ONTAP技術レポート

ONTAP Technical Reports

NetApp
August 07, 2026

目次

ONTAP技術レポート

ONTAPおよびアプリケーション/データベースに関するテクニカルレポート

ONTAPは、多くのエンタープライズアプリケーションやデータベーステクノロジのデータ管理とデータ保護の基盤です。次のテクニカルレポートでは、Microsoft SQL Server、MySQL、Oracle、PostgreSQL、SAP HANA、Epicに対するNetAppの推奨プラクティスと実装手順に関するガイダンスを提供します。

Microsoft SQL Server の場合

SQL ServerはMicrosoftのデータプラットフォームの基盤であり、オンプレミスでもクラウドでも、インメモリテクノロジを使用してミッションクリティカルなパフォーマンスを実現し、あらゆるデータの分析を高速化します。

"ONTAPを使用したMicrosoft SQL Serverのベストプラクティス"ストレージ管理者およびデータベース管理者がMicrosoft SQL ServerをONTAPストレージに正常に導入する方法について説明します。

> このドキュメントは、以前に公開されたテクニカルレポート（TR-4590：『Best Practice Guide for Microsoft SQL Server with ONTAP』）に代わるものです。_

"TR-4976：『Virtualized Microsoft SQL Server performance on NetApp AFF A-Series and C-Series systems』"
NetApp AFF AシリーズおよびCシリーズシステムを使用したMicrosoft SQL Serverのパフォーマンス特性と、ワークロードに基づいて適切なシステムを選択する方法について説明します。

"TR-4714：『Best Practices for Microsoft SQL Server using SnapCenter』"
SnapCenterテクノロジを使用してONTAPストレージにMicrosoft SQL Serverを適切に導入し、データを保護する方法をご紹介します。

MySQL

このドキュメントでは、ONTAPにMySQLを導入するための構成要件と、調整とストレージ構成に関するガイダンスを提供します。

"NetApp ONTAP上のMySQLデータベースのベストプラクティス"MySQLとその派生であるMariaDBやPerconaなどは、多くのエンタープライズアプリケーションで広く使用されています。これらのアプリケーションは、グローバルなソーシャルネットワーキングサイトや大規模なeコマースシステムから、数千ものデータベースインスタンスを含むSMBホスティングシステムまで多岐にわたります。ONTAPにMySQLを導入するための調整とストレージ構成に関する要件とガイダンスについて説明します。

> 本ドキュメントは、以前に公開されたテクニカルレポート（TR-4722）『MySQL database on NetApp ONTAP best practices』に代わるものです。_

Oracle の場合

ONTAPはOracleデータベース向けに設計されています。ONTAPは数十年にわたり、リレーショナルデータベースI/O固有の要求に合わせて最適化されてきました。また、Oracleデータベースのニーズに対応するため

に、さらにはOracle Inc自体の要求にも対応するために、複数のONTAP機能が開発されました。

"ONTAP上のOracleデータベース"ストレージ管理者およびデータベース管理者がONTAPストレージにOracleを正常に導入するための推奨事項について説明します。

"ONTAPによるOracleデータ保護"ストレージ管理者およびデータベース管理者は、ONTAPストレージ上のOracleに対して、バックアップ、リカバリ、複製、ディザスタリカバリを正常に実行できるようにするための推奨されるプラクティスについて説明します。

"ONTAPによるOracle向けディザスタリカバリ"MetroClusterおよびSnapMirrorビジネス継続性を使用してOracleデータベースを運用する場合の推奨事項、テスト手順、およびその他の考慮事項について説明します。

"ONTAPストレージシステムへのOracleデータベースの移行"移行戦略を計画する際の全体的な考慮事項、データ移動を行う3つの異なるレベル、使用可能なさまざまな手順の詳細について説明します。

以前に公開されていたテクニカルレポート（TR-3633：『Oracle databases on ONTAP』、TR-4591：『Oracle data protection：backup、recovery、replication』、TR-4592：『Oracle on MetroCluster』、TR-4534：『Migration of Oracle databases to NetApp storage systems_

"TR-4969：『Oracle database performance on AFF A-Series and C-Series』"
ONTAPは、インライン圧縮、ハードウェアの無停止アップグレード、外部ストレージアレイからのLUNインポートなどの機能を標準搭載した強力なデータ管理プラットフォームです。最大24ノードのクラスタ構成が可能で、Network File System（NFS）、Server Message Block（SMB；サーバメッセージブロック）、iSCSI、Fibre Channel（FC；ファイバチャネル）、Nonvolatile Memory Express（NVMe）の各プロトコルを通じてデータを同時に提供できます。さらに、Snapshotテクノロジは、数万個のオンラインバックアップと完全に運用可能なデータベースクローンを作成するための基盤となります。ONTAPの豊富な機能セットに加えて、データベースのサイズ、パフォーマンス要件、データ保護のニーズなど、ユーザにはさまざまな要件があります。AFFストレージシステム（AシリーズとCシリーズの両方を含む）を使用したベアメタルデータベースのパフォーマンスについて説明し、2つのAFFオプションの最大値と実際の違いについて説明します。

"TR-4971：『Virtualized Oracle database performance on AFF A-Series and C-Series』"
ONTAPは、インライン圧縮、ハードウェアの無停止アップグレード、外部ストレージアレイからのLUNインポートなどの機能を標準搭載した強力なデータ管理プラットフォームです。最大24ノードのクラスタ構成が可能で、Network File System（NFS）、Server Message Block（SMB；サーバメッセージブロック）、iSCSI、Fibre Channel（FC；ファイバチャネル）、Nonvolatile Memory Express（NVMe）の各プロトコルを通じてデータを同時に提供できます。さらに、Snapshotテクノロジは、数万個のオンラインバックアップと完全に運用可能なデータベースクローンを作成するための基盤となります。ONTAPの豊富な機能セットに加えて、データベースのサイズ、パフォーマンス要件、データ保護のニーズなど、ユーザにはさまざまな要件があります。AFFストレージシステム（AシリーズとCシリーズの両方を含む）を使用した仮想データベースのパフォーマンスについて説明し、最大値と2つのAFFオプションの実際の違いについて説明します。

"TR-4695：『Database storage tiering with FabricPool』"
Oracle Relational Database Management System（RDBMS）など、さまざまなデータベースを使用するFabricPoolのメリットと構成オプションについて説明します。

"TR-4899：『Oracle database transparent application failover with SnapMirror active sync』" SnapMirror Active Sync（旧SM-BC）とOracle Real Application Cluster（RAC）は、サイト障害や実際の災害が発生した場合に透過的なアプリケーションフェイルオーバー（TAF）と継続性を提供します。SnapMirror Active SyncをOracle RACのストレージコンポーネントとして使用するAFFストレージアレイの構成ガイダンスと推奨事項について説明します。

"TR-4876：『Oracle multitenancy with ONTAP 解決策and deployment best practices』"

ONTAPストレージを使用してOracleマルチテナントデータベースをプロビジョニング、管理、保護し、Oracleマルチテナントデータベースと ONTAPソフトウェアの機能の両方のメリットを最大限に活用する方法について、解決策が推奨するプラクティスを紹介します。

PostgreSQL

PostgreSQLには、PostgreSQL、PostgreSQL Plus、EDB Postgres Advanced Server（EPAS）などのバリアントが付属しています。PostgreSQLは通常、多層アプリケーションのバックエンドデータベースとして導入されます。NetApp ONTAPは、信頼性、パフォーマンス、効率に優れたデータ管理機能を備えたPostgreSQLデータベースを実行するための優れた選択肢です。

"ONTAP上のPostgreSQLデータベースのベストプラクティス"PostgreSQLには、PostgreSQL、PostgreSQL Plus、EDB Postgres Advanced Server（EPAS）などのバリアントが付属しています。PostgreSQLは通常、多層アプリケーションのバックエンドデータベースとして導入されます。一般的なミドルウェアパッケージ(PHP、Java、Python、Tcl/Tk、ODBCなど)でサポートされています。 とJDBC）は、オープンソースのデータベース管理システムでは、歴史的に人気のある選択肢でした。ONTAPにPostgreSQLを導入するためのチューニングとストレージ構成に関する設定要件とガイダンスについて説明します。

このドキュメントは、以前に公開されたテクニカルレポート_TR-4770：『PostgreSQL database on ONTAP best practices_』に代わるものです。

SAP HANA のサポート

"ONTAP上のSAP HANAデータベースソリューション"SAPソリューションの構成、管理、自動化に関するベストプラクティスについては、NetAppのSAPソリューションページを参照してください。

エピック

"Epic on ONTAPのベストプラクティス"ONTAPに適切に導入するための設定基準を満たしながら、オンプレミスとクラウドにEpicを導入するためのベストプラクティスを理解するためのガイドです。

本ドキュメントは、以前に公開されたテクニカルレポート（TR-3923）『NetApp best practices for Epic_』に代わるものです。

ビジネス継続性に関するテクニカルレポート

NetAppは、アプリケーションやデータが配置されている場所を合理化して、パフォーマンスをコスト効率よく向上する幅広いソリューションを提供しています。データ保護、レプリケーション、継続的可用性：ONTAPデータ管理は、一度設定するだけで運用できるポリシー管理でシンプルなデータ保護を実現し、MetroClusterとSnapMirrorのアクティブな同期機能でビジネスの継続性を維持します。

これらのテクニカルレポートでは、およびの製品ドキュメントについて詳しく説明し "ONTAP SnapMirrorアクティブ同期" "ONTAP MetroCluster" ます。

SnapMirrorアクティブ同期（旧称SM-BC）

"TR-4878：『SnapMirror active sync』" SnapMirrorアクティブ同期は、アプリケーションレベルのきめ細かさを備えた継続的可用性を備えたストレージソリューションです。AFFまたはオールSANアレイ（ASA）ストレージシステムで実行されるONTAPで使用できるため、最も重要なビジネスアプリケーションのRPO 0とRTO 0のニーズを満たすことができます。

MetroCluster

"TR-4705：『NetApp MetroCluster 解決策architecture and design』"
このドキュメントでは、ONTAPのMetroCluster機能のアーキテクチャの概要と設計の概念について説明します。

MetroCluster IP

"TR-4689：『NetApp MetroCluster IP』" MetroClusterは、FASおよびAFFシステム上で動作するONTAP向けの継続的に利用可能なストレージソリューションです。MetroCluster IPは、イーサネットベースのバックエンド ストレージ ファブリックを使用する最新の進化形です。MetroCluster IPは、最も重要なビジネスアプリケーションのニーズを満たすために、高度な冗長構成を提供します。MetroCluster IPはONTAPに含まれており、ONTAPストレージを使用するクライアントおよびサーバーにNASおよびSAN接続を提供します。

MetroCluster FC

"TR-4375：『NetApp MetroCluster FC』"MetroClusterは、ミッションクリティカルなアプリケーション向けに、地理的に離れたデータセンター間で継続的なデータ可用性を実現します。MetroCluster FCの推奨プラクティス、設計上の決定事項、サポートされる構成について説明します。

ONTAPのデータ保護とディザスタリカバリに関するテクニカルレポート

SnapMirrorは、データファブリック全体にわたる、対費用効果に優れた使いやすいユニファイドレプリケーション解決策です。LAN または WAN 経由でデータを高速で複製します。仮想環境と従来の環境の両方で、Microsoft Exchange、Microsoft SQL Server 、Oracleなどのビジネスクリティカルなアプリケーションのデータ可用性を高め、高速なデータレプリケーションを実現できます。1つ以上のONTAPストレージシステムにデータをレプリケートし、セカンダリデータを継続的に更新することで、データを最新の状態に保ち、必要なときにいつでも利用できます。外部レプリケーションサーバは必要ありません。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"ONTAPデータ保護とディザスタリカバリ"ています。

SnapMirror

SnapMirror非同期

"TR-4015：『SnapMirror Asynchronous configuration and best practices』"ボリューム、整合グループ、およびStorage Virtual Machine（SVMディザスタリカバリ）のSnapMirror非同期（SM-A）レプリケーションを設定するための推奨されるプラクティスについて説明します。

"TR-4678：『Data protection and backup ONTAP FlexGroup volumes』"
FlexGroupボリュームに推奨されるデータ保護とバックアップについて説明します。トピックには、Snapshotコピー、SnapMirror、その他のデータ保護ソリューションとバックアップソリューションが含まれます。

SnapMirror Synchronous

"TR-4733：『SnapMirror Synchronous configuration and best practices』"SnapMirror Synchronous（SM-S）レプリケーションを設定するための推奨事項について説明します。

SnapMirrorによるデータセンターの3つのDR

"TR-4832：『Three Data Center disaster recovery using NetApp SnapMirror for ONTAP 9.7』"レプリケーションにONTAP SnapMirrorテクノロジを使用した、データセンター3つのディザスタリカバリ構成について説明します。

SnapMirrorを使用したアプリケーションとインフラ

"TR-4900：『VMware Site Recovery Manager with ONTAP』" ONTAPは、2002年に最新のデータセンターに導入されて以来、業界をリードするVMware vSphere環境向けのストレージソリューションであり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。ONTAP 解決策for VMware Site Recovery Manager（SRM）は、業界をリードするVMwareのディザスタリカバリ（DR）ソフトウェアです。最新の製品情報や推奨されるプラクティスなど、導入の合理化、リスクの軽減、継続的な管理の簡素化を実現します。

ONTAPサイバーボールト

"ONTAPサイバーボールト"NetAppのONTAPベースのサイバーボールトは、最も重要なデータ資産を保護するための包括的で柔軟なソリューションを組織に提供します。ONTAPでは、論理的なエアギャップと堅牢な強化手法を活用することで、進化するサイバー脅威に対して耐障害性に優れた、セキュアで分離されたストレージ環境を構築できます。ONTAPを使用すると、ストレージインフラの即応性と効率性を維持しながら、データの機密性、整合性、可用性を確保できます。

ONTAP FlexCacheおよびFlexGroup Volumeに関するテクニカルレポート

NetApp NASソリューションは、データ管理を簡易化し、コストを最適化しながら成長に対応できるようにします。ONTAP NASソリューションは、ユニファイドアーキテクチャにより、ノンストップオペレーション、実証済みの効率性、シームレスな拡張性を実現します。ONTAPを基盤とするスケールアウトNASは、大規模なONTAPエコシステムを活用し、イノベーションをリードする重要なビジョンと、今後の積極的なイノベーションを実現します。

これらのテクニカルレポートでは、およびの製品ドキュメントについて詳しく説明し "ONTAP FlexCacheボリューム" "ONTAP FlexGroupボリューム" ます。

FlexCache

"TR-4743 ：『 FlexCache in ONTAP 』"
FlexCacheは、同一または異なるONTAPクラスタ上にボリュームの書き込み可能なスパースレプリカを作成するキャッシュテクノロジです。データやファイルをユーザの近くに配置できるため、設置面積を抑えながらスループットを高速化できます。FlexCacheの使用方法、設計と実装に関する推奨事項、制限事項、考慮事項について説明します。

