



概要と概念 ONTAP 9

NetApp
April 24, 2024

目次

概要と概念	1
ONTAP の概念	1

概要と概念

ONTAP の概念

概念の概要

クラスタストレージ、高可用性、仮想化、データ保護など、ONTAPデータ管理ソフトウェアには次の概念があります。Storage Efficiency、セキュリティ、FabricPoolストレージ解決策を設定する前に、ONTAP のすべての機能とメリットを理解しておく必要があります。

追加情報の場合は、以下を参照してください。

- ["クラスタと SVM の管理"](#)
- ["ハイアベイラビリティ \(HA\) ペア"](#)
- ["ネットワークと LIF の管理"](#)
- ["ディスクおよびアグリゲートの管理"](#)
- ["FlexVol 、 FlexClone テクノロジー、 Storage Efficiency 機能"](#)
- ["SAN ホストプロビジョニング"](#)
- NAS ファイルアクセス
 - ["NFS の管理"](#)
 - ["SMBの管理"](#)
- ["ディザスタリカバリとアーカイブ"](#)

ONTAPプラットフォーム

ONTAP データ管理ソフトウェアは、ブロックアクセスプロトコルまたはファイルアクセスプロトコルを使用して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。高速フラッシュから低コストの回転式メディア、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サポートされます。

ONTAPの実装は、ネットアップが開発したFAS、AFF AシリーズとCシリーズ、オールSANフラッシュレイ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) で実行されます。専門的な導入により、業界最高のコンバージドインフラ (FlexPod Datacenter) が提供されます。

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。

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採用されているアーキテクチャです。この実装でほとんどの ONTAP の機能が使用されるため、最初は ONTAP テクノロジーの概念を理解しておくことを推奨します。

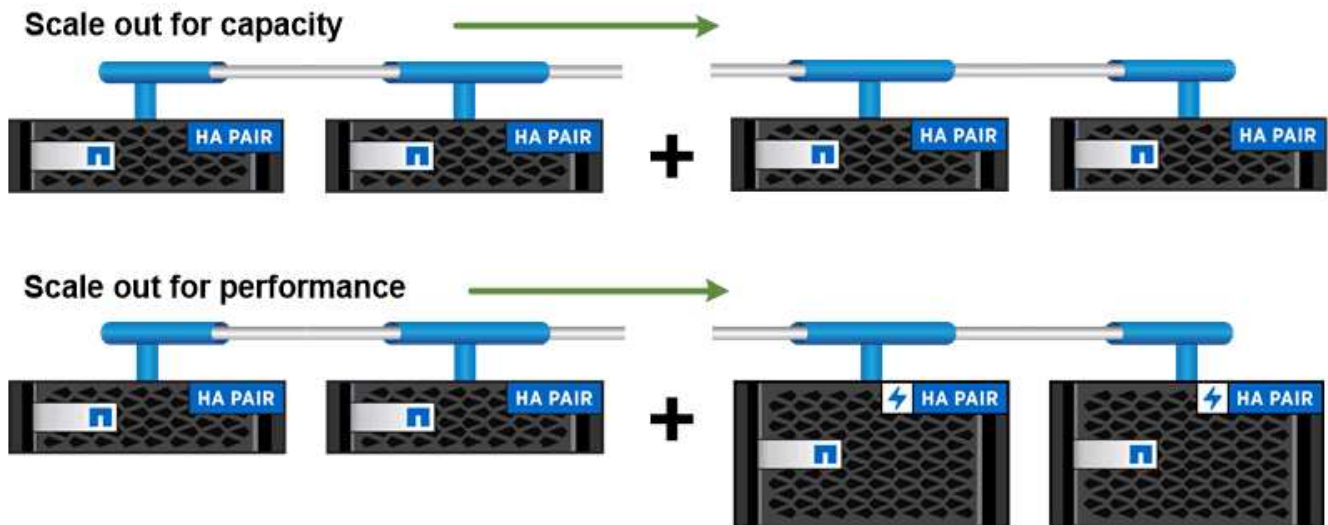
一般にデータセンターアーキテクチャでは、ONTAP データ管理ソフトウェアを実行する専用の FAS コントローラまたは AFF コントローラを導入します。各コントローラとそのストレージ、ネットワーク接続、およびコントローラで実行されている ONTAP のインスタンスを合わせて、*node*. と呼びます

ノードはハイアベイラビリティ（HA）ペアを構成します。このペアを複数配置したものがクラスタです（SAN の場合は最大 12 ノード、NAS の場合は最大 24 ノード）。ノードは、専用のプライベートなクラスター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。物理ストレージと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 ペアの各ノードで同じストレージレイモデルを使用する必要があります。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の組み合わせを使用できます。スケールアウトすることで、容量を増やすには同じストレージ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

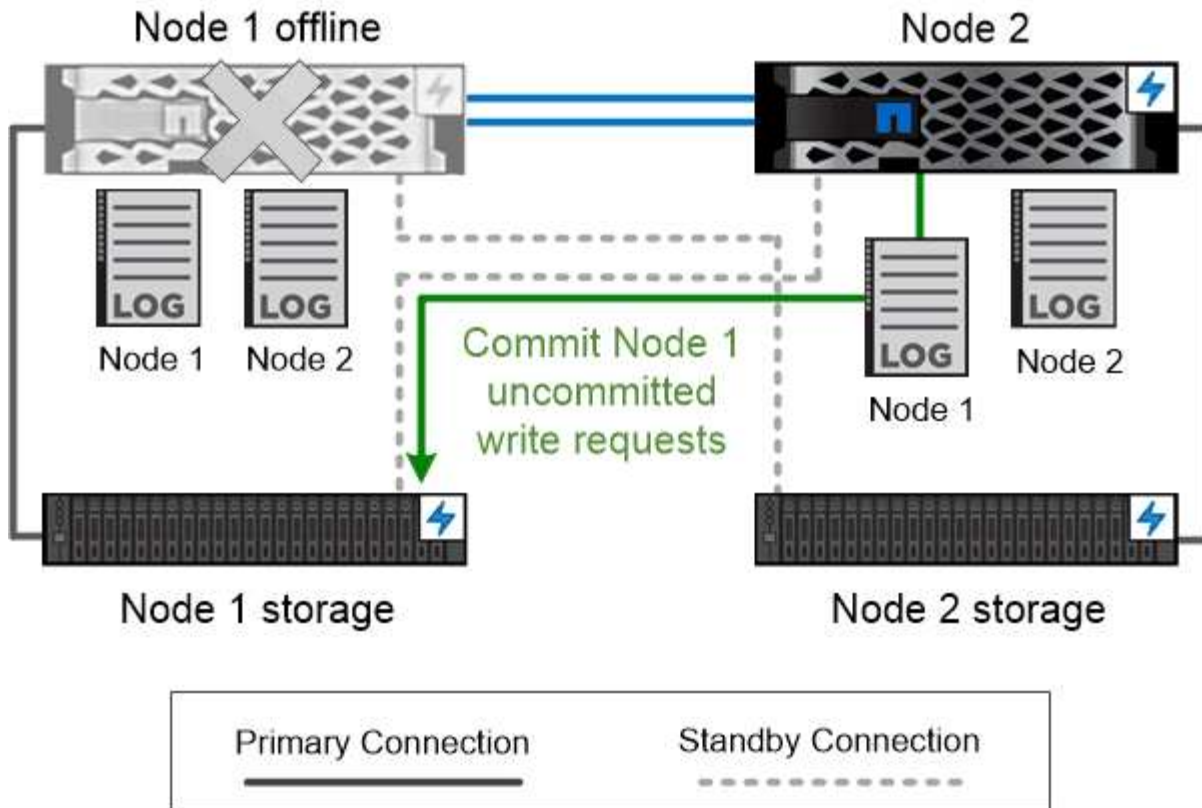
クラスタノードは、フォールトトレランスとノンストップオペレーションを実現するために、`_high-availability (HA) ペア _`で構成されます。ノードに障害が発生した場合や定期的なメンテナンスのためにノードを停止する必要がある場合、パートナーはそのストレージをテイクオーバーしてデータの提供を継続できます。ノードがオンラインに戻ったときに、`partner_ギブバック_storage`を提供します。

HA ペアは、必ず同じモデルのコントローラで構成されます。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発生した場合、両方のノードの NVRAM に要求が記録されたのち、クライアントまたはホストに応答が返されます。フェイルオーバーの際は、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てデータの整合性が維持されます。

テイクオーバーが発生した場合、各ノードはもう一方のコントローラのストレージメディアに接続して他方のノード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、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 50% 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 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続行します。ノードのストレージはテイクオーバーせず、データ提供機能だけをテイクオーバーします。

AutoSupport と Active IQ 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通じて、人工知能を利用した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によって分析された計測データを送信します。

Active IQ では、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でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、Active IQ が提供す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）。

Active IQ 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。Active IQ では、ONTAP の新しいバージョンにアップグレードすることで解

決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。

- システムの健全性を表示します。Active IQ ダッシュボードで、健全性に関する問題が報告されるため、これらの問題の解決に役立ちます。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。
- パフォーマンスを管理Active IQ には、System Manager に表示されるよりも長時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します。
- 効率性の最大化Storage Efficiency 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します。
- インベントリと構成を表示します。Active IQ は、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に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認して、契約期間を終了しないようにします。

関連情報

["ネットアップのマニュアル：Active IQ Digital Advisor"](#)

