの基本

## 2.1 ONTAP ネットワーク共通の基本用語

表 2.1 に、ONTAP で使用される基本用語を示します。

表 2.1 ONTAP の用語

| 用語 | 定義 |
|---|---|
| ノード | ONTAP ストレージサービスを提供する単一のデバイスです。ノードは、スタンドアロン (ETERNUS AX/HX および ASA シャーシ、または Cloud Volumes ONTAP) にすることも、同じ物理シャーシに統合することもできます。通常、ONTAP ストレージクラスタは、1 つ以上の 2 ノード HA ペアで構成されます。 |
| ハイアベイラビリティ (HA) ペア | 高可用性を実現するために構成された、2 つの ONTAP ストレージノードのペアです。<br>ONTAP クラスタは、最大 6 の SAN HA ペア または最大 12 の NAS HA ペアで構成できます。 |
| クラスタ | 相互接続され、単一のストレージソリューションとして管理されている 1 つ以上の HA ペアです。 |
| IPspace | IPspace は、ONTAP を導入したストレージが参加できる個別の IP アドレス空間を定義します。IPspace は、個別のルーティングテーブルを提供します。 |
| ブロードキャストドメイン | ブロードキャストドメインは、単一のレイヤ 2 ネットワークプロトコルを介して通信できる、同じ IPspace 内の物理ネットワークポートのグループです。 |
| クラスタインターコネクト | 同一クラスタ内のノード間の通信およびレプリケーションに使用される、高速で低レイテンシの専用プライベートネットワークです。 |
| データネットワーク | クライアントがデータにアクセスするために使用するネットワークです。データネットワークは、クライアントサーバーとアプリケーションを、さまざまなストレージプロトコルを経由して ONTAP クラスタ内のストレージリソースに接続するために必要です。マルチテナント機能やその他のプライバシーまたはセキュリティ要件をサポートするために、複数のデータネットワークを使用できます。 |
| 管理ネットワーク | クラスタ、SVM、およびノードの管理に使用されるネットワークです。 |
| クラスタインターコネクトネットワーク | 異なるクラスタ間の通信およびレプリケーションに使用されるネットワークです。クラスタインターコネクトネットワークは、ONTAP 環境内の SnapMirror やその他のデータ保護ソリューションによって使用されます。 |
| HA 相互接続 | 1 つの HA ペア内の 2 つのノード間をつなぐ、専用のネットワークです。HA 相互接続は、ノードモデルに応じて内部または外部になります。 |
| 物理ポート | `e0e` または `e0f` イーサネット、`0c` または `0e` FC ポートなどの、物理ネットワークポートです。物理ポートは、イーサネット、FC、または統合プロトコルをサポートします。物理ポートは、仮想ポートや論理インターフェース (LIF) をホストします。 |
| インターフェースグループ (ifgrp) | リンクアグリゲーションに使用される 1 つの論理ポートを作成するために結合された、複数の物理ポートをまとめたものです。ifgrp は、拡張スループット、冗長性、またはその両方を提供できます。 |

| 用語 | 定義 |
|---|---|
| 仮想 LAN (VLAN) | 仮想 LAN は、物理ネットワークを個別のブロードキャストドメインに分割する IEEE 802.1Q 標準プロトコルです。その結果、ルータ ( レイヤー 3) を使用して VLAN に接続しない限り、トラフィックは VLAN 間で完全に分離されます。<br>ONTAP では、VLAN によって物理ポートが複数の仮想ポートに分割されるため、安全なマルチテナントメッセージングの主要コンポーネントの 1 つであるデータの分離が可能になります。 |
| 仮想ポート | 仮想ポートは、さまざまな形式で使用できる論理ネットワークインターフェースです。<br>• ifgrp<br>• VLAN<br>• 仮想 IP ポート |
| 論理インタフェース (LIF) | LIF は、ポートに関連付けられた IP アドレスまたはワールドワイドポート名 (WWPN) です。LIF は、物理ポート (ifgrp または VLAN) に接続できます。LIF には、フェイルオーバールール、ロール、ファイアウォールルールなどの属性が関連付けられています。 |
| データ LIF | データネットワークへの接続に使用される LIF です。 |
| クラスタ間 LIF | クラスタインターコネクトネットワークへの接続に使用される LIF です。<br>クラスタのピアリング関係を確立する前に、クラスタノードごとにクラスタ間 LIF を作成する必要があります。クラスタ間 LIF は、同じノード内のポートにのみフェイルオーバーできます。 |
| 管理 LIF | 管理ネットワークへの接続に使用する LIF です。管理 LIF は、クラスタ、ノード、または SVM の管理に使用できます。 |
| クラスタ LIF | クラスタネットワークへの接続に使用される LIF です。 |
| クラスタピア | クラスタピアは、クラスタ間関係の参加者です。ONTAP データ保護サービスによるデータ移動を実行する前に、クラスタ間ピア関係を作成する必要があります。このクラスタ間関係を作成することを、クラスタピアリングと呼びます。 |
| ストレージ仮想マシン (SVM) | SVM は、ひとつ以上のデータ LIF から LUN やネットワーク接続型ストレージ (NAS) のネームスペースへのデータアクセスを提供する論理ストレージサーバです。 |
| SVM ピア | SVM ピアは、SnapMirror 関係の参加者です。ONTAP データ保護サービスによるデータ移動を実行する前に、SVM 間のピア関係を作成する必要があります。この SVM 間の関係を作成する動作を SVM ピアリングと呼びます。 |

# 2.2　ONTAP ネットワークロールの概要

ONTAP には、図 2.1 に示すように複数のタイプのネットワークがあります。各ネットワークタイプの用途を理解することが重要です。クラスタインターコネクトネットワークは、同じクラスタ内のノード間の通信とレプリケーションに使用される、高速で低レイテンシの専用プライベートネットワークです。この構成は、データへのクライアントアクセスや、クラスタ、ノード、または SVM の管理に使用または共有できない冗長バックエンドネットワークです。データへのクライアントアクセスは、データネットワーク上で行われます。クラスタ、ノード、および SVM の管理は、管理ネットワーク上で行われます。データネットワークと管理ネットワークは、同じポートまたは物理ネットワークを共有する場合があります。ただし、データネットワークと管理ネットワークは、クラスタインターコネクトネットワークとは異なる物理ネットワークである必要があります。

図 2.1　クラスタインターコネクト、データおよび管理ネットワーク

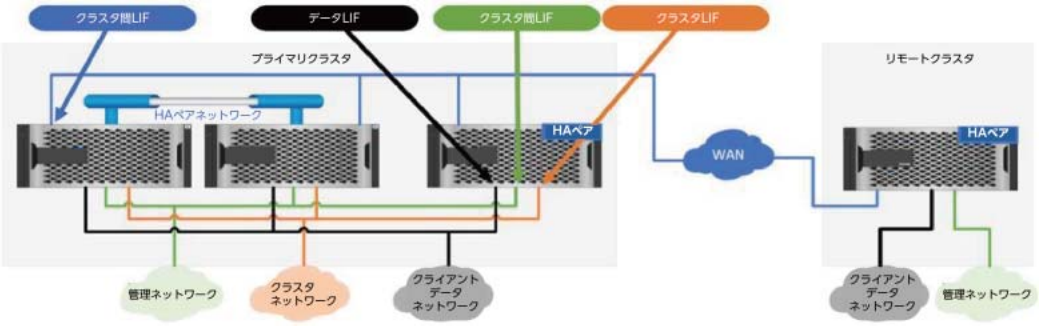



図 2.1 に示すように、地理的に離れた場所から別の場所にデータをレプリケートするためのクラスタピアリングを有効にするには、クラスタインターコネクトネットワークを構成する必要があります。クラスタインターコネクトネットワークは、IP アドレスに対応してノードへのネットワークアクセスポイントを表す LIF を使用します。クラスタ間 LIF は、クラスタのピア構成プロセスの一部として物理ポートまたは仮想ポート (ifgrp、VLAN) に割り当てられます。

# 2.3　クラスタインターコネクトネットワーク

クラスタ間 LIF の要件は次のとおりです。

- ローカルクラスタ内のすべてのノードとリモートクラスタ内のすべてのノードで、少なくとも 1 つのクラスタ間 LIF を構成する必要があります。クラスタの一部のノードのみでのクラスタ間 LIF のプロビジョニングはサポートされていません。
- クラスタ間 LIF に割り当てる IP アドレスは、データ LIF と同じサブネットまたは別のサブネットに置くことができます。クラスタ間 LIF は、割り当てられた IPspace に属するルートを使用します。ONTAP は、IPspace 内のクラスタレベル通信用のシステム SVM を自動的に作成します。
- クラスタピアリングトポロジは、フルメッシュ接続を使用する必要があります。フルメッシュ接続は、1 つのピアクラスタのすべてのクラスタ間 LIF が、他のピアクラスタのすべてのクラスタ間 LIF と通信できることを意味します。特定のリモートクラスタとの通信に使用されるすべてのポートは、同じ IPspace 内にある必要があります。複数の IPspace を使用して、複数のクラスタをピアすることができます。ペアのフルメッシュ接続は、IPspace 内でのみ必要です。また、レプリケーショントラフィックを分離するためにカスタム IPspace を使用することも検討してください。
- クラスタ間 LIF をホストしているポートに障害が発生した場合、LIF のフェイルオーバーポリシーで定義されているように、LIF はそのノード上の別のクラスタ間対応ポートにのみフェイルオーバーできます。クラスタ間のレプリケーションでは、ノードごとに少なくとも 1 つのクラスタ間 LIF が必要です。クラスタ間 LIF( 同じ Maximum Transmission Unit [MTU]、フロー制御、TCP オプションなど ) 間で一貫した設定を維持します。
- ONTAP では、FC ネットワーク経由の SnapMirror レプリケーションは使用できません。
- SnapMirror 操作はデスティネーションで行われるため、ノード障害時の SnapMirror リカバリは、障害の発生したノードの場所 ( ソースクラスタまたはデスティネーションクラスタ ) によって異なります。
  - ソースクラスタの送信ノードに障害が発生した場合、デスティネーションクラスタはソース HA ペアの正常なソースノードからの転送を再開します。
  - デスティネーションクラスタの受信ノードで障害が発生した場合、転送は中止され、新しい転送が試行され、次にスケジュールされている SnapMirror 転送まで正常に開始されない可能性があります。

クラスタインターコネクトネットワークに関する詳細は、富士通マニュアルサイトの「FUJITSU Storage ETERNUS AX/HX series データ保護パワー ガイド」を参照してください。

# 2.4　クラスタ間マルチパスとネットワーク冗長性

SnapMirror 関係に対して複数の物理パスが必要な場合があります。SnapMirror は、SnapMirror 関係に対して最大 2 つのパスをサポートします。複数のパスを使用する場合は、次のいずれかの方法で構成を設定する必要があります。

- 異なる IP 接続に異なるルートが使用されるように、スタティックルートを設定します。
- 2 つの接続に異なるサブネットを使用します。

2 つのパスは、次の 2 つのモードのいずれかで使用できます。

- **フェイルオーバーモード**
  SnapMirror は、最初に指定されたパスを目的のパスとして使用し、最初のパスに障害が発生した後にのみ、2 番目に指定されたパスを使用します。
- **多重化モード**
  SnapMirror は両方のパスを同時に使用し、基本的に転送のロードバランシングを行います。1 つのパスで障害が発生すると、残りのパスで転送が行われます。障害が発生したパスが修復されると、両方のパスを使用して転送が再開されます。

## 2.4.1　フェイルオーバーモード

多くの点で、クラスタ間 LIF はフェイルオーバーに関して CIFS または NFS で使用される LIF と同じように動作しますが、クラスタ間 LIF は異なるノードのポートにフェイルオーバーできない点が異なります。特定のポートに最初に LIF を配置すると、その LIF で使用されるポートが決まります。同じノードでフェイルオーバー用にポートが冗長化されている場合、アクティブパスは最初の LIF が配置されたポートになります。図 2.2 に示す通り、パッシブパスは LIF がフェイルオーバーする可能性のある任意のポートです。

図 2.2　フェイルオーバーマルチパス

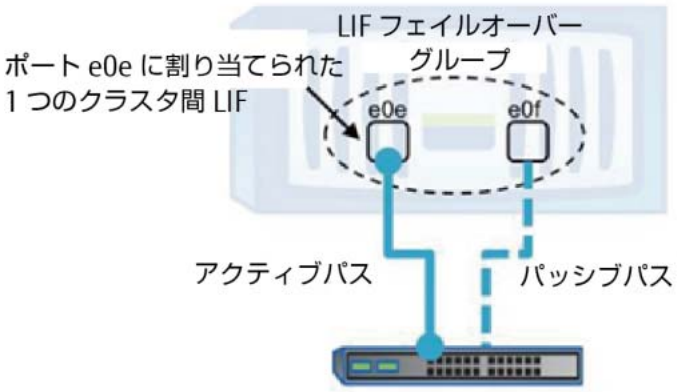
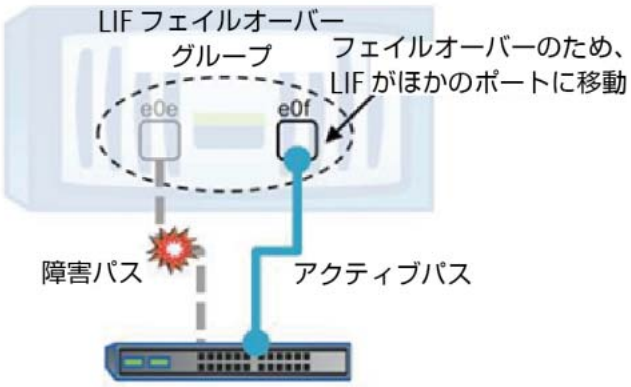


図 2.3 に示す通り、クラスタ間 LIF での通信は、LIF が割り当てられているポートでのみ行われます。ただし、そのポートで障害が発生すると、LIF はその LIF のフェイルオーバーグループ内の別の正常なポートに移動します。

図 2.3　LIF フェイルオーバー中のフェイルオーバーマルチパス



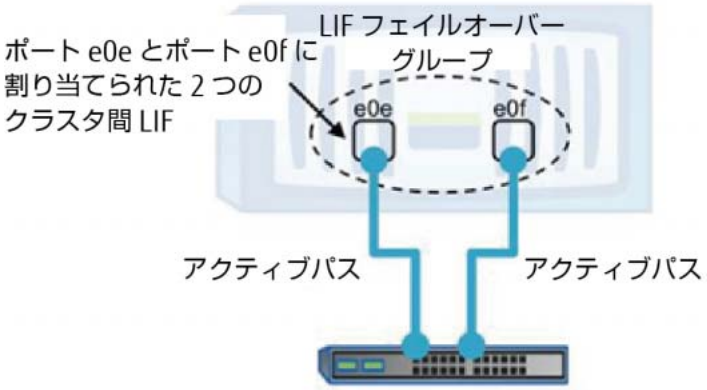

### ■ ベストプラクティス

クラスタ間 LIF をクラスタ間対応ポートに割り当て、その接続をサポートするように別のクラスタ間対応ポートが構成されていることを確認します。LIF のフェイルオーバーポリシーが、フェイルオーバーを正常に実行するために必要なポートを含むフェイルオーバーグループで構成されていることを確認します。

## 2.4.2　多重化モード

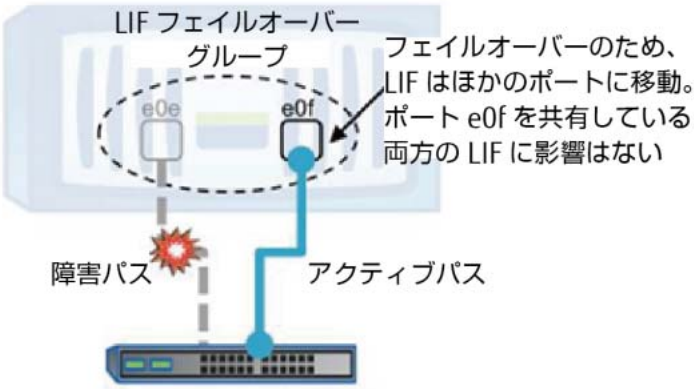
多重化モードでは、ノード上に追加のクラスタ間 LIF を構成する必要があります。SnapMirror では、ソースノードとデスティネーションノードで使用可能なすべてのクラスタ間 LIF を使用して、これらの 2 つのノード間で SnapMirror 関係を転送するすべてのデータを送受信します。図 2.4 に示す通り、2 つのクラスタ間 LIF が構成されており、2 つのポートがクラスタ間通信に使用可能な場合、1 つの LIF を各ポートに割り当てることができ、SnapMirror は、に示すように両方のポートを同時に使用します。

図 2.4　多重化モード



ネットワークのタイプと速度が異なる SnapMirror マルチパスは、高速ポートでのレプリケーションパフォーマンスに悪影響を与えることなくサポートされます。クラスタ間 LIF が各ポートに割り当てられているため、通信は両方のポートで行われます。ポートに障害が発生すると、障害が発生したポート上にあった LIF は、その LIF のフェイルオーバーグループ内の別の正常なポートに移動します。図 2.5 に示す通り、フェイルオーバーグループ内のポート数に応じて、複数の LIF がポートを共有できるようになりました。

図 2.5　多重化モードでの LIF フェイルオーバー




### ■ ベストプラクティス

2 つのクラスタ間 LIF を作成し、各ポートに 1 つの LIF を割り当てます。各 LIF フェイルオーバーポリシーが、フェイルオーバーに必要なポートを含む LIF フェイルオーバーグループを使用するように構成されていることを確認します。

## 2.4.3　マルチパスのためのスイッチベースのリンクアグリゲーション

クラスタ間 LIF は、ifgrp などの論理ポートを含む、システム内の任意の種類のポートに割り当てることができます。ifgrp は、スイッチベースのリンクアグリゲーションをサポートします。複数の物理ポートを 1 つの ifgrp に構成し、クラスタ間 LIF をその ifgrp ポートに割り当てることができます。次に、マルチパスや冗長性を提供する方法として、リンクアグリゲーションテクノロジーを使用してスイッチポートを組み合わせることができます。

スイッチベースのリンクアグリゲーションでは、ifgrp 内の複数の物理パスが同時に使用されることは保証されません。たとえば、単一のクラスタ間 LIF がソースノードとデスティネーションノードの両方に構成されているとします。したがって、各ノードには、クラスタ間通信に使用する 1 つの IP アドレスと 2 ポートの ifgrp があります。ifgrp が IP ハッシュベースの負荷分散方法を使用している場合、負荷分散ハッシュを実行するソース IP アドレスとデスティネーション IP アドレスのペアは 1 つだけです。リンクは、これらの 2 つのノード間のすべての接続を、そのポートグループ内の同じパスに配置できます。

レプリケーションは複数のノード間で実行できることに注意してください。たとえば、1 つのノードが、リモートクラスタ内の異なるノードに異なるボリュームを複製する場合があります。各ノードには、さまざまなクラスタ間 LIF があります。LIF は、ソース IP アドレスとデスティネーション IP アドレスの異なるペアを持ち、リンク内の複数のパスをそのソースノードで使用できるようにします。

スイッチベースのリンクアグリゲーションを使用して、2 つのノード間の複製時に ifgrp 内の複数の物理パスを使用できるようにする場合は、追加のクラスタ間 LIF を 2 つのノードのいずれかに構成できます。ノードごとに最大 8 つのクラスタ間 LIF を設定できます。ONTAP は、SnapMirror のソースノードとデスティネーションノードのすべての LIF 間の接続を自動的に確立します。このアプローチは、負荷分散ハッシュのソース IP アドレスとデスティネーション IP アドレスの追加の組み合わせを提供し、リンク内の異なるパスに配置できます。ただし、この例では、1 つのノードに複数の LIF を構成する目的は、任意の 2 つのノード間の複製に複数のパスを使用できるようにすることです。WAN 帯域幅は ifgrp 内の結合されたリンクの帯域幅よりも大幅に小さい可能性があるため、多くの WAN レプリケーションシナリオでは、この予防措置は必要ありません。2 つのノード間で複数のパスを有効にしても、多くのノードが WAN 帯域幅を共有しなければならないため、メリットがない場合があります。

### ■ ベストプラクティス

スイッチベースのリンクアグリゲーションを使用する場合は、`multimode_lacp` モードで ifgrp を作成し、ifgrp の分散関数を `port` に設定します。分散関数の port 値を使用すると、ifgrp は、使用されているポートだけでなく、ソース / デスティネーション IP アドレスをハッシュすることによって、パス間で接続を分散するように設定されます。この方法では、接続が ifgrp 内のすべてのパスに均等に分散されることは保証されませんが、ifgrp 内で複数の物理リンクを使用できます。

## 2.5　クラスタ間 SnapMirror のネットワーク接続

ONTAP では、クラスタ間 LIF の数によって、SnapMirror のソースノードとデスティネーションノードの間で確立される TCP 接続の数が決まります。TCP 接続は、ボリュームごとまたは関係ごとには作成されません。

ONTAP は、図 2.6 に示すように、データ送信用に少なくとも 12 のクラスタ間 TCP 接続を確立します。これは、ソースノードとデスティネーションノードの両方にクラスタ間 LIF が 1 つしかなく、ソースノードとデスティネーションノードの両方ですべてのクラスタ間 LIF が使用されるように十分な接続が作成されている場合にも当てはまります。

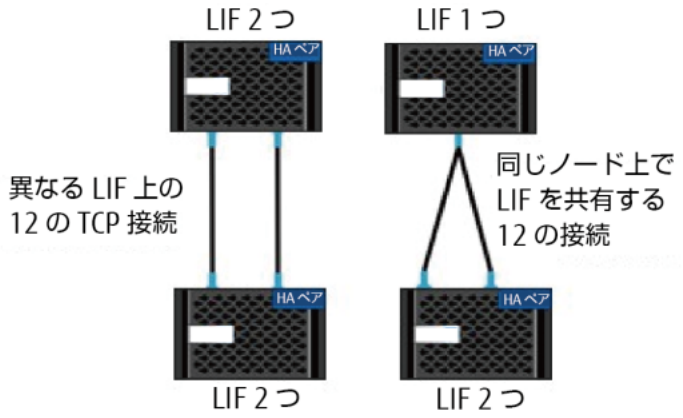
図 2.6　1 つのクラスタ間 LIF を使用した TCP 接続

ソースノード、デスティネーションノードまたは両方のノードに 2 つのクラスタ間 LIF が構成されている場合、ONTAP はデータ送信用に 12 の TCP 接続を確立します。ただし、図 2.7 に示すように、両方の接続で同じ LIF を使用するのではなく、一方の接続では一方の LIF ペアを使用し、もう一方の接続ではもう一方の LIF ペアを使用します。この例は、12 のクラスタ間 TCP 接続を生成するクラスタ間 LIFs の異なる組み合わせを示します。

**注 意**

特定の TCP 接続に使用する特定の LIF ペアを選択することはできません。これらは ONTAP によって自動的に管理されます。

図 2.7　2 つのクラスタ間 LIF を使用した TCP 接続




## ベストプラクティス

必須ではありませんが、操作の一貫性のために、同じ数のクラスタ間 LIF をソースノードとデスティネーションノードの両方で構成できます。複数のクラスタ間 LIF を作成して、複数の物理パスにわたってアクティブ - アクティブマルチパスを有効にできます。
たとえば、ノードがクラスタ間レプリケーション用の 4 つの 1 ギガビットイーサネット (GbE) ポートで構成されている場合、4 つのクラスタ間 LIF が必要です。各ポートに 1 つずつ割り当てて、1 つの GbE リンクを超える帯域幅を提供するためにすべてのパスが使用されるようにします。

# 2.6　ポートを共有または専用にする

クラスタ間通信に専用ポートを使用することも、データネットワークで使用されるポートを共有することもできます。クラスタ間の LIF を専用データポートを使用するように構成すると、共有データポートを使用する場合よりも広い帯域幅を使用できます。データポートを共有するようにクラスタ間 LIF を構成すると、既存のデータポートを使用できますが、このネットワークをクライアントから物理的に分離することはできません。このように構成した場合、管理者は、ルーティングルールまたはデータセンターファイアウォール ( クラスターの外部 ) が、一般クライアントがクラスタ間 LIF で使用される IP アドレスに到達したり、クラスタ間トラフィックを参照したりできないように設定されていることに注意する必要があります。

