



ONTAPの概念

ONTAP 9

NetApp
December 20, 2024

目次

ONTAPの概念	1
ONTAPプラットフォーム	1
ONTAPユーザインターフェイス	2
クラスタストレージ	3
ハイアベイラビリティペア	4
AutoSupportとデジタルアドバイザ	5
ネットワークアーキテクチャ	6
クライアントプロトコル	10
ディスクとアグリゲート	11
ボリューム、qtree、ファイル、LUN	18
ストレージ仮想化	19
パスのフェイルオーバー	23
ロードバランシング	26
レプリケーション	29
Storage Efficiency	36
セキュリティ	47
ONTAPとVMware vSphere	53
アプリケーション対応のデータ管理	55
FabricPool	56

ONTAPの概念

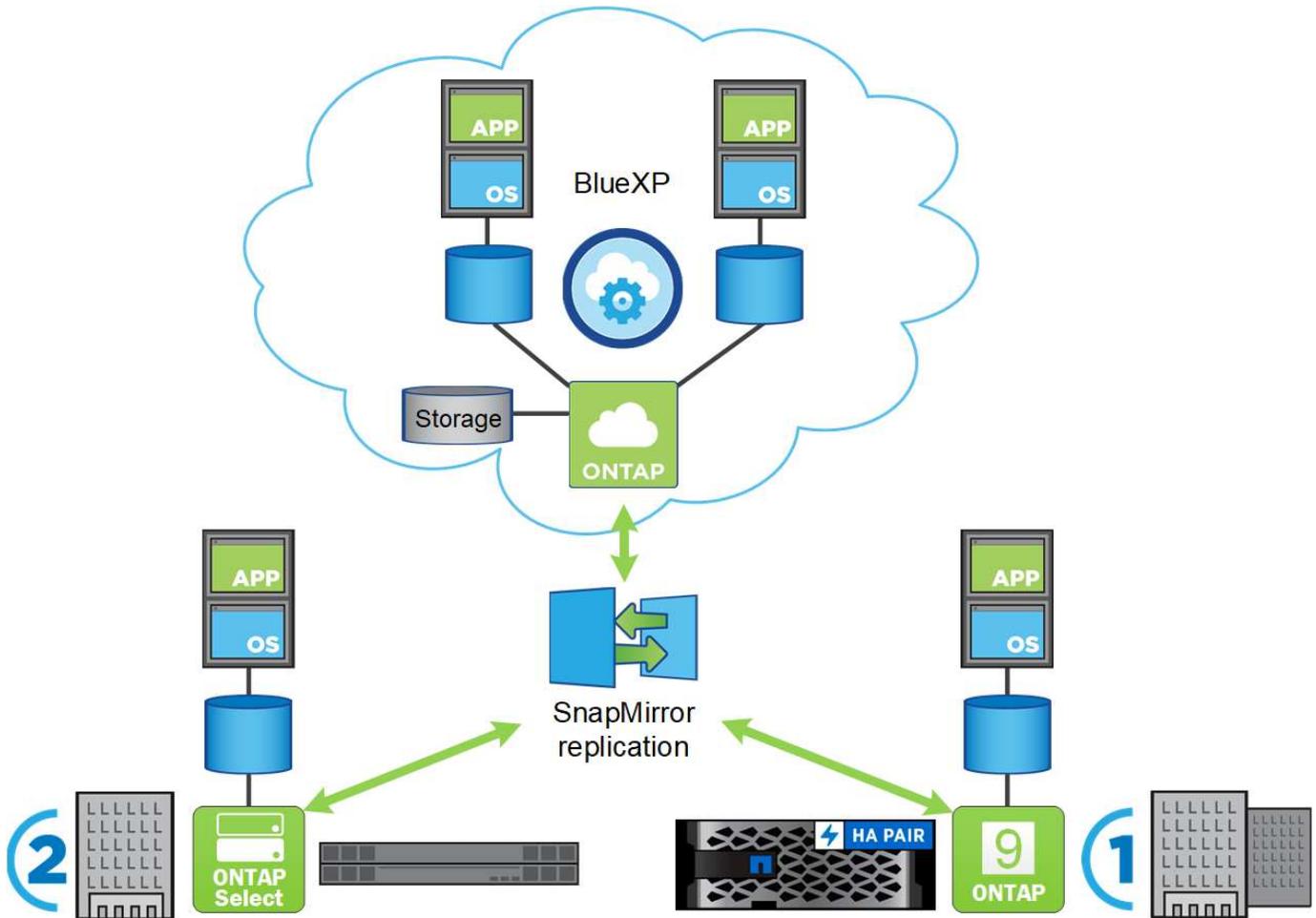
ONTAPプラットフォーム

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の読み取りと書き込みを行う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。高速フラッシュから低価格の回転式メディア、クラウドベースのオブジェクトストレージまで、さまざまなストレージ構成が用意されています。

ONTAPの実装は次の環境で実行されます。

- ネットアップの既成システム： "FASハイブリッドフラッシュシステム、オールフラッシュFAS (AFF) AシリーズとCシリーズ、オールフラッシュSANアレイ (ASA) プラットフォーム"
- コモディティハードウェア： "ONTAP Select"
- プライベートクラウド、パブリッククラウド、ハイブリッドクラウド： "Cloud Volumes ONTAP"、 "NetApp ONTAP 対応の Amazon FSX" "Azure NetApp Files"、 "Google Cloud NetAppボリューム"
- 業界最高のコンバードインフラを提供する特殊な実装 "FlexPod データセンター"

これらの実装を組み合わせることで、_ ネットアップデータファブリックの基本的なフレームワークが形作られます。_ は、共通のソフトウェア定義型アプローチでデータを管理し、プラットフォーム間で高速かつ効率的なレプリケーションを実現します。



ONTAP ユーザーインターフェイス

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。これらのインターフェイスオプションを使用すると、さまざまなレベルのアクセスや機能を提供し、環境に応じてONTAPクラスタを柔軟に管理できます。

これらのインターフェイスのいずれかを使用して、ONTAPクラスタの管理やデータ管理処理を実行できます。

ONTAPシステムマネージャ

ONTAP System Managerは、Webベースのユーザーインターフェイスで、シンプルでわかりやすい方法でクラスタを管理します。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などの一般的な操作を管理できます。System Managerでは、リスクとクラスタのパフォーマンスを監視し、クラスタの問題に対処して問題を未然に先回りするのに役立つ分析情報も提供されます。["詳細"](#)です。

ONTAP 9.7は、ONTAP System Managerにとって重要なジャンクションとなりました。このリリースでは、NetAppからONTAP System Managerの2つのバージョンが提供され、ONTAP 9.7より前のバージョンに加えて、設計が刷新され、より合理的でわかりやすいバージョンが導入されました。ONTAP 9.7以降、再設計されたバージョンはONTAPシステムマネージャとして引き継がれ、旧バージョンはSystem Managerクラシックに名称が変更された。System Manager Classicの最終更新はONTAP 9.7で行われました。System Manager Classicを使用している場合は、そのドキュメントを参照["別々に"](#)できます。

BlueXP

ONTAP 9.12.1以降では、BlueXPのWebベースのインターフェイスを使用して、使い慣れたSystem Manager ダッシュボードを使用しながら、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。BlueXPでは、クラウドストレージ（Cloud Volumes ONTAPなど）の作成と管理、ネットアップのデータサービス（Cloud Backupなど）の使用、多くのオンプレミスストレージデバイスやエッジストレージデバイスの制御を行うことができます。オンプレミスのONTAPシステムをBlueXP に追加すると、すべてのストレージとデータ資産を単一のインターフェイスから管理できるようになります。 ["詳細"](#)です。

ONTAPコマンドラインインターフェイス

は、["ONTAPコマンドラインインターフェイス \(CLI\)"](#) クラスタ、ノード、SVMなどをを使用して操作できるテキストベースのインターフェイスです ["コマンド"](#)。CLIコマンドはに基づいて使用でき ["ロールタイプ"](#) 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、プログラムを使用してクラスタ処理を管理および自動化できるRESTful APIにアクセスできます。APIを使用して、ボリューム、Snapshot、アグリゲートの作成と管理、クラスタのパフォーマンスの監視など、ONTAPのさまざまな管理タスクを実行します。ONTAP REST APIには、curlなどのユーティリティを使用するか、Python、PowerShell、Javaなど、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直接アクセスできます。 ["詳細"](#)です。



ONTAPIは、ONTAP REST APIに先行する独自のONTAP APIです。ONTAPIインターフェイスは、ONTAPの今後のバージョンでは無効になる予定です。ONTAPIを使用している場合は、を計画する必要があります ["ONTAP REST APIへの移行"](#)。

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、自動化コードの作成を容易にする特定の開発言語および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"](#)です。

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および展開できます。 ["詳細"](#)です。

クラスタストレージ

ONTAPの現在のバージョンは、もともとはネットアップのスケールアウトクラスタストレージアーキテクチャ用に開発されたものです。これは、ONTAPのデータセンター実装で一般的に使用さ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テクノロジーを構成する概念の理解から始めることをお勧めします。

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FASコントローラまたはAFFコントローラを導入します。各コントローラとそのストレージ、ネットワーク接続、およびコントローラで実行されているONTAPのインスタンスを合わせて、*node* と呼びます

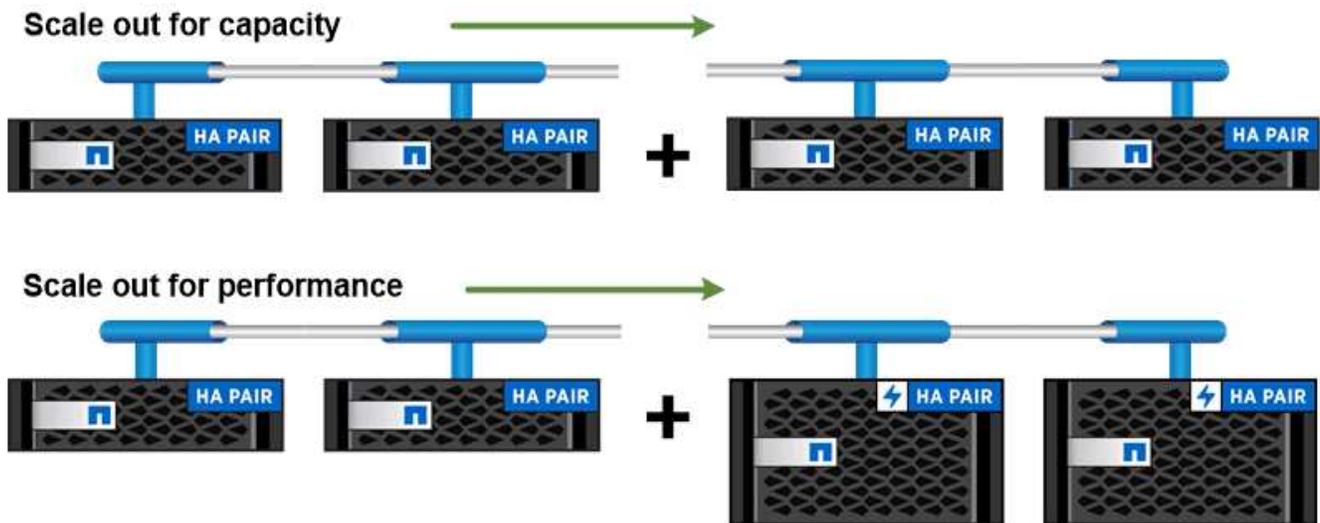
ノードはハイアベイラビリティ（HA）用にペアリングされます。これらのペア（SANの場合は最大12ノード、NASの場合は最大24ノード）を合わせてクラスタを構成します。ノードは、専用のプライベートクラス

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。物理ストレージおよびネットワーク接続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レイモデルは同じでなければなりません。それ以外の場合は、サポートされている任意のコントローラを組み合わせで使用できます。スケールアウトできるのは、同等のストレージレイモデルを使用するノードを追加して容量を増やすか、ハイエンドのストレージレイを使用するノードを追加してパフォーマンスを高めることです。

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ノンストップオペレーションを実現するために、`_high-availability (HA) ペア` で構成されます。ノードに障害が発生した場合や定期的な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、パートナーはそのストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったときに、`partner_ギブバック_storage` を提供します。

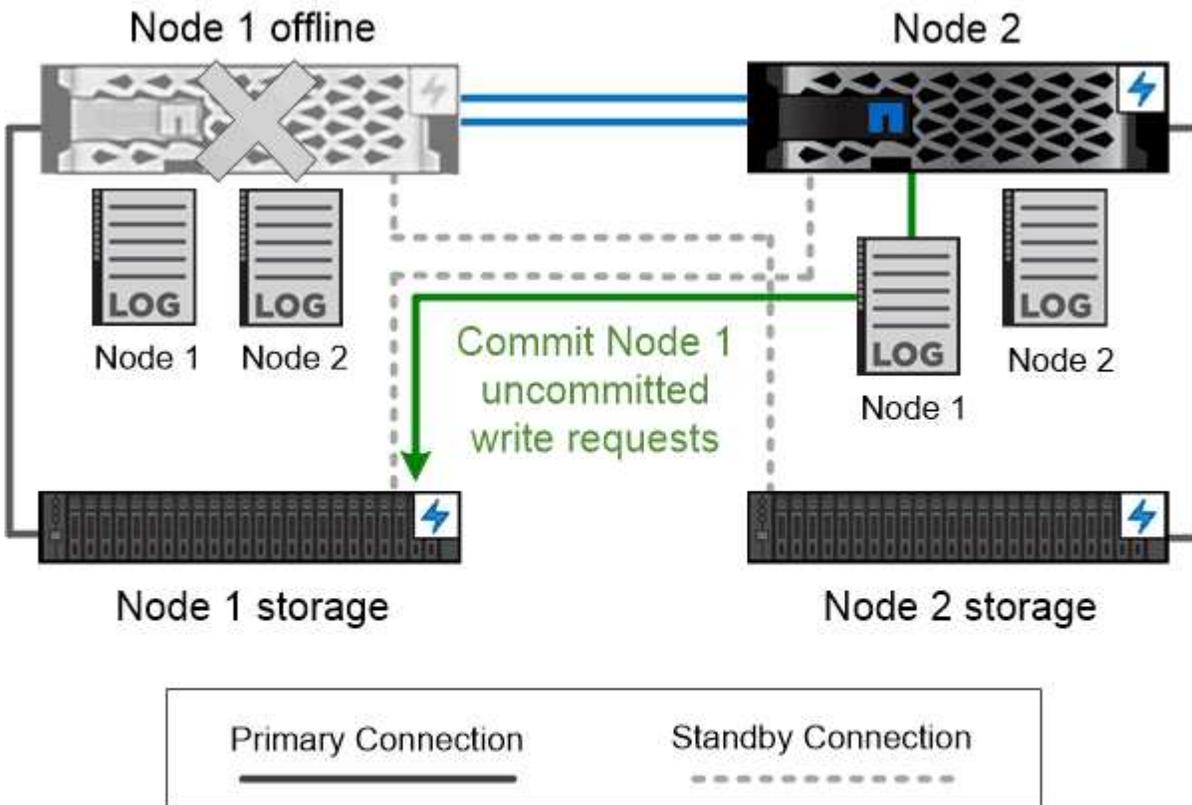
HAペアは、必ず同じようなコントローラモデルで構成されます。通常、コントローラは冗長電源装置を備えた同じシャーシに配置されます。

HAペアはフォールトトレラントなノードであり、さまざまな方法で相互に通信できます。各ノードでは、パートナーの動作を継続的に確認したり、パートナーの不揮発性メモリのログデータをミラーリングしたりできます。あるノードへの書き込み要求が行われると、両方のノードでNVRAMにログインしてから、クライアントまたはホストに応答が返されます。フェイルオーバー時には、障害が発生したノードのコミットされていない書き込み要求が稼働しているパートナーによってディスクにコミットされ、データの整合性が確保されま

す。

もう一方のコントローラのストレージメディアへの接続により、テイクオーバー時に各ノードがもう一方のストレージにアクセスできるようになります。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できます。

可用性を確保するには、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、どちらかの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つのノードに設定できるNAS仮想ネットワークインターフェイスの最大数の50%を超えないようにすることもできます。



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

* _ 仮想 ONTAP 実装でのテイクオーバーとギブバック _ *

ONTAP Select for AWS や Cloud Volumes ONTAP のような仮想化された「不要な」ONTAP 環境では、ノード間でストレージが共有されません。ノードが停止した場合、そのノードのデータの同期ミラーリングされたコピーからパートナーがデータの提供を継続します。ノードのストレージはテイクオーバーされず、データ提供機能のみがテイクオーバーされます。

AutoSupportとデジタルアドバイザー

ONTAP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コンポーネントは、Active IQデジタル

アドバイザー（デジタルアドバイザーとも呼ばれる）によって分析されるテレメトリを送信します。

Digital Advisorは、クラウドベースのポータルとモバイルアプリを通じて、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にわたってデータインフラを最適化します。SupportEdgeと有効な契約を結んでいるNetAppのすべてのお客様が、デジタルアドバイザーによるデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Digital Advisorでできることは次のとおりです。