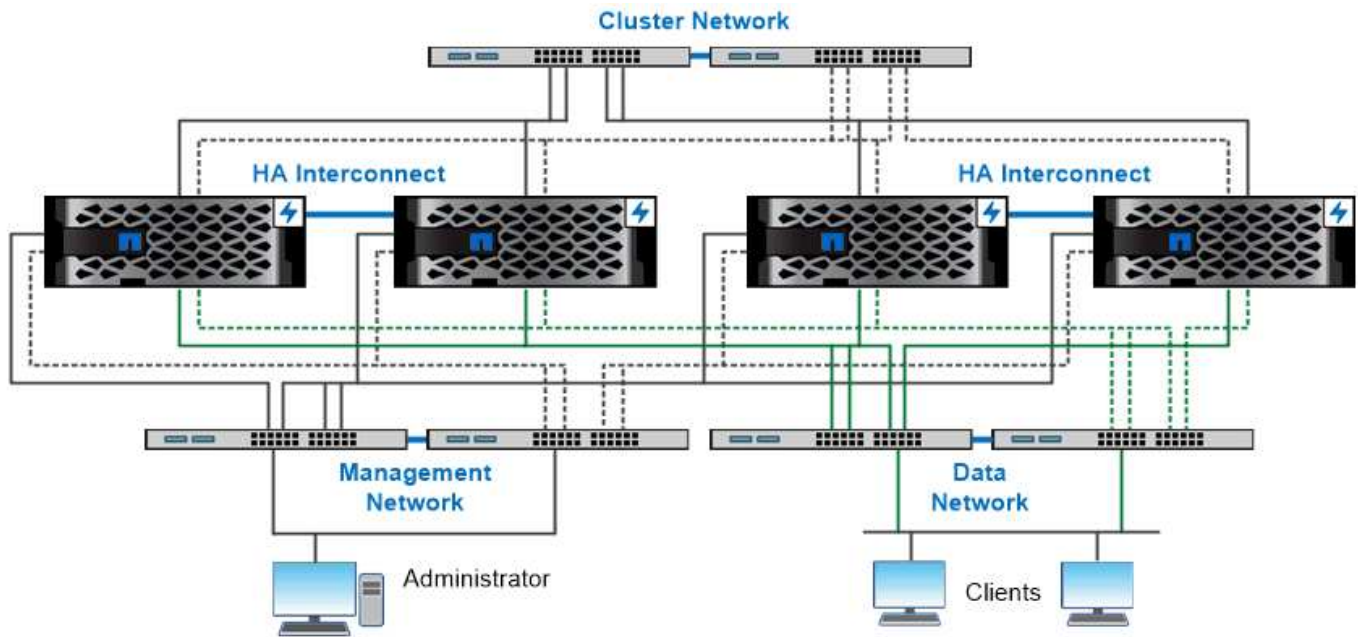
["Active IQ を起動します"](#)

["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

ONTAP データセンターの一般的なネットワークアーキテクチャは、クラスターインターコネクト、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。論理ポートには、インターフェイスグループと VLAN があります。

インターフェイスグループ

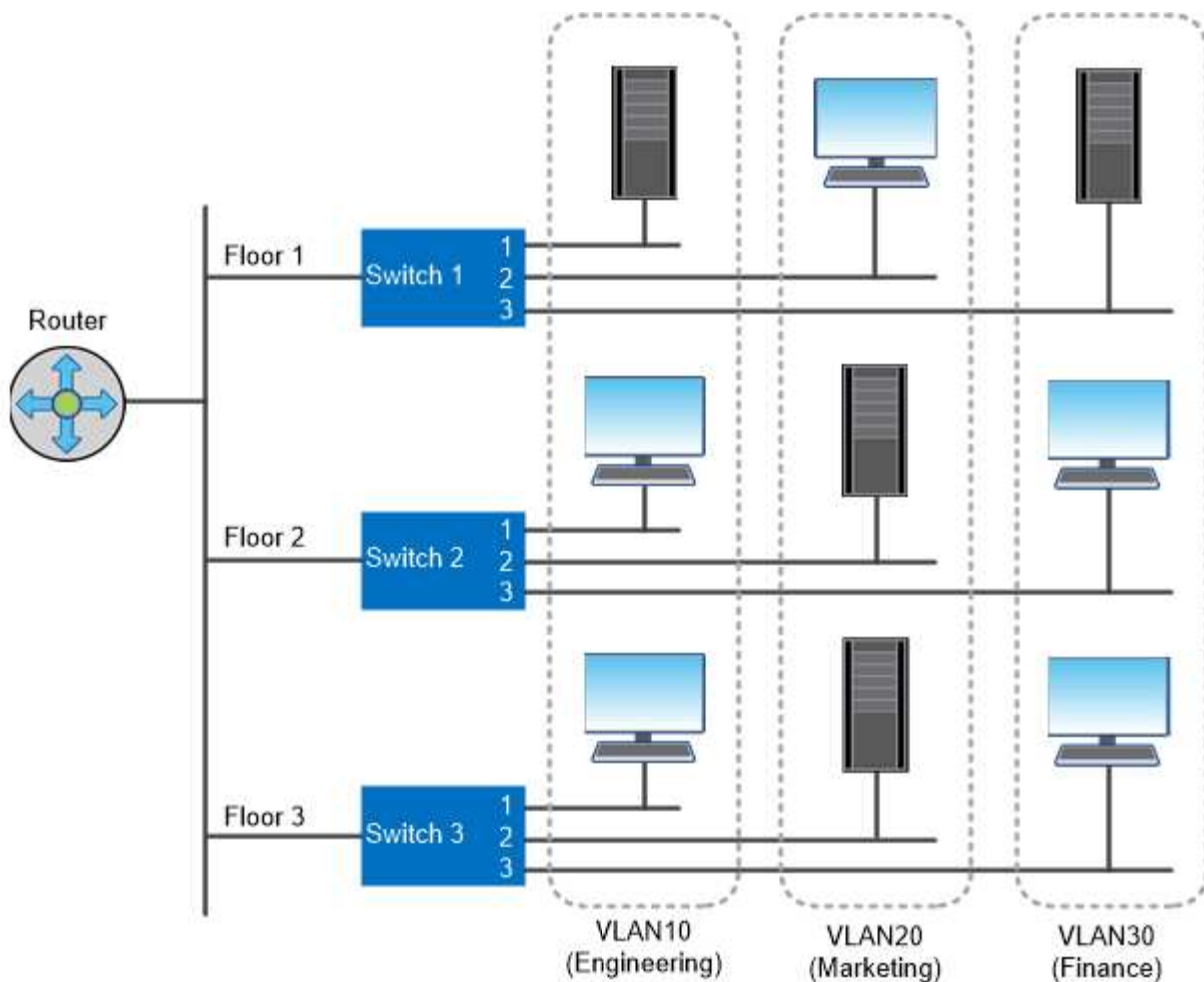
_インタフェースグループ_複数の物理ポートを1つの論理「トランクポート」に結合します。複数のPCIスロット内のNICのポートで構成されるインターフェイスグループを作成することで、1つのスロットに障害が発生した場合でもビジネスクリティカルなトラフィックの停止を回避することができます。

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。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イ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 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。

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いため、地理的に離れた場所に配置することもできます。



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、で説明しています [NAS パスのフェイルオーバー](#)。

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のクライアントが、IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタの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、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 トラップ

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 接続に対する連邦情報処理標準（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 Remote Direct Memory Access（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メモリとホストシステムメモリの間でデータを直接コピーでき、CPU の中断やオーバーヘッドは発生しません。

RDMA 経由の NFS

ONTAP 9.10.1 以降では、を設定できます ["RDMA 経由の NFS"](#) NVIDIA GPU を搭載したホストで GPU アクセラレーション対応のワークロードに NVIDIA GPUDirect Storage を使用できるようにするため。

RDMA クラスターインターコネクト

RDMA クラスターインターコネクトにより、レイテンシが低減され、フェイルオーバー時間が短縮され、クラスター内のノード間の通信が高速化されます。

ONTAP 9.10.1 以降では、X1151A クラスター NIC を使用する場合、特定のハードウェアシステムでクラスターインターコネクト RDMA がサポートされます。ONTAP 9.13.1 以降では、X91153A NIC でクラスターインターコネクト 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 のバージョン
<ul style="list-style-type: none">• A400• ASA A400	ONTAP 9.10.1 以降
<ul style="list-style-type: none">• AFF A900 の略• 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、RDMA インターコネクトを使用するための追加の設定は必要ありません。

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である NFS、SMB、FC、FCoE、iSCSI をすべてサポートしています。NVMe/FC および 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、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、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で、使用可能な専用の FC ネット

ワークがない場合に適しています。

NVMe/FC

NVMe / FC 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てい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) サーバを有効にして、S3バケットを使用してオブジェクトストレージ内でデータを提供できます。

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を2つサポートしています。

- FabricPool 階層をローカルクラスタ（ローカルバケットへの階層）またはリモートクラスタ（クラウド階層）のバケットに配置します。
- S3 クライアントアプリケーションから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、ハードウェアや管理の追加なしで既存のクラスタの S3 機能を利用する場合に適しています。300TB を超える環境の場合、ネットアップの解決策ソフトウェアは、オブジェクトストレージ向けの主力製品である StorageGRID として引き続き提供されます。詳細はこちら ["StorageGRID"](#)。

ディスクとアグリゲート

=
:allow-uri-read:

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）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。

サイジング推奨事項の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。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の必要性和、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。