レプリケーション用にポートを共有するか専用にするかを決定する際には、いくつかの構成と要件を考慮する必要があります。これには以下のものがあります。

- **LAN タイプ**
  10GbE、25GbE、40GbE、100GbE などの高速ネットワークを使用する場合は、データアクセスに使用する 10GbE ポートと同じ 10GbE ポートを使用してレプリケーションを実行するために十分なローカル LAN 帯域幅が必要です。使用可能な WAN 帯域幅と LAN 帯域幅を比較する必要があります。使用可能な WAN 帯域幅が 10GbE より大幅に少ない場合は、WAN がサポートできるネットワーク使用率に制限されることがあります。
- **使用可能な WAN 帯域幅 (LAN 帯域幅との比較 )**
  使用可能な WAN 帯域幅が LAN 帯域幅よりも大幅に少ない場合、WAN はスロットルとして機能します。利用可能な WAN 帯域幅が 10GbE より大幅に少ない場合は、専用ポートを使用する必要があります。

  **注 意**

  このルールの唯一の例外は、クラスタ内のすべてまたは多数のノードがデータを複製する場合です。この場合、帯域幅の使用率は通常、複数のノードに分散されます。

- **レプリケーション間隔**
  使用可能な帯域幅で、レプリケーション間隔中のクライアントアクティビティのレベルをどのように処理するかを検討します。本番以外の時間帯のレプリケーションは、データネットワークに無関係な影響を与える可能性があります。ピーク時以外にレプリケーションを実行する場合は、10GbE LAN 接続がなくても、データポートをレプリケーションに使用できます。ただし、レプリケーションが通常の業務時間内に行われる場合は、レプリケートされるデータの量と、データプロトコルとの競合が発生するほどの帯域幅が必要かどうかを考慮する必要があります。データプロトコル (SMB、NFS、iSCSI) によるネットワーク使用率が 50% を超える場合は、ノードのフェイルオーバーが発生したときでもパフォーマンスが低下しないように、クラスタ間通信に専用のポートを使用する必要があります。
- **レートの変更**
  各インターバルでレプリケートされるデータの量と、共有データポートのデータプロトコルとの競合が発生するほどの帯域幅が必要かどうかを考慮します。レプリケーションにピア関係を使用し、クライアントの動作が最小限またはまったく発生しない場合にのみレプリケーションが実行されるように設定されている場合は、10GbE LAN 接続がなくても、データポートを使用してクラスタ間レプリケーションを正常に実行できる場合があります。

- **ポートの数**
  複製トラフィックがデータトラフィックに干渉していると判断した場合は、クラスタ間 LIF を同じノード上の他のクラスタ間対応の共有ポートに移行できます。VLAN ポートをレプリケーション専用にすることもできます。ポートの帯域幅は、すべての VLAN とベースポートの間で共有されます。ただし、レプリケーション専用のポートには、追加のスイッチポートとケーブル配線が必要です。

**注 意**

- クラスタ間通信専用のポートを使用する場合は、ノードごとに少なくとも 2 つのクラスタ間ポートを構成することをお勧めします。クラスタ間 LIF は別のノードのポートにフェイルオーバーできません。そのフェイルオーバーグループには、同じノード上のクラスタ間対応のポートだけが含まれます。クラスタ間ポートを使用する場合、ONTAP はクラスタ間 LIF のフェイルオーバーグループのクラスタ間ポートだけを使用します。したがって、クラスタ間ポートを使用する場合は、クラスタ間 LIF がフェイルオーバーできるポートが存在するように、ノードごとに少なくとも 2 つのクラスタ間ポートを構成する必要があります。
- 専用ポートを使用しない場合、通常、複製ネットワークの最大転送単位 (MTU) サイズはデータネットワークの MTU サイズと同じにする必要があります。

## ■ ベストプラクティス

- データプロトコル (CIFS、NFS、iSCSI) によって生成されるネットワーク使用率が 50% を超える場合は、ノードのフェイルオーバーが発生したときにパフォーマンスが低下しないように、クラスタ間通信用にポートを専用にする必要があります。
- クラスタ間の LIF は、ノードスコープです ( 同じノード上の他のポートにのみフェイルオーバーします。)。したがって、クラスタ間 LIF の命名規則を使用して、ノード名の後に、クラスタ間 LIF の `ic` または `icl` が続くようにします。たとえば、好みに応じて `node_name_icl#` または `node-name-ic#` とします。
- 関連するすべてのポートが、ポートフェイルオーバー後の通信を許可するために必要なネットワークまたは VLAN にアクセスできることを確認します。
- クラスタ間の LIF が使用可能または使用不可になると、アクティブ IP アドレスのリストが変更される可能性があります。アクティブな IP アドレスの検出は、ノードの再起動時など、特定のイベントで自動的に行われます。`-peer-addrs` オプションでは、リモートクラスタアドレスを 1 つだけ指定する必要があります。ただし、そのアドレスをホストしているノードが停止して使用できなくなった場合は、クラスタピア関係が再検出されないことがあります。したがって、リモートクラスタ内の各ノードから少なくとも 1 つのクラスタ間 IP アドレスを使用して、ノードに障害が発生してもピア関係が安定するようにします。

# 2.7　ファイアウォール要件

SnapMirror は、TCP ソケット上で一般的なソケット、バインド、待機、および受け入れシーケンスを使用します。ファイアウォールとクラスタ間ファイアウォールポリシーでは、次のプロトコルを許可する必要があります。

- ポート 10000、11104、および 11105 上のすべてのクラスタ間 LIF の IP アドレスへの TCP です。ONTAP は、ポート 11104 を使用してクラスタ間通信セッションを管理し、ポート 11105 を使用してデータを転送します。
- クラスタ間 LIF 間の双方向 HTTPS です。
- CLI を使用してクラスタピアリングを設定する場合は HTTPS は必要ありませんが、ONTAP System Manager を使用して DP を設定する場合は、後で HTTPS が必要になります。

# 第 3 章
# レプリケーションの基本

## 3.1 ライセンス

SnapMirror ライセンスを購入して有効にする必要があります。このライセンスは、Data Protection Bundle に含まれています。SnapMirror のソースとデスティネーションが異なるクラスタ上にある場合は、各クラスタで SnapMirror ライセンスを有効にする必要があります。各クラスタのすべてのノードにライセンスが必要です。

## 3.2 SnapMirror 非同期テクノロジー

SnapMirror は、Snapshot コピーを使用して、クラスタ内のソース FlexVol またはソース FlexGroup をデスティネーションクラスタのボリュームに複製します。SnapMirror は次の操作を実行します。

手順 ▶▶▶

1. ソース上のデータの Snapshot コピーが作成されます。
2. Snapshot コピーは、ベースライン同期中にデスティネーションにコピーされます。このプロセスでは、直近の共通 Snapshot コピー時に、ソースと同じデータを含む、オンラインで読み取り専用のデスティネーションが作成されます。
3. デスティネーションが更新され、指定したスケジュールに従ってソースの増分変更が反映されます。

◀◀◀

SnapMirror 関係が確立されると、デスティネーションボリュームは、Snapshot、ボリューム設定、および ONTAP 領域効率機能を含む、ソースの同一のレプリカになります。SnapMirror と Vault の関係では、ターゲットに指定したソース Snapshot のコピーだけをデスティネーションクラスタ上のボリュームにレプリケートします。SnapMirror 関係を解除するとデスティネーションボリュームは書き込み可能になり、通常は SnapMirror を使用して DR 環境にデータを同期するときにフェイルオーバーを実行するために使用されます。SnapMirror は高度な機能を備えているため、フェイルオーバーサイトで変更されたデータを、オンラインに戻ったときにプライマリシステムに効率的に再同期させることができます。その後、元の SnapMirror 関係を再確立できます。

SnapMirror は、いずれかのレプリケーションエンジンを使用してレプリカを作成できます。どちらのエンジンもボリュームレベルで動作しますが、特性が異なります。

- **ブロックレプリケーションエンジン (BRE)**
  BRE は、ソースボリュームからデスティネーションボリュームに、ドライブ上のレイアウトを全体として、または 4K ブロックの増分更新として複製します。つまり、BRE はファイルシステムの知識を使用して、ブロック割り当てレベルで Snapshot 間の違いを判別し、変更されたブロックのみを複製します。したがって、デスティネーション上に作成されたデータのコピーは、ソース上の元のデータセットへの物理ブロックポインタと同じ構造を持ちます。BRE は、ボリュームブロック (VVBN) の読み取りおよび書き込み操作を使用してボリュームをレプリケートします。SnapMirror 関係は、SnapMirror ポリシータイプ `async-mirror` を使用して、`-type DP` で作成されます。

  **注 意**

  9.11.1 の時点では、BRE SnapMirror 関係は、BRE 関係の長期的な廃止プログラムの一部として、従来のデータ保護ポリシーにのみ使用されます。将来のある時点で BRE はサポートされなくなり、BRE SnapMirror 関係をホストしている ONTAP システムは、これらの BRE 関係が LRSE (XDP) に変換されるまで、将来のバージョンの ONTAP にアップグレードできなくなります。

- **ストレージ効率の高い論理レプリケーション (LRSE)**
  LRSE は、ブロックレベルのメタデータとファイルシステムの知識を使用して、Snapshot コピー間の差分を間接ポインタレベルで特定します。LRSE は、ソースからデスティネーションへのデータ転送を 2 つのストリームに編成します。
  - データストリームは、FlexVol 内の特定のボリュームブロック番号 (vvbn#) で転送されるデータブロックで構成されます。この番号は、ファイルコンテキストを指定せずに、データがソース FlexVol ボリュームに格納されるブロック番号を識別するのに役立ちます。デスティネーションでは、vvbn# に対応するファイルブロック番号 (fbn#) を使用して、データがデータウェアハウス (DW) ファイルに書き込まれます。
  - ユーザーファイルは、データウェアハウスファイルとブロックを共有し、特定のオブジェクトに到達するために解析を必要とするバッファツリーを使用しないユーザーファイル inode を使用して、参照によって転送されます。LRSE は、レプリケーション転送の進行中に、DW ブロック ( ドナー ) のブロック共有インフラストラクチャに対して、ユーザーファイル ( レピシエント ) を使用して明示的な要求を行います。

  ミラーは、ソースとはまったく異なるドライブ上の物理レイアウトを持つ元のデータセットへの論理ブロックポインタの構造を持ちます。SnapMirror 関係は次のもので作成されます。SnapMirror ポリシータイプ `async-mirror`、`vault`、または `mirror-vault` を使用した `-type XDP`。

LRSE は、ブロックレベルのメタデータとファイルシステムの知識を使用して、Snapshot コピー間の差分を間接ポインタレベルで特定します。LRSE では、ブロックの共有や圧縮などの機能により、使用されている容量よりもはるかに多くのデータをボリュームに効率的に保持できるため、ストレージ効率が重要です。この効率性は、レプリケーション中に維持する必要があります。これは、レプリカを転送するために必要な時間はもちろん、レプリカが許容できないほど大きなサイズになるのを防ぐためです。また、LRSE を使用すると、プライマリストレージの設定に関係なく、セカンダリストレージにストレージ効率を適用できます。

LRSE では、プライマリストレージとセカンダリストレージのストレージ効率が非対称になるだけでなく、デスティネーションバージョンがソースと異なる場合でも、バージョンの柔軟性が確保されます。また、デスティネーションがソースよりも多くの Snapshot コピーをサポートできる非対称 Snapshot コピーもサポートします。ソースファイルシステム内のすべてのファイルとディレクトリがデスティネーションファイルシステムに作成されます。したがって、古いバージョンの ONTAP を実行しているストレージシステムと、新しいバージョンを実行しているストレージシステムの間でデータをレプリケートできます。このアプローチでは、オーバーヘッドを削減し、複雑なトポロジー ( ファンイン、ファンアウト、カスケード ) を管理しながら、どちらの側のコントローラも無停止でいつでもアップグレードできるため、ダウンタイムを短縮できます。

パフォーマンス特性も元のブロックレプリケーションエンジンと似ています。これは、レプリケーションエンジンが、2 つの Snapshot コピー間の差分だけをプライマリからセカンダリに転送するためです。この増分のみの転送により、ストレージとネットワーク帯域幅が節約されます。SnapMirror のデフォルトのデータ保護(DP)モードは、SnapMirrorの拡張データ保護(XDP)モードに置き換わりました。

SnapMirror を SnapCenter と統合して、エンタープライズデータベースアプリケーションで使用される Snapshot など、アプリケーションと一貫性のある Snapshot を複製することもできます。Snapshot コピーは、アプリケーションと連携して作成されます。これにより、実行中のI/O処理によってSnapshot に不整合が発生しないことが保証されます。アプリケーションと整合性のとれた Snapshot コピーを作成した後、SnapCenter は、これらの Snapshot コピーの SnapMirror レプリケーションをセカンダリストレージシステムにトリガーできます。

## 3.2.1　統合データ保護

SnapMirror ユニファイドレプリケーションでは、SnapMirror の強力な機能と SnapVault テクノロジーと同じ ( 統一した ) 論理レプリケーションエンジンを組み合わせて、DR と同じデスティネーションへのアーカイブを目的とすることにより、シンプルで効率的なレプリケーションによってミッションクリティカルなビジネスデータを保護できます。統合関係タイプは XDP と呼ばれ、単一のベースライン機能を提供します。これにより、ストレージとネットワークの帯域幅が大幅に削減され、即座にコスト削減につながります。SnapMirror ユニファイドレプリケーションの主なメリットは次のとおりです。

- セカンダリストレージに必要なボリュームのベースラインコピーは 1 つだけです。ユニファイドレプリケーションを使用しない場合、SnapMirror と SnapVault はそれぞれ独自のベースラインコピーを必要とします。
- プライマリとセカンダリの間で必要なネットワークトラフィックが少なくて済みます (1 つのベースラインに加え、Snapshot コピーの数が徐々に減ります )。
- 稼働中の異なる ONTAP リリースのストレージシステム間でのレプリケーションの柔軟性。DP SnapMirror では、デスティネーションのリリース版数はソースと同じかそれ以降である必要があります。ユニファイドレプリケーションでは、ソースとデスティネーションの両方が ONTAP 9.7 以降の場合、前のリリースから後のリリースへ、および後のリリースから前のリリースへ複製できます。
- プライマリからセカンダリへのレプリケーションの破損を防ぐために、ユニファイドレプリケーションでは、使用可能な Snapshot コピーからプライマリボリュームをリカバリできます。

全体として、SnapMirror を使用したユニファイドレプリケーションは、仮想化のための強力なデータ管理機能を提供し、重要なデータを保護すると同時に、場所とストレージ階層間（クラウドサービスプロバイダなど）でデータを移動する柔軟性を提供します。SnapMirror 関係は、XDP タイプ、ポリシータイプ（`mirror-vault`）、および定義済みポリシー（`Asynchronous`）で作成されます。特定の Snapshot コピーをバックアップするためのカスタムルールを含めるように、ポリシーをいつでも変更できます。XDP では、ソースコントローラのメジャーバージョン以上の ONTAP メジャーバージョン番号を必要とするデスティネーションコントローラの制限がなくなり、無停止アップグレードが可能になります。さらに、この機能により、デスティネーションで必要なセカンダリ Snapshot コピーの数が削減されます。

次の例は、CLI から MirrorAndVault ポリシーを使用してユニファイドレプリケーションを構成する方法を示します。

```
cluster02::> snapmirror create -source-path snap_src1:Source -destination-path
svm_dst1:Source_dest -type XDP -policy Asynchronous
```

ONTAP 9.8 System Manager 以降では、SnapMirror Asynchronous を構成すると、デフォルトで非同期保護ポリシーが選択されます。ポリシーパラメータを変更するには、カスタムポリシーを作成する必要があります。カスタムポリシーを作成するには、[Protection] > [Overview] > [Local Policy Settings] > [Protection Policies] > [Add] に移動します（図 3.1 および図 3.2）。

## ベストプラクティス

フルミラーを維持することのメリットと、セカンダリストレージの容量の削減、ベースライン転送数の制限、ネットワークトラフィックの削減によってユニファイドレプリケーションが提供するメリットを比較検討する必要があります。ユニファイドレプリケーションの適切性を判断するうえで重要な要素は、アクティブなファイルシステムの変更率です。たとえば、従来のミラーは、データベーストランザクションログの 1 時間ごとの Snapshot コピーを保持するボリュームに適しています。

図 3.1　SnapMirror カスタム保護ポリシーの作成

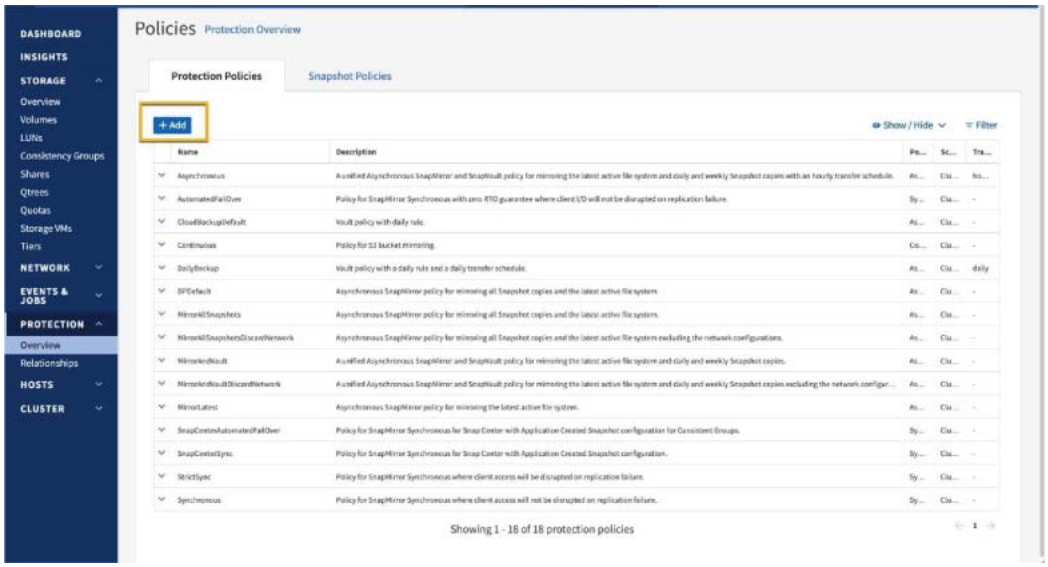
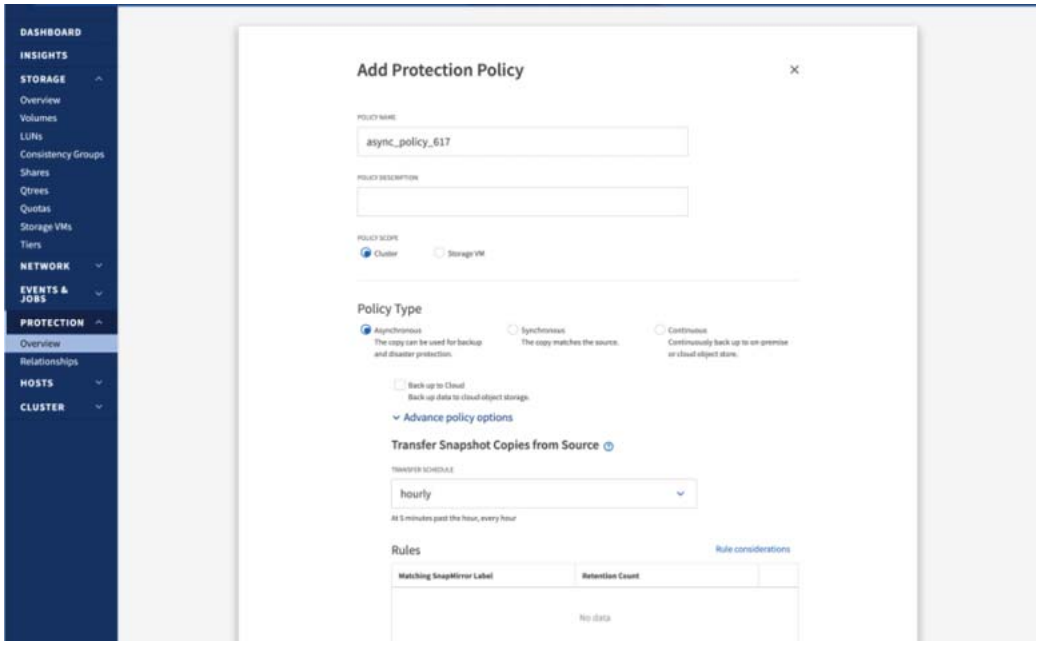


図 3.2　カスタム SnapMirror 保護ポリシーの追加




## 3.2.2　負荷分散ミラー

NAS 環境のすべての SVM には、固有のネームスペースがあります。SVM ルートボリュームは、このネームスペース階層へのエントリポイントです。2 つ以上の HA ペアで構成されるクラスタでは、HA ペアの両方のノードに障害が発生した場合でもクライアントがネームスペースにアクセスできるように、SVM ルートボリュームの負荷分散ミラーを考慮する必要があります。負荷分散ミラーは、単一の HA ペアで構成されるクラスタには適しておらず、MetroCluster 環境にも適していません。

**注 意**

- 負荷分散ミラーはデータボリュームでは使用されず、SVM ルートボリュームでのみサポートされます。
- SnapMirror 負荷分散ミラーは、NAS (CIFS/NFSv3) のみをサポートします。負荷分散ミラーは、NFSv4 クライアントまたは SAN クライアントプロトコル接続 (FC、FCoE、iSCSI など ) をサポートしていません。ただし、NFSv4 と負荷分散ミラーは同じ環境で使用できます。NFSv4 は負荷分散ミラーを使用しません。代わりに、常にソースボリュームが使用されます。

### ■ ベストプラクティス

クラスタのセカンド HA ペアのノード上でのみ、SVM ルートボリュームの負荷分散ミラーを作成します。

### 3.2.3　SnapMirror Synchronous (SM-S)

SM-S は、LAN またはメトロポリタンエリアネットワーク (MAN) 経由でソースボリュームとデスティネーションボリュームの間でデータを同期的に複製する、使いやすい DR ソリューションです。

SM-S は、プライマリサイトやクラスタの障害によってデータが消失することなく、ビジネスクリティカルなアプリケーションに高いデータ可用性と迅速な DR を提供します。

SM-S は、SnapMirror Asynchronous とは異なるメカニズムでボリュームデータを転送します。詳細については関連マニュアルに記載されています。詳細は、富士通マニュアルサイトの「Fujitsu Storage ETERNUS AX/HX series SnapMirror Synchronous 構成とベストプラクティス ONTAP 9.11.1」を参照してください。

## 3.3　SnapVault テクノロジー

SnapVault は、標準的なコンプライアンスやその他のガバナンス関連の目的のために、ドライブからドライブへの Snapshot のコピーレプリケーション用に設計されたバックアップテクノロジーです。通常、デスティネーションにはソースボリューム内の現在のSnapshotコピーのみが含まれるSnapMirrorとは対照的に、SnapVaultは通常、はるかに長期間にわたって作成されたポイントインタイムSnapshotコピーを保持します。たとえば、政府の会計規則に準拠するために、データの Snapshot コピーを 20 年間にわたって毎月保存することができます。ヴォールトストレージからデータを提供する必要がないため、デスティネーションシステムでは低速で低コストのドライブを使用できます。SnapVault テクノロジーは、LRSE も使用します。LRSE は、`vault` および `XDPDefault`（事前定義）というポリシータイプと組み合わせて、拡張データ保護 (XDP) 関係と呼ばれる、バージョンに依存しないバックアップレプリケーションの柔軟性を提供します。富士通システムで SnapVault 機能を有効にするには、ソースクラスタとデスティネーションクラスタの両方にSnapMirrorライセンスをインストールする必要があります。

SnapVault バックアップにボリュームをバックアップするには、次の手順を実行する必要があります。

**手順 ▶▶▶**

1. **ベースライン転送を開始します。**
   SnapMirror と同様に、SnapVault は初回起動時にベースライン転送を実行します。SnapMirror ポリシーは、ベースラインの内容と更新を定義します。デフォルトの SnapVault ポリシー (`XDPDefault`) に基づくベースライン転送では、ソースボリュームの Snapshot コピーが作成され、そのコピーと、ソースボリュームが参照するデータブロックがデスティネーションボリュームに転送されます。SnapMirror とは異なり、SnapVault は古い Snapshot コピーをベースラインに含めません。