FlexCacheライトバック

"FlexCacheライトバック" ONTAP 9.15.1で導入されたFlexCacheライトバックは、キャッシュへの書き込み処理の代替モードです。ライトバックを使用すると、書き込みがキャッシュの安定したストレージにコミットされ、データが元のストレージに到達するのを待たずにクライアントに確認応答が返されます。データは非同期的に元のデータにフラッシュされます。その結果、グローバルに分散されたファイルシステムが実現し、特定のワークロードや環境に対してローカルに近い速度で書き込みを実行できるようになり、パフォーマンスが大幅に向上します。

FlexGroup ボリューム

"TR-4571：『NetApp ONTAP FlexGroup volumes best practices and Implementation guide』"
FlexGroupボリューム、推奨されるプラクティス、実装のヒントを紹介します。FlexGroupボリュームは、ONTAPスケールアウトNASコンテナの進化形であり、メタデータ負荷の高いワークロードにおいて、ほぼ無限の容量と予測可能な低レイテンシのパフォーマンスを兼ね備えています。

"TR-4678：『Data protection and backup of FlexGroup volumes』"
Snapshotコピー、SnapMirror、その他のデータ保護およびバックアップのソリューションなど、FlexGroupボリュームのデータ保護とバックアップについて説明します。

ONTAPネットワークテクニカルレポート

ONTAPは、非常に要件の厳しいスケールアウトアプリケーションに対応するために、さまざまなネットワーク機能と構成を提供します。ネットワーク機能と機能を使用することで、企業はデータへの信頼性の高い安全なアクセスを作成できます。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載されている"ONTAPネットワーク管理"ています。

ルーティング

"TR-4949：『BGP / VIP with ONTAP in the data center』"
ONTAPに基本的なBGP設定を迅速に導入する方法について説明します。

ネームサービス

"TR-4523：『DNS load balancing in ONTAP』"
ONTAPのDNSを含むDNSロードバランシング方式で使用するためのONTAPの設定方法、さまざまな設定方法、および推奨される方法について説明します。

"TR-4668：『Name services best practices guide』"
CIFS / SMBやNFSなどのネットワーク接続型ストレージ（NAS）ソリューションをONTAPに実装する際の推奨されるプラクティス、制限事項、考慮事項について説明します。

"TR-4835：『How to configure LDAP in ONTAP multiprotocol NAS identity management』"
マルチプロトコルNAS用にONTAPでLightweight Directory Access Protocol（LDAP）ID管理を設定する方法について説明します。

NFS

ONTAP NFS テクニカルレポート

NetApp NFSソリューションはデータ管理を簡素化し、コストを最適化しながら成長ペースに対応できるよう支援します。

NFS

"TR-4067：『NFS in ONTAP best practice and implementation guide』"
ONTAPでのNFSの基本概念、サポート情報、設定のヒント、および推奨される方法について説明します。

"TR-4962：『NFSv4.2 extended attributes』"
ONTAP 9.12.1以降でのNFSv4.2拡張属性の有効化と使用について説明します。

マルチプロトコル

"TR-4887：『Multiprotocol NAS in ONTAP Overview and Best Practices』"
ONTAPでのマルチプロトコルNASアクセスの仕組みと、マルチプロトコル環境の推奨事項について説明します。

NFS over TLS

NFS over TLSの概要

ONTAP 9.19.1では、NFSトラフィックを暗号化するための待望の「簡単ボタン」であるNFS over TLSが導入されました。

この機能以前は、飛行中のNFSペイロードの暗号化はIPsecまたはKerberosに限定されていました。どちらも効果的ではあるものの、設定が煩雑で、パフォーマンスの低下も著しいという欠点がありました。どちらの方法も「後付け」のソリューションであり、NFS専用のRFCで具体的に定義されたソリューションではありませんでした。"RFC 9289"、「Toward Remote Procedure Call Encryption by Default」と題されたこの文書がそれを変えました。NFSv3およびNFSv4.xでは、TLS 1.3を使用してNFS RPCトラフィックを転送中に暗号化できるようになりました。Kerberosは不要です。IPsecは不要です。

前提条件

ONTAP NFS over TLS を使用するには、以下の要件を満たす必要があります。

- …ONTAP 9.19.1が実行されている必要があります
  - ONTAPクラウドパーソナリティは現時点ではサポートされていません
- …NFSライセンスを取得しています
- …NFSクライアントが"NetApp Interoperability Matrix"に見つかりました

できないこと

NFS over TLSはトランスポート層を保護するものであり、NFSによるユーザ認証の方法を変更するものでは

ありません。

証明書ベースのユーザ認証**TLS** 上の **NFS** は、*新しいユーザ認証機構を提供しません。ユーザ認証には、引き続き `auth_sys`または `krb5`が必要です。引き続き `krb5i`および `krb5p`を使用できますが、TLS によってそれらの整合性とプライバシー保護が冗長になり、パフォーマンスの低下は避けられません。

ユースケースとワークロード

TLS 上の NFS は、Kerberos インフラストラクチャなしでの回線暗号化、共有エクスポートでのクライアントごとの TLS 強制、相互クライアント認証という 3 つの一般的な展開シナリオに適しています。

すべてのワークロードが同じように恩恵を受けるわけではありません。どのパターンが適していて、どのパターンが適していないかを把握することで、導入計画を立てやすくなります。

ユースケース

*Kerberosインフラストラクチャなしで、ネットワーク上でNFS暗号化を実現します。*NFSのデータ転送時の暗号化が必要だが、キー配布センター（KDC）の導入と運用、クライアントへのキータブの配布、NASクライアントをカバーするためのKerberosレルムの拡張はしたくない場合、NFS over TLSがこれを直接解決します。ストレージ仮想マシン（SVM）ごとにサーバー証明書をインストールし、暗号化されたNFSを伝送する各データ論理インターフェース（LIF）でNFS over TLSを有効にし、クライアントは標準NFSポート上でTLS 1.3をインバンドでネゴシエートします。新たな認証サービスは不要です。

*共有NFSエクスポートにおけるクライアントごとのTLSのみの強制適用。*暗号化が必要なクライアントと暗号化を必要としないクライアントが混在している場合、他のクライアントに影響を与えずに、規制対象のクライアントを強制的に暗号化されたパスに誘導する方法が必要です。エクスポートポリシールールオプション `-allow-nfs-tls-only true`は、まさにその目的を果たします。これは、TCP経由で一致するクライアントからの非TLSマウントを拒否する一方で、他のエクスポートポリシールールには影響を与えません。

*ストレージとクライアント間の信頼関係構築のための相互クライアント認証（mTLS）。*ゼロトラストネットワークの原則に基づいて運用している場合、またはストレージコントローラが接続するすべてのクライアントのホストIDを検証することを義務付けるセキュリティ強化要件がある場合は、LIFごとの相互TLSオプションを使用してください。 `-enforce-host-auth true`に設定します。 `vserver nfs tls interface enable`または `vserver nfs tls interface modify`。ONTAPは、TLSハンドシェイク時に、接続してくる各クライアントのX.509証明書をSVMにインストールされている認証局（CA）の信頼チェーンに対して検証し、信頼できる証明書を提示しないクライアントを拒否します。これにより、「登録済みのホスト群のみがこのNFS LIFにアクセスできる」という暗号化による強制が可能になり、既存のエクスポートポリシーホストフィルタに加えて機能します。

ワークロード

暗号化は無料ではありません。TLSハンドシェイクには測定可能なコストがかかり、TLSレコードの暗号化はすべてのRPCにオーバーヘッドを追加します。パフォーマンスへの影響は、ワークロード、プラットフォーム、およびハードウェアオフロードが利用可能かどうかによって大きく異なります。詳細については、"Performance"を参照してください。

ワークロードパターン

安定したクライアント数を持つ、長期間稼働するNFSマウントは最適です。TLSハンドシェイクは、マウント時とセッション再確立時に発生する接続ごとのコストです。一度マウントすると数時間または数日間マウント状態を維持する、小規模で安定したクライアント群であれば、そのコストを問題なく吸収できます。

例えば、DNSレコードを自分で管理するなどして、LIFとホスト名のマッピングを既に適切に管理している場合、TLS経由のNFSのプロビジョニングは容易です。この機能はLIFごとに設定されます。LIFの完全修飾ドメイン名（FQDN）と一致するコモンネーム（CN）を持ち、サブジェクト代替名（SAN）リストにLIFのIPアドレスを含むサーバー証明書をインストールします。

NFS over TLS は、ネットワーク上の機密性、サーバーの身元確認、そして必要に応じてクライアントホストの身元確認がセキュリティ要件となる場合に最適なツールです。これらはまさに TLS が提供する特性です。

ワークロードのアンチパターン

接続チャーンが高い場合や大規模なマウントストームが発生する場合は、適していません。新しい TLS 接続ごとに、非対称暗号化、証明書の検証、およびオプションの mTLS チェーン検証を含む TLS 1.3 ハンドシェイクコストが発生します。多数のクライアントがマウントし、少量の作業を行い、アンマウントして繰り返し再接続すると、ハンドシェイクのコストを償却するのではなく、何度も支払うことになります。

アーキテクチャ

NFS over TLS は、ONTAP NFSサーバのLIFごとのトランスポートセキュリティ機能です。クライアントとONTAP NFSサーバ間のNFSトラフィックにTLS保護を適用します。設定は `vserver nfs tls interface`コマンドファミリーと対応する `/api/protocols/nfs/tls/interfaces`RESTリソースを通じて管理されます。

設定はSVMスコープで、LIFごとに適用され、クラスタ全体にレプリケートされます。現在LIFをホストしているすべてのノードに、同じTLS設定が適用されます。クラスタ全体のオン/オフスイッチはありません。有効化と無効化は、LIFごとの操作です。

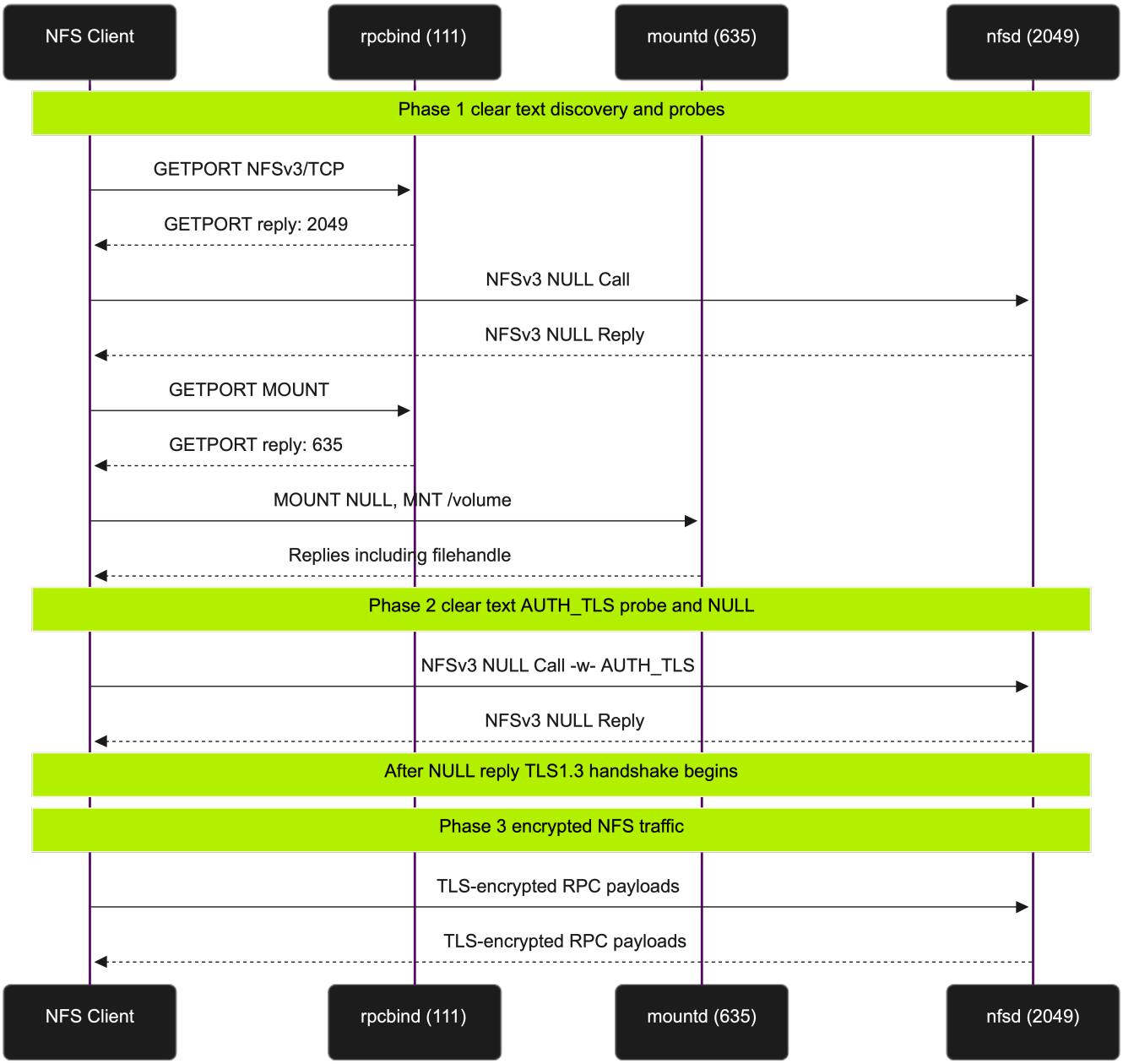
外部依存関係

9.19.1では、NFS TLSハンドシェイクパスから外部認証局（CA）またはOCSPレスポンダーへの発信呼び出しは行われません。証明書チェーンとサブジェクト代替名（SAN）の検証は、SVMにインストールされている証明書マテリアルに対してローカルで実行されます。