ミラーされた、ミラーされていないローカル階層（アグリゲート）

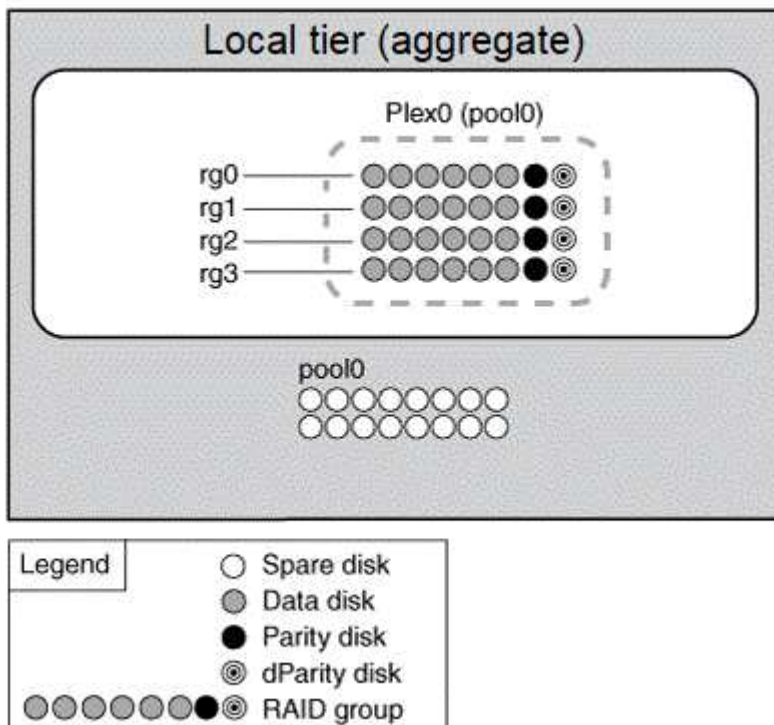
ONTAP には、SyncMirror というオプション機能があります。この機能を使用すると、コピー内のローカル階層（アグリゲート）データまたはプレックスを同期的にミラーリングし、別々のRAIDグループに格納することができます。プレックスを使用すると、RAID タイプで保護されるディスク数よりも多くのディスクで障害が発生した場合や、RAID グループのディスクへの接続が切断された場合に、データ損失を防ぐことができます。

System ManagerまたはCLIを使用してローカル階層を作成する場合は、ローカル階層をミラーリングするかミラーしないかを指定できます。

ミラーされていないローカル階層（アグリゲート）の機能

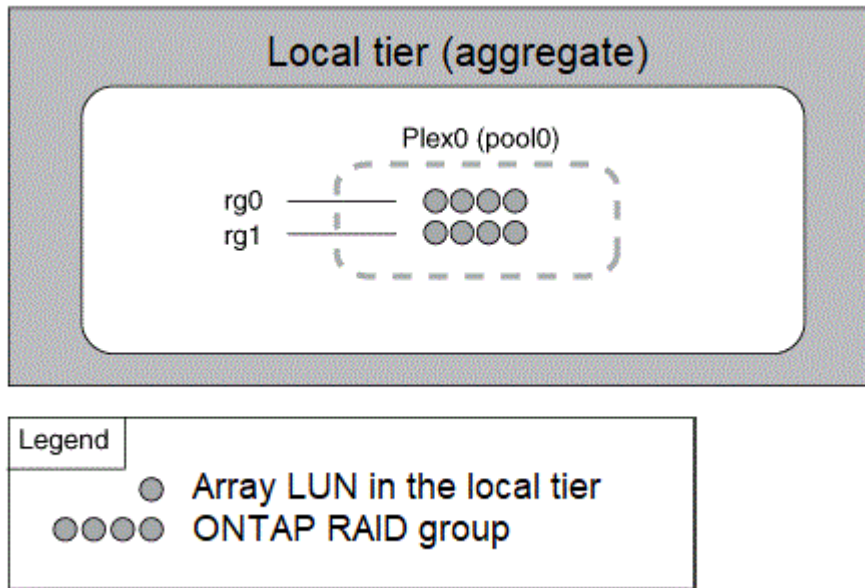
ローカル階層をミラーリングするように指定しない場合、ミラーされていないローカル階層（アグリゲート）として作成されます。ミラーされていないローカル階層には、プレックス_（データのコピー）が1つだけ含まれ、このローカル階層に属するすべてのRAIDグループが含まれます。

次の図に、1つのプレックスを含む、ディスクで構成されたミラーされていないローカル階層を示します。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があり、パリティディスクとdparity（ダブルパリティ）ディスクが1本ずつ含まれます。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



次の図に、1つのプレックスを含む、アレイLUNを含むミラーされていないローカル階層を示します。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するすべてのアレイ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することができます。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）、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、影響を受けていないプレックスで障害の原因を修正する間もデータの提供が継続されるため、データ損失が防止されます。問題のあるプレックスが修正されたら、2つのプレックスが再同期化され、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 のデータの複製であり、RAID グループも同じです。32本のスペアディスクは、各プールに16本のディスクを使用してpool0またはpool1に割り当てられます。

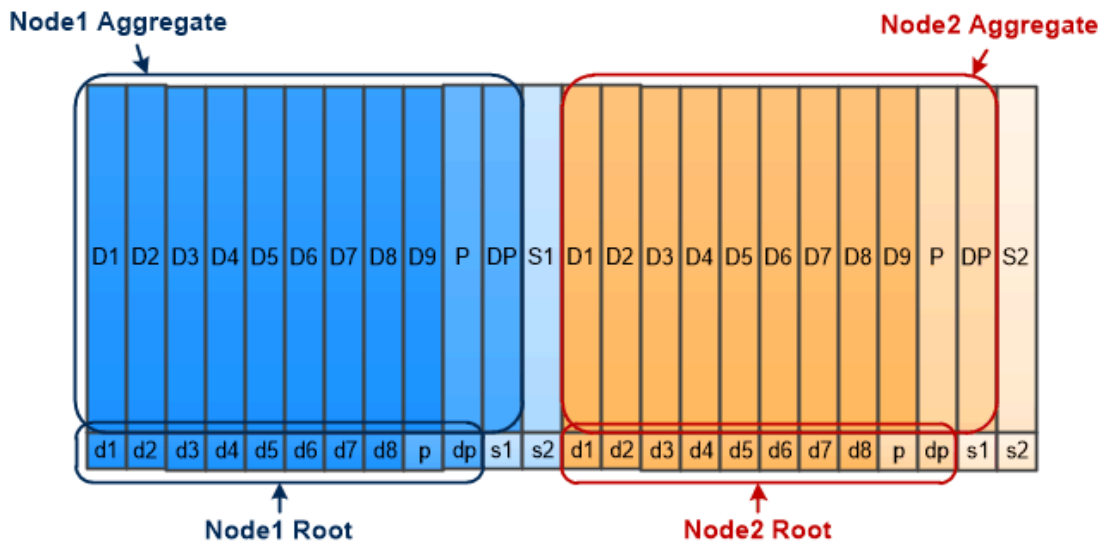
ルート / データパーティショニング

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やルート / 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。

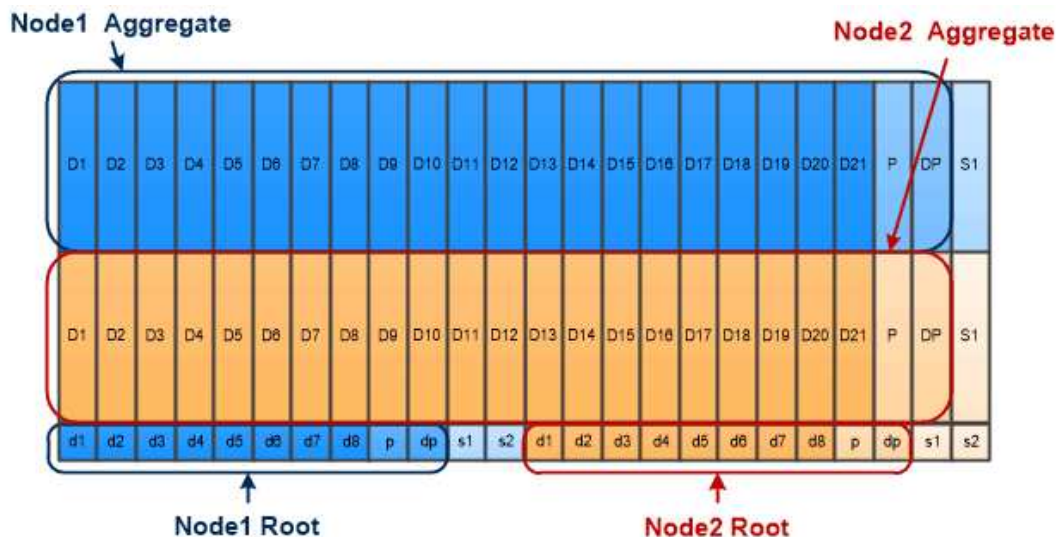
RAID-DP タイプのルートアグリゲートは、通常、1つのデータディスクと2つのパリティディスクで構成されます。これは、アグリゲート内の各 RAID グループ用に2つのディスクがパリティディスクとしてすでにリザーブされている場合、ストレージシステムファイルの料金を支払う「パリティ税」として相当します。

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.

