



ストレージVMとデータの管理

AFX

NetApp
February 11, 2026

目次

ストレージVMとデータの管理	1
データを管理する	1
AFXストレージシステムのデータ管理の準備	1
AFX ストレージ システムにボリュームを作成して構成する	3
AFXストレージシステムのボリュームを管理する	3
AFX ストレージ システムに S3 バケットを作成して設定する	4
AFXストレージシステムバケットを管理する	5
AFX ストレージ システムの監視とトラブルシューティング	5
データの保護	5
AFXストレージシステムのデータを保護する準備をする	5
AFX ストレージ システムに整合性グループを作成する	6
AFX ストレージ システム上の整合性グループを管理する	7
AFX ストレージ システムにスナップショットを作成する	8
AFX ストレージ システム上のスナップショットを管理する	11
AFXストレージシステムでクラスタ間SVMピア関係を作成する	12
AFX ストレージ システムでのスナップショット レプリケーションの管理	12
AFXストレージシステムのデータ保護ポリシーとスケジュールを管理する	17
安全なデータ	19
AFXストレージシステムのデータを保護する準備	19
AFX ストレージ システムに保存されているデータを暗号化する	19
AFXストレージシステム上の安全なIP接続	20
AFX ストレージ システム SVM の追加管理	21
ストレージ管理とパフォーマンス	21
データ保護	22
セキュリティ	22
ONTAPイベントとパフォーマンスの監視	22
関連情報	22

ストレージVMとデータの管理

データを管理する

AFXストレージシステムのデータ管理の準備

AFX データを管理する前に、基本的な概念と機能について理解しておく必要があります。



AFFおよびFASシステムで使用できる概念や管理手順の多くはAFX ストレージ システムと同じであるため、Unified ONTAP のドキュメントを確認すると役立ちます。リンクを参照してください [\[関連情報\]](#) 詳細についてはこちらをご覧ください。

用語とオプション

AFX ストレージに関連して、知っておくべき用語がいくつかあります。

フレックスボリューム

FlexVolは、AFX ストレージ システムで使用される論理コンテナの一種です。FlexVolボリュームは、拡張、縮小、移動、効率的なコピーが可能です。また、qtree を使用してより管理しやすい単位に分割したり、クォータを使用してリソース使用量を制限することもできます。

FlexGroup

FlexGroupボリュームは、高パフォーマンスと自動負荷分散の両方を提供するスケールアウト NAS コンテナです。それぞれは、トラフィックを透過的に共有する複数のボリュームで構成されています。FlexGroupボリュームには、スケーラビリティとパフォーマンスの向上、管理の簡素化など、さまざまな利点があります。

FlexCache

FlexCacheは、同じまたは異なるONTAPクラスタ上のボリュームのスパースな書き込み可能なレプリカを作成するONTAPキャッシュ テクノロジーです。データをユーザーの近くに配置することでデータ アクセス パフォーマンスを向上させるように設計されており、フットプリントが小さくなり、スループットが高速化されます。FlexCacheは、読み取り集中型のワークフローに特に役立ち、頻繁にアクセスされるボリュームからのトラフィックのオフロードに役立ちます。

S3バケット

S3 バケットは、クラウド内のオブジェクトまたはデータを保持するストレージ コンテナです。ONTAPでは、S3 NAS バケットは S3 バケット名と NAS パス間のマッピングであり、既存のボリュームとディレクトリ構造を持つ SVM 名前空間の任意の部分に S3 がアクセスできるようになります。

データコンテナ

AFX システムのコンテキストでは、データ コンテナは一般的な用語であり、ボリュームまたは S3 バケットのいずれかになります。

qtree

qtree は、データを管理および整理するために作成できるボリューム内の論理的な細分化です。これにより、プロパティとセキュリティ スタイル (NTFS または UNIX) を指定でき、親ボリュームからエクスポート ポリシーを継承したり、独自のポリシーを持つことができます。qtree にはファイルとディレクトリを含めることができ、ボリューム内の権限とクォータをより細かく管理するためによく使用されます。

クォータ

ONTAPのクォータは、ユーザー、グループ、または qtree が使用できるストレージ容量またはファイル数に設定される制限です。クォータは、ストレージ システム内のリソースの使用を管理および制御するために使用され、単一のユーザーまたはアプリケーションが過剰な量のリソースを消費できないようにします。

NFSセッションランキング

NFS トランキングは、NFS v4.1 クライアントが NFS サーバー上の異なる LIF への複数の接続を開くことを可能にするテクノロジーです。これにより、データ転送速度が向上し、トランキング対応クライアントにボリュームをエクスポートするときに複数のパスを通じて復元力が提供されます。トランクに参加するには、LIF が同じノード上に存在している必要があります。

トランキングを有効にするには、NFS 用に SVM を設定し、NFSv4.1 を有効にする必要があります。また、構成の変更後にはすべての NFSv4.x クライアントを再マウントする必要があり、混乱が生じる可能性があります。NFS トランキングのサポートおよび構成手順は、すべてのONTAPシステムで同じです。詳細は [こちら "NFS トランキング"](#)

ファイルシステム分析

ファイル システム分析 (FSA) は、FlexGroup または FlexVol ボリューム内のファイル使用状況とストレージ容量の傾向をリアルタイムで表示するONTAP機能です。ストレージの使用率と最適化の機会に関する洞察を提供することで、外部ツールの必要性を排除します。FSA は、SVM、ボリューム、ディレクトリ、ファイル レベルなど、ボリュームのファイル システム階層のさまざまなレベルで詳細なビューを提供します。