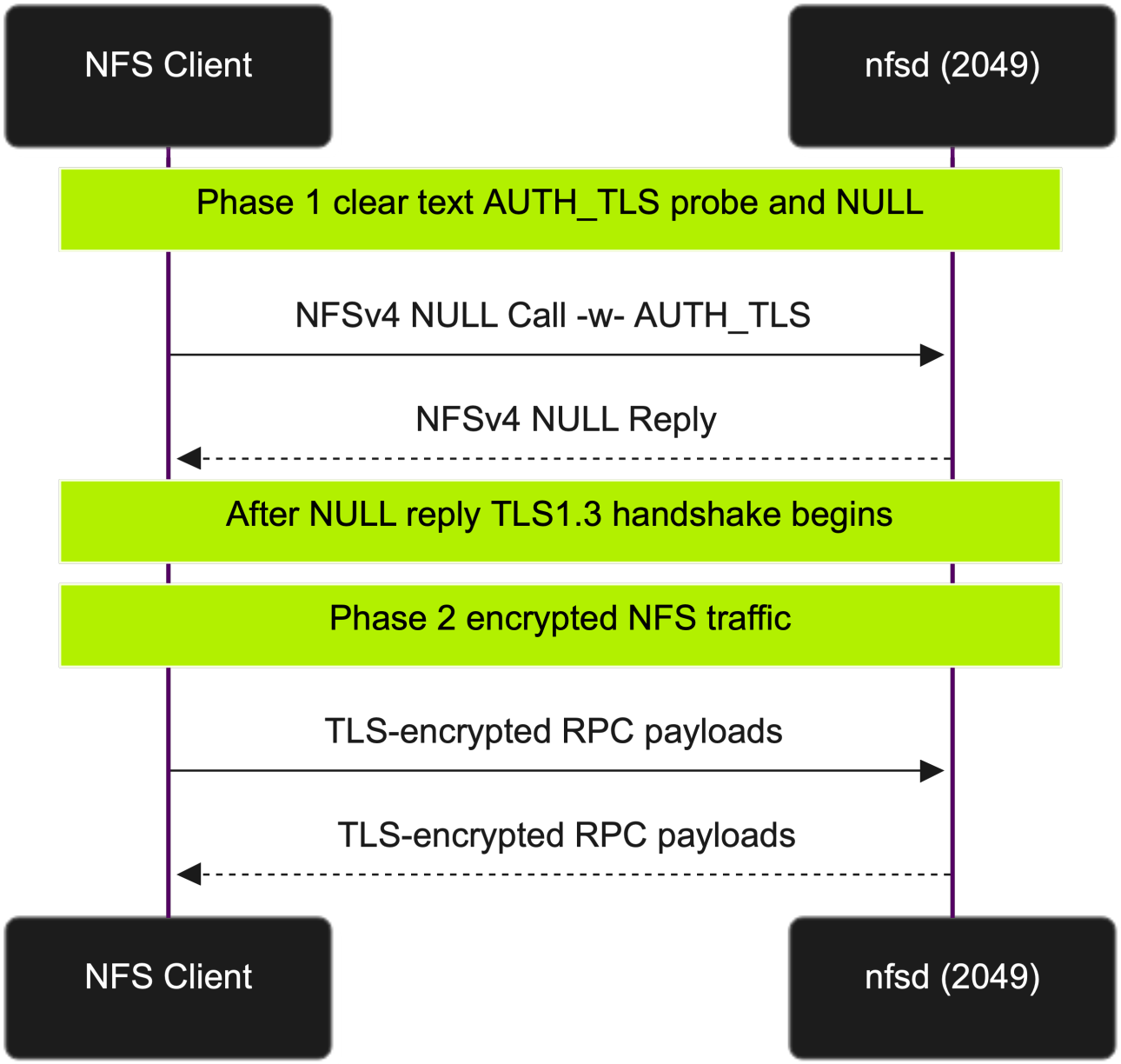
データフロー

NFSv3とNFSv4はどちらも、TCPポート2049への最初のNULL呼び出し/応答ペアの後に、NFSペイロード全体を暗号化します。NULL呼び出しには、RFC 9289で定義された新しい `AUTH_TLS`クレデンシャルフレーバーが含まれており、クライアントがTLSを使用する意図を示します。サーバーは、TLSアップグレードを受け入れるか拒否するかを示すNULL応答を返します。クライアントが承認を受け取ると、同じTCP接続上でTLS 1.3ハンドシェイクに進みます。ハンドシェイクが正常に完了すると、以降のすべてのNFS RPCはTLSレコードにカプセル化され、転送中に暗号化されます。

NFSv3とNFSv4.xには1つの違いがあります。NFSv3は補助プロトコルに依存しています。-`rpcbind`（ポートマッパー）、 `mountd`、NLM（Network Lock Manager）、およびNSM（Network Status Monitor）——これらはTLSで保護された接続を介して伝送されず、平文で送信されます。ストレージトラフィックの完全な暗号化を義務付けるコンプライアンス要件を持つ組織は、NFSv3とNFSv4.xのどちらを選択するかを決定する際に、この点を考慮する必要があります。NFSv4.xはこれらのサイドチャネルプロトコルを排除します。NFSv4.xのすべてのトラフィックはポート2049に集約され、TLSハンドシェイク後に暗号化されます。



NFSv4.xは補助プロトコルを使用しないため、すべてのNFSv4.x RPCはTLSハンドシェイク後に暗号化されます。



ONTAPは、現在LIFをホストしているノード上のNFSサーバでTLSを終端します。トランスポート層より上では、NFSサーバはRPCをTLSを使用しないNFS接続と同様に処理します。

HAテイクオーバーの動作

既存のNFS over TLSセッションは、HAテイクオーバーや予期しないノードパニックが発生しても維持されません。TLSはTCPを基盤としたセッションレベルのトランスポートプロトコルです。ノードとのTCP接続が切断されると、TLSセッションも同時に切断されます。

引き継ぎ後、クライアントは再接続し、TLS 1.3 ハンドシェイクを新たに完了します。パートナーノードは、構成レコードがクラスタ全体に複製されているため、証明書バインディング、ホスト認証設定、SAN検証設定など、同じ複製された TLS 構成を使用します。

TLSセッションチケットと事前共有鍵（PSK）はノードローカルであり、パートナーには転送されません。引

き継ぎ時には、TLSハンドシェイク全体を伴う再接続の嵐が発生することが予想されます。

MetroClusterおよびSVM-DRの動作

TLS インターフェイス証明書と構成は、標準の SVM-DR および MetroCluster SVM レベルのレプリケーション パスを介して SVM とレプリケートされます。ID 保持スイッチオーバー後、デスティネーション SVM は LIF ごとの同じ TLS 構成を保持します。

エクスポートポリシールールの `-allow-nfs-tls-only`フィールドは、標準のエクスポートポリシーレプリケーションパスを通じて、エクスポートポリシールールの残りの部分とともにレプリケートされます。SVM-DRでは、ポリシーがSVMでレプリケートされる際に、ルールもポリシーとともに引き継がれます。

NFS over TLSの設定

NFS over TLS は、 `vserver nfs tls interface`コマンドファミリー、 `/api/protocols/nfs/tls/interfaces` REST エンドポイント、またはSystem ManagerのNFS設定を使用して、LIF ごとに構成されます。

エクスポート ルールに、一致するクライアントに対してTLSのみのアクセスを強制できる補助フィールドが追加されました。コマンドリファレンスについては、"docs.netapp.com"を参照してください。組み込みのSwaggerドキュメントを使用してREST APIをインタラクティブに操作できます。ブラウザで次のアドレスにアクセスしてください： `https://<cluster-mgmt-ip>/api/docs`

ONTAPの前提条件

以下の手順は、次の前提条件が満たされていることを前提としています。

- Data ONTAP 9.19.1以降
- NFSプロトコルが有効になっているSVM
- 少なくとも1つのデータLIFが基本的なNFSアクセス用に構成されている

ステップ1：ONTAP でルートCAを作成する

> *外部認証局オプション*組織が外部の認証局を使用している場合は、この手順をスキップしてください。ステップ2とステップ5のCSRを外部CAに送信し、結果として得られた署名済み証明書をONTAPにインストールしてください。残りの手順は同じです。

ONTAPは、ラボ環境や社内環境への展開において、内部認証局（CA）として機能することができます。この手順では、SVM上に自己署名ルートCAを作成します。このルートCAは、サーバー証明書（およびオプションで相互TLS用のクライアント証明書）に署名するために使用されます。

```
ontap9::> security certificate create -vserver <svm> -common-name <ca-
name> -type root-ca -size 2048 -hash-function SHA256 -expire-days 3652
-country US -state <state> -locality <city> -organization <org> -unit
<unit>
```

コマンドが完了したら、CAシリアル番号を取得して記録してください。これはステップ2で必要であり、相互TLSを使用する場合はステップ5でも必要です。

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields serial
```

シリアル番号を記録します。これは後の手順で `<ca-serial>`になります。

ステップ**2**：データ**LIF**用のサーバ証明書を生成する

ONTAPは、TLSハンドシェイク中に、この証明書をNFSクライアントに提示します。証明書の共通名（CN）とサブジェクト代替名（SAN）は、LIFのFQDNとIPアドレスと一致している必要があります。これは、クライアント上のtlshdが、サーバのIDを両方に対して検証するためです。

> *IP SAN要件。*TLS上のNFSでNFSv4.1セッショントランキングを構成する予定がある場合、またはマウントコマンドがホスト名の代わりに生のIPアドレスを使用する場合、証明書にはクライアントが接続するすべてのLIF IPアドレスのIP SANエントリが含まれている必要があります。これがないと、IPアドレスで指定されたパスの場合、TLSハンドシェイクが「Certificate owner unexpected」というエラーで失敗します。

ONTAP CSR ジェネレーター（security certificate generate-csr）は、 `-ipaddr`を介して IP SAN を直接サポートします。これは、カンマ区切りの IP アドレスのリストを受け付けます。

2a.CSRと秘密鍵を生成します

NFS over TLS トラフィックを伝送するすべての LIF IP をカンマ区切りでリストした `-ipaddr`を含めます。マウントコマンドで使用するホスト名に対応した `-dns-name`を含めます。

```
ontap9::> security certificate generate-csr -common-name <lif-fqdn>
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name <lif-fqdn> -ipaddr <lif-ip>[,<lif-ip-2>,...] -country
US -state <state> -locality <city> -organization <org> -unit <unit>
```

例えば、単一のLIFの場合：

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130 -country US
-state CA -locality SanJose -organization "MyOrg" -unit "Storage"
```

2つのLIF IPにまたがるセッション トランキングの場合は、両方をカンマ区切りのリストで指定してください：

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130,192.0.2.131
-country US -state CA -locality SanJose -organization "MyOrg" -unit
"Storage"
```

このコマンドは、証明書署名要求（CSR）のPEMブロックと秘密鍵のPEMブロックを出力します。両方をコピーして保存してください。秘密鍵は一度しか表示されません。

署名前にCSRに期待されるSANが含まれていることを確認するには、OpenSSLがインストールされている任意のクライアントで以下を実行します：

```
echo <paste CSR PEM> | openssl req -noout -text | grep -A3 "Subject
Alternative"
```

期待される出力：

```
X509v3 Subject Alternative Name: critical
    DNS:nfs.example.com, IP Address:192.0.2.130
```

2b.ONTAP CAで**CSR**に署名します。

```
ontap9::> security certificate sign -vserver <svm> -ca <ca-name> -ca
-serial <ca-serial> -expire-days 365 -hash-function SHA256
```

指示が表示されたら、CSR PEMブロックを貼り付けてください。出力から署名済み証明書のPEMをコピーしてください。

2c.署名付きサーバー証明書をインストールします

```
ontap9::> security certificate install -vserver <svm> -type server -cert
-name <cert-name>
```

プロンプトが表示されたら：

- 署名済みの証明書（PEM形式）を貼り付けてください。
- 秘密鍵のPEMを貼り付けてください。
- 中間証明書またはルート証明書を求められたら、CA証明書のPEMを貼り付けてEnterキーを押し、証明書の追加を停止するには「n」と答えてください。

2d.インストールされている証明書を確認します。

```
ontap9::> security certificate show -vserver <svm> -type server -common
-name <cert-name>
```

有効期限と、該当項目が存在することを確認してください。

ステップ**3**：データ**LIF**上で**TLS**経由の**NFS**を有効にする

サーバ証明書をインストールしたら、対象のLIF上でTLS経由のNFSを有効にします。

```
ontap9::> vserver nfs tls interface enable -vserver <svm> -lif <lif>
-certificate-name <cert-name>
```

LIFがTLSに対応していることを確認してください。

```
ontap9::> vserver nfs tls interface show -vserver <svm>
```

期待される出力：

```
Vserver:              <svm>
Logical Interface:    <lif>
IP Address:           <lif-ip>
TLS Status:           enabled
TLS Certificate Name: <cert-name>
Enforce Host Authentication: false
```

`TLS Status: enabled` は、ONTAPがこのLIFのポート2049でTLSをネゴシエートすることを確認します。`xprtsec=tls`または `xprtsec=mtls`を使用するクライアントは、TLSで保護された接続を受け取ります。ステップ7で強制が追加されない限り、TLSを要求しないクライアントは引き続き平文で接続します。

ステップ**4**：**Linux**クライアントに**CA**証明書をインストールする

LinuxクライアントはONTAPのサーバー証明書に署名したCAを信頼する必要があります。これがないと、`tlshd`サーバーの証明書が信頼されていないため、TLSハンドシェイクを拒否します。

ONTAP CAを使用した場合（手順**1**）

CA証明書をONTAPからエクスポートします：

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields cert
```

出力から証明書の PEM をコピーしてファイルに保存します（例： `nfs-ca.crt`）。このファイルを Linux クライアントに転送します。

外部認証局を使用した場合

外部 CA インフラストラクチャから CA 証明書 PEM を取得し、ファイルに保存します （例： `nfs-ca.crt` ）。このファイルを Linux クライアントに転送します。

CA証明書をシステム信頼ストアにインストールする

RHEL / Rocky / AlmaLinux / Fedora：

```
sudo cp nfs-ca.crt /etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
sudo update-ca-trust
```

Debian / Ubuntu：

```
sudo cp nfs-ca.crt /usr/local/share/ca-certificates/nfs-tls-ca.crt
sudo update-ca-certificates
```

tlshd がこの **CA** を信頼ストアとして使用するように設定します

編集 `/etc/tlshd.conf`：

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
```

CA証明書を配置した場所に合わせて、 `x509.truststore`パスを調整してください。

設定を適用するには、tlshdを再起動してください：

```
sudo systemctl restart tlshd
```

tlshdが正常に起動したことを確認します：

```
journalctl -u tlshd -n 20 --no-pager
```

出力にエラー行があってはなりません。

ステップ**5**：クライアント上で**LIF FQDN**を解決する

`tlshd`は、マウントコマンドで使用されているホスト名に対してサーバー証明書を検証します。マウントする前に、クライアント上で `<lif-fqdn>`が `<lif-ip>`に解決されることを確認してください。

```
getent hosts <lif-fqdn>
```

ホスト名がDNS経由で解決されない場合は、静的エントリを追加します。

```
echo <lif-ip> <lif-fqdn> | sudo tee -a /etc/hosts
```

ステップ**6**：**TLS**経由の**NFS**でマウントする

カーネルTLSモジュールがまだロードされていない場合は、ロードします。

```
sudo modprobe tls
```

マウントポイントを作成してマウントします。

```
sudo mkdir -p <mountpoint>
sudo mount -t nfs \
  -o vers=4.1,xprtsec=tls \
  <lif-fqdn>:<export-path> <mountpoint>
```

ステップ**7**：**TLS**接続を確認する

クライアント側

マウントがアクティブで、次のように表示されていることを確認します `xprtsec=tls`：

```
mount | grep nfs
```

期待される出力（マウントを含む行）：

```
<lif-fqdn>:<export-path> on <mountpoint> type nfs4
(rw,...,xprtsec=tls,...)
```

TLSハンドシェイクが正常に完了したことを確認します `tlshd`：

```
journalctl -u tlshd -n 10 --no-pager
```

以下の内容を含む行を探してください：

```
Handshake with '<lif-fqdn>' (...) was successful
```

ONTAP側

接続が `TLS/nfs`としてリストされていることを確認してください（接続が確立されたばかりの場合は、まず少量のI/Oを生成してください）：

```
ontap9::> network connections active show -vserver <svm>
```

予想されるエントリー：

```
<lif>:2049  <client-fqdn>:<port>  TLS/nfs
```

TLSハンドシェイクエラーが発生していないことを確認してください。