図からわかるように、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。どちらも出荷時点で構成され、エントリレベルの FAS2xxx、FAS9000、FAS8200、FAS80xx、および AFF システムについてはルート / データパーティショニング、AFF システムについてはのみルート / データ / データパーティショニングが使用されます。

の詳細を確認してください ["アドバンスドドライブパーティショニング"](#)。

ルートアグリゲート用にパーティショニングされたドライブ

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するドライブ数を把握しておく、ルートパーティション用にリザーブす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決定する際に役立ちます。

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、オールフラッシュ 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。

SSD だけが接続されている All Flash FAS プラットフォームおよび FAS プラットフォームでは、システムの初期化時にコントローラに接続されるすべてのドライブがパーティショニングされます。ノードあたりの最大数は 24 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、および 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、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 を拡張および縮小したり、FlexVol ボリュームを移動したり、FlexVol ボリュームの効率的なコピーを作成したりできます。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。

NAS 環境ではボリュームに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、FlexVol ボリュームの 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す。ONTAP が残りの処理を実行します。

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。SVM は、ハイパーバイザーで実行される仮想マシンと同様に、物理リソースを抽象化した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。

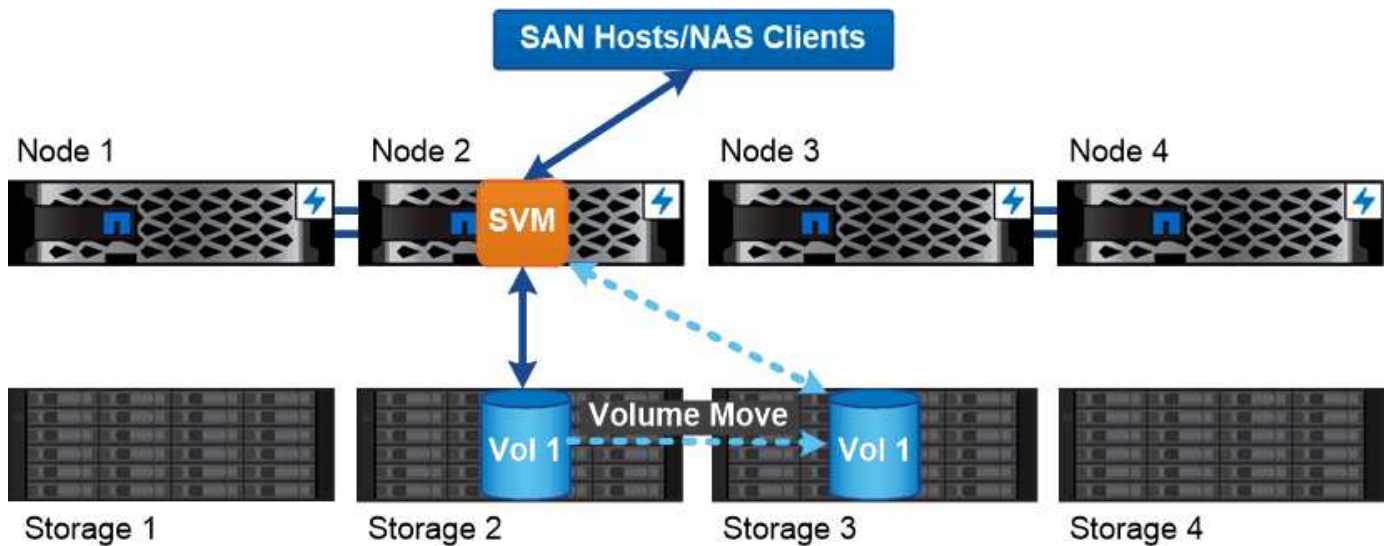
SVM は、1 つ以上のボリュームから 1 つ以上の `network_logical interfaces` (LIF ; ネットワーク論理インターフェイス) を通じてクライアントおよびホストにデータを提供します。ボリュームは、クラスタ内の任意のデータアグリゲートに割り当てることができます。LIF は任意の物理ポートまたは論理ポートでホストできます。ハードウェアのアップグレード、ノードの追加、パフォーマンスの分散、アグリゲート間での容量の最適化などを行う際、ボリュームと LIF のどちらもデータサービスを中断することなく移動できます。

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、それぞれ独自のセキュリティ、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に追加されると、`_node svm_is` が作成されます。
- IPspace 内のクラスタレベルの通信用に、`_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 もあります。



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仕様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とクラスタ管理者（予約された名前） `admin` は、クラスタのセットアップ時に自動的に作成されます。

デフォルトを持つクラスタ管理者 `admin` ロールは、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、が割り当てられます `vsadmin` デフォルトではロール。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。

`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。

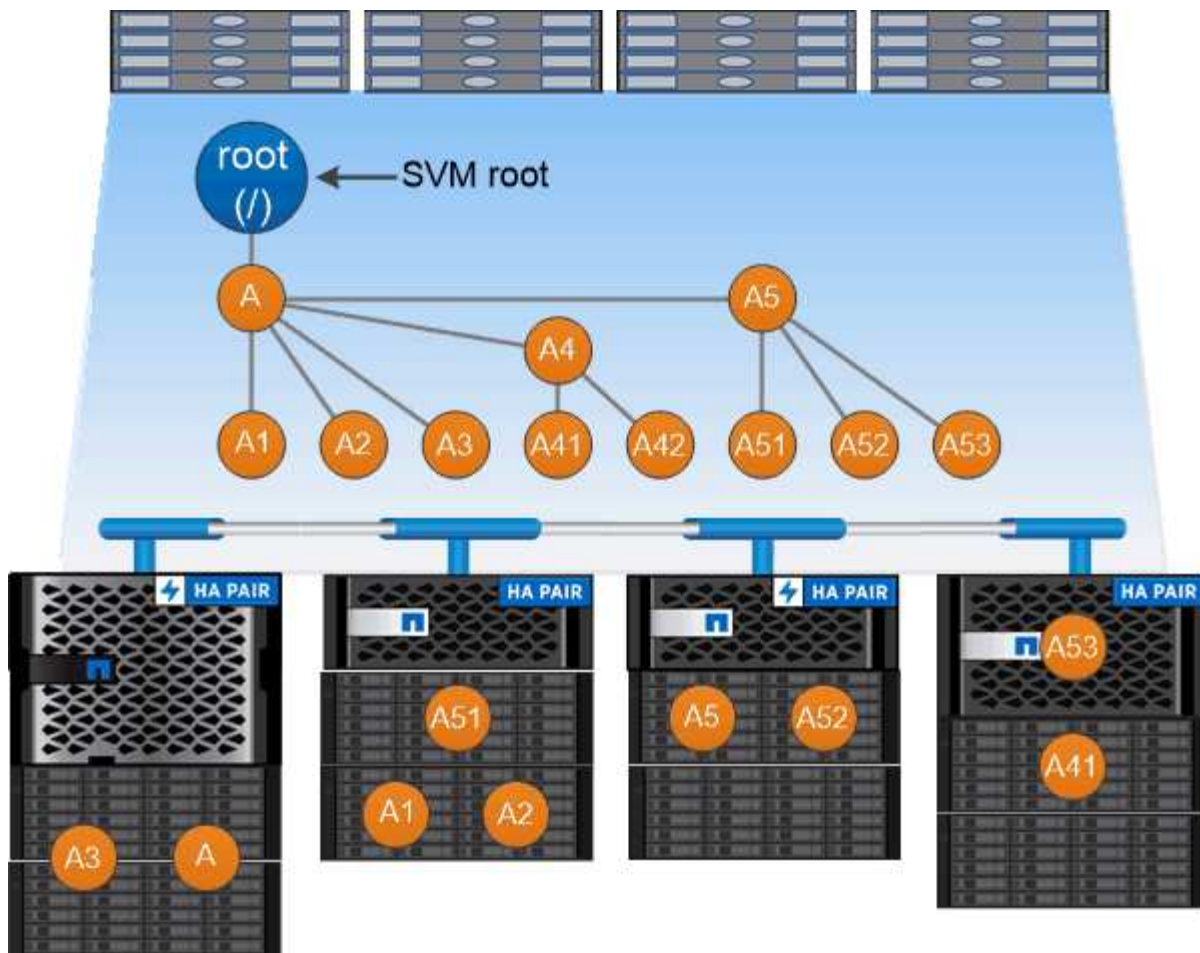
NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、`nfs_export_` をマウントするか、`SMB_share` にアクセスします。`_` エクスポートまたは共有は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされたボリュームにのみアクセスします。

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、になることがあります `/vol1/vol2/vol3`` または ``/vol1/dir2/vol3`` あるいは ``/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の概要

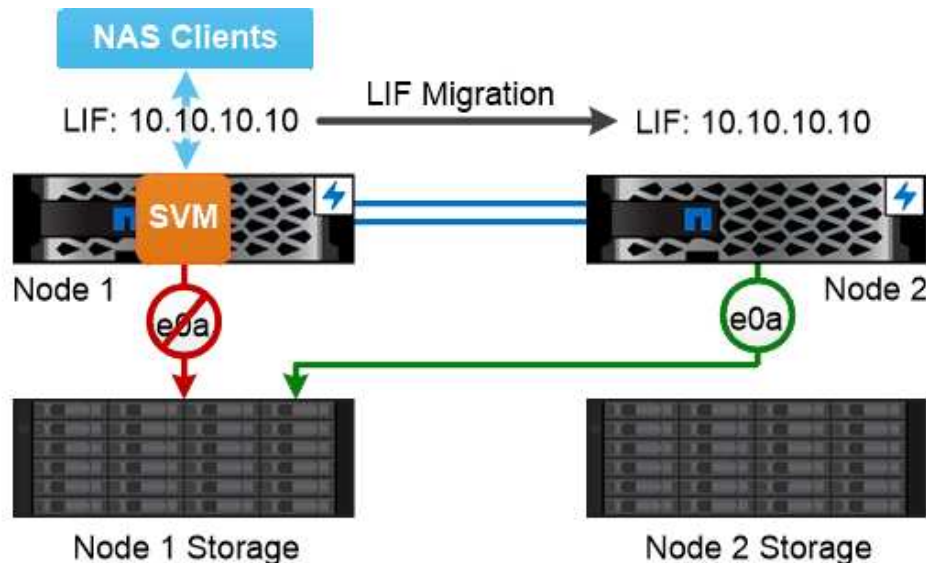
ONTAP でのパスのフェイルオーバーは、NAS トポロジと SAN トポロジで大きく異なります。NAS LIF は、リンク障害が発生すると別のネットワークポートに自動的に移行します。SAN LIF は、障害の発生後に手動で移動しないかぎり移行しません。代わりに、ホストのマルチパステクノロジーによって、同じ SVM 上の、別のネットワークポートにアクセスしている別の LIF にトラフィックが転送されます。

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たものです。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には、各 VLAN で別々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、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た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場合、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した方が一般に簡単で間違いも少なくなります。

