



ONTAPの詳細

ONTAP 9

NetApp
February 13, 2026

目次

| | |
|------------------------------------------|----|
| ONTAPの詳細 | 1 |
| ONTAPプラットフォーム | 1 |
| ONTAPのユーザ インターフェイス | 2 |
| ONTAP System Manager | 2 |
| NetApp Console | 3 |
| ONTAPコマンドライン インターフェイス | 3 |
| ONTAP REST API | 3 |
| NetAppのツールキットとフレームワーク | 3 |
| ONTAP System ManagerをNetApp Consoleと統合する | 3 |
| NetApp Console と ONTAP 9.12.1 | 4 |
| NetApp Consoleの詳細 | 5 |
| クラスタ ストレージ | 5 |
| ハイアベイラビリティ ペア | 6 |
| AutoSupportとDigital Advisor | 7 |
| ネットワーク アーキテクチャ | 8 |
| ネットワーク アーキテクチャ - 概要 | 8 |
| 論理ポート | 9 |
| 業界標準のネットワーク テクノロジーのサポート | 10 |
| RDMAの概要 | 11 |
| クライアント プロトコル | 12 |
| NFS | 12 |
| SMB | 13 |
| FC | 13 |
| FCoE | 13 |
| iSCSI | 13 |
| NVMe / FCとNVMe / TCP | 13 |
| S3 | 14 |
| ディスクとローカル階層 | 14 |
| ディスクとONTAPローカル階層 | 14 |
| ONTAP RAID グループとローカル階層 | 15 |
| ミラーリングされたローカル層とミラーリングされていないローカル層 | 16 |
| ルート データ パーティショニング | 19 |
| ボリューム、qtree、ファイル、LUN | 20 |
| ストレージ仮想化 | 22 |
| ストレージ仮想化 - 概要 | 22 |
| SVMのユースケース | 22 |
| クラスタとSVMの管理 | 23 |
| ネームスペースとジャンクション ポイント | 24 |
| パスのフェイルオーバー | 25 |

| | |
|-------------------------------------|----|
| パスのフェイルオーバー - 概要 | 25 |
| NASパスのフェイルオーバー | 26 |
| SANパスのフェイルオーバー | 27 |
| ONTAPのロード バランシング | 28 |
| スループットの上限 | 28 |
| スループットの下限 | 29 |
| アダプティブQoS | 30 |
| レプリケーション | 31 |
| Snapshot 数 | 31 |
| SnapMirrorによるディザスタ リカバリとデータ転送 | 32 |
| オブジェクト ストレージへのSnapMirrorクラウドのバックアップ | 33 |
| SnapVaultアーカイブ | 34 |
| クラウド バックアップと従来のバックアップのサポート | 36 |
| MetroClusterの継続的可用性 | 36 |
| ストレージ効率 | 38 |
| ONTAP Storage Efficiencyの概要 | 38 |
| シンプロビジョニング | 41 |
| 重複排除 | 41 |
| 圧縮 | 42 |
| FlexCloneのボリューム、ファイル、LUN | 42 |
| ONTAP容量レポートと測定について学ぶ | 43 |
| ONTAPの温度に影響されるストレージ効率について学ぶ | 47 |
| ONTAP専用オフロードプロセッサのストレージ効率について学ぶ | 49 |
| セキュリティ | 51 |
| クライアント認証と許可 | 51 |
| 管理者認証とRBAC | 52 |
| ウイルススキャン | 53 |
| 暗号化 | 54 |
| WORMストレージ | 56 |
| ONTAPとVMware vSphere | 57 |
| 主な概念と用語 | 57 |
| NetAppプラグインと関連テクノロジー | 58 |
| 追加情報へのアクセス | 59 |
| FabricPool | 59 |

ONTAPの詳細

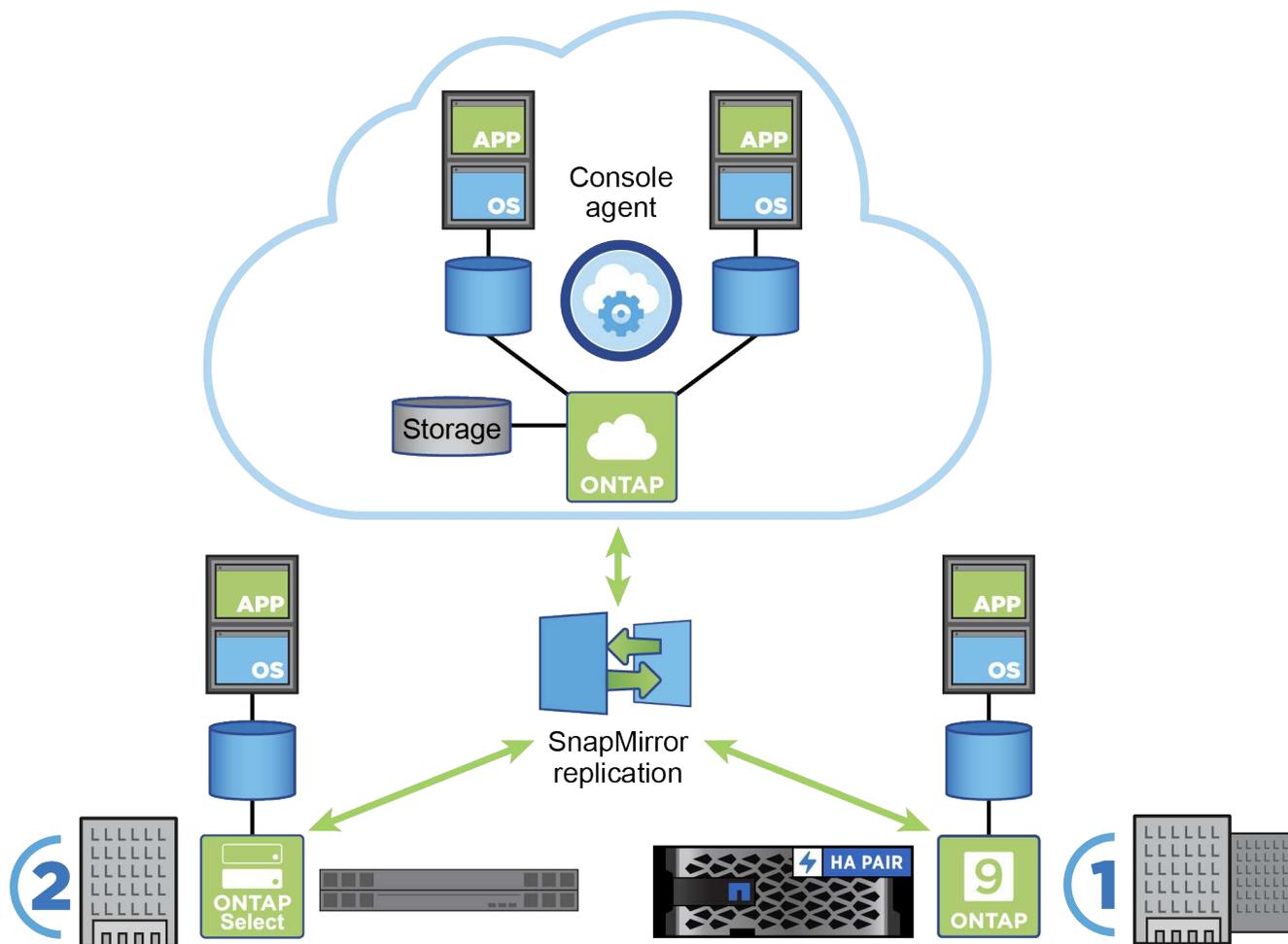
ONTAPプラットフォーム

ONTAPデータ管理ソフトウェアは、ブロック データやファイル データを読み書きするアプリケーションにユニファイド ストレージを提供します。高速なフラッシュから低コストの回転式メディアやクラウドベースのオブジェクト ストレージまで、ストレージ構成には幅広いオプションがあります。

ONTAP実装は、以下の環境で実行されます。

- **NetApp** エンジニアリング システム："[AFF、AFX、ASA、およびFASストレージ システム](#)"
- **ONTAP** ストレージ パーソナリティ："[AFXおよびASA r2ストレージシステム](#)"特定のプロトコルに重点を置いた分散型ONTAPストレージを提供する専用のONTAPパーソナリティを実行します。
- 市販のハードウェア："[ONTAP Select](#)"
- プライベート、パブリック、またはハイブリッドクラウド："[Cloud Volumes ONTAP](#)"、"[Amazon FSx for NetApp ONTAP](#)"、"[Azure NetApp Files](#)"、および "[Google Cloud NetApp Volumes](#)"
- 特化した実装（"[FlexPod データセンター](#)"業界最高の統合インフラストラクチャを提供するを含む）

これらの実装を組み合わせることで、インテリジェント データ インフラストラクチャの基本フレームワークが形成されます。このフレームワークは、データ管理に対する共通のソフトウェアで定義されるアプローチと、プラットフォーム間的高速かつ効率的なレプリケーションを備えています。



ONTAPのユーザ インターフェイス

ONTAPデータ管理ソフトウェアには、ONTAPクラスタの管理に使用できる複数のインターフェイスが用意されています。複数のインターフェイス オプションがあることで、環境に応じてさまざまなアクセス レベルや機能を使い分けて、柔軟にONTAPクラスタを管理できます。

これらのインターフェイスのいずれかを使用して、ONTAPクラスタを管理したり、データ管理操作を実行したりできます。

ONTAP System Manager

ONTAP System Managerは、Webベースのユーザ インターフェイスです。シンプルかつわかりやすい操作でクラスタを管理できます。ストレージ構成、データ保護、ネットワークのセットアップと管理といった一般的な処理を行えます。System Managerでは、リスクとクラスタのパフォーマンスを監視する機能や、クラスタの問題に対処したり問題を発生前に先取りしたりするのに役立つ分析情報も提供されます。["詳細情報"](#)。

ONTAP 9.7は、ONTAP System Managerにとって重要な節目となりました。このリリースでは、NetAppがONTAP System Managerの2つのバージョンを提供し、再設計されたより合理化された直感的なバージョンと、ONTAP 9.7以前のバージョンを導入しました。ONTAP 9.7以降、再設計されたバージョンはONTAP System Managerとして継承され、その前身はSystem Manager Classicに改名されました。System Manager ClassicはONTAP 9.7で最後に更新されました。System Manager Classicをご利用の場合は、ドキュメントを

ご覧ください ["別途"](#)。

NetApp Console

ONTAP 9.12.1以降、NetApp ConsoleのWebベースのインターフェイスを使用して、従来のSystem Manager ダッシュボードを維持しながら、単一のコントロールプレーンからハイブリッドマルチクラウドインフラを管理できます。Consoleを使用すると、クラウドストレージ（例：NetApp Backup and Recovery）の作成や管理、NetAppのデータサービス（例：Cloud Backup）の利用、多くのオンプレミスおよびエッジストレージデバイスの制御が可能です。オンプレミスのONTAPシステムをConsoleに追加することで、すべてのストレージおよびデータ資産を単一のインターフェイスから管理できます。 ["詳細情報"](#)。

ONTAP コマンドライン インターフェイス

"[ONTAP コマンドライン インターフェイス \(CLI\)](#)" は、"[コマンド](#)"を使用してクラスタ、ノード、SVMなどを操作できるテキストベースのインターフェイスです。CLIコマンドは、"[ロールタイプ](#)"に基づいて使用できます。ONTAP CLIには、SSHまたはクラスタ内のノードへのコンソール接続を介してアクセスできます。

ONTAP REST API

ONTAP 9.6以降では、クラスタ操作をプログラムで管理および自動化できるRESTful APIにアクセスできます。このAPIを使用して、ボリューム、Snapshot、アグリゲートの作成と管理、クラスタパフォーマンスの監視など、さまざまなONTAP管理タスクを実行できます。ONTAP REST APIには、curlなどのユーティリティを使用して直接アクセスすることも、Python、PowerShell、JavaなどのRESTクライアントをサポートする任意のプログラミング言語を使用してアクセスすることもできます。 ["詳細情報"](#)。



ONTAPIは、ONTAP REST APIに先行する独自のONTAP APIです。ONTAPIを使用している場合は、["ONTAP REST APIへの移行"](#)を計画する必要があります。

NetAppのツールキットとフレームワーク

NetAppには、ONTAP REST APIを抽象化して簡単に自動化コードを作成できる、特定の開発言語と開発環境用のクライアント ツールキットが用意されています。 https://docs.netapp.com/us-en/ontap-automation/get-started/ontap_automation_options.html#client-software-toolkits [\["詳細情報"\]](#)。

これらのツールキットに加えて、フレームワークを使用して自動化コードを作成し、展開することもできます ["詳細情報"](#)。

ONTAP System ManagerをNetApp Consoleと統合する

NetApp ConsoleのSystem Managerを使用して、ONTAP 9.10.1以降のリリースを管理できます。この統合により、使い慣れたSystem Managerのユーザーインターフェイスを維持しながら、統合されたコントロールプレーンを使用してハイブリッドマルチクラウドインフラストラクチャを効率的に監視できます。

コンソールを使用すると、クラウド ストレージ（Cloud Volumes ONTAP など）を作成および管理したり、NetAppデータ サービス（Cloud Backup など）を使用したり、多数のオンプレミスおよびエッジ ストレージ デバイスを制御したりできます。

NetApp Consoleでは、クラスターを検出して管理するための2つの方法が提供されています：

- System Manager (ONTAP 9.12.1以降) を介した管理のための直接検出
- Console エージェントによる検出。

コンソールエージェントは、環境にインストールされるソフトウェアです。これにより、System Manager を通じて管理機能にアクセスしたり、NetApp クラウドサービスにアクセスしてデータレプリケーション、バックアップとリカバリ、データ分類、データ階層化などの機能を利用したりできるようになります。

"[NetApp Console を使用したオンプレミスの ONTAP クラスタ管理](#)"についての詳細をご覧ください。

手順

1. NetApp Console にログインします。
 - a. Console ログインがある場合はそれを使用します。
 - b. 初めての場合は、NetApp Support Siteの資格情報を使用してログインを選択し、Consoleログインページで資格情報を入力します。
2. Console エージェントまたは直接検出を使用して、Console でオンプレミスクラスタを検出します。詳細については、<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>[オンプレミス ONTAP クラスタの検出]をご覧ください。
 - a. "[直接検出されたクラスタを管理する](#)"方法を学びましょう。
 - b. "[Console エージェントで検出されたクラスタを管理する](#)"方法を学びましょう。
3. System Managerを使用してオンプレミスクラスタを管理します。「My working environments Systems」ページでクラスタを選択し、「Services」リストから「System Manager」をクリックします。
 - a. "[直接検出されたクラスタを管理する](#)"についての詳細をご覧ください。
 - b. "[Console エージェントで検出されたクラスタを管理する](#)"方法を学びましょう。

NetApp Console と ONTAP 9.12.1

注意：ONTAP 9.12.1 を使用している場合、NetApp Console をお試しいただくよう促すメッセージが表示されます。

+ クラスタがNetApp Consoleに接続されている場合は、ログイン プロンプトが表示されます。

1. **Continue to NetApp Console** をクリックして、コンソールへのリンクに進みます。



システム設定で外部ネットワークがブロックされている場合、Consoleにアクセスできません。Consoleを使用してSystem Managerにアクセスするには、システムから「cloudmanager.cloud.netapp.com」というアドレスにアクセスできることを確認してください。アクセスできない場合は、プロンプトで、ONTAPシステムにインストールされているバージョンのSystem Managerを使用するように選択できます。

2. Console のログイン ページで、*NetApp Support Site の資格情報を使用してログイン*を選択し、資格情報を入力します。

すでにNetApp Consoleを使用しており、メールとパスワードを使用してログインしている場合は、代わりにそのログイン オプションを引き続き使用する必要があります。

"[NetApp Consoleへのログインの詳細](#)".

3. プロンプトが表示されたら、新しいNetApp Console アカウントの名前を入力します。

ほとんどの場合、NetApp Consoleはクラスターのデータに基づいて自動的にアカウントを作成します。

4. クラスタ管理者のクレデンシャルを入力します。

結果

System Manager が表示され、NetApp Console からクラスターを管理できるようになります。

NetApp Consoleの詳細

- ["NetApp Consoleの概要"](#)
- ["NetApp Console を使用して NetApp AFF および FAS システムを管理"](#)

クラスタ ストレージ

ONTAPの現在のイテレーションは、もともとNetAppのスケールアウト型_クラスタ_ストレージ アーキテクチャ用に開発されました。これは、データセンターでのONTAP実装で一般的に見られるアーキテクチャです。この実装ではONTAPのほとんどの機能が実行されるため、ONTAPテクノロジーの基礎となる概念を理解するための出発点として最適です。

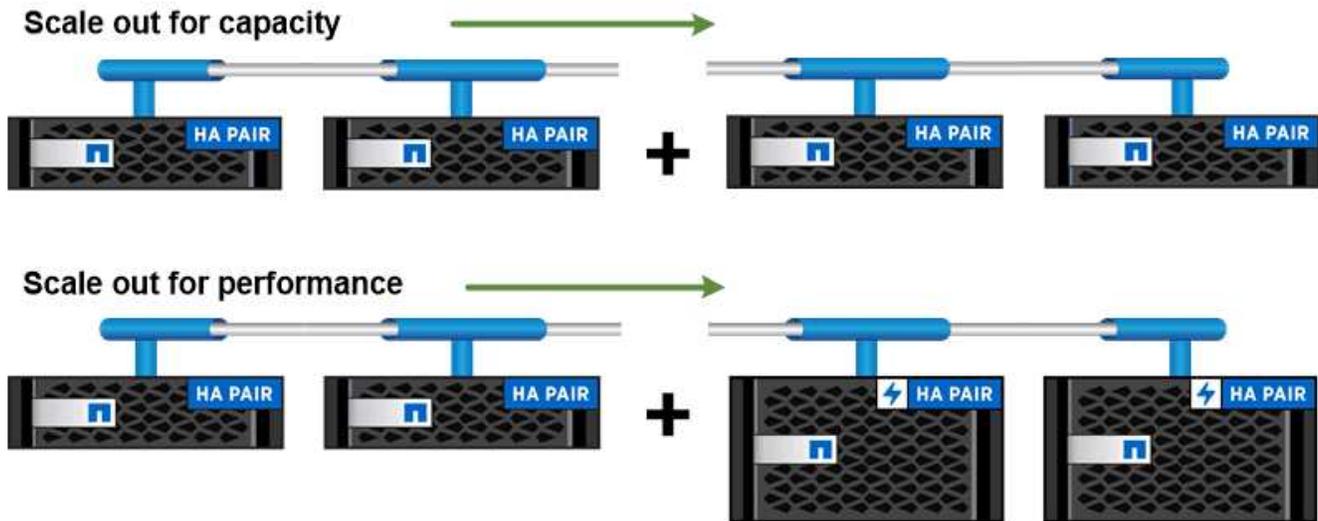
データセンター アーキテクチャでは通常、ONTAP データ管理ソフトウェアを実行する専用の AFF、ASA、または FAS システムを導入します。各コントローラ、そのストレージ、ネットワーク接続、およびコントローラ上で実行される ONTAP のインスタンスは、_ノード_と呼ばれます。

ノードはハイアベイラビリティ (HA) ペアを構成します。このペアを複数配置したものが (SANの場合は最大12ノード、NASの場合は最大24ノード) クラスタです。ノードは専用のプライベートなクラスタ インターコネクトを介して相互に通信します。

ノードのストレージは、コントローラのモデルに応じて、フラッシュ ディスク、大容量ドライブ、またはその両方で構成されます。データへのアクセスはコントローラのネットワーク ポートから提供されます。物理ストレージやネットワーク接続のリソースは仮想化され、クラスタ管理者のみが見ることができ、NASクライアントやSANホストからは見えません。

HAペアの各ノードで使用するストレージ アレイ モデルは同じでなければなりません。ペアが異なれば、サポートされる任意のコントローラを組み合わせる使用できません。スケールアウトする場合、容量を増やすには同じストレージ アレイ モデルを使用するノードを追加し、パフォーマンスを高めるにはハイエンドのストレージ アレイを使用するノードを追加します。

もちろん、従来の方法によるスケールアップもすべて可能で、必要に応じてディスクやコントローラをアップグレードできます。ONTAPの仮想化されたストレージ インフラでは、データを無停止で簡単に移動できるため、スケールアップやスケールアウトをダウンタイムなしで実行できます。



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

ハイアベイラビリティ ペア

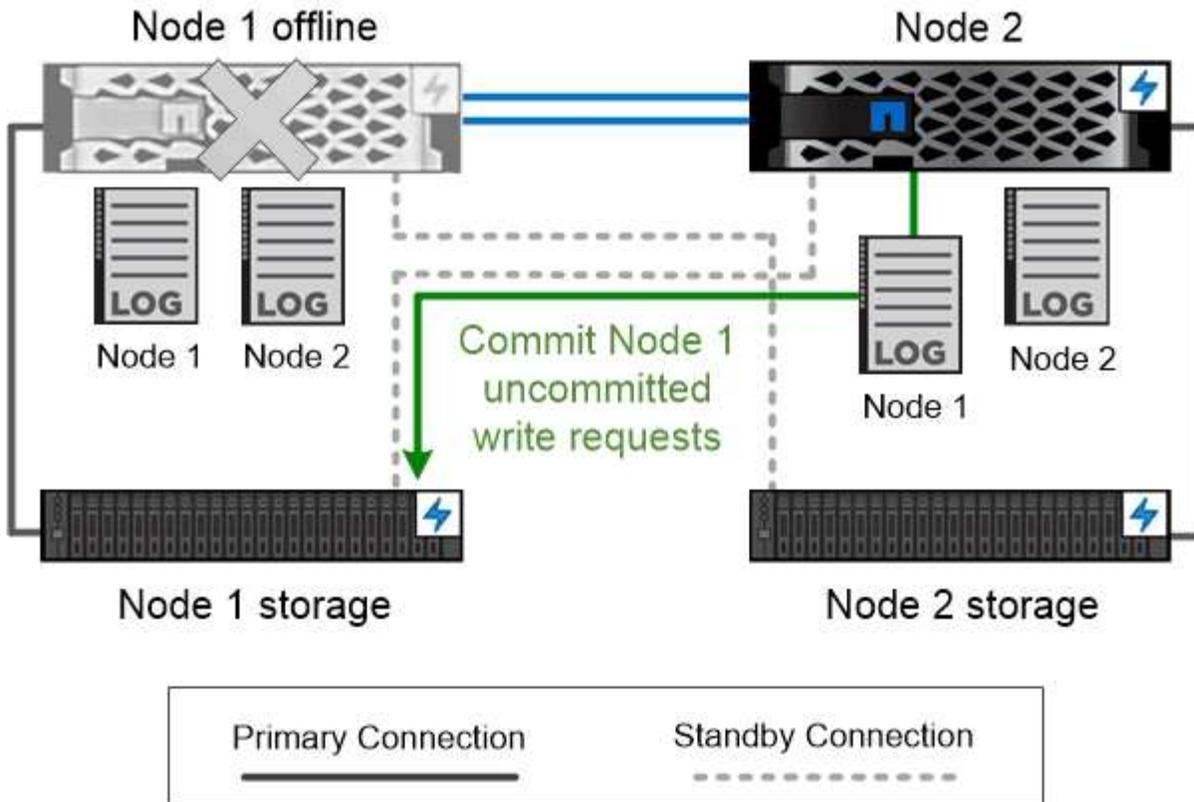
クラスタノードは、フォールトトレランスと無停止運用を実現するために、高可用性 (HA) ペアで構成されます。ノードに障害が発生した場合、または定期メンテナンスのためにノードを停止する必要がある場合、そのノードのパートナーがストレージを引き継ぎ、引き続きそこからデータを提供します。ノードがオンラインに戻ると、パートナーはストレージを返還します。