```
ontap9::> event log show -severity error -message-name
Nblade.TLSHandshakeFailed
```

マウント試行以降に新たなエントリがないということは、ハンドシェイクが成功したことを意味します。

オプション：特定のクライアントに対して**TLS**を必須にする（エクスポート ポリシーの適用）

デフォルトでは、TLS を介した NFS はオプトイン方式です。TLS を要求しないクライアントでも、TLS が有効になっている LIF 上で平文で接続できます。特定のエクスポート ルールに TLS を強制するには、 `-allow-nfs-tls-only true`を設定します。

```
ontap9::> vserver export-policy rule modify -vserver <svm> -policyname
<policy-name> -ruleindex <rule-index> -allow-nfs-tls-only true
```

この設定を行うと、そのルールに一致するNFSクライアントのうち、TLSを使用しないクライアントは、エクスポート ルールの評価時点で拒否されます。既存のTLS接続には影響はありません。

確認：

```
ontap9::> vserver export-policy rule show -vserver <svm> -policyname
<policy-name> -fields allow-nfs-tls-only
```

オプション：相互**TLS** （クライアント認証）

標準のNFS over TLSは、サーバーをクライアントに対して認証します（サーバーのみのTLS）。相

互TLS(`xprtsec=mtls`さらに、クライアントにはONTAPが検証する証明書の提示が求められます。これにより、両側で暗号化によるホスト認証が提供されます。

*クライアント OS の要件*相互 TLS には `ktls-utils` 0.12 以降が必要です。RHEL 9.7 に同梱されているバージョン（(`ktls-utils 0.11`）は機能しません。設定に関係なく、クライアント証明書を送信しません。RHEL 10.1（(`ktls-utils 1.2.1`）は検証済みです。続行する前に `ktls-utils`のバージョンを確認してください。

マウントオプション `xprtsec=mtls`を使用し、 `xprtsec=tls`は使用*しないでください*。 `xprtsec=tls`を使用すると、カーネルは認証モード `HANDSHAKE_AUTH_UNAUTH`を `tlshd`に送信します。これにより匿名ハンドシェイクパスが使用され、クライアント証明書が設定されていても提示されません。

ステップ **1**：クライアント証明書用の **CA** を作成する （**ONTAP**）

これはステップ1と同じCAでも、別のCAでも構いません。本番環境では、サーバーとクライアントの証明書チェーンが分離されるように、別のCAを使用することをお勧めします。

```
ontap9::> security certificate create -vserver <svm> -common-name "NFS-
mTLS-CA" -type root-ca -expire-days 3652 -hash-function SHA256
```

シリアル番号を `<mtls-ca-serial>`として記録します。

ステップ **2**：**CA** をクライアント **CA** トラスト アンカーとしてインストールする （**ONTAP**）

CA証明書をエクスポートします：

```
ontap9::> security certificate show -vserver <svm> -common-name "NFS-mTLS-
CA" -type root-ca -fields cert
```

タイプ `client-ca`としてインストールします：

```
ontap9::> security certificate install -vserver <svm> -type client-ca
```

プロンプトが表示されたら、CA証明書のPEMを貼り付けてください。確認：

```
ontap9::> security certificate show -vserver <svm> -type client-ca
```

ステップ **3**：**LIF** で **enforce-host-auth** を有効にする（**ONTAP**）

```
ontap9::> vserver nfs tls interface modify -vserver <svm> -lif <lif>
-enforce-host-auth true
```

確認：

```
ontap9::> vserver nfs tls interface show -vserver <svm> -instance
```

確認： `Enforce Host Authentication: true`。

ステップ**4**：クライアントキーと**CSR**を生成する（**Linux**クライアント）

```
sudo mkdir -p /etc/nfs
sudo openssl genrsa -out /etc/nfs/client.key 2048
sudo chmod 600 /etc/nfs/client.key

sudo openssl req -new \
  -key /etc/nfs/client.key \
  -subj "/CN=<client-fqdn>/C=US" \
  -addext "subjectAltName=DNS:<client-fqdn>,IP:<client-ip>" \
  -out /tmp/client.csr

cat /tmp/client.csr
```

手順 **5**：クライアント **CSR** に **ONTAP CA** で署名する

ONTAPクラスタで：

```
ontap9::> security certificate sign -vserver <svm> -ca "NFS-mTLS-CA" -ca
-serial <mtls-ca-serial> -expire-days 365 -hash-function SHA256
```

プロンプトが表示されたら、 `/tmp/client.csr`の内容を貼り付けます。出力から署名済み証明書のPEMをコピーします。

ステップ**6**：クライアント証明書チェーンファイルを作成する（**Linux**クライアント）

署名済みの証明書を `/tmp/client-signed.crt`に保存します。CA証明書PEM（`nfs-mtls-ca.crt`）も取得してください。それらを連結してチェーンファイルを作成します。

```
sudo bash -c "cat /tmp/client-signed.crt /path/to/nfs-mtls-ca.crt \
  > /etc/nfs/client-chain.crt"
sudo chmod 600 /etc/nfs/client-chain.crt
```

なぜチェーンファイルを使用するのか？ `tlshd`1.2.1 は `gnutls_pcert_list_import_x509_raw`を使用し、GnuTLS が `find_x509_client_cert`コールバック中に発行者を正しく解決するために、証明書チェーン全体（リーフに続いて CA）が必要です。リーフのみのファイルを使用すると、GnuTLS のアサーションエラーが発生します。

ステップ**7**：**/etc/tlshd.conf**をクライアント証明書で更新する（**Linux**クライアントの場合）

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
x509.certificate=/etc/nfs/client-chain.crt
x509.private_key=/etc/nfs/client.key
```

tlshdを再起動します。

```
sudo systemctl restart tlshd
```

ステップ**8**：**xprtsec=mtls**を指定してマウントする

```
sudo mount -t nfs \
  -o vers=4.1,xprtsec=mtls \
  <lif-fqdn>:<export-path> <mountpoint>
```

ステップ**9**：相互**TLS**を確認する

クライアント：

```
mount | grep nfs
# Confirm: xprtsec=mtls in mount options

journalctl -u tlshd -n 5 --no-pager
# Confirm: "Handshake with '<lif-fqdn>' (...) was successful"
```

ONTAP：

```
ontap9::> network connections active show -vserver <svm>
# Confirm: <lif>:2049  <client-fqdn>:<port>  TLS/nfs

ontap9::> event log show -severity error -message-name
Nblade.TLSHandshakeFailed
# No new entries = success
```

重要なデフォルト設定

- `-enforce-host-auth = false`--NFS over TLS は、デフォルトではホストベースの認証を強制しません。これはより緩やかな設定です。これを `true`に設定すると、証明書のIDがLIFのホストIDと一致しないTLS接続が拒否されます。
- `-skip-san-validation = false`--SANチェックはデフォルトで実行されます。これを `true`に設定すると、証明書とLIFのIDバインディングが緩和されます。このパラメータは書き込み専用です：後続の `show`または `GET`では値が反映されないため、管理者は有効化時または変更時にSAN検証がスキップされたかどうかを後から判断できません。
- `-allow-nfs-tls-only = false`--エクスポートポリシールールは、デフォルトではTLSを要求しません。LIF上でTLS経由のNFSを有効にしても、それ自体では平文NFSを拒否することにはなりません。TLSのみを厳格に使用したい場合は、ルールごとにオプトインし、まずそれらのクライアントにデータを提供するすべてのデータLIFでTLSが有効になっていることを確認してください。そうしないと、アクセスが拒否されます。

  `vserver export-policy rule create`および `vserver export-policy rule modify`コマンドに新しいフィールド `-allow-nfs-tls-only`が追加されました。これは、一致するクライアントをNFS over TLS接続のみに制限するものです。

RESTエンドポイント

組み込みの Swagger ドキュメントを使用して REST API をインタラクティブに参照できます。ブラウザで `https://<cluster-mgmt-ip>/api/docs`にアクセスしてください。TLS 上の NFS エンドポイントは、LIF 構成の `/api/protocols/nfs/tls/interfaces`パスと、エクスポートポリシールールフィールドの `/api/protocols/nfs/export-policies/{policy.id}/rules`にあります。

セキュリティ

このページでは、ONTAP 9.19.1 における TLS 経由の NFS に関する RBAC 要件、証明書の検証、暗号化パラメータ、監査、および既知のセキュリティ制限について説明します。

役割と**RBAC**の要件

`vserver nfs tls interface`コマンドファミリー（`-enable`、 `disable`、 `modify`、および `show`）はSVMスコープです。クラスター `admin`ロール、または所有するSVMの `vsadmin`によって実行できます。

`vserver export-policy rule`上の `-allow-nfs-tls-only`フィールドは、既存のexport-ruleオブジェクトの書き込みフィールドです。標準のexport-policyルールRBACを使用します。

`/api/protocols/nfs/tls/interfaces`配下のREST エンドポイントは、上記のCLIコマンドと1対1で対応しています。標準のNAS管理者RBACを使用します。個別のRESTロールは定義されていません。

認証と許可

LIF 上で TLS 経由の NFS を有効にするには、 `security certificate install`を使用して SVM にサーバ X.509 証明書をインストールする必要があります。証明書は、 `-certificate-name`を使用して有効化時に LIF ごとにバインドされます。

ONTAPは、提供されたサーバー証明書に対して2つのチェックを実施します。

1. 証明書の共通名（CN）は、LIFの完全修飾ドメイン名（FQDN）と一致している必要があります。
2. LIFのIPアドレスは、証明書のサブジェクト代替名（SAN）リストに記載されている必要があります。

オプション `-skip-san-validation`ブール値（デフォルト `false`）は、有効化時または変更時にSANチェックを抑制します。

チェックが失敗するたびに、それぞれ異なるエラーが返されます。

相互TLS（mTLS）ホスト認証はオプトイン方式です。 `-enforce-host-auth true`を `vserver nfs tls interface enable`または `modify`に設定して有効にしてください。デフォルトは `false`で、サーバー側のみの認証を意味します。クライアント証明書は、SVMにインストールされているCAトラストチェーンに対して検証されます。このCAトラストチェーンのプロビジョニングはお客様の責任となります。

ユーザ認証

ユーザ認証はTLSによって変更されません。TLSは、通信回線上の機密性とホスト認証を追加します。 `AUTH_SYS`UNIX UID/GIDまたは `RPCSEC_GSS`/KerberosをRPCのユーザ認証に引き続き使用する必要があります。RFC 9289はこれについて明確に述べています：TLSはトランスポートを保護し、既存のNFS認証フレーバーはこれまでと同様にユーザ認証を処理します。

暗号化

転送中

LIF上でTLS経由のNFSが有効になっている場合、使用されるバージョンはTLS 1.3のみです。以下の暗号スイートがサポートされています：

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`
- `TLS_CHACHA20_POLY1305_SHA256`

キー交換では、 `secp384r1`曲線上で ECDHE を使用します。暗号化は、TLS対応LIF上で伝送されるNFSv3およびNFSv4.xトラフィックに適用されます。

監査

NFS over TLS のすべての構成変更は、標準の ONTAP 監査ログ（(`security audit log show`）に記録さ

れます。以下の操作がログに記録されます：

- `vserver nfs tls interface enable`
- `vserver nfs tls interface modify`
- `vserver nfs tls interface disable`
- `vserver export-policy rule create -allow-nfs-tls-only`
- `vserver export-policy rule modify -allow-nfs-tls-only`

読み取り専用 `show`および `GET`操作は標準の ONTAP 監査ポリシーに従い、監査がログを記録するように設定されていない限り、通常は記録されません。

NFS over TLS データ パスで、顧客から見える3つのEMSイベントが発信されます。イベントの詳細、トリガー条件、およびレート制限については、"EMSメッセージ"を参照してください。

テナント境界線

NFS over TLSの設定はSVMごとに行われます。SVM管理者は、自身のSVMに属するLIF上のTLS設定のみを表示および管理できます。クラスタ管理者はすべてのSVMを表示できます。

サーバー証明書の参照先はSVMローカルです。この設定はクラスタ全体に複製されるため、特定のLIFを処理するすべてのノードが同じTLS設定を適用します。

既知のセキュリティ関連の制限事項

自己署名証明書に関する注意点CLI `enable`および `modify`コマンドは、自己署名証明書を使用すると中間者攻撃にさらされる可能性があると警告します。 `security certificate install`を使用してインストールされた CA 署名証明書を使用してください。

相互**TLS**はオプトイン方式です。 デフォルト `-enforce-host-auth false`では、TLS上のNFSはネットワーク上の機密性と完全性を保護し、サーバーをクライアントに対して認証しますが、クライアントホストを暗号化によって認証するわけではありません。必要な場合は、mTLSを明示的に有効にしてください。

TLSのみの適用は、エクスポートポリシールールごとに行われ、グローバルには適用されません。関連するエクスポートポリシールールに `-allow-nfs-tls-only true`を設定するまで、同じLIFは、そのルールによって許可されているクライアントからの非TLS NFS接続を引き続き受け入れることができます。

TLS 経由の NFS を監視する

TLS 上の NFS は、 `nfs_tls`オブジェクトのカウンターマネージャカウンターと、接続状態および強制動作の追跡に使用できる 4 つの EMS イベントを公開します。

Counter Manager カウンター

NFS over TLS カウンターマネージャのすべてのカウンターは、admin-scope オブジェクト上にあります `nfs_tls`。次のコマンドで確認できます `statistics show -object nfs_tls`。 `-counter <name>`を使用して単一のカウンターにフィルタリングするか、 `-instance`を使用して特定のSVMまたはノード行に範囲を絞り込みます。

識別子/ラベルカウンター（文字列）：

- `nfs_tls:instance_name`--行のインスタンス名（構成要素SVM名）。
- `nfs_tls:instance_uuid`--行のインスタンスUUID（構成要素SVM識別子）。
- `nfs_tls:vserver_id`--集計された行のSVM識別子ラベル。
- `nfs_tls:vserver_name`--集計された行のSVM名ラベル。
- `nfs_tls:node_name`--集計行のノード名ラベル。

接続量カウンター（レート）：

- `nfs_tls:tls_total_connection_requests`--処理されたNFS over TLS接続要求の総数（成功＋失敗）。
- `nfs_tls:tls_connection_success`-- NFS over TLS接続が成功しました。
- `nfs_tls:tls_disabled_connection_failures`--SVMでTLS経由のNFSが無効になっているため、接続が拒否されました。
- `nfs_tls:tls_connection_handshake_failures`--TLSハンドシェイク中に失敗した接続。
- `nfs_tls:tls_configuration_not_found`--SVM/LIFペアにTLS設定が存在しないため、接続試行が拒否されました。
- `nfs_tls:tls_connection_mismatch`--メモリ内の接続識別子がハンドシェイク完了時に観測された接続と一致しなかったために失敗した接続。

レイテンシカウンター（平均）：

- `nfs_tls:tls_handshake_average_latency`--TLSハンドシェイクの平均遅延時間（マイクロ秒）。基本カウンター： `tls_connection_success`。

Event Management System（EMS）メッセージ

顧客から見える 4 つの EMS イベントが、NFS over TLS のデータ パス上の NFSサーバによって送信されます。次のコマンドで確認できます： `event log show`