データ移行オプション

データ移行にはいくつかのオプションがあります。重点は、外部データを AFX クラスターに移行することにあります。

AFF または FAS システムからのデータの移行

次のテクノロジーを使用することで、AFF または FAS システム (Unified ONTAP パーソナリティを実行) から AFX への完全に統合された移行パスが利用できます。

- SnapMirror
- SVM 移行
- SVM DR

さらに、FlexCache ボリュームは、AFX システムと AFF または FAS システムの間でどちらの方向にも接続できます。

ONTAP 以外のソースからのデータの移行

ONTAP 以外のシステムからのデータ移行は、ファイル レベルのコピー操作を使用して実行できます。高速コピーユーティリティ "**XCP**" または "**コピーと同期**" RoboCopy (SMB 用) や rsync (NFS 用) などの標準ユーティリティや、DataDobi などのサードパーティ ツールも使用できます。

移行の制限

ソース データ ボリュームに LUN または NVMe 名前空間が含まれていない場合は、AFF または FAS システムから AFX にデータを複製できます。AFX から AFF または FAS システムにレプリケートする場合、AFF または FAS システムでサポートされる最小のONTAPバージョンは 9.16.1 です。これは、高度な容量バランシング

をサポートする最初のONTAPリリースです。

ストレージの概要を表示する

AFX データの管理を開始するには、ストレージの概要を表示する必要があります。

タスク概要

AFX クラスターに定義されているすべてのボリュームとバケットにアクセスできます。これらはそれぞれデータ コンテナと見なされます。

手順

1. システムマネージャで*ストレージ*を選択し、次に*概要*を選択します。
2. *ボリューム*の横にある → ボリュームのリストを表示します。
3. *バケット*の横にある → バケットのリストを表示します。
4. 必要に応じてデータ コンテナを更新または作成します。

関連情報

- ["ONTAPファイル システム分析について学ぶ"](#)
- ["追加のAFX SVM管理"](#)
- ["AFX システムの管理を準備する"](#)
- ["AFX システム SVM を移行する"](#)
- ["NetApp Interoperability Matrix Tool"](#)

AFX ストレージ システムにボリュームを作成して構成する

ボリュームを作成して SVM に接続できます。各ボリュームは、AFX でサポートされているアクセス プロトコルのいずれかを使用してクライアントに公開できます。

タスク概要

ボリュームを作成するときは、最小限の構成詳細を指定する必要があります。追加の詳細は、作成中または作成後にボリュームを編集することによって提供できます。追加の SVM を作成した場合は、ボリュームの SVM を選択する必要があります。

手順

1. システム マネージャーで、[ストレージ] を選択し、[ボリューム] を選択します。
2. 選択 **+ Add** 名前、容量、最適化などの基本構成を提供します。
3. 必要に応じて、データ保護、SnapLock、NFS アクセスに関連する追加の構成については、[その他のオプション] を選択します。
4. ボリュームを追加するには、[保存] を選択します。

AFXストレージシステムのボリュームを管理する

AFX クラスターで定義されたボリュームの管理の一環として実行できる管理タスクがい

くつかあります。

qtreeを作成する

qtree は、データを整理および管理するために作成できるボリューム内の論理的な細分です。

手順

1. システム マネージャーで、ストレージ を選択し、次に **Qtrees** を選択します。
2. 選択 **+ Add** 名前、ボリューム、セキュリティ スタイルなどの基本構成を提供し、必要に応じてクォータを構成します。
3. *保存*を選択してqtreeを追加します。

クォータを作成する

クォータとは、ユーザー、グループ、または qtree が使用できるストレージ容量またはファイル数に設定される制限です。クォータは、AFX システム内のリソース使用量を管理および制御するために使用されます。

手順

1. システム マネージャーで、ストレージ を選択し、次に クォータ を選択します。
2. *使用状況*タブを選択すると、すべてのボリュームのアクティブなクォータのリストが表示されます。
3. ボリューム タブを選択すると、AFX クラスターで定義されているボリュームのリストが表示されます。特定のボリュームを選択すると、追加情報が表示されます。
4. クォータを定義するには、[ルール] タブを選択します。
5. クォータターゲット、タイプ、制限などの構成の詳細を指定します。
6. クォータを追加するには、[保存] を選択します。

AFX ストレージ システムに S3 バケットを作成して設定する

バケットを作成して SVM に接続できます。各バケットは、AFX でサポートされている S3 アクセス プロトコルを使用してクライアントに公開できます。

タスク概要

バケットを作成するときは、最小限の構成詳細を指定する必要があります。追加の詳細は、バケットの作成時または作成後に編集することで提供できます。追加の SVM を作成した場合は、バケットの SVM を選択する必要があります。

開始する前に

クライアントがバケットにアクセスできるようにするには、SVM の S3 サービスを設定する必要があります。

手順

1. システム マネージャーで、ストレージ を選択し、次に バケット を選択します。
2. 選択 **+ Add** 名前や容量などの基本構成を提供します。
3. 必要に応じて、データ保護、ロック、および権限に関連する追加の構成については、[その他のオプション] を選択します。

4. バケットを追加するには、[保存] を選択します。

AFXストレージシステムバケットを管理する

AFX S3 バケットとクライアント アクセスの管理の一環として実行できる管理タスクがいくつかあります。AFX での S3 構成とサポートは、Unified ONTAPで提供されるものと同じです。詳細については、Unified ONTAP のドキュメントを参照してください。

関連情報

["ONTAP S3 の構成について学ぶ"](#)