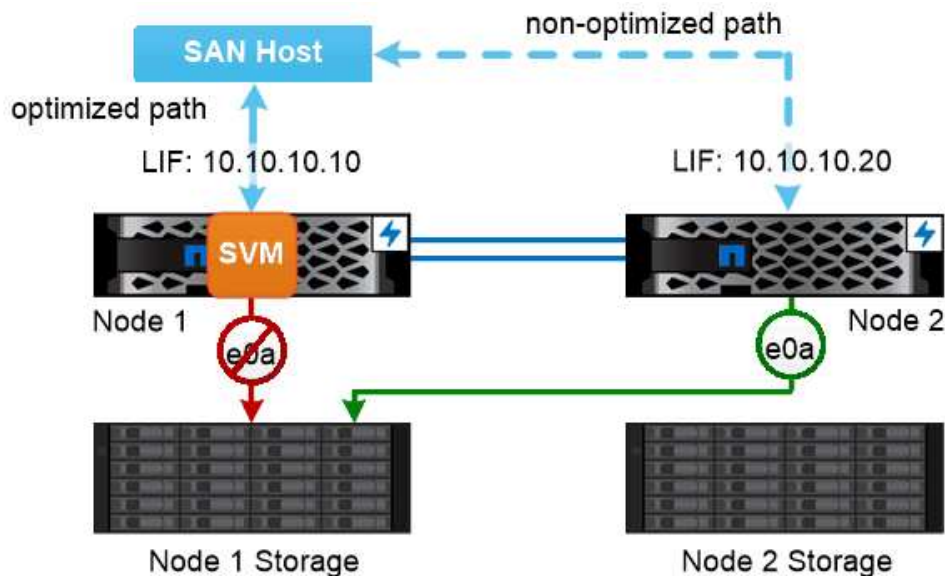
SANパスのフェイルオーバー

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_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 の選択的 LUN マップ（SLM）は、ホストから LUN へのパスの数をデフォルトで制限します。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。

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、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。

負荷分散

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することができます。

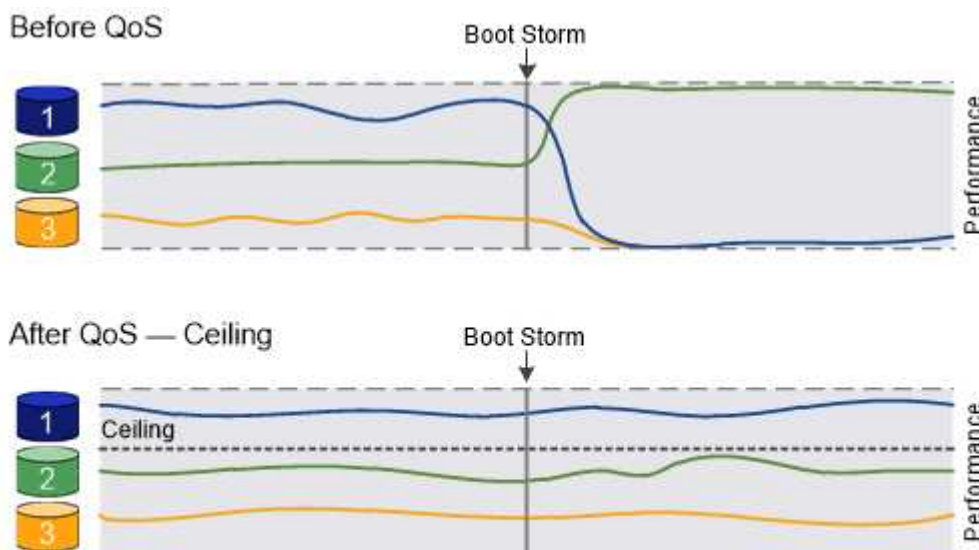
スループットの上限

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しています。

`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。



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 のスループットの下限により、ワークロード 2 からの要求に関係なく、最小スループットが確保されています。

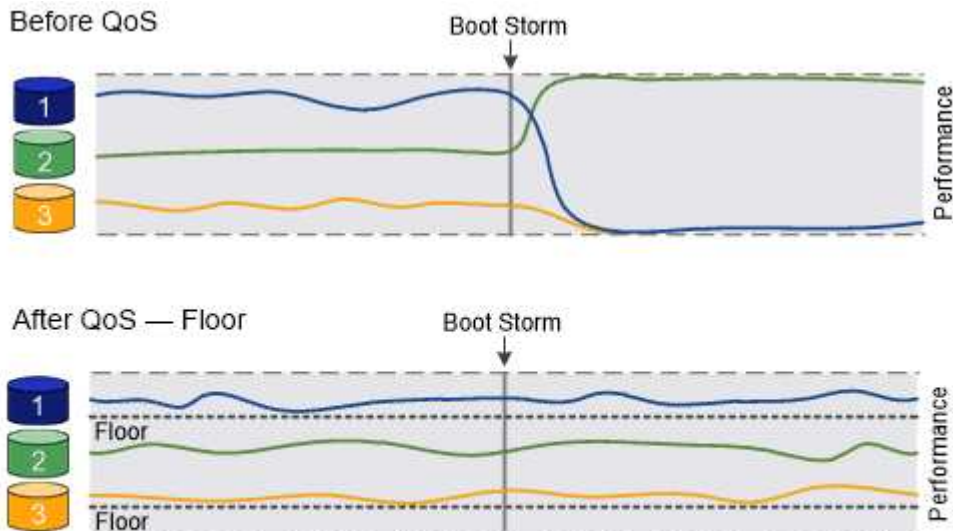


これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

ワークロードとは、ボリューム、LUN、または ONTAP 9.3 以降のファイルの I/O 処理のことです。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るときや重要な処理を実行していないときでも、ワークロードのスループットは指定された下限を 5% まで下回ることができます。



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。

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。



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 以前では使用できません。

[+]

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更されないかぎり 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た 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 によって比率が一定になるように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 の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。その後、クラウドサービスが登場し、ネットアップ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 ONTAP レプリケーションが採用されるようになりました。これらすべての用途において、ONTAP の Snapshot テクノロジーが基盤となります。

Snapshot コピー₁ 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。

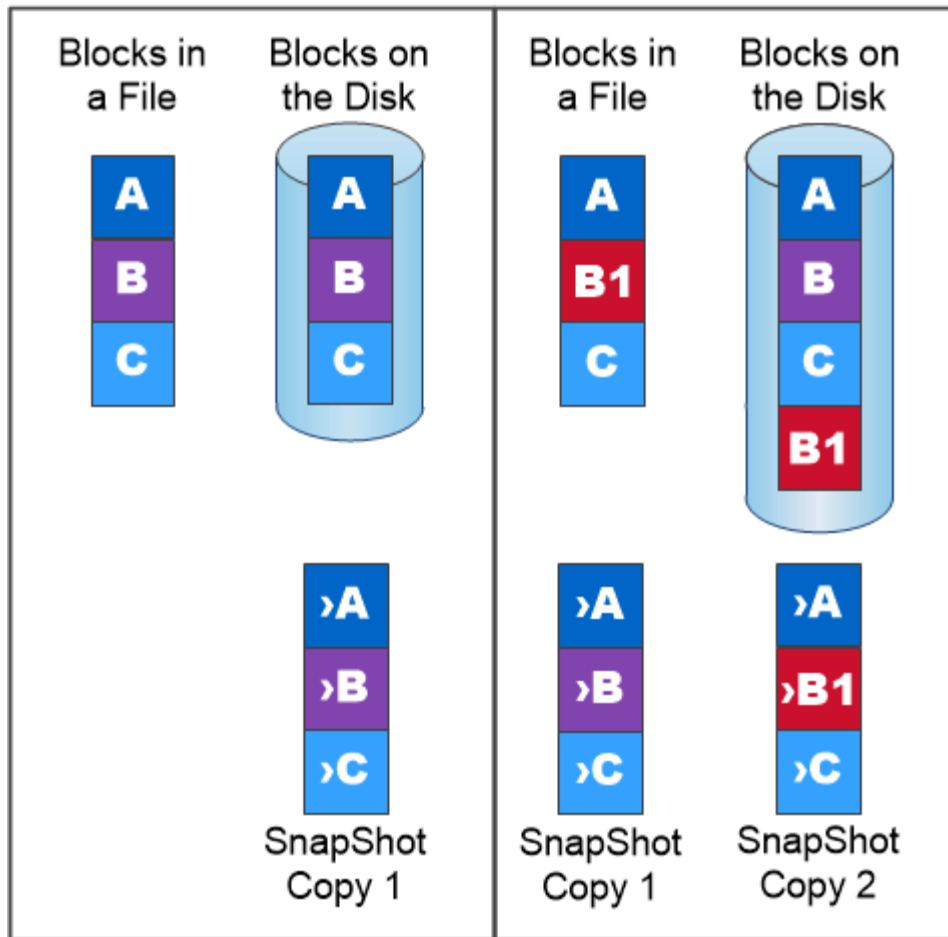
Snapshot コピーの効率性は、ONTAP の中核的なストレージ仮想化テクノロジーである ITS Write Anywhere File Layout（WAFL）によって実現します。₂ WAFL は、データベースと同様に、メタデータを使用してディスク上の実際のデータブロックを参照します。ただし、データベースとは異なり、WAFL は既存のブロックを上書きしません。更新されたデータは新しいブロックに書き込まれ、メタデータが変更されます。

Snapshot コピーの効率性は、コピーデータブロックではなく、ONTAP が Snapshot コピーの作成時にメタデータを参照するためです。これにより、他のシステムがコピーするブロックを特定する際に発生する「シーク時間」と、コピー自体を作成するコストの両方が削減されます。

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。ONTAP は、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を再構築します。

Snapshot ポリシー₃ 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 コピーの命名方法、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 Snapshot コピーを 1 つ作成し、最新のコピーを 2 つ保持して、「毎日」（タイムスタンプ付き）という名