`Nblade.TLSConfigError`

重大度 `ERR`、10分間のレート制限。クライアントがTLS設定のないSVM/LIFに対してTLS経由のNFS接続を試みた際にトリガーされます。ログに記録されるフィールド：クライアントIPアドレス、SVM名、LIF IPアドレス。解決するには、 `vserver nfs tls interface enable`で設定を有効にしてください。

`Nblade.TLSHandshakeFailed`

重大度 `ERR`、10分間のレート制限。クライアントとサーバー間のTLSハンドシェイクが失敗した場合にトリガーされます。ログに記録されるフィールド：SVM名、LIF IPアドレス、クライアント（リモート）IPアドレス、サーバー証明書UUID。解決するには、LIF上のTLS設定を確認し、ネットワークの状態をチェックしてください。問題が解決しない場合は、NetAppサポートにお問い合わせください。

`Nblade.NfsTlsDisabled`

重大度 `ALERT`、レート制限は24時間です。クライアントが、この機能が無効になっているSVM上でTLS経由のNFS接続を試みた際にトリガーされます。記録されるフィールド：SVM名。

`Nblade.nfsTLSAccessErr`

重大度 `ERR`。エクスポートポリシールールに一致するクライアントが `-allow-nfs-tls-only true`

TLSなしでNFSパスをマウントまたはアクセスしようとしたときにトリガーされます。このイベントを使用して、TLS非対応クライアントが意図どおりにブロックされていることを確認してください。

Performance

TLSは、CPU、メモリ、ネットワークという3つのリソース面でコストを増加させます。

リソースコストの概要

CPUが主なコスト要因です。TLS 1.3ハンドシェイクは、非対称暗号化、証明書の解析、および鍵交換をカバーする接続ごとの1回限りの費用です。接続が確立されると、定常状態のオーバーヘッドは、AES-GCMまたはChaCha20-Poly1305を使用した対称レコード暗号化になります。Mellanox ConnectX-6 Dx (CX6-Dx) またはConnectX-7 (CX7) NICを搭載したプラットフォームでは、NIC自体がカーネルTLS（KTLS）オフロードを介して暗号化と復号化を実行するため、定常状態のCPUコストが大幅に削減されます。

*メモリ*への影響は低いです。TLSは、接続ごとのセッション状態と、ノードごとのTLS構成キャッシュを追加します。キャッシュサイズには上限があり、エントリは有効期限（TTL）に基づいて管理され、バックグラウンドで更新されます。

*ネットワーク*のオーバーヘッドは小さいです。TLS 1.3のレコードフレーミングでは、レコードごとに固定のオーバーヘッドと認証タグが追加されます。ハンドシェイクは、接続確立時のみ往復通信を追加し、RPCごとには追加しません。

TLSのパフォーマンス低下

ONTAP における TLS 経由の NFS には、ハードウェアオフロードパスとソフトウェア TLS パスという 2 つの明確な経路があります。ハードウェアオフロードパスは、CX6-Dx または CX7 NIC を搭載したプラットフォームで利用できます。ソフトウェア TLS パスは、オフロード対応 NIC を搭載していないプラットフォームで使用されます。

オフロード機能を備えたNICを搭載したプラットフォームでは、さまざまなワークロードにおいて、パフォーマンスはプレーンテキストNFSの約10%以内であることが確認されました。オフロード機能を備えたNICを搭載していないプラットフォームでは、ソフトウェアTLSパスはワークロードの影響を受けやすく、最悪の場合、プレーンテキストNFSと比較してスループットが約30%低下する可能性があります。これらは特性を示す数値であり、保証された仕様ではありません。結果はワークロードの種類、I/Oサイズ、および接続数によって異なります。同じノード上でTLSトラフィックと非TLSトラフィックを混在させる場合、非TLSトラフィックのスループットにも何らかの影響が出る可能性があります。

スケーリング係数

以下の要因により、TLSの集約CPUコストまたはハンドシェイクレイテンシが増加します：

*接続のチャーン*新たな接続はすべて、ハンドシェイクのコストが発生します。NFSサーバへのTCP接続を頻繁に開閉するワークロードは、接続が長時間続くワークロードよりも、TLS CPUの総使用量が高くなります。

*テイクオーバーまたはネットワークイベント後のマウントストーム。*HAテイクオーバー後など、多数のクライアントが同時に再接続するワークロードでは、接続ごとにTLS 1.3ハンドシェイクのコストが全額発生します。モニター `nfs_tls:tls_handshake_average_latency`し、それに応じて接続のヘッドルームを計画してください。

*多数の異なるクライアントID（相互TLS）*相互TLS（mTLS）の導入では、検証される固有のクライアント証明書の数に応じて、ハンドシェイク用のCPUリソースが拡張されます。

*mTLSとサーバーオンリーTLSの比較*ホスト認証（mTLS）を有効にすると、サーバー側でクライアント証明書の検証が追加されるため、各ハンドシェイクのコストはサーバーのみのTLSよりも若干高くなります。定常状態におけるRPCあたりのコストは変わりません。

*TLS設定の変更*TLSインターフェース構成の頻繁な変更（証明書のローテーション、有効化/無効化のサイクルなど）は、ノードごとのTLS構成キャッシュを無効にし、ルックアップを管理ホストに戻すことを強制するため、一時的にハンドシェイクのレイテンシが増加します。

相互運用性と制限

TLS 上の NFS は、標準の ONTAP エクスポートポリシー制御と連携し、SVM-DR および MetroCluster を介してレプリケートされます。また、導入前に把握しておくべき、プラットフォーム上のいくつかの厳格な制限事項と運用上の推奨事項があります。

相互運用性

共存可能なサポート機能

*エクスポートポリシー、qtreeエクスポート、およびジャンクションパス。*エクスポートポリシールールは `-allow-nfs-tls-only`フィールドを取得します。このフィールドにより、ルールごとにTLSを要求することができます。これは、既存のクライアントマッチ、プロトコル、読み取り専用/読み書き、スーパーユーザー、匿名、chown-mode、allow-suid、およびNTFS-UNIXセキュリティ制御と連携します。qtreeエクスポートとジャンクションパスのマウントは、同じエクスポートポリシーメカニズムを通じてTLS要件を継承します。System Managerは、NFSアクセス選択画面で `-allow-nfs-tls-only`設定を表示します。

TLS経由のNFSレプリケーションおよびDRサポートの概要を以下の表に示します。複製メカニズムの背景については、"アーキテクチャ"を参照してください。

レプリケーション／災害復旧	**9.19.1** での **TLS** 経由の **NFS**
SVM-DR	*サポート対象です。*TLSインターフェース行はSVMスコープでレプリケートされます（ステータス、証明書名とUUID、enforce-host-auth）。の `-allow-nfs-tls-only`エクスポートルールフィールドは、エクスポートポリシーと一緒にレプリケートされます。
MetroCluster（SVMレベルの複製）	*サポート対象です。*SVM-DRと同じレプリケーションパス。宛先SVM上の証明書マテリアルのライフサイクルは、証明書マネージャーが管理します。
SnapMirror（ボリューム複製）	*サポート対象です。*クライアント側TLSトランスポートとは独立しています。
クラウドホスト型ONTAPバリアント	9.19.1ではサポートされていません。

制約付き機能

*クライアントの要件*NFSクライアントは、"RFC 9289"に従ってONC RPC用のTLSを実装する必要があります。Linuxでは、これは `xprtsec=tls`（または `xprtsec=mtls`）マウント オプションをサポートするカーネル内NFSクライアントによって提供され、 `ktls-utils`パッケージのユーザ空間TLSハンドシェイク ヘルパー `tlshd`と組み合わせて使用されます。最小カーネル バージョン、ユーザ空間パッケージ バージョン、サポート対象のLinuxディストリビューションを含む、確定的なクライアント マトリックスについては、Interoperability Matrix Tool（IMT）を参照してください。

制限事項および注意事項

- *クラウドホスティングONTAPバリアント。*Cloud Volumes ONTAPおよびその他のクラウドホスト型ONTAPバリアントは、ONTAP 9.19.1ではサポートされていません。
- *NFS over Remote Direct Memory Access (RDMA)*NFS over RDMAとNFS over TLSは、同じLIF上で相互に排他的です。

ノードごとの制限

現在、ONTAP の NFS over TLS にはハードコードされた接続制限はありません。サポートされている制限に関する最新情報については、"Hardware Universe"を参照してください。

ベストプラクティス： マウントストームやHAテイクオーバーに備えて余裕を持たせるため、ノードごとのNFS over TLS接続数を10,000未満に抑えてください。

クラスターごとの制限

コード上で、クラスター全体に対する個別の集計上限は設定されていません。

LIFごとおよびオブジェクトごとの制限

- 構成テーブルは、 `(SVM, LIF)`タプルをキーとしています。各LIFには、NFS over TLSの設定行が0行または1行含まれています。
- NFS over TLSが有効になっているLIFごとに、サーバ証明書が正確に1つバインドされます。証明書は `vserver nfs tls interface enable`時に指定され、 `… modify -certificate-name`で変更できます。
- `-allow-nfs-tls-only`はエクスポートポリシールールごとに1つのブール値です。この機能では、ルール数の上限が別途追加されることはありません。ポリシーごとおよびSVMごとのエクスポートルールの標準最大値が適用されます。

強制動作

`-allow-nfs-tls-only true` 強制。このフィールドが `true`一致するエクスポートポリシールールに設定されている場合、RFC 9289に従ってONC RPC に TLS を使用していない一致するクライアントからの NFS 接続試行は、エクスポートルールの評価時に拒否されます。これらのクライアントからの既存の TLS 接続は影響を受けません。

`-enforce-host-auth true``の適用。 `**true**`が `**(SVM, LIF)**`で有効になっている場合、クライアント証明書の**ID**が**LIF**に設定されたホスト**ID**と一致しない**TLS**ハンドシェイクは、**TLS**ハンドシェイク中に拒否されます。**EMS**イベント `**Nblade.TLSHandshakeFailed**（重大度 `ERR`、イベントソースごとに10分に1回のレート制限）は、ハンドシェイクが失敗するたびに発行されます。

EMSレート制限。
`Nblade.TLSConfigError`および `Nblade.TLSHandshakeFailed`は、イベントソースごとに10分に1回のレート制限が適用されます。 `Nblade.NfsTlsDisabled`は、イベントソースごとに24時間に1回のレート制限が適用されます。これらは、継続的な障害発生時におけるイベントログの容量に対して意図的に設けられた上限です。バースト発生時には、各レート制限ウィンドウ内で最初に発生した事象のみが記録されます。

ソフトリミットと推奨事項

以下は推奨事項であり、厳密な上限値ではありません。

- *ノードあたり10,000 NFS-over-TLS接続数のヘッドルームを維持してください。*ハードコードされた上限はありませんが、ノードごとのNFS-over-TLS接続数は10,000以下に抑えてください。
- *HA（高可用性）による引き継ぎ後、TLS の完全な再ハンドシェイクを計画してください。*TLS セッションは TCP スコープであり、テイクオーバーが発生すると維持されません。すべてのクライアントは、存続しているノードまたは宛先ノードで新しい TLS 1.3 ハンドシェイクを使用して再接続するため、マウントストームに備えてください。接続数を 10,000 未満に抑えておくことで、その急増を吸収できる余裕が生まれます。

ONTAP SANテクニカルレポート

ONTAP SANストレージは、シンプルなSAN環境を実現し、ミッションクリティカルなデータベースやその他のSANワークロードに高可用性を提供します。ONTAP SANは、Oracle、SAP、Microsoft SQL Serverのデータベースに加え、VMwareやその他の主要なハイパーバイザーとの業界最高レベルのデータサービス統合により、エンタープライズデータベースアプリケーションの価値実現までの時間を短縮します。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載されている"ONTAP SANストレージ管理"ています。

"TR-4080：『Best Practices for Modern SAN in ONTAP』"
ONTAPのブロックプロトコルと推奨事項について説明します。

"TR-4684：『Implementing and configuring Modern SANs with NVMe over Fabrics（NVMe-oF）』"
NVMe over Fabricsトランスポート（NVMe over Fibre ChannelおよびNVMe over TCP）の実装と設定方法について説明します。トピックには、NVMeプロトコルとトランスポートを使用して可用性とパフォーマンスに優れた最新SANソリューションを構築するための設計、実装、設定、管理ガイドライン、推奨プラクティスなどがあります。

"TR-4968：『NetApp All-SAN Array data availability and integrity』"
オールSANアレイシステムのさまざまなデータ保護機能とデータ整合性機能によってアプリケーションのアップタイムを最大限に高める方法と、SANネットワークの設計、実装、管理に関する推奨事項について説明します。

"最新のSANクラウド対応フラッシュ解決策"
このNetApp検証済みアーキテクチャは、NetApp、VMware、Broadcomによって共同で設計および検証されています。最新のBrocade、Emulex、VMware vSphereテクノロジソリューションとNetAppオールフラッシュストレージを併用しており、エンタープライズSANストレージとデータ保護の新たな標準を打ち立て、卓越したビジネスバリューを生み出します。

セキュリティ

ONTAPセキュリティテクニカルレポート

ONTAPは進化を続けており、セキュリティは解決策に不可欠な要素となっています。ONTAPの最新リリースには多数のセキュリティ機能が新たに追加されており、ハイブリッドクラウド全体でデータを保護し、ランサムウェア攻撃を防止し、業界の推奨プラクティスに準拠するうえで、組織にとって計り知れない価値があります。これらの新機能は、組織のゼロトラストモデルへの移行もサポートします。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"ONTAPセキュリティとデータ暗号化"ています。

ONTAPサイバーボールト

"ONTAPサイバーボールト"NetAppのONTAPベースのサイバーボールトは、最も重要なデータ資産を保護するための包括的で柔軟なソリューションを組織に提供します。ONTAPでは、論理的なエアギャップと堅牢な強化手法を活用することで、進化するサイバー脅威に対して耐障害性に優れた、セキュアで分離されたストレージ環境を構築できます。ONTAPを使用すると、ストレージインフラの即応性と効率性を維持しながら、データの機密性、整合性、可用性を確保できます。

ランサムウェア

"TR-4572：『The NetApp 解決策for ransomware』" ランサムウェアに対応したNetAppソリューションを使用して、ランサムウェアがどのように進化したか、攻撃を特定し、拡散を防止し、できるだけ迅速にリカバリする方法をご紹介します。このドキュメントで提供されるガイダンスとソリューションは、情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成しながら、サイバーレジリエントなソリューションを組織に提供することを目的としています。

"TR-4526：『Compliant WORM storage using NetApp SnapLock』"
多くの企業では、コンプライアンス要件を満たすため、または単にデータ保護戦略にレイヤを追加するために、Write Once、Read Many（WORM）データストレージをある程度使用しています。ONTAPのWORM解決策であるSnapLockを、WORMデータストレージが必要な環境に統合する方法を説明します。

ゼロトラスト

"NetAppとゼロトラスト" ゼロトラストは、従来、マイクロコアと境界（MCAP）を構築してデータ、サービス、アプリケーション、資産を保護するネットワーク中心のアプローチであり、セグメンテーションゲートウェイと呼ばれる制御機能を備えていました。ONTAPは、ゼロトラストに対してデータ主体のアプローチを採用しています。このアプローチでは、ストレージ管理システムがセグメンテーションゲートウェイとなり、お客様のデータへのアクセスを保護および監視します。特に、FPolicyゼロトラストエンジンとFPolicyパートナーエコシステムは、正常なデータアクセスパターンと異常なデータアクセスパターンを詳細に把握し、内部の脅威を特定するためのコントロールセンターとなります。