AFX ストレージ システムの監視とトラブルシューティング

AFX システムには、各クラスターが管理するストレージを監視するためのいくつかのオプションが含まれています。

NASクライアントを表示する

現在 AFX クラスターに接続されている NFS および SMB/CIFS クライアントのリストを表示できます。

手順

1. システム マネージャーのナビゲーション ペインで [クライアント] を選択します。
2. 必要に応じて、**NFS** または **SMB/CIFS** タブを選択します。
3. 表示をカスタマイズし、必要に応じてクライアント情報を検索およびダウンロードします。

関連情報

- ["AFXデータを管理する準備"](#)

データの保護

AFXストレージシステムのデータを保護する準備をする

AFX データを保護する前に、いくつかの重要な概念と機能について理解しておく必要があります。



AFFおよびFASシステムで利用可能な概念や管理手順の多くはAFXストレージシステムと同じであるため、Unified ONTAPのドキュメントで ["データ保護とディザスタ リカバリ"](#)役に立つかもしれません。

用語とオプション

AFX データ保護に関連して、知っておくべき用語がいくつかあります。

Snapshot

スナップショットは、ボリュームの読み取り専用の特定時点のイメージです。これは、ONTAP のレプリケ

ーションおよびデータ保護サービスの基盤となるテクノロジーです。

一貫性グループ

整合性グループは、1つの単位として管理されるボリュームの集まりです。整合性グループを作成すると、アプリケーションワークロードのストレージ管理とデータ保護を簡素化できます。たとえば、個々のボリュームの代わりに整合性グループを使用することで、1回の操作で複数のボリュームのスナップショットを作成できます。

階層的整合性グループ

階層的整合性グループはONTAP 9.16.1で導入され、AFXで利用できます。階層構造では、1つ以上の整合性グループを親の下の子として構成できます。これらの階層グループを使用すると、子の整合性グループに個別のスナップショットポリシーを適用し、親を複製することで、すべての子のスナップショットを単一のユニットとしてリモートクラスターに複製できます。

SnapLock

SnapLockは、ファイルを一度書き込み、何度も読み取り可能な (WORM) 状態に移行して保護できるONTAPの機能です。これにより、指定された保持期間中は変更や削除が防止されます。作成されたSnapLockボリュームは、保持期間に基づいて作成後に非SnapLockボリュームから変換することはできません。

AFXデータ保護の制限

AFXストレージシステムによって適用されるONTAPデータ保護の制限と制約事項を認識しておく必要があります。

SnapMirror同期 (SM-S)

SM-Sを使用する場合、スケール制限があります。単一のAFXシステムクラスター全体で最大400のリレーションシップを設定できます。

関連情報

- ["追加のAFX SVM管理"](#)
- ["AFXシステムを管理する準備をする"](#)

AFXストレージシステムに整合性グループを作成する

整合性グループを作成すると、アプリケーションワークロードのストレージ管理とデータ保護を簡素化できます。整合性グループは、既存のボリュームまたは新しいボリュームに基づくことができます。

開始する前に

新たに1つのボリュームを作成する予定の場合は、新しいボリュームを作成するときに構成オプションに注意する必要があります。

手順

1. システムマネージャーで、保護を選択し、次に整合性グループを選択します。
2. 選択 **+ Add** 次のいずれかを選択します。
 - 既存のボリュームを使用する

◦ 新しいNASボリュームの使用

3. 名前、ボリューム、アプリケーションの種類、保護などの構成の詳細を指定します。
4. *追加*を選択します。

関連情報

- ["一貫性グループの管理"](#)
- ["AFXボリュームを作成して構成する"](#)

AFX ストレージ システム上の整合性グループを管理する

AFX システム上の整合性グループを管理できます。これにより、ストレージ管理が効率化されます。

整合性グループにスナップショットデータ保護を追加する

整合性グループにスナップショット データ保護を追加すると、事前定義されたスケジュールに基づいて、整合性グループのローカル スナップショットを定期的に取り得できるようになります。

手順

1. システム マネージャーで、保護 を選択し、次に 整合性グループ を選択します。
2. 保護する整合性グループの上にマウスを置きます。
3. 選択 ; 次に、[編集] を選択します。
4. *ローカル保護*の下で、*スナップショットのスケジュール*を選択します。
5. スナップショット ポリシーを選択します。

デフォルトのスナップショット ポリシーを受け入れるか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のスナップショットポリシーを選択する	選択  デフォルト ポリシーの横にある  をクリックし、使用する既存のポリシーを選択します。

オプション	手順
新しいSnapshotポリシーを作成します。	<p>a. 選択 + Add; 新しいポリシー名を入力します。</p> <p>b. ポリシーのスコープを選択します。</p> <p>c. *スケジュール*の下で選択 + Add。</p> <p>d. *スケジュール名*の下に表示される名前を選択します。</p> <p>次に選択 ▼。</p> <p>e. ポリシースケジュールを選択します。</p> <p>f. *最大スナップショット*の下に、整合性グループの保持するスナップショットの最大数を入力します。</p> <p>g. オプションで、「* SnapMirrorラベル*」の下にSnapMirrorラベルを入力します。</p> <p>h. *保存*を選択します。</p>

6. *編集*を選択します。

関連情報

- ["ONTAPコンシステンシーグループについて学ぶ"](#)

AFX ストレージ システムにスナップショットを作成する

AFX システムのデータをバックアップするには、スナップショットを作成する必要があります。スナップショットを手動で作成することも、整合性グループを使用して自動的に作成されるようにスケジュールすることもできます。

開始する前に

スナップショットは、ボリュームを特定の時点で復元するために使用できる、データのローカルの読み取り専用コピーです。スナップショットは、必要に応じて手動で作成することも、["スナップショットポリシーとスケジュール"](#)。