- 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コンポーネント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します。デジタルアドバイザーのダッシュボードが健全性に関する問題を報告し、問題の修正を支援します。システム容量を監視して、ストレージスペースが不足しないようにします。
- パフォーマンスの管理Digital Advisorでは、System Managerよりも長い期間の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している構成やシステムの問題を特定します。
- 効率を最大化Storage Efficiencyの指標を表示し、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します。Digital Advisorは、完全な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を表示します。サービス契約の有効期限を確認して、サポート期間を維持できます。

関連情報

["NetAppのドキュメント：デジタルアドバイザー"](#)

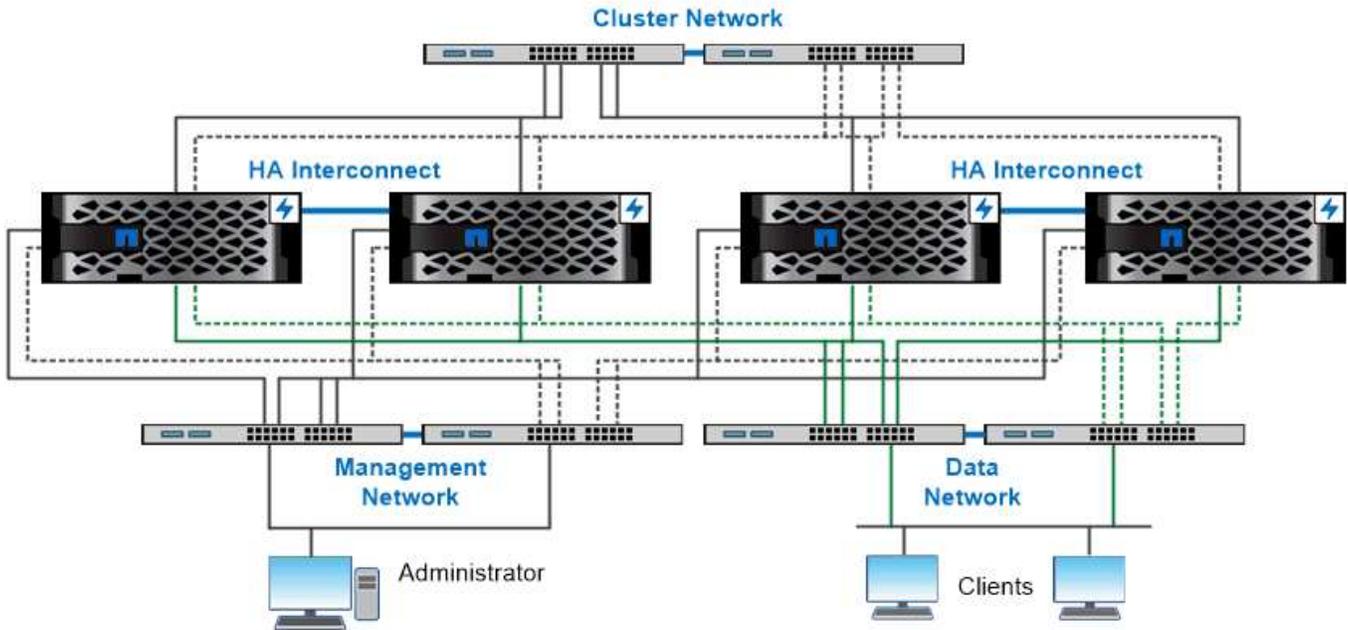
["Digital Advisorを起動"](#)

["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の概要

通常、ONTAPデータセンター実装の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。NIC（ネットワークインターフェイスカード）は、イーサネット接続用の物理ポートを提供します。HBA（ホストバスアダプタ）は、FC接続用の物理ポートを提供します。



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

各ノードに搭載されている物理ポートに加え、logical ports 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イスグループまたはVLANです。

インターフェイスグループ

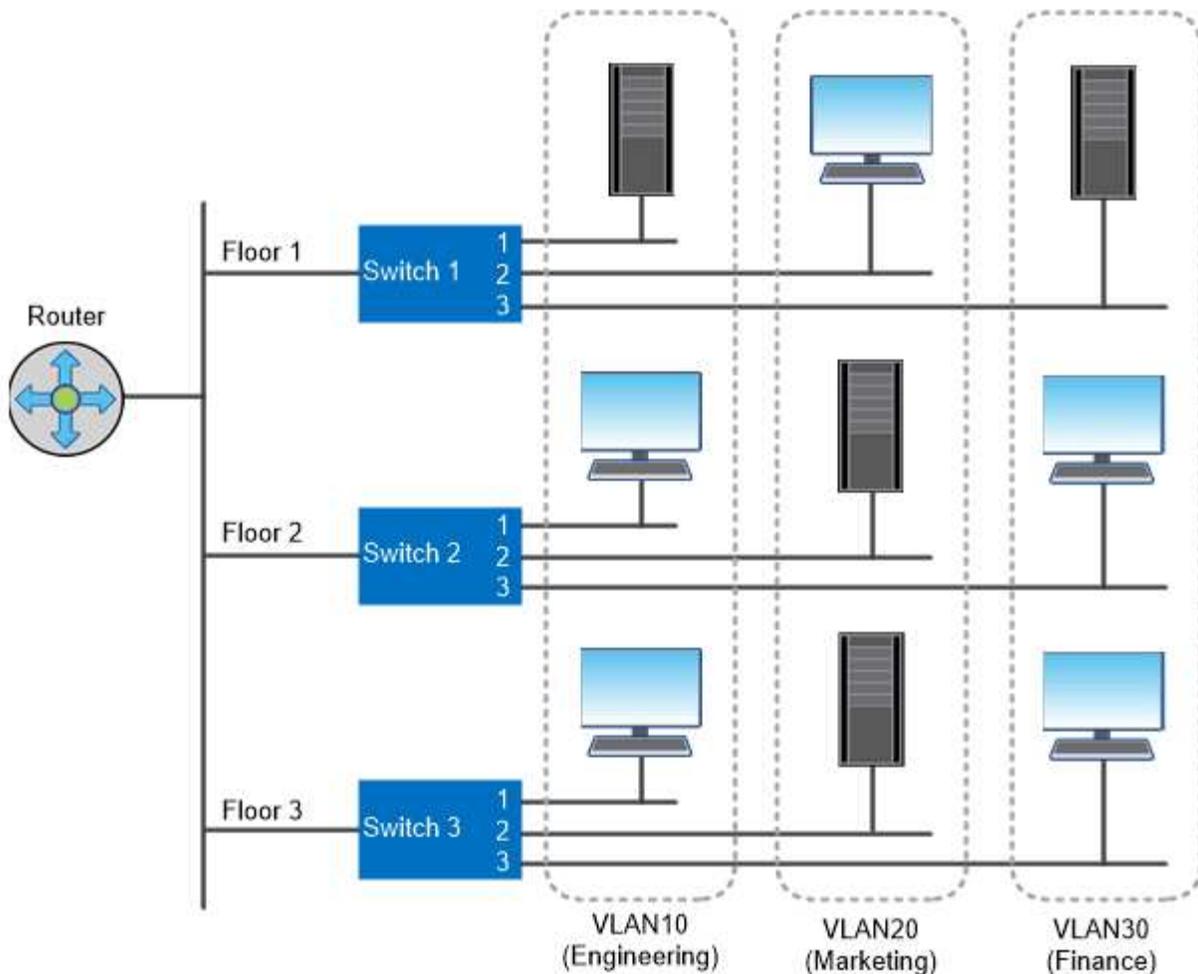
インターフェイスグループ 複数の物理ポートを1つの論理「トランクポート」に結合します。1つのスロットで障害が発生してビジネスクリティカルなトラフィックが停止しないようにするには、異なるPCIスロットのNICのポートで構成されるインターフェイスグループを作成します。

インターフェイスグループには、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があります。各モードでは、フォールトトレランスのレベルが異なります。どちらのタイプのマルチモードインターフェイスグループも、ネットワークトラフィックの負荷分散に使用できます。

VLAN

VLAN ネットワークポート（インターフェイスグループ）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に基づいて定義された論理セグメントに分離します。VLAN に属する end-stations 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。

エンドステーションは、エンジニアリングやマーケティングなどの部門ごと、またはrelease1やrelease2などのプロジェクトごとにグループ化できます。VLANではエンドステーションの物理的な近接性は無関係であるため、エンドステーションは地理的に離れた場所に配置できます。



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、すべての主要な業界標準ネットワークテクノロジーをサポートしています。主なテクノロジーには、IPspace、DNSロードバランシング、SNMPトラップなどがあります。

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、を[NASパスのフェイルオーバー](#)参照してください。

IPspace

IPspace を使用すると、クラスタ内の仮想データサーバごとに個別の IP アドレススペースを作成できます。これにより、管理上分離された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アドレスを使用してクラスタデータにアクセスできます。

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ロトハランシク

DNS ロードバランシング_を使用すると、使用可能なポートにユーザネットワークトラフィックを分散できます。DNSサーバは、インターフェイ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イスを動的に選択します。

SNMPトラツフ

SNMP トラップ_を使用すると、しきい値または障害を定期的にチェックできます。SNMPトラップは、SNMPエージェントからSNMPマネージャに非同期で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接続で連邦情報処理標準（FIPS）140-2に準拠しています。SSL FIPSモードをオンまたはオフにしたり、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、サポート対象のNVIDIA GPUを搭載したホストで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設定できます"[NFS over RDMA](#)"。

RDMA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は、レイテンシを低減し、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。

X1151AクラスタNICを使用する場合、ONTAP 9.10.1以降では、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。X91153A NICでは、ONTAP 9.13.1以降でクラスタインターコネクトRDMAもサポートされます。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 A400• ASA A400	ONTAP 9.10.1以降
<ul style="list-style-type: none">• AFF A900用• ASA A900• FAS9500	ONTAP 9.13.1以降

ストレージシステムが適切にセットアップされていれば、追加の設定をしなくてもRDMAインターコネクト

を使用できます。

クライアントプロトコル

ONTAPは、業界標準の主要なクライアントプロトコル（NFS、SMB、FC、FCoE、iSCSI、NVMe、S3、

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形式のアクセス権、NTFS形式のアクセス権、またはその両方を組み合わせて制御できます。

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

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、権限形式の混在もサポートされています。

SMB 1.0も使用できますが、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、ネットワークに接続され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プロトコルでは、専用のFCネットワークと専用のFCスイッチを使用するため、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。

LUNは仮想ディスクを表し、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、それらのクライアントが書き込みの競合を防止するクラスタに属している場合のみです。

FCoE

FCoEはFCと基本的に同じプロトコルですが、従来のFCトランスポート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特別に設計された最新のブロックプロトコルです。スケーラブルなセッションを提供し、レイテンシの大幅な低減と並列処理能力の向上を実現するため、インメモリデータベースや分析など、低レイテンシで高スループットの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、S3バケットを使用してオブジェクトストレージにデータを提供できるようになりました。

ONTAPでは、S3オブジェクトストレージを提供する次の2つのオンプレミスユースケースシナリオがサポートされています。

- FabricPool階層をローカルクラスタのバケット（ローカルバケットへの階層化）またはリモートクラスタ（クラウド階層）に移動します。
- 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S3クライアントアプリケーションアクセス。



ONTAP S3は、既存のクラスタで追加のハードウェアや管理作業を行わずにS3機能を利用する場合に適しています。300TBを超える環境では、引き続きNetApp StorageGRIDソフトウェアがNetAppのオブジェクトストレージ向け主力ソリューションとなります。詳細はこちらをご覧ください "[StorageGRID](#)"。

ディスクとアグリゲート

ディスクとローカル階層（アグリゲート）の概要

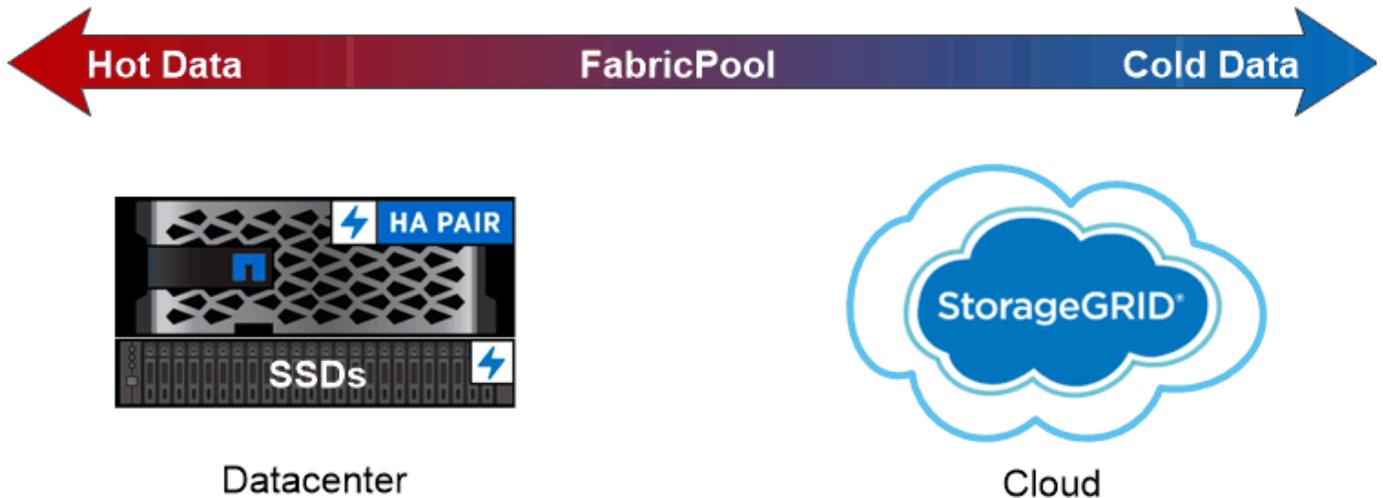
ONTAP物理ストレージは、System ManagerとCLIを使用して管理できます。ローカル階層（アグリゲート）の作成、拡張、管理、Flash Poolローカル階層（アグリゲート）の使用、ディスクの管理、およびRAIDポリシーの管理を行うことができます。

ローカル階層（アグリゲート）とは

ローカル階層（別名「_Aggregates」）は、ノードで管理されるディスクのコンテナです。ローカル階層を使用すると、パフォーマンス要件が異なるワークロードを分離したり、アクセスパターンが異なるデータを階層化したり、規制要件に準拠するためにデータを分離したりできます。

- レイテンシを最小限に抑え、パフォーマンスを最大限に高める必要があるビジネスクリティカルなアプリケーションの場合は、SSDのみで構成されるローカル階層を作成します。

- アクセスパターンに応じてデータを階層化する場合は、_hybrid local tier_を作成し、作業データセットにはフラッシュを導入して高性能なキャッシュを利用しながら、アクセス頻度が低いデータには低コストのHDDやオブジェクトストレージを使用することができます。
 - a_Flash Poolは、SSDとHDDの両方で構成されます。
 - a_ssd FabricPool_は、オブジェクトストアが接続されたオールSSDローカル階層で構成されています。
- 規制要件に準拠するためにアクティブなデータからアーカイブデータを分離する必要がある場合は、大容量HDDまたはパフォーマンス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。



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.