多要素認証

"TR-4647：『Multifactor authentication in ONTAP best practices and Implementation guide』"
System Manager、Active IQ Unified Manager、およびONTAP Secure Shell（SSH）CLI認証を使用した管理

者アクセス用のONTAPの多要素認証機能について説明します。

"TR-4717：『ONTAP SSH authentication with a common access card』"
サードパーティのSSHクライアントをActivClientソフトウェアと組み合わせて設定し、Common Access Card（CAC;共通アクセスカード）に保存されている公開鍵を使用してONTAPストレージ管理者を認証する方法について説明します（ONTAPで設定されている場合）。

マルチテナンシー

"TR-4160：『Secure multitenancy in ONTAP』"
ONTAPでStorage VMを使用してセキュアマルチテナンシーを実装する方法と、設計上の考慮事項や推奨事項について説明します。

標準

"TR-4401：『PCI-DSS 4.0 and ONTAP』"
PCI DSS 4.0規格に照らしてシステムを検証する方法と、NetApp ONTAPシステムに適用する制御の要件を満たす方法について説明します。

属性ベースのアクセス制御

"ONTAPによる属性ベースのアクセス制御"NFSv4.2のセキュリティラベルと拡張属性（xattrs）を設定してRole-Based Access Control（RBAC；ロールベースアクセス制御）とAttribute-Based Access Control（ABAC；属性ベースアクセス制御）をサポートする方法について説明します。ABACは、ユーザ、リソース、および環境の属性に基づいて権限を定義する認証方式です。

ランサムウェア向け**NetApp**ソリューション

ランサムウェアと**NetApp**の保護ポートフォリオ

ランサムウェアは、2024年に組織のビジネス中断を引き起こす最も重大な脅威の1つです。の "Sophosランサムウェアの現状2024"調査によると、ランサムウェア攻撃は調査対象者の72%に影響を及ぼしています。ランサムウェア攻撃はより高度で標的型に進化しており、脅威アクターは人工知能などの高度な手法を採用して影響と利益を最大化しています。

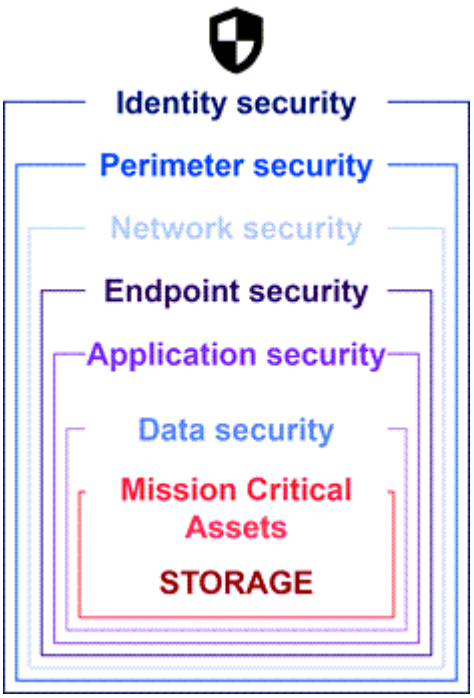
組織は、境界、ネットワーク、ID、アプリケーション、データの保存場所など、セキュリティ体制全体をストレージレベルで把握し、これらのレイヤを保護する必要があります。今日の脅威の状況では、ストレージレイヤでサイバー保護にデータ主体のアプローチを採用することが不可欠です。単一のソリューションですべての攻撃を阻止することはできませんが、パートナーシップやサードパーティなどのソリューションポートフォリオを使用することで、多層的な防御を実現できます。

にはNetApp製品ポートフォリオ、可視化、検出、修復のためのさまざまな効果的なツールが用意されており、ランサムウェアの早期発見、拡散の防止、必要に応じた迅速なリカバリを支援して、コストのかかるダウンタイムを回避できます。可視化と検出のためのサードパーティやパートナーソリューションと同様に、従来の階層型防御ソリューションは依然として普及しています。効果的な修復は、あらゆる脅威への対応において依然として重要な部分を占めています。書き換え不能なNetApp SnapshotテクノロジとSnapLockの論理的エアギャップソリューションを活用する業界独自のアプローチは、ランサムウェア対策機能における業界の差別化要因であり、業界のベストプラクティスでもあります。

2024年7月以降、以前PDFとして公開されていたテクニカルレポート『TR-4572：NetApp Ransomware Protection_』のコンテンツがdocs.netapp.comで公開されました。

データが主なターゲット

サイバー犯罪者は、データの価値を認識し、データを直接ターゲットにすることが増えています。境界、ネットワーク、およびアプリケーションのセキュリティは重要ですが、バイパスすることができます。ソースであるストレージレイヤでのデータ保護に重点を置き、重要な最終防衛線を提供します。ランサムウェア攻撃の目的は、本番環境のデータにアクセスして暗号化したりアクセス不能にしたりすることです。そのためには、攻撃者は境界からアプリケーションのセキュリティまで、今日組織によって導入されている既存の防御をすでに貫通している必要があります。



残念ながら、多くの組織はデータレイヤのセキュリティ機能を利用していません。そこで登場するのが、NetAppランサムウェア対策ポートフォリオであり、最前線でお客様を保護します。

ランサムウェアの真のコスト

身代金の支払い自体は、ビジネスへの最大の金銭的影響ではありません。支払い額はわずかではありませんが、ランサムウェアインシデントの被害によるダウンタイムコストと比べると、わずかです。

身代金の支払いは、ランサムウェア攻撃に対処する際のリカバリコストの要素の1つにすぎません。支払われた身代金を除くと、2024年の組織の報告によると、ランサムウェア攻撃からの復旧に要する平均コストは2730万ドルであり、2023年に報告された1820万ドルから100万ドル近く増加して "2024 Sophosランサムウェアの現状"います。Eコマース、株式取引、医療など、ITの可用性に大きく依存している組織の場合、コストは10倍以上になる可能性があります。

また、被保険企業がランサムウェア攻撃を受ける可能性が非常に高いことから、サイバー保険のコストも上昇し続けています。

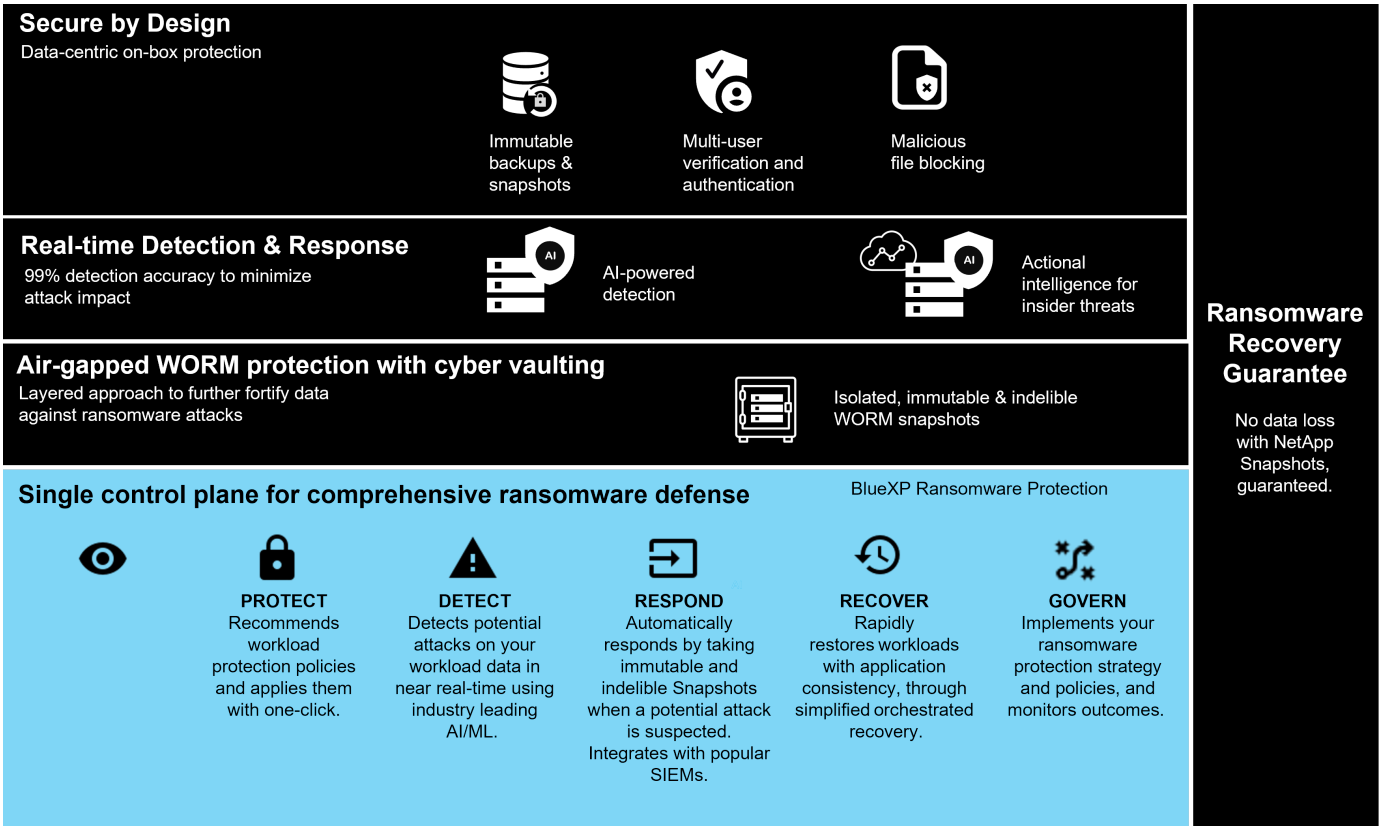
データレイヤでのランサムウェア対策

NetAppは、境界からストレージレイヤでのデータの配置場所まで、組織全体にわたってセキュリティ体制が広く深く浸透していることを認識しています。セキュリティスタックは複雑であり、テクノロジスタックのあらゆるレベルでセキュリティを提供する必要があります。

データレイヤでのリアルタイムの保護は、さらに重要であり、独自の要件があります。効果的に機能するには、この層のソリューションが次の重要な属性を提供する必要があります。

- *設計によるセキュリティ*により、攻撃が成功する可能性を最小限に抑える
- *リアルタイムの検出と対応*により、攻撃が成功した場合の影響を最小限に抑えます。
- *エアギャップによるWORM保護*重要なデータのバックアップを分離
- *単一のコントロールプレーン*による包括的なランサムウェア防御

NetAppはこれらすべてを実現し、さらに多くの機能を提供します。



NetAppのランサムウェア対策ポートフォリオ

NetAppは、"組み込みのランサムウェア対策"重要なデータに対してリアルタイムで堅牢かつ多面的な防御を提供します。その中核である、AIを活用した高度な検出アルゴリズムは、データパターンを継続的に監視し、99%の精度で潜在的なランサムウェアの脅威を迅速に特定します。攻撃に迅速に対応することで、ネットアップのストレージはデータのスナップショットを迅速に作成し、コピーを保護して迅速なリカバリを実現します。

データをさらに強化するために、NetAppの"サイバーヴォールティング"機能は論理的なエアギャップでデータを分離します。重要なデータを保護することで、迅速なビジネス継続性を確保します。

NetApp"NetAppランサムウェア保護"単一のコントロール プレーンで運用上の負担を軽減し、エンドツーエンドのワークロード中心のランサムウェア防御をインテリジェントに調整および実行します。これにより、リスクのある重要なワークロード データを 1 回のクリックで識別して保護し、潜在的な攻撃の影響を制限するために正確かつ自動的に検出して対応し、数日ではなく数分以内にワークロードを回復して、貴重なワークロード データを保護し、コストのかかる中断を最小限に抑えることができます。

データへの不正アクセスを保護するためのネイティブの組み込みONTAPソリューションとして、"マルチ管理者認証（MAV）"ボリュームの削除、管理ユーザの追加作成、Snapshotの削除などの処理を、2人目の指定管理者から承認を得た場合にのみ実行できる堅牢な機能セットを備えています。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。スナップショットを削除する前に、指定された管理者承認者を必要な数だけ設定できます。

NetApp ONTAPは、System ManagerにおけるWebベースの "多要素認証（MFA）"およびSSH CLI認証の要件に対応しています。

NetAppのランサムウェア対策は、進化し続ける脅威の状況にも安心して対応します。その包括的なアプローチは、現在のランサムウェア攻撃から防御するだけでなく、新たな脅威にも適応し、データインフラに長期的なセキュリティを提供します。

その他の保護オプションについて

- "Digital Advisorによるランサムウェア対策"
- "Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ"
- "FPolicy"
- "SnapLockと改ざん防止スナップショット"

ランサムウェアからのリカバリ保証

NetAppは、ランサムウェア攻撃が発生した場合にSnapshotデータをリストアすることを保証します。当社の保証：スナップショットデータのリストアをサポートできない場合は、適切に対応します。この保証は、AFF Aシリーズ、AFF Cシリーズ、ASA、FASシステムの新規購入時に利用できます。

詳細

- "リカバリ保証サービスの説明"
- "ランサムウェア対策保証ブログ"です。

関連情報

- "NetAppサポートサイトのリソースページ"
- "NetApp製品のセキュリティ"

SnapLockと改ざん防止スナップショットでランサムウェアを保護

NetAppのスナップ兵器の重要な武器は、ランサムウェアの脅威からの保護に非常に効果的であることが証明されているSnapLockです。不正なデータ削除を防止することで、SnapLockは追加のセキュリティレイヤを提供し、悪意のある攻撃が発生した場合でも重要なデータに影響を与えずにアクセスできるようにします。

SnapLock Compliance

SnapLock Compliance（SLC）は、データを消去できない方法で保護します。SLCでは、管理者がアレイを再初期化しようとした場合でも、データの削除が禁止されています。他の競合製品とは異なり、SnapLock Complianceはそれらの製品のサポートチームを通じてソーシャルエンジニアリングのハッキングに対して脆弱ではありません。SnapLock Complianceボリュームで保護されているデータは、そのデータが有効期限に達するまでリカバリできます。

SnapLockを有効にするには"ONTAP One"、ライセンスが必要です。

詳細

- "SnapLockのドキュメント"

スナップショットの改ざん防止

改ざん防止Snapshot（TPS）コピーを使用すると、悪意のある行為からデータを簡単かつ迅速に保護できます。SnapLock Complianceとは異なり、TPSは通常、ユーザが決められた時間データを保護し、高速リカバリのためにローカルに残しておくことができるプライマリシステムや、プライマリシステムからデータをレプリケートする必要がないプライマリシステムで使用されます。TPSはSnapLockテクノロジを使用して、同じSnapLock保持期限を使用しているONTAP管理者でもプライマリSnapshotが削除されないようにします。SnapLockが有効になっていなくても、Snapshotは削除できません。ただしSnapshotには、SnapLock Complianceと同じ消去不能な性質はありません。