スナップショット ポリシーとスケジュールでは、スナップショットを作成するタイミング、保持するコピーの数、スナップショットの名前の付け方、レプリケーション用のラベルの付け方などの詳細を指定します。たとえば、システムは毎日午前 12 時 10 分にスナップショットを 1 つ作成し、最新の 2 つのコピーを保持し、それらに「daily」（タイムスタンプを追加）という名前を付け、レプリケーション用に「daily」というラベルを付けます。

スナップショットの種類

単一のボリュームまたは整合性グループのオンデマンド スナップショットを作成できます。複数のボリュームを含む整合性グループの自動スナップショットを作成することもできます。ただし、単一ボリュームの自動スナップショットを作成することはできません。

- オンデマンドスナップショット

ボリュームのオンデマンド スナップショットはいつでも作成できます。オンデマンド スナップショットによって保護されるボリュームは、整合性グループのメンバーである必要はありません。整合性グループのメンバーであるボリュームのスナップショットを作成した場合、整合性グループ内の他のボリュームはスナップショットに含まれません。整合性グループのオンデマンド スナップショットを作成すると、整合性グループ内のすべてのボリュームが含まれます。

- 自動スナップショット

自動スナップショットは、スナップショット ポリシー定義に基づいて作成されます。自動スナップショット作成のためにボリュームにスナップショット ポリシーを適用するには、ボリュームが同じ整合性グループのメンバーである必要があります。整合性グループにスナップショット ポリシーを適用すると、整合性グループ内のすべてのボリュームが保護されます。

スナップショットを作成する

ボリュームまたは整合性グループのスナップショットを作成します。

整合性グループのスナップショット

手順

1. システム マネージャーで、保護 を選択し、次に 整合性グループ を選択します。
2. 保護する整合性グループの名前の上にマウスを置きます。
3. 選択 ; 次に、[保護] を選択します。
4. オンデマンドで即時スナップショットを作成する場合は、[ローカル保護] で [今すぐスナップショットを追加] を選択します。

ローカル保護では、ボリュームを含む同じクラスター上にスナップショットが作成されます。

- a. スナップショットの名前を入力するか、デフォルト名を受け入れ、オプションでSnapMirrorラベルを入力します。

SnapMirrorラベルはリモート宛先によって使用されます。

5. スナップショット ポリシーを使用して自動スナップショットを作成する場合は、[スナップショットのスケジュール] を選択します。
 - a. スナップショット ポリシーを選択します。

デフォルトのスナップショット ポリシーを受け入れるか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のスナップショットポリシーを選択する	選択  デフォルト ポリシーの横にある をクリックし、使用する既存のポリシーを選択します。
新しいSnapshotポリシーを作成します。	<ol style="list-style-type: none">i. 選択  Add; 次に、スナップショット ポリシー パラメータを入力します。ii. *ポリシーの追加*を選択します。

6. スナップショットをリモート クラスターに複製する場合は、[リモート保護] で [リモート クラスターに複製] を選択します。
 - a. ソース クラスターとストレージ VM を選択し、レプリケーション ポリシーを選択します。

デフォルトでは、レプリケーションの初期データ転送がすぐに開始されます。

7. *保存*を選択します。

ボリュームのスナップショット

手順

1. システム マネージャーで、[ストレージ] を選択し、[ボリューム] を選択します。
2. 保護するボリュームの名前の上にマウスを置きます。
3. 選択 ; 次に、[保護] を選択します。オンデマンドで即時スナップショットを作成する場合は、[ローカル保護] で [今すぐスナップショットを追加] を選択します。

ローカル保護では、ボリュームを含む同じクラスター上にスナップショットが作成されます。

- スナップショットの名前を入力するか、デフォルト名を受け入れ、オプションでSnapMirrorラベルを入力します。

SnapMirrorラベルはリモート宛先によって使用されます。

- スナップショット ポリシーを使用して自動スナップショットを作成する場合は、[スナップショットのスケジュール] を選択します。
 - スナップショット ポリシーを選択します。

デフォルトのスナップショット ポリシーを受け入れるか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のスナップショットポリシーを選択する	選択 <input checked="" type="checkbox"/> デフォルト ポリシーの横にある をクリックし、使用する既存のポリシーを選択します。
新しいSnapshotポリシーを作成します。	<ol style="list-style-type: none">選択 <input type="checkbox"/> Add; 次に、スナップショット ポリシー パラメータを入力します。*ポリシーの追加*を選択します。

- スナップショットをリモート クラスターに複製する場合は、[リモート保護] で [リモート クラスターに複製] を選択します。
 - ソース クラスターとストレージ VM を選択し、レプリケーション ポリシーを選択します。

デフォルトでは、レプリケーションの初期データ転送がすぐに開始されます。
- *保存***を選択します。

関連情報

- ["ONTAPスナップショットポリシーを作成する"](#)

AFX ストレージ システム上のスナップショットを管理する

AFX システムでスナップショットを管理できます。詳細については、Unified ONTAP のドキュメントを参照してください。

関連情報

- ["ONTAPスナップショットポリシーを作成する"](#)
- ["スナップショットを使用してONTAP FlexGroupボリュームを保護する"](#)

AFXストレージシステムでクラスタ間SVMピア関係を作成する

ピア関係は、クラスタとストレージ仮想マシン (VM) が安全にデータを交換できるようにするネットワーク接続を定義します。異なるクラスタ上のストレージ VM 間にピア関係を作成し、SnapMirrorを使用してデータ保護と災害復旧を有効にすることができます。