2. **スケジュールされた増分転送を実行します。**
   更新は非同期であり、設定したスケジュールに従います。SnapMirror ポリシーで定義するルールによって、更新に含める新しい Snapshot コピーと、保持するコピーの数が決まります。ポリシー ( 例えば毎月 ) で定義されたラベルは、ソースの Snapshot ポリシーで定義された 1 つ以上のラベルと一致する必要があります。それ以外の場合、レプリケーションは失敗します。`XDPDefault` ポリシーの下で更新が行われるたびに、SnapMirror は最後の更新以降に作成された Snapshot コピーを転送します。ただし、それらのコピーにポリシールールで定義されているラベルと一致するラベルがあることが条件です。

3. **SnapVault の共通 Snapshot コピーを更新します。**
   複数の Snapshot コピーの転送を含む各 Snapshot コピー転送セッションの最後に、SnapVault バックアップ内の最新の増分 Snapshot コピーが使用されて、プライマリボリュームとセカンダリボリューム間に新しい共通ベースが確立され、アクティブなファイルシステムとしてエクスポートされます。

4. **要求に応じてデータをリストアします。**
   データをプライマリボリュームまたは新しいボリュームにリストアする必要がある場合、SnapVault セカンダリは指定されたデータを SnapVault バックアップから転送します。

◀◀◀

# 3.4 Cloud Volume プラットフォーム用 SnapMirror

SnapMirror を使用して、オンプレミスまたはクラウドホストの ONTAP ボリュームと SVM のデータ保護を提供できます。富士通は、Google、Amazon、および Microsoft と協力して、総合的なデータ管理ファブリックとして使用できる、幅広い ONTAP クラウド製品を提供しています。次のセクションでは、SnapMirror での使用がサポートされている各製品について説明します。

## 3.4.1 Cloud Volumes ONTAP

Cloud Volumes ONTAP は、パフォーマンスとコストを最適化したクラウドストレージを、オンプレミスの ONTAP データ管理と組み合わせて使用できるようにします。Cloud Volumes ONTAP は、クラウドプロバイダ固有のコンピューティング、ストレージ、およびネットワーク製品を基盤として、幅広い ONTAP API とデータ管理サービスを提供しています。Cloud Volumes ONTAP のサービスは、アマゾンウェブサービス (AWS) 、Microsoft Azure、Google Cloud から利用できます。

## 3.4.2 Amazon FSx for ONTAP

Amazon FSx for ONTAP は、完全に管理された ONTAP をサービスとして提供するネイティブの AWS サービスで、Cloud Manager または AWS Management Console、AWS CLI、REST API などの管理ツールの AWS スイートを通じて管理できます。Amazon FSx for ONTAP クラスタを設定すると、別の Amazon FSx for ONTAP、Cloud Volumes ONTAP、または ONTAP オンプレミスクラスタとの SnapMirror 関係で、ソースクラスタまたはデスティネーションクラスタとして使用できます。

# 第 4 章
# SnapMirror 構成

## 4.1 クラスタピアリング

ONTAP のクラスタピアリング機能を使用すると、独立したクラスタの管理者はクラスタ間でピア関係を確立できます。クラスタインターコネクトネットワークを使用して、クラスターがアプリケーションデータ、構成情報、および座標操作を安全に交換できるようにするネットワーク接続を定義できます。クラスタ間 LIF の役割は、クラスタ間トラフィックを処理するインターフェイスです。管理者は、クラスタ間通信で使用するネットワーク上のアドレス範囲を定義し、これらのアドレスのルーティングを調整し ( たとえば、ルーティンググループ別 )、この役割の LIF をクラスタ間ポートまたはデータポートに割り当てる必要があります。クラスタ間 LIF を作成し、クラスタインターコネクトネットワークを構成した後、SnapMirror を使用して別のクラスターとの間でレプリケーションを行うためのクラスターピアを作成できます。ピア関係は、1 つのクラスタに対して最大 255 のリモートクラスタと構成できます。

クラスタピアリングを設定する前に、接続、ポート、IP アドレス、サブネット、ファイアウォール、およびクラスタの名前付けの要件が満たされていることを確認する必要があります。クラスタピアリングの要件は次のとおりです。

- ピアリングが成功するためには、クラスタ上の時間が 300 秒 (5 分 ) 以内に同期している必要があります。クラスタピアは異なるタイムゾーンに存在できます。
- クラスタ内のすべてのノードに、少なくとも 1 つのクラスタ間 LIF を作成する必要があります。
- ローカルクラスタ IPspace のすべてのクラスタ間 LIF は、リモートクラスタ IPspace のすべてのクラスタ間 LIF と通信できなければなりません。
- すべてのクラスタ間 LIF には、クラスタ間複製専用の IP アドレスが必要です。
- ポートの MTU 設定は一貫している必要があります。デフォルト値の 1,500 は、ほとんどの環境に適しています。
- クラスタ間複製に使用されるノード上のすべてのパスは、同じパフォーマンス特性を持つ必要があります。

**注 意**

- クラスタピアリングの要件の詳細については、富士通マニュアルサイトの「FUJITSU Storage ETERNUS AX/HX series クラスタ /SVM ピアリング パワーガイド」を参照してください。
- SnapMirror はネットワークアドレス変換 (NAT) をサポートしていません。

クラスタピアリングの確立は、クラスタ管理者が実行する必要がある 1 回限りの操作です。クラスタピア関係とは、実際には、異なるクラスタ内の構成オブジェクトの 2 つの対応する集合にすぎません。したがって、1 つのクラスタに含まれるクラスタピア関係は、クラスタピア関係全体の半分にすぎません。クラスタピア関係が完全であると見なされ、正しく機能するためには、各クラスタがその構成の一部をピアと共有する必要があります。クラスタピア関係は、2 つのクラスタ間に正確に存在します。

ピア関係は、いくつかの方法で作成できます。

- 1 つ目の方法では、ピア関係は、リモートクラスタのセキュリティ資格情報 ( クラスタ管理ログインとパスワード ) を持つクラスタ管理者によって作成されます。

- もう 1 つの方法では、クラスタ管理パスワードを交換しない 2 人の管理者がクラスタをピア接続できます。この方法では、各管理者は、他のクラスタのクラスタ間 IP アドレスを指定する `cluster peer create` コマンドを入力します。
- `-generate-passphrase` 機能を使用して、事前にクラスタ間 LIF IP アドレスがわからないクラスタとピア関係を作成できます。これにより、開始クラスタがリモートクラスタで自身を認証する必要がなくなります。

1 つのクラスタを最大 255 のクラスタとピア関係にすることができ、複数のクラスタ間での複製が可能になります。

`-generate-passphrase` 機能を使用して、事前にクラスタ間 LIF IP アドレスがわからないクラスタとピア関係を作成できます。これにより、開始クラスタがリモートクラスタで自身を認証する必要がなくなります。

ONTAP 9.7 以降、クラスタピアリングでは暗号化された通信が使用されるようになりました。つまり、作成される SnapMirror 関係では、TLS 暗号化による追加のセキュリティ層が使用されます。

### ■ ベストプラクティス

ソースシステムの名前と IP アドレスは、デスティネーションシステムの `hosts` ファイルに含まれている必要があります。また、デスティネーションシステムの名前と IP アドレスは、ソースシステムの `hosts` ファイルに含まれている必要があります。あるいは名前と IP アドレスはネットワークベースの DNS サーバで解決できる必要があります。

## 4.2　SVM ピアリング

SVM ピアリングは、2 つの SVM を接続して、SVM 間でのレプリケーションを可能にします。これには、最初にクラスタのピアリングが必要です。SVM ピアリングを使用すると、アクセスの細分性や、さまざまなレプリケーション操作の SVM 管理者への委任が可能になります。

### ■ ベストプラクティス

一意の完全修飾ドメイン名 (FQDN) を使用して SVM に名前を付けます。
例 :`dataVserver.HQ` または `mirrorVserver.Offsite`。
SVM ピアリングには一意の SVM 名が必要であり、FQDN 命名スタイルを使用すると、一意性の確立が非常に簡単になります。

クラスタピアリングの要件の詳細については、富士通マニュアルサイトの「FUJITSU Storage ETERNUS AX/HX series クラスタ /SVM ピアリング パワーガイド」を参照してください。

# 4.3 SnapMirror 関係

プライマリストレージのソースボリューム ( たとえば、FlexVol ボリュームや FlexGroup ボリューム ) とセカンダリストレージのデスティネーションの間に作成される関係を、データ保護関係と呼びます。SnapMirror 関係の作成は、IP アドレス解決のための SVM ホスト名に依存しません。ただし、クラスタ名はクラスタピア関係によって解決され、SVM 名はクラスタによって内部的に解決されます。ソース SVM、デスティネーション SVM、およびクラスタのホスト名は、ONTAP で SnapMirror 関係を作成するために使用されます。クラスタ間 LIF の IP アドレスを使用する必要はありません。

**注 意**

ピア関係は、同じクラスタ内の 2 つの SVM 間、または同じ SVM 内の 2 つのボリューム間でデータをミラーリングするためには必要ありません。

SnapMirror 関係には次の特性があります。

- SnapMirror 関係は、デスティネーションクラスタで作成および管理されます。
- SnapMirror 関係転送は、デスティネーションクラスタのスケジューラによってトリガーされます。
- SnapMirror 初期化を成功させるには、DP のボリュームタイプ (`-type DP`) でデスティネーションボリュームを作成する必要があります。ボリュームの作成後にボリュームの `-type` プロパティを変更することはできません。
- SnapMirror 関係のデスティネーションボリュームは、フェイルオーバーが行われるまで読み取り専用です。
- SnapMirror ブレーク操作を使用してセカンダリコピーにフェイルオーバーし、デスティネーションボリュームを書き込み可能にできます。SnapMirror ブレークは、ボリュームごとに個別に実行する必要があります。
- デスティネーションボリュームは、読み取り専用のまま SVM 名前空間にマウントできますが、最初の転送が完了した後にのみマウントできます。
- 2 つのクラスタ間に構成された SnapMirror 関係の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じネームスペースにマウントできません。これは、クラスタ間の関係が異なるクラスタにある ( 異なるネームスペースである異なる SVM に存在する ) ためです。ただし、ソースボリュームとデスティネーションボリュームの両方が同じ SVM に存在する場合は、クラスタ内で構成された SnapMirror 関係のデスティネーションボリュームを、ソースボリュームと同じ名前空間にマウントできます。ただし、同じマウントポイントにマウントすることはできません。
- ミラーデスティネーションボリュームに含まれる LUN は、イニシエータグループ (igroup) にマッピングしてクライアントに接続できます。ただし、クライアントが読み取り専用 LUN への接続をサポートできる必要があります。
- データ保護ミラー関係は、ONTAP CLI、ONTAP System Manager、および Active IQ Unified Manager を使用して管理できます。
- 進行中の転送がネットワークの停止によって中断されたり、管理者によって中止されたりした場合、その転送の後続の再開は、保存された再開チェックポイントから自動的に継続されます。

クラスタ間 SnapMirror 関係を作成する前に、次の要件を満たしてください。

- クラスタインターコネクトネットワークのソースノードとデスティネーションノードを構成します。
- ソースクラスタとデスティネーションクラスタをクラスタピア関係で設定します。

- ソース SVM とデスティネーション SVM の両方で異なる言語タイプを使用できますが、ソースボリュームとデスティネーションボリュームの言語タイプは同じである必要があります。
- ソース SVM とデスティネーション SVM を SVM ピア関係で設定します。
- レプリケートされたボリュームと、構成された保護ポリシーによって保持される Vault Snapshot コピーをホストするのに十分な領域が、デスティネーションアグリゲートに必要です。
- ユーザーアクセス、認証、およびクライアントアクセスに関する環境の要件を満たすように、両方のクラスタを適切に構成および設定する必要があります。
- レプリケートされたボリュームと、構成された保護ポリシーごによって保持される Vault Snapshot コピーをホストするのに十分な領域を確保した、`- type DP` のデスティネーションボリュームを作成します。
- デスティネーションクラスタ内の SnapMirror 関係にスケジュールを割り当てて、定期的な更新を実行します。既存のスケジュールのいずれかが適切でない場合は、新しいスケジュールエントリーが作成できます。
- 保護ポリシー ( デフォルトまたはカスタム ) を SnapMirror 関係に割り当てます。

SnapMirror 関係は、次のいずれかの設定で作成できます。

- **クラスタ間**
  ONTAP で動作する異なるクラスタ内の 2 つの異なる SVM 内のボリューム間のレプリケーション。これらは主に、別のサイトまたは場所に DR を提供するために使用されます。
- **クラスタ内**
  同じクラスタ内の異なる SVM 内の 2 つのボリューム間、または同じ SVM 内の 2 つのボリューム間のレプリケーション。これらは主に、ローカルバックアップコピーの管理に使用されます。

## ■ ベストプラクティス

- 既存の SnapMirror 関係からデスティネーションボリュームを再利用しないでください。新しい SnapMirror 関係を開始するには、常に新しく作成したボリュームを使用します。
- データをデスティネーションにコピーする前に、SnapMirror がソースボリュームに作成する Snapshot コピーを削除しないでください。最新の SnapMirror Snapshot コピーは、最新の共通 Snapshot コピー (NCS) と呼ばれます。デスティネーションに対する増分変更は、NCS によって異なります。SnapMirror は、ソース上で必要な Snapshot コピーを見つけられない場合、デスティネーションに対して差分変更を実行できません。
- デスティネーションのデータ保護 FlexGroup ボリュームの不要な自動サイズ変更を避けるために、ボリューム作成時の FlexGroup ボリュームの合計サイズがプライマリ FlexGroup ボリュームと必ず同じになるように設定してください。
- SnapMirror が転送するように設定されている間は、デスティネーションボリュームを制限したりオフラインにしたりしないでください。デスティネーションをオフラインにすると、SnapMirror はデスティネーションへの更新を実行できなくなります。
- プライマリ FlexGroup の構成要素の数は、`-aggr-list` パラメータで指定する必要があるアグリゲートエントリの数に直接関係します。`-aggr-list` で指定するアグリゲートを選択するときは、アグリゲートに構成要素用の十分なスペースがあることを確認してください。
- FlexGroup ボリュームの SnapMirror オペレーションを効率的に行うには、同じアグリゲートのセットによってホストされる各 FlexGroup について、`-aggr-list` パラメータで異なる順序を使用してください。推奨設定のひとつは、ラウンドロビン方式でアグリゲートをローテーションさせることです。
- 各デスティネーション構成要素のサイズが、プライマリ構成要素からデータを取り込むことができるサイズであることを確認します。そうしないと、SnapMirror オペレーションは領域不足時に失敗します。

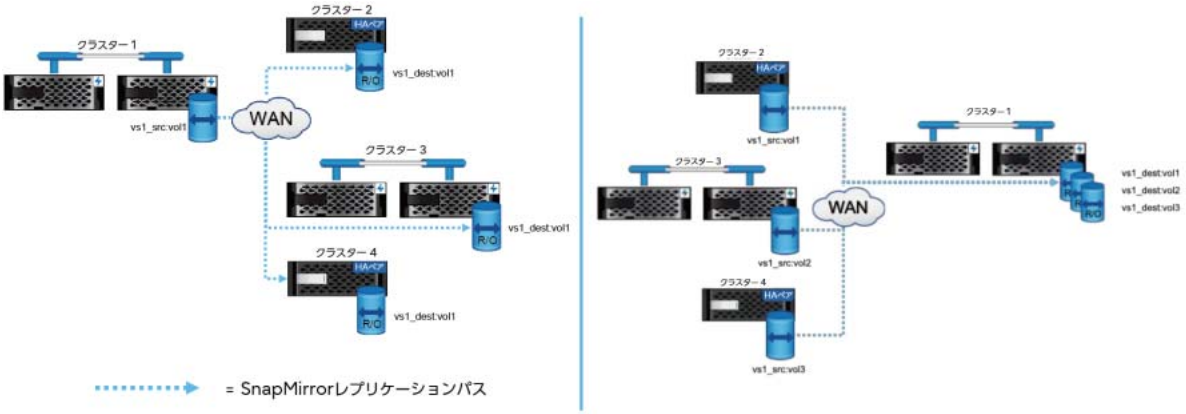
## 4.3.1　ファンインとファンアウト

図 4.1 に示すように、ソースクラスタ内のボリュームを複数の異なるデスティネーションにレプリケートしたり ( ファンアウト )、異なるソースのボリュームを 1 つのデスティネーションにレプリケートしたり ( ファンイン ) することができます。

**注 意**

ONTAP 9.11.1 では、1 つのソースボリュームから最大 8 つのデスティネーションボリュームをファンアウトできるようになりました。

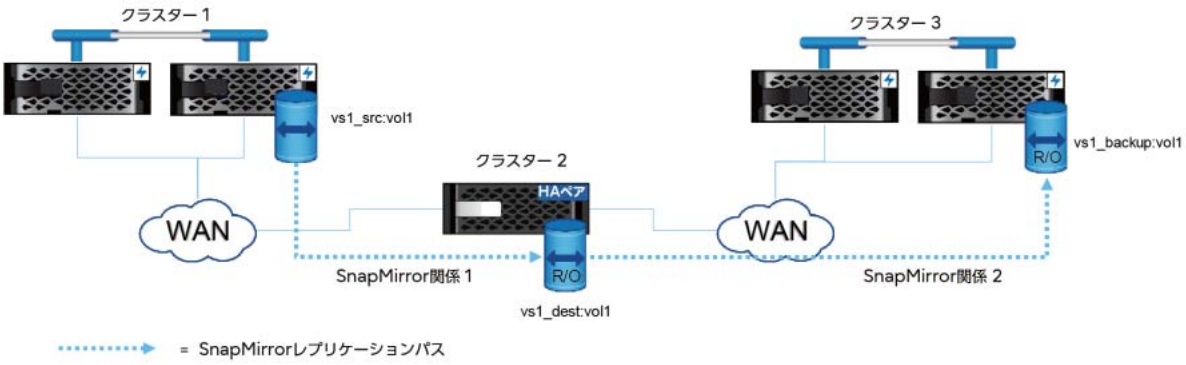
図 4.1　SnapMirror ファンアウトとファンイン




## 4.3.2　カスケード関係

SnapMirror を使用して、SnapMirror デスティネーションから別のシステムにデータをレプリケートできます。したがって、あるSnapMirror関係のデスティネーションであるシステムは、別のSnapMirror関係のソースとして機能できます。これは、1 つのサイトから複数のサイトにデータをコピーする必要がある場合に便利です。1 つのソースから各デスティネーションにデータをレプリケートする代わりに、あるデスティネーションから別のデスティネーションにデータを連続してレプリケートできます。これはカスケードと呼ばれます。カスケードトポロジでは、プライマリクラスタとセカンダリクラスタの間、およびセカンダリクラスタとターシャリクラスタの間にクラスタインターコネクトネットワークを作成するだけで済みます。プライマリクラスタとターシャリクラスタの間にクラスタインターコネクトネットワークを作成する必要はありません。2 段階のカスケード構成の例を図 4.2 に示します。

図 4.2　SnapMirror カスケード




この展開の機能は、ネットワーク全体のさまざまな場所からユーザーが読み取り専用で統一されたデータセットを利用できるようにし、そのデータを一定の間隔で統一的に更新できるようにすることです。

Snapshot コピーの動作は次のとおりです。

- SnapMirror は、ソースボリュームの Snapshot コピーにソフトロック ( タグ ) を作成します。
- デスティネーションシステムは、追加の Snapshot コピーを保持します。

SnapMirror は、カスケードの各接続に対して異なるデータ保護関係をサポートします。カスケードチェーンのいずれのデータ保護関係でも、Mirror または Vault に指定できます。したがって、ロングチェーンカスケードでは、チェーン内の任意の 3 つのクラスタ間で次のデータ保護関係の組合せを使用できます。

表 4.1　SnapMirror 関係

| 1-2 台目 | 2-3 台目 | 説明 |
|---|---|---|
| Mirror | Mirror | 1 台目のクラスタは 2 台目のクラスタと、2 台目のクラスタは 3 台目のクラスタと Mirror 関係にあります。 |
| Mirror | Vault | 1 台目のクラスタは 2 台目のクラスタと Mirror 関係にあり、2 台目のクラスタは 3 台目のクラスタと Vault 関係にあります。 |
| Vault | Vault | 1 台目のクラスタは 2 台目のクラスタと Vault の関係にあり、2 台目のクラスタは 3 台目のクラスタと Vault の関係にあります。 |

**注 意**

カスケード構成の場合は、最初のデータ保護関係のみを同期 SnapMirror とすることができます (`sync` または `strictsync`)。カスケード内の後続の Mirror 関係はすべて非同期でなければなりません。

### ■ ベストプラクティス

データ保護関係にあるすべての転送が正常に完了し、SnapMirror の更新が `snapmirror busy` エラーで失敗しないことを確認します。

Mirror-Vault、ファンアウト、またはカスケードデプロイメントを組み合わせて使用する場合は、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 コピーが存在しないと、更新が失敗することに注意する必要があります。snapmirror snapshot-owner create コマンドを使用して、Mirror-Vault 環境内のセカンダリ上のラベル付き Snapshot コピーを保存します。これにより、Vault 関係を更新するための共通 Snapshot コピーが提供されます。

カスケード SnapMirror 関係の使用例を次に示します。

- バックアップ管理者は、特定の Snapshot コピーの負荷をターシャリストレージに移動できるため、1 つのボリュームでサポートされる Snapshot コピーの実際の数よりも多くのコピーを保持できます ( 現在は 1023 まで )。
- バックアップ管理者は、複数のバックアップコピーを階層化できます。セカンダリストレージ (B) には、より頻繁な Snapshot コピーを ( たとえば、毎日および毎週 ) 保存できます。ターシャリストレージ (C) には、月単位および年単位の Snapshot コピーを保存できます。
- データは SSD から SATA ドライブに移動できます。
- データは、継続的な運用に支障をきたすことなく、世界中の場所に分散できます。さらに、アーカイブストレージとしてクラウドに移動することもできます。

## 4.3.3　デュアルホップボリューム SnapMirror

この構成には、3 つのクラスタ間でのボリューム SnapMirror レプリケーションが含まれます。これは、ソースボリュームがセカンダリボリュームにミラー化され、セカンダリボリュームがターシャリボリュームにミラー化される一連の関係で構成されます。セカンダリボリュームが使用できなくなった場合は、新しいベースライン転送を実行しなくても、プライマリボリュームとターシャリボリュームの関係を同期させることができます。

```
vs1_src:vol1 > vs1_dest:vol1 > vs1_backup:vol1
```

上記の構成では、`vs1_src:vol1` から `vs1_dest:vol1` および `vs1_dest:vol1` から `vs1_backup:vol1` への転送が同時に実行できます。

# 4.4　保護ポリシー

ONTAP はポリシーに基づいて、Snapshot コピーを作成するタイミングや、関係の一部として保持またはレプリケートするコピーの数を決定します。また、このポリシーは、ソースとデスティネーションの間に存在する関係の種類を判別するのに役立ちます。SnapMirror レプリケーションでは、ベースライン転送の内容が、初期化時に SnapMirror によって作成される Snapshot コピーに制限されます。更新のたびに、SnapMirror はソースの別の Snapshot コピーを作成します。次に、この Snapshot コピーと前回転送された Snapshot コピー (Mirror) の差分を、Snapshot ポリシールールで定義されているものと同じラベルを持つ新しい Snapshot コピー( ポリシーが Vault の場合 ) と一緒に転送します ONTAP には、事前に定義された保護ポリシーがいくつか用意されています。