HAペアは、必ず同じシリーズのコントローラ モデルで構成されます。通常、コントローラは冗長電源装置を備えた同じシャーシに配置されます。

HAペアは、異なる方法で相互通信できるフォールトトレラントノードです。これにより、各ノードはパートナーノードの動作状態を継続的に確認し、もう一方のノードの不揮発性メモリのログデータをミラーリングできます。ノードへの書き込み要求は、クライアントまたはホストに応答が返される前に、両方のノードのNVRAMに記録されます。フェイルオーバー時には、存続しているパートナーノードが障害の発生したノードの未コミットの実行要求をディスクにコミットすることで、データの整合性を確保します。存続しているノードは、以前は障害の発生したノードのNVRAMのミラーとして機能していたNVRAMパーティションに書き込みを記録し続けます。

パートナー ノードのコントローラのストレージ メディアとの接続が確保されているため、テイクオーバー時に各ノードはパートナーのストレージにアクセスできます。ネットワーク パスのフェイルオーバー メカニズムにより、クライアントとホストは稼働しているノードと引き続き通信することが可能です。

可用性を確保するためには、フェイルオーバー時の追加のワークロードに対応できるように、各ノードのパフォーマンス容量利用率を50%に抑える必要があります。同じ理由で、1つのノードに割り当てるNAS仮想ネットワーク インターフェイスは最大数の半分までにすることを推奨します。



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

仮想化されたONTAP実装におけるテイクオーバーとギブバック

ONTAP Selectのような仮想化された「shared-nothing」ONTAP実装では、ストレージはノード間で共有されません。ノードがダウンした場合、そのパートナーはノードのデータの同期ミラーコピーからデータの提供を継続します。パートナーはノードのストレージを引き継ぐのではなく、データ提供機能のみを引き継ぎます。

AutoSupportとDigital Advisor

ONTAPでは、Webポータルとモバイル アプリを使用して人工知能によるシステムの監視とレポートを提供します。ONTAPのAutoSupportコンポーネントから計測データが送信され、Active IQ Digital Advisor（Digital Advisorとも呼ばれます）で分析されます。

Digital Advisorはクラウドベースのポータルとモバイル アプリで構成されます。実用的な予測分析とプロアクティブなサポートを提供することで、グローバル ハイブリッド クラウド全体でのデータ インフラの最適化を実現します。NetAppと有効なSupportEdge契約を締結しているお客様であれば、Digital Advisorからデータ主体の分析情報と推奨事項を受け取ることができます（機能は製品およびサポート レベルによって異なります）。

以下は、Digital Advisorで実行できる機能の一例です。

- アップグレードを計画する。Digital Advisorは新しいバージョンのONTAPにアップグレードすることで解決できる環境内の問題を特定し、Upgrade Advisorがアップグレードの計画を支援します。
- システムの健全性を表示する。Digital Advisorダッシュボードに健全性に関する問題が報告され、問題の解決方法が提示されます。ストレージ スペースが不足しないようにシステム容量を監視できます。
- パフォーマンスを管理する。Digital Advisorでは、System Managerよりも長期間にわたるシステム パフォーマンスが表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定できます。
- 効率を最大化する。ストレージ効率の指標を確認し、より多くのデータをより少ないスペースに格納する方法を特定できます。
- インベントリと構成を表示する。Digital Advisorでは、すべてのインベントリおよびソフトウェアとハードウェアの構成情報が表示されます。サービス契約が期限切れにならないように契約期間を確認できます。

関連情報

["NetAppドキュメント：Digital Advisor"](#)

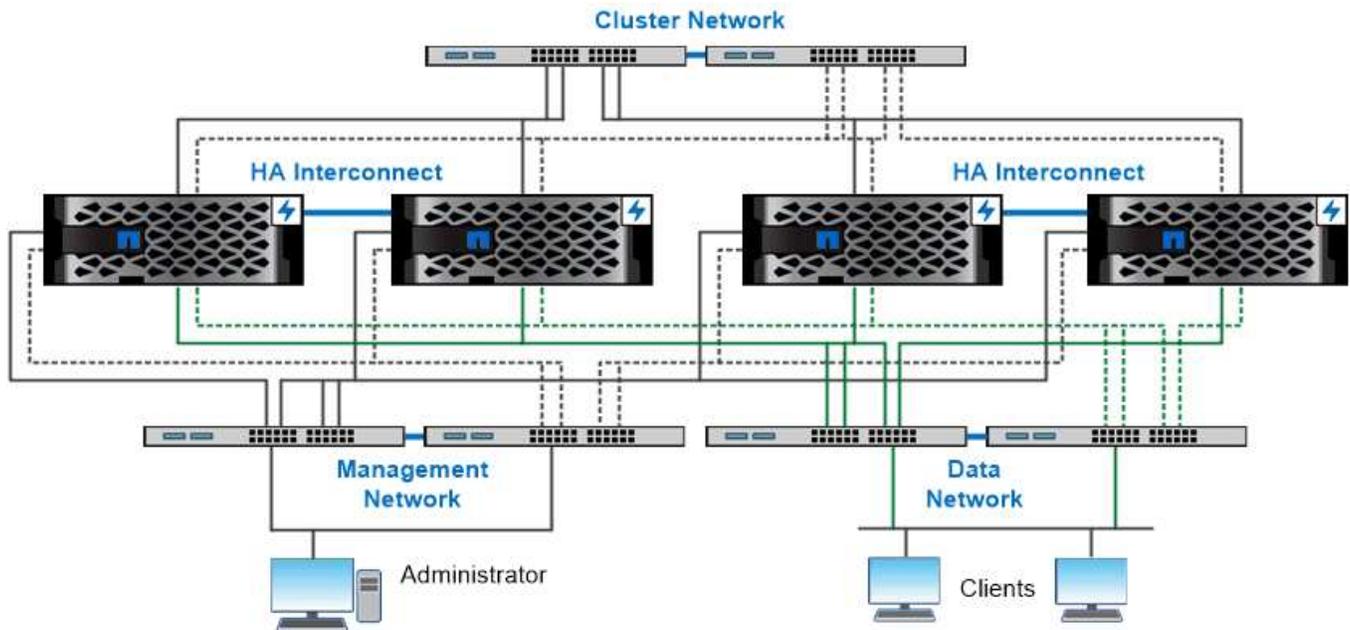
["Digital Advisorのリリース"](#)

["SupportEdgeサービス"](#)

ネットワーク アーキテクチャ

ネットワーク アーキテクチャ - 概要

ONTAPデータセンターの代表的なネットワーク アーキテクチャは、クラスタ インターコネクト、クラスタ管理用の管理ネットワーク、およびデータ ネットワークで構成されます。イーサネット接続用の物理ポートにはNIC（ネットワーク インターフェイス カード）を使用し、FC接続用の物理ポートにはHBA（ホスト バス アダプタ）を使用します。



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

論理ポート

各ノードに提供される物理ポートに加えて、論理ポートを使用してネットワークトラフィックを管理できます。論理ポートはインターフェースグループまたはVLANです。

インターフェースグループ

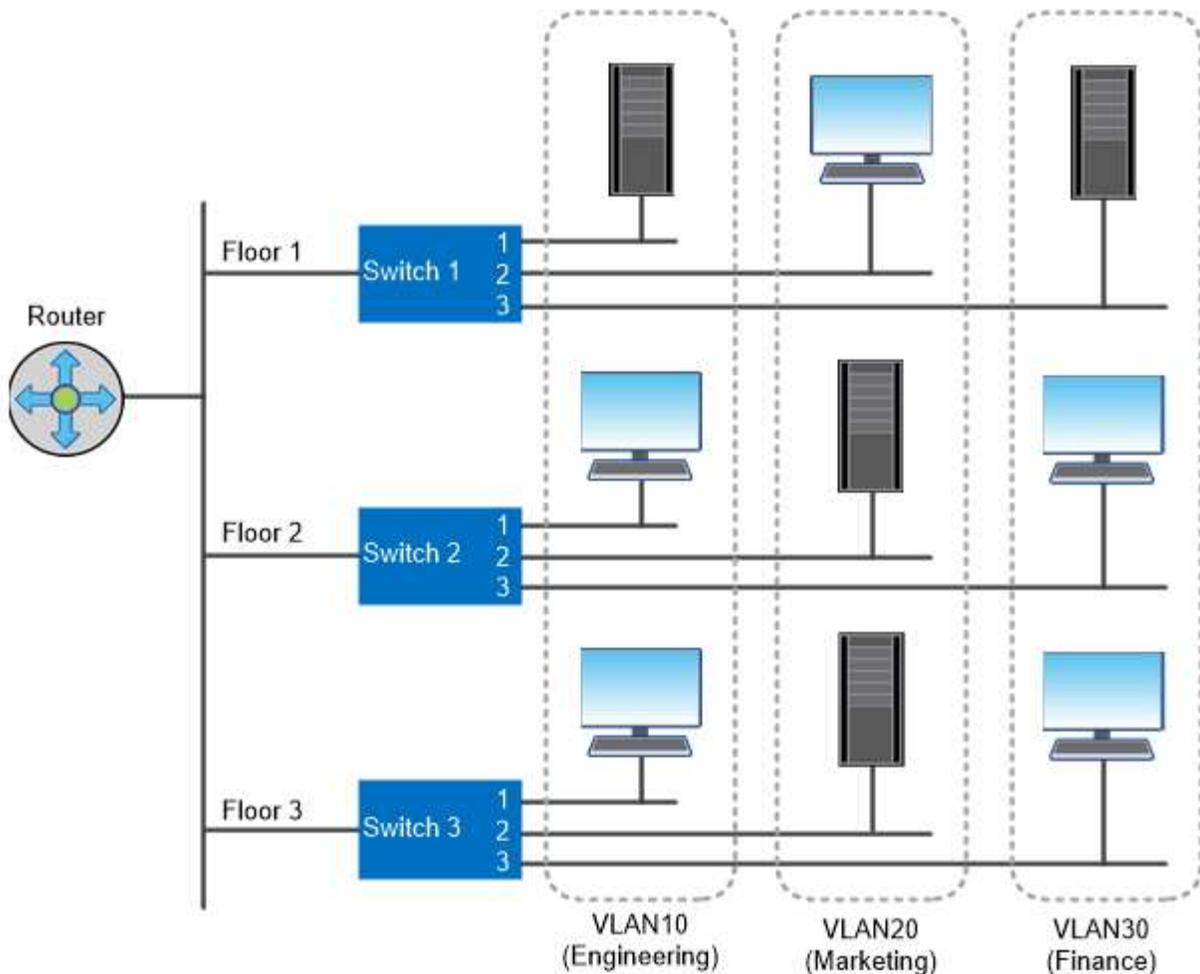
インターフェースグループは、複数の物理ポートを単一の論理「トランクポート」に統合します。異なるPCIスロットのNICのポートで構成されるインターフェースグループを作成することで、スロット障害によるビジネスクリティカルトラフィックのダウンを防ぐことができます。

インターフェースグループには、シングルモード、マルチモード、またはダイナミックマルチモードという3つのモードがあります。モードごとにフォールトトレランスのレベルが異なります。どちらかのタイプのマルチモードインターフェースグループを使用すると、ネットワークトラフィックを負荷分散できます。

VLAN

VLANは、ネットワークポート（インターフェースグループの場合もあります）からのトラフィックを、物理的な境界ではなくスイッチポート単位で定義された論理セグメントに分割します。VLANに属するエンドステーションは、機能またはアプリケーションによって関連付けられます。

たとえば、エンジニアリングやマーケティングなどの部門単位、またはリリース1やリリース2などのプロジェクト単位で、エンドステーションをまとめることができます。VLANではエンドステーションが物理的に近接していることは重要ではなく、地理的に離れた場所に配置することができます。



You can use VLANs to segregate traffic by department.

業界標準のネットワーク テクノロジーのサポート

ONTAPは、業界標準の主要なネットワーク テクノロジーをすべてサポートしています。たとえば、IPspace、DNSロード バランシング、SNMPトラップなどです。

ブロードキャスト ドメイン、フェイルオーバー グループ、およびサブネットについては、[NASパスのフェイルオーバー](#)で説明します。

IPspace

IPspace を使用すると、クラスタ内の各仮想データ サーバーに個別のIPアドレス空間を作成できます。これにより、管理上異なるネットワーク ドメインに属するクライアントは、同じIPアドレス サブネット範囲の重複するIPアドレスを使用しながら、クラスタ データにアクセスできるようになります。

たとえば、サービス プロバイダは、クラスタへのアクセス用に同じIPアドレスを使用してテナントごとに異なるIPspaceを設定できます。

DNSロード バランシング

`_DNSロードバランシング_`を使用すると、利用可能なポート間でユーザーのネットワーク トラフィックを分

散できます。DNSサーバーは、インターフェースにマウントされているクライアントの数に基づいて、トラフィック用のネットワーク インターフェースを動的に選択します。

SNMPトラップ

SNMPトラップを使用すると、動作しきい値や障害を定期的を確認できます。SNMPトラップは、SNMPエージェントから SNMP マネージャーに非同期的に送信されるシステム監視情報をキャプチャします。

FIPS準拠

ONTAPは、すべてのSSL接続について連邦情報処理標準 (FIPS) 140-2に準拠しています。SSL FIPSモードを有効または無効にしたり、SSLプロトコルをグローバルに設定したり、RC4などの弱い暗号を無効にしたりできます。

RDMAの概要

ONTAPのリモートダイレクトメモリアクセス (RDMA) ソリューションは、レイテンシの影響を受けやすい広帯域幅のワークロードをサポートします。RDMAを使用すると、ストレージシステムとホストシステムのメモリ間でデータが直接コピーされるため、CPUの中断やオーバーヘッドを回避できます。

NFS over RDMA

ONTAP 9.10.1 以降では、"[NFS over RDMA](#)"を設定して、サポートされている NVIDIA GPU を搭載したホスト上の GPU アクセラレーションワークロードに NVIDIA GPUDirect Storage を使用できるようにすることができます。



RDMA は SMB プロトコルではサポートされていません。

クラスタ インターコネクト RDMA

クラスタ インターコネクト RDMA は、レイテンシを削減し、フェイルオーバー時間を短縮し、クラスタ内のノード間の通信を高速化します。

ONTAP 9.10.1以降では、X1151AクラスタNICを使用する場合に、特定のハードウェア システムでクラスタ インターコネクトRDMAがサポートされます。ONTAP 9.13.1以降では、X91153A NICでもクラスタ インターコネクトRDMAがサポートされます。各ONTAPリリースでサポートされるシステムについては、表を参照してください。

| システム | サポートされるONTAPバージョン |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <ul style="list-style-type: none"> • AFF A50 • AFF A30 • AFF A20用 • AFF C80用 • AFF C60 • AFF C30 • ASA A50 • ASA A30 • ASA A20 | ONTAP 9.16.1以降 |
| <ul style="list-style-type: none"> • AFF A1K用 • AFF A90 • AFF A70 • ASA A1K • ASA A90 • ASA A70 • FAS90 • FAS70 | ONTAP 9.15.1以降 |
| <ul style="list-style-type: none"> • AFF A900用 • ASA A900 • FAS9500 | ONTAP 9.13.1以降 |
| <ul style="list-style-type: none"> • AFF A400用 • ASA A400 | ONTAP 9.10.1以降 |

適切なストレージシステムがセットアップされていれば、クラスタ インターコネクト RDMA を使用するために追加の構成は必要ありません。

クライアント プロトコル

ONTAPは、NFS、SMB、FC、FCoE、iSCSI、NVMe、S3など、業界標準の主要なクライアント プロトコルをすべてサポートしています。

NFS

NFSは、UNIXおよびLinuxシステム向けの従来のファイル アクセス プロトコルです。クライアントは、次のプロトコルを使用してONTAPボリューム内のファイルにアクセスできます。

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- pNFS

ファイル アクセスは、UNIX形式の権限、NTFS形式の権限、またはその両方の組み合わせを使用して制御できます。

クライアントは、同じファイルにNFSプロトコルとSMBプロトコルの両方を使用してアクセスできます。

SMB

SMBは、Windowsシステム向けの従来のファイル アクセス プロトコルです。クライアントは、SMB 2.0、SMB 2.1、SMB 3.0、およびSMB 3.1.1の各プロトコルを使用してONTAPボリューム内のファイルにアクセスできます。NFSと同様に、複数の形式の権限の組み合わせがサポートされています。

SMB 1.0も使用可能ですが、ONTAP 9.3以降のリリースではデフォルトで無効になっています。

FC

Fibre Channelは、ネットワークを使用した最初のブロック プロトコルです。ブロック プロトコルは、ファイルではなく、仮想ディスク全体をクライアントに提供します。従来のFCプロトコルは専用のFCネットワークとFCスイッチを使用し、クライアント コンピュータにFCネットワーク インターフェイスが必要です。

仮想ディスクはLUNとして表され、1つ以上のLUNがONTAPボリュームに格納されます。FC、FCoE、およびiSCSIの各プロトコルを使用して同じLUNにアクセスできますが、複数のクライアントから同じLUNにアクセスできるのは、クライアントが書き込みの競合を防ぐように設定されたクラスターに属している場合だけです。

FCoE

FCoEは、FCプロトコルと基本的に同じですが、従来のFC転送の代わりにデータセンター クラスのイーサネット ネットワークを使用します。クライアントにはFCoE固有のネットワーク インターフェイスが必要です。

iSCSI

iSCSIは、標準のイーサネット ネットワークで実行できるブロック プロトコルです。ほとんどのクライアント オペレーティング システムには、標準のイーサネット ポートで動作するソフトウェア イニシエータが搭載されています。iSCSIは、特定のアプリケーションにブロック プロトコルが必要な状況で、専用のFCネットワークがない場合に適しています。

NVMe / FCとNVMe / TCP

NVMeは、フラッシュベースのストレージと連携するように設計された最も新しいブロック プロトコルです。スケーラブルなセッションを通じてレイテンシの大幅な低減と並列処理機能の強化を実現できるため、インメモリ データベースや分析など、低レイテンシと高スループットが求められるアプリケーションに適しています。

FCやiSCSIとは異なり、NVMeはLUNを使用しません。代わりに、ONTAPボリュームに格納されるネームスペ

ースを使用します。NVMeネームスペースには、NVMeプロトコルでのみアクセスできます。

S3

ONTAP 9.8以降では、ONTAPクラスタでONTAP Simple Storage Service (S3) サーバを有効にすることで、オブジェクトストレージのデータをS3バケットを使用して提供できます。

ONTAPでは、S3オブジェクトストレージを提供するオンプレミスのユースケース シナリオを2つサポートしています。

- FabricPoolによるローカル クラスタ（ローカル バケット階層）またはリモート クラスタ（クラウド階層）のバケットへの階層化。
- S3クライアント アプリケーションによるローカル クラスタまたはリモート クラスタのバケットへのアクセス。



ONTAP S3は、追加のハードウェアや管理なしに既存のクラスタでS3機能を利用したい場合に最適です。300TBを超える環境では、NetApp StorageGRIDソフトウェアがNetAppのオブジェクトストレージの主力ソリューションであり続けています。"[StorageGRID](#)"の詳細をご覧ください。

ディスクとローカル階層

ディスクとONTAPローカル階層

ローカル層（_アグリゲート_とも呼ばれます）は、ノードによって管理されるディスクの論理コンテナです。ローカル層を使用することで、パフォーマンス要件の異なるワークロードを分離したり、アクセスパターンの異なるデータを階層化したり、規制上の目的でデータを分離したりすることができます。



ONTAP 9.7より前のバージョンでは、System Managerは_ローカル階層_を説明するために_aggregate_という用語を使用します。ONTAPバージョンに関係なく、ONTAP CLIでは_aggregate_という用語が使用されます。

- レイテンシを最小限に抑えながらパフォーマンスを最大限に高めることが求められるビジネス クリティカルなアプリケーションに対しては、SSDのみで構成されるローカル階層を作成できます。
- アクセス パターンが異なるデータを階層化するには、_ハイブリッド ローカル層_を作成し、作業用データセットのハイパフォーマンス キャッシュとしてフラッシュを導入し、アクセス頻度の低いデータには低コストのHDDまたはオブジェクト ストレージを使用します。
 - "[Flash Pool](#)"は SSD と HDD の両方で構成されています。
 - "[FabricPool](#)"は、オブジェクト ストアが接続された、すべて SSD のローカル層で構成されます。
- 規制要件に準拠する目的でアクティブなデータとは別にアーカイブ データを保持する必要がある場合は、大容量HDDのみ、またはハイパフォーマンスHDDと大容量HDDで構成されるローカル階層を使用できます。



Datacenter



Cloud

You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

MetroCluster構成内のローカル層の操作

MetroCluster構成がある場合は、“MetroCluster”ドキュメントに記載されている初期構成とローカル層およびディスク管理のガイドラインの手順に従う必要があります。