ローカル階層（アグリゲート）の使用

次のタスクを実行できます。

- ["ローカル階層（アグリゲート）の管理"](#)
- ["ディスクの管理"](#)
- ["RAID構成の管理"](#)
- ["Flash Pool階層の管理"](#)

次の条件に該当する場合は、これらのタスクを実行します。

- 自動スクリプトツールを使用しない。
- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- MetroCluster構成を使用しており、ドキュメントの初期設定手順およびローカル階層（アグリゲート）とディスクの管理に関するガイドラインに従っている["MetroCluster"](#)。

関連情報

- ["FabricPoolクラウド階層の管理"](#)

ローカル階層（アグリゲート）とRAIDグループ

最新のRAIDテクノロジーは、障害が発生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て'消失したデータを再構築しますダウンタイムや多大なパフォーマンス・コストは発生しません

ローカル階層（アグリゲート）は、1つ以上の RAIDグループ で構成されます。ローカル階層の RAIDタイプ は、RAIDグループ内のパリティディスクの数、およびRAID構成で保護される同時ディスク障害の数を決定します。

デフォルトのRAIDタイプであるRAID-DP（RAID-ダブルパリティ）は、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た場合にデータ損失から保護されます。RAID-DPの推奨RAIDグループサイズは、HDD 12~20本、SSD 20~28本です。

サイジングに関する推奨事項の上位にRAIDグループを作成することで、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。これは特に、容量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グループのリビルド時間が長くなるなどの相反する要因のバランスを取る必要があります。

ミラーされたローカル階層とミラーされていないローカル階層（アグリゲート）

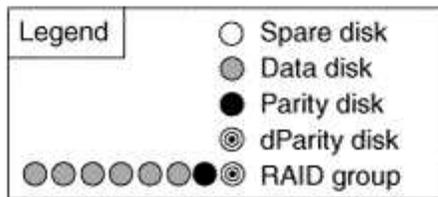
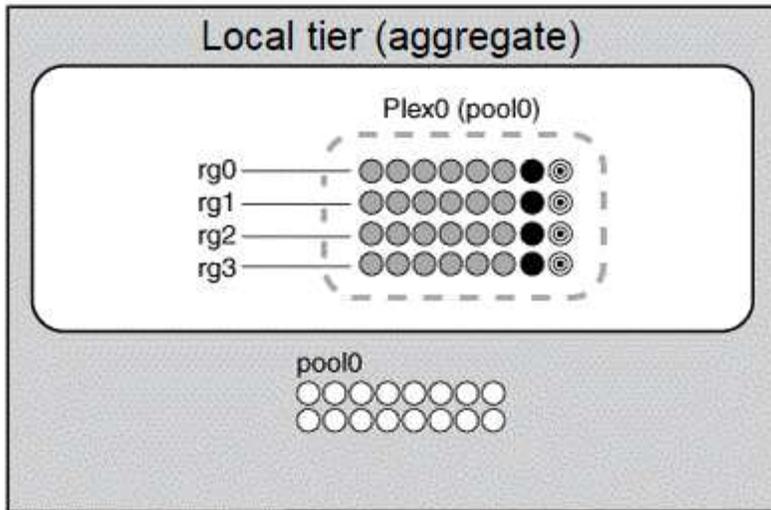
ONTAP には、SyncMirror というオプション機能があります。この機能を使用すると、コピー内のローカル階層（アグリゲート）データまたはプレックスを同期的にミラーリングし、別々のRAIDグループに格納することができます。プレックスを使用すると、RAIDタイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や、RAIDグループのディスクへの接続が失われた場合でも、データ損失を防ぐことができます。

System ManagerまたはCLIを使用してローカル階層を作成するときに、ローカル階層をミラーするかどうかを指定できます。

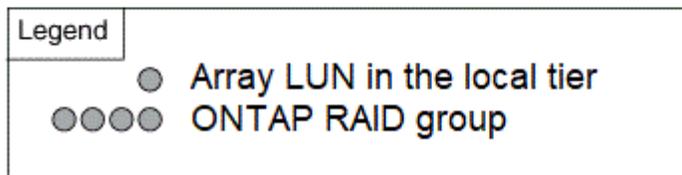
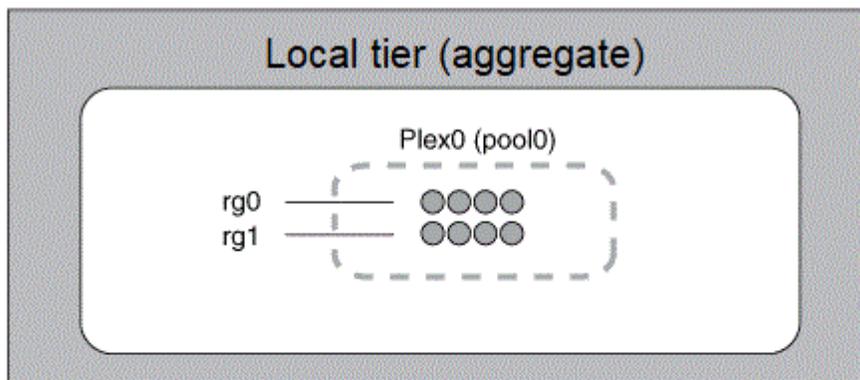
ミラーされていないローカル階層（アグリゲート）の仕組み

ローカル階層をミラーするように指定しない場合、ミラーされていないローカル階層（アグリゲート）として作成されます。ミラーされていないローカル階層には、プレックス_（データのコピー）が1つだけ含まれ、このローカル階層に属するすべてのRAIDグループが含まれます。

次の図は、1つのプレックスを含む、ディスクで構成されるミラーされていないローカル階層を示しています。ローカル階層には、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本のデータディスク、1本のパリティディスク、および1本のdparity（ダブルパリティ）ディスクがあります。ローカル階層で使用されるすべてのディスクは'同じプールであるpool0から提供されます



次の図は、1つのプレックスを含む、アレイLUNで構成されるミラーされていないローカル階層を示しています。このノードには、rg0とrg1の2つのRAIDグループがあります。ローカル階層で使用されるすべてのアレイLUNは同じプールであるpool0から提供されます



ミラーされたローカル階層（アグリゲート）の機能

ミラーされたアグリゲートには、2_bプレックス（データコピー）があります。これらのアグリゲートでは、SyncMirror機能を使用してデータを複製し、冗長性を確保します。

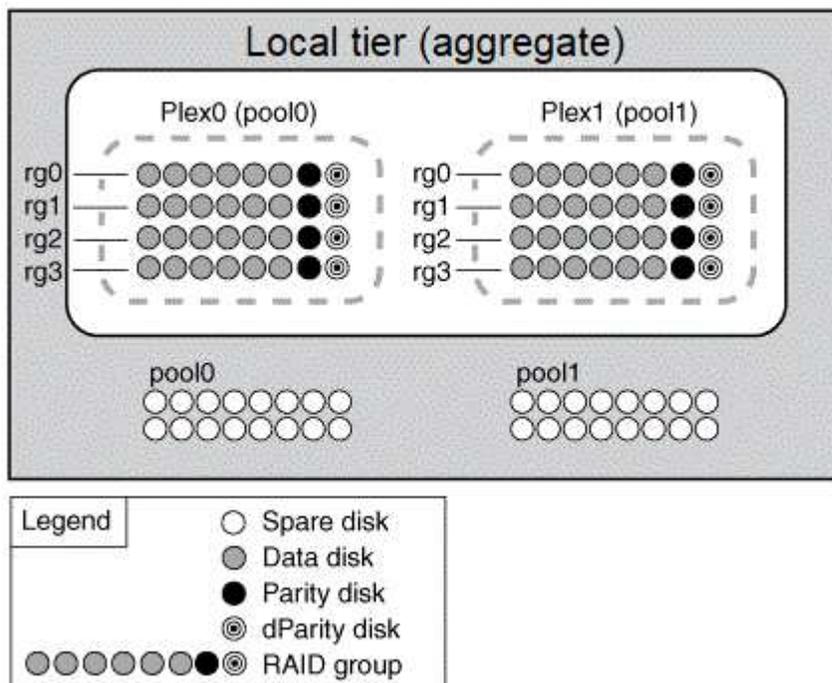
ローカル階層を作成するときに、ミラーされたローカル階層として指定できます。また、ミラーされていない既存のローカル階層に2つ目のプレックスを追加して、ミラーされた階層にすることもできます。SyncMirror機能を使用すると、ONTAPは元のプレックス（plex0）のデータを新しいプレックス（plex1）にコピーしま

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グループと独自のプールがあります）、同時に更新されます。

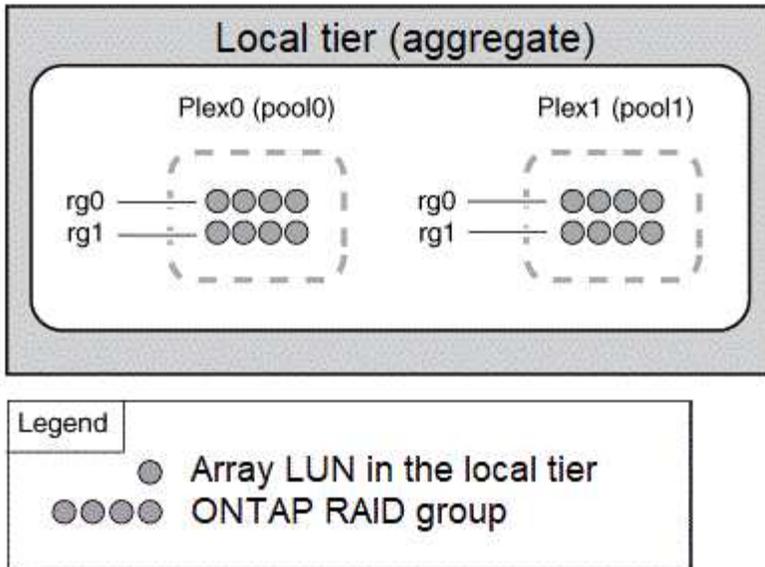
この構成では、アグリゲートのRAIDレベルで保護されるディスク数よりも多くのディスクで障害が発生した場合や接続が切断された場合に、障害の原因を修正しながら影響を受けないプレックスがデータの提供を継続するため、データ損失に対する保護が強化されます。問題のあるプレックスが修正されると、2つのプレックスが再同期され、ミラー関係が再確立されます。

システム上のディスクとアレイルUNはpool0とpool1という2つのプールに分かれています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機能を有効にして実装したディスクで構成されるローカル階層を示しています。ローカル階層「plex1」用に2つ目のプレックスが作成されました。plex1のデータはplex0のデータのコピーであり、RAIDグループも同じです。各プールに16本のディスクを使用して、32本のスペアディスクがpool0またはpool1に割り当てられます。



次の図は、SyncMirror機能を有効にして実装したアレイルUNで構成されるローカル階層を示しています。ローカル階層「plex1」用に2つ目のプレックスが作成されました。plex1はplex0のコピーであり、RAIDグループも同じです。



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、ミラーアグリゲートでは少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、パフォーマンスに悪影響を及ぼす可能性があります。

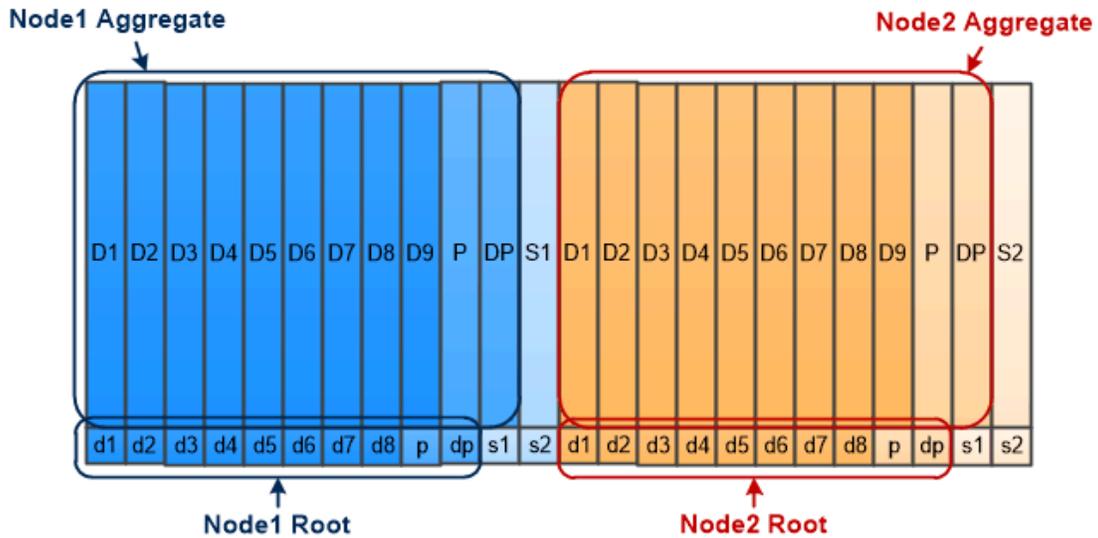
ルート/データパーティショニング

すべてのノードに、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と同じです。

System Managerでは、ルート/データパーティショニングとルート/データ/データパーティショニングはサポートされません。

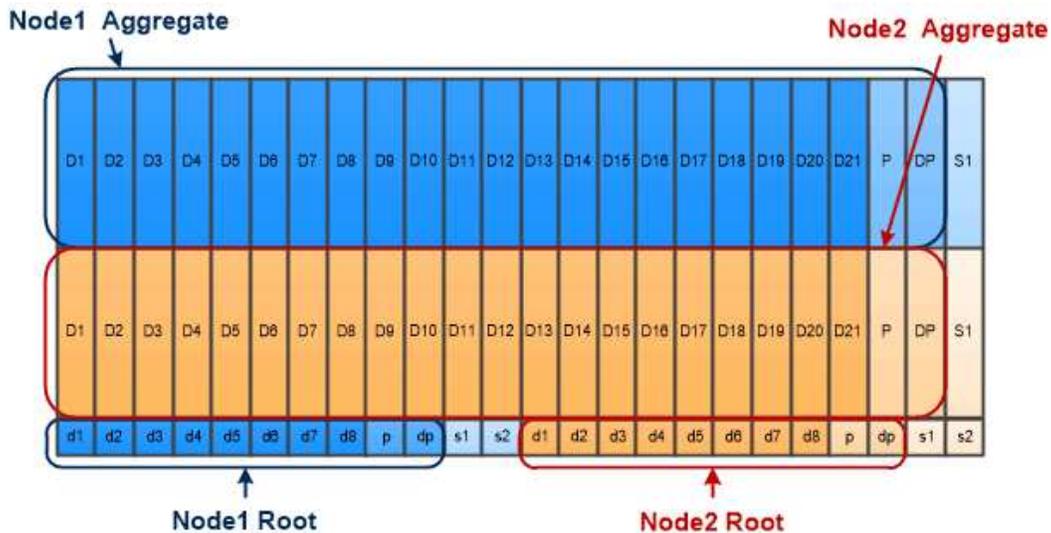
RAID-DPタイプのルートアグリゲートは、通常、1本のデータディスクと2本のパリティディスクで構成されます。これは、アグリゲート内の各 RAID グループ用に 2 つのディスクがパリティディスクとしてすでにリザーブされている場合、ストレージシステムファイルの料金を支払う「パリティ税」として相当します。

Root-data partitioning ルートアグリゲートを複数のディスクパーティションに分散し、各ディスク上に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、データ用に大きなパーティションを 1 つリザーブすることで、パリティの負担を軽減します。



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

図に示すように、ルートアグリゲートの格納に使用するディスクの数が多いほど、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 root-data-data partitioning の場合でもあります。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のアドバンスドドライブパーティショニング(ADP)機能の一部です。どちらも工場出荷時に構成され、エントリーレベルの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システムでのみルート/データ/データパーティショニングが使用されます。

詳細については、をご覧ください ["アドバンスドドライブパーティショニング"](#)。

ドライブがパーティショニングされてルートアグリゲート用に使用される

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ドライブは、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ているドライブの数を把握しておく、ルートパーティション用にリザーブされているドライブ容量と、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、および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（ノードあたり最大24個）。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包含アグリゲートと緩やかに結合されているため、従来のボリュームよりも柔軟にデータを管理できます。

1つのアグリゲートに複数のFlexVolを割り当てて、それぞれ異なるアプリケーションやサービス専用にすることができます。FlexVol volumeの拡張と縮小、FlexVol volumeの移動、FlexVol volume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パーティショニングしたり、クォータ_ を使用してボリュームのリソース使用量を制限したりできます。

ボリュームには、NAS環境ではファイルシステムが格納され、SAN環境ではLUNが格納されます。LUN（論理ユニット番号）は、SAN プロトコルによって対処される a_logical unit_ という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理解しておく必要があります。

- a_node root volume_ (通常は「vol0」) には、ノードの構成情報とログが格納されます。
- SVM ルートボリュームは、SVM によって提供されるネームスペースへのエントリポイントとして機能し、ネームスペースディレクトリ情報が格納されます。
- System volume_ には、サービス監査ログなどの特別なメタデータが格納されます。

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 volumes _ *

企業によっては、単一のネームスペースにペタバイト規模のストレージが必要になる場合があります。これは、FlexVol volumeの100TB容量をはるかに超えています。

FlexGroup volume__ は、200 個のコンスティチュエントメンバーボリュームを含む最大 4、000 億個のファイルをサポートします。このメンバーボリュームはコラボレーションにより、負荷を動的に分散し、すべてのメンバーに均等にスペースを割り当てます。

FlexGroupボリュームの場合、メンテナンスや管理のオーバーヘッドは必要ありません。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す。残りはONTAPが行います。

ストレージ仮想化

ストレージ仮想化の概要

クライアントやホストにデータを提供するには、_ Storage Virtual Machine (SVM) _ を使用します。ハイパーバイザー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 経由でアクセスされるデータはストレージ内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 network_logical interfaces (LIF ; ネットワーク論理インターフェイス) を通じてクライアントおよび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

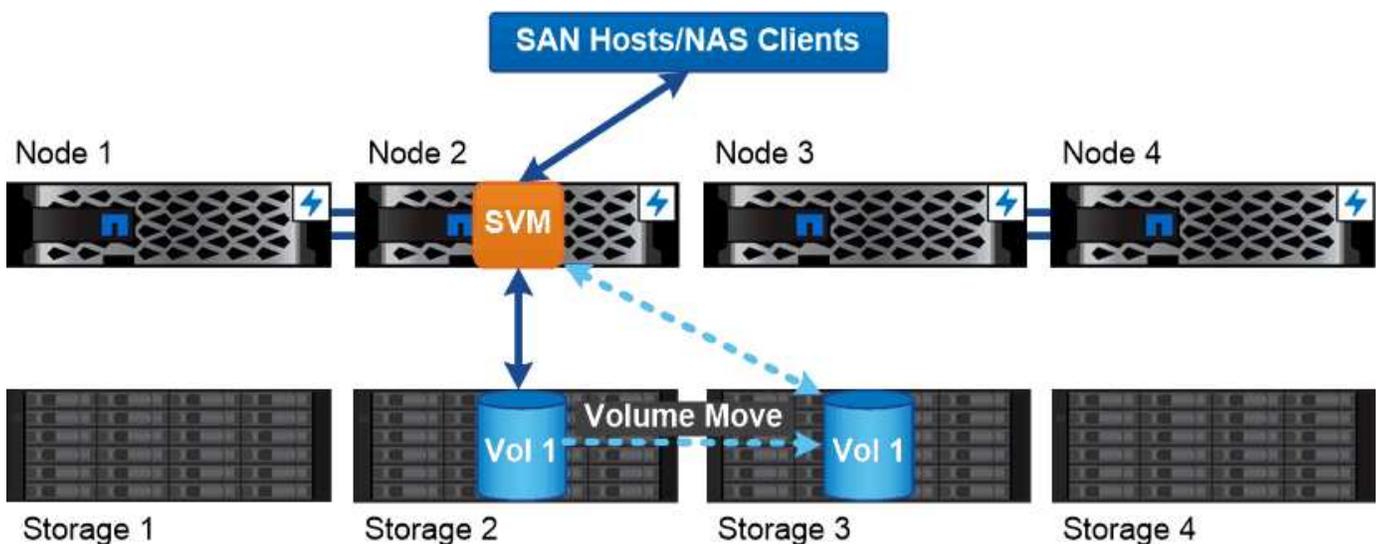
す。ハードウェアのアップグレード、ノードの追加、パフォーマンスの分散、アグリゲート間での容量の最適化など、ボリュームとLIFの両方を、データサービスを中断することなく移動できます。