## 4.4.1　ポリシータイプ

各 SnapMirror 保護ポリシー ( 標準またはカスタム ) は、複数の異なるポリシータイプの 1 つです。表 4.2 にポリシータイプを示します。

表 4.2　SnapMirror ポリシータイプ

| ポリシータイプ | 定義 |
|---|---|
| Async-mirror | Async-mirror ポリシータイプは、SnapMirror で次の 2 つのタイプの Snapshot コピーを転送するために使用されます。<br>• SnapMirror エンジンによって作成されたソース Snapshot のコピーです。(rule label = `sm_created`)<br>• 他の Snapshot コピーポリシーによってボリューム上に作成された、またはソースボリューム上で手動で作成されたすべてのソース Snapshot コピーです。(rule label = `all_source_snapshots`)<br>**注 意**<br>タイプが async-mirror の保護ポリシーに他のルールを適用することはできません。 |
| Vault | Vault ポリシータイプは、各ルールで提供されるラベルと一致するソースボリューム Snapshot コピーのみをコピーするために SnapMirror で使用されます。このレプリケーションは、データ保護に使用される SnapMirror のデフォルト (`sm_created`) レプリケーションプロセスとは無関係です。<br>Vault ポリシータイプは、SnapVault 機能のデフォルトです。このポリシーでは、SnapMirror 関係 (label= `sm_created`) によって作成された Snapshot コピーはレプリケートされません。 |
| Mirror-vault | Mirror-vault ポリシータイプは、SnapMirror のレプリケーションエンジンによって作成された Snapshot コピー (snapshot label= `sm_created`)、および各ルールで定義された Snapshot コピーラベルと一致する必要なソース Snapshot コピーを転送するために、SnapMirror によって使用されます。<br>Mirror-vault 保護ポリシーには、目的のデータ保護要件に一致する複数のルールを定義できます。 |
| Sync-mirror | Sync-mirror ポリシーは、SM-S のデフォルトポリシーです。このポリシーでは、ソースボリュームとデスティネーションボリュームが短期間同期しない状態がサポートされます。このような状況では、デスティネーションデータ保護クラスタから書込み確認を受信しない場合でも、書込み確認はアプリケーションに転送されます。<br>SM-S の詳細については、関連マニュアルに記載されています。詳細は、富士通マニュアルサイトの「Fujitsu Storage ETERNUS AX/HX series SnapMirror Synchronous 構成とベストプラクティス ONTAP 9.11.1」を参照してください。 |
| Strict-sync-mirror | Strict-sync-mirror ポリシータイプは、SM-S 用のポリシーです。このポリシーでは、書き込み確認がアプリケーションに送信される前に、SnapMirror 関係の両方のクラスタによってすべての書き込み操作が確認される必要があります。データ保護クラスタから書き込み確認を受信しない場合、書き込み失敗がアプリケーションに送信され、ボリュームは故障モードと見なされます。 |

| ポリシータイプ | 定義 |
|---|---|
| Continuous | S3 SnapMirror 関係には、continuous ポリシータイプが使用されます。S3 SnapMirror は、ONTAP S3 バケットを、ONTAP S3 またはクラウドベースの S3 バケットを実行する別のクラスタに保護するために使用されます。 |
| Automated-failover | Automated-failover ポリシータイプは、SnapMirror-Business Continuity によって使用されます。非同期データ保護のカスタムデータ保護ポリシーで使用するようには設計されていません。 |

## 4.4.2　標準非同期保護ポリシー

SnapMirror 非同期関係の作成では、次の保護ポリシーを使用できます。

- **Asynchronous**
  これは、mirror-vault ポリシータイプの非同期 SnapMirror ポリシーです。したがって、非同期保護ポリシーは最新のファイルシステムを一時間ごとにミラーリングし、ソースボリュームから 1 日ごとのラベルで Snapshot コピーを 7 ファイル、1 週間ごとのラベルで Snapshot コピーを 52 ファイル保持します。これは SnapMirror 関係作成のデフォルトポリシーであり、以前のバージョンの ONTAP でデフォルトの保護ポリシーとして使用されていた DPDefault の代わりとなるものです（図 4.3）。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `mirror-vault` です。
  - Create snapshot が `true` に設定されています。
  - 以下のルールがあります。
    - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。
    - `daily` は、7 ファイルの Snapshot コピーを毎日保持します。
    - `weekly` は、52 ファイルの Snapshot コピーを毎週保持します。

図 4.3　SnapMirror 非同期ポリシー定義

```
EcoSystems-A200-A::> snapmirror policy show -policy Asynchronous -instance

                     Vserver: EcoSystems-A200-A
       SnapMirror Policy Name: Asynchronous
       SnapMirror Policy Type: mirror-vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
               Create Snapshot: true
                      Comment: A unified Asynchronous SnapMirror and SnapVault policy for mirroring the late
st active file system and daily and weekly Snapshot copies with an hourly transfer schedule.
        Total Number of Rules: 3
                   Total Keep: 60
       Transfer Schedule Name: hourly
                     Throttle: unlimited
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 sm_created                       1 false       0 -        -
 daily                            7 false       0 -        -
 weekly                          52 false       0 -        -
```

- **DailyBackup**
  このポリシーは、vault ポリシータイプの非同期 SnapMirror ポリシーです。これを使用して、「daily」のラベルがついたソースボリュームの Snapshot コピーから SnapValut アーカイブを作成し、直近の 7 ファイルの Snapshot コピーをデータ保護ボリューム上に保存します。Create Snapshot フィールドが False に設定されている場合、このポリシーは SnapMirror 関連の Snapshot コピーをソースボリューム上に作成しません。

  ここに記載されている保護ポリシーはレガシーポリシーと見なされますが、追加のデータ保護戦略をサポートする際に非常に役立ちます。ONTAP System Manager では、これらのポリシーは、保護関係を作成または編集するときに「Show Legacy Policies」オプションが選択されている場合にのみ表示されます (図 4.4)。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `vault` です。
  - Create Snapshot の値が `false` に設定されている場合、更新がトリガーされてもポリシーは Snapshot コピーを作成しません。
  - 以下のルールがあります。
    - 7 ファイルの Snapshot コピーを毎日保持します。

図 4.4　DailyBackup 非同期 SnapMirror ポリシーの定義

```
EcoSystems-A200-B::> snapmirror policy show -policy DailyBackup -instance

                       Vserver: EcoSystems-A200-B
       SnapMirror Policy Name: DailyBackup
       SnapMirror Policy Type: vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: false
                      Comment: Vault policy with a daily rule and a daily transfer schedule.
        Total Number of Rules: 1
                   Total Keep: 7
       Transfer Schedule Name: daily
                     Throttle: unlimited
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 daily                            7 false       0 -        -
```

- **DPDefault**
  これは、すべての Snapshot コピーと最新のアクティブなファイルシステムをソースからデスティネーションにミラーリングするための非同期 SnapMirror ポリシーです。このポリシーは、従来の SnapMirror 関係で使用できます。管理者は、新しい SnapMirror 関係に新しい MirrorAllSnapshots ポリシーを使用する必要があります。

  この構成では、SnapMirror エンジンは Snapshot コピーを作成した後、新しい SnapMirror の Snapshot コピーと以前の Snapshot コピーおよび他のすべての Snapshot コピーとの差分を複製します。SnapMirror 関係が初期化されている場合は、Snapshot コピーが作成され、それ以前のすべての Snapshot コピーがレプリケートされます。更新が完了すると、古い Snapshot コピーが削除され、共通の SnapMirror Snapshot コピーが 1 つだけ残ります (図 4.5)。

このポリシーは、次の設定で構成されます。

- ポリシータイプは `async-mirror` です。
- Create snapshot が `true` に設定されています。
- 以下のルールがあります。
  - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。
  - `all_source_snapshots` は、ソースボリュームからの一意の Snapshot コピーごとに 1 つのコピーを保持します。

図 4.5　DPDefault 非同期 SnapMirror ポリシーの定義

```
cluster_dst::> snapmirror policy show -policy DPDefault -instance

                      Vserver: vs0
       SnapMirror Policy Name: DPDefault
       SnapMirror Policy Type: async-mirror
                 Policy Owner: cluster-admin
                  Tries Limit: 8
             Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
               Create Snapshot: true
                      Comment: Asynchronous SnapMirror policy for mirroring all
Snapshot copies and the latest active file system.
        Total Number of Rules: 2
                   Total Keep: 2
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 sm_created                       1 false       0 -        -
 all_source_snapshots             1 false       0 -        -
```

- **MirrorAllSnapshots**
  これも、すべての Snapshot コピーと最新のアクティブなファイルシステムをプライマリからセカンダリにミラーリングするための非同期ポリシーです。このポリシーは DPDefault に似ています (図 4.6)。

  このポリシーは、次の設定で構成されます。

  - ポリシータイプは `async-mirror` です。
  - Create snapshot が `true` に設定されています。
  - 以下のルールがあります。
    - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。
    - `all_source_snapshots` は、ソースボリュームからの一意の Snapshot コピーごとに 1 つのコピーを保持します。

図 4.6　MirrorAllSnapshots 非同期 SnapMirror ポリシーの定義

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: Asynchronous SnapMirror policy for mirroring all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn Schedule Prefix
                              ----------------     ----  -------- ---- -------- ------
                              sm_created              1  false       0 -        -
                              all_source_snapshots    1  false       0 -        -
```

- **MirrorLatest**
  最新のアクティブなファイルシステムをプライマリからセカンダリにミラーリングするための非同期ポリシーです。SnapMirror エンジンは、このポリシーを使用して Snapshot を作成し、新しい SnapMirror Snapshot コピーと前の SnapMirror Snapshot コピーの差分を複製します。関係が初期化されている場合は、Snapshot が作成され、それ以前のすべての Snapshot がレプリケートされます。更新が完了すると、古い Snapshot が削除され、共通の SnapMirror Snapshot コピーが 1 つだけ残ります (図 4.7)。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `async-mirror` です。
  - Create snapshot が `true` に設定されています。
  - 以下のルールがあります。
    - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。

図 4.7　MirrorLatest 非同期 SnapMirror ポリシーの定義

```
cluster_dst::> snapmirror policy show -policy MirrorLatest -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorLatest
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: Asynchronous SnapMirror policy for mirroring the latest active
file system.
       Total Number of Rules: 1
                  Total Keep: 1
 Rules:
 SnapMirror Label             Keep Preserve Warn Schedule Prefix
 ---------------------------- ---- -------- ---- -------- ----------
 sm_created                      1 false       0 -        -
```

- **MirrorAndVault**
  これは、最新のアクティブなファイルシステムと、毎日および毎週の Snapshot コピーをミラーリングするための、SnapMirror と SnapVault の統合ポリシーです。データ保護モードが指定されていない場合、または関係のタイプとして XDP モードが指定されている場合は、MirrorAndVault が新しいデフォルトポリシーになります (図 4.8)。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `mirror-vault` です。
  - Create snapshot が `true` に設定されています。
  - 以下のルールがあります。
    - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。
    - `daily` は、7 ファイルの Snapshot コピーを毎日保持します。
    - `weekly` は、52 ファイルの Snapshot コピーを毎週保持します。

図 4.8　MirrorAndVault 非同期 SnapMirror ポリシーの定義

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                      Vserver: vs0
       SnapMirror Policy Name: MirrorAndVault
       SnapMirror Policy Type: mirror-vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: true
                      Comment: A unified Asynchronous SnapMirror and SnapVault policy for
mirroring the latest active file system and daily and weekly Snapshot copies.
        Total Number of Rules: 3
                   Total Keep: 60
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 sm_created                       1 false       0 -        -
 daily                            7 false       0 -        -
 weekly                          52 false       0 -        -
```

- **Unified7year**
  このポリシーでは、毎月の Snapshot コピーを転送して 7 年間保持するという monthly の追加ルールがあります (図 4.9)。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `mirror-vault` です。
  - Create snapshot が `true` に設定されています。
  - 以下のルールがあります。
    - `sm_created` は、SnapMirror で最後に生成された Snapshot コピー以降のソースボリューム上の変更をレプリケートします。
    - `daily` は、7 ファイルの Snapshot コピーを毎日保持します。
    - `weekly` は、52 ファイルの Snapshot コピーを毎週保持します。
    - `monthly` は、84 ファイルの Snapshot コピーを 7 年間保持します。

図 4.9　Unified7year 非同期 SnapMirror ポリシーの定義

```
cluster_dst::> snapmirror policy show -policy Unified7year -instance

                      Vserver: vs0
       SnapMirror Policy Name: Unified7year
       SnapMirror Policy Type: mirror-vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: true
                      Comment: Unified SnapMirror policy with 7year retention.
        Total Number of Rules: 4
                   Total Keep: 144
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 sm_created                       1 false       0 -        -
 daily                            7 false       0 -        -
 weekly                          52 false       0 -        -
 monthly                         84 false       0 monthly  -
```

- **XDPDefault**
  これは、ラベルが「Daily」および「Weekly」のすべての Snapshot コピーをミラーリングするための非同期 SnapVault ポリシーです。これは従来の vault-only ポリシーであり、SnapVault 関係の作成に使用できます (図 4.10)。

  このポリシーは、次の設定で構成されます。
  - ポリシータイプは `vault` です。
  - Create Snapshot の値が `false` に設定されている場合、更新がトリガーされてもポリシーは Snapshot コピーを作成しません。
  - 以下のルールがあります。
    - `daily` は、7 ファイルの Snapshot コピーを毎日保持します。
    - `weekly` は、52 ファイルの Snapshot コピーを毎週保持します。

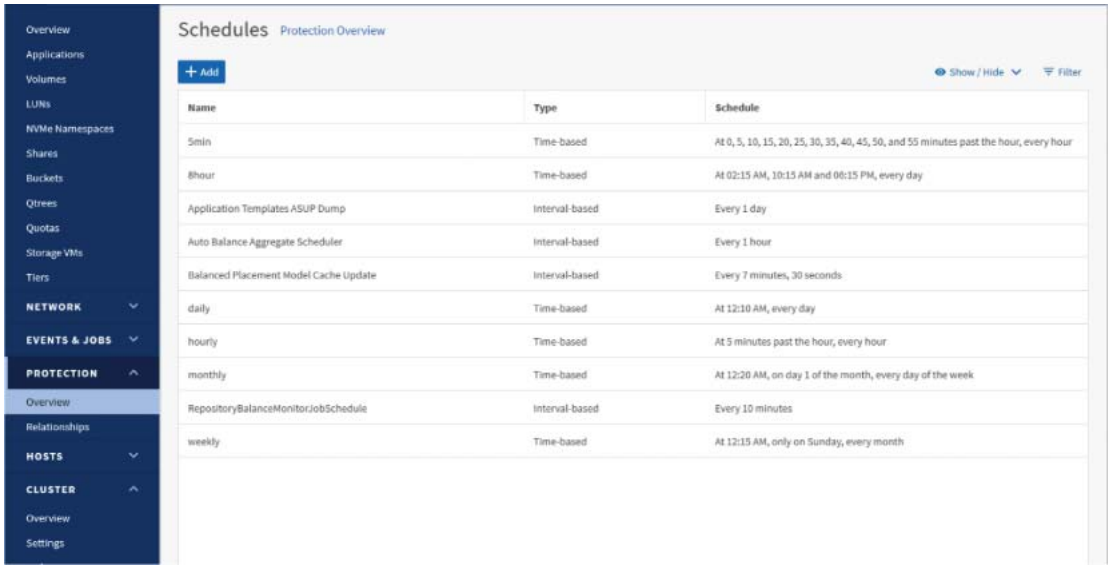
図 4.10　XDPDefault SnapVault ポリシー定義

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                      Vserver: vs0
       SnapMirror Policy Name: XDPDefault
       SnapMirror Policy Type: vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: false
                      Comment: Vault policy with daily and weekly rules.
        Total Number of Rules: 2
                   Total Keep: 59
 Rules:
 SnapMirror Label              Keep Preserve Warn Schedule Prefix
 ----------------------------- ---- -------- ---- -------- ----------
 daily                            7 false       0 -        -
 weekly                          52 false       0 -        -
```

# 4.5　SnapMirror スケジュール

SnapMirror ポリシーには、デスティネーションクラスタ内の SnapMirror 関係にスケジュールを割り当てることによって定期的な非同期レプリケーションを実行するために作成できる、少なくとも 1 つの SnapMirror ジョブスケジュールが必要です。図 4.11 に、ONTAP System Manager で使用可能なジョブスケジュールを示します。

図 4.11　ONTAP System Manager で一覧表示および作成できる SnapMirror スケジュール




または、CLI から `job schedule cron create` コマンドを使用してスケジュールを作成することもできます。図 4.12 の例は、`Hourly_SnapMirror` という名前のスケジュールを作成し、毎時の最初に ( 毎時 0 分に ) 実行する方法を示します。

図 4.12　CLI を使用して一覧表示および作成できる SnapMirror スケジュール

```
cluster02::> job schedule cron create Hourly_SnapMirror -minute 0
cluster02::> job schedule cron show
Name                Description
----------------    ---------------------------------------------------
5min                @:00,:05,:10,:15,:20,:25,:30,:35,:40,:45,:50,:55
8hour               @2:15,10:15,18:15
Hourly_SnapMirror   @:00
avUpdateSchedule    @2:00
daily               @0:10
hourly              @:05
weekly              Sun@0:15
```

スケジュールは、作成時の SnapMirror 関係には、`-schedule` オプション、または既存の関係には `snapmirror modify` コマンドと `-schedule` オプションを使用して適用できます。この例では、Hourly_SnapMirror スケジュールが既存の関係に適用されます。

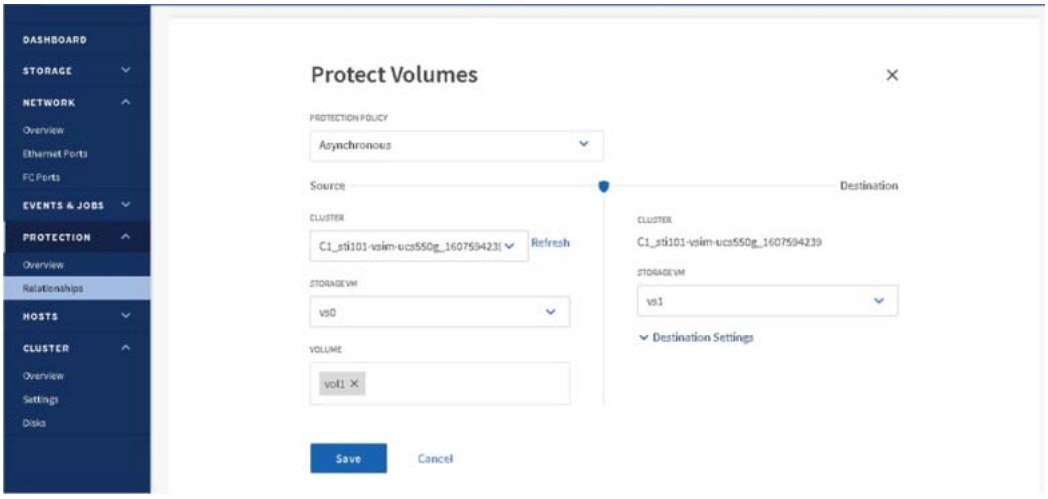
```
cluster02::> snapmirror modify -destination-path cluster02://vs1/vol1 -schedule Hourly_SnapMirror
```

# 4.6　SnapMirror 関係の作成

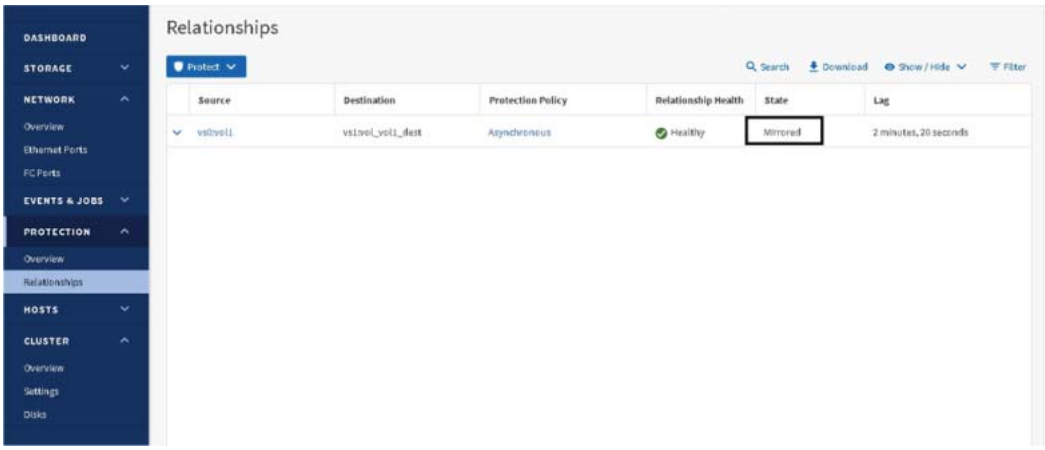
DR のデータをレプリケートするためのデータ保護を有効にするには、1 つのクラスタ上のソースとピアリングされたクラスタ上のデスティネーションの間に SnapMirror 関係を作成する必要があります。デスティネーションクラスタ上の ONTAP System Manager から、次の手順を実行します。

## 手順 ▶▶▶

1. [Relationships] をクリックします。
2. ミラー関係を作成するボリュームを選択し、[Save] をクリックします。




3. ミラー関係の作成と初期化が完了したら、次に示すように、SnapMirror 関係のミラーステータスが Mirrored であることを確認します。



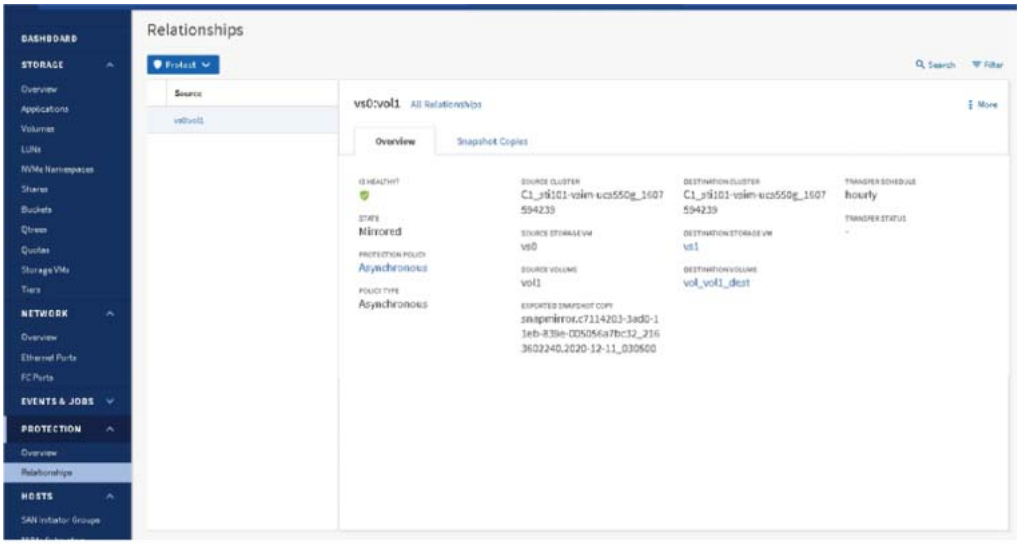

4. ソースボリュームとデスティネーションボリュームの間の SnapMirror 関係を選択し、[Details] タブでステータスを確認します。
5. [Details] タブには、SnapMirror 関係の稼働状態が表示され、転送エラーと遅延時間が表示されます。
6. [Is Healthy] フィールドに [Yes] が表示されている必要があります。

7 ほとんどの SnapMirror データ転送エラーの場合、フィールドには No と表示されます。ただし、失敗した場合でも、フィールドには、Yes と表示されます。[Details] セクションで転送エラーをチェックして、データ転送エラーが発生していないことを確認する必要があります。

8 [State] フィールドに [Mirrored] と表示されている必要があります。

9 遅延時間は転送スケジュール間隔以下でなければなりません。たとえば、転送スケジュールが時間単位の場合、遅延時間は 1 時間を超えてはなりません。

10 また、[Volumes] ウィンドウに移動し、SnapMirror 関係を作成したボリュームを選択します。ボリュームをダブルクリックして、ボリュームの詳細とデータ保護の状態を表示します。




## 4.7　SnapMirror 関係の初期化中のベースライン転送

新しい SnapMirror 関係が作成されると、その関係とそれを定義するメタデータが確立されます。オプションで [Initialize the Relationship] を選択すると、ベースラインの内容と更新を定義する SnapMirror ポリシーに基づいて、ソースからデスティネーションへのベースライン転送を実行できます。プロセスは次のとおりです。

**手順 ▶▶▶**

1 ソースの Snapshot コピーを作成します。

2 Snapshot コピーをデスティネーションに転送します。

3 関係に関連づけられている SnapMirror ポリシーに応じて、他の Snapshot コピーもソースからデスティネーションに転送されます。

**4** ベースライン転送後、SnapMirror 関係に割り当てられたスケジュールに従って、この関係が更新されます。

デスティネーションは、すでに作成して制限付きとしてマークしたボリュームです。SnapMirror はデータの転送が完了すると、デスティネーションを読み取り専用状態でオンラインにします。最初のデータ転送が行われている間は、`vol status` コマンドの出力でデスティネーションが無効とマークされます。最初の転送が完了すると、ボリュームは有効になり、オンラインになります。これで、ソースボリューム内のファイルと Snapshot コピーがデスティネーションで使用可能になります。

# 4.8　SnapMirror 関係の手動更新

最新の Snapshot コピーまたは特定の Snapshot コピーから手動で SnapMirror 関係を更新して、今後の停電、スケジュールされたメンテナンス、またはデータ移行によるデータ消失を防ぐ必要がある場合があります ( 図 4.13 および図 4.14 を参照 )。

図 4.13　SnapMirror 関係の更新を開始する

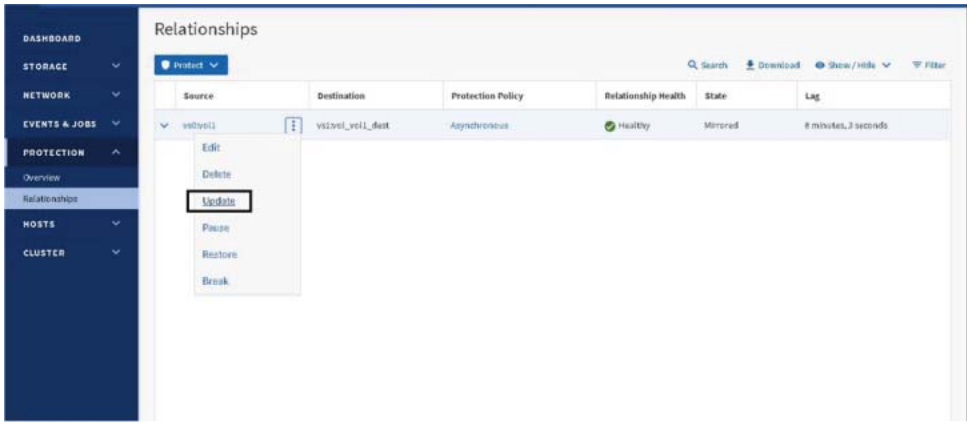
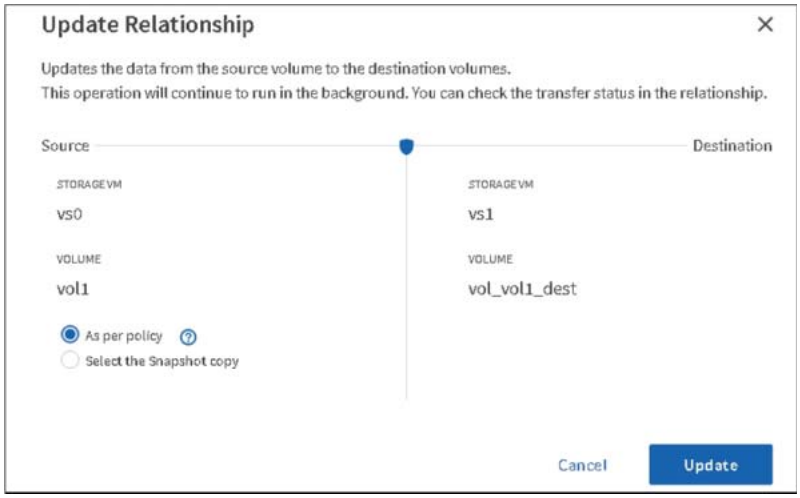



図 4.14　関係の更新ダイアログボックス




更新が完了すると、[Transfer State] フィールドが [Transferring] から [Idle] に変わります。

# 第 5 章
# 異なるデータ保護モード間での変換

## 5.1 従来の DP SnapMirror 関係を XDP SnapMirror 関係へ変換する

ONTAP 9.11.1 では、DP タイプの SnapMirror 関係は、クラスタ内の既存の SnapMirror 関係についてのみサポートされています。これは、将来の ONTAP リリースで DP タイプの SnapMirror 関係を完全に非推奨にするための段階的な取り組みです。DP タイプの SnapMirror 関係が非推奨になる準備として、富士通では、既存の DP 関係を新しい XDP 関係に変換することを推奨しています。

この変換を実行するには、次の高度な手順を実行します。

手順 ▶▶▶

1. デスティネーションクラスタ上の SnapMirror 関係を停止します。
2. デスティネーションクラスタ上の SnapMirror 関係を解除します。
3. この SnapMirror 関係を削除します。
4. 同じエンドポイント間に SnapVault 関係 (MirrorAndVault: XDP のデフォルト保護ポリシー ) を作成します。
5. エンドポイント間で再同期を実行します。この再同期により、DR のデスティネーションが別のベースラインなしで Vault のデスティネーションに変換されます。メタデータの再構築には、ソースデータ 1TB あたり 10 ～ 12 分かかります。

◀◀◀

このプロセスの詳細は、次の手順で説明します。

手順 ▶▶▶

1. SnapMirror 関係を停止します。