開始する前に

ストレージ VM ピア関係を作成する前に、ローカル クラスタとリモート クラスタ間にクラスタ ピア関係を確立しておく必要があります。["クラスタ ピア関係の作成"](#)まだ行っていない場合は、行ってください。

手順

1. システム マネージャーで、保護 > 概要 を選択します。
2. ストレージ VM ピア の下で ストレージ VM ピアの追加 を選択します。
3. ローカル クラスタ上のストレージ VM を選択し、次にリモート クラスタ上のストレージ VM を選択します。
4. *ストレージ VM ピアの追加*を選択します。

関連情報

- ["仲間関係についてもっと学ぶ"](#)。

AFX ストレージ システムでのスナップショット レプリケーションの管理

スナップショット レプリケーションは、AFX システム上の整合性グループを地理的に離れた場所にコピーするプロセスです。最初のレプリケーションの後、整合性グループへの変更は、レプリケーション ポリシーに基づいてリモート ロケーションにコピーされます。複製された整合性グループは、災害復旧やデータ移行に使用できます。

スナップショット レプリケーションを設定するには、AFX ストレージ システムとリモート ロケーションの間にレプリケーション関係を確立する必要があります。レプリケーション関係はレプリケーション ポリシーによって管理されます。すべてのスナップショットを複製するデフォルトのポリシーは、クラスタのセットアップ中に作成されます。デフォルトのポリシーを使用することも、オプションで新しいポリシーを作成することもできます。

ステップ1: クラスタピア関係を作成する

データをリモート クラスタに複製して保護する前に、ローカル クラスタとリモート クラスタの間にクラスタ ピア関係を作成する必要があります。

開始する前に

クラスタ ピアリングの前提条件は、AFX システムでも他のONTAPシステムと同じです。["クラスタピアリングの前提条件を確認する"](#)。

手順

1. ローカル クラスタの System Manager で、クラスタ > 設定 を選択します。
2. クラスタ間設定*の*クラスタピア*の横にある  をクリックし、[*クラスタ ピアの追加] を選択します。

3. リモート クラスターの起動 を選択します。これにより、リモート クラスターでの認証に使用するパスフレーズが生成されます。
4. リモート クラスターのパスフレーズが生成されたら、それをローカル クラスターの **Passphrase** の下に貼り付けます。
5. 選択 **+ Add**; 次に、クラスタ間ネットワーク インターフェイスの IP アドレスを入力します。
6. *クラスタ ピ어링の開始*を選択します。

次の手順

ローカル AFX クラスターをリモート クラスターとピアリングしました。レプリケーション関係を作成できるようになりました。

ステップ2: 必要に応じてレプリケーションポリシーを作成する

スナップショット レプリケーション ポリシーは、AFX クラスターで実行された更新がリモート サイトにいつレプリケートされるかを定義します。

手順

1. System Manager で、保護 > ポリシー を選択し、レプリケーション ポリシー を選択します。
2. 選択 **+ Add** 。
3. レプリケーション ポリシーの名前を入力するか、デフォルト名を受け入れて、説明を入力します。
4. ポリシー スコープ を選択します。

レプリケーション ポリシーをクラスター全体に適用する場合は、クラスター を選択します。レプリケーション ポリシーを特定のストレージ VM 内のボリュームにのみ適用する場合は、ストレージ **VM** を選択します。

5. *ポリシータイプ*を選択します。

オプション	手順
データがソースに書き込まれた後、リモート サイトにコピーします。	<ol style="list-style-type: none"> a. *非同期*を選択します。 b. *ソースからスナップショットを転送*の下で、デフォルトの転送スケジュールを受け入れるか、別のスケジュールを選択します。 c. すべてのスナップショットを転送するか、転送するスナップショットを決定するルールを作成するかを選択します。 d. 必要に応じて、ネットワーク圧縮を有効にします。
ソース サイトとリモート サイトに同時にデータを書き込みます。	<ol style="list-style-type: none"> a. *同期*を選択します。

6. *保存*を選択します。

次の手順

レプリケーション ポリシーが作成され、AFX システムとリモート ロケーション間のレプリケーション関係を作成する準備が整いました。

ステップ3: レプリケーション関係を作成する

スナップショット レプリケーション関係により、AFX システムとリモート ロケーション間の接続が確立され、整合性グループをリモート クラスターにレプリケートできるようになります。複製された整合性グループは、災害復旧やデータ移行に使用できます。

ランサムウェア攻撃から保護するために、レプリケーション関係を設定するときに、宛先スナップショットをロックすることを選択できます。ロックされたスナップショットは、誤ってまたは悪意を持って削除されることはありません。ボリュームがランサムウェア攻撃によって侵害された場合、ロックされたスナップショットを使用してデータを回復できます。

開始する前に

ロックされた宛先スナップショットの有無にかかわらず、レプリケーション関係を作成します。

ロックされたスナップショット

手順

1. System Manager で、保護 > 整合性グループ を選択します。
2. 整合性グループを選択します。
3. 選択 : 次に、[保護] を選択します。
4. *リモート保護*の下で、*リモート クラスタにレプリケート*を選択します。
5. *レプリケーション ポリシー*を選択します。

vault レプリケーション ポリシーを選択する必要があります。

6. *宛先設定*を選択します。
7. *削除を防ぐために宛先スナップショットをロックする*を選択します
8. 最大および最小のデータ保持期間を入力します。
9. データ転送の開始を遅らせるには、[すぐに転送を開始] の選択を解除します。