同じ 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。クライアントとホストから 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保持されます。ポートは複数の LIF をホストできます。SVM には、それぞれ独自のセキュリティ、管理、および名前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。

- クラスターのセットアップ時に `admin SVM` が作成されます。
- ノードが新規または既存のクラスターに追加されると、`_node svm_is` が作成されます。
- IPspace 内のクラスターレベルの通信用に、`_system svm_is` を自動的に作成します。

これらの SVM はデータの提供には使用できません。また、クラスター内およびクラスター間のトラフィック用、およびクラスターとノードの管理用に特別な LIF があります。



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

ONTAPがミドルウェアに似ている理由

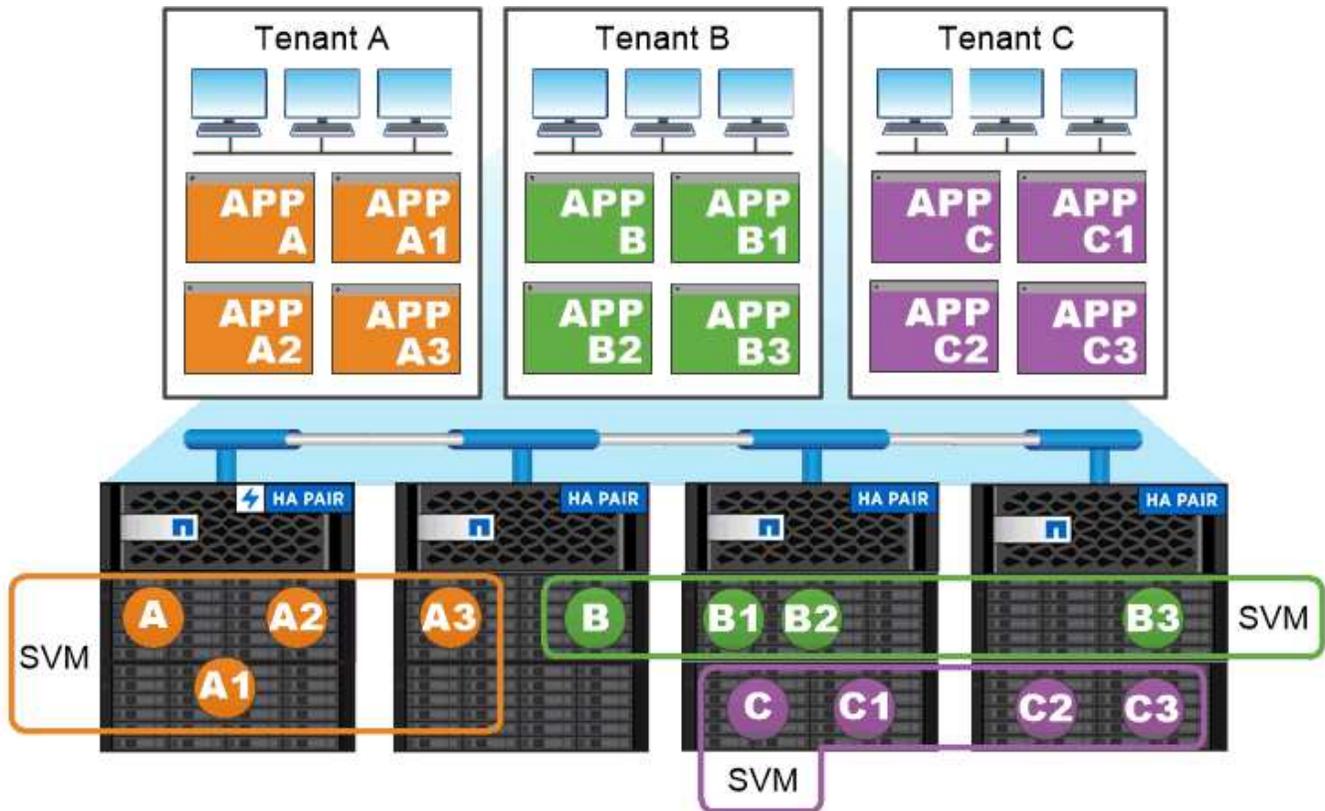
ONTAPがストレージ管理タスクに使用する論理オブジェクトは、適切に設計されたミドルウェアパッケージでよく知られている目標を達成します。具体的には、管理者を低レベルの実装の詳細から保護し、ノードやポートなどの物理特性の変更から構成を切り離すことです。管理者は、ストレージインフラ全体ではなくいくつかのフィールドを再設定して、ボリュームやLIFを簡単に移動できるようにすることが基本的な考え方です。

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環境で SVM を使用し、各テナントのデータを分離し、テナントごとに専用の認証と管理を実装して、チャージバックを簡易化します。複数の LIF を同じ SVM に割り当てて異なる顧客のニーズに対応したり、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「Bully」にな

らないようにしたりすることができます。

企業の管理者も同じような目的に SVM を使用します。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と予約された名前のクラスタ管理者は `admin`、クラスタのセットアップ時に自動的に作成されます。

デフォルトのロールを持つクラスタ管理者は、`admin`クラスタとそのリソース全体を管理できます。クラスタ管理者は、必要に応じて別のロールを割り当てた別のクラスタ管理者を作成することができます。

SVM administrator 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、デフォルトでロールが割り当てられ `vsadmin` ます。クラスタ管理者は、必要に応じて SVM 管理者に別のロールを割り当てることができます。

* _ ロールベースアクセス制御 (RBAC) _ *

管理者がアクセスできるコマンドは、管理者に割り当てられている `_role_assigned` コマンドで決まります。ロールは管理者のアカウントを作成するときに割り当てます。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できます。

ネームスペースとジャンクションポイント

`nas_namespace_` は、`_junction points_to` によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限があるクライアントは、ストレージ内のファイルの場所を指定せずに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。

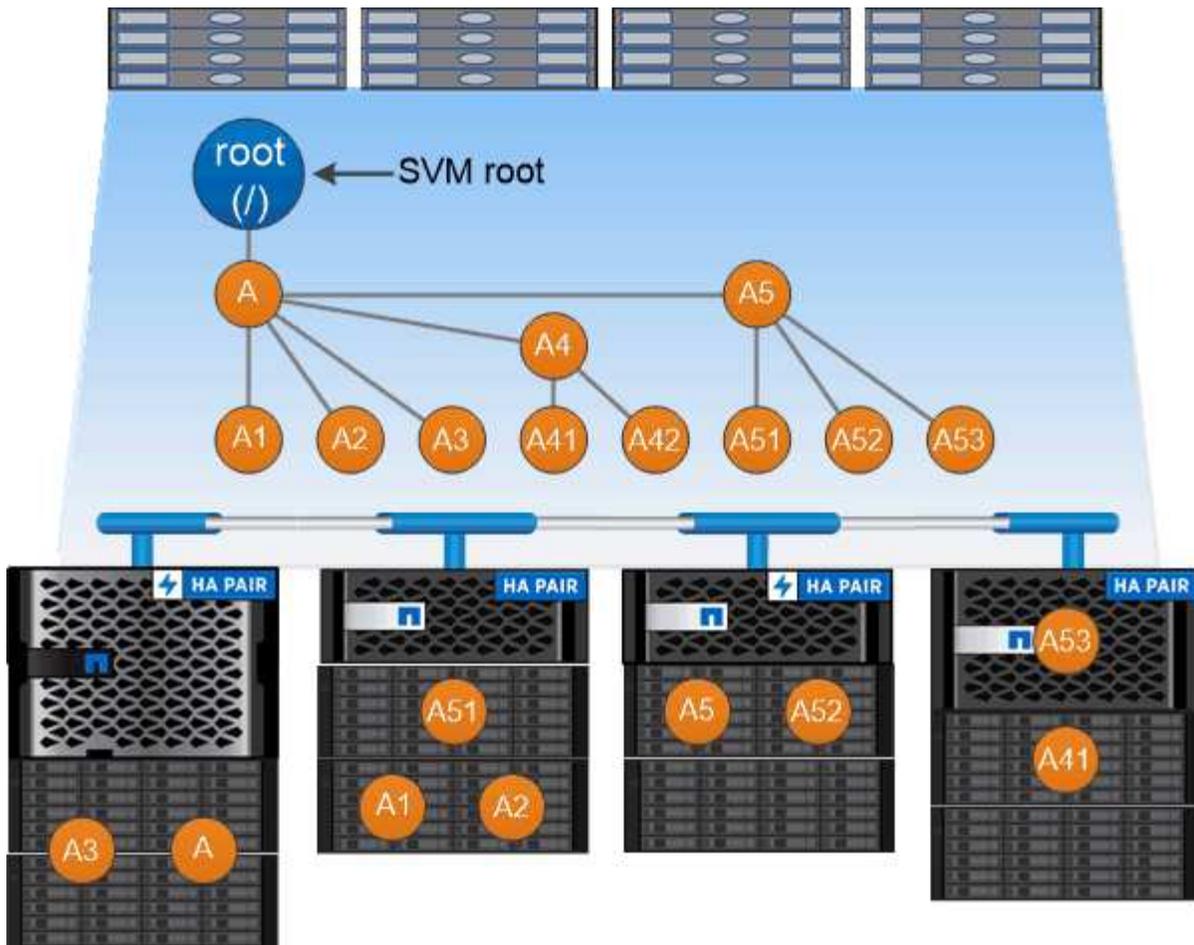
NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、`nfs_export_` をマウントするか、`SMB_share` にアクセスします。`_export` または共有は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされているボリュームにのみアクセスします。

ネームスペースには必要に応じて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すぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。「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、またはの `/vol1/dir2/vol3`` ようになります ``/vol1/vol2/vol3 /dir1/dir2/vol3`。このパスのことを `_junction` パスと呼びます。 `_`

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へのエントリポイントです。



ノードに障害やフェイルオーバーが発生したときにデータを引き続き利用できるようにするには、SVM ルートボリュームに `_load-sharing mirror_copy` 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