```
Remote::> snapmirror quiesce -destination-path vs1:vol_vol1_dr
Operation succeeded: snapmirror quiesce for destination "vs1:vol_vol1_dr".
```

2. SnapMirror の解除操作を実行します。

```
Remote::> snapmirror break -destination-path vs1:vol_vol1_dr
[Job 128] Job succeeded: SnapMirror Break Succeeded
```

SnapMirror 関係のステータスは、[`Broken Off`] として表示されます。

```
Remote::> snapmirror show -destination-path vs1:vol1_vol1_dr -fields state
source-path                  desitnation-path             state
---------------------------- ---------------------------- ----------------
Vs0:vs0vol1                  vs1:vol1_vol1_dr             broken off
```

解除操作の結果、デスティネーションボリュームが DP から RW に変わります。

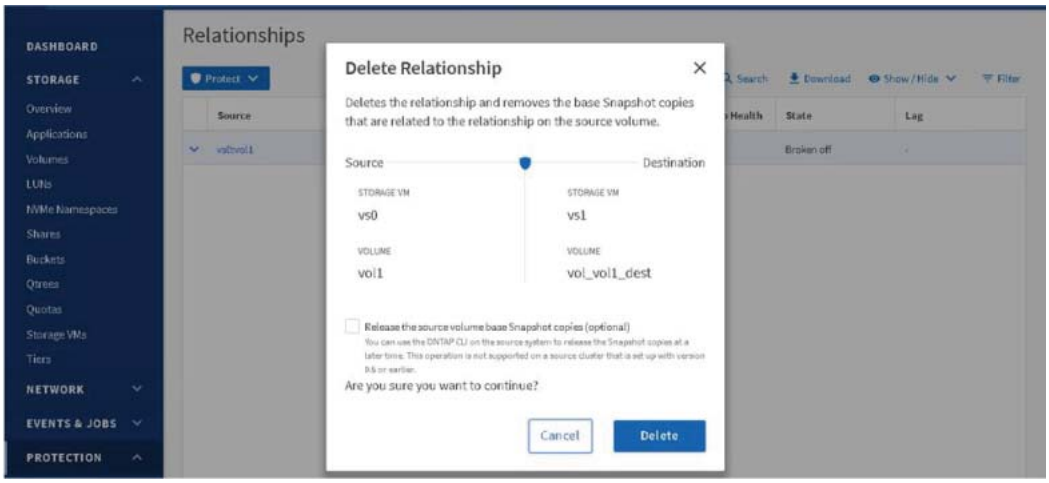
```
Remote::> volume show -volume vol1_vol1_dr -fields type
vserver                     volume                      type
--------------------------- --------------------------- ----------------
Vs1                         vol1_vol1_dr                RW
```

**3** snapmirror delete コマンドを実行します。

```
Remote::> snapmirror delete -destination-path vs1:vol_vol1_dr
Operation succeeded: snapmirror delete the relationship with destination vs1:vol_vol1_dr.
```

**注 意**

ONTAP System Manager は、ベースの Snapshot コピーを解放せずに SnapMirror 関係を削除することで、リリース操作を組み込みます。新しいベースラインが作成されないようにするには、[Release the Source Volume Base Snapshot Copies] オプションをオフにします。これは、SnapVault 関係の作成時に別のベースラインが不要になるように、これらの基本 Snapshot コピーを必要とするためです。




**4** SnapVault 関係を作成します。

```
Remote::> snapmirror create -source-path vs0:vol1 -destination-path vs1:vol_vol1_dr -type XDP
Operation succeeded: snapmirror create the relationship with destination vs1:vol_vol1_dr .
```

**5** SnapVault 関係が作成されており、[Mirror State] が [Broken-off] になっていることを確認します。

```
Remote::> snapmirror show
                                                                    Progress
Source            Destination  Mirror  Relationship  Total         Last
Path        Type  Path         State   Status        Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
vs0:vol1
            XDP  vs1:vol_vol1_dr
                             Broken-off
                                     Idle           -         true    -
```

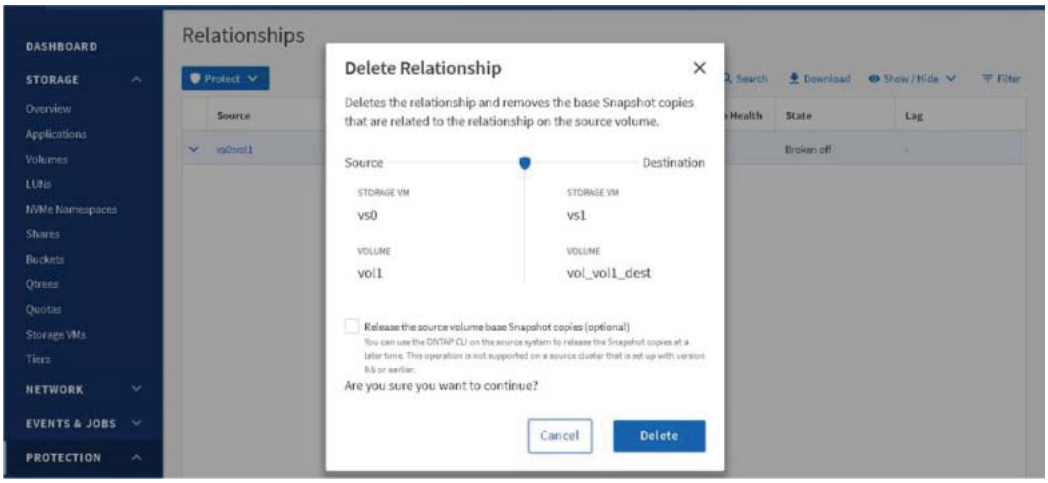
**6** `SnapMirror resync` 処理を実行します。

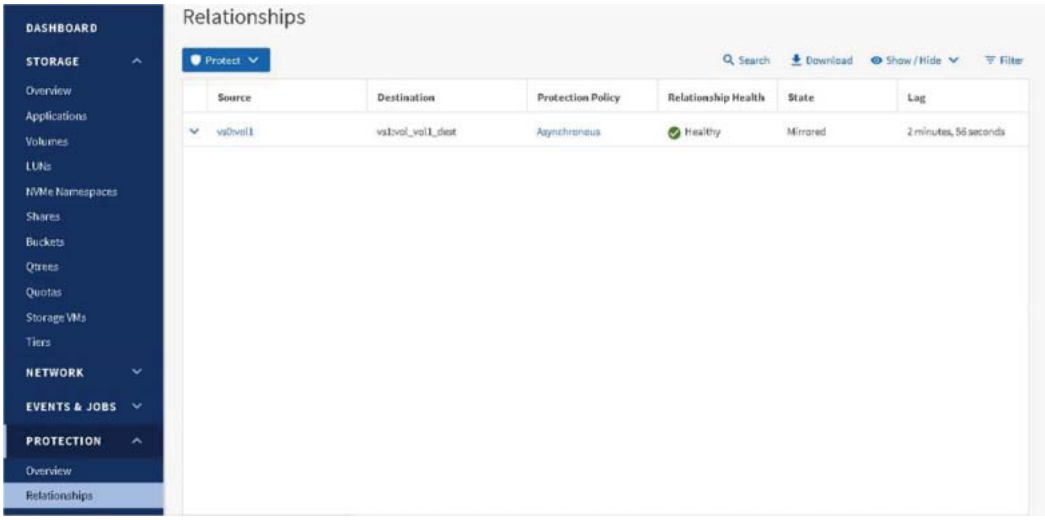
```
Remote::> snapmirror resync -destination-path vs1:vol_vol1_dr

Warning: All data newer than Snapshot copy snapmirror.c7114203-3ad0-11eb-839e-
005056a7bc32_2163602240.2020-12-11_032052 on
         volume vs1:vol_vol1_dest will be deleted.
Do you want to continue? {y|n}: y
Operation is queued: initiate snapmirror resync to destination "vs1:vol_vol1_dest".
```

**7** `snapmirror show` コマンドを実行して、SnapVault 関係のタイプとステータスを表示します。

```
Remote::> snapmirror show
                                                                    Progress
Source            Destination  Mirror  Relationship  Total          Last
Path        Type  Path         State   Status        Progress  Healthy Updated
----------- ---- ------------- ------- -------------- --------- ------- --------
vs0:vol1
            XDP  vs1:vol_vol1_dr
                              Snapmirrored
                                      Idle           -         true    -
```

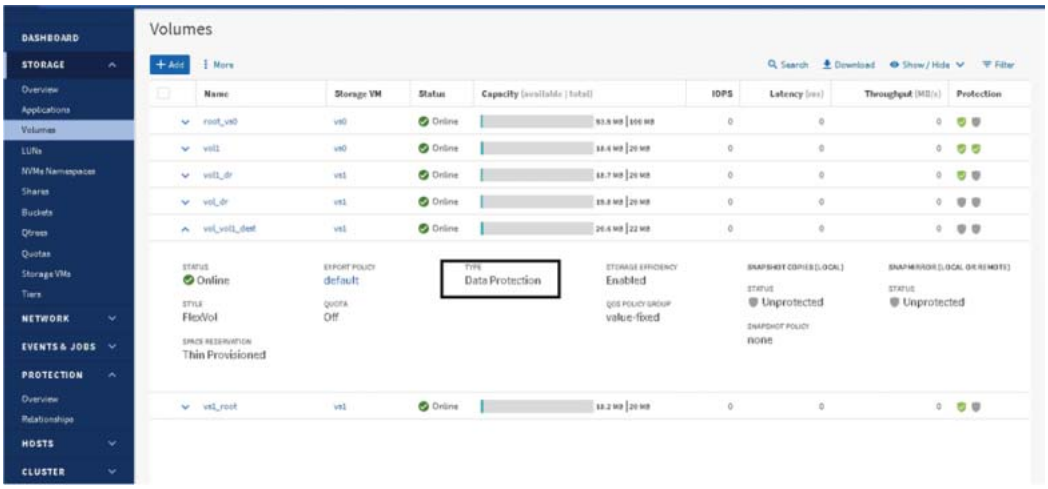
ONTAP System Manager で、SnapVault 関係ステータスが `Snapmirrored` であることを確認できます。



**8** SnapVault のデスティネーションボリュームは、DR ボリュームとして使用する `Data Protection` タイプのボリュームです。

```
Remote::> volume show -volume vol1_vol1_dr -fields type
vserver                     volume                      type
--------------------------- --------------------------- ----------------
Vs1                         vol1_vol1_dr                DP
```




## 5.2　SnapMirror をユニファイドレプリケーションに変換

SnapMirror を使用している既存のお客様が、SnapMirror ユニファイドレプリケーションを使用して単一のデスティネーションボリュームを DR とバックアップに使用したいと考えているとします。変換の手順は、次のとおりです。

**手順 ▶▶▶**

**1** デスティネーションクラスタ上の SnapMirror ボリューム関係を解除します。

**2** SnapMirror ボリューム関係を削除します。

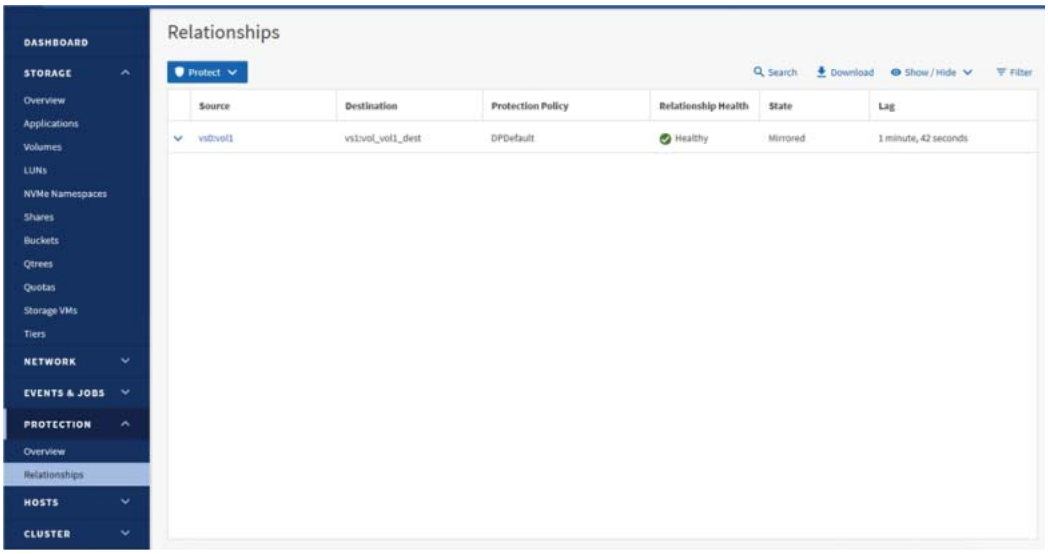
**3** デフォルトの SnapMirror ユニファイドレプリケーションポリシーのいずれかを使用して、同じエンドポイント間に統合関係 (MirrorAndVault) を作成します。

**4** エンドポイント間で再同期操作を実行します。この再同期により、ベースラインを作り直すことなく、関係が SnapMirror ユニファイドレプリケーション構成に変換されます。

このプロセスの詳細は、次の手順で説明します。

## 手順 ▶▶▶

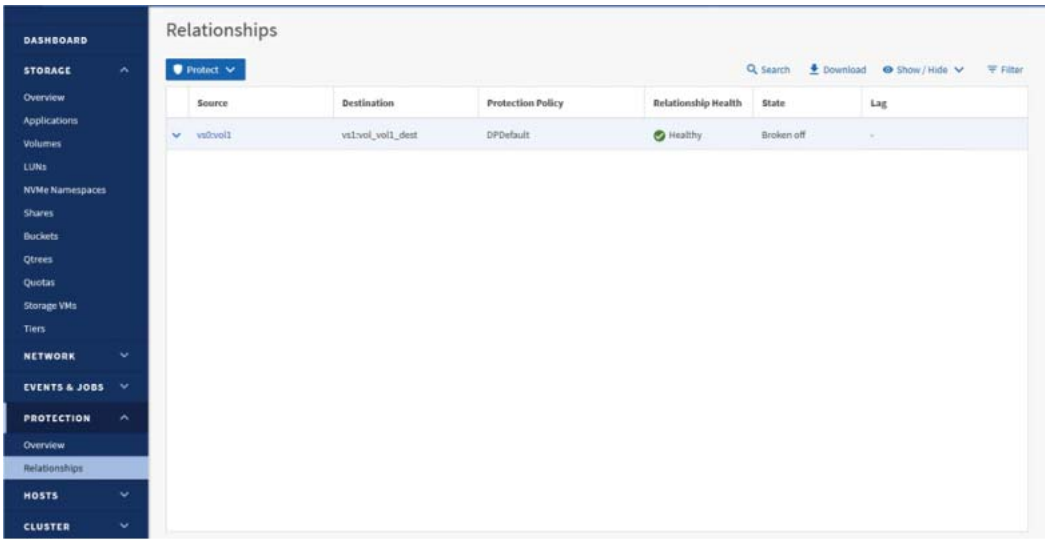
**1** SnapMirror 関係のステータスを表示します。SnapMirror 関係のステータスに「Mirrored」が表示されます。




**2** SnapMirror ユニファイドレプリケーションに変換するには、SnapMirror Break 操作を実行します。

```
Remote::> snapmirror break -destination-path vs1:vol_vol1_dr
[Job 128] Job succeeded: SnapMirror Break Succeeded
```

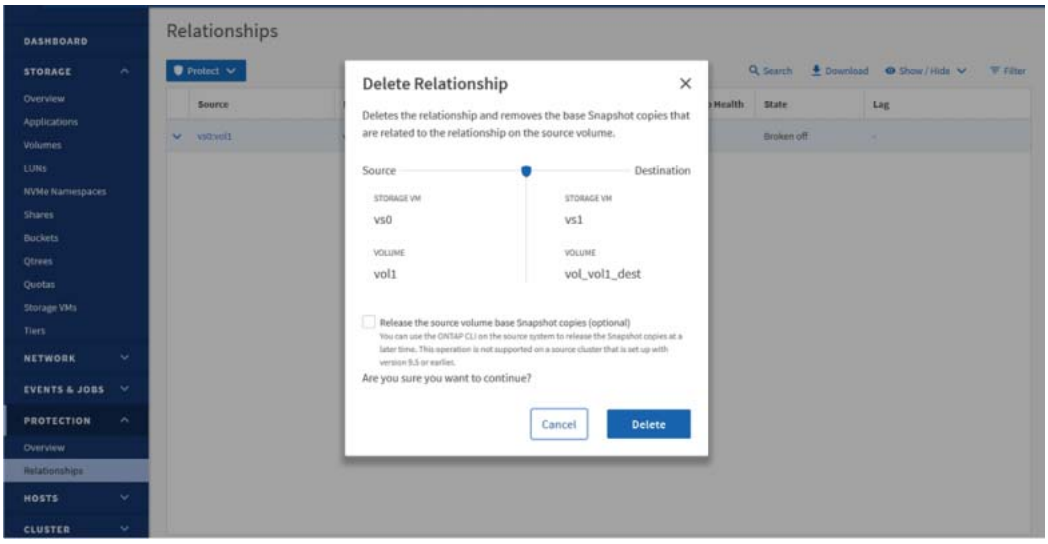
SnapMirror 関係が 「Broken Off」と表示されます。




**3** `snapmirror delete` コマンドを実行します。

```
Remote::> snapmirror delete -destination-path vs1:vol_vol1_dr -relationship-info-only true
Operation succeeded: snapmirror delete the relationship with destination vs1:vol_vol1_dr.
```

**4** 基本 Snapshot コピーを解放せずに、SnapMirror 関係を削除します。



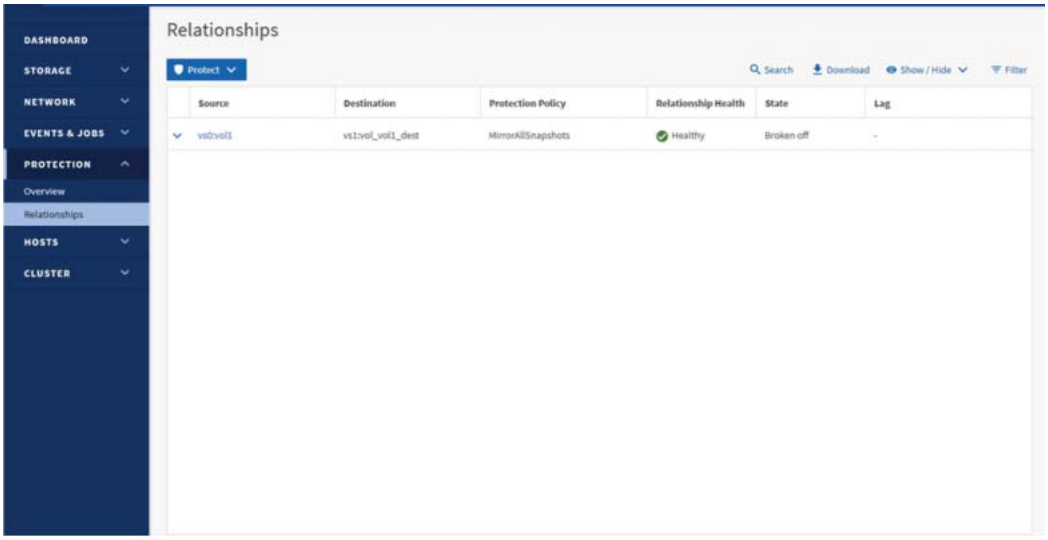

この関係は、[Protection] > [Relationships] の下のデスティネーションクラスタから削除されます。

**5** `Snapmirror create` コマンドを実行して、ユニファイドレプリケーション関係を作成します。