前を付け、レプリケーション用に「毎日」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 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。

データのミラーリングはボリュームレベルで行われます。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、クラスタと SVM の交換が可能になります データをセキュアに保護



また、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、S3 SnapMirror 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 以外のシステムで使用できます。

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。保持処理によって、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。

ベースライン作成後は 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事例で示すように、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上のコントローラがプライマリシステム上のコントローラと同じであるか、ほぼ同じ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、ネットアップ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 ポリシーを作成するときに、レプリケーションを 1 回だけ行うか繰り返し行うかを選択できます。

SnapMirror Cloud は、データ保護ワークフローをクラウドに移行する ONTAP ユーザ向けに設計されたバックアップおよびリカバリのテクノロジーです。従来のバックアップからテープへのアーキテクチャから脱却するには、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代替リポジトリとして使用できます。**SnapMirror Cloud** は、持続的な増分バックアップ戦略の一環として、ONTAP とオブジェクト間のストレージレプリケーションを提供します。

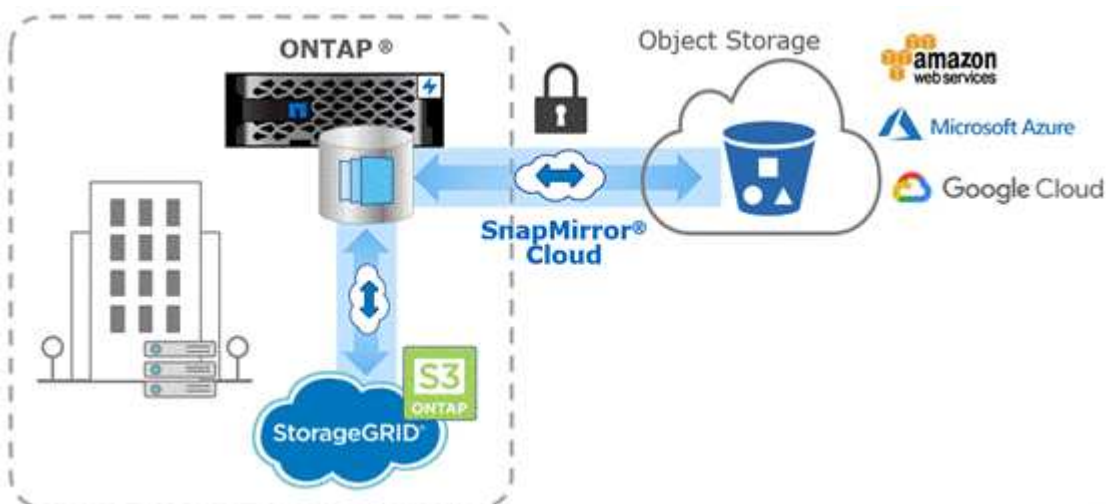
SnapMirror Cloud は、ONTAP 9.8 で **SnapMirror** レプリケーションテクノロジーファミリーの拡張機能として導入されました。**SnapMirror** は ONTAP から ONTAP へのバックアップによく使用されますが、**SnapMirror Cloud** は同じレプリケーションエンジンを使用して、ONTAP の Snapshot コピーを S3 準拠のオブジェクトストレージバックアップに転送します。

バックアップのユースケースをターゲットとした **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ます。**SnapMirror** と同様に、最初の **SnapMirror Cloud Backup** はボリュームのベースライン転送を実行します。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 Cloud 関係は、ONTAP システムと、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（Amazon S3、Google Cloud Storage、Microsoft Azure Blob Storage など）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 Cloud 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をオーケストレーションするための承認されたアプリケーションが必要です。**SnapMirror Cloud** 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 Cloud** レプリケーションのサポートを提供するサードパーティのバックアップパートナーが複数存在する。参加ベンダーは、で入手できます ["ネットアップのブログ"](#)。
- ネットアップネイティブの ONTAP 環境向け解決策向け BlueXP バックアップ/リカバリ
- 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ための API、または自動化ツールを活用するための API



SnapVault アーカイブ

SnapMirror ライセンスは、バックアップの SnapVault 関係とディザスタリカバリの 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 ライセンスが廃止され、SnapMirror ライセンスを使用してバックアップ関係、ミラー関係、およびミラー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 コピーを ONTAP から ONTAP にレプリケートするために使用されます。これにより、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がサポートされます。

_ 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。SnapMirror 関係では、通常、ソースボリューム内の Snapshot コピーだけがデスティネーションに含まれますが、SnapVault デスティネーション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 コピーを保持します。

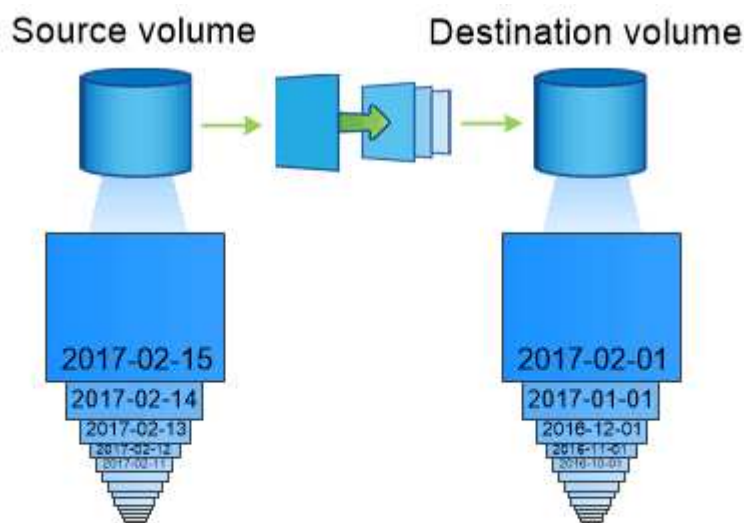
たとえば、ビジネスに関する政府会計規則に準拠するために、20 年にわたってデータの月次 Snapshot コピーを保持しなければならない場合があります。SnapVault ストレージからデータを提供する必要はないため、デスティネーションシステムでは低速かつ低コストのディスクを使用できます。

SnapMirror と同様に、SnapVault を初めて起動すると、ベースライン転送が実行されます。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ィネーションボリュームに転送されます。SnapMirror とは異なり、SnapVault 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 コピーおよび保持するコピーの数が特定されます。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.

ONTAP 9.7以前でのみディスクツーディスクで実行されていたSnapMirrorと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。

多数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の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。

ONTAP 9.8 以降では、SnapMirror クラウドにより、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が可能になりました。SnapMirror クラウドレプリケーションを使用するには、データ保護ワークフローのオーケストレーションおよび管理用に、ライセンスベースのアプリケーションが必要です。ONTAP システムでは、SnapMirror クラウド関係を使用して、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を選択できます。対象となるストレージには、AWS S3、Google Cloud Storage Platform、Microsoft Azure Blob Storage などがあり、これにより、ベンダーバックアップソフトウェアによる効率が向上します。サポートされている認定アプリケーションおよびオブジェクトストレージのベンダーの一覧については、ネットアップ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、オンプレミスのボリュームとパブリッククラウドのCloud Volumes ONTAP インスタンスの間にSnapMirrorまたはSnapVault 関係を設定できます。

BlueXPでは、ソフトウェアサービス（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ています。ユーザは、NetApp Cloud Central のクラウドバックアップを使用して、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 および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、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` 設定は、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。

いずれの場合も、クラスタ間でピア関係を設定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.

MetroCluster以外の実装でのSyncMirrorの使用

必要に応じて、MetroCluster以外の実装でSyncMirror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に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原因の修正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は、ミラーリングされていないアグリゲートの 2 倍のストレージを必要とす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。

ストレージ効率

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、ボリューム内および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。圧縮は手動で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。

従来のデータセット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テクノロジーを使用すると、大規模なデータセットでもほぼ瞬時にコピーできます。

- 温度に敏感なストレージ効率

ONTAPの特長 **"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、メリットが得られます。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。

温度識別型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ボリュームでは自動的に有効になります。

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であるとしします。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。

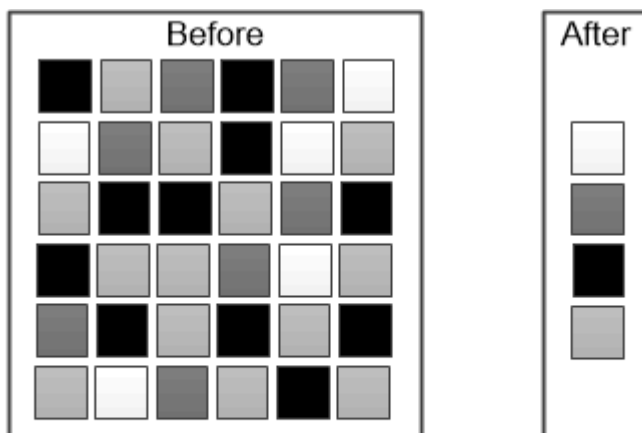
シンプロビジョニングを使用すると、使用しない可能性があるストレージを購入することなく、ストレージを大量に消費するユーザのニーズを満たすことができます。ストレージスペースは実際に消費されるまで割り当てられないため 2TB のアグリゲートを「オーバーコミット」するには、アグリゲートに含まれる 5、000 ボリュームのそれぞれに名目上は 1GB のサイズを割り当てる必要があります。

ライトユーザとヘビーユーザの 10 : 1 という比率に間違いがなければ、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 _ 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あった場合、カタログの作成後にそのブロックが変更されていないかどうかを検証するために 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。