関連情報

- ["ローカル階層を管理する"](#)
- ["ディスクの管理"](#)
- ["RAID構成の管理"](#)
- ["Flash Pool階層の管理"](#)
- ["FabricPoolクラウド階層の管理"](#)

ONTAP RAID グループとローカル階層

最新のRAIDテクノロジーは、故障したディスクのデータをスペア ディスク上に再構築することで、ディスク障害から保護します。システムは「パリティ ディスク」上のインデックス情報と残りの正常なディスク上のデータを比較し、失われたデータを再構築します。このプロセスは、ダウンタイムやパフォーマンスの大幅な低下を招くことなく実行されます。

ローカル層は1つ以上の `_RAIDグループ_` で構成されます。ローカル層の `_RAIDタイプ_` によって、RAIDグループ内のパリティ ディスクの数と、RAID構成で保護される同時ディスク障害の数が決まります。

デフォルトのRAIDタイプであるRAID-DP（RAIDダブルパリティ）の場合、RAIDグループごとに2本のパリティ ディスクが必要であり、同時に2本のディスクで障害が発生してもデータ損失から保護されます。RAID-DPの推奨されるRAIDグループ サイズは、HDDの場合は12～20本、SSDの場合は20～28本です。

この推奨範囲内でより多くの本数のRAIDグループを作成すると、パリティ ディスクのオーバーヘッド コスト

を分散させることができます。特に、HDDドライブよりもはるかに信頼性が高いSSDの場合に当てはまります。HDDを使用するローカル階層の場合は、ディスクストレージを最大化する必要性と、大規模なRAIDグループほど再構築に要する時間が長くなるといった相反する要件とのバランスを取る必要があります。

ミラーリングされたローカル層とミラーリングされていないローカル層

ONTAPの `_SyncMirror_` を使用すると、異なるRAIDグループに保存されたコピー、または `_plex_` としてローカル階層データを同期的にミラーリングできます。plexは、RAIDタイプで保護されている以上のディスク障害が発生した場合や、RAIDグループディスクへの接続が失われた場合でも、データ損失を防ぎます。

ローカル層を作成するときに、ローカル層をミラーリングするかミラーされていないアグリゲートにするかを指定できます。

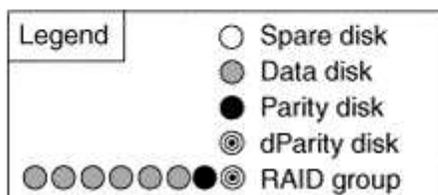
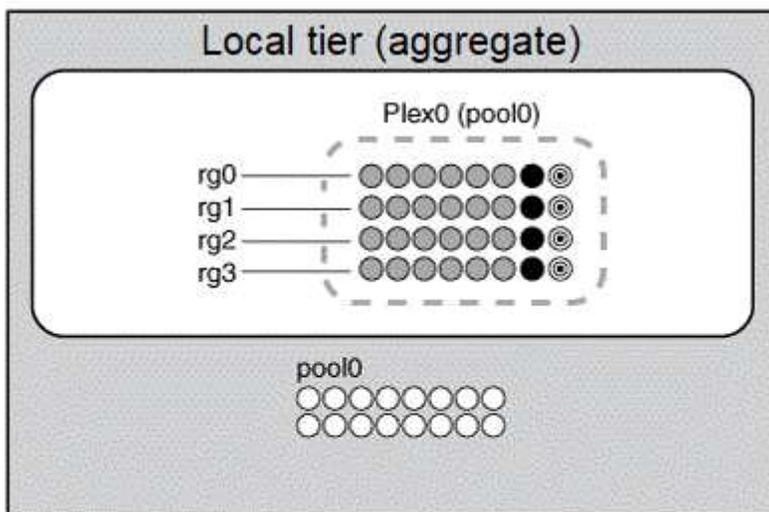


ONTAP 9.7より前のバージョンでは、System Managerは `_ローカル階層_` を説明するために `_aggregate_` という用語を使用しています。ONTAPバージョンに関係なく、ONTAP CLIでは `_aggregate_` という用語が使用されます。ローカル階層の詳細については、"[ディスクとローカル階層](#)"を参照してください。

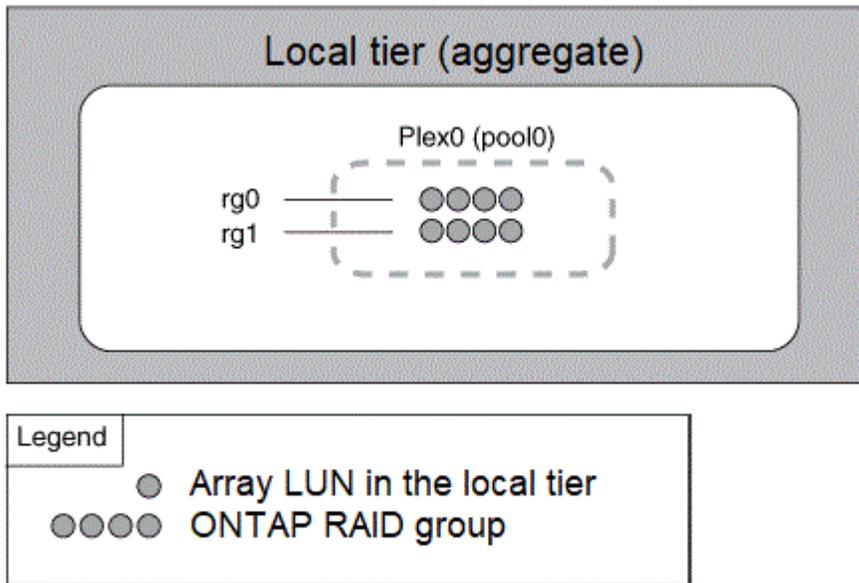
ミラーされていないローカル階層の仕組み

ローカル階層をミラーリングするように指定しない場合、ミラーされていない状態で作成されます。ミラーされていないローカル階層には、そのローカル階層に属するすべてのRAIDグループを含む `_plex_` (データのコピー) が1つだけ存在します。

次の図は、複数のディスクが1つのプレックスにグループ化された、ミラーされていないローカル層を示しています。ローカル層には、`rg0`、`rg1`、`rg2`、`rg3`の4つのRAIDグループがあります。各RAIDグループには、6つのデータディスク、1つのパリティディスク、1つのdparity (ダブルパリティ) ディスクがあります。ローカル層で使用されるすべてのディスクは、同じプール「`pool0`」から取得されます。



次の図は、アレイLUNが1つのプレックスにグループ化された、ミラーされていないローカル層を示しています。この層には2つのRAIDグループ（rg0とrg1）があります。ローカル層で使用されるすべてのアレイLUNは、同じプール「pool0」から取得されます。



ミラーリングされたローカル層の仕組み

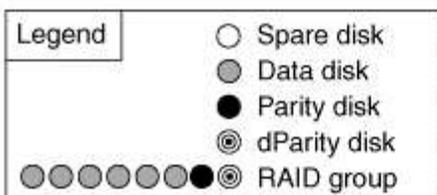
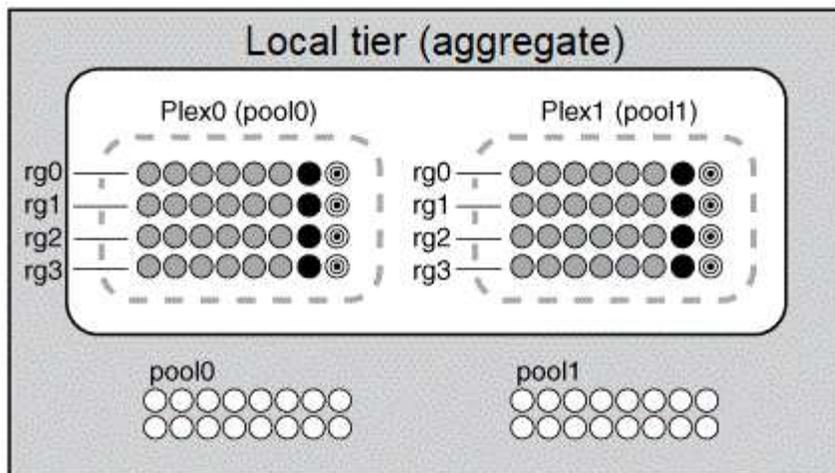
ミラーリングされたローカル層には2つのプレックス（データのコピー）があり、SyncMirror 機能を使用してデータを複製し、冗長性を提供します。

ローカル階層を作成する際に、ミラーリングするように指定できます。また、既存のミラーリングされていないローカル階層に2つ目のプレックスを追加して、ミラーリングされた階層にすることもできます。SyncMirrorを使用すると、ONTAPは元のプレックス（plex0）のデータを新しいプレックス（plex1）にコピーします。プレックスは物理的に分離されており（各プレックスには独自のRAIDグループとプールがあります）、プレックスは同時に更新されます。

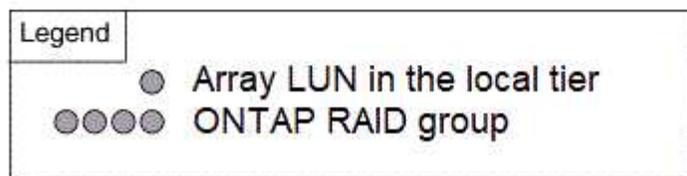
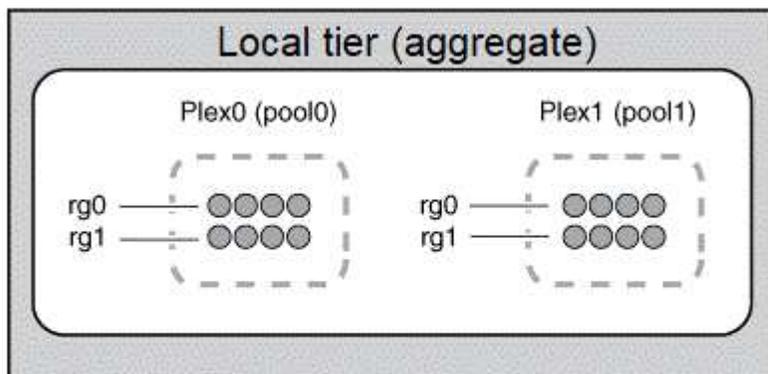
この構成では、ローカル層のRAIDレベルで保護できる以上のディスク障害が発生した場合、または接続が失われた場合でも、障害の原因を修復する間、影響を受けていないプレックスが引き続きデータを提供するため、データ損失に対する保護が強化されます。問題が発生したプレックスが修復されると、2つのプレックスは再同期され、ミラー関係が再確立されます。

システム上のディスクとアレイ LUN は、`pool0`と`pool1`の2つのプールに分割されます。Plex0 は pool0 からストレージを取得し、plex1 は pool1 からストレージを取得します。

次の図は、SyncMirrorが有効化され実装されたディスクで構成されたローカル層を示しています。ローカル層には2つ目のプレックスが作成されています plex1。プレックス1のデータはプレックス0のデータのコピーであり、RAIDグループも同一です。32本のスペアディスクは、プール0またはプール1に割り当てられ、各プールに16本のディスクが割り当てられています。



次の図は、SyncMirror機能が有効化され実装されたアレイLUNで構成されたローカル層を示しています。ローカル層には2つ目のプレックスが作成されています plex1。プレックス1はプレックス0のコピーであり、RAIDグループも同一です。



ストレージのパフォーマンスと可用性を最適化するために、ミラーリングされたアグリゲートには少なくとも20%の空きスペースを確保することをお勧めします。ミラーリングされていないアグリゲートの場合は10%が推奨されていますが、追加の10%のスペースはファイルシステムによって増分変更の吸収に使用される可能性があります。ONTAPのリダイレクトオンライトスナップショットベースのアーキテクチャにより、増分変更はミラーリングされたアグリゲートのスペース使用率を増加させます。これらのベストプラクティスを遵守しないと、パフォーマンスに悪影響を与える可能性があります。

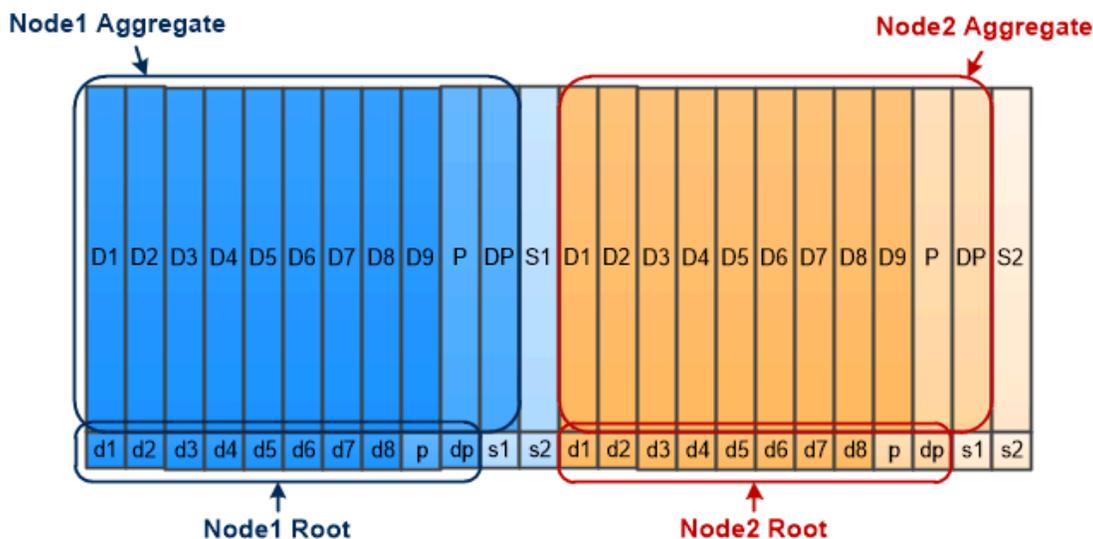
ルート データ パーティショニング

すべてのノードにはストレージ システムの構成ファイル用のルート アグリゲートが必要です。ルート アグリゲートのRAIDタイプは、データ アグリゲートのRAIDタイプと同じです。

System Managerでは、ルート / データ パーティショニングまたはルート / データ / データ パーティショニングがサポートされていません。

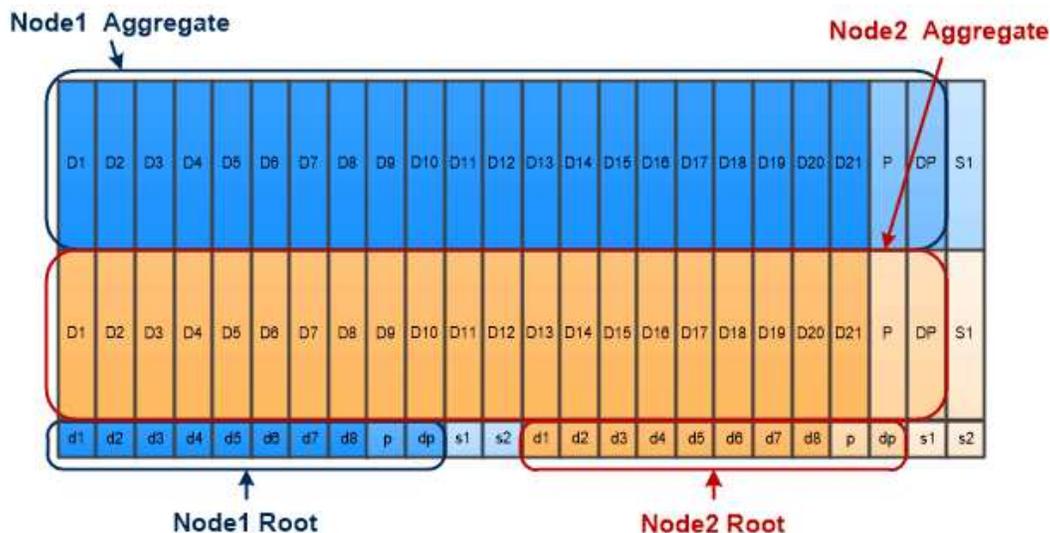
RAID-DPタイプのルート アグリゲートは、通常、1つのデータ ディスクと2つのパリティ ディスクで構成されます。システムが既にアグリゲート内の各RAIDグループに2つのディスクをパリティ ディスクとして確保している場合、これはストレージ システム ファイルに対して支払うべき大きな「パリティ税」となります。

「ルートデータパーティショニング」は、ルート アグリゲートをディスク パーティション全体に分散し、各ディスク上の1つの小さなパーティションをルートパーティションとして予約し、1つの大きなパーティションをデータ用に予約することで、パリティ タックスを削減します。



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

図からわかるように、ルート アグリゲートの保存に使用されるディスクの数が増えるほど、ルートパーティションは小さくなります。これは、ルート データ パーティショニングの一種である「ルート データ データパーティショニング」にも当てはまります。このパーティショニングでは、ルートパーティションとして小さなパーティションを1つ作成し、データ用に同じサイズの大きなパーティションを2つ作成します。



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

どちらのタイプのルートデータ・パーティショニングも、ONTAP Advanced Drive Partitioning (ADP) 機能の一部です。どちらも工場出荷時に構成されています。エントリレベルの FAS2xxx、FAS9000、FAS8200、FAS80xx、および AFF システムではルートデータ・パーティショニング、AFF システムのみではルートデータ・データ・パーティショニングが設定されます。

"アドバンスド ドライブ パーティショニング"についての詳細をご覧ください。

ルート アグリゲート用にパーティショニングされるドライブ

どのドライブがルート アグリゲートで使用するためにパーティショニングされるかは、システム構成によって異なります。

ルート アグリゲートに使用されるドライブ数を把握しておく、と、ルート パーティション用にリザーブされるドライブの容量とデータ アグリゲートで使用可能な容量を判断するのに役立ちます。

ルートデータのパーティショニング機能は、エントリレベルのプラットフォーム、All-Flash FASプラットフォーム、SSDのみが接続されたFASプラットフォームでサポートされます。

エントリレベルのプラットフォームでは、内蔵ドライブのみがパーティショニングされます。

All Flash FASプラットフォームおよびSSDのみが接続されたFASプラットフォームでは、システム初期化時にコントローラに接続されたすべてのドライブがパーティショニングされます（上限はノードあたり24個です）。システムの構成後に追加されたドライブはパーティショニングされません。

ボリューム、qtree、ファイル、LUN

ONTAP は、FlexVol ボリュームと呼ばれる論理コンテナからクライアントとホストにデータを提供します。これらのボリュームはそれを含むアグリゲートと緩く結合されているため、従来のボリュームよりもデータ管理の柔軟性が高くなります。

複数のFlexVolボリュームをアグリゲートに割り当てることができ、それぞれを異なるアプリケーションまたはサービス専用にすることができます。FlexVolボリュームの拡張や縮小、FlexVolボリュームの移動、FlexVol

ボリュームの効率的なコピーの作成が可能です。_qtree_を使用してFlexVolボリュームをより管理しやすい単位に分割したり、_quota_を使用してボリュームのリソース使用量を制限したりすることができます。

ボリュームには、NAS環境ではファイルシステム、SAN環境ではLUNが含まれます。LUN（論理ユニット番号）は、SANプロトコルによってアドレス指定される「論理ユニット」と呼ばれるデバイスの識別子です。

LUNは、SAN構成におけるストレージの基本単位です。Windowsホストは、ストレージシステム上のLUNを仮想ディスクとして認識します。LUNは、必要に応じて無停止で別のボリュームに移動できます。

データ ボリュームのほかに、いくつかの特別なボリュームについて覚えておく必要があります。

- ノード ルート ボリューム（通常は「vol10」）には、ノードの構成情報とログが含まれています。
- SVM ルート ボリューム は、SVM によって提供される名前空間へのエントリ ポイントとして機能し、名前空間のディレクトリ情報を含みます。
- システム ボリューム には、サービス監査ログなどの特別なメタデータが含まれます。

これらのボリュームはデータの格納には使用できません。



Volumes contain files in a NAS environment and LUNs in a SAN environment.