```
Remote::> snapmirror create -source-path vs0:vol1 -destination-path vs1:vol_vol1_dr-type XDP -
policy MirrorAllSnapshot
Operation succeeded: snapmirror create the relationship with destination svm_dst1:Source_dest.
```

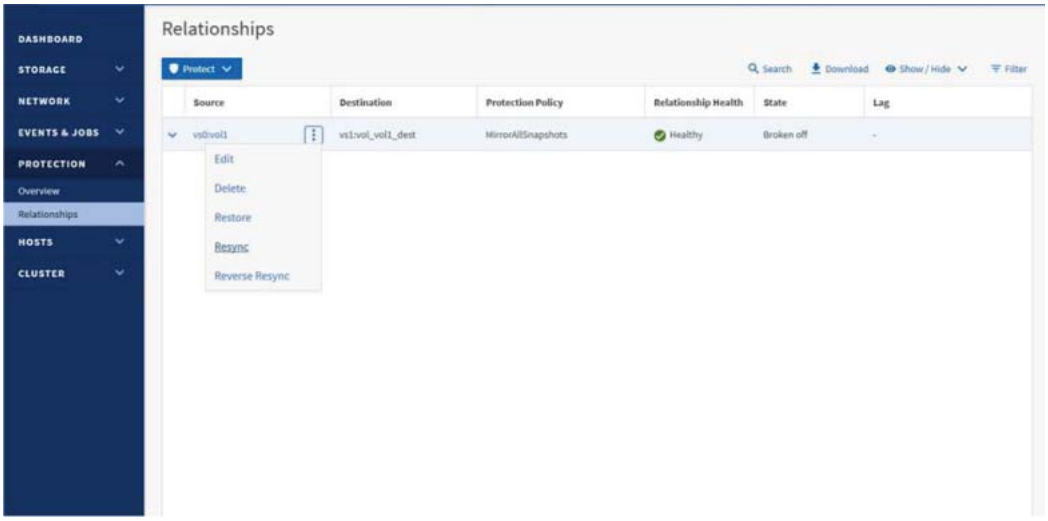
**6** `snapmirror show` コマンドを実行して、作成されたユニファイドレプリケーション関係を確認します。

```
Remote::> snapmirror show
                                                                    Progress
Source            Destination  Mirror  Relationship  Total          Last
Path        Type  Path         State   Status        Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
vs0:vol1
            XDP  vs1:vol_vol1_dr
                              Broken-off
                                      Idle           -         true    -
```



**7** CLI または ONTAP System Manager を使用して、`snapmirror resync` コマンドを実行します。

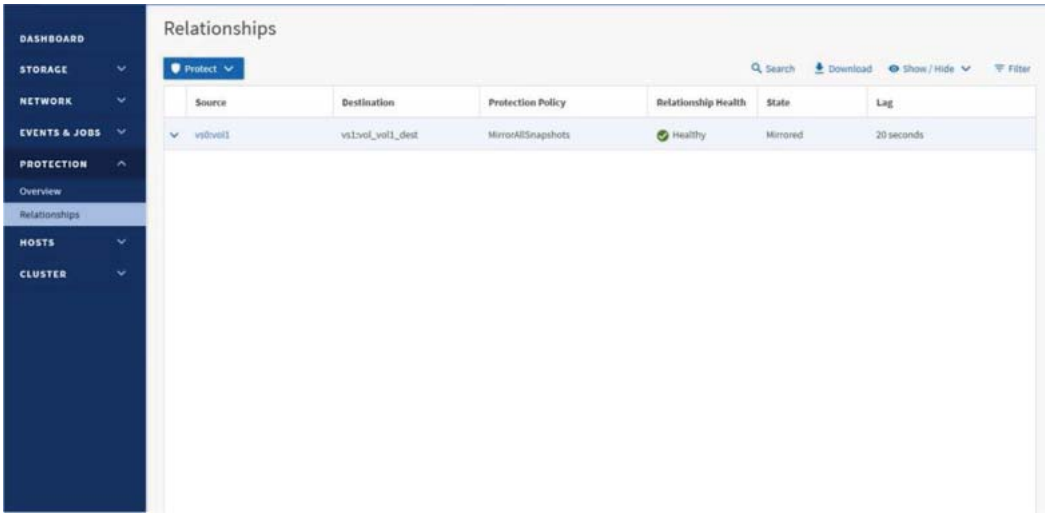
```
Remote::> snapmirror resync -destination-path vs1:vol_vol1_dr

Warning: All data newer than Snapshot copy snapmirror.12ceb7f0-b078-11e8-baec-
005056b013db_2160175149.2020-01-24_091316 on volume
         vs1:vol_vol1_drwill be deleted.
Do you want to continue? {y|n}: y
Operation is queued: initiate snapmirror resync to destination "vs1:vol_vol1_dr".
```



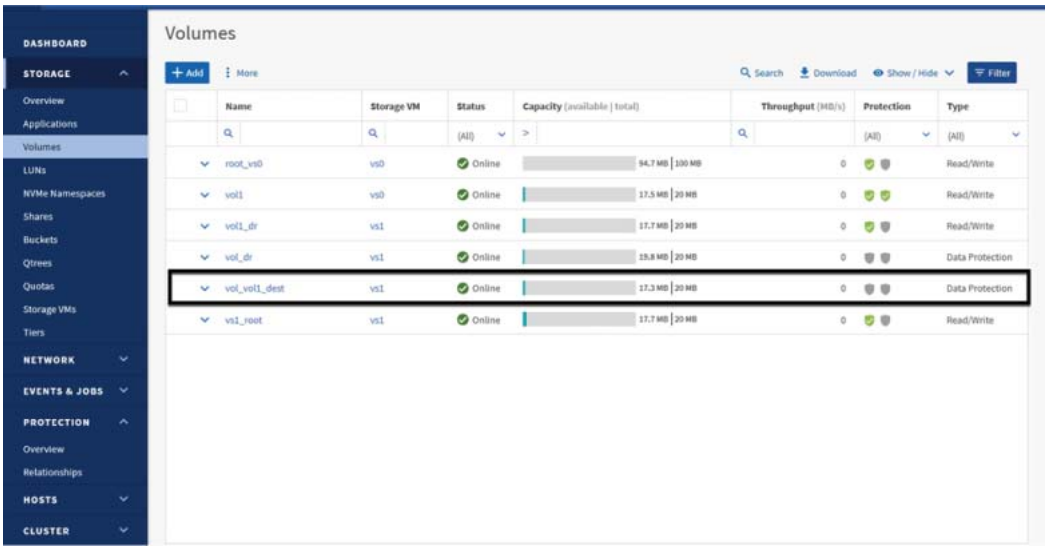

**8** `snapmirror show` コマンドを実行して、作成されたユニファイドレプリケーション関係のステータスを確認します。

```
Remote::> snapmirror show
                                                                   Progress
Source            Destination  Mirror  Relationship  Total         Last
Path        Type  Path         State   Status        Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
vs0:vol1
            XDP  vs1:vol_vol1_dr
                              Snapmirrored
                                      Idle           -         true    -
```

SnapMirror 関係のタイプが `MirrorAllSnapshots` になります。



**9** デスティネーションボリュームのタイプが `rw` から `dp` に変更されます。



# 第 6 章
# SnapMirror と ONTAP 機能の相互作用

## 6.1 SnapMirror と Snapshot コピー

SnapMirror は、レプリケーション更新を実行する前に Snapshot コピーを作成します。SnapMirror Snapshot コピーがソースボリューム上に作成され、`sm_created` の Snapshot コピーラベルが適用されます。新しい Snapshot コピーは、データ保護ボリュームにレプリケートされた以前の SnapMirror Snapshot コピーと比較されます。新しい SnapMirror Snapshot コピーと前の SnapMirror Snapshot コピー (2 つの SnapMirror Snapshot コピー間のボリューム上のすべての Snapshot コピーと、それらの Snapshot コピー内のすべてのデータを含む ) の間のデータ変更の差分は、デスティネーションボリュームに複製されます。SnapMirror の更新が完了すると、新しい SnapMirror Snapshot コピーがデスティネーションシステムにエクスポートされます。SnapMirror は、1 つの SnapMirror Snapshot コピーの履歴をソースボリュームに保持し、2 つの SnapMirror Snapshot コピーの履歴をデスティネーションボリュームに保持します。

### ■ ベストプラクティス

SnapMirror更新が、ソースボリューム上で他のSnapshotコピーと同時に実行されるようにスケジュールされていないことを確認します。

ONTAP は、SnapMirror によって作成された Snapshot コピーが誤って削除されないように、これらの Snapshot コピーがスケジュールされた更新を実行するために必要であるという理由で、Snapshot コピーに対してロックを維持します。SnapMirror で作成された Snapshot コピーを削除する必要がある場合でも、ボリュームを再同期できます。2 つのボリューム間で共通する Snapshot コピーがボリューム上に他にもまだ存在する場合は、完全なベースラインを実行する必要はありません。

次の例では、SnapMirror によって作成されたすべての Snapshot コピーが削除されたボリュームに対して SnapMirror 再同期が実行され、1 時間ごとの Snapshot コピーが再同期のベースとして使用されます。

```
cluster02::> snapmirror resync -source-path cluster01://vs1/vol1 -destination-path
cluster02://vs2/vol1
Warning: All data newer than Snapshot copy hourly.2011-12-06_1805 on volume cluster02://vs2/vol1
will be deleted.
Do you want to continue? {y|n}: y
[Job 1364] Job is queued: snapmirror resync to destination cluster02://vs2/vol1.
```

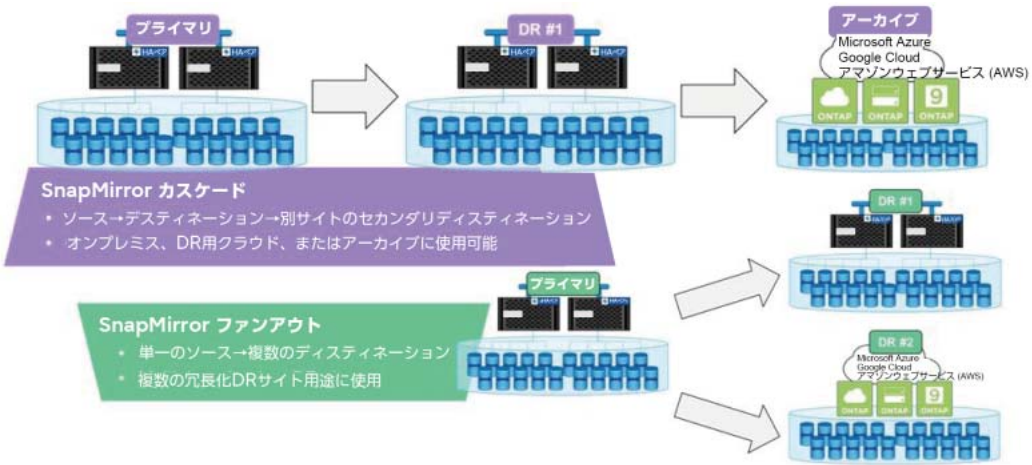
# 6.2　SnapMirror と Qtree

Qtree は、NAS のファイルシステムクォータの適用を可能にする特別なディレクトリです。ONTAP を使用すると、qtree を作成できます。また、SnapMirror を使用して複製されるボリュームに qtree を置くこともできます。ただし、SnapMirror レプリケーションはボリュームレベルでのみ動作するため、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を実行することはできません。

# 6.3　SnapMirror ボリュームと FlexGroup ボリューム

ONTAP 9.9.1 から、SnapMirror はカスケードおよびファンアウト構成のソースおよびデスティネーションとして FlexGroup ボリュームをサポートしています (図 6.1)。デスティネーションには、オンプレミスまたはクラウドホスト型の Cloud Volumes ONTAP クラスタを使用できます。

図 6.1　SnapMirror カスケードおよびファンアウト構成で使用される FlexGroup ボリューム



# 6.4　SnapMirror による SVM 保護

SVM DR は、SnapMirror により SVM を保護する機能です。SVM DR には、SVM が所有する FlexVol と FlexGroup ボリューム、および SVM 設定と ID 情報の、リモートデスティネーションへの複製が含まれます。SVM DR は、ボリュームに対して SnapMirror と同じ SnapMirror レプリケーションテクノロジーを使用しますが、いくつかの違いがあります。

表 6.1　SVM DR と SnapMirror の違い

| SVM DR | SnapMirror |
|---|---|
| SVM レベルの粒度で動作 | ボリュームレベルの粒度で動作 |
| FlexVol および FlexGroup データと SVM 構成を保護 | FlexVol および FlexGroup ボリュームに保存されたデータのみを保護 |
| サポートされる最少 RPO ( 目標復旧ポイント ) は 15 分 | サポートされる最小 RPO は 5 分 |

表 6.2　SVM DR スケーラビリティ

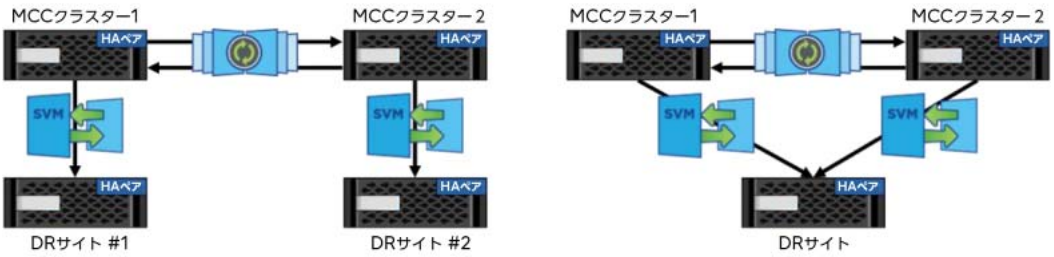
| ONTAP バージョン | サポートされるデータ保護関係 |
|---|---|
| ONTAP 9.9 以前 | クラスタごとに 32 |
| ONTAP 9.10.1 | クラスタごとに 64 |
| ONTAP 9.11.1 | クラスタごとに 128 |

データ保護関係にある SVM は、最大 600 個の FlexVol ボリュームをホストできます。

snapmirror create コマンドの `-identity-preserve` パラメータと `-discard-configs` パラメータを使用すると、SVM DR を 2 つのモードで設定できます。

ONTAP 9.11.1 では、MetroCluster 関係のいずれかの端にある SVM を SVM DR のソース SVM として使用できます。MetroCluster と SVM DR を組み合わせて使用すると、3 拠点の DR トポロジを構築できます。このトポロジは、ローカルまたは大都市間の距離での継続的な可用性と、より長い距離での DR 機能を提供し、3 つの拠点すべてで SVM ID を維持する機能を備えています ( 図 6.2)。

図 6.2　MetroCluster を使用した SVM DR



## 6.4.1　FlexGroup ボリュームに対する SVM DR サポート

ONTAP 9.9.1 以降では、SVM DR を FlexGroup ボリュームで使用できます。このサポートにより、デスティネーションクラスタに転送される SnapMirror SVM 関係は、FlexGroup ボリュームを完全に認識したままで、DR シナリオでこれらのボリュームを適切にマウントします。

FlexGroup ボリュームを使用する SVM DR では、次の機能はサポートされません。

- FabricPool
- ソースまたはデスティネーションクラスタ上の FlexClone ボリューム
- SnapMirror ファンアウト構成
- SnapMirror カスケード構成
- FlexVol ボリュームから FlexGroup ボリュームへの変換

## 6.4.2　SVM データモビリティ

SVM データモビリティは、クラスタ管理者が SVM( データおよび SVM 設定情報を含む ) をクラスタ間で移動できるようにする機能です。この機能は、移動する SVM に以前の SVM DR 関係が設定されているかどうかに依存しません。

SVM 移行は SAN プロトコルをサポートしません。

SVM 移行では、SVM ごとに最大 100 の FlexVol ボリュームがサポートされます。

ほとんどの NFSv3、NFSv4.1、および NFSv4.2 のワークロードでは、ETERNUS AX series の HA ペア間で無停止 (NDO) の SVM 移行がサポートされています。

ONTAP 9.11.1 以降、SVM 移行では、ソースクラスタまたはデスティネーションクラスタで最大 3 つの HA ペアを持つクラスタがサポートされます。ONTAP 9.11.1 より前のバージョンでは、SVM 移行は単一の HA ペアを持つクラスタでのみサポートされていました。

データ保護関係にある SVM は、最大 600 個の FlexVol ボリュームをホストできます。

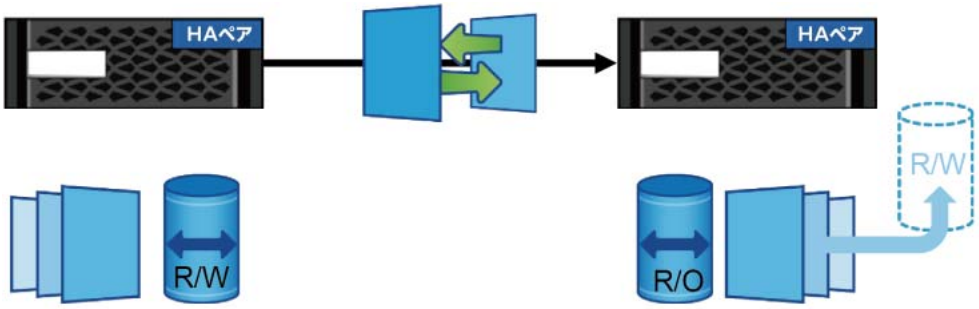
表 6.3　SVM 移行制限の概要

| 特徴 | SVM データモビリティ |
|---|---|
| スケール | 100 個の FlexVol ボリューム<br>6 つのノードクラスタ |
| ネットワーク | RTT 遅延が 2 ミリ秒未満の L2 |
| プラットフォーム | ETERNUS AX series のみ<br>ONTAP バージョン 9.10.1 以降 |
| プロトコル | NFSv3、NFSv4.1、NFSv4.2 |
| データ管理 | Snapshot コピー<br>ストレージ効率 |
| データセキュリティ | VE<br>OKM<br>外部キー管理 (EKM) |

# 6.5　SnapMirror および FlexClone テクノロジー

FlexClone テクノロジーにより、SnapMirror のレプリケーションプロセスを中断することなく、読み取り専用のSnapMirrorのデスティネーションボリュームから書き込み可能なボリュームを作成できます。SnapMirror 関係は FlexClone ボリュームをソースとして使用して作成できますが、SnapMirror デスティネーションボリュームを FlexClone ボリュームにすることはできません。図 6.3 は、SnapMirror デスティネーションでの FlexClone ボリュームの作成を示しています。

図 6.3　SnapMirror デスティネーションでの FlexClone ボリュームの作成




SnapMirror は、Snapshot コピー履歴をソースボリュームからデスティネーションボリュームに複製します。ソースボリュームから Snapshot コピーが削除されると、次の SnapMirror 更新によって、その Snapshot コピーがデスティネーションボリュームから削除されます。その Snapshot コピーが FlexClone ボリュームの基本 Snapshot コピーである場合、SnapMirror 更新は失敗します。SnapMirror 更新を続行する唯一の方法は、FlexClone ボリュームを削除するか分割して、Snapshot コピーの依存関係を削除することです。

SnapMirror デスティネーションで FlexClone ボリュームを作成する際にこの問題を回避するには、図 6.3 に示すように、ソースシステムで FlexClone ボリュームに必要な基本の Snapshot コピーを手動で作成します。FlexClone ボリューム用にこの方法で特別に作成された Snaspshot コピーを使用すると、自動的に作成された Snaspshot コピーがソースシステムから削除されるため、SnapMirror の更新が失敗するのを防ぐことができます。この Snaspshot コピーに関連づけられたラベルでは、有効な SnapMirror レプリケーションポリシールールに関連づけられたラベルも使用しないでください。これにより、既存のラベルを使用する Snaspshot コピーの保存ポリシーが、FlexClone ボリュームに関連付けられた Snaspshot コピーを削除することがありません。

# 6.6　SnapMirror とのストレージ効率

SnapMirrorは、レプリケートされたボリュームにおけるストレージ効率のメリットを維持します。ソースボリュームが重複排除されている場合、デスティネーションボリュームも重複排除された状態になります。SnapMirror は、転送中に重複排除されたデータを拡張しません。ソースボリュームが圧縮されている場合、デスティネーションボリュームも圧縮された状態になります。圧縮ボリュームのレプリケーションでは、転送用のデータを読み取るためにソースボリュームが解凍されることはありません。むしろ、データは圧縮された状態でデスティネーションボリュームにレプリケートされます。

従来の SnapMirror 関係 (`type -dp`) を使用している場合、ソースボリュームとデスティネーションボリュームに対して異なるストレージ効率構成を有効にすることはできません。たとえば、SnapMirror ソースボリュームで圧縮または重複排除を有効にしないと、SnapMirror デスティネーションボリュームだけを圧縮または重複排除することはできません。

SnapMirror は、更新転送を実行する前に Snapshot コピーを作成します。Snapshot コピー内のブロックはロックされ、重複排除できません。したがって、重複排除による最大の領域節約が必要な場合は、SnapMirror 更新を実行する前に重複排除プロセスを実行します。

## ■ ベストプラクティス

重複排除と SnapMirror オペレーションが同時に実行されないようにします。重複排除操作が完了したら、重複排除ボリュームの SnapMirror 転送を開始する必要があります。これにより、重複排除の進行中にレプリケーションのパフォーマンスに影響が及ぶことを防ぎ、重複排除されていないデータと追加の一時的な重複排除メタデータファイルをネットワーク経由で送信することを防ぎます。

# 6.7　SnapMirror とボリューム移動

ボリューム移動機能を使用すると、volume move コマンドを使用して、クラスタ内のノード間で無停止でボリュームを移動できます。ボリューム移動の実行時に、ソースまたはデスティネーションで SnapMirror 関係を再構成または変更する必要はありません。クラスタ間 SnapMirror 関係にあるボリュームを移動する場合、SnapMirror 更新を正常に実行するには、ボリュームの移動先のノードにクラスタ間 LIF があり、クラスタインターコネクトネットワークに接続されている必要があります。

ボリューム移動が SnapMirror 関係に与える影響は、ソースボリュームまたはデスティネーションボリュームのどちらを移動するかによって異なります。SnapMirror 転送が現在進行中で、SnapMirror ソースボリュームを移動する場合、SnapMirror 転送とボリューム移動転送の両方を同時に実行できます。ただし、ボリューム移動のカットオーバーが発生すると (ONTAP が I/O を新しいボリュームにリダイレクトする瞬間 )、アクティブな SnapMirror 転送は一時的に中断され、ソースボリュームの新しい場所から自動的に続行されます。

## 6.8　SnapMirror によるドライブシェルフ障害保護

同じクラスタ上の異なる HA ペアのノードにボリュームをミラー化できます。別の HA ペアにミラーリングすると、別のボリュームが常に別のドライブシェルフにあることを確認できます。同じノード上の別のドライブシェルフにミラーしようとする場合、ミラーは別のアグリゲートに存在する必要があります。ドライブの障害とスペアの割り当てが原因で、アグリゲートがドライブシェルフの構成ドライブを使用するリスクがまだあります。この構成により、単一点障害が回避され、ドライブシェルフの障害から保護されます。

ここでの注意点は、構成が自動的にフェイルオーバーしないことです。SnapMirror 関係を手動で解除し、クライアントをアンマウントし、デスティネーションボリュームにクライアントを再マウントして、NFS エクスポートポリシーを変更する必要があります。

## 6.9　SnapMirror とボリュームの自動サイズ設定

SnapMirror XDP 関係を使用すると、XDP 関係で使用される LRSE に備わっている統合データ効率により、ソースのより大きなボリュームをデスティネーションのそれより小さなボリュームにミラーリングできます。デスティネーションボリュームのサイズはソースボリュームと同程度 ( またはそれ以上 ) にし、Autosize オプションを有効にすることをお勧めします。

### ■ ベストプラクティス

- デスティネーションボリュームの Auto Grow オプションを有効にした状態で、ソースボリュームとデスティネーションボリュームのサイズを同じにするか、デスティネーションボリュームの方が少し大きくなるように設定します。
- ソースで Autosize 設定が有効になっている場合、SnapMirror 転送に十分な容量を確保するために、デスティネーションでは Auto Grow 設定を有効にすることを推奨します。

Autosize 設定によって SnapMirror 関係のソースボリュームのサイズが大きくなると、デスティネーションボリュームのサイズも自動的に大きくなります。

# 6.10　SnapMirror と NDMP

NDMP バックアップは、SnapMirror のソースボリュームまたはデスティネーションボリュームのいずれかから実行できます。SnapMirror デスティネーションがダンプエンジンを使用してテープにバックアップされる場合、ボリューム内のデータのみがバックアップされます。ただし、SnapMirror デスティネーションが SMTape を使用してテープにバックアップされる場合は、メタデータもバックアップされます。SnapMirror 関係および関連するメタデータはテープにバックアップされません。したがって、リストア時には、そのボリューム上のデータのみがリストアされますが、関連する SnapMirror 関係はリストアされません。ソースボリュームからではなく、SnapMirror デスティネーションボリュームから NDMP バックアップを実行することには、次のようなメリットがあります。

- SnapMirror 転送は迅速に実行でき、ソースシステムへの影響は少なくなります。バックアップの最初の段階として Snapshot コピーを使用し、プライマリシステムから SnapMirror レプリケーションを実行して、バックアップウィンドウを大幅に短縮または排除します。次に、セカンダリシステムからテープへの NDMP バックアップを実行します。
- SnapMirror のソースボリュームは、デスティネーションの DR ボリュームに比べると、本番環境を最適化するために移動される可能性が高くなります。

# 6.11　SnapMirror と FabricPool

SnapMirror レプリケーション間隔は、FabricPool 階層化ポリシーよりも低い値に設定して、すべてのデータが確実に保護されるようにする必要があります。FabricPool だけでは、データ保護戦略にはなりません。

# 第 7 章
# パフォーマンス

レプリケーションのパフォーマンスに影響を与える要因は複数あります。

- ノードの CPU 使用率
  CPU は、アプリケーションのデータアクセスやデータ保護操作などの様々なデータ操作に共有されます。
- 同時 SnapMirror 操作数
  各転送操作では、データを移動するために追加の CPU サイクルとネットワーク帯域幅が必要です。特定の時間に発生する同時転送が少ないほど、各転送操作の完了が速くなります。サポートされる同時転送の数は、ノードモデルと ONTAP バージョンによって異なります。
- 転送のタイプ：初期転送または更新
  新しい SnapMirror 関係を作成した場合は、SnapMirror 関係の初期設定時にボリューム内のすべてのデータを含むベースライン Snapshot コピーを転送する必要があります。その後の更新では、前回の SnapMirror　Snapshot コピー作成以降の差分データの変更のみが転送されます。
- ノードハードウェアタイプ
  ノードモデルの構成 ( ドライブタイプ、アグリゲート内のドライブ数、アグリゲート内のボリューム数、およびクラスタインターコネクトネットワークの物理ポートタイプを含む ) は、SnapMirror のパフォーマンスに直接影響します。

# 7.1　パフォーマンスのための SnapMirror および SnapVault スループットの計算

関係のスループットは、設定された期間に移動されたデータ量に基づいて決定できます。スループットを確認するには、「Last Transfer Size」フィールドと「Last Transfer Duration」フィールドに注目してください。転送スループットを調べるには、転送サイズを転送時間で割ります。