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成し`/eng/home`ます。

```
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

パスノフェイルオーバーノガイヨウ

ONTAP でのパスのフェイルオーバーは、NAS トポロジと SAN トポロジで大きく異なります。NAS LIF は、リンク障害が発生すると別のネットワークポートに自動的に移行します。SAN LIF は、障害の発生後に手動で移動しないかぎり移行しません。代わりに、ホストのマルチパステクノロジによって、同じSVM上の別のネットワークポートに

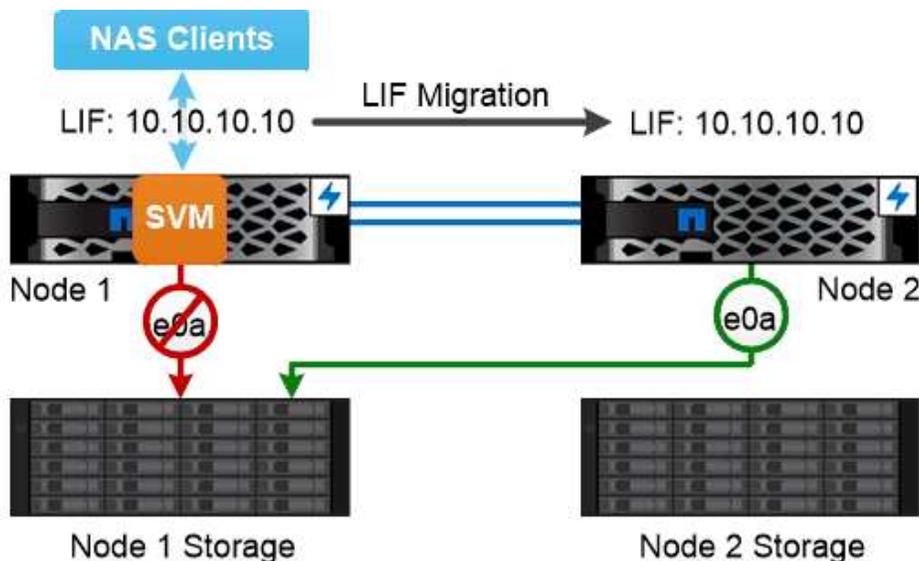
アクセスしている別のLIFにトラフィックが転送されます。

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、稼働しているネットワークポートに自動的に移行します。この移行先のポートは、LIFの *failover group* のメンバーである必要があります。_failover group policy_n を使用すると、データ LIF のフェイルオーバーターゲットが、データとその HA パートナーを所有するノード上のポートに移動します。

管理を容易にするため、ONTAP で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_ 用のフェイルオーバーグループが作成されます。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。VLANを使用している場合、たとえば部門（エンジニアリング、マーケティング、財務など）ごとにトラフィックを分離する場合は、VLANごとに個別のブロードキャストドメインが定義されます。ブロードキャストドメインに関連付けられている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の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。

ほとんどの場合、フェイルオーバーグループを最新の状態に保つためには、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を推奨します。ただし、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することもできます。たとえば、ブロードキャストドメインに定義されているポートの一部にのみLIFをフェイルオーバーするように設定できます。



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

• _サブネット_ *

a_subnet_ 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。LIFアドレスを定義するときに、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。

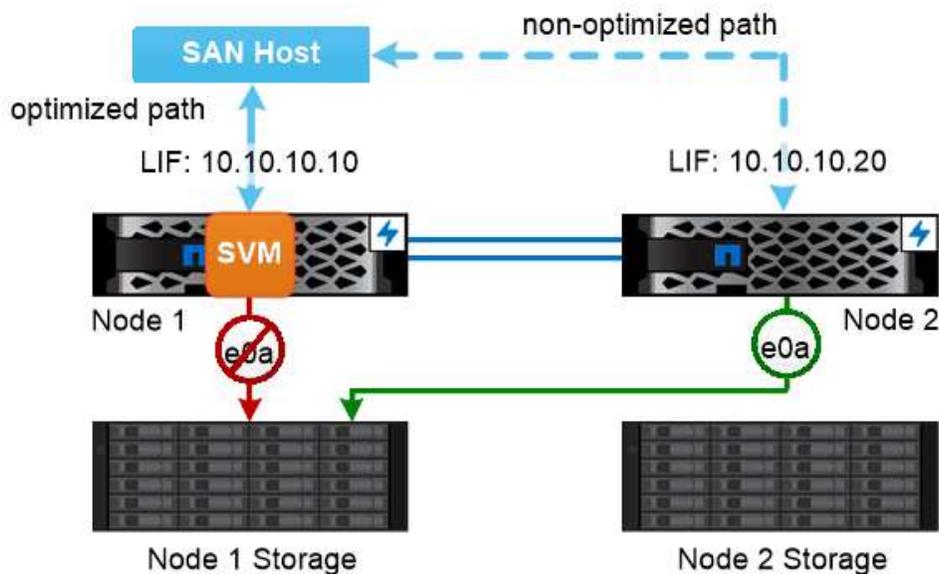
SANパスのフェイルオーバー

リンク障害が発生した場合、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、稼働しているLIFにトラフィックを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_targetsへの要求の_イニシエータ_とみなされます。_MPIO_を使用すると、イニシエータからターゲットへの複数のパスを使用できます。ALUAは、「_optimized paths_」と呼ばれる最も直接パスを特定します。_

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設定します。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選択的LUNマップ（SLM）では、ホストからLUNへのパスの数がデフォルトで制限されます。新しく作成したLUNには、そのLUNを所有するノードまたはそのHAパートナーへのパス経由でのみアクセスできます。また、イニシエータに対してport setでLIFを設定して、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の選択的LUNマップ（SLM）_は、SANホストからLUNへのパスの数を制限します。新しく作成したLUNには、LUNを所有するノードまたはHAパートナーであるLUNの_reporting nodes_へのパス経由でのみアクセスできます。

つまり、ボリュームを別のHAペアのノードに移動する場合は、デスティネーション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セットアップで新しいパスを指定できます。ボリュームの移動が完了したら、ソースHAペアのレポートノードをマッピングから削除できます。

ロードバランシング

ノードでの作業量が使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がレイテンシの影響を受け始めます。ノードが過負荷になった場合は、使用可能なリソースを増やす（ディスクまたはCPUをアップグレードする）か、負荷を軽減する（必要に応じてボリュームまたはLUNを別のノードに移動する）ことで対処できます。

また、ONTAPストレージのサービス品質（QoS）_を使用して、重要なワークロードのパフォーマンスが競合するワークロードの影響を受けて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対して QoS スループットの上限を設定すると、そのワークロードによるシステムリソースへの影響を制限できます（最大 QoS）。
- 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すると、競合するワークロードによる要求に関係なく、必要な最小スループットを確保できます（最小 QoS）。
- 同じワークロードに対してQoSの上限と下限を設定できます。

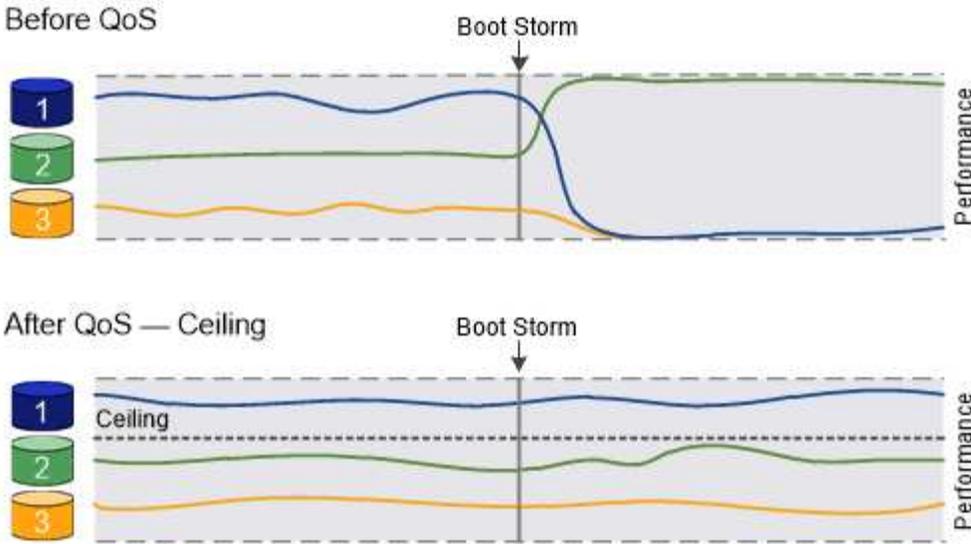
スループットの上限

スループットの上限は、ワークロードのスループットを最大IOPSまたはMB/秒に制限します。次の図では、ワークロード 2 のスループットの上限により、ワークロード 1 および 3 の「負荷」が発生しないようになっています。

`a_policy group_` は、1 つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、`a_storage` オブジェクト：_a 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 の I/O 処理のことです。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%までは超えることができます。バーストに対処するために、上限を50%まで超過することがあります。



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のスループットの下限が設定されているため、ワークロード2からの要求に関係なく、必要な最小スループットが確保されています。

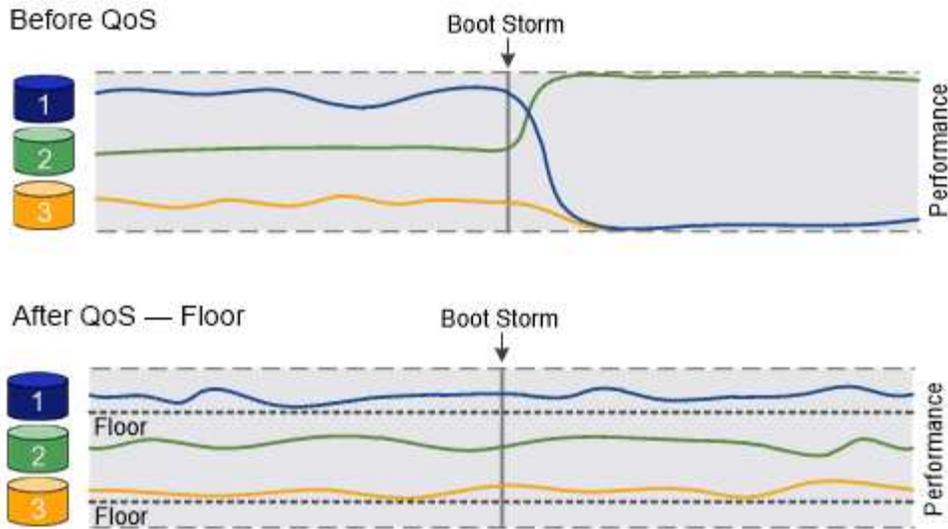


これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

ワークロードは、ボリューム、LUN、またはONTAP 9.3以降のfileのI/O処理を表します。スループットの下限が定義された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ます。また、ワークロードを監視したあとで指定することもできます。



ノードや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）がない場合やなどの重要な処理の実行中は、ワークロードのスループットが指定された下限を下回ることがあります volume move trigger-cutover。利用可能な容量が十分にあり、重要な処理を実行していない場合でも、ワークロードのスループットが指定された下限を最大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る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場合は、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。

アダプティブ QoS_ ワークロードのサイズの変更に合わせてポリシーグループの値が自動的に調整され、TB または GB あたりの IOPS が一定に維持されます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

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加した場合）にも使用できます。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。



ONTAP 9.5以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4以前のスループットの下限ではサポートされません。

+ 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。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が100 IOPS/GBの場合、150GBのボリュームのスループットの上限は、ボリュームのサイズが変わらないかぎり15,000 IOPSです。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の上限が30,000 IOPSに調整されます。
- a_used space-policy（デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、IOPS/TB|GB の比率を維持します。比率が100 IOPS/GBの場合、100GBのデータが格納されている150GBのボリュームのスループットの上限は10,000 IOPSです。使用済みスペースの量が変わると、アダプティブQoSによって比率に応じてスループットの上限が調整されます。

レプリケーション

Snapshotコピー

従来、ONTAPレプリケーションテクノロジー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きました。クラウドサービスの登場に伴い、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用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のSnapshotテクノロジーです。

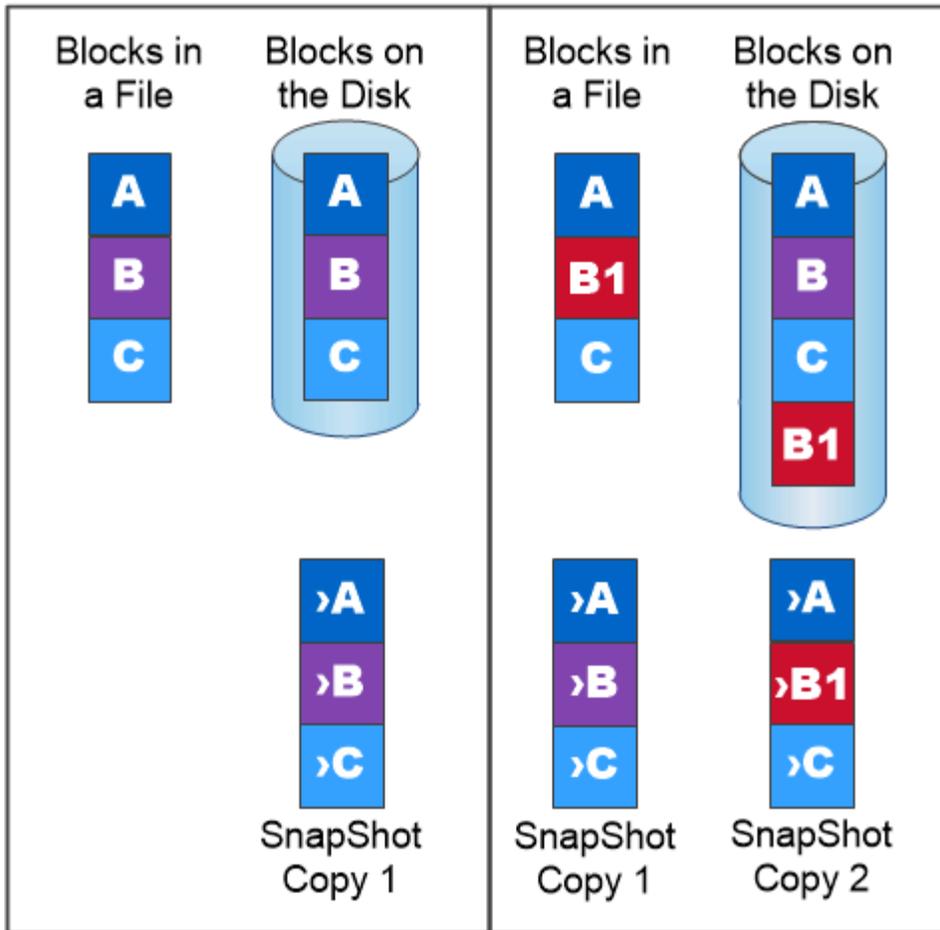
Snapshot コピー `_` は、ボリュームの読み取り専用のポイントインタイムイメージです。Snapshotコピーが作成されると、アクティブファイルシステムとSnapshotコピーは同じディスクブロックを参照するため、追加のディスクスペースは使用されません。イメージにはSnapshotコピーが最後に作成されてからのファイルへの変更のみが記録されるため、時間の経過とともに消費されるストレージスペースは最小限で済み、パフォーマンスのオーバーヘッドもわずかです。

Snapshot コピーの効率性は、ONTAPの中核的なストレージ仮想化テクノロジーであるITS Write Anywhere File Layout（WAFL）によって実現します。`_`WAFLは、データベースと同様に、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。

Snapshotコピーは、データブロックをコピーするのではなく、Snapshotコピーの作成時にONTAPがメタデータを参照する仕組みになっているので、効率的です。他のシステムと違ってコピーするブロックを探す「シーク時間」も、コピー自体を作成するコストも発生しません。

Snapshotコピーを使用して、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リストアしたりできます。Snapshotコピーのポインタ情報をディスク上のデータと比較することで、ダウンタイムや多大なパフォーマンスコストなしで損失オブジェクトや破損オブジェクトが再構築されます。

Snapshot ポリシー `_` は、ボリュームのSnapshot コピーの作成方法を定義します。このポリシーは、Snapshotコピーを作成するタイミング、保持するコピーの数、Snapshotコピーに名前を付ける方法、およびSnapshotコピーにレプリケーション用のラベルを付ける方法を指定します。たとえば、毎日午前12時10分に1つのSnapshotコピーを作成し、最新の2つのコピーを保持して「daily」（タイムスタンプを付加）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 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のプライマリストレージからセカンダリストレージへのフェイルオーバー用に設計されたディザスタリカバリテクノロジーです。名前が示すように、`SnapMirror` はセカンダリストレージに作業データのレプリカ (`_mirror`) を作成します。このデータから、プライマリサイトで災害が発生した場合にもデータの提供を継続できます。

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、`_data` 保護関係と呼ばれます。`_` ボリュームが存在するクラスターと、ボリュームからデータを提供する SVM は `_peered` になります。`_a` ピア関係を設定することで、クラスターと SVM の交換が可能になります。データをセキュアに保護



SVM間にデータ保護関係を作成することもできます。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バケット間の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システムに配置することも、ONTAP以外のシス

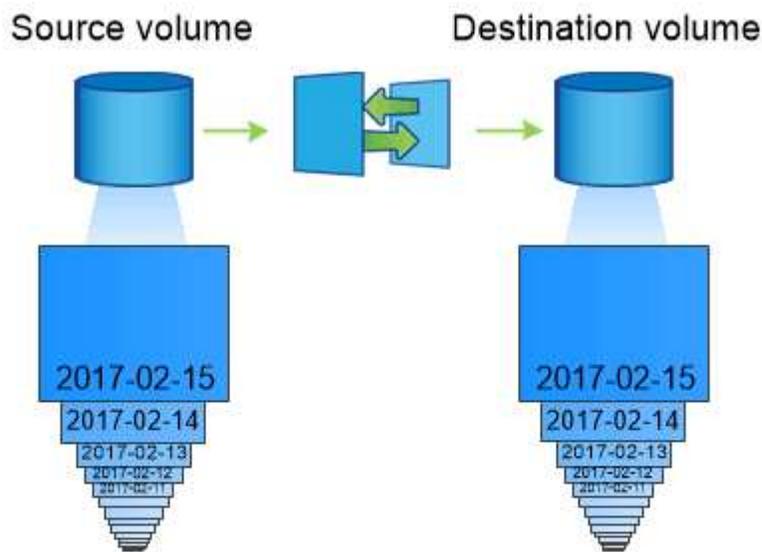
テム（StorageGRIDやAWSなど）に配置することもできます。

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。ベースライン転送の一般的な手順は次のとおりです。

- ソースボリュームのSnapshotコピーを作成します。
- Snapshotコピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。
- 「アクティブ」ミラーが破損した場合に備えて、ソースボリューム上の最新ではない残りの Snapshot コピーをデスティネーション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Snapshotコピーだけをミラーに転送します。更新は、設定したスケジュールに従って非同期に行われます。保持では、ソース上のSnapshotポリシーがミラーリングされます。プライマリサイトで災害が発生した場合は最小限のシステム停止でデスティネーションボリュームをアクティブ化し、サービスの復旧後にソースボリュームを再アクティブ化できます。

ベースラインの作成後はSnapMirrorでSnapshotコピーだけが転送されるため、無停止で高速なレプリケーションが可能です。フェイルオーバーのユースケースが示すように、ミラーリングされたストレージからデータを効率的に提供するには、セカンダリシステムのコントローラが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レプリケート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。

SnapMirrorクラウドによるオブジェクトストレージへのバックアップ

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ユーザー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。従来のテープバックアップアーキテクチャから脱却した組織は、長期的なデータ保持とアーカイブの代替リポジトリとしてオブジェクトストレージを使用できます。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。

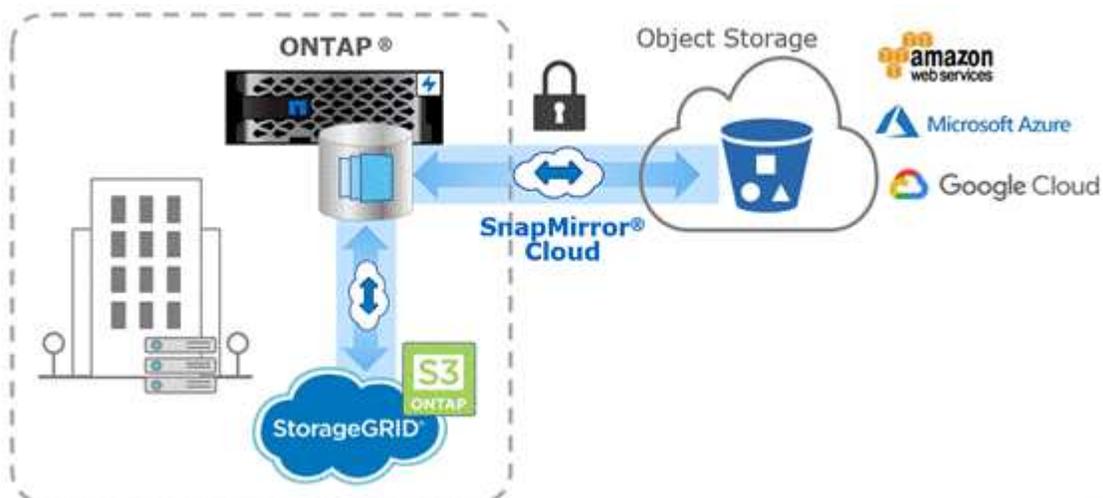
SnapMirrorクラウドは、SnapMirrorレプリケーションテクノロジーファミリーの拡張としてONTAP 9.8で導入されました。SnapMirrorはONTAPからONTAPへのバックアップによく使用されますが、SnapMirrorクラウドでは同じレプリケーションエンジンを使用して、ONTAPのSnapshotコピーをS3準拠のオブジェクトストレージバックアップに転送します。

バックアップのユースケースをターゲットにしたSnapMirror Cloudは、長期保持とアーカイブの両方のワークフローをサポートしています。SnapMirrorと同様に、SnapMirrorの初回クラウドバックアップでボリュームのベースライン転送が実行されます。以降のバックアップでは、SnapMirror CloudによってソースボリュームのSnapshotコピーが生成され、変更されたデータブロックのみを含むSnapshotコピーがオブジェクトストレージターゲットに転送されます。

SnapMirrorクラウド関係は、ONTAPシステムと、Amazon S3、Google Cloud Storage、Microsoft Azure Blob Storageなどのオンプレミスと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の間で設定できます。その他のオンプレミスオブジェクトストレージターゲットには、StorageGRIDやONTAP S3などがあります。

SnapMirrorクラウドレプリケーションはONTAPのライセンス機能であり、データ保護ワークフローのオーケストレーションには承認済みのアプリケーションが必要です。SnapMirrorクラウドバックアップの管理には、次のオーケストレーションオプションを使用できます。

- 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バックアップパートナー。参加ベンダーは、から入手でき["ネットアップのブログ"](#)です。
- ONTAP環境向けのNetAppネイティブソリューション向けBlueXP バックアップ/リカバリ
- データ保護ワークフロー向けのカスタムソフトウェアを開発したり、自動化ツールを活用したりするためのAPI



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以降では、SnapVaultライセンスは廃止され、SnapMirrorライセンスを使用してバックアップ関係、ミラー関係、ミラー関係とバックアップ関係を設定できます。SnapMirrorレプリケーションは、SnapshotコピーのONTAPからONTAPへの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に対応します。

_ SnapVault _ は、基準への準拠およびその他のガバナンス関連の目的で、ディスクツーディスクの Snapshot コピーレプリケーション用に設計されたアーカイブテクノロジーです。通常、ソースボリューム内の Snapshot コピーだけがデステーションに格納される SnapMirror 関係とは異なり、SnapVault デステーションには、より長期間にわたって作成されたポイントインタイムの Snapshot コピーが保持されます。