FlexGroup volume

企業によっては、FlexVolの100TBの容量をもはるかに超えるペタバイト規模のストレージが単一のネームスペースで必要になることがあります。

FlexGroup volume は、200 個の構成メンバー ボリュームで最大 4000 億個のファイルをサポートします。これらのボリュームは連携して動作し、すべてのメンバー間で負荷とスペースの割り当てを動的に均等に分散します。

FlexGroupボリュームではメンテナンスや管理の手間も必要ありません。単にFlexGroupボリュームを作成してNASクライアントと共有するだけで、面倒な処理はONTAPが行います。

ストレージ仮想化

ストレージ仮想化 - 概要

クライアントとホストにデータを提供するには、**_ストレージ仮想マシン (SVM) _**を使用します。ハイパーバイザー上で実行される仮想マシンと同様に、SVMは物理リソースを抽象化する論理エンティティです。SVMを介してアクセスされるデータは、ストレージ内の特定の場所にバインドされません。SVMへのネットワーク アクセスは、物理ポートにバインドされません。



SVMは、以前は「Vserver」と呼ばれていました。ONTAPのコマンドライン インターフェイスでは、引き続き「vserver」という用語が使用されます。

SVMは、1つ以上のボリュームから、1つ以上のネットワーク_論理インターフェイス (LIF) _を介してクライアントとホストにデータを提供します。ボリュームはクラスタ内の任意のデータ アグリゲートに割り当てることができます。LIFは任意の物理ポートまたは論理ポートでホストできます。ボリュームとLIFはどちらも、ハードウェアのアップグレード、ノードの追加、パフォーマンスのバランス調整、アグリゲート間の容量の最適化など、データ サービスを中断することなく移動できます。

1つのSVMにNASトラフィック用のLIFとSANトラフィック用のLIFを設定することができます。クライアントやホストからSVMにアクセスするために必要なのは、LIFのアドレス (NFS、SMB、iSCSIの場合はIPアドレス、FCの場合はWWPN) だけです。LIFのアドレスは移動しても変わりません。ポートは複数のLIFをホストできます。SVMにはそれぞれ固有のセキュリティ、管理、およびネームスペースがあります。

ONTAPでは、データSVMに加え、管理用の特別なSVMを使用します。

- クラスタがセットアップされると、**_admin SVM_**が作成されます。
- ノードが新しいクラスタまたは既存のクラスタに参加すると、**ノード SVM**が作成されます。
- IPspace 内のクラスタレベルの通信用に、**システム SVM**が自動的に作成されます。

これらのSVMはデータの提供には使用できません。さらに、クラスタ内およびクラスタ間のトラフィック用のLIFや、クラスタおよびノードの管理用のLIFなど、特別なLIFがあります。

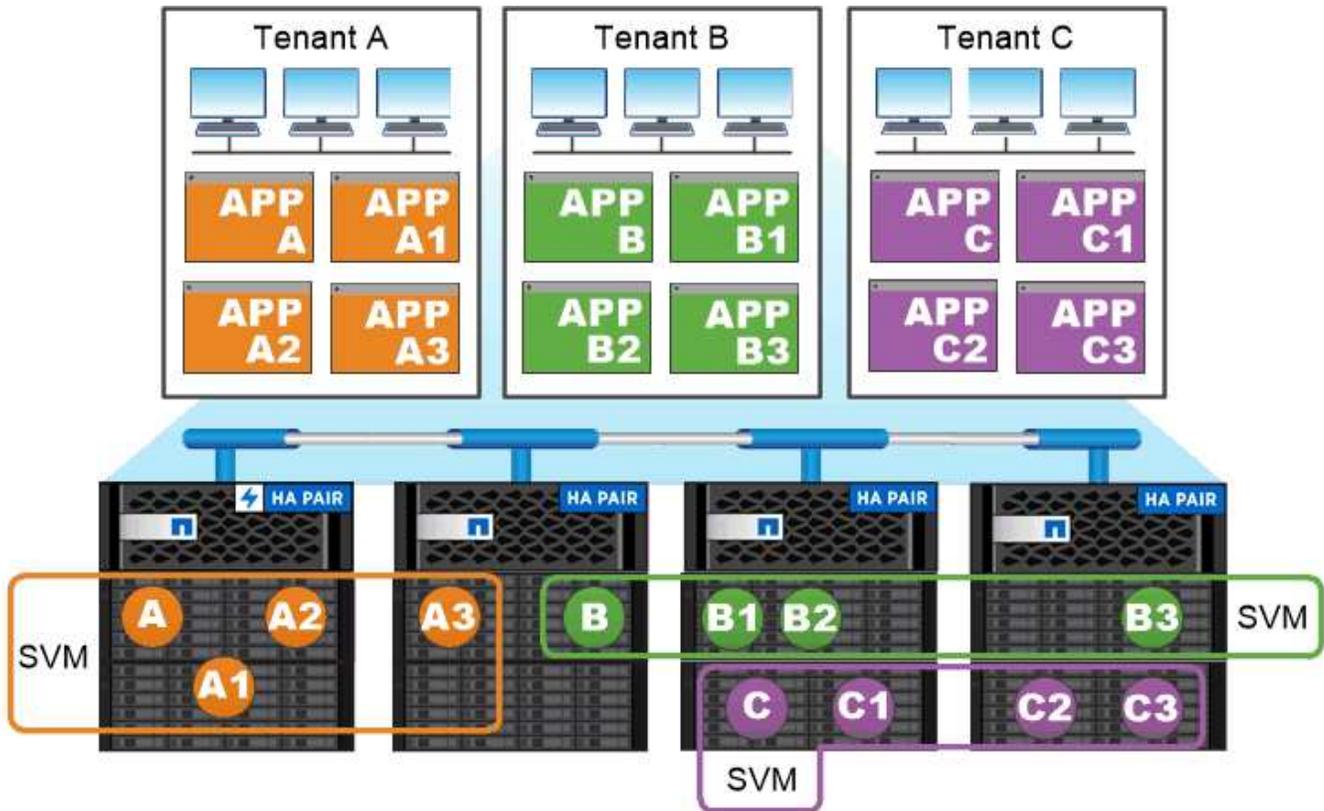
ONTAPがミドルウェアにたとえられる理由

ONTAPでストレージ管理タスクに使用される論理オブジェクトは、適切に設計されたミドルウェア パッケージが従来担っていた役割を果たし、管理者を細かな実装作業から解放し、ノードやポートなどの物理要素の変更が設定に影響しないようにします。管理者がストレージ インフラ全体ではなく一部を再設定するだけで、ボリュームやLIFを簡単に移動できるようにすることが、基本的な目的です。

SVMのユースケース

サービス プロバイダは、セキュアなマルチテナンシー構成でSVMを使用して、各テナントのデータを分離し、各テナントに独自の認証と管理を提供し、チャージバックを簡素化します。同じSVMに複数のLIFを割り当てて、さまざまな顧客ニーズに対応できます。また、QoSを使用して、テナントのワークロードが他のテナントのワークロードを「圧迫」するのを防ぐことができます。

企業の管理者も同じような目的にSVMを使用できます。たとえば、データを部門別に分離したり、ホストがアクセスするストレージボリュームとユーザの共有ボリュームを別々のSVMに分けたりできます。iSCSI / FC LUNおよびNFSデータストアとSMB共有とでSVMを分ける管理者もいます。



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

クラスタとSVMの管理

_クラスタ管理者_は、クラスタの管理SVMにアクセスします。管理SVMと予約名`admin`を持つクラスタ管理者は、クラスタのセットアップ時に自動的に作成されます。

デフォルトの`admin`ロールを持つクラスタ管理者は、クラスタ全体とそのリソースを管理できます。クラスタ管理者は、必要に応じて、異なるロールを持つ追加のクラスタ管理者を作成できます。

_SVM管理者_はデータSVMにアクセスします。クラスタ管理者は必要に応じてデータSVMとSVM管理者を作成します。

SVM管理者には、デフォルトで`vsadmin`ロールが割り当てられます。クラスタ管理者は、必要に応じてSVM管理者に異なるロールを割り当てることができます。

ロールベースのアクセス制御 (RBAC)

管理者に割り当てられた_ロール_によって、管理者がアクセスできるコマンドが決まります。このロールは、管理者のアカウントを作成する際に割り当てます。必要に応じて、別のロールを割り当てたり、カスタムロールを定義したりすることもできます。

ネームスペースとジャンクションポイント

NAS ネームスペースとは、ジャンクションポイントで結合されたボリュームの論理的なグループであり、単一のファイルシステム階層を形成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定することなく、ネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームは、クラスタ内の任意の場所に配置できます。

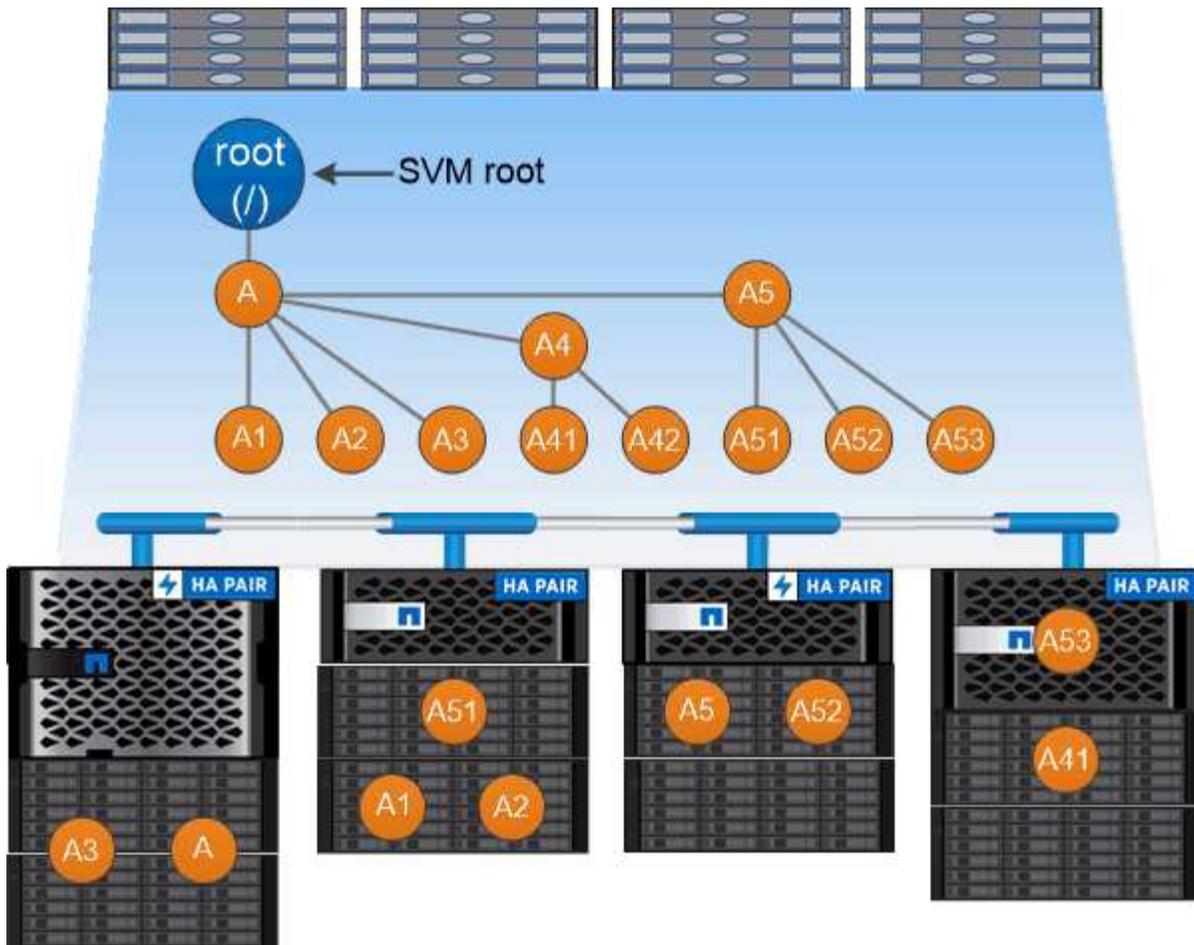
NASクライアントは、対象となるファイルを含むすべてのボリュームをマウントするのではなく、NFSエクスポートをマウントするか、SMB共有にアクセスします。エクスポートまたは共有は、名前空間全体、または名前空間内の中間位置を表します。クライアントは、アクセスポイントの下にマウントされたボリュームのみにアクセスします。

必要に応じて、名前空間にボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションの直下、またはボリューム内のディレクトリに作成できます。「vol3」という名前のボリュームのボリュームジャンクションへのパスは /vol1/vol2/vol3、 /vol1/dir2/vol3、あるいは `dir1/dir2/vol3` などです。このパスは_ジャンクションパス_と呼ばれます。

すべてのSVMには、それぞれ一意のネームスペースがあります。SVMルートボリュームは、ネームスペース階層のエントリポイントです。



ノードの停止やフェイルオーバーが発生した場合でもデータが利用可能であることを保証するには、SVMルートボリュームの_負荷共有ミラー_コピーを作成する必要があります。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

例

次の例では、ジャンクションパスを持つ SVM vs1 上に「home4」という名前のボリュームを作成します
/eng/home :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

パスのフェイルオーバー

パスのフェイルオーバー - 概要

ONTAP が NAS トポロジと SAN トポロジでパス フェイルオーバーを管理する方法には重要な違いがあります。NAS LIF はリンク障害発生後に自動的に別のネットワークポートに移行します。SAN LIF は（障害発生後に手動で移動しない限り）移行しません。代わりに、ホスト上のマルチパス テクノロジによってトラフィックが同じ SVM 上の別の

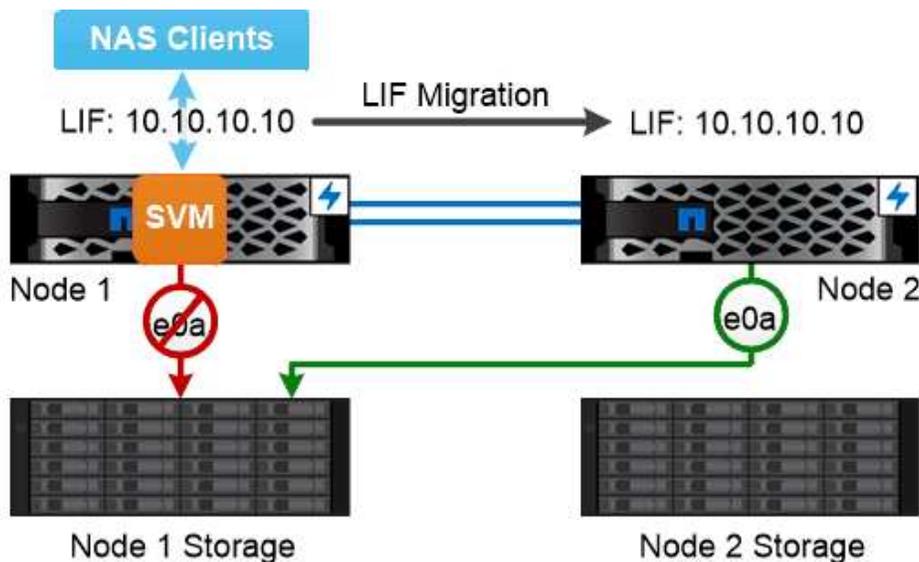
LIF に転送されますが、その LIF は別のネットワーク ポートにアクセスします。

NASパスのフェイルオーバー

NAS LIFは、現在のポートでリンク障害が発生すると、正常に動作しているネットワーク ポートに自動的に移行します。LIFの移行先ポートは、LIFの_フェイルオーバー グループ_のメンバーである必要があります。_フェイルオーバー グループ ポリシー_により、データLIFのフェイルオーバー先は、データを所有するノードとそのHAパートナーのポートに絞り込まれます。

管理の利便性のため、ONTAPはネットワーク アーキテクチャ内の各_ブロードキャスト ドメイン_に対してフェイルオーバー グループを作成します。ブロードキャスト ドメインは、同じレイヤ2ネットワークに属するポートをグループ化します。例えば、VLANを使用してトラフィックを部門（エンジニアリング、マーケティング、財務など）ごとに分離している場合、各VLANは個別のブロードキャスト ドメインを定義します。ブロードキャスト ドメインに関連付けられたフェイルオーバー グループは、ブロードキャスト ドメイン ポートを追加または削除するたびに自動的に更新されます。

フェイルオーバー グループを常に最新の状態に保つために、ブロードキャスト ドメインを使用してフェイルオーバー グループを定義することは、ほとんどの場合に推奨されます。ただし、場合によっては、ブロードキャスト ドメインに関連付けられていないフェイルオーバー グループを定義したい場合があります。たとえば、ブロードキャスト ドメインで定義されたポートのサブセット内のポートにのみLIFをフェイルオーバーさせたい場合などです。



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

サブネット

_サブネット_は、ブロードキャスト ドメイン内のIPアドレスのブロックを予約します。これらのアドレスは同じレイヤ3ネットワークに属し、LIFの作成時にブロードキャスト ドメイン内のポートに割り当てられます。通常、LIFアドレスを定義する際にIPアドレスとネットワーク マスクを指定するよりも、サブネット名を指定する方が簡単でエラーも少なくなります。

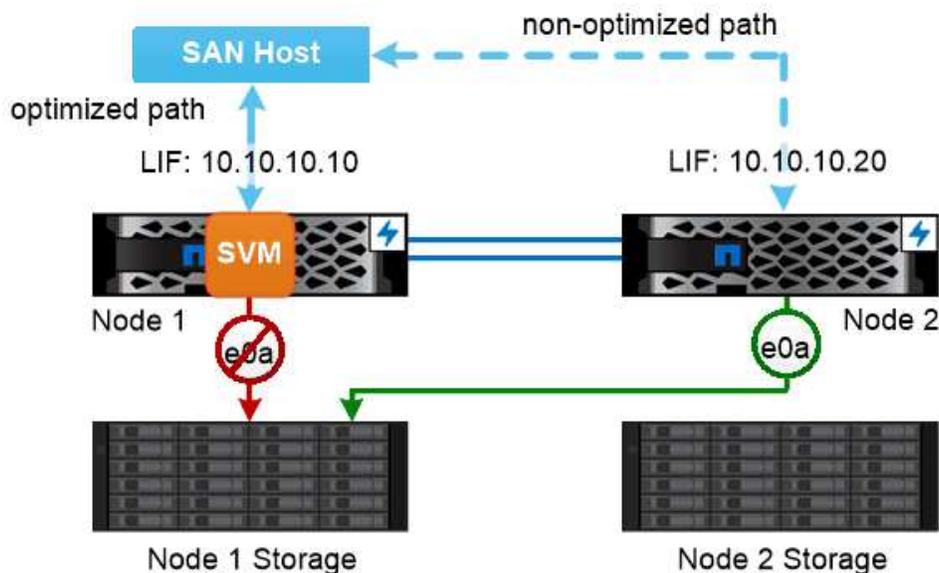
SANパスのフェイルオーバー

リンク障害が発生すると、SANホストはALUA（非対称論理ユニット アクセス）とMPIO（マルチパスI/O）を使用してトラフィックを稼働しているLIFに再ルーティングします。SVMが提供するLUNへの使用可能なルートは、事前に定義されたパスで決まります。

SAN環境では、ホストはLUN_ターゲット_へのリクエストの_イニシエーター_として扱われます。MPIOは、イニシエーターからターゲットへの複数のパスを可能にします。ALUAは、_最適化されたパス_と呼ばれる最も直接的なパスを識別します。

通常は、LUNの所有者ノード上のLIFへの最適パスと、HAパートナー上のLIFへの最適化されていないパスを、それぞれ複数構成します。所有者ノードの1つのポートで障害が発生すると、稼働しているポートにトラフィックがルーティングされます。すべてのポートで障害が発生した場合は、最適化されていないパスを介してトラフィックがルーティングされます。

ONTAP Selective LUN Map (SLM) は、デフォルトでホストからLUNへのパス数を制限します。新規に作成されたLUNには、LUNを所有するノードまたはそのHAパートナーへのパスを通じてのみアクセスできます。また、イニシエータの_ポート セット_にLIFを設定することで、LUNへのアクセスを制限することもできます。



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

SAN環境でのボリュームの移動

デフォルトでは、ONTAP Selective LUN Map (SLM) は、SANホストからLUNへのパス数を制限します。新しく作成されたLUNには、LUNを所有するノード、またはそのHAパートナー（LUNの_レポートノード）へのパスを通じてのみアクセスできます。

そのため、ボリュームを別のHAペアのノードに移動した場合、移動先のHAペアのレポートノードをLUNマッピングに追加する必要があります。その後、MPIOに新しいパスを指定します。ボリュームの移動が完了したら、元のHAペアのレポートノードはマッピングから削除できます。

ONTAPのロード バランシング

ノードでの作業量が利用可能なリソースを超えると、ワークロードのパフォーマンスにレイテンシが発生し始めます。ノードの負荷が許容量を超えた場合は、利用可能なリソースを増やす（ディスクやCPUをアップグレードする）か、負荷を減らす（ボリュームやLUNを必要に応じて別のノードに移動する）ことで対処します。

また、ONTAP ストレージ サービス品質（QoS） を使用して、競合するワークロードによって重要なワークロードのパフォーマンスが低下しないようにすることもできます：

- 競合するワークロードに QoS スループットの上限を設定して、システム リソースへの影響を制限できます（QoS Max）。
- 重要なワークロードに対して QoS スループットの下限を設定し、競合するワークロードの需要に関係なく、最小スループット目標を満たすようにすることができます（QoS Min）。
- 同じワークロードに対してQoSの上限と下限を設定することができます。

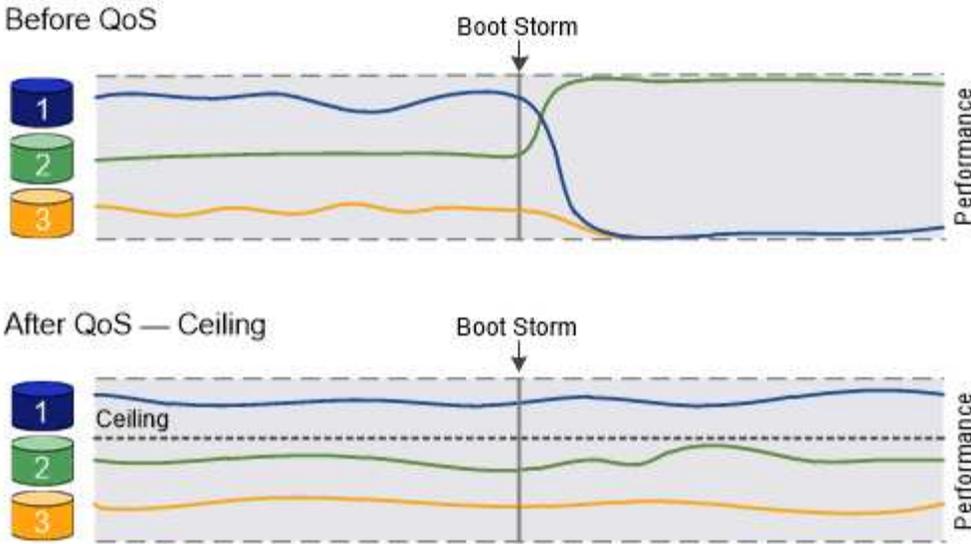
スループットの上限

スループット上限は、ワークロードのスループットを最大IOPS数またはMB/秒に制限します。下の図では、ワークロード2のスループット上限によって、ワークロード1と3が「圧迫」されることのないようになっています。

ポリシー グループ_は、1つ以上のワークロードのスループット上限を定義します。ワークロードは、_ストレージ オブジェクト（ボリューム、ファイル、LUN、またはSVM内のすべてのボリューム、ファイル、LUN）に対するI/O処理を表します。上限は、ポリシー グループの作成時に指定することも、ワークロードを監視してから指定することもできます。



ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を10%までは超過することができます。バースト時には、上限を50%まで超過することができます。



The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

スループットの下限

スループットの下限はワークロードのスループットが最小IOPSを下回らないことを保証します。次の図では、ワークロード1とワークロード3にスループットの下限が設定され、ワークロード2からの要求量に関係なく、最小スループットが確保されています。