デフォルトでは、初期データ転送がすぐに開始されます。

10. オプションで、デフォルトの転送スケジュールを上書きするには、[宛先設定] を選択し、[転送スケジュールの上書き] を選択します。

転送スケジュールをサポートするには、最低 30 分にする必要があります。

11. *保存*を選択します。

ロックされたスナップショットなし

手順

1. システム マネージャーで、保護 > レプリケーション を選択します。
2. ローカル宛先またはローカルソースとのレプリケーション関係を作成する場合に選択します。

オプション	手順
地元の目的地	<ol style="list-style-type: none">a. *ローカル目的地*を選択し、。b. ソース整合性グループを検索して選択します。 <p><i>source</i> 整合性グループは、複製するローカル クラスタ上の整合性グループを指します。</p>

オプション	手順
地元の情報源	<p>a. *ローカルソース*を選択し、。</p> <p>b. ソース整合性グループを検索して選択します。</p> <p><i>source</i> 整合性グループは、複製するローカル クラスタ上上の整合性グループを指します。</p> <p>c. レプリケーション先 で、レプリケート先のクラスタを選択し、ストレージ VM を選択します。</p>

- レプリケーション ポリシーを選択します。
- データ転送の開始を遅らせるには、[宛先設定] を選択し、[すぐに転送を開始] の選択を解除します。
デフォルトでは、初期データ転送がすぐに開始されます。
- オプションで、デフォルトの転送スケジュールを上書きするには、[宛先設定] を選択し、[転送スケジュールの上書き] を選択します。
転送スケジュールをサポートするには、最低 30 分にする必要があります。
- *保存*を選択します。

次の手順

レプリケーション ポリシーと関係を作成したので、レプリケーション ポリシーで定義されたとおりに初期データ転送が開始されます。オプションでレプリケーション フェイルオーバーをテストして、AFX システムがオフラインになった場合にフェイルオーバーが正常に実行されることを確認できます。

ステップ4: レプリケーションフェイルオーバーをテストする

オプションで、ソース クラスタがオフラインの場合に、リモート クラスタ上の複製されたボリュームからデータを正常に提供できることを検証します。

手順

- システム マネージャーで、保護 > レプリケーション を選択します。
- テストしたいレプリケーション関係にマウスを移動し、。
- *フェイルオーバーのテスト*を選択します。
- フェイルオーバー情報を入力し、*フェイルオーバーのテスト*を選択します。

次の手順

災害復旧のためのスナップショットレプリケーションでデータが保護されたので、"保存データを暗号化する" AFX システム内のディスクが再利用、返却、紛失、盗難された場合でも、ディスクを読み取ることはできません。

AFXストレージシステムのデータ保護ポリシーとスケジュールを管理する

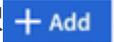
スナップショット ポリシーを使用すると、自動化されたスケジュールに基づいて整合性グループ内のデータを保護できます。スナップショット ポリシー内のポリシー スケジュールによって、スナップショットが作成される頻度が決まります。

新しい保護ポリシースケジュールを作成する

保護ポリシー スケジュールは、スナップショット ポリシーが実行される頻度を定義します。日数、時間数、分数に基づいて、定期的に行うスケジュールを作成できます。たとえば、1時間ごとに実行するスケジュールや、1日に1回だけ実行するスケジュールを作成できます。特定の曜日や月の特定の時間に実行するスケジュールを作成することもできます。たとえば、毎月20日の午前12時15分に行うスケジュールを作成できます。

さまざまな保護ポリシー スケジュールを定義することで、さまざまなアプリケーションのスナップショットの頻度を柔軟に増減できます。これにより、重要度の低いワークロードに必要なレベルよりも高いレベルの保護と、重要なワークロードに対するデータ損失のリスクの低減が可能になります。

手順

1. *保護*を選択し、次に*ポリシー*を選択して、*スケジュール*を選択します。
2. 選択 。
3. スケジュールの名前を入力し、スケジュール パラメータを選択します。
4. *保存*を選択します。

次の手順

新しいポリシー スケジュールを作成したので、ポリシー内で新しく作成したスケジュールを使用して、スナップショットが作成されるタイミングを定義できます。

Snapshotポリシーの作成

スナップショット ポリシーは、スナップショットが作成される頻度、許可されるスナップショットの最大数、およびスナップショットが保持される期間を定義します。

手順

1. システム マネージャーで、[保護]、[ポリシー]の順に選択し、[スナップショット ポリシー]を選択します。
2. 選択 。
3. スナップショット ポリシーの名前を入力します。
4. クラスタ全体にポリシーを適用するには、「クラスタ」を選択します。個々のストレージ VM にポリシーを適用するには、「ストレージ VM」を選択します。
5. *スケジュールの追加*を選択し、スナップショット ポリシー スケジュールを入力します。
6. *ポリシーの追加*を選択します。

次の手順

スナップショット ポリシーを作成したので、それを整合性グループに適用できます。スナップショット ポリシーで設定したパラメータに基づいて、整合性グループのスナップショットが取得されます。

整合性グループにスナップショットポリシーを適用する

整合性グループにスナップショット ポリシーを適用して、整合性グループのスナップショットを自動的に作成、保持、ラベル付けします。

手順

1. システム マネージャーで、[保護]、[ポリシー] の順に選択し、[スナップショット ポリシー] を選択します。
2. 適用するスナップショット ポリシーの名前の上にマウスを置きます。
3. 選択 ; 次に、[適用] を選択します。
4. スナップショット ポリシーを適用するコンシステンシー グループを選択し、[適用] を選択します。

次の手順

スナップショットでデータが保護されたので、"[レプリケーション関係を設定する](#)"バックアップと災害復旧のために、整合性グループを地理的に離れた場所にコピーします。