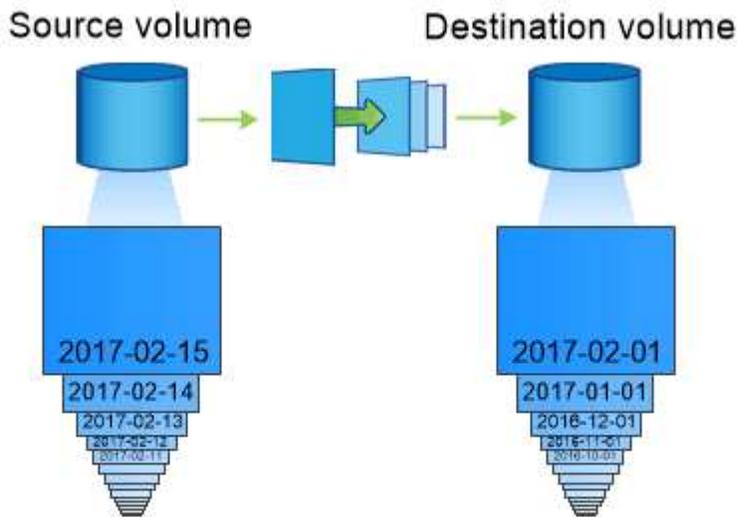
たとえば、ビジネスに関する政府会計規制に準拠するために、データの月次 Snapshot コピーを20年間にわたって保持することができます。SnapVault ストレージからデータを提供する必要はないため、デステーションシステムでは低速で低コストのディスクを使用できます。

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Snapshotコピーが作成され、そのコピーおよびコピーが参照するデータブロックがデステーションボリュームに転送されます。SnapMirrorとは異なり、SnapVaultではベースラインに古いSnapshotコピーは含まれません。

更新は、設定したスケジュールに従って非同期に行われます。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コピーと保持するコピーの数が決まります。ポリシーで定義されているラベル ("s only,") は、ソース上の Snapshot ポリシーで定義されている 1 つ以上のラベルと一致する必要があります。そうしないと、レプリケーションが失敗します。



SnapMirrorとSnapVaultは同じコマンドインフラストラクチャを共有します。ポリシーの作成時に使用する方法を指定します。どちらの方法でも、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

ONTAP 9.7以前でのみディスクツーディスクであったSnapMirrorおよびSnapVaultのデータ保護関係に加えて、より低コストで長期的なデータ保持を実現できるバックアップソリューションがいくつか登場しました。

多くのサードパーティ製データ保護アプリケーションが、ONTAPで管理されるデータに対して従来のバックアップを提供しています。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。

Snapshot.8以降でONTAP 9は、SnapMirror Cloudが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Snapshotコピーの非同期レプリケーションを提供します。SnapMirrorの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を行うための、ライセンスが必要です。SnapMirrorのクラウド関係は、ONTAPシステムからオンプレミスと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）への移行がサポートされ、ベンダーのバックアップソフトウェアで効率性が向上します。サポートされる認定アプリケーションやオブジェクトストレージベンダーの一覧については、NetAppの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、BlueXP 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インスタンスの間にSnapMirror関係またはSnapVault関係を設定できます。

BlueXP は、ソフトウェアサービス（SaaS）モデルを使用したCloud Volumes ONTAPインスタンスのバックアップも提供します。NetApp Cloud CentralにあるCloud Backup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とBlueXP のドキュメントリソース"](#)

["NetApp Cloud Central"](#)

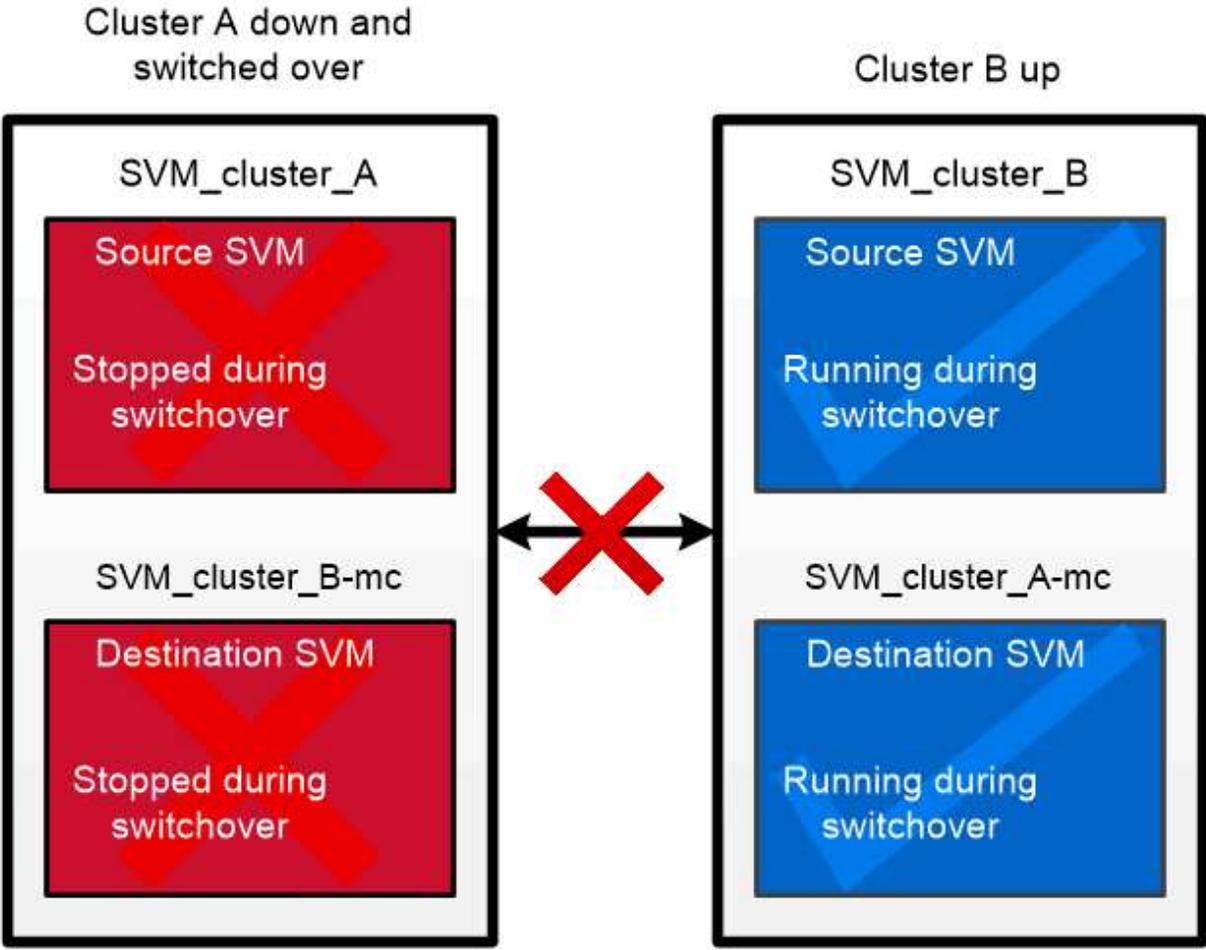
MetroClusterの継続的可用性

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とSVMの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場合、管理者は、ミラーされたSVMをアクティブ化し、サバイバーサイトからデータの提供を開始できます。

- ファブリック接続型MetroCluster_および MetroCluster IP_構成は、メトロポリタン規模のクラスタをサポートします。
- _Stretch MetroCluster_ configurations は、キャンパス全体のクラスタをサポートします。

どちらの場合も、クラスタ間でピア関係を確立する必要があります。

MetroCluster では、_ SyncMirror _ という ONTAP 機能を使用して、もう一方のクラスタのストレージでコピーまたは_ フレックス _ の形式で各クラスタのアグリゲートデータを同期的にミラーリングします。スイッチオーバーでは、サバイバークラスタ上のリモートフ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.

* _ MetroCluster 以外の実装で SyncMirror を使用する _ オプションで MetroCluster 以外の実装で SyncMirror を使用することにより 'RAID タイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や 'RAID グループのディスクへの接続が失われた場合のデータ損失を防ぐことができますこの機能はHAペアに対してのみ使用できます。

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にミラーリングされます。いずれかのシェルフが使用できなくなった場合、障害の原因を修正しながら、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に注意してください。各プレックスに、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。たとえば、1、440GB のアグリゲートをミラーリングするには、プレックス1つにつき1、440GB、合計で2、880GB のディスクスペースが必要です。

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、ミラーアグリゲート用に少なくとも20%の空きスペースを確保することを推奨します。ミラーされていないアグリゲートでは10%が推奨されますが、追加の10%のスペースはファイルシステムで増分変更に対応するために使用できます。増分変更を行うと、ONTAPのcopy-on-write Snapshotベースのアーキテクチャにより、ミラーされたアグリゲートのスペース使用率が向上します。これらのベストプラクティスに従わないと、SyncMirrorの再同期のパフォーマンスが低下し、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します。



SyncMirrorは、FlexArray仮想化の実装にも使用できます。

Storage Efficiency

ONTAPの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、書き込み済み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使用可能なスペースを効果的に利用する方法のことです。Storage Efficiencyが高いほど、最大限のデータを最小限のスペースに最小限のコストで格納できます。たとえば、重複するデータブロックとゼロでいっぱいデータブロックを検出して排除するStorage Efficiencyテクノロジーを利用すると、必要な物理ストレージの総容量が削減され、全体的なコストが削減されます。

ONTAPは、さまざまなStorage Efficiencyテクノロジーを提供しています。このテクノロジーを使用すると、データが消費する物理ハードウェアやクラウドストレージの量を削減できます。また、データの読み取り速度、データセットのコピー速度、VMのプロビジョニング速度など、システムのパフォーマンスも大幅に向上します。

ONTAPのStorage Efficiencyテクノロジーは次のとおりです。

- * シンプロビジョニング *

シンプロビジョニング ボリュームまたはLUNのストレージを事前にリザーブするのではなく、必要に応じて割り当てることができます。現在使用されていないスペースをリザーブすることなく、潜在的な使用量に基づいてボリュームまたはLUNを過剰に割り当てることができるため、必要な物理ストレージの量が削減されます。

• * 重複排除 *

重複排除ボリュームに必要な物理ストレージの量を3つの方法で削減します。

◦ ゼロブロック重複排除

ゼロブロック重複排除は、すべてゼロでいっぱいになったデータブロックを検出して排除し、メタデータのみを更新します。ゼロブロックで一般的に使用されているスペースの100%が削減されます。ゼロブロック重複排除は、すべての重複排除ボリュームでデフォルトで有効になります。

◦ インライン重複排除

インライン重複排除は、重複するデータブロックを検出し、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、ボリュームレベルまたはアグリゲートレベルで実行できます。AFFシステムおよび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も、重複するデータブロックを検出して一意の共有ブロックへの参照に置き換えますが、データがディスクに書き込まれたあとに実行することで、ストレージ効率がさらに向上します。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、バックグラウンド重複排除を設定できます。たとえば、ボリュームの利用率が10%に達したときにバックグラウンド重複排除を実行できます。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、特定のスケジュールで実行されるように設定することもできます。AFFシステムおよび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、ボリューム内と、アグリゲート内のボリューム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 *

圧縮データブロックを圧縮グループに結合し、各ブロックを単一のブロックとして格納することで、ボリュームに必要な物理ストレージの量を削減します。読み取り要求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、圧縮されるファイルのサイズの拡張性が向上します。

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、ディスクに書き込む前にメモリ内のデータを圧縮することで、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、まずブロックが圧縮されていない状態でディスクに書き込まれ、次にスケジュールされた時刻にデータが圧縮されます。AFAシステムではデフォルトで有効になっています。他のすべてのシステムでは、手動で圧縮を有効にする必要があります。

• 圧縮

コンパクションを使用すると、サイズが4KB未満のデータチャンクを作成して単一のブロックに結合することで、ボリューム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に残ってい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システムおよび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、手動でコンパクションを有効にする必要があります。

- * FlexCloneボリューム、ファイル、LUN *

FlexCloneテクノロジー Snapshotメタデータを活用して、ボリューム、ファイル、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。コピーはデータブロックを親と共有し、変更がコピーまたはその親に書き込まれるまでメタデータに必要な分以外ストレージを消費しません。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。

- 温度に敏感なストレージ効率

ONTAPを使用すると "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ができます。アクセス頻度の低いコールドデータの場合は、大容量のデータブロックが圧縮されます。頻繁にアクセスされて上書きされるホットデータの場合は、小さいデータブロックが圧縮されるため、プロセスが効率化されます。

ONTAP 9.8で導入されたTemperature-Sensitive Storage Efficiency (TSSE) は、新しく作成したシンプロビジョニングAFFボリュームで自動的に有効になります。ハードウェアオフロードプロセッサを使用するONTAP 9.15.1で導入されたでは、この機能は有効になっていません "AFF A70、AFF A90、およびAFF A1Kプラットフォーム"。

- * 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以降では、ONTAPがAFF A70、AFF A90、AFF A1K、FAS70、FAS90の各プラットフォームにデータコンパクション機能を提供して "CPUまたは専用オフロードプロセッサのストレージ効率" があります。AFF A70、AFF A90、およびAFF A1Kシステムでは、Storage Efficiencyが自動的に有効になるため、設定は必要ありません。

これらのテクノロジーのメリットを日常業務で最小限の労力で実現できます。たとえば、5,000人のユーザ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、任意のユーザが必要とする最大スペースが1GBであるとした場合、潜在的なストレージニーズに合わせて、5TBのアグリゲートを事前にリザーブすることもできます。ただし、ホームディレクトリの容量要件は組織によって大きく異なることもわかっています。組織用に合計スペースを5TBリザーブする代わりに、2TBのアグリゲートを作成できます。シンプロビジョニングを使用すると、名目上は各ユーザに1GBのストレージを割り当てることができますが、ストレージは必要に応じてのみ割り当てることができます。時間の経過とともにアグリゲートをアクティブに監視し、実際の物理サイズを必要に応じて増やすことができます。

別の例として、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仮想デスクトップインフラ (VDI) を使用しているとします。重複排除は、VDI全体で重複する情報ブロックを自動的に排除し、元のブロックへのポインタに置き換えることで、ストレージの使用量を削減します。他のONTAPのStorage Efficiencyテクノロジー (圧縮など) も、手動操作なしでバックグラウンドで実行できます。

ONTAPディスクパーティショニングテクノロジーは、ストレージ効率も向上します。RAID DPテクノロジーは、パフォーマンスを犠牲にしたり、ディスクミラーリングのオーバーヘッドを増大させたりすることなく、二重ディスク障害からデータを保護します。ONTAP 9を使用した高度なSSDパーティショニングにより、使用可能容量が約20%増加します。

NetAppは、オンプレミスのONTAPと同じStorage Efficiency機能をクラウドで提供します。オンプレミスのONTAPからクラウドにデータを移行する場合は、既存のストレージ効率が維持されます。たとえば、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するとします。BlueXP のデータレプリケーションを使用してデータを移行できます。また、移行プロセスの一環として、クラウド内のSnapshotコピーに対して最新のオンプレミスポリシーを有効にすることもできます。

シンプロビジョニング

ONTAP は、Snapshot コピーに加え、Storage Efficiency テクノロジーも幅広く提供しています。主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 の割り当てが可能です。Snapshot コピーと同様に、いずれも ONTAP の Write Anywhere File Layout (WAFL) を基盤としています。

シンプロビジョニングされたボリュームまたは LUN は、ストレージが事前に予約されていないボリュームです。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、空きスペースはストレージシステムに戻されます。

たとえば、5、000 人のユーザ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。ホームディレクトリの消費スペースは、最大で 1GB と推定されます。

この状況では、5TB の物理ストレージを購入することが考えられます。ホームディレクトリを格納するボリュームごとに、最もスペースを消費するユーザのニーズを満たす十分なスペースを確保します。

しかし実際には、ホームディレクトリに必要なとされる容量はコミュニティによって大きく異なることもわかっています。ストレージを大量に消費するユーザごとに、ほとんど、またはまったく消費しないユーザが 10 人あります。

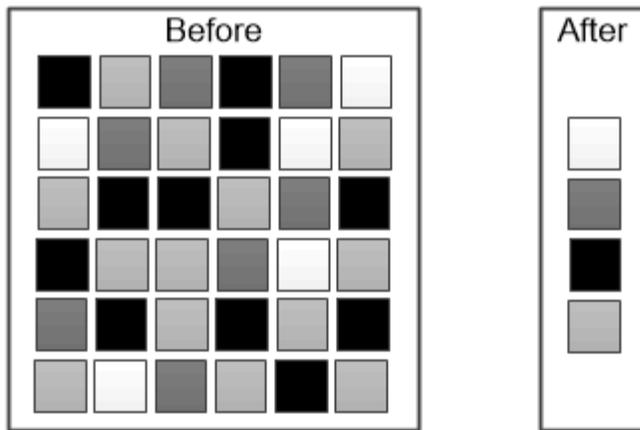
シンプロビジョニングを使用すると、使用しない可能性があるストレージを購入することなく、ストレージを大量に消費するユーザのニーズを満たすことができます。ストレージスペースは実際に消費されるまで割り当てられないため 2TB のアグリゲートを「オーバーコミット」するには、アグリゲートに含まれる 5、000 ボリュームのそれぞれに名目上は 1GB のサイズを割り当てる必要があります。

ライトユーザとヘビーユーザの比率が 10：1 であること、およびアグリゲートの空きスペースをアクティブ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 _ 重複するブロックを破棄して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の量を削減します。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。ノードに負荷が集中している場合を除き、書き込みによる影響もほとんどありません。

通常の使用で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。_ 重複排除の開始後、ONTAP はカタログ内のシグネチャを比較して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は、カタログの作成後に候補ブロックが変更されていないことを確認するために、1バイトずつ比較されます。すべてのバイトが一致した場合にのみ、重複ブロックが破棄され、そのディスクスペースが解放されます。



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

圧縮

_Compression : _圧縮グループ内のデータブロックを結合し、それぞれを1つのブロックとして格納することで、ボリュームに必要な物理ストレージの量を減らします。ONTAPでは、ファイルや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が解凍されるため、従来の圧縮手法よりも短時間で圧縮されたデータを読み取ることができます。

インライン圧縮とポストプロセス圧縮の2つがあり、個別に実行することも組み合わせて実行することもできます。

- **_Inline compression** **_compression** は、データをメモリで圧縮してからディスクに書き込まれます。ボリュームへの書き込み I/O は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。負荷の高い処理は次のポストプロセス圧縮処理まで保留されます。