```
cluster::> snapmirror show -destination-path vs3:dst -instance

                            Source Path: vs1:src_test
                       Destination Path: vs3:dst
                      Relationship Type: DP
                  Relationship Group Type: none
                      SnapMirror Schedule: -
                   SnapMirror Policy Type: async-mirror
                      SnapMirror Policy: DPDefault
                            Tries Limit: -
                      Throttle (KB/sec): unlimited
                          Mirror State: Snapmirrored
                      Relationship Status: Transferring
                  File Restore File Count: -
                   File Restore File List: -
                      Transfer Snapshot: snapmirror.89659724-bd35-11e4-9f11-
000c299bf0b8_2147484674.2015-03-02_134417
                      Snapshot Progress: 0B
                         Total Progress: 0B
                Network Compression Ratio: 2:1
                      Snapshot Checkpoint: 0B
                         Newest Snapshot: snapmirror.89659724-bd35-11e4-9f11-
000c299bf0b8_2147484674.2015-02-25_134212
                Newest Snapshot Timestamp: 02/25 13:22:08
                      Exported Snapshot: snapmirror.89659724-bd35-11e4-9f11-
000c299bf0b8_2147484674.2015-02-25_134212
              Exported Snapshot Timestamp: 02/25 13:22:08
                                  Healthy: true
                       Unhealthy Reason: -
                 Constituent Relationship: false
                  Destination Volume Node: vsim
                          Relationship ID: d8b4cbc8-bd36-11e4-9f11-000c299bf0b8
                    Current Operation ID: 46da2fc6-c125-11e4-9f1a-000c299bf0b8
                           Transfer Type: update
                          Transfer Error: -
                       Current Throttle: unlimited
                Current Transfer Priority: normal
                      Last Transfer Type: initialize
                     Last Transfer Error: -
                      Last Transfer Size: 240GB
Last Transfer Network Compression Ratio: 3.1:1
                  Last Transfer Duration: 02:13:32
                      Last Transfer From: vs1:src_test
              Last Transfer End Timestamp: 02/25 13:42:15
                    Progress Last Updated: 03/02 13:44:17
                  Relationship Capability: 8.2 and above
                                 Lag Time: 120:22:10
            Number of Successful Updates: 0
                Number of Failed Updates: 0
            Number of Successful Resyncs: 0
                Number of Failed Resyncs: 0
             Number of Successful Breaks: 0
                 Number of Failed Breaks: 0
                    Total Transfer Bytes: 245760
          Total Transfer Time in Seconds: 3
```

# 7.2　SnapMirror とネットワーク圧縮

ネットワーク帯域幅コストの増加とデータの増加に伴い、お客様はより少ないリソースでより多くの成果を上げる必要があります。保護対象のデータ量が増加すると、RPO( 目標復旧時点 ) を維持するために必要なネットワーク帯域幅が増加します。そうしないと、ネットワーク経由で DR サイトに送信されるデータの量が増えるにつれて、レプリケーション時間が長くなります。つまり、ネットワーク帯域幅を増加させたくない場合、または増加させることができない場合は、RPO 値が大きくなる原因となっているレプリケーションの頻度を下げる必要があるため、データ消失のリスクが増大します。

SnapMirror のネイティブネットワーク圧縮機能を使用すると、ネットワーク経由で複製されるデータ量を削減できます。また、次のセクションで説明するように、柔軟性と選択肢が増えます。

## 7.2.1　同じ RPO レベルの維持

- **課題**
  データレプリケーションのニーズは増大しています。同じレベルの RPO を維持するためには、より多くの帯域幅が必要です。
- **解決策**
  ネットワーク圧縮を使用すると、ネットワーク帯域幅を増やさずに同じ RPO を維持できます。

## 7.2.2　帯域幅を増やさずに RPO を向上

- **課題**
  すべてのネットワーク帯域幅を使用しています。ただし、お客様はデータ消失のリスクを軽減し、RPO を向上させたいと考えています。
- **解決策**
  ネットワーク圧縮を使用すると、ネットワーク帯域幅を増やさずに RPO を向上させることができます。

## 7.2.3　ネットワーク帯域幅を他の目的に使用する

- **課題**
  レプリケーションによってすべての帯域幅が消費されています。帯域幅を増やさずに、クライアントアクセスやアプリケーションなどの目的でネットワーク帯域幅を使用する場合。
- **解決策**
  ネットワーク圧縮を使用すると、RPO を犠牲にすることなく SnapMirror が消費する帯域幅を削減できるため、他の目的のためにネットワーク帯域幅を解放できます。

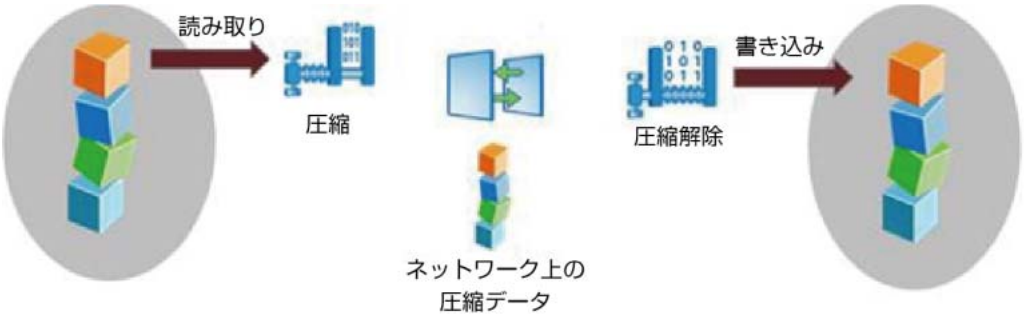
## 7.2.4　初期転送の高速化

- **課題**
  SnapMirror の初期転送はサイズが大きくなる可能性があるため、帯域幅の制約があると完了までに長い時間がかかる場合があります。
- **解決策**
  ネットワーク圧縮を使用すると、最初の SnapMirror 転送を高速化できます。

## 7.2.5　SnapMirror ネットワーク圧縮とは？

ネットワーク圧縮は SnapMirror に組み込まれているため、ネットワークを介したより効率的な SnapMirror 転送が可能です。ただし、保存されているデータは圧縮されません。SnapMirror のネットワーク圧縮は、ボリューム圧縮とは異なります。図 7.1 は、SnapMirror ネットワーク圧縮の非常に大まかなフローを示しています。

図 7.1　SnapMirror のネットワーク圧縮機能の図




ソースシステムでは、デスティネーションシステムに送信する必要のあるデータブロックが圧縮エンジンに渡され、データブロックが圧縮されます。ソースシステムの圧縮エンジンは、ストレージシステムで使用可能な CPU の数に応じて、複数のスレッドを作成します。これらの圧縮スレッドは、データを並列に圧縮するのに役立ちます。圧縮されたブロックはネットワークを介して送信されます。

デスティネーションシステムでは、圧縮されたブロックが受信され、マルチスレッドを使用して並列に解凍されます。圧縮解除されたデータは、適切なボリュームに書き込まれます。

## 7.2.6　ネットワーク圧縮を有効または無効にする

SnapMirror ネットワーク圧縮は、SnapMirror ポリシーの `-is-network-compression-enabled` オプションで有効または無効にできます。アクティブな転送では有効にできません。既存の転送で圧縮を有効にするには、まず転送を中止し、SnapMirror ポリシーで `-is-network-compression-enabled` オプションを true に設定してから、転送を再開する必要があります。

### ■ ベストプラクティス

SnapMirror ネットワーク圧縮により、SnapMirror のソースシステムとデスティネーションシステムの両方でリソース使用率が向上します。したがって、圧縮を展開する前に、リソースの使用率と利点を評価する必要があります。たとえば、高帯域幅で低遅延の接続では、圧縮は役に立ちません。ただし、WAN 接続など、比較的帯域幅の狭い接続には便利です。

## 7.2.7　圧縮率のレポート

SnapMirror のネットワーク圧縮率は、`snapmirror show-instance` の出力で報告されます。

```
cluster::> snapmirror show -destination-path vs3:dst -instance

                            Source Path: vs1:src_test
                       Destination Path: vs3:dst
                      Relationship Type: DP
                Relationship Group Type: none
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: async-mirror
                      SnapMirror Policy: DPDefault
                            Tries Limit: -
                      Throttle (KB/sec): unlimited
                           Mirror State: Snapmirrored
                    Relationship Status: Transferring
                File Restore File Count: -
                 File Restore File List: -
                      Transfer Snapshot: snapmirror.89659724-bd35-11e4-9f11-
000c299bf0b8_2147484674.2015-03-02_134417
                      Snapshot Progress: 0B
                         Total Progress: 0B
              Network Compression Ratio: 2:1
                    Snapshot Checkpoint: 0B
                        Newest Snapshot: snapmirror.89659724-bd35-11e4-9f11-
000c299bf0b8_2147484674.2015-02-25_134212
               Newest Snapshot Timestamp: 02/25 13:22:08
                      Exported Snapshot: snapmirror.89659724-bd35-11e4-9f11
000c299bf0b8_2147484674.2015-02-25_134212
            Exported Snapshot Timestamp: 02/25 13:22:08
                                Healthy: true
                       Unhealthy Reason: -
                 Constituent Relationship: false
                  Destination Volume Node: vsim
                          Relationship ID: d8b4cbc8-bd36-11e4-9f11-000c299bf0b8
                     Current Operation ID: 46da2fc6-c125-11e4-9f1a-000c299bf0b8
                            Transfer Type: update
                           Transfer Error: -
                       Current Throttle: unlimited
              Current Transfer Priority: normal
                     Last Transfer Type: initialize
                    Last Transfer Error: -
                     Last Transfer Size: 240KB
Last Transfer Network Compression Ratio: 1:1
                  Last Transfer Duration: 0:0:3
                     Last Transfer From: vs1:src_test
            Last Transfer End Timestamp: 02/25 13:42:15
                  Progress Last Updated: 03/02 13:44:17
                  Relationship Capability: 8.2 and above
                                 Lag Time: 120:22:10
           Number of Successful Updates: 0
               Number of Failed Updates: 0
           Number of Successful Resyncs: 0
               Number of Failed Resyncs: 0
            Number of Successful Breaks: 0
                Number of Failed Breaks: 0
                   Total Transfer Bytes: 245760
         Total Transfer Time in Seconds: 3
```

圧縮率は転送状態でのみ表示されます。

# 7.3　SnapMirror スロットル

SnapMirror スロットル設定は、消費されるネットワーク帯域幅を抑制するために使用され、クラスタ間 SnapMirror で使用される帯域幅の量が制限されます。つまり、SnapMirror スロットルはネットワーク帯域幅を制御しません。むしろ、WAFL が SnapMirror 転送に使用できるブロックを制限することで機能します。

**注 意**

ONTAP のすべてのレプリケーションスロットルの単位は KB/ 秒です。

SnapMirror スロットルは、`-throttle` オプションを使用し、`snapmirror modify` コマンドで既存の関係を変更することで、新しい関係の作成時に関係に基づいて設定できます。この例では、`snapmirror modify` コマンドを使用して 10MB/ 秒のスロットルを既存の関係に適用しています。

```
cluster02::> snapmirror modify -destination-path cluster02://vs1/vol1 -throttle 10240
```

**注 意**

- アクティブな SnapMirror 関係のスロットルを変更するには、既存の転送を終了して再開し、新しい値を使用します。SnapMirror は、最初からやり直すのではなく、新しいスロットル値を使用して、最後の再開チェックポイントから転送を再開します。
- クラスタ内スロットルがサポートされており、クラスタ間スロットルと同様に動作します。

ONTAP 9 では、クラスタ内の各ノードで実行可能なグローバル SnapMirror スロットルが導入されています。これにより、発信および着信転送用の固定最大帯域幅で SnapMirror 転送が実行されます。SnapMirror グローバルスロットリングは、SnapMirror および SnapVault の送受信で使用される帯域幅を制限します。この制限は、クラスタ内のすべてのノードでクラスタ全体に適用されます。この機能は、前述の各 SnapMirror 関係のスロットルに追加されます。各ノードには、送信側 ( 発信 ) 転送だけでなく、受信側 ( 着信 ) 転送のグローバルスロットルと、このスロットルを有効または無効にするオプションがあります。転送単位スロットルは、グローバルノードスロットル値を超えると、ノードレベルのスロットルに制限されます。それ以外の場合は、指定した値で転送が行われます。

グローバルスロットルは、SnapMirror 転送および SnapVault 転送の関係ごとのスロットル機能と連動します。関係ごとのスロットルは、関係ごとの転送の総帯域幅がグローバルスロットルの値を超えるまで適用され、その後グローバルスロットルが適用されます。スロットル値 0 は、グローバルスロットルが無効であることを意味します。

**注 意**

SnapMirror Synchronous 関係があるクラスタでは、グローバルスロットルを有効にしないでください。

最小スロットル帯域幅は 4KBps、最大スロットル帯域幅は 2TBps です。スロットル帯域幅が 0 の場合は、転送がスロットルされていないか、帯域幅が無制限であることを意味します。

スロットリングを制御する新しいクラスタ全体のオプションは次のとおりです。

```
cluster::> options replication*

cluster
   replication.throttle.enable       on                  -
   replication.throttle.incoming.max_kbs
                                     4000                -
   replication.throttle.outgoing.max_kbs
                                     2000                -
3 entries were displayed.
```

各エントリは個別に編集できます。enable オプションは、発信スロットルと着信スロットルの両方を有効または無効にします。

```
cluster::> options replication.throttle.enable on
1 entry was modified.
```

発信スロットルと着信スロットルの変更は、enable オプションがオンの場合にのみ実際の転送に反映されます。発信スロットル値と着信スロットル値は、enable オプションの値に関係なく変更できます。

```
cluster::> options replication.throttle.outgoing.max_kbs 8000
1 entry was modified.

cluster::> options replication.throttle.incoming.max_kbs 5000
1 entry was modified.
```

# 7.4　TCP 受信バッファサイズを変更する方法

SnapMirror は、クラスタ間 (WAN ネットワーク ) およびクラスタ内 (LAN ネットワーク ) の両方の複製に対して、調整可能な TCP 受信バッファウィンドウを持つネットワークサービス ctlopcp を使用します。TCP 受信バッファウィンドウはクラスタごとに構成され、TCP 受信バッファサイズの増加はすぐに有効になり、再起動の必要はありません。

表 7.1　TCP 受信バッファウィンドウ

| | デフォルト | 最小値 | 最大値 |
|---|---|---|---|
| クラスタ間 TCP 受信バッファウィンドウ | 2MB | 256KB | 7MB |
| クラスタ内 TCP 受信バッファウィンドウ | 256KB | 256KB | 7MB |

# 7.5　同時レプリケーションオペレーション

サポートされる同時 SnapMirror オペレーションの数には制限があります。この制限はノード単位であり、プラットフォームと ONTAP のバージョンによって異なります。1 つのノードで同時に実行できる SnapMirror 操作の数については、富士通マニュアルサイトの「FUJITSU Storage ETERNUS AX/HX series データ保護パワーガイド」を参照してください。

## ■ ベストプラクティス

- 同時オペレーションを計画する場合は、SnapMirror レプリケーションに加えて、環境内でのボリューム移動およびボリュームコピーオペレーションの頻度を考慮することがベストプラクティスです。
- CPU ワークロードを実行できるだけの十分な CPU ヘッドルームを使用して、システムのサイズを正しく設定します。

ONTAP は、2 つのノードを超えるクラスタの拡張を可能にすることで、より高いレベルのスケーラビリティを提供します。クラスタ内の各ノードは、そのノードが所有するボリュームの複製に使用される CPU リソースとメモリーリソースを提供します。

## ■ ベストプラクティス

レプリケーションを最適化するには、レプリケーションを必要とするすべてのボリュームを 1 つのノードに配置するのではなく、クラスタ内の異なるノードにレプリケートされたボリュームを分散します。このベストプラクティスでは、クラスタ内のすべてのノードが複製アクティビティーを共有できます。

# 7.6　推奨されるレプリケーション間隔

SnapMirror 更新では、ソースノードとデスティネーションノード間の通信セッションを確立し、Snapshot コピーを作成および削除して、デスティネーションに送信するデータブロックを決定する必要があります。したがって、ONTAP スケジューラは毎分実行されるスケジュールの作成をサポートしていますが、SnapMirror 更新操作を毎分実行することは推奨されません。

# 7.7　ネットワークサイズの要件

SnapMirror を導入する場合、ネットワーク距離によって書き込みレイテンシが発生するため、ソースからデスティネーションストレージシステムへのパケットの往復移動時間を考慮する必要があります。アプリケーションのパフォーマンスに影響を与えないように、システムデータの転送に使用できる適切な帯域幅を持つネットワークが、目的のレプリケーション間隔をサポートするために必要です。クラスタ間レプリケーションでサポートされるネットワーク特性には制限があります。

## 7.7.1　クラスタ間レプリケーションのネットワークサイズ要件

クラスタインターコネクトネットワークのサイズは、ソリューションの RPO と個々のノードのパフォーマンス特性を満たすために、データ変更率と更新間隔に応じて適切に設定する必要があります。クラスタ間 SnapMirror は、次の特性を持つネットワーク間でサポートされます。

- 最小帯域幅が 0.5Mbps
- パケット損失が 1%

### ■ ベストプラクティス

クラスタ間レプリケーションに使用されるすべてのパスは、同じパフォーマンス特性を持つ必要があります。ノードが低速パス上に 1 つのクラスタ間 LIF を持ち、高速パス上に別のクラスタ間 LIF を持つようにマルチパスを構成すると、データが両方のパスに同時に多重化されるため、パフォーマンスが低下します。

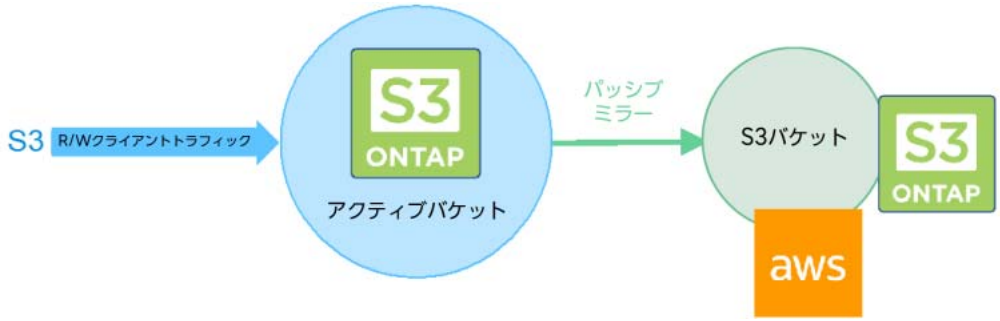
## 7.7.2　クラスタ内レプリケーションのためのネットワークサイジング要件

SnapMirror、ボリューム移動、およびボリュームコピー操作などのすべてのクラスタ内転送では、同じクラスタ内のノード間でプライベートクラスタインターコネクトが使用されます。

# 第 8 章
# S3 SnapMirror

ONTAP 9.10.1 は ONTAP S3 SnapMirror を導入しました。S3 SnapMirror は、ONTAP S3 オブジェクトストア用のネイティブレプリケーションおよびバックアップソリューションをお客様に提供します。S3 SnapMirror では、別の ONTAP S3 バケット、ONTAP Cloud Volumes ONTAP S3 バケット、AWS S3 などのクラウドが提供するネイティブの S3 バケットなど、データ保護と DR 用のさまざまな S3 ターゲットがサポートされています (図 8.1)。

図 8.1　ONTAP S3 SnapMirror の概要




S3 SnapMirror は、FlexVolume および FlexGroup 非同期レプリケーション用に SnapMirror で使用される標準の LRSE レプリケーションエンジンとは異なる、専用のレプリケーションエンジンを使用します。S3 SnapMirror 関係を設定するときに使用されるレプリケーション保護ポリシーは Continuous (`-type continuous`) です。

# 第 9 章
# 相互運用性

富士通サポートサイトでサポート組み合わせ表を参照して、このドキュメントで説明されている製品と機能のバージョンが、ご使用の環境でサポートされているかどうかを確認してください。サポート組み合わせ表は、富士通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とバージョンを定義します。具体的な結果は、公開されている仕様に従ったお客様のインストール状況によって異なります。SnapMirror 関係を作成する前に、ソースボリュームとデスティネーションボリュームが互換性のある ONTAP バージョンを実行中であることを確認する必要があります。

# 第 10 章
# トラブルシューティングのヒント

## 10.1　クラスタピアの関係のトラブルシューティング

手順 ▶▶▶

1. `cluster peer show` コマンドを実行して、クラスタピア関係の可用性を確認します。
このコマンドは、既存の構成済みクラスタピアの関係をすべて表示します。

```
cluster01::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
------------------------- --------------------- ---------------
cluster02                 1-80-000013           Available
```

2. クラスタピアの詳細情報を表示するには、コマンドに `-instance` を追加します。
特定のクラスタの結果を表示するには、`-cluster <cluster name>` を含めます。
`-instance` オプションは、クラスタ間通信に使用されるリモートアドレスを表示します。

```
cluster01::> cluster peer show -cluster cluster02 -instance
            Peer Cluster Name: cluster02
Remote Intercluster Addresses: 10.12.12.3,10.12.12.4
                Availability: Available
          Remote Cluster Name: cluster02
          Active IP Addresses: 10.12.12.3,10.12.12.4
        Cluster Serial Number: 1-80-000013
```

**3** `cluster peer ping` コマンドを実行して、各クラスタ間アドレス間の接続に関する情報 (RTT 応答時間など ) を表示します。複数のクラスタピアが構成されている場合は、`-cluster <cluster_name>` オプションを使用して、特定のピア関係に対して ping を実行します。`cluster peer ping` コマンドは、クラスタ間インターフェイス間での ping の結果を表示します。前述のように、ローカルクラスタとリモートクラスタ間の複数のパスでクラスタ間 SnapMirror ミラーリングを実行する場合、各パスのパフォーマンス特性は同じである必要があります。この例では、ping 応答時間 (RTT) は、デスティネーションクラスタが `cluster 02` と表示されているノードへの ping と比較的同じです。

```
cluster01::> cluster peer ping cluster02

Node: cluster01-01            Destination Cluster: cluster01
Destination Node IP Address       Count TTL  RTT(ms) Status
---------------- ---------------- ----- ---- ------- --------------------
cluster01-01     10.12.12.1       1     255  0.186   interface_reachable
cluster01-02     10.12.12.2       1     255  1.156   interface_reachable