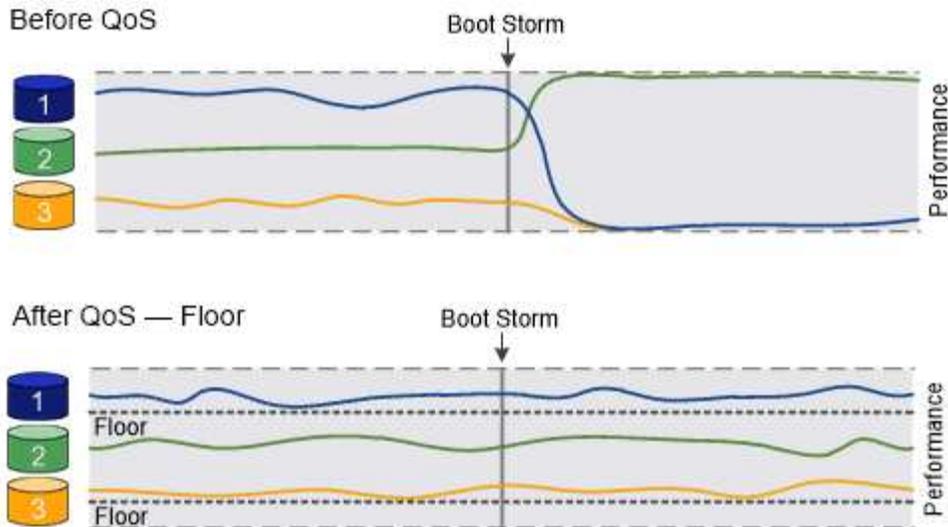


これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

ワークロードは、ボリューム、LUN、またはファイル（ONTAP 9.3以降）のI/O処理を表します。スループットの下限を定義するポリシーグループは、SVMには適用できません。下限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。



ノードまたはアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合、または`volume move trigger-cutover`などの重要な操作が実行されている場合、ワークロードへのスループットが指定された下限値を下回ることがあります。十分な容量があり、重要な操作が実行されていない場合でも、ワークロードへのスループットは指定された下限値を最大5%下回ることがあります。



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

アダプティブQoS

通常、ストレージ オブジェクトに割り当てたポリシー グループの値は固定値です。ストレージ オブジェクトのサイズが変わったときは、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

Adaptive QoS は、ワークロードのサイズが変化しても IOPS と TB/GB の比率を維持しながら、ポリシー グループの値を自動的にワークロードのサイズに合わせて調整します。これは、大規模な導入環境で数百、数千のワークロードを管理する際に大きなメリットとなります。

アダプティブQoSは、主にスループットの上限の調整に使用しますが、下限の管理（ワークロード サイズが増えた場合）に使用することもできます。ワークロードのサイズは、ストレージ オブジェクトに割り当てられたスペースまたはストレージ オブジェクトで使用されているスペースのいずれかで表されます。



使用済みスペースは ONTAP 9.5 以降ではスループット フロアに使用できます。ONTAP 9.4 以前では、スループット フロアにはサポートされていません。

+ ONTAP 9.13.1 以降では、アダプティブ QoS を使用して、SVM レベルでスループットの下限と上限を設定できます。

- **割り当て領域 ポリシー**は、ストレージ オブジェクトの公称サイズに応じてIOPS/TB|GB比を維持します。比が100 IOPS/GBの場合、150GBのボリュームのスループット上限は、ボリュームがそのサイズを維持する限り15,000 IOPSになります。ボリュームのサイズが300GBに変更されると、アダプティブQoSによってスループット上限が30,000 IOPSに調整されます。
- **使用済みスペース ポリシー**（デフォルト）は、ストレージ効率化前の実際のデータ保存量に応じてIOPS/TB|GB比率を維持します。比率が100 IOPS/GBの場合、150 GBのボリュームに100 GBのデータを保存した場合、スループット上限は10,000 IOPSになります。使用済みスペースの量が変化すると、アダプティブQoSは比率に応じてスループット上限を調整します。

レプリケーション

Snapshot 数

従来、ONTAPレプリケーション技術は、ディザスタリカバリ（DR）とデータ アーカイブのニーズに対応していました。クラウドサービスの登場により、ONTAPレプリケーションはNetAppデータファブリック内のエンドポイント間のデータ転送に適応されるようになりました。これらすべての用途の基盤となるのがONTAPスナップショット技術です。

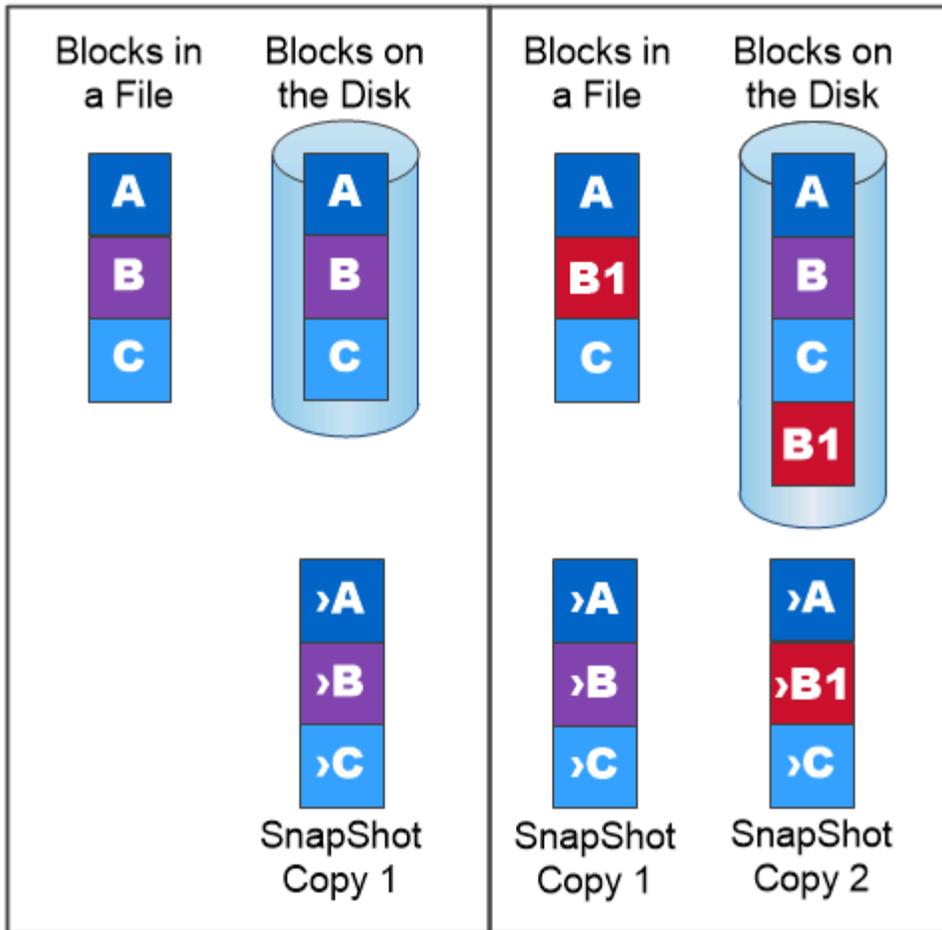
スナップショット（旧称_Snapshot copy_）は、ボリュームの読み取り専用のポイントインタイムイメージです。スナップショットの作成後、アクティブ ファイル システムとスナップショットは同じディスク ブロックを参照するため、スナップショットは余分なディスク容量を使用しません。時間の経過とともに、最後のスナップショット作成以降のファイルの変更のみを記録するため、イメージが消費するストレージ容量は最小限に抑えられ、パフォーマンス オーバーヘッドもごくわずかです。

スナップショットの効率性は、ONTAPの中核となるストレージ仮想化テクノロジーである_Write Anywhere File Layout (WAFL)_によって実現されています。データベースと同様に、WAFLはメタデータを使用してディスク上の実際のデータブロックを参照します。ただし、データベースとは異なり、WAFLは既存のブロックを上書きしません。更新されたデータは新しいブロックに書き込まれ、メタデータが変更されます。

スナップショットは、データ ブロックをコピーするのではなく、ONTAPがスナップショットを作成する際にメタデータを参照するため、効率的です。これにより、他のシステムがコピーするブロックを見つけるために発生する「シーク時間」と、コピー自体の作成コストの両方が削減されます。

スナップショットを使用すると、個々のファイルまたはLUNをリカバリしたり、ボリュームの内容全体を復元したりできます。ONTAPは、スナップショット内のポインタ情報とディスク上のデータを比較し、ダウンタイムや大幅なパフォーマンス オーバーヘッドを発生させることなく、失われたオブジェクトや破損したオブジェクトを再構築します。

_スナップショット ポリシー_は、システムがボリュームのスナップショットを作成する方法を定義します。このポリシーは、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、レプリケーション用のラベル付け方法を指定します。例えば、システムは毎日午前0：10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、それらの名前に「daily」（タイムスタンプを付加）を付け、レプリケーション用のラベルを「daily」と付けることができます。



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

SnapMirrorによるディザスタ リカバリとデータ転送

SnapMirror は、地理的に離れたサイトにあるプライマリ ストレージからセカンダリ システムへのフェイルオーバーを目的とした災害復旧テクノロジーです。その名の通り、SnapMirrorはセカンダリ ストレージに作業データのレプリカ（ミラー）を作成します。プライマリ サイトで災害が発生した場合でも、このミラーから引き続きデータを提供できます。

データはボリューム レベルでミラーリングされます。プライマリ ストレージのソース 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 ボリュームの関係は、_データ保護関係_と呼ばれます。ボリュームが存在するクラスタと、ボリュームからデータを提供するSVMは、_ピアリング_されている必要があります。ピア関係により、クラスタとSVMは安全にデータを交換できます。



SVM間にもデータ保護関係を作成できます。このタイプの関係では、SVMのすべてまたは一部の設定がNFSエクスポートおよびSMB共有からRBACにレプリケートされます。また、SVMが所有するボリューム内のデータもレプリケートされます。

ONTAP 9.10.1以降では、SnapMirror S3を使用してS3バケット間にデータ保護関係を作成できます。デスティネーション バケットは、ローカルまたはリモートのONTAPシステム、あるいはStorageGRIDやAWSなど

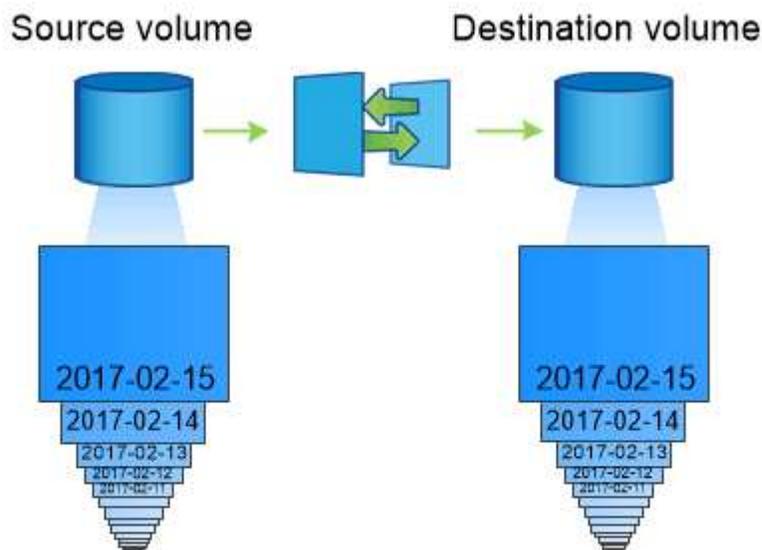
のONTAP以外のシステムに配置できます。

SnapMirrorを初めて起動すると、ソースボリュームからデスティネーションボリュームへの_ベースライン転送_が実行されます。ベースライン転送には通常、以下の手順が含まれます：

- ソースボリュームのスナップショットを作成します。
- スナップショットとそれが参照するすべてのデータ ブロックを宛先ボリュームに転送します。
- 「active」ミラーが破損した場合に備えて、ソース ボリュームに残っている、それほど新しくないスナップショットを宛先ボリュームに転送します。

ベースライン転送が完了すると、SnapMirrorは新しいスナップショットのみをミラーに転送します。更新は非同期で、設定されたスケジュールに従って行われます。保持ポリシーは、ソース上のスナップショット ポリシーをミラーリングします。プライマリ サイトで災害が発生した場合、最小限の中断でデスティネーション ボリュームをアクティブ化し、サービスが復旧したらソース ボリュームを再アクティブ化できます。

SnapMirrorはベースライン作成後はスナップショットのみを転送するため、レプリケーションは高速かつ無停止で実行されます。フェイルオーバーのユースケースからもわかるように、ミラーリングされたストレージから効率的にデータを提供するには、セカンダリ システムのコントローラはプライマリ システムのコントローラと同等、またはほぼ同等である必要があります。



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

SnapMirrorを使用したデータ転送

SnapMirrorを使用して、NetAppデータファブリック内のエンドポイント間でデータを複製することもできます。SnapMirrorポリシーの作成時に、1回限りのレプリケーションと定期的なレプリケーションのどちらかを選択できます。

オブジェクト ストレージへの**SnapMirror**クラウドのバックアップ

_SnapMirror cloud_は、データ保護ワークフローをクラウドに移行したいONTAPユーザ

一向けに設計されたバックアップおよびリカバリ テクノロジーです。従来のテープへのバックアップ アーキテクチャから移行する組織は、オブジェクト ストレージを長期的なデータ保持とアーカイブのための代替リポジトリとして使用できます。SnapMirror cloudは、永久増分バックアップ戦略の一環として、ONTAPからオブジェクト ストレージへのレプリケーションを提供します。

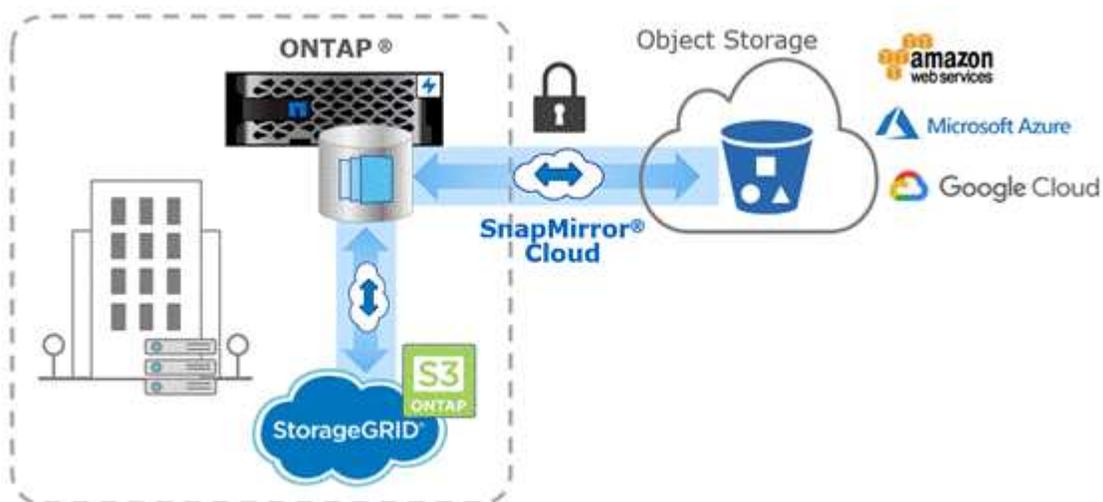
SnapMirror クラウドレプリケーションは、ライセンスが必要なONTAPの機能です。SnapMirror クラウドは、SnapMirror レプリケーションテクノロジーのファミリーを拡張するものとして、ONTAP 9.8で導入されました。SnapMirror はONTAP間のバックアップによく使用されますが、SnapMirror クラウドは同じレプリケーションエンジンを利用して、ONTAPからS3準拠のオブジェクトストレージへのバックアップ用スナップショットを転送します。

バックアップのユースケースを対象としたSnapMirrorクラウドは、長期保存とアーカイブのワークフローの両方をサポートします。SnapMirrorと同様に、最初のSnapMirrorクラウド バックアップでは、ボリュームのベースライン転送を実行します。その後のバックアップでは、SnapMirrorクラウドはソース ボリュームのスナップショットを生成し、変更されたデータ ブロックのみを含むスナップショットをオブジェクト ストレージターゲットに転送します。

SnapMirrorクラウドでは、ONTAPシステムから一部のオンプレミスおよびパブリック クラウドのオブジェクト ストレージ ターゲット（Amazon S3、Google Cloud Storage、Microsoft Azure Blob Storage） への関係を設定できます。オンプレミスのオブジェクト ストレージ ターゲットとしては、StorageGRIDとONTAP S3も対象となります。

ONTAP System Managerを使用してSnapMirrorクラウド構成を管理するだけでなく、SnapMirrorクラウド バックアップを管理するためのいくつかのオーケストレーション オプションも利用できます：

- SnapMirrorクラウドレプリケーションのサポートを提供する複数のサードパーティ製バックアップパートナー。参加ベンダーは["NetAppブログ"](#)でご確認いただけます。
- NetApp Backup and Recovery：ONTAP環境向けのNetAppネイティブソリューション
- API：データ保護ワークフロー用のカスタム ソフトウェアを開発する場合、または自動化ツールを活用する場合。



SnapVaultアーカイブ

SnapMirrorライセンスは、バックアップ用のSnapVault関係とディザスタリカバリ用

のSnapMirror関係の両方をサポートするために使用されます。ONTAP 9.3以降、SnapVaultライセンスは廃止され、SnapMirrorライセンスを使用してヴォールト、ミラー、およびミラーとヴォールトの関係を設定できます。SnapMirrorレプリケーションは、スナップショットのONTAP間レプリケーションに使用され、バックアップとディザスタリカバリの両方のユースケースをサポートします。

SnapVault はアーカイブ テクノロジーで、標準規格への準拠やその他のガバナンス関連の目的のために、ディスク間のスナップショット レプリケーション用に設計されています。SnapMirror関係では、通常、ソースボリュームに現在存在するスナップショットのみがデスティネーションに含まれますが、それとは対照的に、SnapVaultデスティネーションは通常、はるかに長い期間にわたって作成されたポイントインタイム スナップショットを保持します。

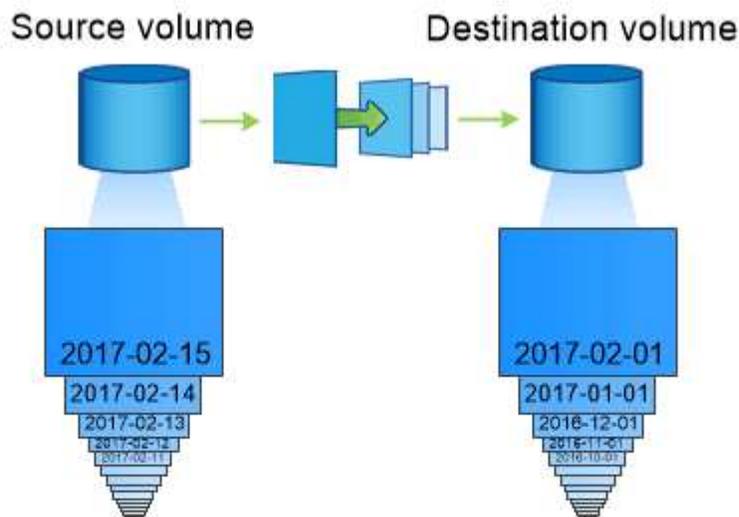
例えば、政府の会計規制を遵守するために、20年間にわたって毎月のデータのスナップショットを保持したい場合があります。Vaultストレージからデータを提供する必要がないため、移行先システムでは低速で安価なディスクを使用できます。

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。ソースボリュームのスナップショットを作成し、そのコピーとそれが参照するデータブロックを宛先ボリュームに転送します。SnapMirrorとは異なり、SnapVaultは古いスナップショットをベースラインに含みません。

更新は非同期で、設定したスケジュールに従って行われます。関係の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と保持するコピー数が決まります。ポリシーで定義されたラベル（例：「monthly」）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している必要があります。一致しない場合、レプリケーションは失敗します。



SnapMirrorとSnapVaultは同じコマンド インフラを共有します。どちらを使用するかはポリシーの作成時に指定します。どちらの方法にもピア クラスタとピアSVMが必要です。



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

クラウド バックアップと従来のバックアップのサポート

SnapMirrorおよびSnapVaultによるデータ保護関係（ONTAP 9.7以前はディスクツーディスクのみ）に加え、現在は低コストで長期的なデータ保持が可能な複数のバックアップソリューションがあります。

ONTAPで管理されているデータ向けに従来のバックアップを提供する他社製データ保護アプリケーションは数多くあります。たとえばVeeam、Veritas、CommvaultなどがONTAPシステム向けの統合バックアップ機能を提供しています。

ONTAP 9.8以降、SnapMirrorクラウドはONTAPインスタンスからオブジェクトストレージエンドポイントへのスナップショットの非同期レプリケーションを提供します。SnapMirrorクラウドレプリケーションには、データ保護ワークフローのオーケストレーションと管理のためのライセンスアプリケーションが必要です。SnapMirrorクラウド関係は、ONTAPシステムから選択したオンプレミスおよびパブリッククラウドのオブジェクトストレージターゲット（AWS S3、Google Cloud Storage Platform、Microsoft Azure Blob Storage など）へサポートされ、ベンダーのバックアップソフトウェアによる効率性の向上を実現します。サポートされている認定アプリケーションとオブジェクトストレージベンダーのリストについては、NetApp担当者にお問い合わせください。

クラウドネイティブのデータ保護に関心がある場合は、NetApp コンソールを使用して、オンプレミス ボリュームとパブリック クラウド内の Cloud Volumes ONTAP インスタンス間のSnapMirrorまたはSnapVault関係を設定できます。

コンソールは、Software as a Service (SaaS) モデルを使用してCloud Volumes ONTAPインスタンスのバックアップも提供します。ユーザーは、NetApp Backup and Recoveryを使用して、Cloud Volumes ONTAPインスタンスをS3およびS3準拠のパブリック クラウド オブジェクト ストレージにバックアップできます。

["Cloud Volumes ONTAPのドキュメント"](#)

["NetApp Console のドキュメント"](#)

["NetApp Console"](#)