- **_ポスト プロセス圧縮 :** ディスクに書き込まれたデータを、重複排除と同じスケジュールで圧縮します。

* **_インラインデータコンパクション_*** ゼロで埋められた小さなファイルまたは I/O は、4KB の物理ストレージが必要かどうかに関係なく、4KB 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_** では、通常であれば複数の 4KB ブロックを消費するデータチャンクをディスク上の 1つの 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にある間に行われるため、高速のコントローラに適しています。

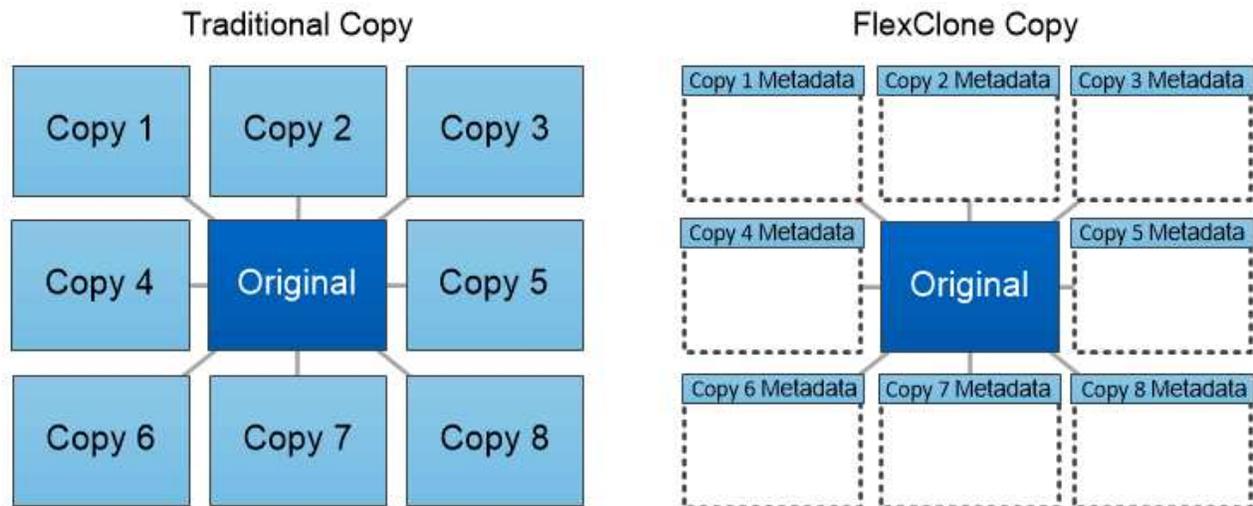
FlexCloneボリューム、ファイル、LUN

_FlexClone technology は、Snapshot 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ています。コピーはデータブロックを親と共有し、変更がコピーに書き込まれるまでメタデータに必要な分以外ストレージを消費しません。FlexCloneファイルとFlexClone LUNは同じテクノロジーを使用しますが、元のSnapshotコピーは必要ありません。

従来型のコピーの作成には数分から数時間かかることがありますが、FlexCloneソフトウェアを使用すると、大規模なデータセットでもほぼ瞬時にコピーできます。そのため、同一のデータセットの複数のコピー（仮想

デスクトップ環境など）やデータセットの一時的なコピー（本番環境のデータセットに対してアプリケーションをテストする）が必要な状況に最適です。

既存のFlexCloneボリュームをクローニングしたり、LUNクローンを含むボリュームをクローニングしたり、ミラーとバックアップのデータをクローニングしたりできます。FlexClone ボリュームは親からスプリットできます。スプリットされた場合、コピーには独自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.

System Managerでの容量測定

システム容量は、物理スペースと論理スペースのどちらかで測定できます。ONTAP 9.7 以降では、System Managerで物理容量と論理容量の両方を測定できます。

次の説明では、2つの測定値の違いについて説明します。

- 物理容量：物理スペースは、ボリュームまたはローカル階層で使用されているストレージの物理ブロックを表します。Storage Efficiency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、使用済み物理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：論理スペースは、ボリュームまたはローカル階層で使用可能なスペース（論理ブロック）です。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のスペースをどのように使用できるかを指します。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に、設定されているStorage Efficiency機能（重複排除や圧縮など）による削減量を加えた値になります。この測定値にはSnapshotコピー、クローン、その他のコンポーネントが含まれ、データ圧縮などの物理スペース削減量が反映されないため、使用済み物理容量よりも多く表示されることがあります。したがって、合計論理容量がプロビジョニング済みスペースよりも大きくなる可能性があります。



System Managerでは、容量表現に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。

使用済み容量の測定値

使用済み容量の測定値は、次の表で説明するように、使用しているSystem Managerのバージョンによって表示されます。

System Manager のバージョン	容量に使用される用語	参照される容量のタイプ
9.9.1以降	使用済み論理容量	使用済み論理スペース（Storage Efficiency の設定が有効になっている場合）
9.7および9.8	使用済み	使用済みの論理スペース（Storage Efficiency の設定が有効になっている場合）
9.5 および 9.6（クラシックビュー）	使用済み	使用済みの物理スペース

容量の測定条件

容量の定義には次の用語が使用されます。

- 割り当て容量：Storage VM内のボリュームに割り当てられているスペースの量。
- 使用可能：Storage VMまたはローカル階層でデータの格納やボリュームのプロビジョニングに使用できる物理スペースの量。
- ボリューム間の容量：Storage 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に使用されているスペースの量（物理または論理）。
 - ONTAP 9.13.1以降では、クライアントデータで使用されている容量を*論理使用済み*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
 - ONTAP 9.12.1以前では、クライアントデータに使用されている容量がSnapshotコピーで使用されている容量に追加された容量を*論理使用済み*と呼びます。
- * Committed *：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格納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、ほとんどのストレージ効率化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量には、使用済み物理スペースに対するすべての使用済み論理スペースの総削減率が表示され、Snapshotコピーやその他のStorage Efficiency機能の使用によるメリットも含まれます。
 - 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ている物理スペースと比較した、クライアントデータのみで使用されている論理スペースの比率の両方が表示されます。これを「Snapshotコピーとクローンなし」*と呼びます。
- 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で使用されている容量を*論理使用済み*と呼び、Snapshotコピーで使用されている容量は別々に表示されます。
 - ONTAP 9.12.1以前では、クライアントデータで使用されている容量がSnapshotコピーで使用されている容量に追加された容量を*論理使用済み*と呼びます。
- * Logical Used%*：Snapshotリザーブを除く、プロビジョニング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での効率化による削減も含まれるため、100%を超える場合があります。

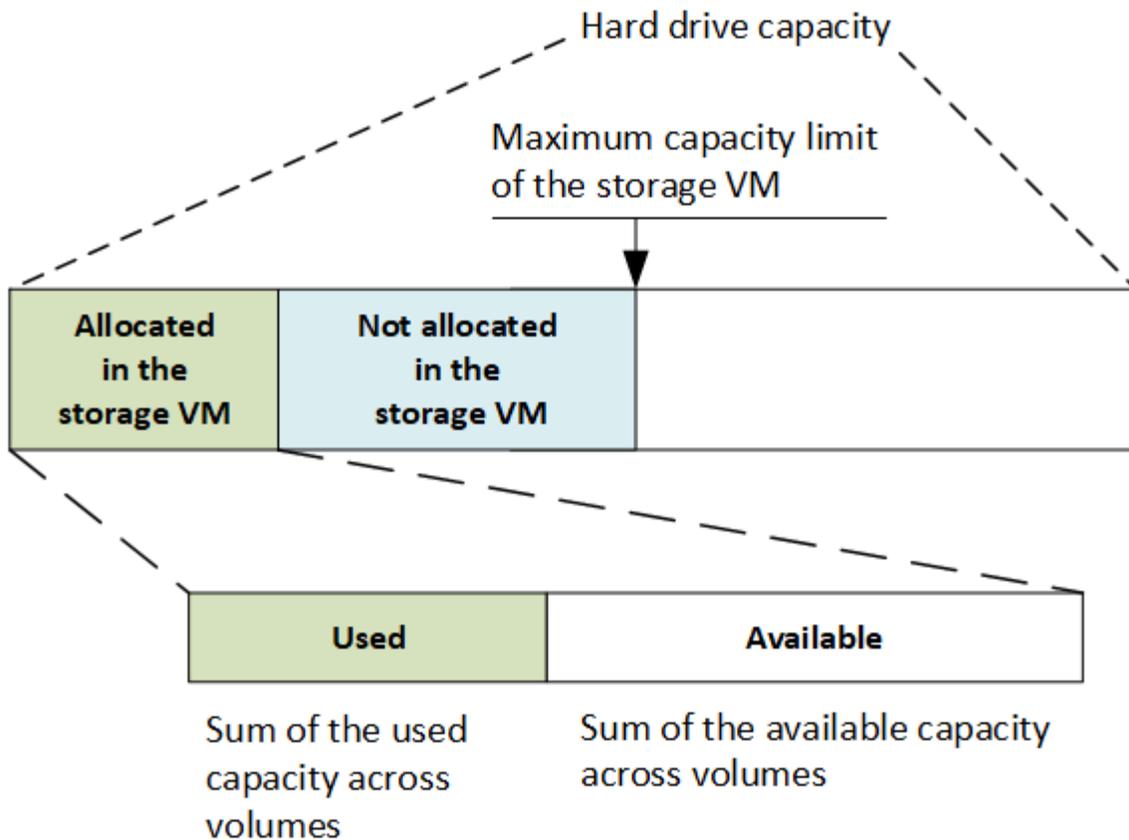
- 最大容量：Storage VM上のボリュームに割り当てられる最大スペース。
- 使用済み物理容量：ボリュームまたはローカル階層の物理ブロックで使用されている容量。
- * Physical Used %*：ボリュームの物理ブロックで使用されている容量の、プロビジョニングされたサイズに対する割合。
- プロビジョニングされた容量：Cloud Volumes ONTAPシステムから割り当てられ、ユーザやアプリケーションのデータを格納できる状態にあるファイルシステム（ボリューム）。
- * Reserved *：ローカル階層ですでにプロビジョニングされているボリューム用にリザーブされているスペースの量。
- 使用済み：データが格納されているスペースの量。
- * usedおよびreserved *：使用済みの物理スペースとリザーブスペースの合計です。

Storage VMの容量

Storage VMの最大容量は、ボリュームに割り当てられている合計スペースに未割り当ての残りスペースを足したものです。

- ボリュームの割り当てスペースは、FlexVol、FlexGroup、およびFlexCache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、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格納されている場合でも、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の値が合計で使用されます。自動拡張を使用しない場合は、ボリュームの実際の容量が合計で使用されます。

次のグラフは、ボリューム間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以降では、クラスタ管理者が使用できます"[Storage VMの最大容量制限を有効にする](#)"。ただし、データ保護、SnapMirror関係、またはMetroCluster構成のボリュームを含むStorage VMに対してストレージ制限を設定することはできません。また、Storage VMの最大容量を超えるようにクォータを設定することはできません。

最大容量制限の設定後は、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。

Storage VMが最大容量に達すると、一部の処理を実行できなくなります。System Managerには、の次の手順"[インサイト](#)"に関する推奨事項が表示されます。

容量の測定単位

System Manager は、1024 (2^{10}) 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。

- .10.1以降では、ONTAP 9 Managerにストレージ容量の単位がKiB、MiB、GiB、TiB、およびPiBとして表示されます。
- ONTAP 9 .10.0以前では、これらの単位は、System ManagerにKB、MB、GB、TB、およびPBとして表示されます。



System Managerでスループットに使用される単位は、ONTAPのすべてのリリースで、KB/秒、MB/秒、GB/秒、TB/秒、およびPB/秒のままです。

ONTAP 9.10.0 以前の System Manager で表示される容量の単位	ONTAP 9.10.1以降の System Manager に表示される容量単位	計算	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"](#)

温度に基づく Storage Efficiencyの概要

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、温度に影響されるStorage Efficiency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の場合は大容量のデータブロックが圧縮され、頻繁にアクセスされて上書きされるホットデータの場合は小さなデータブロックが圧縮されるため、プロセスが効率化されます。

Temperature-Sensitive Storage Efficiency (TSSE) はONTAP 9.8で導入された機能で、新しく作成したシンプロビジョニングAFFボリュームで自動的に有効になります。既存のAFFボリュームおよびシンプロビジョニングされた非AFF DPボリュームでは、温度に基づくStorage Efficiencyを有効にすることができます。



温度に基づくストレージ効率化は、AFF A70、AFF A90、およびAFF A1Kのプラットフォームには適用されません。これらのプラットフォームでは、ホットデータやコールドデータに基づいて圧縮が行われないため、データがコールドになるのを待たずに圧縮が開始されます。

「デフォルト」モードと「効率的」モードの導入

ONTAP 9.10.1以降では、AFFシステムにのみ `_default_and_efficient_volume-level` のStorage Efficiencyモードが導入されています。この2つのモードでは、新しいAFFボリュームの作成時のデフォルトモードであるファイル圧縮（デフォルト）と、温度に基づくStorage Efficiency（効率的）のどちらかを選択できます。["温度に基づくストレージ効率化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を有効にするには、ONTAP 9.10.1を使用します。ただし、AFFプラットフォームでは、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などの他のStorage Efficiency機能が、デフォルトモードと効率モードのどちらでもデフォルトで有効になります。

どちらのStorage Efficiencyモード（デフォルトと効率化）も、FabricPool対応のアグリゲートでサポートさ

れ、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温度に基づくStorage Efficiencyを有効化

温度に基づくStorage Efficiencyは、AFF Cシリーズプラットフォーム、および次のリリースがインストールされたデスティネーションでボリューム移動またはSnapMirrorを使用して、非TSSEプラットフォームからTSSE対応Cシリーズプラットフォームにボリュームを移行する場合、デフォルトで有効になります。

- ONTAP 9.12.1P4以降
- ONTAP 9.13.1以降

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

既存のボリュームでは、温度に基づくStorage Efficiencyは自動的に有効になりませんが、["Storage Efficiencyモードを変更します"](#)で手動で効率化モードに変更できます。



Storage Efficiencyモードを効率化モードに変更したあとに元に戻すことはできません。

連続する物理ブロックをシーケンシャルにパッキングすることでストレージ効率が向上

ONTAP 9.13.1以降では、温度に左右されるストレージ効率化機能によって、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。システムをONTAP 9にアップグレードすると、温度の影響を受けやすいStorage Efficiencyが有効になっているボリュームでは、シーケンシャルパッキングが自動的に有効になります。13.1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します"](#)を実行する必要があります。

アップグレード時の考慮事項

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、ボリュームで現在有効になっている圧縮のタイプに基づいてStorage Efficiencyモードが割り当てられます。アップグレードの実行中、圧縮が有効なボリュームにはデフォルトモードが割り当てられ、温度に基づくStorage Efficiencyが有効なボリュームには効率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、Storage Efficiencyモードは空白のままです。

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以降では、ONTAPでAFF A70、AFF A90、AFF A1K、FAS70、FAS90の各プラットフォームでStorage Efficiencyとデータコンパクションを実行できます。

プラットフォームに応じて、アップグレード時に次の条件が適用されます。

- 圧縮は、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。
- Storage Efficiencyは、シンプロビジョニングされたすべてのボリュームまたは既存のボリュームでデフォルトで有効になります。

AFF A70、AFF A90、またはAFF A1Kプラットフォームの場合、Storage Efficiencyは自動的に有効になり、設定は必要ありません。これは、新しく作成したすべてのシンプロビジョニングボリュームと既存のデータ（他のプラットフォームからAFF A70、AFF A90、またはAFF A1Kプラットフォームに移動されたボリュームを含む）に適用されます。

FAS70またはFAS90プラットフォームでは、アップグレード前にStorage Efficiency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でのみ、Storage Efficiencyがデフォルトで有効になります。CLIま

たはREST APIメソッドを使用して、新しく作成したボリュームでStorage Efficiencyを有効にできます。

- 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、32Kのインライン圧縮に自動的に変換されます。

AFF A70、AFF A90、またはAFF A1Kプラットフォームの場合、データは自動的に変換されます。

FAS70またはFAS90プラットフォームでは、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データが変換されます。

温度に基づくストレージ効率化は、AFF A70、AFF A90、AFF A1K、FAS70、FAS90のプラットフォームには適用されません。これらのプラットフォームでは、ホットデータやコールドデータに基づいて圧縮が行われなため、データがコールドになるのを待たずに圧縮が開始されます。

AFF A70、AFF A90、AFF A1K、FAS70、およびFAS90プラットフォームのStorage Efficiencyでは、連続する物理ブロックのシーケンシャルバッキングを使用して、圧縮データのストレージ効率がさらに向上します。

コントローラをAFF A70、AFF A90、AFF A1K、FAS70、またはFAS90にアップグレードする方法については、を参照して ["ONTAPハードウェアのアップグレードに関するドキュメント"](#) ください。

セキュリティ

クライアント認証と許可

ONTAPでは、標準的な方法を使用して、クライアントと管理者によるストレージへのアクセスを保護し、ウィルスから保護します。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を使用できます。

ONTAPは、信頼できるソースでIDを検証することで、クライアントマシンおよびユーザを認証します。ONTAPは、ユーザのクレデンシャル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

ローカルまたはリモートのユーザアカウントを作成できます。

- 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上に格納されます。
- 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、およびネームマッピング情報を検索します。ONTAP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

`a_name service switch table_` には、ネットワーク情報を検索するソースと、その検索順序を指定します (

UNIX システムの /etc/nsswitch.conf ファイルに相当する機能を提供します)。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 supportKerberos は、クライアント / サーバ実装でユーザ・パスワードを暗号化することによって「三次認証」を提供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を備えたKerberos 5認証 (krb5i) とプライバシーチェック機能を備えたKerberos 5認証 (krb5p) をサポートしています。