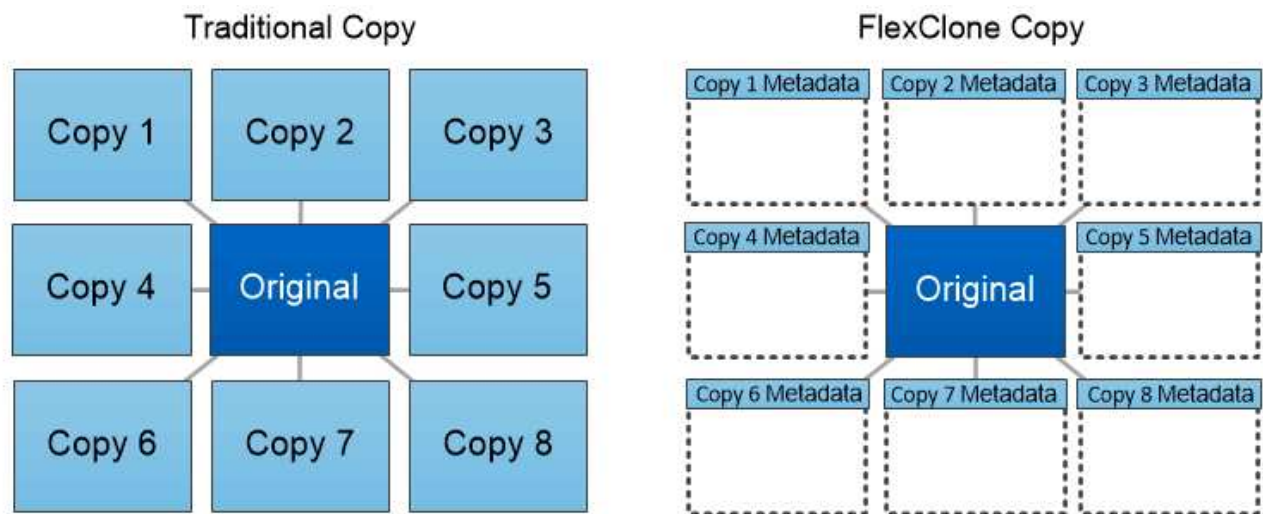
* **_インラインデータコンパクション_** * ゼロで埋められた小さなファイルまたは I/O は、4KB の物理ストレージが必要かどうかに関係なく、4KB ブロックに格納されます。**_インラインデータコンパクション_** では、通常であれば複数の 4KB ブロックを消費するデータチャンクをディスク上の 1 つの 4KB ブロックに結合します。コンパクションはデータがメモリにある間に行われるため、高速のコントローラに適しています。

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。コピーと親でデータブロックが共有されるため、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しかストレージは消費されません。FlexClone ファイルと FlexClone LUN も使用するテクノロジーは同じですが、元の Snapshot コピーは必要ありません。

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、同一の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、ミラーや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 で測定される容量

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。

2 つの測定値の違いについては、次の説明を参照してください。

- 物理容量：物理スペースとは、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のことです。通常、使用済み物理容量の値は、ストレージ効率化機能（重複排除や圧縮など）によるデータの削減が原因で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は、使用済みの物理スペースの量に加えて、設定済みの Storage Efficiency 機能（重複排除や圧縮など）による削減量から導き出されます。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、この測定値は、多くの場合、物理使用容量よりも大きく表示されます。したがって、合計論理容量は、プロビジョニング済みスペースよりも多くなる可能性があります。



System Manager では、ルートストレージ階層（アグリゲート）の容量は表示されません。

使用済み容量の測定値

使用済み容量の測定値の表示方法は、次の表に示すように、使用している System Manager のバージョンによって異なります。

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	使用済みの論理容量	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)

9.7 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

容量測定条件

容量の説明では次の用語を使用します。

- 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よって使用されている容量（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：
 - ONTAP 9.13.1以降では、データ削減比率が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、SnapshotコピーなどのStorage Efficiency機能を使用した場合に達成される大幅な削減量を考慮していない、使用済み論理スペースと物理スペースの割合です。
 - 詳細パネルを表示すると、概要パネルに表示された比率と、物理使用済みスペースと比較したすべての使用済み論理スペースの総比率の両方が表示されます。 Snapshotコピーを使用する*と呼ばれるこの値には、Snapshotコピーやその他のStorage Efficiency機能を使用することによるメリットが含まれています。
 - 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。

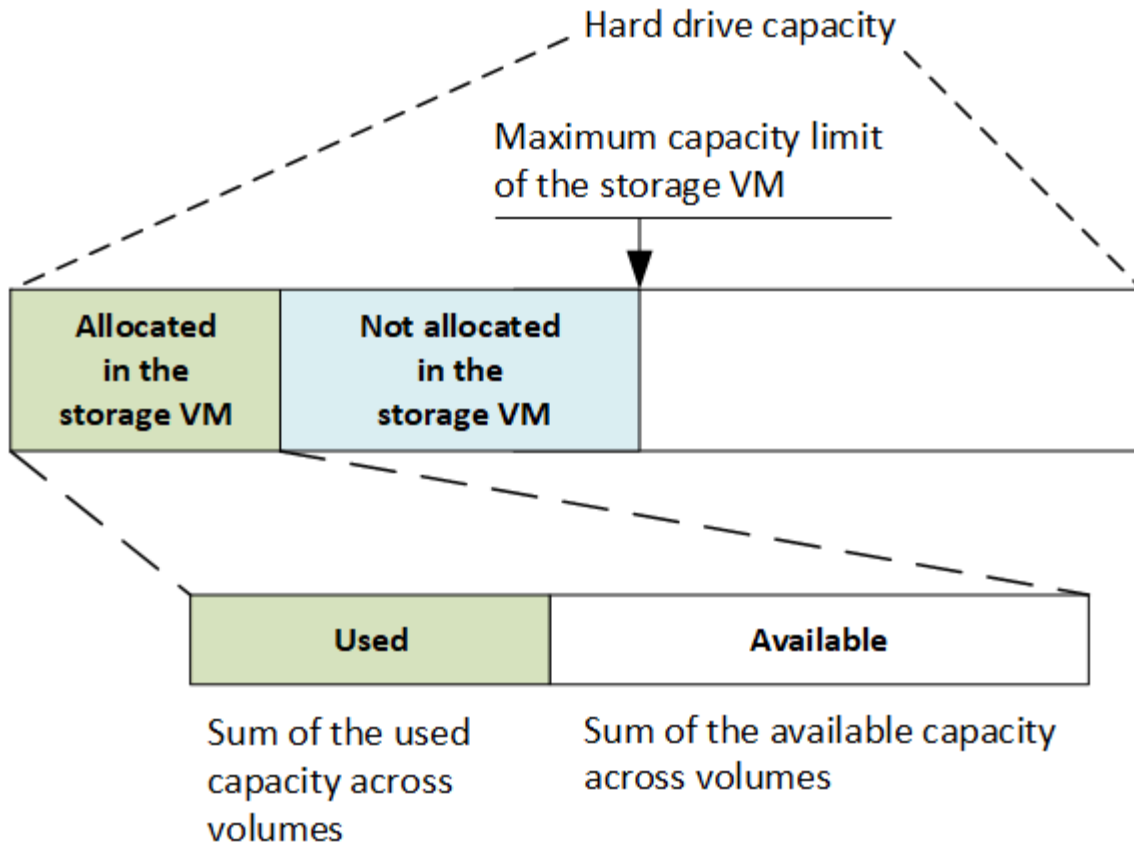
- * Logical Used%*：Snapshotリザーブを除く、プロビジョニングサイズに対する現在の使用済み論理容量の割合。この値は、ボリューム内での効率化による削減も含まれるため、100%より大きい値にすることができます。
- 最大容量：Storage VM上のボリュームに割り当てられる最大スペース。
- 使用済み物理容量：ボリュームまたはローカル階層の物理ブロックで使用されている容量。
- * Physical Used %*：ボリュームの物理ブロックで使用されている容量の、プロビジョニングされたサイズに対する割合。
- プロビジョニングされた容量：Cloud Volumes ONTAP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、の次の手順に関する推奨事項が表示されます ["インサイト"](#)。

容量の単位

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。

- ONTAP 9.10.1以降では、System 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 のスループットに使用される単位は、すべてのリリースの ONTAP について、KB/ 秒、MB/ 秒、GB/ 秒、および PB / 秒です。

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	一、〇二四	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
容量	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"](#)

["ボリュームの論理スペースのレポートと適用"](#)

温度に敏感なストレージ効率の概要

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。

温度識別型 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 ボリュームでは自動的に有効になります。既存の AFF ボリュームとシンプロビジョニングされた AFF DP 以外のボリュームでは、温度に基づく Storage Efficiency を有効にすることができます。

「デフォルト」モードと「効率的」モードが導入されました

ONTAP 9.10.1 以降では、AFF システムに対してのみ、ボリュームレベルの 2 つの Storage Efficiency モード (*default_* と *_efficient*) が導入されました。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。ONTAP 9.10.1 では、["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 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** を有効にします

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、温度に基づくStorage Efficiencyが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、有効にすることはできます ["Storage Efficiencyモードを変更します"](#) 手動で効率モードに変更します。



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します

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 9.13.1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、自動的にシーケンシャルパッキングが有効になります。シーケンシャルパッキングを有効にした後は、を実行する必要があります ["既存のデータを手動で再バックします"](#)。

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時、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、温度に影響されるストレージ効率化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、Storage Efficiency モードは空白のままです。

セキュリティ

クライアントの認証と許可

ONTAP では、標準的な方法を使用して、クライアントや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や WORM ストレージでは、高度なテクノロジーも使用できます。

ONTAP では、信頼できるソースで ID を検証して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対して設定されている権限を比較して、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

プ、および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

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 support Kerberos 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 では、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。

承認

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

指定された NFS エクスポートまたは SMB 共有へのエクスポートおよび共有セキュリティ環境クライアントアクセス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の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環境 SVM ボリュームへの SMB および NFS クライアントアクセスNTFS のアクセス権のみがサポートされています。ONTAP で、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 認証を設定する"**。