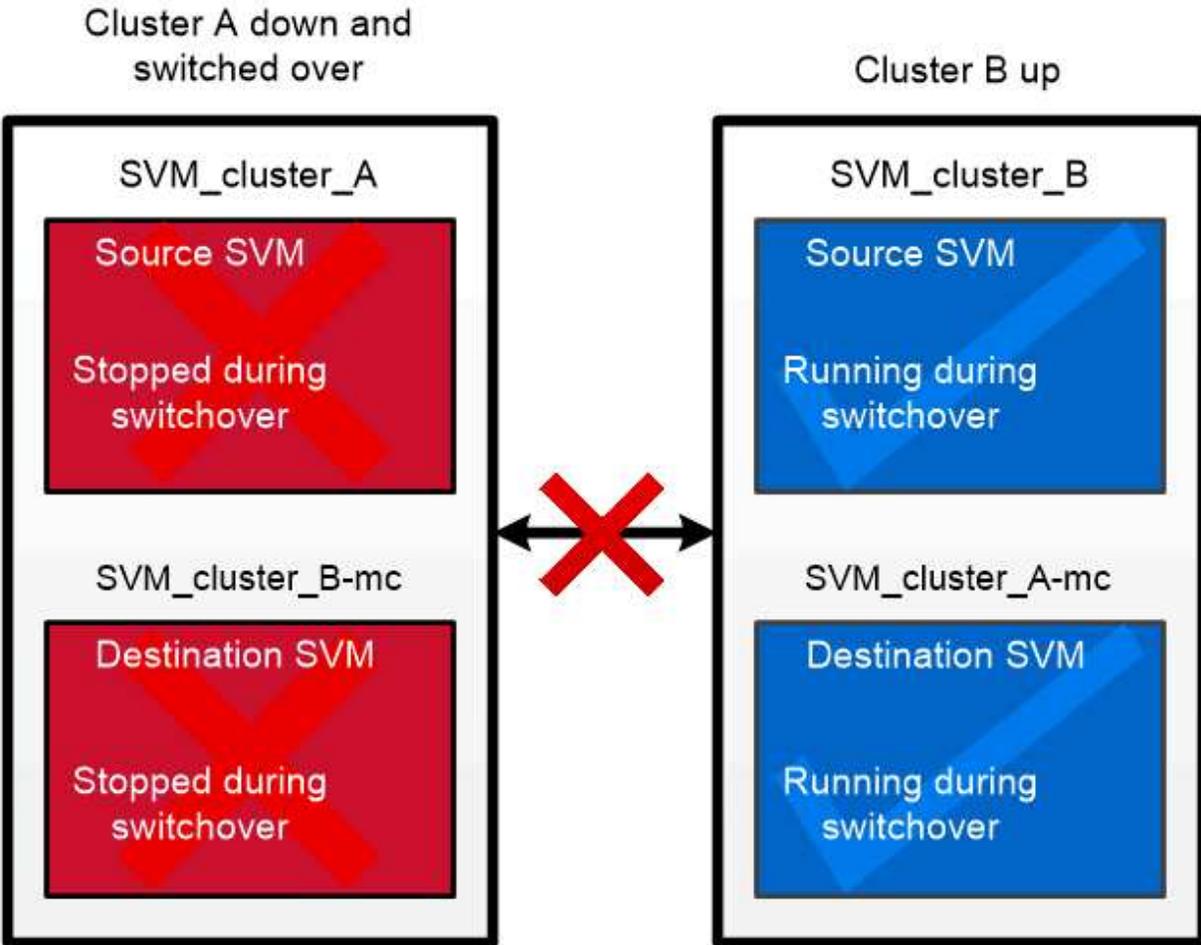
MetroClusterの継続的可用性

MetroCluster構成は、物理的に分離された2つのミラー クラスタを実装することでデータを保護します。各クラスタが、もう一方のクラスタのデータおよびSVM設定を同期的にレプリケートします。一方のサイトで災害が発生したときは、管理者はミラーリングされたSVMをアクティブ化し、ミラーリングされたデータをセカンダリ サイトから提供できます。

- ファブリック接続 *MetroCluster* および *MetroCluster IP* 構成は、メトロポリタン全体のクラスターをサポートします。
- *_Stretch MetroCluster_* 構成は、キャンパス全体のクラスターをサポートします。

いずれの場合も、クラスタ間でピア関係を確立する必要があります。

MetroClusterは、ONTAPの*_SyncMirror_*と呼ばれる機能を使用して、各クラスタのアグリゲートデータをコピー（プレックス）として他のクラスタのストレージに同期的にミラーリングします。スイッチオーバーが発生すると、残存クラスタのリモート プレックスがオンラインになり、セカンダリSVMがデータの提供を開始します。



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

非MetroCluster環境でのSyncMirrorの使用 非MetroCluster環境でも、RAIDタイプが保護できる以上のディスク障害やRAIDグループディスクへの接続喪失によるデータ損失を防ぐために、オプションでSyncMirrorを使用できます。この機能はHAペアでのみ利用可能です。

アグリゲート データは、別々のディスク シェルフに格納されたプレックス間でミラーリングされます。一方のシェルフが使用できなくなった場合、影響を受けていないプレックスが障害からの復旧作業中も引き続きデータを提供します。

SyncMirrorを使用してミラーリングされたアグリゲートには、ミラーされていないアグリゲートの2倍のストレージが必要であることを注意してください。各プレックスには、ミラーリングするプレックスと同じ数のディスクが必要です。例えば、1,440 GBのアグリゲートをミラーリングするには、プレックスごとに1,440 GB、つまり2,880 GBのディスク容量が必要になります。

SyncMirrorでは、ストレージのパフォーマンスと可用性を最適化するために、ミラーリングされたアグリゲートに少なくとも20%の空きスペースを確保することをお勧めします。ミラーリングされていないアグリゲートの推奨値は10%ですが、追加の10%のスペースは、ファイルシステムが増分変更を吸収するために使用される場合があります。ONTAPのcopy-on-writeスナップショットベースのアーキテクチャにより、増分変更によってミラーリングされたアグリゲートのスペース使用率が上昇します。これらのベストプラクティスに従わないと、SyncMirror再同期のパフォーマンスに悪影響を与える可能性があり、非共有クラウド環境のNDUやMetroCluster環境のスイッチバックなどの運用ワークフローに間接的に影響を及ぼします。

ストレージ効率

ONTAP Storage Efficiencyの概要

ストレージ効率とは、ストレージ リソースを最適化し、無駄なスペースを最小限に抑え、書き込まれたデータの物理的なフットプリントを削減することで、ストレージ システムが利用可能なスペースをどれだけ効率的に使用しているかを示す指標です。ストレージ効率が低いほど、最小限のスペースに最大限のデータ量を、最小限のコストで保存できます。例えば、重複したデータ ブロックやゼロで埋められたデータ ブロックを検出して排除するストレージ効率化テクノロジーを活用することで、必要な物理ストレージの総量を削減し、全体的なコストを削減できます。

ONTAPには、データによって消費される物理的ハードウェアやクラウド ストレージの量を減らしつつ、データの読み取り、データセットのコピー、VMのプロビジョニングを高速化するなどしてシステムのパフォーマンスを大幅に向上させる、さまざまなStorage Efficiencyテクノロジーが搭載されています。

ONTAPのStorage Efficiencyテクノロジーには、次のようなものがあります。

- シンプロビジョニング

シンプロビジョニングを使用すると、事前に予約するのではなく、必要に応じてボリュームまたはLUNにストレージを割り当てることができます。これにより、現在使用されていないスペースを予約することなく、潜在的な使用量に基づいてボリュームまたはLUNを過剰割り当てできるため、必要な物理ストレージの量を削減できます。

- 重複排除

重複排除は、ボリュームに必要な物理ストレージの量を3つの異なる方法で削減します。

- ゼロブロック重複排除

ゼロ ブロック重複排除では、ゼロだけで埋められたデータ ブロックが検出、排除され、メタデータのみが更新されます。通常、ゼロ ブロックで使用されていたスペースが100%解放されます。ゼロ ブロック重複排除は、すべての重複排除ポリシーでデフォルトで有効になっています。

- インライン重複排除

インライン重複排除では、重複するデータ ブロックが検出され、データがディスクに書き込まれる前に一意の共有ブロックへの参照に置き換えられます。インライン重複排除により、VMのプロビジョニングが20~30%高速化されます。インライン重複排除は、ONTAPのバージョンとプラットフォームに応じて、ポリシーレベルかアグリゲートレベルで実行できます。AFFシステムとASAシステムでは、デフォルトで有効になっています。FASシステムでは、インライン重複排除を手動で有効にする必要があります。

- バックグラウンド重複排除

バックグラウンド重複排除でも、重複するデータ ブロックが検出され、一意の共有ブロックへの参照に置き換えられますが、データがディスクに書き込まれたあとで置き換えが行われるので、さらにストレージ効率が高くなります。バックグラウンド重複排除は、ストレージ システムで特定の条件が満たされたときに実行されるように設定できます。たとえば、ポリシーの利用率が10%に達したときにバックグラウンド重複排除が実行されるように設定できます。バックグラウンド重複排除は、手動でトリガーすることも、指定したスケジュールに基づいて実行されるように設定することもできます。AFFシステムとASAシステムでは、デフォルトで有効になっています。FASシステムでは、バックグラウンド重複排除を手動で有効にする必要があります。

重複排除は、ポリシー内と、アグリゲート内のポリシー間でサポートされます。通常、重複排除されたデータの読み取りがパフォーマンスに影響することはありません。

- 圧縮

圧縮は、データ ブロックを圧縮グループにまとめ、各グループを単一のブロックとして格納することで、ポリシーに必要な物理ストレージの容量を削減します。読み取りまたは上書き要求を受信すると、ファイル全体ではなく、少数のブロック グループのみが読み取られます。このプロセスにより、読み取りと上書きのパフォーマンスが最適化され、圧縮対象ファイルのサイズのスケールビリティが向上します。

圧縮は、インラインまたはポストプロセスで実行できます。インライン圧縮では、メモリ内のデータがディスクに書き込まれる前に圧縮されるので、スペースを即座に削減できます。ポストプロセス圧縮では、まず圧縮されていない状態でブロックがディスクに書き込まれ、その後スケジュールされた時刻にデータが圧縮されます。AFFシステムでは、デフォルトで有効になっています。その他のすべてのシステムでは、圧縮を手動で有効にする必要があります。

- コンパクション

コンパクションでは、4KBのブロックに格納されているもののサイズが4KB未満のデータ チャンクが単一のブロックに結合されることにより、ポリシーに必要な物理ストレージの量が削減されます。コンパクションはデータがメモリ上にある間に実行されるため、ディスク上で不要なスペースが消費されることはありません。AFFシステムとASAシステムでは、デフォルトで有効になっています。FASシステムでは、コンパクションを手動で有効にする必要があります。

- FlexCloneポリシー、ファイル、LUN

FlexCloneテクノロジーは、Snapshotメタデータを活用して、ポリシー、ファイル、またはLUNの書き込み可能なポイントインタイムコピーを作成します。コピーは親とデータ ブロックを共有し、コピーまた

は親に変更が書き込まれるまで、メタデータに必要なストレージ以外は消費しません。変更が書き込まれると、差分のみが保存されます。

従来の手法でコピーを作成すると数分から数時間かかりますが、FlexCloneテクノロジーを使用すれば大規模なデータセットのコピーもほぼ瞬時に作成できます。

- 温度に依存したストレージ効率

ONTAPは、"温度に敏感なストレージ効率"ボリュームのデータへのアクセス頻度を評価し、その頻度とデータに適用される圧縮レベルをマッピングすることで、メリットを提供します。アクセス頻度の低いコールドデータについては、大きなデータブロックを圧縮します。アクセス頻度が高く、上書きされる頻度が高いホットデータについては、小さなデータブロックを圧縮することで、処理効率を高めます。

ONTAP 9.8で導入された温度感応ストレージ効率 (TSSE) は、新規作成されたシンプロビジョニングAFFボリュームで自動的に有効化されます。ONTAP 9.15.1で導入された"[AFF A70](#)、[AFF A90](#)、および[AFF A1Kプラットフォーム](#)"、ハードウェアオフロードプロセッサを使用するボリュームでは有効化されません。



TSSEはシック プロビジョニングされたボリュームではサポートされていません。

- CPUまたは専用オフロード プロセッサのストレージ効率

ONTAP 9.15.1以降、"[CPUまたは専用オフロード プロセッサによるストレージ効率化](#)"は一部のAFFおよびFASプラットフォームで自動的に有効になり、設定は不要です。これらのプラットフォームでは、温度に依存するストレージ効率化は使用されません。圧縮は、データがコールド状態になるのを待たずに開始され、メインCPUまたは専用オフロード プロセッサを使用して実行されます。また、これらのプラットフォームでは、連続する物理ブロックのシーケンシャル パッキングを使用して、圧縮データのストレージ効率をさらに向上させます。

これらのテクノロジーのメリットは、最小限の労力で日常業務に活かすことができます。たとえば、5,000人のユーザーにホーム ディレクトリ用のストレージを提供する必要があり、ユーザー1人あたりに必要な最大容量は1GBと見積もっているとします。潜在的なストレージ ニーズの合計を満たすために、事前に5TBのアグリゲートを予約しておくことができます。ただし、ホーム ディレクトリの容量要件は組織全体で大きく異なることもわかっています。組織全体で5TBの容量を予約する代わりに、2TBのアグリゲートを作成できます。その後、シン プロビジョニングを使用して、各ユーザーに名目上1GBのストレージを割り当て、必要な場合にのみストレージを割り当てることができます。アグリゲートを継続的に監視し、必要に応じて実際の物理サイズを増やすことができます。

別の例として、仮想デスクトップ インフラ (VDI) を使用していて、仮想デスクトップ間で大量の重複データが発生している状況があるとします。重複排除機能を使用すれば、VDI全体で重複する情報ブロックが自動的に排除され、元のブロックへのポインタに置き換えられるので、ストレージの使用量を減らせます。圧縮など、ONTAPのその他のStorage Efficiencyテクノロジーも、ユーザが操作しなくてもバックグラウンドで実行されるようにできます。

ONTAPのディスク パーティショニング テクノロジーによっても、ストレージ効率が向上します。RAID DPテクノロジーは、パフォーマンスの低下や、ディスクミラーリングのオーバーヘッド増大を伴うことなく、二重ディスク障害からデータを保護します。ONTAP 9の高度なSSDパーティショニングにより、使用可能な容量が20%近く増加します。

NetAppは、オンプレミスのONTAPで利用可能な同じストレージ効率機能をクラウドでも提供します。オンプレミスのONTAPからクラウドにデータを移行しても、既存のストレージ効率は維持されます。例えば、ビジネス クリティカルなデータを含むSQLデータベースをオンプレミス システムからクラウドに移行したいとし

ます。NetApp Consoleのデータ レプリケーションを使用してデータを移行し、移行プロセスの一環として、クラウドのスナップショットに最新のオンプレミス ポリシーを適用できます。

シンプロビジョニング

ONTAPは、スナップショットに加えて、幅広いストレージ効率化テクノロジーを提供しています。主要なテクノロジーには、シンプロビジョニング、重複排除、圧縮、FlexCloneボリューム、ファイル、LUNなどがあります。スナップショットと同様に、これらはすべてONTAPのWrite Anywhere File Layout (WAFL) に基づいて構築されています。

シンプロビジョニングされたボリュームまたはLUNとは、ストレージが事前に予約されていないボリュームまたはLUNのことです。代わりに、ストレージは必要に応じて動的に割り当てられます。ボリュームまたはLUN内のデータが削除されると、空き領域はストレージシステムに解放されます。

組織で5,000人のユーザーにホームディレクトリ用のストレージを提供する必要があるとします。最大のホームディレクトリは1 GBの容量を消費すると見積もっています。

このような状況では、5 TBの物理ストレージを購入することができます。ホームディレクトリを格納するボリュームごとに、最大の利用者のニーズを満たすのに十分なスペースを確保します。

しかし、現実的には、ホームディレクトリの容量要件はコミュニティ全体で大きく異なることもご存知でしょう。ストレージを大量に使用するユーザー1人に対して、ほとんど、あるいは全く容量を消費しないユーザーが10人いるのです。

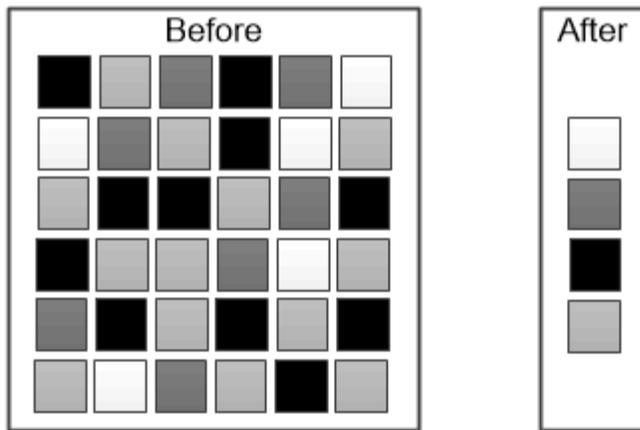
シンプロビジョニングを使用すると、使用しない可能性のあるストレージを購入することなく、大規模なストレージ利用者のニーズを満たすことができます。ストレージ容量は消費されるまで割り当てられないため、2TBのアグリゲートに含まれる5,000個のボリュームそれぞれに1GBのサイズを名目上割り当てることで、2TBのアグリゲートを「オーバーコミット」できます。

ライト ユーザとヘビー ユーザの比率が10:1という想定が正しければ、アグリゲートの空きスペースを能動的に監視しているかぎり、スペース不足によってボリュームへの書き込みが失敗することはありません。

重複排除

重複排除は、重複ブロックを破棄し、単一の共有ブロックへの参照に置き換えることで、ボリューム（またはAFFアグリゲート内のすべてのボリューム）に必要な物理ストレージ容量を削減します。重複排除されたデータの読み取りには通常、パフォーマンス負荷は発生しません。書き込みには、過負荷のノードを除き、ごくわずかな負荷しかかかりません。

通常の使用中にデータが書き込まれると、WAFLはバッチプロセスを使用してブロックシグネチャのカタログを作成します。重複排除が開始されると、ONTAPはカタログ内のシグネチャを比較し、重複ブロックを特定します。一致するブロックが存在する場合、バイト単位で比較が行われ、候補ブロックがカタログ作成以降に変更されていないことが確認されます。すべてのバイトが一致した場合にのみ、重複ブロックは破棄され、そのディスク スペースが再利用されます。



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

圧縮

圧縮は、データブロックを圧縮グループにまとめ、各グループを単一のブロックとして保存することで、ボリュームに必要な物理ストレージ容量を削減します。ONTAPはファイル全体またはLUN全体ではなく、要求されたデータを含む圧縮グループのみを解凍するため、圧縮データの読み取りは従来の圧縮方法よりも高速です。

インライン圧縮またはポストプロセス圧縮を個別または組み合わせて実行できます：

- インライン圧縮は、データをディスクに書き込む前にメモリ内で圧縮するため、ボリュームへの書き込みI/O量が大幅に削減されますが、書き込みパフォーマンスが低下する可能性があります。パフォーマンスを著しく低下させる操作は、次のポストプロセス圧縮操作（ある場合）まで延期されます。
- ポストプロセス圧縮は、重複排除と同じスケジュールで、データがディスクに書き込まれた後にデータを圧縮します。

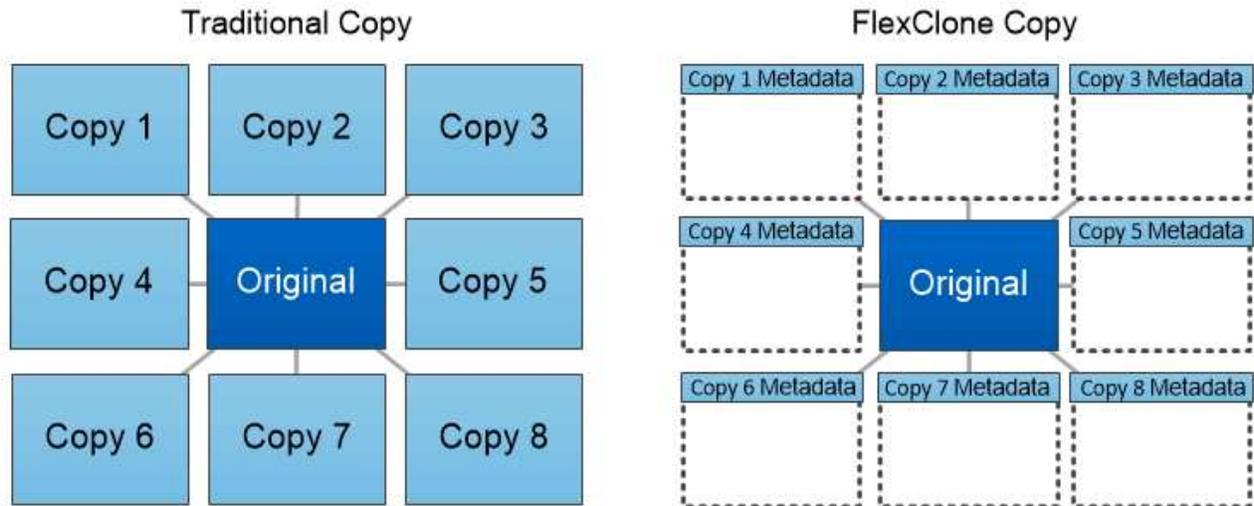
インライン データ コンパクション 小さなファイルやゼロでパディングされたI/Oは、4KBの物理ストレージを必要とするかどうかにかかわらず、4KBのブロックに格納されます。インライン データ コンパクションは、通常複数の4KBブロックを占めるデータ チャンクを、ディスク上の単一の4KBブロックに結合します。コンパクションはデータがメモリ内にある間に実行されるため、高速なコントローラに最適です。

FlexCloneのボリューム、ファイル、LUN

FlexCloneテクノロジーは、スナップショットのメタデータを参照して、ボリュームの書き込み可能なポイントインタイムコピーを作成します。コピーは親ボリュームとデータブロックを共有し、変更がコピーに書き込まれるまで、メタデータに必要なストレージ容量以外は消費しません。FlexCloneファイルとFlexClone LUNは、バックアップのスナップショットが不要であることを除き、同一のテクノロジーを使用します。

従来の手法でコピーを作成すると数分から数時間かかりますが、FlexCloneソフトウェアを使用すれば大規模なデータセットのコピーもほぼ瞬時に作成できます。そのため、同じデータセットのコピーが複数必要な状況（仮想デスクトップ環境など）や一時的にデータセットのコピーが必要な状況（本番環境のデータセットでアプリケーションをテストする場合など）に適しています。

既存のFlexCloneボリュームのクローン、LUNクローンを含むボリュームのクローン、ミラーデータとボールドデータのクローンを作成できます。FlexCloneボリュームを親ボリュームから_分割_することもできます。その場合、コピーには専用のストレージが割り当てられます。