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操作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決定されます。

- 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Privilegesを持つユーザは、SMBクライアントおよび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のファイルとディレクトリのセキュリティ

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のアクセス権限のみがサポートされます。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実行するには、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の標準のファイルレベルセキュリティ

ストレージオブジェクトを表すファイルまたはディレクトリには、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では、リモートユーザの認証でSecurity Assertion Markup Language (SAML) がサポートされます。いくつかの一般的なIDプロバイダ (IdP) がサポートされています。サポートされているIdPとSAML認証を有効にする手順の詳細については、[を参照してください](#) **"SAML認証の設定"**。

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。

OAuth 2.0の標準的な機能は、いくつかの一般的な認証サーバとともにサポートされています。相互TLSベースの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や、ONTAP RESTロールやローカル ユーザ定義との統合など、多様な認証オプションを利用できます。詳細については、[を参照してください](#) **"ONTAP OAuth 2.0実装の概要"**。

カンリシヤニンシヨウト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。管理者がアクセスできるコマンドは、Role-Based Access Control (RBAC; ロールベースアクセス制御) によって決まります。

認証

クラスタおよび SVM の管理者アカウントは、ローカルまたはリモートのいずれか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、公開鍵、セキュリティ証明書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 では、DNS を除き、管理者アカウントの認証にクライアントの認証と同じネームサービスを使用します。

RBAC

管理者がアクセスできるコマンドは、管理者に割り当てられている `_role_assigned` コマンドで決まります。ロールは管理者のアカウントを作成するときに割り当てます。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できます。

ウィルススキャン

ストレージシステムに統合されたウィルス対策機能を使用すると、ウィルスやその他の悪意のあるプログラムからデータを保護できます。ONTAP ウィルススキャン (`_vscan`) は、クラス最高のサードパーティ製ウィルス対策ソフトウェアと ONTAP 機能を組み合わせたもので、どのファイルをスキャンするか、いつスキャンするかを柔軟に制御できます。

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバにオフロードされます。ネットアップが提供し、外部サーバにインストールされる ONTAP Antivirus Connector は、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。

- クライアントが SMB 経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、`_on_access_scanning_to` を使用します。ファイル処理は、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中断されます。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。それ以外の場合は、サーバからの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、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。たとえば、ピーク時を避けてスキャンを実行する場合などに便利です。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB経由で次回ファイルがアクセスされたときにそれらのファイル（ファイルが変更されていない場合）のファイルアクセスレイテンシが短縮されます。

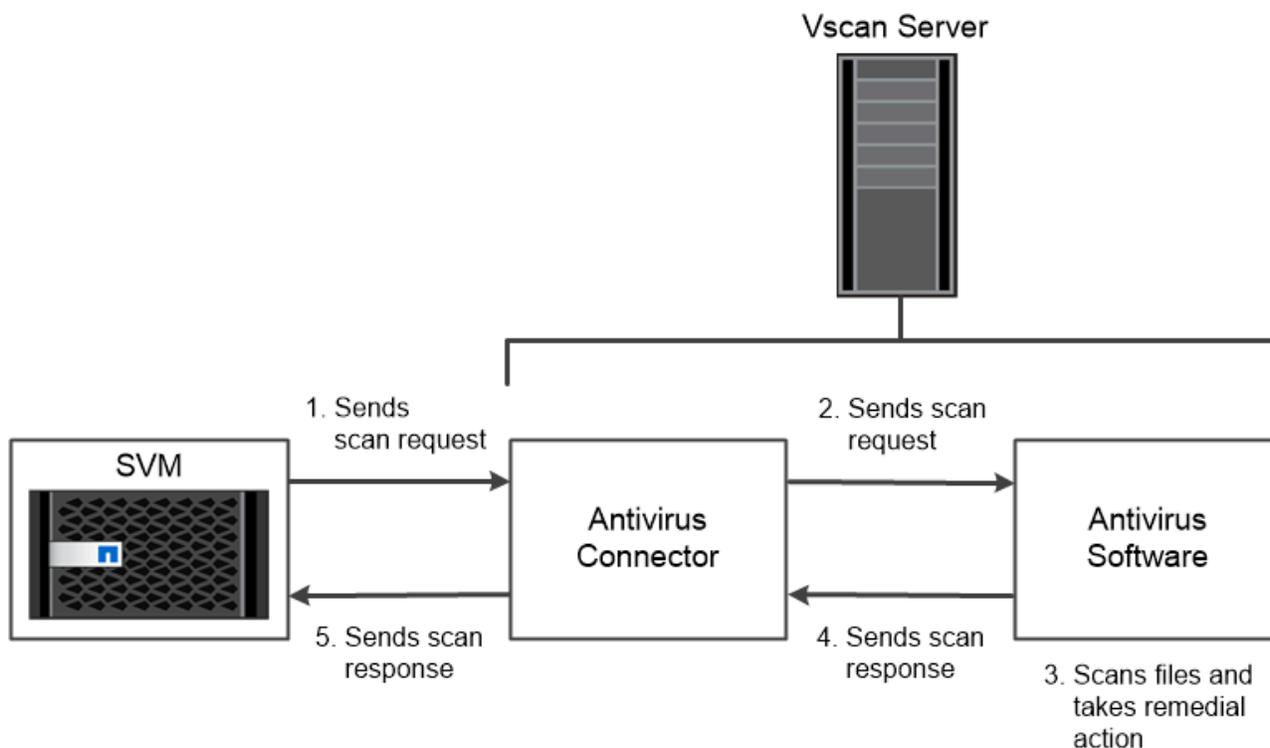
オンデマンドスキャンは、NFS経由でのみエクスポートされたボリュームも含め、SVMネームスペース内

の任意のパスに対して使用できます。

通常は、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、ウィルス対策ソフトウェアはソフトウェアの設定に基づいて感染ファイルに対して修復アクションを実行します。

* _ 災害復旧および MetroCluster 設定でのウイルススキャン _ *

ディザスタリカバリ構成およびMetroCluster構成では、ローカルクラスターとパートナークラスター用に個別のVscanサーバをセットアップ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接続で連邦情報処理標準（FIPS）140-2に準拠しています。次の暗号化ソリューションを使用できます。

- ハードウェアソリューション：

- NetAppストレージ暗号化（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は、FIPS 140-2認証を取得していないNVMe SEDに対してFull Disk Encryptionを提供します。

- ソフトウェアソリューション：

- NetAppアグリゲート暗号化 (NAE)

NAEは、アグリゲートごとに一意のキーを使用して、あらゆるドライブタイプ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ボリューム暗号化 (NVE)

NVEは、あらゆるドライブタイプ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、ボリュームごとに一意のキーを使用して有効にします。

ソフトウェア (NAEまたはNVE) 暗号化ソリューションとハードウェア (NSEまたはNVMe SED) 暗号化ソリューションの両方を使用して、保存データを二重に暗号化できます。NAE暗号化またはNVE暗号化は、ストレージ効率に影響しません。

NetAppストレージ暗号化

NetAppストレージ暗号化 (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。ディスクに保存されている暗号化キーがないと、データを読み取ることはできません。暗号化キーには、認証されたノードだけがアクセスできます。

I/O要求に対して、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は、自己暗号化HDDとSSDをサポートしています。NetAppボリューム暗号化とNSEを併用すると、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

NVMe SEDはFIPS 140-2認定を取得していませんが、AES 256ビット透過的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初めてディスクにアクセスしたときに生成されます。その後、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、ディスクで保存データが保護されます。

NetAppアグリゲート暗号化

NetAppアグリゲート暗号化 (NAE) は、アグリゲート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となり、NVEボリュームは除外されることです。

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ます。

ONTAP 9.7以降では"[NVEライセンス](#)"、およびオンボードまたは外部のキー管理を使用している場合、新しく作成し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ボリューム暗号化

NetApp Volume Encryption (NVE) は、一度に1つのボリュームの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、基盤となるデバイスがシステムから分離されている場合でもボリュームのデータが読み取られることはありません。

データ (Snapshotコピーを含む) とメタデータの両方が暗号化されます。データへのアクセスには、ボリュームごとに1つの一意のXTS-AES-256キーが使用されます。キーは、組み込みのオンボードキーマネージャによってデータと同じシステムに保護されます。

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、サポートされている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 サーバを使用するタイミング _](#) * オンボードキーマネージャを使用する方が安価で通常は便利ですが、次のいずれかに該当する場合は KMIP サーバをセットアップする必要があります。

- 暗号化キー管理ソリューションが、Federal Information Processing Standards (FIPS ; 連邦情報処理標準) 140-2またはOASIS KMIP標準に準拠している必要があります。
- マルチクラスターソリューションが必要です。KMIPサーバでは、複数のクラスターの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、複数のクラスターの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 Volume EncryptionおよびNetApp Aggregate Encryption"](#)

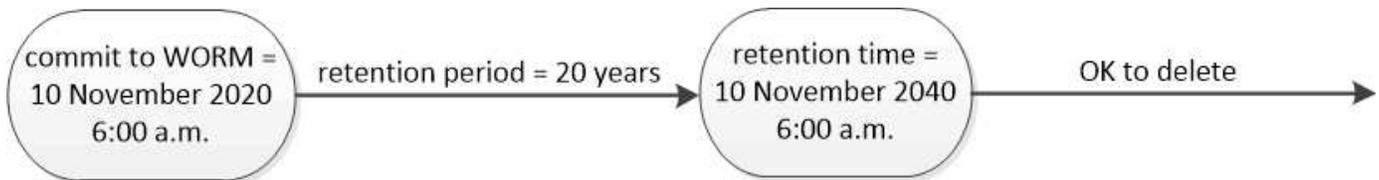
WORMストレージ

[_ 解決策 _](#) は、規制やガバナンスに準拠するために変更不可能な状態で重要なファイルを保管するために、[_ 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なコンプライアンス SnapLock です。

1つのライセンスで、SnapLockをStrict_Complianceモードで使用したり、SEC Rule 17a-4 (f) などの外部の

要件を満たすために_を使用したり、Looser_Enterpriseモードで_を使用したりすることができます。また、デジタル資産の保護に関する社内で義務付けられている規制を満たすこともできます。SnapLock では、改ざん防止機能を備えた ComplianceClock _を使用して、WORM ファイルの保持期間が経過したかどうかを判断します。

SnapVault から WORM 方式でセカンダリストレージの Snapshot コピーを保護するには、_ SnapLock for を使用します。SnapMirrorを使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所にWORMファイルをレプリケートできます。



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。

選択された概念と用語

VMware環境でのONTAPおよび関連するNetApp製品の使用方法について理解しておく、最初にいくつかの主要な用語と概念を理解しておく役立ちます。

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、SCSI (Small Computer System Interface) プロトコルまたはそのカプセル化された派生物の1つ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

VMware vSphere Storage API - Storage Awareness (VASA) は、ストレージ アレイとvCenterを統合して管理するための一連のAPI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_など、複数のコンポーネントに基づいています。ONTAPでは、プロバイダはONTAP Tools for VMware vSphereの一部として実装されます。

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 デバイスの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 システムを使用してアプリケーション、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を保護する、拡張性に優れた一元化されたプラットフォームです。Snapshot、SnapRestore、FlexClone、SnapMirror、SnapVaultなど、ネイティブのONTAP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、a_stretched cluster_deployment.vMSCソリューションを有効にして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のアクティブ同期 (旧称SMBC) でサポートされます。これらのソリューションは、ドメインに障害が発生した場合のビジネス継続性を強化します。耐障害性モデルは、選択した構成に基づいています。

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永続的予約について"](#)
- ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)

アプリケーション対応のデータ管理

アプリケーション対応のデータ管理を使用すると、ONTAPで導入するアプリケーションを、ストレージではなくアプリケーションの観点から指定できます。System ManagerとREST APIを使用して、最小限の入力でアプリケーションを設定し、データを提供できるように準備することができます。

アプリケーション対応のデータ管理機能を使用すると、個々のアプリケーションレベルでストレージをセットアップ、管理、監視できます。この機能には、関連するONTAPのベストプラクティスが組み込まれており、必要なパフォーマンスサービスレベルと使用可能なシステムリソースに基づいてストレージオブジェクトを分散配置し、アプリケーションを最適にプロビジョニングできます。

アプリケーション対応のデータ管理機能には、一連のアプリケーションテンプレートが含まれています。各テンプレートは、アプリケーションの構成をまとめて記述する一連のパラメータで構成されています。これらのパラメータは、アプリケーション管理者がONTAPシステムでプロビジョニングするストレージの特性（データベースサイズ、サービスレベル、LIFなどのプロトコルアクセス要素、ローカルの保護条件、リモートの保護条件など）を定義します。これらのパラメータにはデフォルト値があらかじめ設定されていることがよくあります。ONTAPは、指定されたパラメータに基づいて、LUNやボリュームなどのストレージエンティティをアプリケーションに適したサイズとサービスレベルで設定します。

アプリケーションに対して次のタスクを実行できます。

- アプリケーションテンプレートを使用してアプリケーションを作成する
- アプリケーションに関連付けられたストレージを管理する
- アプリケーションの変更または削除
- アプリケーションの表示
- アプリケーションのSnapshotコピーを管理します。
- 同じボリュームまたは異なるボリュームのLUNを複数選択してデータ保護機能を提供するために作成 [整合グループ](#)

FabricPool

NetAppをご利用のお客様の多くは、ほとんどアクセスされない大量のデータを格納しています。これは、`_COM_DATA`と呼ばれます。また、お客様は頻繁にアクセスされるデータも保有しており、これを`_hot_data`と呼んでいます。最高のパフォーマンスを得るためには、ホットデータを最速のストレージに保存することが理想的です。コールドデータは、必要に応じてすぐに利用できるかぎり、低速のストレージに移動できます。では、データのどの部分がホットで、どの部分がコールドであるかを知るには、どうすればよいでしょうか。

FabricPoolは、ハイパフォーマンスなローカル階層（アグリゲート）とクラウド階層の間で、アクセスパターンに基づいてデータを自動的に移動するONTAPの機能です。階層化することで、高価なローカルストレージをホットデータ用に解放し、コールドデータを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利用できる状態に保ちます。FabricPoolはデータアクセスを常時監視し、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ことは、クラウドの効率性を高め、ハイブリッドクラウド構成を作成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します。

しかし、FabricPoolは、オンプレミスのデータをクラウドに階層化するだけのものではありません。多くのお客様がCloud Volumes ONTAPでFabricPoolを使用して、クラウドプロバイダ内の高コストのクラウドストレージから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、またはを使用してFabricPool対応ボリュームで分析をキャプチャできます"[ファイルシステム分析](#)"[温度に敏感なストレージ効率](#)"。

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、アプリケーションを変更す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、継続的な管理は必要ありません。

コールドデータは、大手クラウドプロバイダのオブジェクトストレージに格納できます。また、NetApp StorageGRIDを選択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持することで、パフォーマンスを最大限に高め、データを完全に管理できます。

関連情報

["FabricPool System Managerのドキュメント"](#)

["BlueXP の階層化"](#)

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

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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