スナップショットの改ざんを防止するには、"ONTAP One"ライセンスが必要です。

詳細

- "Snapshotをロックしてランサムウェア攻撃から保護"です。

FPolicyファイルブロッキング

FPolicyは、エンタープライズクラスのストレージアプライアンスへの不要なファイルの保存をブロックします。FPolicyは、既知のランサムウェアファイル拡張子をブロックする方法も提供します。ユーザには引き続きホームフォルダに対するフルアクセス権限がありますが、FPolicyでは管理者がブロック済みとしてマークしたファイルを格納することはできません。これらのファイルがMP3ファイルであるか、既知のランサムウェアファイル拡張子であるかは関係ありません。

FPolicyネイティブモードで悪意のあるファイルをブロック

NetApp FPolicyのネイティブモード（ファイルポリシーという名前を発展させたもの）は、不要なファイル拡張子が環境に侵入するのをブロックできるファイル拡張子ブロックフレームワークです。10年以上にわたってONTAPの一部として提供されており、ランサムウェアからの保護に非常に役立ちます。このゼロトラストエンジンは、Access Control List（ACL;アクセスコントロールリスト）権限以外にもセキュリティ対策を追加できるため、価値があります。

ONTAP System Manager およびNetApp Consoleでは、3000 を超えるファイル拡張子のリストを参照できます。

一部の拡張機能はご使用の環境では正当なものであり、ブロックすると予期しない問題が発生する可能性があります。ネイティブFPolicyを設定する前に、環境に適した独自のリストを作成してください。

ONTAPのネイティブモードはすべてのライセンスに含まれています。

詳細

- "ブログ：ランサムウェアとの戦い：パート3—ONTAP FPolicy、もう1つの強力なネイティブ（別名フリー）ツール"

FPolicy外部モードを使用したユーザとエンティティの動作分析（**UEBA**）の有効化

FPolicy外部モードは、ファイルアクティビティとユーザアクティビティを可視化するための、ファイルアクティビティの通知および制御フレームワークです。これらの通知は、外部ソリューションでAIベースの分析を実行して悪意のある動作を検出するために使用できます。

FPolicy外部モードは、特定のアクティビティを許可する前にFPolicyサーバからの承認を待機するように設定することもできます。このような複数のポリシーを1つのクラスタに設定できるため、柔軟性に優れています。

承認を提供するように設定されている場合、FPolicyサーバはFPolicy要求に応答する必要があります。そうしないと、ストレージシステムのパフォーマンスが低下する可能性があります。

FPolicy外部モードはに含まれてい"スヘテノONTAPライセンス"ます。

詳細

- "ブログ：Fighting Ransomware: Part Four—UBA and ONTAP with FPolicy external mode"

Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ

ストレージ ワークロード セキュリティ (SWS) は、 ONTAP環境のセキュリティ体制、回復性、アカウンタビリティを大幅に強化するNetApp Data Infrastructure Insightsの機能です。SWSはユーザ中心のアプローチを採用し、環境内のすべての認証済みユーザからのすべてのファイル アクティビティを追跡します。高度な分析を使用して、すべてのユーザの通常のアクセス パターンと季節的なアクセス パターンを確立します。これらのパターンは、ランサムウェア シグネチャを使用せずに疑わしい動作を迅速に特定するために使用されます。

SWS は、潜在的なランサムウェアやデータ削除を検出すると、次のような自動アクションを実行できます。

- 該当するボリュームのSnapshotを作成します。
- 悪意のあるアクティビティの疑いがあるユーザアカウントとIPアドレスをブロックします。
- 管理者にアラートを送信します。

SWSは、内部の脅威を迅速に阻止し、すべてのファイルアクティビティを追跡する自動化されたアクションを実行できるため、ランサムウェアイベントからのリカバリをはるかに簡単かつ迅速に実行できます。高度な監査ツールとフォレンジックツールが組み込まれているため、攻撃の影響を受けたボリュームやファイル、攻撃元のユーザアカウント、実行された悪意のあるアクションをすぐに確認できます。Snapshotの自動作成に

より、被害を軽減し、ファイルのリストアを高速化します。

ONTAPのAutonomous Ransomware Protection（ARP;自律型ランサムウェア対策）によるアラートもSWSに表示されるため、ARPとSWSの両方を使用してランサムウェア攻撃から保護する単一のインターフェイスが提供されます。

詳細

- "NetAppData Infrastructure Insights"

NetApp ONTAPに搭載されたAIベースの検出と応答機能

ランサムウェアの脅威がますます巧妙になるにつれ、防御メカニズムも進化していきます。NetAppの自律型ランサムウェア対策（ARP）は、ONTAPに組み込まれたインテリジェントな異常検出機能を備えたAIを基盤としています。オンにすると、サイバーレジリエンスに新たな防御レイヤを追加できます。

ARPとARP / AIは、ONTAPの組み込みの管理インターフェイスとSystem Managerを使用して設定でき、ボリューム単位で有効にできます。

自律型ランサムウェア防御（**ARP**）

ONTAP 9.10.1以降のもう1つのネイティブ組み込みONTAPソリューションである自律型ランサムウェア対策（ARP）では、NASストレージボリュームのワークロードのファイルアクティビティとデータエントロピーを調べて、潜在的なランサムウェアを自動的に検出します。ARPは、管理者にリアルタイムの検出、分析情報、データリカバリポイントを提供し、これまでにないオンボックスの潜在的なランサムウェア検出を可能にします。

ARPをサポートするONTAP 9 .15.1以前のバージョンでは、ARPは学習モードで開始され、一般的なワークロードのデータアクティビティを学習します。ほとんどの環境では、この処理に7日かかることがあります。ラーニングモードが完了すると、ARPは自動的にアクティブモードに切り替わり、ランサムウェアの可能性がある異常なワークロードアクティビティを探し始めます。

異常なアクティビティが検出された場合は、即座にSnapshotが自動作成され、感染データを最小限に抑えながら、可能な限り攻撃時点に近いリストアポイントが提供されます。同時に、管理者が異常なファイルアクティビティを確認できる自動アラート（設定可能）が生成され、アクティビティが実際に悪意のあるものかどうかを判断して適切なアクションを実行できるようになります。

アクティビティが想定されるワークロードである場合、管理者は簡単に誤検出としてマークできます。ARPはこの変更を通常のワークロードアクティビティとして学習し、今後の潜在的な攻撃としてフラグを立てなくな

ります。

ARPをイネーブルにするには"ONTAP One"、ライセンスが必要です。

詳細

- "自律型ランサムウェア対策"

自律型ランサムウェア対策 **/ AI**（**ARP / AI**）

ONTAP 9.15.1で技術プレビューとして導入されたARP / AIを使用することで、NASストレージ システムの組み込みのリアルタイム検出は次のレベルに引き上げられます。AIを活用した新しい検出テクノロジは、100万件を超えるファイルやさまざまな既知のランサムウェア攻撃についてトレーニングされています。ARPで使用される信号に加えて、ARP/AIはヘッダー暗号化も検出します。AIパワーと追加信号により、ARP/AIは99%以上の検出精度を実現します。これは、ARP/AIに最高のAAA評価を与えた独立したテストラボであるSE Labsによって検証されています。

モデルのトレーニングはクラウドで継続的に行われるため、ARP / AIはラーニングモードを必要としません。オンになった瞬間にアクティブになります。継続的なトレーニングとは、ARP / AIが発生したときに常に新しいタイプのランサムウェア攻撃に対して検証されることも意味します。ARP/AIには、自動更新機能も搭載されており、ランサムウェアの検出を最新の状態に保つために、すべてのお客様に新しいパラメータを提供します。ARPの他のすべての検出、インサイト、およびデータ復旧ポイント機能は、ARP/AI用に維持されます。

ARP/AIを有効にするには"ONTAP One"、ライセンスが必要です。

詳細

- "ブログ：NetAppのAI-based real-time ransomware detection solution achieves AAA rating"

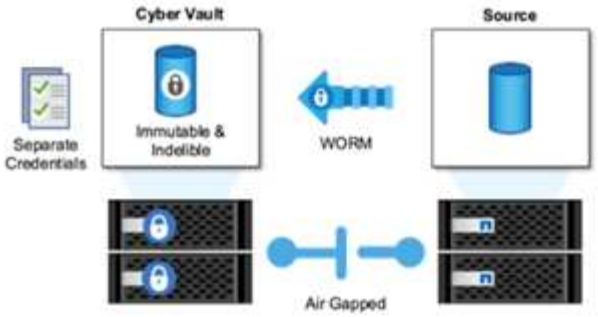
ONTAPでのサイバーヴォールティングによるエアギャップによる**WORM**保護

NetAppのサイバーボールトへのアプローチは、論理的にエアギャップを埋めるサイバーボールトのために構築されたリファレンスアーキテクチャです。このアプローチでは、SnapLockなどのセキュリティ強化テクノロジやコンプライアンステクノロジを活用して、変更や消去が不可能なSnapshotを作成できます。

SnapLock Complianceと論理的なエアギャップによるサイバーヴォールティング

攻撃者がバックアップコピーを破棄し、場合によっては暗号化する傾向が高まっています。そのため、サイバーセキュリティ業界の多くが、全体的なサイバーレジリエンス戦略の一環としてエアギャップバックアップを使用することを推奨しています。

問題は、従来のエアギャップ（テープとオフラインメディア）によってリストア時間が大幅に増加し、ダウンタイムと全体的な関連コストが増加することです。エアギャップソリューションに対するより現代的なアプローチでさえ、問題が発生する可能性があります。たとえば、新しいバックアップコピーを受信するためにバックアップヴォールトを一時的に開いてから、プライマリデータへのネットワーク接続を切断して閉じ、再び「エアギャップ」状態にすると、攻撃者はこの一時的なオープンを利用する可能性があります。接続がオンラインになっている間に、攻撃者がデータを侵害または破壊する可能性があります。このタイプの設定は、一般に不要な複雑さを追加します。論理的なエアギャップは、バックアップをオンラインに維持しながらセキュリティ保護の原則が同じであるため、従来のエアギャップや最新のエアギャップの代替として最適です。NetAppでは、変更不可のスナップショットとNetApp SnapLock Complianceを使用して、テープやディスクのエアギャップの複雑さを論理的なエアギャップで解決できます。



NetAppは、医療保険の携行性と責任に関する法律（HIPAA）、サーベンスオクスリー法、その他の規制データ規則など、データコンプライアンスの要件に対応するために、10年以上前にSnapLock機能をリリースしました。また、プライマリSnapshotをSnapLockボリュームにバックアップしてコピーをWORM状態にコミットし、削除を回避することもできます。SnapLockライセンスには、SnapLock ComplianceとSnapLock Enterpriseの2つのバージョンがあります。NetAppでは、ランサムウェア対策のためにSnapLock Complianceを推奨しています。ONTAP管理者やNetAppサポートがSnapshotをロックして削除できない特定の保持期間を設定できるためです。

詳細

- "ブログ：ONTAP cyber vault overview"

スナップショットの改ざん防止

SnapLock Complianceを論理的なエアギャップとして活用することで、攻撃者によるバックアップコピーの削除を防止できますが、SnapVaultを使用してSnapshotをセカンダリSnapLock対応ボリュームに移動する必要があります。そのため、多くのお客様がネットワーク経由でセカンダリストレージにこの構成を導入しています。これにより、プライマリストレージにプライマリボリュームのSnapshotをリストアするよりもリストア時間が長くなる可能性があります。

ONTAP 9.12.1以降では、改ざん防止スナップショットを使用して、プライマリストレージとプライマリボリュームのスナップショットをほぼSnapLock Complianceレベルで保護できます。SnapVaultを使用してSnapLockedのセカンダリボリュームにSnapshotをバックアップする必要はありません。改ざんを防止するSnapshotには、SnapLockテクノロジを使用して、ONTAPのフル管理者が同じSnapLock保持期限を使用していても、プライマリSnapshotが削除されないようにします。これにより、リストア時間が短縮され、改ざん防止されたSnapshotを使用してFlexCloneボリュームをバックアップできるようになります。これは、従来のSnapLock Complianceで保存されたSnapshotではできません。

SnapLock Compliance SnapLock Complianceスナップショットと改ざん防止スナップショットの主な違いは、保存されたスナップショットがまだ有効期限に達していない場合、SnapLock ComplianceではONTAPアレイの初期化と消去を実行できない点です。スナップショットの改ざんを防止するには、SnapLock Complianceライセンスが必要です。

詳細

- "Snapshotをロックしてランサムウェア攻撃から保護"

Digital Advisorによるランサムウェア対策

Active IQを基盤とするDigital Advisorは、NetAppストレージのプロアクティブなケアと最適化を、実用的なインテリジェンスによって簡素化し、最適なデータ管理を実現します。多様なインストールベースから得られるテレメトリデータを活用し、高度なAIとML

技術を駆使して、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を発見します。

> https://www.netapp.com/data-services/digital-advisor/["NetAppデジタルアドバイザ"^]は支援できるだけでなくhttps://www.netapp.com/blog/fix-security-vulnerabilities-with-active-iq/["セキュリティの脆弱性を排除"^]、ランサムウェア対策に特化した洞察やガイダンスも提供しています。専用のウェルネスカードには、必要な対策と対処すべきリスクが示されているため、システムがこれらのベストプラクティスの推奨事項を満たしていることを確認できます。

[Ransomware Defense Wellness]ページで追跡されるリスクとアクションには、次のものが含まれます（その他多数）。

- ボリュームのSnapshot数が少ないため、ランサムウェアによる保護の可能性が低下しています。
- NASプロトコル用に設定されたすべてのStorage Virtual Machine（SVM）でFPolicyが有効になっているわけではありません。

ランサムウェア対策の動作を確認するには、"Digital Advisor"を参照してください。

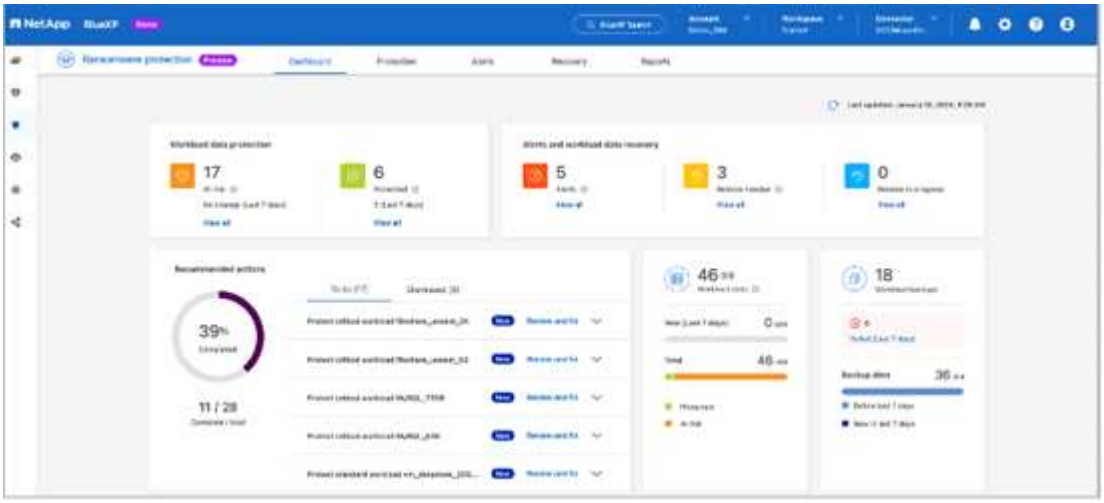
NetAppランサムウェア保護による包括的な回復力

ランサムウェアの検出は、拡散を防ぎ、コストのかかるダウンタイムを回避できるように、できるだけ早く実施することが重要です。しかし、ランサムウェアを効果的に検出するには、複数の保護レイヤが必要です。NetApp のランサムウェア保護は、NetApp Consoleを使用したデータ サービスにまで拡張されるリアルタイムのオンボックス機能と、サイバー ボールティング用の分離された階層化ソリューションを含む包括的なアプローチを採用しています。