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。クライアントがREST APIを使用してONTAPにアクセスする場合、OAuth 2.0のみを使用して認証とアクセス制御を行うことができます。ただし、この機能は、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して設定および有効化できます。

標準のOAuth 2.0機能は、いくつかの一般的な認可サーバーとともにサポートされています。相互TLSに基づいて送信者に制限された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、さまざまな認証オプションを利用できます。を参照してください ["ONTAP OAuth 2.0実装の概要"](#) を参照してください。

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。管理者がアクセスできるコマンドは、ロールベースアクセス制御 (RBAC) に基づいて決まります。

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して、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することができます。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で実行されます。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レポート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。

オンアクセススキャンは NFS ではサポートされていません。

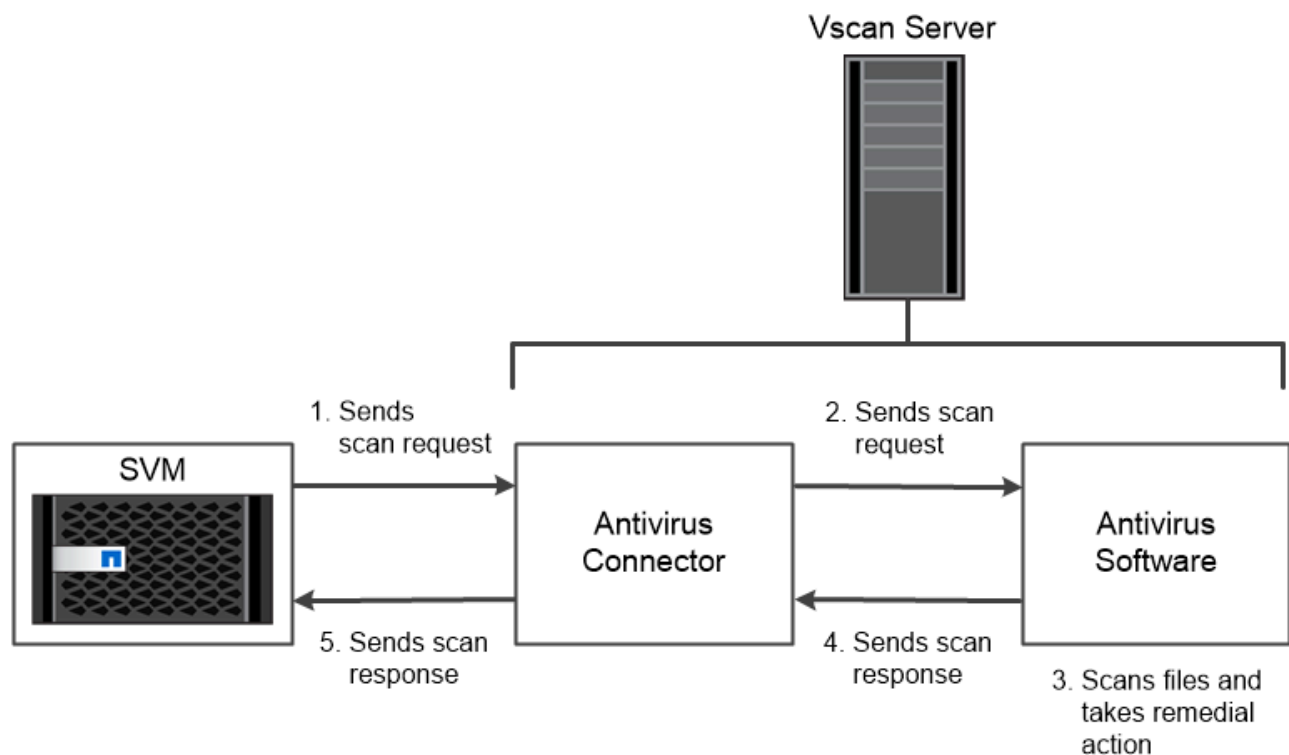
- オンデマンドスキャン _ を使用すると、ファイルのウイルスチェックをただちにまたはスケジュールに基づいて実行できます。たとえば、ピーク時を避けてスキャンを実行する場合などに便利です。外部サーバはチェックしたファイルのスキャンステータスを更新するため、SMB 経由で次回それらのファイルがアクセスされたときには（ファイルが変更されていなければ）ファイルアクセスレイテンシが低減されます。

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。

通常、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 設定でのウイルススキャン _ *

ディザスタリカバリ構成と 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ことが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

ログを提供します。

ONTAP は、すべての SSL 接続に対する連邦情報処理標準（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 Storage Encryption（NSE）

NSE は、Self-Encrypting Drive（SED；自己暗号化ドライブ）を使用するハードウェア解決策です。

- NVMe SED

ONTAP は、FIPS 140-2 認定を取得していない NVMe SED の完全なディスク暗号化を提供します。

- ソフトウェアソリューション：

- NetApp Aggregate Encryption（NAE）

NAE 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解決策です。NAE は、アグリゲートごとに固有のキーを使用して有効にします。

- NetApp Volume Encryption（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解決策です。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）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して、保存データを二重に暗号化できます。NAE または NVE 暗号化はストレージ効率に影響しません。

NetApp Storage Encryption の略

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ません。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は、Flash Cacheモジュール上のデータを暗号化しません。

NVMe 自己暗号化ドライブ

NVMe SED には FIPS 140-2 認定はありませんが、これらのディスクでは 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が保護されます。

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るため、保存データがディスクで保護されます。

NetApp Aggregate Encryption の略

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、ボリュームがアグリゲートレベルの重複排除に含まれているのに対し、NVE ボリュームは除外されることです。

NAE が有効になっている場合は、アグリゲートキーを使用してアグリゲート内のボリュームを暗号化できます。

ONTAP 9.7以降では、新規に作成したアグリゲートとボリュームがデフォルトで暗号化されます。"[NVEライセンス](#)" およびオンボードまたは外部のキー管理

NetApp Volume Encryption の略

NetApp Volume Encryption (NVE) は、一度に 1 ボリュームずつ保管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。

Snapshot コピー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 つずつ、一意の XTS-AES-256 キーを使用します。このキーは、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) と併用して、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。

- 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解決策が必要な場合。
- マルチクラスタ解決策が必要な場合。KMIP サーバでは、複数のクラスタ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

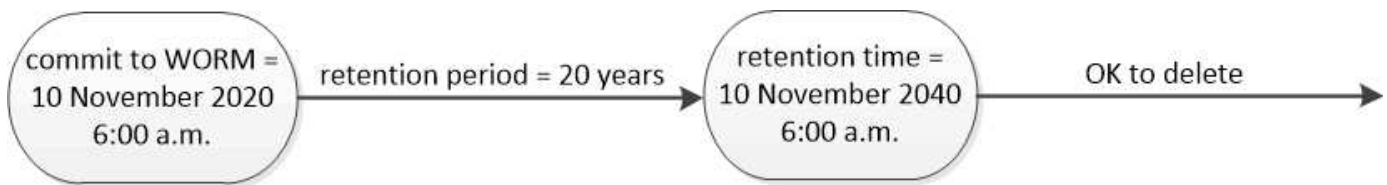
["FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"](#)

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、SEC Rule 17a-4 などの社外規定に準拠するための strict **Compliance** モードと、社内規定に準拠してデジタル資産を保護するためのより緩やかな **Enterprise** モードで SnapLock を使用できます。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.

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では、ONTAP 経由で導入するアプリケーションを、ストレージの観点ではなくアプリケーションの観点で設定できます。アプリケーションは、System Manager と REST API を使用して、最小限の入力で簡単に設定してデータを提供できる状態に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。関連する ONTAP のベストプラクティスを組み込むことで、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を基に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します。

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設定をまとめた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、多くの場合デフォルト値であらかじめ設定されていますが、データベースのサイズ、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、ONTAP システムでストレージをプロビジョニングする際にアプリケーション管理者が指定できる特性を定義します。ONTAP は、LUN やボリュームなどのストレージエンティティを、指定されたパラメータに基づいて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は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します
- アプリケーションに関連付けられているストレージを管理します
- アプリケーションを変更または削除します

- アプリケーションを表示します
- アプリケーションの Snapshot コピーを管理する
- 作成 [整合グループ](#) 同じボリュームまたは異なるボリュームの複数の LUN を選択してデータ保護機能を提供します

FabricPool

ネットアップのお客様の多くは、ほとんどアクセスされない膨大な量の保存データを保有しています。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、ホットデータを最速のストレージに保存するのが理想的です。コールドデータは、必要に応じてすぐに使用可能であれば、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コールドなのかをどのようにして把握していますか？

FabricPool は、アクセスパターンに基づいて高パフォーマンスのローカル階層（アグリゲート）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。階層化によって、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容易に利用できるようにしながら、ホットデータ用の高価なローカルストレージを解放できます。FabricPool では、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、パフォーマンスを最大限に高め、コストを削減します。

FabricPool を使用してコールドデータをクラウドに階層化するのは、クラウドの効率化と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ではありません。多くのお客様が、Cloud Volumes ONTAP in FabricPool を使用して、コールドデータを高コストの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階層化しています。ONTAP 9.8 以降では、を使用して FabricPool 対応ボリュームの分析を取得できます ["File System Analytics の略"](#) または ["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、アプリケーションの変更は必要ありません。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。

主要なクラウドプロバイダのいずれかからオブジェクトストレージにコールドデータを格納できます。また、コールドデータをプライベートクラウドに保存して、最高のパフォーマンスと完全なデータ管理を実現することも StorageGRID できます。

関連情報

["FabricPool システムマネージャドキュメント"](#)

["BlueXPの階層化"](#)

["NetApp TechComm TV で FabricPool 関連ビデオを視聴する"](#)

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。