Node: cluster01-01            Destination Cluster: cluster02
Destination Node IP Address       Count TTL  RTT(ms) Status
---------------- ---------------- ----- ---- ------- --------------------
cluster02-01     10.12.12.3       1     255  7.164   interface_reachable
cluster02-02     10.12.12.4       1     255  7.065   interface_reachable

Node: cluster01-02            Destination Cluster: cluster01
Destination Node IP Address       Count TTL  RTT(ms) Status
---------------- ---------------- ----- ---- ------- --------------------
cluster01-01     10.12.12.1       1     255  1.324   interface_reachable
cluster01-02     10.12.12.2       1     255  0.809   interface_reachable

Node: cluster01-02            Destination Cluster: cluster02
Destination Node IP Address       Count TTL  RTT(ms) Status
---------------- ---------------- ----- ---- ------- --------------------
cluster02-01     10.12.12.3       1     255  7.279   interface_reachable
cluster02-02     10.12.12.4       1     255  7.282   interface_reachable
```

◀◀◀

# 10.2　SVM ピア関係のトラブルシューティング

一般的な問題とそのトラブルシューティング方法を次に示します。

- クラスタ間環境での SVM ピアアクションの失敗 :
  - ピアクラスタが到達可能であることを確認します。
  - 両方のクラスタが、SVM ピアリング機能を有効にした ONTAP バージョンをサポートしていることを確認します。
  - ピア SVM 名が SVM ピアリングテーブル内のピア SVM 名から別のクラスタに関連付けられていないことを確認します。
  - エラーメッセージの `mgwd.log` とコンソールログをチェックしてください。
- クラスタ内またはクラスタ間環境での SVM ピアアクションの失敗 :
  - 両方のクラスタが ONTAP バージョンをサポートし、SVM ピアリング機能が有効になっていることを確認します。ローカル SVM 名とピア SVM 名が同じでないことを確認します。
  - エラーメッセージの `mgwd.log` とコンソールログをチェックしてください。

- `vserver peer show` コマンドを実行して、SVM ピアの関係を確認します。このコマンドは、設定済みのすべての SVM ピア関係を表示します。

```
cluster02::> vserver peer show
            Peer        Peer
Vserver     Vserver     State
----------- ----------- ------------
vs1_dest    vs1_backup  peered
vs1_dest    vs1_src     peered
```

- `vserver peer show-all` コマンドで通知を確認します。

```
cluster02::> vserver peer show-all
            Peer        Peer                                    Peering
Vserver     Vserver     State        Peer Cluster               Applications
----------- ----------- ------------ -------------------------- ---------------
vs1_dest    vs1_backup  peered       cluster03                  snapmirror
vs1_dest    vs1_src     peered       cluster01                  snapmirror
```

# 10.3　SnapMirror の関係ステータスについて

Healthy 列は、SnapMirror 関係の状態を示します。この列は、CLI の `snapmirror show` コマンドの出力および ONTAP System Manager で表示される SnapMirror 関係のステータスの Healthy 列に表示されます。

```
cluster02::> snapmirror show
                                                                    Progress
Source            Destination  Mirror  Relationship  Total         Last
Path        Type  Path         State   Status        Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
vs1_src:vol1
            XDP   vs1_dest:vol1
                              Snapmirrored
                                      Transferring   128KB     true    02/25 15:43:53
```

デスティネーションボリュームがオフラインであるか、アクセスできない場合は、Mirror State 列も表示されます。

# 10.4　SnapMirror 関係のトラブルシューティング

特定の関係に対する最後の SnapMirror 転送がいつ完了したかを確認するには、インスタンス情報のエクスポートされた Snapshot のタイムスタンプ欄を参照してください。

```
cluster02::> snapmirror show -instance

                            Source Path: snap_src1:SMSource
                       Destination Path: svm_dst1:SMSource_dest
                      Relationship Type: XDP
                Relationship Group Type: none
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: vault
                      SnapMirror Policy: XDPDefault
                            Tries Limit: -
                      Throttle (KB/sec): unlimited
                           Mirror State: Snapmirrored
                    Relationship Status: Idle
                File Restore File Count: -
                 File Restore File List: -
                      Transfer Snapshot: -
                      Snapshot Progress: -
                         Total Progress: -
              Network Compression Ratio: -
                    Snapshot Checkpoint: -
                        Newest Snapshot: snapmirror.12ceb7f0-b078-11e8-baec-0050
56b013db_2160175147.2020-01-24_043858
              Newest Snapshot Timestamp: 01/24 04:38:59
                      Exported Snapshot: snapmirror.12ceb7f0-b078-11e8-baec-0050
56b013db_2160175147.2020-01-24_043858
           Exported Snapshot Timestamp: 01/24 04:38:59
                               Healthy: true
                      Unhealthy Reason: -
               Constituent Relationship: false
                Destination Volume Node: cluster2-01
                        Relationship ID: 1a46a611-3e64-11ea-86bf-005056b013db
                   Current Operation ID: -
                          Transfer Type: -
                         Transfer Error: -
                       Current Throttle: -
              Current Transfer Priority: -
                     Last Transfer Type: resync
                    Last Transfer Error: -
                     Last Transfer Size: 0B
Last Transfer Network Compression Ratio: 1:1
                 Last Transfer Duration: 0:0:1
                     Last Transfer From: snap_src1:SMSource
           Last Transfer End Timestamp: 01/24 04:45:16
                 Progress Last Updated: -
                Relationship Capability: 8.2 and above
                               Lag Time: 5:27:1
          Identity Preserve Vserver DR: -
                Volume MSIDs Preserved: -
                Is Auto Expand Enabled: -
          Number of Successful Updates: 0
              Number of Failed Updates: 0
          Number of Successful Resyncs: 1
              Number of Failed Resyncs: 0
           Number of Successful Breaks: 0
               Number of Failed Breaks: 0
                   Total Transfer Bytes: 0
        Total Transfer Time in Seconds: 1
```

SnapMirror 関係のトラブルシューティングについては、関係に関する情報をイベントログ内で確認してください。次の例に示すように、`event log show` コマンドに `-messagename` オプションを使用して、SnapMirror に関連するメッセージのイベントログをフィルタリングします。`mgmt.snapmir*` メッセージ名を指定して、出力をフィルタリングし、SnapMirror に関連するメッセージのみを検索します。

```
cluster01::> event log show -messagename mgmt.snapmir*
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
12/6/2011 17:35     cluster02-01     ERROR         mgmt.snapmir.update.fail: Update from source
volume 'cluster01://vs1/vol03' to destination volume(s) 'cluster02://vs2/vol03' failed with error
'Failed to setup transfer. (Duplicate transfer specified. (Other error.))'. Job ID 1322.
12/6/2011 17:34:35  cluster02-01     DEBUG         mgmt.snapmir.abnormal.abort: Source Path
cluster01://vs1/vol01, Destination Path cluster02://vs2/vol01, Error Transfer failed.
(Destination volume cluster02://vs2/vol01 is smaller than the source volume.), Function
copySnapshot, line 5030, job ID 1355.
12/5/2011 05:15:45  cluster02-01     DEBUG         mgmt.snapmir.abnormal.abort: Source Path
cluster01://vs2/vol12, Destination Path cluster02://vs8/vol12, Error Failed to delete Snapshot
copy weekly.2011-12-04_0015 on volume cluster02://vs8/vol12. (Snapshot is in use.), Function
deleteSnapshot, line 4285, job ID 1215.
```

特定のボリュームに関するエラーメッセージを検索するには、次の例に示すように、`-event` オプションでアスタリスクで囲まれたボリューム名を指定して、メッセージ一覧をさらにフィルタします。

```
cluster01::> event log show -messagename mgmt.snapmir* -event *vol01*
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
12/6/2011 17:34:35  cluster02-01     DEBUG         mgmt.snapmir.abnormal.abort: Source Path
cluster01://vs1/vol01, Destination Path cluster02://vs2/vol01, Error Transfer failed.
(Destination volume cluster02://vs2/vol01 is smaller than the source volume.), Function
copySnapshot, line 5030, job ID 1355.
```

すべての SnapMirror イベントは、デスティネーションボリュームが存在するノード上の `SnapMirror_audit.log` ファイルおよび `SnapMirror_error.log` ファイルに記録されます。このノードは、コマンドが発行されたノードとは異なる場合があります。オペレーションを実行しているノードを特定するには、`snapmirror show -fields destination-volume-node` コマンドを実行します。ONTAP System Manager では、SnapMirror ログファイルを表示できます。

# 第 11 章
# DR 構成のベストプラクティス

- ソースサイトの 1 つの SVM に属するボリュームは、デスティネーションサイトの 1 つの SVM にレプリケートする必要があります。SVM は、NAS クライアントの NAS ネームスペースのルートであり、SAN 環境の単一のストレージデスティネーションです。一部の NAS ボリュームが 1 つの SVM からデスティネーションの別の SVM にレプリケートされる場合、それらのすべてのボリュームを同じネームスペースにリカバリすることはできません。LUN を含むボリュームについても同様です。デスティネーションでボリュームが異なる SVM にレプリケートされる場合、すべての LUN が同じ SAN ターゲットの下に表示されません。
- デスティネーション SVM は、ソース SVM がメンバーになっているのと同じ Active Directory、LDAP、または NIS ドメインのメンバーである必要があります。NAS ボリュームが Access Control List (ACL) を認証できない SVM にリカバリされた場合に、NAS ファイルに格納されている ACL が破損しないように、この設定を行う必要があります。ファイルレベル ACL を変更して別のドメインからのアクセス用に修正するプロセスは、非常に困難で時間がかかる場合があります。また、この設定は、SnapCenter Plug-in for Windows などの SAN クライアントで動作するツールの認証が同じ認証情報を使用して実行されるためにも重要です。
- デスティネーション SVM はソース SVM とは異なる SVM であり、富士通では同じ Active Directory ドメインのメンバーになることを推奨しているため、デスティネーション SVM は異なる SVM 名でドメインに参加する必要があります。ソースシステムとは異なる名前の DR システムを使用するのが一般的です。DR フェイルオーバーのシナリオでは、通常、DNS 名前解決を変更するか、DNS エイリアスを使用してクライアントをリカバリされたストレージシステムの名前にリダイレクトします。この方法では、確実に、CIFS 共有が同じ UNC パス名を使用して引き続きアクセス可能であるようにし、NFS クライアントも予期したパスにアクセスできるようにします。

  **注 意**

  これは、個別のボリュームではなく SVM をレプリケート (SVM DR) するように SnapMirror を設定するのが本来の使用方法です。

- ソースボリューム名と同じデスティネーションボリューム名を使用する必要はありません。ただし、この方法を使用すると、ボリュームがマウントされているジャンクションパスにボリュームと同じ名前が付いている場合に、デスティネーションボリュームをデスティネーションにマウントする際の管理が容易になります。
- パスとディレクトリ構造がソース SVM と同じになるように、SVM のデスティネーション NAS ネームスペースを作成します。
- 多くの SAN クライアントは、SnapMirror デスティネーションボリュームなど、完全に読み取り専用のコンテナ内にある LUN にアクセスできません。通常、LUN は、SnapMirror ブレーク操作の実行後に、igroup にマップし、SAN クライアントによってマウントする必要があります。
- 次のセクションで説明するように、デスティネーション SVM を事前に設定します。このアプローチにより、ストレージシステムの DR プロセスが大幅に高速化され、一部の SnapMirror ブレーク操作と一部の DNS エイリアスの更新にまで短縮される可能性があります。
- ソースサイトで新しいボリュームが作成されたら、それらのボリュームをレプリケートするために SnapMirror 関係を作成する必要があります。災害発生時に準備できるように、ボリュームの作成と複製が完了したら、DR サイトのボリュームに関する構成設定を行う必要があります。

# 第 12 章
# DR の構成とフェイルオーバー

本章では、クラスタ内 SnapMirror データ保護 (async-mirror) レプリケーションの DR プロセスの概要における、DR の構成とフェイルオーバーについて説明します。このプロセスを 2 つのセクションに分けて説明します。最初のセクションでは、フェイルオーバー用にデスティネーションを準備するためにフェイルオーバーが必要になる前に完了しておく必要のある手順について説明します。DR サイトで DR シナリオを準備するには、次の手順を実行する必要があります。2 番目のセクションでは、フェイルオーバーの実行に必要な手順について説明します。

どの環境にも固有の特性があります。各環境は DR 計画に影響を与える可能性があります。導入されている DR ソリューションのタイプによって、各組織の DR の状況は大きく異なります。成功を実現するには、適切な計画、文書化、および DR シナリオの現実的なウォークスルーが必要です。

## 12.1 環境のフェイルオーバー要件と前提条件

DR を成功させるには、いくつかの一般的な要件と前提条件を考慮します。以下は、すべてを含むリストではありません。

- システム管理者は、DR サイトの管理とフェイルオーバーの実行に使用するワークステーションまたはサーバのデスクトップセッションにアクセスできます。
- システム管理者は、システムへのアクセスに必要なすべての適切な認証情報、アカウント、パスワードなどを持っています。
- DR ネットワークへの接続は、オペレーションが実行されるすべての場所から利用できます。
- 一部のインフラストラクチャサーバは DR サイトにすでに存在し、アクセス可能です。これらのシステムは、管理者が環境内で作業し、回復計画を実行するために必要な基本サービスを提供します。
  - 認証を提供する DR サイト Active Directory サービス。
  - 名前解決を提供する DR サイト DNS サービス。
  - ライセンスサービスを必要とするすべてのアプリケーションにライセンスサービスを提供する DR サイトのライセンスサーバー。

**注 意**

必要な Active Directory FS MO ロールを実行するには、DR サイトでサーバーを使用できる必要があります。稼働している Active Directory サーバへの役割の転送、または障害が発生したサーバからの役割の取得については、Microsoft KB 255504 を参照してください。

- DR サイトは、プライマリサイトと同じソース、またはプライマリサイトと同期しているソースと時刻が同期しています。
- 必要なすべてのボリュームは、SnapMirror を使用して DR サイトに複製されます。
- SnapMirror オペレーションは監視されており、設計された RPO に関して最新の状態になっています。

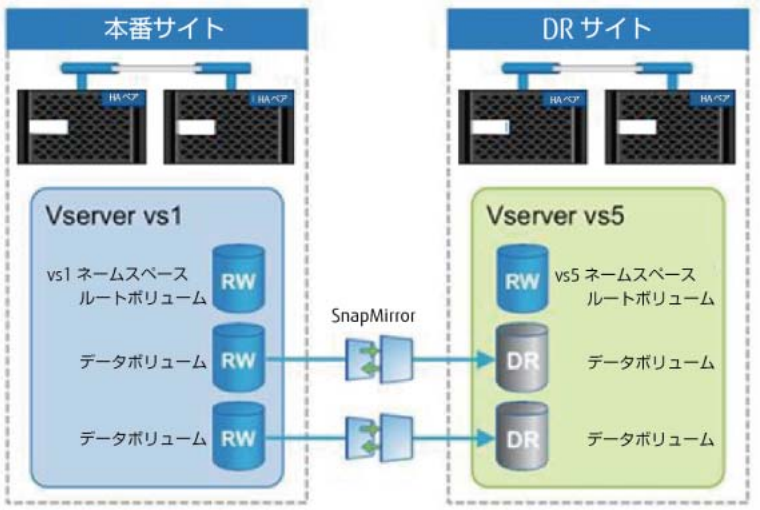
- DR コントローラに必要な容量が存在します。これは、DR 環境で計画されている日常業務をサポートするために必要な容量を指します。
- すべての DR サイトのアプリケーションサーバは、DR ストレージアレイに接続できるように適切に接続されています。
- 障害が発生したプライマリネットワークを DR サイトから隔離またはフェンスする方法があります。この方法は、災害の原因となった事象が一時的または断続的なもの ( 長時間の停電など ) である場合に必要です。プライマリサイトのシステムが再起動すると、サービスが DR サイトで実行されているリカバリされたオペレーションと競合する場合があります。
- ユーザーとアプリケーションが DR サイトのデータとサービスにアクセスできるようにする計画が立てられています。たとえば、プライマリサイトの SVM へのホームディレクトリのマウント要求が DR サイト SVM に送信されるように DNS を更新する場合です。

# 12.2　フェイルオーバー先の準備

DR プロセスの多くの部分は、DR イベントの前に事前に準備できます。たとえば、ネームスペースへのボリュームのマウント、CIFS 共有の作成、NFS エクスポートポリシーの割り当ては、すべて事前に実行できます。SnapMirror を使用して、デスティネーションの SVM で独立している可能性がある構成情報を複製することはできません。これらの構成には、SVM ドメインメンバーシップ、CIFS 構成、NFS ポリシー、Snapshot ポリシースケジュール、Storage Efficiency ポリシーなどがあります。

図 12.1 は、DR のボリュームレイアウトを示しています。

図 12.1　DR のボリュームレイアウト




ボリュームの複製が完了したら、次の手順を実行して、デスティネーションシステムにフェイルオーバーの準備をします。

## 12.2.1　NAS および SAN 環境

手順 ▶▶▶

1. デスティネーション SVM メンバーシップを適切な Active Directory、LDAP、または NIS ドメインに構成します。
2. デスティネーション SVM がソース SVM と同じドメインのメンバーであることを確認します。この構成では、SnapMirror によって複製されるファイルレベル ACL に対して同じユーザーが認証されることも保証されます。
3. デスティネーションクラスタで必要なデフォルト以外の Snapshot コピーポリシーを作成します。

   注 意

   ソースと同じスケジュールでデスティネーションクラスタの Snapshot コピーポリシーを構成することを推奨しています。Snapshot コピーポリシーは、フェイルオーバー後に DP ボリュームに適用する必要があります。

4. デスティネーション SVM に Storage Efficiency ポリシーを作成します。

   注 意

   ソース SVM のボリュームに Storage Efficiency ポリシーが割り当てられている場合は、DR サイトでのフェイルオーバー後に重複排除プロセスをスケジュールするために、デスティネーション SVM でポリシーを作成する必要があります。Storage Efficiency ポリシーは、フェイルオーバー後に DP ボリュームに適用する必要があります。

◀◀◀

## 12.2.2　NAS 環境

手順 ▶▶▶

1. ソース SVM のすべての必要なボリュームがデスティネーション SVM にレプリケートされていることを確認します。ボリュームは、サブフォルダまたは名前空間内の他のボリューム内にマウントできます。この状態が存在する場合は、デスティネーションで名前空間を正しく再構築するために必要なすべてのボリュームが複製されていることを確認することが重要です。
2. デスティネーション SVM ルートボリュームのセキュリティスタイルと権限を確認します。デスティネーション SVM ネームスペースのルートのセキュリティスタイルと権限を正しく設定する必要があります。正しく設定しないと、フェイルオーバー後に NAS ネームスペースにアクセスできなくなる可能性があります。

**3** デスティネーション NAS ボリュームをデスティネーション SVM ネームスペースにマウントします。

SnapMirror は、SVM ネームスペースジャンクションパス情報を複製しません。NAS ボリュームにはジャンクションパスがないため、SnapMirror の中断後は、フェイルオーバー前に事前マウントされていない限り、またはフェイルオーバー後にマウントされるまでアクセスできません。ボリュームをマウントする場合は、ソースボリュームがソース SVM でマウントされたのと同じジャンクションパスを使用して、ネームスペースにマウントします。この構成は、リカバリされたネームスペース内のパスがプライマリサイトに存在していたパスと異なることがないようにするために重要です。パスが異なると、クライアントのマウントポイント、リンク、ショートカット、エイリアスが正しいパスを見つけられない場合があります。

注 意

ボリュームは、まだ DP 状態の他のボリューム内にマウント ( ネスト ) できません。snapmirror break コマンドを使用した後は、レプリケートされたボリューム内にマウントポイントがネストされているボリュームをマウントし、CIFS 共有を作成する必要があります。

**4** ソースで使用されたのと同じ共有名を使用して、デスティネーション SVM 上に CIFS 共有を作成します。クライアントは CIFS 共有にアクセスできます。ただし、ボリュームがフェイルオーバーされるまで、すべてのデータは読み取り専用です。

**5** デスティネーションの CIFS 共有に適切な ACL を適用します。

**6** デスティネーション SVM に対して適切な NFS エクスポートポリシーを作成します。

**7** デスティネーションボリュームに NFS エクスポートポリシーを割り当てます。クライアントは NFS エクスポートにアクセスできますが、ボリュームがフェイルオーバーされるまで、すべてのデータは読み取り専用です。

### 12.2.3　SAN 環境

手順

**1** デスティネーション SVM がポートセットを使用している場合は、フェイルオーバー前に必要に応じて構成できます。

**2** デスティネーション SVM で igroup を設定します。

通常、DR サイトのリカバリされたストレージに接続するアプリケーションサーバは複数あります。これらのサーバからのイニシエータは、デスティネーション SVM の適切な igroup に事前構成できます。

一部のホストは、SnapMirror デスティネーションボリュームである読み取り専用コンテナ内の LUN への接続をサポートしていないため、通常はフェイルオーバー後に LUN から igroup へのマッピングが実行されます。

# 12.3　フェイルオーバーの実行

フェイルオーバーの前に DR に必要な構成のほとんどが実行されるため、DR シナリオ中にフェイルオーバーに必要な実際の手順が大幅に削減されます。以下のとおりです。

## 12.3.1　NAS 環境

**手順 ▶▶▶**

1. SnapMirror ブレーク操作を実行して、各ボリュームをフェイルオーバーします。ONTAP では、ワイルドカードを使用して、1 つのコマンドで複数のボリューム上で SnapMirror オペレーションを実行できます。次の例では、vs5 という名前のデスティネーション SVM 内のすべてのボリュームに対してフェイルオーバーを実行します。コマンドでボリューム名の一部を使用すると、特定のボリュームに制限できます。

```
cluster02::> snapmirror break -destination-path cluster02://vs5/*
```

2. ボリュームがネームスペースにマウントされ、CIFS 共有および NFS エクスポートポリシーが作成および適用されている場合、クライアントは NAS データに対する読み取り / 書き込みアクセス権を持ちます。
3. リカバリされたストレージにクライアントをリダイレクトします。

◀◀◀

ソースシステムとは異なる名前の DR システムを使用するのが一般的な方法です。DR フェイルオーバーのシナリオでは、通常、DNS 名前解決を変更するか、DNS エイリアスを使用してクライアントをリカバリされたストレージシステムの名前にリダイレクトします。このアプローチでは、同じ UNC パス名を使用した CIFS 共有アクセスが可能になり、NFS クライアントも目的のパスにアクセスできます。または、障害が発生したソースストレージシステムを Active Directory から削除できます。その後、リカバリストレージシステムを削除し、ソースシステムと同じ名前を使用して Active Directory に再度追加できます。ただし、この変更が大規模な Active Directory 環境に反映されるまでに時間がかかる場合があります。

### 12.3.2　SAN 環境

手順 ▶▶▶

1. SnapMirror ブレーク操作を実行して、各ボリュームをフェイルオーバーします。ワイルドカードを使用すると、1 つのコマンドで複数のボリュームに対して SnapMirror オペレーションを実行できます。次の例では、`vs5` という名前のデスティネーション SVM 内のすべてのボリュームに対してフェイルオーバーを実行します。コマンドでボリューム名の一部を使用すると、特定のボリュームに制限できます。

```
cluster02::> snapmirror break -destination-path cluster02://vs5/*
```

2. LUN を適切な igroup にマッピングして、DR サイトの SAN クライアントがボリューム内の LUN を使用できるようにします。
3. SAN クライアントで、ストレージの再スキャンを実行して、接続されている LUN を検出します。

◀◀◀

## 12.4　フェイルオーバー後のボリューム構成

Snapshot コピーポリシーと Storage Efficiency ポリシーは、DP 状態のボリュームには割り当てることができないため、フェイルオーバー後に割り当てる必要があります。

手順 ▶▶▶

1. ONTAP Snapshot コピースケジュールを使用している場合は、Snapshot コピーポリシーをリカバリされたボリュームに割り当てます。SAN 環境では、Snapshot コピーは通常、クライアントでスケジュール設定されます。
2. Storage Efficiency テクノロジーを使用している場合は、リカバリしたボリュームに Storage Efficiency ポリシーを割り当てます。

◀◀◀

Fujitsu Storage
ETERNUS AX series オールフラッシュアレイ ,
ETERNUS HX series ハイブリッドアレイ
ONTAP 9.11.1 用 SnapMirror 構成およびベストプラクティスガイド

P3AG-5642-04Z0

発行年月　2023 年 4 月
発行責任　富士通株式会社

FUJITSU