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

ONTAP容量レポートと測定について学ぶ

ONTAPストレージ容量は、物理スペースまたは論理スペースのいずれかで測定できます。これらの測定値の報告方法は、ONTAPバージョンと、System Managerまたはコマンドラインインターフェイス (CLI) のどちらを使用しているかによって異なります。ストレージの使用状況を監視する際には、容量に関連するさまざまな用語、物理容量と論理容量の違い、および容量タイプの報告方法を理解することが重要です。

- 物理容量：物理スペースとは、ボリュームまたはローカル層で使用されるストレージの物理ブロックを指します。ストレージ効率化機能（重複排除や圧縮など）によってデータが削減されるため、通常、物理使用容量の値は使用済み論理容量の値よりも小さくなります。
- 論理容量：論理スペースとは、ボリュームまたはローカル階層内の使用可能なスペース（論理ブロック）を指します。論理スペースとは、重複排除や圧縮の結果を考慮せずに、理論上使用できるスペースを指します。使用済み論理スペースの値は、使用済み物理スペースの量と、設定されているストレージ効率化機能（重複排除や圧縮など）による削減量から算出されます。この測定値は、Snapshotコピー、クローン、その他のコンポーネントが含まれており、データ圧縮やその他の物理スペースの削減が反映されていないため、物理使用容量よりも大きく表示されることがよくあります。したがって、論理容量の合計はプロビジョニングされたスペースよりも大きくなる可能性があります。

CLIでの容量レポート

ONTAP CLI では、使用している ONTAP のバージョンによって物理使用済みスペースの報告方法が異なります。ONTAP 9.13.1 以前では、`physical used` パラメータが `volume show` コマンド出力に表示され、ボリュームに適用されたすべてのストレージ効率化による節約分が含まれます。ONTAP 9.14.1 以降では、`physical used` パラメータには、温度感応型ストレージ (TSSE)、インライン圧縮、コンパクション、ボリューム間重複排除などのアグリゲートレベルのストレージ効率化による節約分が含まれないため、ボリュームの物理使用済みスペースを正確に反映しません。ONTAP 9.14.1 以降では、ボリュームの正確な物理使用済

みスペースを確認するには、`vol show-footprint` コマンドと `effective_total_footprint` パラメータを使用してください。

| ONTAPバージョン | コマンド | パラメータ | 概要 |
|------------|------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------|
| 9.14.1以降 | <code>volume show-footprint</code> | <code>effective_total_footprint</code> | アグリゲートからの削減量を含む、実際に使用されているディスク容量を反映します。 |
| | <code>volume show-space</code> | <code>physical used</code> | アグリゲートからの削減量を含む、ボリュームレベルのストレージ効率による削減量を反映します。 |
| | <code>volume show</code> | <code>physical used</code> | 集約レベルのストレージ効率の節約は含まれていないため、 "TSSE対応プラットフォーム" のボリュームの物理的な使用領域を正確に反映しません。 |
| 9.13.1以前 | <code>volume show-footprint</code> | <code>effective_total_footprint</code> | アグリゲートからの削減量を含む、実際に使用されているディスク容量を反映します。 |
| | <code>volume show-space</code> | <code>physical used</code> | ボリュームレベルのストレージ効率化による削減量のみを反映します。 |
| | <code>volume show</code> | <code>total physical used</code> | ボリュームレベルのストレージ効率化による削減量のみを反映します。 |

関連情報

- ["9.14.1 以降の物理使用領域レポートの変更"](#)の詳細については、こちらをご覧ください。
- ["スペース使用情報を表示するためのコマンド"](#)についての詳細をご覧ください。

System Managerの容量レポート

使用容量の測定値は、ONTAP のバージョンに応じて System Manager で異なる方法で表示されます。ONTAP 9.7 以降、System Manager は物理容量と論理容量の両方の測定値を提供します。



System Managerでは、ルート ストレージ階層（アグリゲート）の容量は考慮されません。

| System Managerのバージョン | 容量を表す用語 | 参照される容量のタイプ |
|----------------------|----------|-----------------------------------|
| 9.9.1以降 | 使用済み論理容量 | ストレージ効率設定が有効になっている場合に使用される論理スペース) |

| | | |
|----------------------|------|----------------------------------|
| 9.7 と 9.8 | 使用済み | 使用済み論理スペース（ストレージ効率設定が有効になっている場合） |
| 9.5 および 9.6（クラシック表示） | 使用済み | 使用済みの物理スペース |

容量測定関連の用語

容量のタイプに使用される用語は次のとおりです。

- 割り当て容量：Storage VM 内のボリュームに割り当てられたスペースの量。
- 使用可能：ストレージ VM またはローカル層でデータを保存したりボリュームをプロビジョニングしたりするために使用できる物理スペースの量。
- ボリューム全体の容量：ストレージ VM 上のすべてのボリュームの使用済みストレージと使用可能なストレージの合計。
- クライアント データ：クライアント データ（物理または論理）によって使用されるスペースの量。
 - ONTAP 9.13.1 以降では、クライアント データによって使用される容量は 論理使用容量 と呼ばれ、スナップショットによって使用される容量は別途表示されます。
 - ONTAP 9.12.1 以前では、クライアント データによって使用される容量とスナップショットによって使用される容量を合計したものは、*使用済み論理容量*と呼ばれます。
- コミット済み：ローカル階層のコミット済み容量。
- データ削減：取り込まれたデータのサイズと保存されたデータのサイズの比率。
 - ONTAP 9.13.1以降、データ削減機能では、重複排除や圧縮など、ほとんどのStorage Efficiency機能の結果が考慮されますが、Snapshotやシンプロビジョニングはデータ削減率に含まれません。
 - ONTAP 9.12.1以前では、データ削減比率は次のように表示されます。
 - *容量*パネルに表示されるデータ削減値は、すべての使用済み論理容量と使用済み物理容量の全体的な比率であり、Snapshotやその他のストレージ効率化機能の使用から得られる利点が含まれません。
 - 詳細パネルを表示すると、概要パネルに表示された 全体 の比率と、クライアント データのみで使用される使用済み論理容量とクライアント データのみで使用される物理使用領域の比率（スナップショットとクローンなし と呼ばれます）の両方が表示されます。
- 使用済み論理容量：
 - ONTAP 9.13.1 以降では、クライアント データによって使用される容量は 論理使用容量 と呼ばれ、スナップショットによって使用される容量は別途表示されます。
 - ONTAP 9.12.1 以前では、スナップショットによって使用される容量に追加されたクライアント データによって使用される容量は、*論理使用容量*と呼ばれます。
- 論理使用率 %：スナップショット リザーブを除く、プロビジョニング済みサイズに対する現在の使用済み論理容量の割合。この値には、ボリュームの効率化による削減量が含まれるため、100%を超える場合があります。
- 最大容量：ストレージ VM 上のボリュームに割り当てられるスペースの最大量。
- 物理使用量：ボリュームまたはローカル層の物理ブロックで使用されている容量。

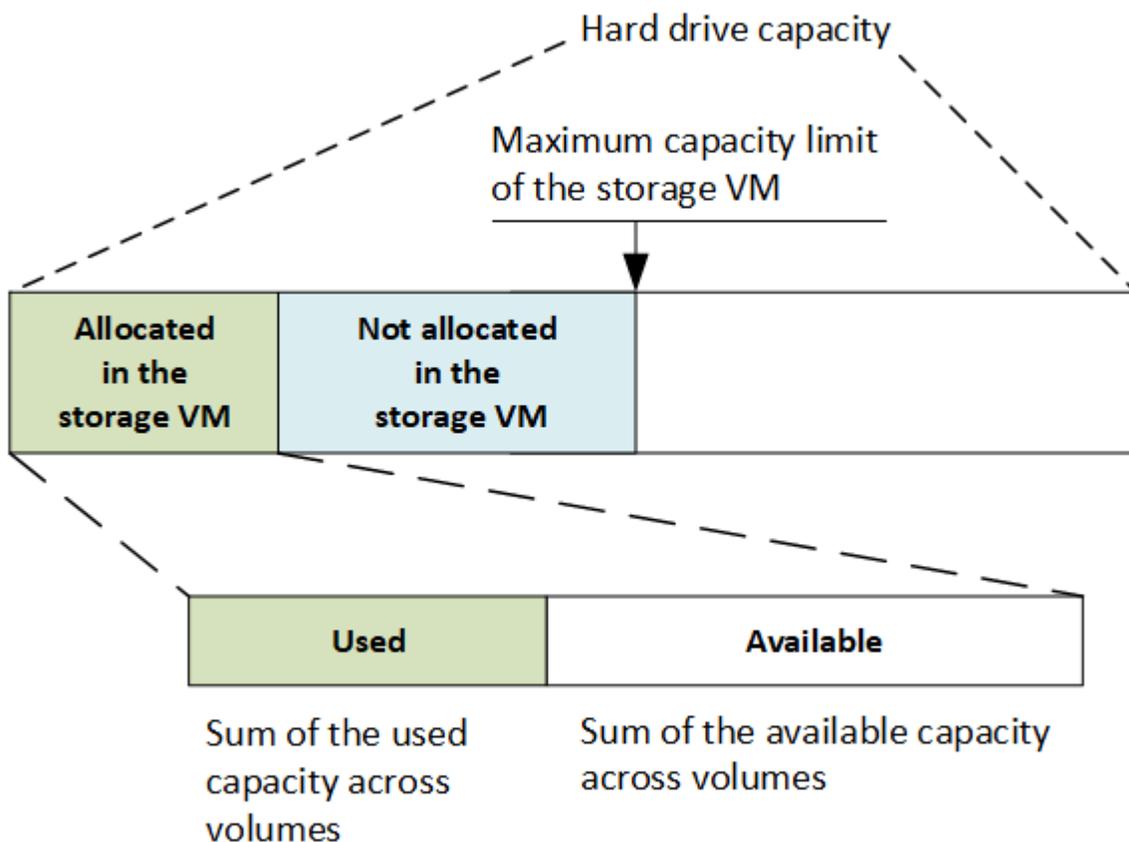
- 物理使用率 %：プロビジョニングされたサイズと比較した、ボリュームの物理ブロックで使用されている容量の割合。
- プロビジョニングされた容量：Cloud Volumes ONTAPシステムから割り当てられ、ユーザーまたはアプリケーションのデータを保存する準備ができていないファイル システム（ボリューム）。
- 予約済み：ローカル階層ですでにプロビジョニングされているボリューム用にリザーブされているスペースの量。
- 使用済み：データが含まれているスペースの量。
- 使用済みおよび予約済み：物理的な使用済みスペースとリザーブ スペースの合計。

Storage VMの容量

Storage VMの最大容量は、各ボリュームに割り当てられているスペースの合計に、残りの未割り当てのスペースを足したものです。

- ボリュームに割り当てられているスペースは、FlexVol、FlexGroup、FlexCacheボリュームの使用済み容量と使用可能容量の合計です。
- ボリュームの容量は、そのボリュームが制限されている場合、オフラインの場合、または削除後にリカバリ キューに登録されている場合も、合計に含まれます。
- ボリュームに自動拡張が設定されている場合は、ボリュームの最大オートサイズが使用されます。自動拡張が設定されていない場合は、ボリュームの実際の容量が使用されます。

次の図は、ボリューム全体の容量の測定値と最大容量の関係を示しています。



ONTAP 9.13.1以降、クラスタ管理者は"[ストレージ VM の最大容量制限を有効にする](#)"。ただし、データ保護用のボリューム、SnapMirrorリレーションシップ内のボリューム、またはMetroCluster構成内のボリュームを含むストレージVMには、ストレージ制限を設定できません。また、ストレージVMの最大容量を超えるクォータを設定することもできません。

一度設定した最大容量を、現在割り当てられている容量よりも小さいサイズに変更することはできません。

ストレージVMが最大容量制限に達すると、特定の操作を実行できなくなります。System Managerは、"[インサイト](#)"で次の手順を提案します。

System Managerの容量測定単位

System Managerは、1024 (2¹⁰) バイトのバイナリ単位に基づいてストレージ容量を計算します。

- ONTAP 9.10.1以降のSystem Managerでは、ストレージ容量の単位はKiB、MiB、GiB、TiB、PiBとして表示されます。
- ONTAP 9.10.0以前のSystem Managerでは、これらの単位はKB、MB、GB、TB、PBとして表示されません。



スループットの単位については、ONTAPのすべてのリリースのSystem Managerで、KB/秒、MB/秒、GB/秒、PB/秒が引き続き使用されます。

| ONTAP 9.10.0 以前の System Manager に表示される容量単位 | ONTAP 9.10.1以降の System Manager に表示される容量単位 | 計算式 | バイト単位の値 |
|--------------------------------------------|-------------------------------------------|----------------------------------|--------------------------|
| KB | KiB | 1024 | 1024バイト |
| MB | MiB | 1024 * 1024 | 1,048,576バイト |
| GB | GiB | 1024 * 1024 * 1024 | 1,073,741,824バイト |
| TB | TiB | 1024 * 1024 * 1024 * 1024 | 1,099,511,627,776バイト |
| PB | PiB | 1024 * 1024 * 1024 * 1024 * 1024 | 1,125,899,906,842,624バイト |

関連情報

["System Manager でクラスタ、階層、SVM の容量を監視する"](#)

["ボリュームの論理スペースのレポートと適用"](#)

ONTAPの温度に影響されるストレージ効率について学ぶ

ONTAPは、ボリュームのデータへのアクセス頻度を評価し、その頻度とデータに適用される圧縮レベルをマッピングすることで、温度感応ストレージ効率 (TSSE) のメリットを提供します。アクセス頻度の低いコールドデータについては大きなデータブロックを

圧縮し、アクセス頻度が高く、上書きされる頻度が高いホットデータについては小さなデータブロックを圧縮することで、処理効率を高めます。

TSSEはONTAP 9.8で導入され、新規に作成されたシンプロビジョニングAFFボリュームで自動的に有効化されます。温度に敏感なストレージ効率は、既存のシンプロビジョニングAFFボリュームと、シンプロビジョニングされた非AFF DPボリュームで有効にできます。TSSEはシックプロビジョニングボリュームではサポートされません。

温度に依存するストレージ効率化は、次のプラットフォームには適用されません：

| プラットフォーム | ONTAPのバージョン |
|------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <ul style="list-style-type: none">• AFF A1K用• AFF A90• AFF A70• FAS90• FAS70 | 9.15.1以降 |
| <ul style="list-style-type: none">• AFF C80用• AFF C60• AFF C30• AFF A50• AFF A30 | 9.16.1以降 |

これらのプラットフォームは"[CPUまたは専用オフロード プロセッサによるストレージ効率化](#)"を使用します。圧縮は、ホット データまたはコールド データに基づかず、メイン CPU または専用のオフロード プロセッサを使用して実行されます。



時間の経過とともに、ボリュームで使用されるスペースの量は、TSSEでは8Kアダプティブ圧縮よりも顕著になる可能性があります。この動作は、TSSEと8Kアダプティブ圧縮のアーキテクチャ上の違いによるものです。

「default」モードと「efficient」モードの導入

ONTAP 9.10.1以降、AFFシステムのみにもボリュームレベルのストレージ効率モード `_default_` と `_efficient_` が導入されました。これらの2つのモードでは、新規AFFボリューム作成時のデフォルトモードであるファイル圧縮 (default) と、自動適応型圧縮を用いてアクセス頻度の低いコールドデータの圧縮率を向上させる温度感応型ストレージ効率 (efficient) のいずれかを選択できます。

ONTAP 9.10.1以降にアップグレードする場合、既存のボリュームには、現在ボリュームで有効になっている圧縮のタイプに基づいてストレージ効率モードが割り当てられます。アップグレード中、圧縮が有効になっているボリュームにはデフォルト モードが割り当てられ、温度に依存するストレージ効率が有効になっているボリュームには効率的モードが割り当てられます。圧縮が有効になっていない場合、ストレージ効率モードは空白のままになります。

ONTAP 9.10.1では、"[温度に敏感なストレージ効率は明示的に設定する必要があります](#)"自動アダプティブ圧縮が有効になります。ただし、インライン データ コンパクション、自動重複排除スケジュール、インライン重複排除、ボリューム間インライン重複排除、ボリューム間バックグラウンド重複排除といったその他のスト

レイジ効率化機能はAFFプラットフォームではデフォルトモードと効率化モードの両方でデフォルトで有効になっています。

両方のストレージ効率モード（デフォルトと効率的）は、FabricPool対応アグリゲートおよびすべての階層化ポリシータイプでサポートされます。

CシリーズプラットフォームでTemperature Sensitive Storage Efficiencyを有効にする

温度に敏感なストレージ効率はAFF C シリーズプラットフォームではデフォルトで有効になっています。また、ボリューム移動を使用して、またはSnapMirrorを使用して、移行先に次のリリースがインストールされている状態で、非 TSSE プラットフォームから TSSE 対応の C シリーズプラットフォームにシンプロビジョニングされたボリュームを移行する場合にも有効になっています。

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

詳細については、"[ボリューム移動処理とSnapMirror処理でのStorage Efficiencyの動作](#)"を参照してください。

既存のシンプロビジョニングボリュームでは、温度に敏感なストレージ効率は自動的に有効になりませんが、"[ストレージ効率モードを変更する](#)"を使用して手動で効率モードに変更できます。



いったんStorage Efficiencyモードをefficientに変更すると、元には戻せません。

連続する物理ブロックのシーケンシャルパッキングによるストレージ効率の向上

ONTAP 9.13.1以降、温度に敏感なストレージ効率に、連続する物理ブロックのシーケンシャルパッキングが追加され、ストレージ効率がさらに向上します。温度に敏感なストレージ効率が有効になっているボリュームでは、システムをONTAP 9.13.1にアップグレードすると、シーケンシャルパッキングが自動的に有効になります。シーケンシャルパッキングを有効にした後は、"[既存のデータを手動で再パックする](#)"する必要があります。

ONTAP専用オフロードプロセッサのストレージ効率について学ぶ

専用オフロードプロセッサによるストレージ効率は、連続する物理ブロックをシーケンシャルパッキングし、専用のオフロードプロセッサを用いて32KBデータ圧縮を行います。32KB圧縮では、8KBアダプティブ圧縮を使用するプラットフォームのようにボリュームレベルでスペース節約を実現するのとは異なり、アグリゲートレベルでスペース節約を実現します。専用オフロードプロセッサによるストレージ効率を使用するプラットフォームは、温度感知型ストレージ効率（TSSE）を採用していません。つまり、圧縮はホットデータとコールドデータに基づいていません。そのため、パフォーマンスに影響を与えることなく、即座にスペース節約を実現できます。

専用オフロードプロセッサストレージ効率は、次のプラットフォームおよびONTAPバージョンでデフォルトで有効になっています。



AFF A20プラットフォームは、専用オフロードプロセッサによるストレージ効率をサポートしていません。AFF A20プラットフォームでは、SnapMirrorテクノロジーを使用して移行されたデータは、メインCPUを使用して自動的に32kインライン圧縮に変換されます。

| プラットフォーム | ONTAPのバージョン |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <ul style="list-style-type: none"> • AFF A1K用 • AFF A90 • AFF A70 • FAS90 • FAS70 | 9.15.1以降 |
| <ul style="list-style-type: none"> • AFF C80用 • AFF C60 • AFF C30 • AFF A50 • AFF A30 | 9.16.1以降 |

以下のプラットフォームでは、ストレージ効率¹は自動的に有効化され、設定は不要です。これは、新規に作成されたすべてのシンプロビジョニングボリュームと、他のプラットフォームから移行されたボリュームを含む既存のデータに適用されます。重複排除は、スペースギャランティの設定に関係なく有効になります。圧縮とデータコンパクションはどちらも、スペースギャランティを none に設定する必要があります。ボリューム移動またはSnapMirrorテクノロジーを使用して移行されたデータは、自動的に32k インライン圧縮に変換されません。

- AFF C80用
- AFF C60
- AFF C30
- AFF A1K用
- AFF A90
- AFF A70
- AFF A50
- AFF A30

以下のプラットフォームでは、ONTAP 9.15.1以降にアップグレードする前にストレージ効率が有効になっていた既存のシンプロビジョニングボリュームに対してのみ、ストレージ効率がデフォルトで有効になります。新規に作成されたボリュームでは、CLIまたはREST APIメソッドを使用してストレージ効率を有効にできません。ボリューム移動またはSnapMirrorテクノロジーを使用して移行されたデータは、元のプラットフォームで圧縮が有効になっている場合にのみ、32KBのインライン圧縮に変換されます。

- FAS90
- FAS70

コントローラをサポートされているプラットフォームのいずれかにアップグレードする方法については、"[ONTAP ハードウェア アップグレード ドキュメント](#)"を参照してください。

セキュリティ

クライアント認証と許可

ONTAPは、クライアントと管理者のストレージへのアクセスを保護し、ウイルスから保護するために標準的な方法を使用しています。保存データの暗号化とWORMストレージには、高度なテクノロジーが利用可能です。

ONTAPは、信頼できるソースを使用してクライアントマシンとユーザーのIDを検証することで、それらを認証します。ONTAPは、ユーザーの認証情報とファイルまたはディレクトリに設定されている権限を比較することで、ユーザーにファイルまたはディレクトリへのアクセスを許可します。

認証

ユーザ アカウントは、ローカルまたはリモートとして作成できます。

- ローカル アカウントでは、アカウント情報がストレージ システムに格納されます。
- リモート アカウントでは、アカウント情報がActive Directoryドメイン コントローラ、LDAPサーバ、またはNISサーバに格納されます。

ONTAPは、ローカルまたは外部のネーム サービスを使用して、ホスト名、ユーザ、グループ、ネットグループ、ネーム マッピング情報を検索します。ONTAPでは、次のネーム サービスをサポートしています。

- ローカル ユーザ
- DNS
- 外部NISドメイン
- 外部LDAPドメイン

`_ネーム サービス スイッチ テーブル_` は、ネットワーク情報の検索元と検索順序を指定します（UNIXシステムの`/etc/nsswitch.conf`ファイルと同等の機能を提供します）。NASクライアントがSVMに接続すると、ONTAPは指定されたネーム サービスをチェックして必要な情報を取得します。

Kerberos サポート Kerberos は、クライアント/サーバ実装においてユーザパスワードを暗号化することで「強力な認証」を実現するネットワーク認証プロトコルです。ONTAP は、整合性チェック機能付き Kerberos 5 認証 (krb5i) とプライバシーチェック機能付き Kerberos 5 認証 (krb5p) をサポートしていません。