スナップショットポリシーを編集、削除、または無効化する

スナップショット ポリシーを編集して、ポリシー名、スナップショットの最大数、またはSnapMirrorラベルを変更します。ポリシーを削除すると、ポリシーとそれに関連付けられたバックアップ データがクラスターから削除されます。ポリシーを無効にして、ポリシーで指定されたスナップショットの作成または転送を一時的に停止します。

手順

1. システム マネージャーで、[保護]、[ポリシー] の順に選択し、[スナップショット ポリシー] を選択します。
2. 編集するスナップショット ポリシーの名前にマウスを置きます。
3. 選択 ; 次に、[編集]、[削除]、または [無効化] を選択します。

結果

スナップショット ポリシーを変更、削除、または無効化しました。

レプリケーションポリシーを編集する

レプリケーション ポリシーを編集して、ポリシーの説明、転送スケジュール、およびルールを変更します。ポリシーを編集して、ネットワーク圧縮を有効または無効にすることもできます。

手順

1. システム マネージャーで、[保護] を選択し、[ポリシー] を選択します。
2. *レプリケーション ポリシー*を選択します。
3. 編集したいレプリケーションポリシーにマウスを移動し、。
4. *編集*を選択します。
5. ポリシーを更新し、[保存] を選択します。

安全なデータ

AFXストレージシステムのデータを保護する準備

AFX データを管理する前に、主要な概念と機能について理解しておく必要があります。

用語とオプション

AFX データ セキュリティに関連して、知っておくべき用語がいくつかあります。

ランサムウェア

ランサムウェアは、ファイルを暗号化してユーザーがアクセスできないようにする悪意のあるソフトウェアです。通常、データを復号化するには何らかの支払いが要求されます。ONTAP は、Autonomous Ransomware Protection (ARP) などの機能を通じて、ランサムウェアから保護するソリューションを提供します。

暗号化

暗号化とは、適切な認証なしには簡単に読み取ることができない安全な形式にデータを変換するプロセスです。ONTAP は、保存中のデータを保護するために、ソフトウェア ベースとハードウェア ベースの両方の暗号化テクノロジーを提供します。これにより、ストレージ メディアが再利用、返却、紛失、盗難された場合でも、読み取ることができなくなります。これらの暗号化ソリューションは、外部のキー管理サーバーまたはONTAPが提供するオンボード キー マネージャーを使用して管理できます。参照["AFX ストレージシステムに保存されているデータを暗号化する"](#)詳細についてはこちらをご覧ください。

デジタル証明書とPKI

デジタル証明書は、公開鍵の所有権を証明するために使用される電子文書です。公開キーと関連する秘密キーは、通常、TLS や IPsec などの大規模なセキュリティ フレームワークの一部として ID を確立するなど、さまざまな方法で使用できます。これらのキーと、それをサポートするプロトコルおよびフォーマット標準は、公開キー インフラストラクチャ (PKI) の基礎を形成します。参照["AFX ストレージシステム上の証明書を管理する"](#)詳細についてはこちらをご覧ください。

インターネットプロトコルセキュリティ

IPsec は、IP レベルでネットワーク エンドポイント間を流れるトラフィックに対して、転送中のデータの暗号化、整合性、および認証を提供するインターネット標準です。NFS や SMB などの上位レベルのプロトコルを含む、ONTAPとクライアント間のすべての IP トラフィックを保護します。IPsec は、データに対する悪意のあるリプレイ攻撃や中間者攻撃から保護します。参照["AFXストレージシステム上の安全なIP接続"](#)詳細についてはこちらをご覧ください。

関連情報

- ["追加のAFX SVM管理"](#)
- ["AFX システムの管理を準備する"](#)

AFX ストレージ システムに保存されているデータを暗号化する

ハードウェア レベルとソフトウェア レベルでデータを暗号化し、二重の保護を実現できます。保存データを暗号化すると、ストレージ メディアが再利用、返却、紛失、盗難された場合でも、データを読み取ることができなくなります。

NetApp Storage Encryption (NSE) は、自己暗号化ドライブ (SED) を使用したハードウェア暗号化をサポートします。SED は書き込まれるデータを暗号化します。各 SED には一意の暗号化キーが含まれています。SED に保存された暗号化されたデータは、SED の暗号化キーがなければ読み取ることができません。SED からの読み取りを試みるノードは、SED の暗号化キーにアクセスするために認証を受ける必要があります。ノードは、キー マネージャーから認証キーを取得し、その認証キーを SED に提示することによって認証されます。認証キーが有効な場合、SED はノードに暗号化キーを提供し、ノードに含まれるデータにアクセスできるようにします。

開始する前に

AFX オンボード キー マネージャーまたは外部キー マネージャーを使用して、ノードに認証キーを提供します。NSE に加えて、ソフトウェア暗号化を有効にして、データのセキュリティをさらに強化することもできます。

手順

1. システム マネージャーで、**クラスター** を選択し、次に **設定** を選択します。
2. **セキュリティ セクション** の **暗号化** で、**構成** を選択します。
3. キー マネージャーを構成します。

オプション	手順
オンボードキーマネージャーを構成する	<ol style="list-style-type: none"> a. キー サーバーを追加するには、[オンボード キー マネージャー] を選択します。 b. パスフレーズを入力します。
外部キー管理ツールの設定	<ol style="list-style-type: none"> a. キー サーバーを追加するには、[外部キー マネージャー] を選択します。 b. 選択 + Add キーサーバーを追加します。 c. KMIP サーバーの CA 証明書を追加します。 d. KMIP クライアント証明書を追加します。

4. ソフトウェア暗号化を有効にするには、「**二重層暗号化**」を選択します。
5. ***保存***を選択します。

関連情報

- ["暗号化"](#)

AFXストレージシステム上の安全なIP接続

IP セキュリティ (IPsec) は、ネットワーク エンドポイント間を流れるトラフィックに対して IP レベルでデータの暗号化、整合性、および認証を提供するインターネット プロトコル標準です。IPsec を使用すると、AFX クラスターとクライアント間のフロントエンド ネットワークのセキュリティを強化できます。

AFX システムでの IPsec の構成

AFX ストレージ システムの IPsec 構成手順は、ハードウェア オフロード機能で使用されるサポートされているネットワーク インターフェイス コントローラ (NIC) カードを除き、AFFおよびFASシステムと同じです。参照 ["ONTAPネットワークのIPセキュリティを設定するための準備"](#) 詳細についてはこちらをご覧ください。

ハードウェアオフロード機能

暗号化や整合性チェックなどの IPsec 暗号化操作のいくつかは、AFX システムでサポートされている NIC カードにオフロードできます。これにより、IPsec によって保護されたネットワーク トラフィックのパフォーマンスとスループットが大幅に向上します。



ONTAP 9.18.1 以降では、IPsec ハードウェア オフロード機能が拡張され、IPv6 トラフィックがサポートされるようになりました。

ONTAP 9.17.1 以降の AFX ストレージ システムの IPsec ハードウェア オフロード機能では、次の NIC カードがサポートされています。

- X50130B (2p、40G/100G イーサネット コントローラ)
- X50131B (2p、40G/100G/200G/400G イーサネット コントローラ)

参照 ["NetApp Hardware Universe"](#) AFX システムで実行されている ONTAP リリースでサポートされているカードの詳細については、[こちら](#) を参照してください。

関連情報

- ["ONTAPネットワークのIPセキュリティを設定するための準備"](#)
- ["NetApp Hardware Universe"](#)

AFX ストレージ システム SVM の追加管理

一般的な AFX SVM 管理に加えて、環境に応じて実行する必要がある他のタスクがある場合があります。追加タスクのほとんどは System Manager を使用して実行できますが、場合によっては CLI を使用する必要があることもあります。



ここで説明する ONTAP の機能と管理は、AFX ストレージ システムと、Unified ONTAP を実行する AFF または FAS システムに共通です。関連する Unified ONTAP ドキュメントへのリンクが必要に応じて含まれています。

ストレージ管理とパフォーマンス

AFX 展開で構成および使用できるオプションのストレージ管理およびパフォーマンス機能がいくつかあります。

ONTAP NAS ストレージ管理

ネットワーク接続ストレージ (NAS) は、ネットワーク内の複数のクライアントがアクセスできる専用のファイル ストレージを提供します。ONTAP は複数の NAS プロトコルをサポートしています。参照 ["NAS ストレージの管理"](#) 詳細についてはこちらをご覧ください。

ONTAP FlexCacheボリューム

FlexCacheは、ONTAPのリモート キャッシュ機能です。データがクライアントに近づくため、アクセス パフォーマンスが向上し、コストが削減されます。最初に元のファイル システムからメタデータのみをコピーするFlexCacheボリュームを作成すると、ファイルの配布が簡素化され、WAN トラフィックが削減されます。参照 ["ONTAP FlexCacheボリュームについて学ぶ"](#)詳細についてはこちらをご覧ください。

ONTAP FlexGroupボリューム

FlexGroupボリュームは、トラフィックを自動的かつ透過的に共有する複数のメンバー ボリュームで構成されます。FlexGroupボリュームには、高パフォーマンスや管理の簡素化など、さまざまな利点があります。参照 ["FlexGroupボリュームのセットアップ"](#)詳細についてはこちらをご覧ください。

データ保護

AFX 展開で構成および使用できるオプションのデータ保護機能がいくつかあります。

一貫性グループ

整合性グループは、1つの単位として管理されるボリュームの集まりです。参照 ["ONTAP コンシステンシーグループについて学ぶ"](#)詳細についてはこちらをご覧ください。

SnapLock

ボリューム レベルでファイルを一度だけ書き込み、何度も読み取り可能 (WORM) 状態に変換することで、ファイルを保護できます。SnapLock は2つのモードをサポートしています。コンプライアンス モードでは、政府または業界固有の規制に対応するため、ファイルの保持期間が過ぎるまでファイルを削除できないようにします。エンタープライズ モードでは、特権ユーザーは保持期間が終了する前にファイルを削除できます。参照 ["ONTAP SnapLockについて学ぶ"](#)詳細についてはこちらをご覧ください。

セキュリティ

AFX 展開で構成および使用できるオプションのセキュリティ機能がいくつかあります。

FPolicy

FPolicy は、ストレージ仮想マシン (SVM) 上のファイル アクセス イベントを監視および管理するために使用されるファイル アクセス通知フレームワークです。FPolicy を使用すると、定義した基準に基づいて、監視するファイル操作、およびオプションでブロックするファイル操作を定義するポリシーを作成できます。FPolicy は、セキュリティ監査、コンプライアンス、データ ガバナンスによく使用されます。参照 ["ONTAP FPolicyソリューションについて学ぶ"](#)詳細についてはこちらをご覧ください。

ONTAPイベントとパフォーマンスの監視

クラスターの健全性とパフォーマンスを監視できます。これには、イベントのアラートの設定とシステムヘルスアラートの通知の管理が含まれます。参照 ["イベント、パフォーマンス、健全性の監視"](#)詳細についてはこちらをご覧ください。

関連情報

- ["AFX ストレージ システムに関する FAQ"](#)

- "AFX クラスターの追加管理"

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。