許可

ONTAPでは、3つのレベルのセキュリティを評価して、SVM上にあるファイルおよびディレクトリに対して要求された処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、セキュリティ レベルの評価後に有効な権限によって判断されます。

- エクスポート (NFS) および共有 (SMB) セキュリティ

エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアント アクセスに適用されます。管理者権限を持つユーザは、SMBクライアントとNFSクライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護ファイルおよびディレクトリ セキュリティ

ストレージレベルのアクセス保護セキュリティは、SVMボリュームへのSMBおよびNFSクライアント アクセスに適用されます。NTFSのアクセス権のみがサポートされています。ONTAPがストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスするUNIXユーザのセキュリティ チェックを行うには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。

- NTFS、UNIX、およびNFSv4のネイティブのファイルレベルのセキュリティ

ストレージ オブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスにSMBとNFSのどちらを使用するかに関係なく有効です。

SAMLによる認証

ONTAPは、リモート ユーザの認証にSecurity Assertion Markup Language (SAML) をサポートしています。いくつかの一般的なアイデンティティ プロバイダ (IdPs) がサポートされています。サポートされているIdPsとSAML認証を有効にする手順の詳細については、"[SAML 認証の設定](#)"を参照してください。

OAuth 2.0とONTAP REST APIクライアント

ONTAP 9.14以降では、Open Authorization (OAuth 2.0) フレームワークがサポートされています。クライアントでREST APIを使用してONTAPにアクセスする場合、認証とアクセス制御には、OAuth 2.0しか使用できません。ただし、その機能を有効にするためには、CLI、System Manager、REST APIなどの任意のONTAP管理インターフェイスを使用できます。

標準的なOAuth 2.0機能に加え、いくつかの一般的な認可サーバーもサポートされています。Mutual TLSに基づく送信者制約付きアクセストークンを使用することで、ONTAPのセキュリティをさらに強化できます。また、自己完結型スコープ、ONTAP RESTロールやローカルユーザー定義との統合など、幅広い認可オプションをご利用いただけます。詳細については、"[ONTAP OAuth 2.0導入の概要](#)"をご覧ください。

管理者認証とRBAC

管理者は、ローカルまたはリモートのログインアカウントを使用して、クラスタおよびSVMへの認証を行います。ロールベース アクセス制御 (RBAC) によって、管理者がアクセスできるコマンドが決定されます。

認証

ローカルまたはリモートのクラスタおよび SVM 管理者アカウントを作成できます：

- ローカル アカウントとは、アカウント情報、公開キー、またはセキュリティ証明書がストレージ システム上に存在するアカウントです。
- リモート アカウントでは、アカウント情報がActive Directoryドメイン コントローラ、LDAPサーバ、またはNISサーバに格納されます。

DNS を除き、ONTAP はクライアントの認証に使用するのと同じネーム サービスを使用して管理者アカウントを認証します。

RBAC

管理者に割り当てられた_ルール_によって、管理者がアクセスできるコマンドが決まります。このルールは、管理者のアカウントを作成する際に割り当てます。必要に応じて、別のルールを割り当てたり、カスタムルールを定義したりすることもできます。

ウイルススキャン

ストレージシステムに統合されたウイルス対策機能を使用することで、ウイルスやその他の悪意のあるコードによるデータの侵害を防ぐことができます。ONTAPウイルススキャン (Vscan) は、業界最高のサードパーティ製ウイルス対策ソフトウェアとONTAP機能を組み合わせることで、スキャンするファイルとそのタイミングを柔軟に制御できます。

ストレージシステムは、サードパーティベンダーのウイルス対策ソフトウェアをホストする外部サーバにスキャン処理をオフロードします。NetAppが提供し、外部サーバにインストールされる_ONTAP Antivirus Connector_が、ストレージシステムとウイルス対策ソフトウェア間の通信を処理します。

- オンアクセススキャンを使用すると、クライアントがSMB経由でファイルを開く、読み込む、名前を変更する、または閉じる際にウイルスチェックを行うことができます。外部サーバからファイルのスキャンステータスが報告されるまで、ファイル操作は一時停止されます。ファイルがすでにスキャンされている場合、ONTAPはファイル操作を許可します。そうでない場合は、サーバにスキャンを要求します。

NFS ではオンアクセス スキャンはサポートされていません。

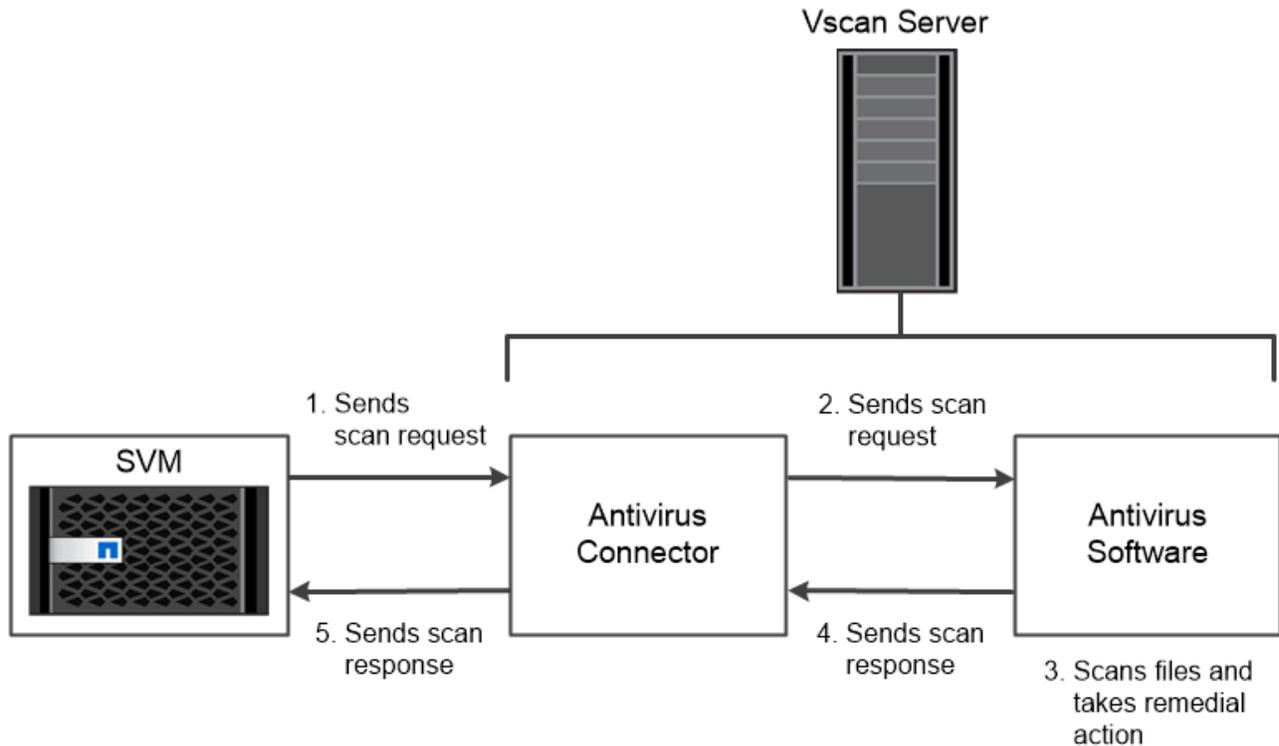
- オンデマンドスキャンを使用すると、ファイルのウイルスチェックを即時またはスケジュールに従って実行できます。例えば、オフピーク時にのみスキャンを実行したい場合などです。外部サーバはチェック済みのファイルのスキャンステータスを更新するため、これらのファイル（変更されていない場合）への次回SMB経由アクセス時のファイルアクセス遅延は通常短縮されます。

オンデマンド スキャンは、NFS経由でのみエクスポートされたボリュームも含め、SVMネームスペース内のすべてのパスに対して使用できます。

一般的には、SVMに対して両方のスキャン モードを有効にします。どちらのモードでも、感染したファイルにはウイルス対策ソフトウェアで設定した処理が実行されます。

災害復旧およびMetroCluster構成におけるウイルススキャン

ディザスタ リカバリ構成およびMetroCluster構成では、ローカル クラスタとパートナー クラスタのそれぞれに対してVscanサーバを個別に設定する必要があります。



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

暗号化

ONTAPは、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られないようにソフトウェアベースとハードウェアベースの暗号化テクノロジーを提供します。

ONTAPは、すべてのSSL接続について連邦情報処理標準（FIPS）140-2に準拠しています。使用可能な暗号化ソリューションは次のとおりです。

- ハードウェアソリューション：

- NetApp Storage Encryption（NSE）

NSEは、自己暗号化ドライブ（SED）を使用するハードウェアソリューションです。

- NVMe SED

ONTAPでは、FIPS 140-2認定を取得していないNVMe SEDに対するフルディスク暗号化が可能です。

- ソフトウェアソリューション：

- NetApp Aggregate Encryption（NAE）

NetApp Aggregate Encryption（NAE）は、アグリゲートごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータボリュームを暗号化できるソフトウェアソリューションです。

- NetApp Volume Encryption (NVE)

NetApp Volume Encryption (NVE) は、ボリュームごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。

ソフトウェア (NAEまたはNVE) とハードウェア (NSEまたはNVMe SED) の両方の暗号化ソリューションを使用することで、保存時の二重暗号化を実現できます。NAEまたはNVE暗号化はストレージ効率に影響を与えません。

NetApp Storage Encryption

NetApp Storage Encryption (NSE) は、データを書き込み時に暗号化するSEDをサポートします。ディスクに格納された暗号化キーがないとデータを読み取ることはできず、その暗号化キーには認証されたノードからしかアクセスできません。

I/O要求を受け取ったノードは、外部キー管理サーバまたはオンボード キー マネージャから取得した認証キーを使用してSEDへの認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードに認証キーを提供します。
- オンボード キー マネージャは組み込みのツールで、データと同じストレージ システムからノードに認証キーを提供します。

NSEでは、HDDとSSDの自己暗号化ディスクをサポートしています。NetApp Volume EncryptionをNSEとともに使用すれば、NSEドライブのデータを二重に暗号化できます。



Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEでは、Flash Cacheモジュール上のデータは暗号化されません。

NVMe自己暗号化ドライブ (SED)

NVMe SED は FIPS 140-2 認定を取得していませんが、これらのディスクは AES 256 ビットの透過的なディスク暗号化を使用して保存データを保護します。

認証キーの生成などのデータ暗号化処理は、内部的に実行されます。認証キーは、ストレージ システムがディスクに初めてアクセスしたときに生成されます。以降、データ処理が要求されるたびにストレージ システム認証が要求されて、ディスク上の保存データが保護されます。

NetApp Aggregate Encryption

NetApp Aggregate Encryption (NAE) は、アグリゲート内のすべてのデータを暗号化するためのソフトウェアベースのテクノロジーです。NAEのメリットは、ボリュームはアグリゲートレベルの重複排除の対象になりませんが、NVEボリュームは除外される点です。

NAEを有効にすると、アグリゲート内のボリュームをアグリゲート キーで暗号化できるようになります。

ONTAP 9.7 以降では、"[NVEライセンス](#)"とオンボードまたは外部のキー管理がある場合、新しく作成されたアグリゲートとボリュームはデフォルトで暗号化されます。

NetApp Volume Encryption

NetApp Volume Encryption (NVE) は、一度に1ボリュームずつ保存データを暗号化するためのソフトウェアベースのテクノロジーです。暗号化キーにはストレージシステムからしかアクセスできないため、基盤のデバイスがシステムから分離されている場合、ボリュームのデータが読み取られることはありません。

スナップショットを含むデータとメタデータは暗号化されています。データへのアクセスは、ボリュームごとに1つずつ、固有のXTS-AES-256キーによって許可されます。内蔵のOnboard Key Managerにより、これらのキーはデータと同じシステム上で安全に保管されます。

NVEは、アグリゲートのタイプ (HDD、SSD、ハイブリッド、アレイLUN) やRAIDタイプを問わず、サポートされるすべてのONTAP環境 (ONTAP Selectを含む) で使用できます。NVEをNetApp Storage Encryption (NSE) とともに使用して、NSEドライブのデータを二重に暗号化することもできます。

KMIP サーバーを使用する場合 オンボード キー マネージャーを使用の方がコストが安く、通常はより便利ですが、次のいずれかに該当する場合は KMIP サーバーを設定する必要があります：

- 連邦情報処理標準 (FIPS) 140-2またはOASIS KMIP標準に準拠した暗号化キー管理ソリューションが必要な場合。
- マルチクラスタ ソリューションが必要な場合。KMIPサーバでは、複数のクラスタにわたる暗号化キーの一元管理がサポートされます。

KMIPサーバでは、複数のクラスタにわたる暗号化キーの一元管理がサポートされます。

- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

KMIPサーバでは、データとは別に認証キーが格納されます。

関連情報

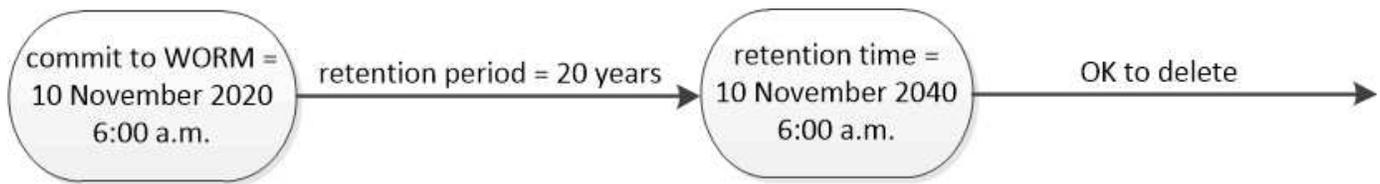
["FAQ - NetApp ボリューム暗号化とNetApp アグリゲート暗号化"](#)

WORMストレージ

`_SnapLock_` は、規制やガバナンスの目的で重要なファイルを変更されていない形式で保持するために `_write once, read many (WORM)_` ストレージを使用する組織向けのハイパフォーマンス コンプライアンスソリューションです。

1つのライセンスでSnapLockを、SEC Rule 17a-4(f)などの外部規制を満たすための厳格な `_コンプライアンスモード_` と、デジタル資産の保護に関する内部規制を満たすためのより緩やかな `_エンタープライズモード_` の両方で使用できます。SnapLockは、改ざん防止機能付きの `_ComplianceClock_` を使用して、WORMファイルの保存期間が経過したかどうかを判断します。

SnapLock for SnapVault を使用すると、セカンダリ ストレージ上のスナップショットを WORM 保護できます。SnapMirror を使用すると、災害復旧などの目的で、WORM ファイルを別の地理的な場所に複製できます。



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAPとVMware vSphere

ONTAPおよび関連するNetApp製品をVMware vSphereに統合できます。お使いのテクノロジー環境やビジネス ニーズに応じた、いくつかのオプションが用意されています。

主な概念と用語

VMware環境でのONTAPおよび関連するNetApp製品の使用方法を確認するにあたり、最初に理解しておく役立ついくつかの主な用語と概念を以下に記載します。

論理ユニット番号

LUNは、ストレージ エリア ネットワーク (SAN) 内の_論理ユニット_を識別するために使用される番号です。これらのアドレス指定可能なデバイスは、通常、Small Computer System Interface (SCSI) プロトコルまたはそのカプセル化された派生プロトコルを介してアクセスされる論理ディスクです。

VMware vSphere仮想ボリューム

仮想ボリューム (vVol) は、仮想マシンで使用されるストレージをボリュームレベルで抽象化します。これにはいくつかの利点があり、従来のLUNの代わりに使用できます。

永続的予約

永続的予約はSCSI-3でサポートされ、以前のSCSI-2予約よりも強化されています。これにより、複数のクライアント イニシエータが1つのターゲットと通信しながら、他のノードをロックアウトできます。エラーリカバリのためにバスがリセットされた場合でも、予約は維持できます。



ONTAP 9.15.1以降では、SCSI-3を使用して仮想ボリュームの永続的予約を作成できます。この機能は、Windows Serverフェイルオーバー クラスタ (WSFC) でONTAP Tools for VMware vSphere 9を使用する場合にのみサポートされます。

Windows Serverフェイルオーバー クラスタリング

Microsoft Windows Serverフェイルオーバー クラスタリング (WSFC) は、フォールトトレランスと高可用性を提供するWindows Serverオペレーティング システムの機能です。一連の (物理または仮想) サーバノードをクラスタとして統合することにより、障害発生時の耐障害性を確保します。WSFCは、一般にデータベース サーバ、ファイル サーバ、ネームスペース サーバなどのインフラ サービスを導入するために使用されます。

VMware vSphere Storage API - Storage Awareness

VASAは、ストレージレイとvCenterの管理・運用を統合するAPIセットです。このアーキテクチャは、VMware vSphereとストレージシステム間の通信を処理する_VASA Provider_を含む複数のコンポーネントに基づいています。ONTAPでは、このProviderはONTAP tools for VMware vSphereの一部として実装

されています。

VMware vSphere Storage APIs - Array Integration

VMware vSphere Storage API – Array Integration (VAAI) は、VMware vSphere ESXiホストとストレージデバイス間の通信を可能にする一連のAPIです。このAPIには、ストレージ処理をアレイにオフロードするためにホストが使用する一連の基本処理が含まれています。VAAIは、ストレージを大量に消費するタスクのパフォーマンスを大幅に向上させることができます。

NetApp SnapCenter

SnapCenterは、ONTAPストレージシステムを使用するアプリケーション、データベース、ホスト ファイルシステム、仮想マシンのデータ保護を提供する、一元化されたスケーラブルなプラットフォームです。SnapshotやSnapRestore、FlexClone、SnapMirror、SnapVaultなどのONTAPネイティブテクノロジーを活用します。

NetAppプラグインと関連テクノロジー

NetAppは、ONTAPおよび関連製品をVMware vSphereテクノロジーと統合するための堅牢なサポートを提供します。

ONTAP tools for VMware vSphere

ONTAP Tools for VMware vSphereは、ONTAPとvSphereを統合するための一連のツールです。VASA APIフレームワークのプロバイダ機能を実装します。ONTAP Toolsには、vCenterプラグイン、VMware Site Recovery Manager用のStorage Replication Adapter (SRA)、自動化アプリケーションの構築に使用できるREST APIサーバーも含まれています。

NFS Plug-In for VMware VAAI

NetApp NFS Plug-In for VMware VAAIでは、VAAI機能にアクセスできます。このプラグインはESXiホストにインストールできるため、ホストがONTAP上のNFSデータストアでVAAIを活用できます。クローニング、スペース リザベーション、Snapshotのオフロードなど、複数の処理を実行できます。

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) は、ディザスタ リカバリ機能を提供します。SRMは、ONTAP Tools for VMware vSphereと統合されているため、ONTAPのデータ管理機能にアクセスして活用できます。

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) は、_ストレッチ クラスタ_環境でvSphereを実現し、サポートするテクノロジーです。vMSCソリューションは、NetApp MetroClusterおよびSnapMirror active sync (旧称SMBC) でサポートされています。これらのソリューションは、ドメイン障害が発生した場合のビジネス継続性を強化します。回復力モデルは、お客様固有の構成の選択に基づいています。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere (SCV) は、SnapCenterサーバーと一緒に導入することも、スタンドアロンアプリケーションとして導入することもできるLinuxベースの仮想アプライアンスです。どちらの場合も、SCVはVM、データストア、VMDKのバックアップ処理とリストア処理を提供します。各処理は高速でスペース効率に優れ、クラッシュ整合性、VM整合性を備えています。

追加情報へのアクセス

VMware vSphere環境にONTAPを導入するための準備に役立つその他のリソースがいくつか用意されています。

- ["ONTAP tools for VMware vSphereのドキュメント"](#)
- ["エンタープライズ アプリケーション：VMware vSphereとONTAP"](#)
- ["NetApp KB：SCSI 予約と SCSI 永続予約とは何ですか？"](#)
- ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)

FabricPool

多くのNetAppのお客様は、めったにアクセスされない大量のデータを保有しています。これを_コールド_データと呼んでいます。また、頻繁にアクセスされるデータを_ホット_データと呼んでいます。理想的には、最高のパフォーマンスを得るために、ホットデータを最速のストレージに保存する必要があります。コールド データは、必要に応じてすぐに利用できる限り、低速のストレージに移動できます。しかし、データのどの部分がホットで、どの部分がコールドなのかをどのように判断すればよいのでしょうか。

FabricPoolは、アクセス パターンに基づいて、ハイパフォーマンスのローカル階層とクラウド階層の間でデータを自動的に移動するONTAPの機能です。階層化により、高価なローカル ストレージをホット データ用に解放し、コールド データはクラウド内の低コストのオブジェクト ストレージからいつでもアクセスできるようになります。FabricPoolは、データ アクセスを常に監視し、階層間でデータを移動することで、最高のパフォーマンスと最大限のコスト削減を実現します。

FabricPoolを使用してコールド データをクラウドに階層化する方法は、クラウドを効率化してハイブリッドクラウド環境を構築する最も簡単な方法の1つです。FabricPoolはストレージ ブロック レベルで機能するため、ファイル データとLUNデータの両方に対応できます。

しかし、FabricPoolはオンプレミスデータをクラウドに階層化するだけではありません。多くのお客様は、Cloud Volumes ONTAPでFabricPoolを使用して、高価なクラウド ストレージからクラウド プロバイダ内の低コストのオブジェクト ストレージにコールド データを階層化しています。ONTAP 9.8以降では、"[ファイルシステム分析](#)"または"[温度に敏感なストレージ効率](#)"を使用して、FabricPool対応ボリュームの分析情報を取得できます。

データを使用するアプリケーションは、データが階層化されていることを認識しないため、アプリケーションに変更を加える必要はありません。階層化は完全に自動化されているため、継続的な管理は不要です。

コールド データは、主要なクラウド プロバイダが提供するオブジェクト ストレージに格納できます。また、NetApp StorageGRIDを使用してコールド データを自社のプライベート クラウドに保管すれば、データを完全に制御しながら最大限のパフォーマンスを実現できます。

関連情報

["ONTAP System ManagerのFabricPool関連ドキュメント"](#)

["NetApp Cloud Tiering"](#)

["NetApp TechComm TVのFabricPool関連ビデオ"](#)

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。