NetAppランサムウェア保護

NetApp Consoleは、包括的かつワークロード中心のランサムウェア防御をインテリジェントにオーケストレーションする単一のコントロール プレーンです。 NetAppランサムウェア保護は、ARP、FPolicy、改ざん防止スナップショットなどのONTAPの強力なサイバーレジリエンス機能と、 NetApp Backup and Recoveryなどのデータ サービスを組み合わせています。自動化されたワークフローによる推奨事項やガイダンスも追加されており、単一のUIでエンドツーエンドの防御を実現します。ワークロード レベルで動作し、業務を支えるアプリケーションを保護して、攻撃が発生した場合に可能なかぎり迅速にリカバリを行えるようにしま

す。



お客様にもたらされるメリット：

- ランサムウェアへの備えを支援することで、運用上のオーバーヘッドを軽減し、効果を向上
- AI / MLを活用した異常検出により、高い精度と迅速な対応でリスクを抑制
- アプリケーションと整合性のあるガイド付きリストアにより、ワークロードを数分で簡単にリカバリできます。

"NetAppランサムウェア保護"これらの NIST 機能をより簡単に実現できます。

- アプリケーションベースの最上位のワークロードに重点を置いて、NetAppストレージ*内のデータを自動的に*検出*し、優先順位を付けます*。
- トップワークロードのデータバックアップ、不変で安全な構成、悪意のあるファイルブロッキング、さまざまなセキュリティドメインのワンクリック保護。
- 次世代の**AI**ベースの異常検出*を使用して、*ランサムウェアを*可能な限り*迅速に*正確に検出*します。
- 自動化された応答とワークフロー、およびトップ* SIEMおよびXDRソリューションとの統合*。
- シンプルな*オーケストレーションされたリカバリ*を使用してデータを迅速にリストアし、アプリケーションのアップタイムを短縮します。
- ランサムウェア対策*戦略と*ポリシー*を導入し、*成果を監視*します。

NetAppとゼロトラスト

NetAppとゼロトラスト

ゼロトラストは、従来、マイクロコアと境界（MCAP）を構築してデータ、サービス、アプリケーション、資産を保護するネットワーク中心のアプローチであり、セグメンテーションゲートウェイと呼ばれる制御機能を備えていました。NetApp ONTAPは、ゼロトラストに対してデータ主体のアプローチを採用しています。このアプローチでは、ストレージ管理システムが、お客様のデータへのアクセスを保護および監視するためのセグメンテーションゲートウェイになります。特に、FPolicyゼロトラストエンジンとFPolicyパートナーエコシステムは、正常なデータアクセスパターンと異常なデータア

クセスパターンを詳細に把握し、内部の脅威を特定するためのコントロールセンターとなります。

2024年7月より、以前はPDF形式で公開されていたテクニカルレポート『TR-4829：NetApp and Zero Trust：Enabling a data-centric Zero Trust model_』のコンテンツがdocs.netapp.comで公開されました。

データは、組織にとって最も重要な資産です。2022年の調査によると、データ侵害の18%は内部脅威が原因となっています "Verizon Data Breach Investigationsレポート"。組織は、NetApp ONTAPデータ管理ソフトウェアを使用して、データに対する業界最先端のゼロトラスト制御を導入することで、警戒を強化できます。

ゼロトラストとは

ゼロトラストモデルは、Forrester ResearchのJohn Kindervagによって最初に開発されました。外部からではなく内部からのネットワークセキュリティを想定しています。 Inside-Out Zero Trustアプローチは、マイクロコアと境界（MCAP）を特定します。MCAPは、包括的な制御セットで保護するデータ、サービス、アプリケーション、資産の内部定義です。安全な外部境界の概念は廃止されています。信頼され、境界を介して正常に認証されることが許可されているエンティティは、組織を攻撃に対して脆弱にする可能性があります。内部関係者は、定義上、すでに安全な境界内にいます。従業員、請負業者、およびパートナーは内部関係者であり、組織のインフラストラクチャ内で役割を実行するための適切な制御で運用できるようにする必要があります。

ゼロトラストは、2019年9月に国防総省に約束する技術として言及されました "FY19-23 DoDのデジタル最新化戦略"。Zero Trustは、「データ漏えいを阻止するためにアーキテクチャ全体にセキュリティを組み込むサイバーセキュリティ戦略です。このデータ中心のセキュリティモデルは、信頼できるネットワーク、デバイス、ペルソナ、またはプロセスという概念を排除し、最小特権アクセスの概念の下で認証および承認ポリシーを可能にするマルチ属性ベースの信頼レベルに移行します。ゼロトラストを実装するには、既存のインフラストラクチャを使用して、よりシンプルで効率的な方法でセキュリティを実装する方法を再考する必要があります。

2020年8月、NISTは(ZTA)を発表しまし "Special Pub 800-207ゼロトラストアーキテクチャ" た。ZTAは、ネットワークセグメントではなくリソースの保護に重点を置いています。これは、ネットワークの場所がリソースのセキュリティ体制の主要なコンポーネントではなくなったためです。リソースとはデータとコンピューティングです。ZTA戦略は、エンタープライズネットワークアーキテクト向けです。ZTAでは、元のForresterの概念から新しい用語がいくつか導入されています。ポリシー決定ポイント（PDP）およびポリシー施行ポイント（PEP）と呼ばれる保護メカニズムは、Forresterセグメンテーションゲートウェイに似ています。ZTAでは、次の4つの導入モデルを導入

- デバイスエージェントまたはゲートウェイベースの展開
- Enclaveベースの導入（Forrester MCAPに似ています）
- リソースポータルベースの導入
- デバイスアプリケーションのサンドボックス化

このドキュメントの目的のために、NIST ZTAではなくForrester Researchの概念と用語を使用しています。

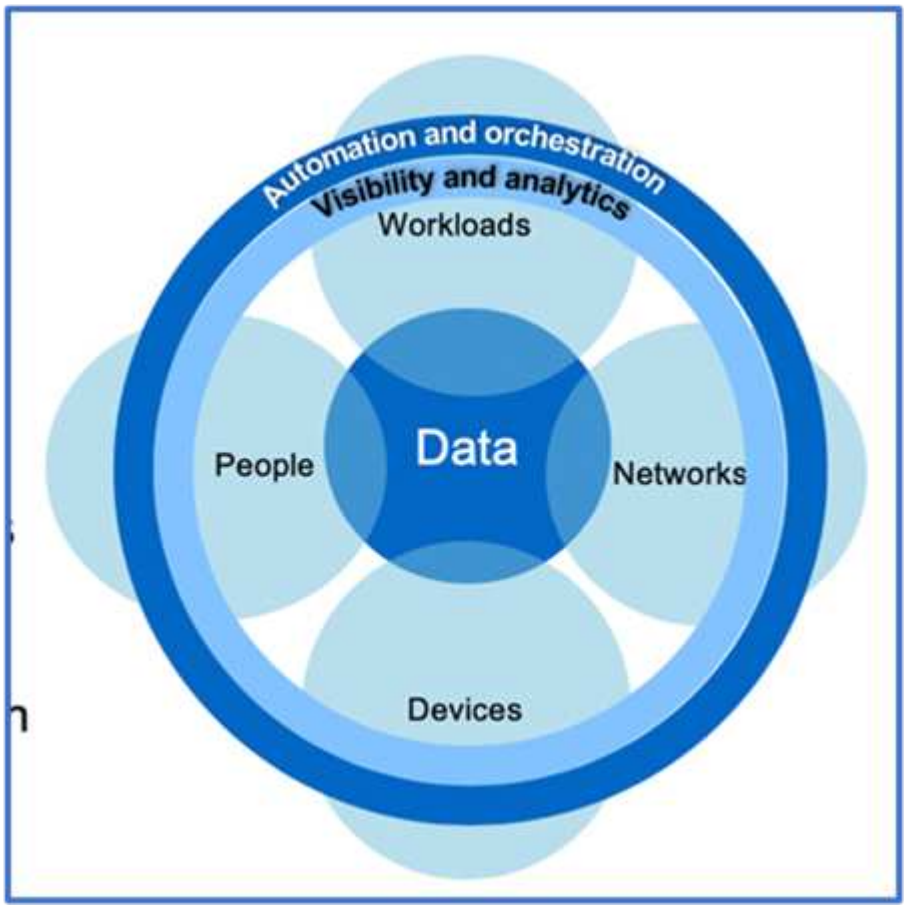
セキュリティリソース

脆弱性とインシデントの報告、NetAppのセキュリティ対応、および顧客の機密性の詳細については、を参照してください "NetAppセキュリティポータル"。

ONTAPでデータ主体のアプローチでゼロトラストを実現

ゼロトラストネットワークは、データ中心のアプローチによって定義され、セキュリティ制御は可能な限りデータに近いものにする必要があります。ONTAPの機能とNetApp FPolicyパートナーエコシステムを組み合わせることで、データ中心のゼロトラストモデルに必要な制御を提供できます。

ONTAPは、NetAppが提供するセキュリティリッチなデータ管理ソフトウェアです。FPolicyゼロトラストエンジンは業界をリードするONTAP機能で、きめ細かなファイルベースのイベント通知インターフェイスを提供します。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。



ゼロトラストのデータ主体の**MCAP**を設計

データ中心のゼロトラストMCAPを設計するには、次の手順を実行します。

1. すべての組織データの場所を特定します。
2. データを分類
3. 不要になったデータを安全に破棄できます。
4. データ分類へのアクセス権を持つ役割を理解する。
5. 最小権限の原則を適用して、アクセス制御を適用します。
6. 管理アクセスとデータアクセスに多要素認証を使用します。

7. 保存中のデータと転送中のデータに暗号化を使用
8. すべてのアクセスを監視してログに記録します。
9. 不審なアクセスまたは動作を警告します。

すべての組織データの場所を特定する

ONTAPのFPolicy機能とパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザーの行動分析の詳細については、「すべてのアクセスを監視してログに記録する」を参照してください。データがどこにあり、誰がデータにアクセスできるかを理解していない場合、ユーザー行動分析は、経験的観察から分類とポリシーを構築するためのベースラインを提供できます。

データを分類

ゼロトラストモデルの用語では、データの分類には有害なデータの特定が含まれます。有害データとは、組織外に公開することを意図していない機密データのことです。有害データの開示は、規制遵守に違反し、組織の評判を損なう可能性があります。規制遵守の観点から、有害データにはカード所有者データ "クレジットカード業界の データ セキュリティ 標準 (PCI-DSS)"、EU向けの個人データ "一般データ保護規則（GDPR）"、または医療データ "医療保険の携行性と責任に関する法律（HIPAA）"が含まれます。AIを活用したツールキットであるNetApp "NetApp Data Classification"（旧称：Cloud Data Sense）を使用して、データを自動的にスキャン、分析、分類することができます。

不要になったデータを安全に廃棄

組織のデータを分類した後、一部のデータが不要になったり、組織の機能と関連性がなくなったりすることがあります。不要なデータの保持は責任であり、そのようなデータは削除する必要があります。暗号化によってデータを消去する高度なメカニズムについては、「保存データの暗号化」でのセキュアパージの説明を参照してください。

データ分類へのアクセス権が必要な役割を理解し、アクセス制御を実施するために最小権限の原則を適用する

機密データへのアクセスをマッピングし、最小権限の原則を適用すると、組織内のユーザーに、業務の遂行に必要なデータのみにアクセスできるようになります。このプロセスにはロールベースアクセス制御が含まれ("RBAC"ます）。これは、データアクセスと管理アクセスに適用されます。

ONTAPでは、Storage Virtual Machine（SVM）を使用して、ONTAPクラスタ内のテナントによる組織のデータアクセスを分割できます。RBACは、SVMへのデータアクセスと管理アクセスに適用できます。RBACはクラスタ管理レベルでも適用できます。

RBACに加えて、ONTAP（MAV）を使用して、またはなどのコマンドの承認を1人以上の管理者に要求することができます "マルチ管理者認証" `volume delete` `volume snapshot delete`。MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

スナップショットを保護するもう1つの方法は、ONTAP"Snapshotロック"です。Snapshotロックは、ボリュームSnapshotポリシーの保持期間に応じて手動または自動でSnapshotを消去できないようにするSnapLock機能です。スナップショットロックは、改ざん防止スナップショットロックとも呼ばれます。スナップショットロックの目的は、不正な管理者や信頼されていない管理者が、プライマリおよびセカンダリONTAPシステム上のスナップショットを削除するのを防ぐことです。ランサムウェアによって破損したボリュームをリストアするために、プライマリシステム上のロックされたSnapshotの迅速なリカバリを実現できます。

管理アクセスとデータアクセスに多要素認証を使用

クラスター管理RBACに加えて、https://www.netapp.com/pdf.html?item=/media/17055-tr4647.pdf["多要素認証（MFA）"^]はONTAPのWebアクセスおよびSecure Shell（SSH）コマンドラインアクセスに展開できます。管理アクセスにおけるMFAは、米国の公共機関、またはPCI-DSSに準拠する必要のある組織にとって必須要件です。MFAにより、攻撃者はユーザー名とパスワードのみを使用してアカウントを侵害することが不可能になります。MFAでは、認証に2つ以上の独立した要素が必要です。二要素認証の例としては、ユーザーが所有するもの（秘密鍵など）と、ユーザーが知っているもの（パスワードなど）を組み合わせる方法があります。ONTAP System ManagerまたはActive IQ Unified Managerへの管理Webアクセスは、Security Assertion Markup Language（SAML）2.0によって有効化されます。SSHコマンドラインアクセスでは、公開鍵とパスワードを用いた連鎖型二要素認証が使用されます。

ONTAPのIDおよびアクセス管理機能を使用して、APIを使用してユーザおよびマシンのアクセスを制御できます。

- ユーザ：
  - *認証と承認。*SMBとNFSのNASプロトコル機能を介して提供
  - *監査。*アクセスおよびイベントのsyslog。認証ポリシーと許可ポリシーをテストするためのCIFSプロトコルの詳細な監査ログ。詳細なNASアクセスをファイルレベルできめ細かくFPolicyで監査
- デバイス：
  - *認証。*APIアクセス用の証明書ベースの認証。
  - *承認。*デフォルトまたはカスタムのRole-Based Access Control（RBAC；ロールベースアクセス制御）。
  - *監査。*実行されたすべてのアクションのsyslog。

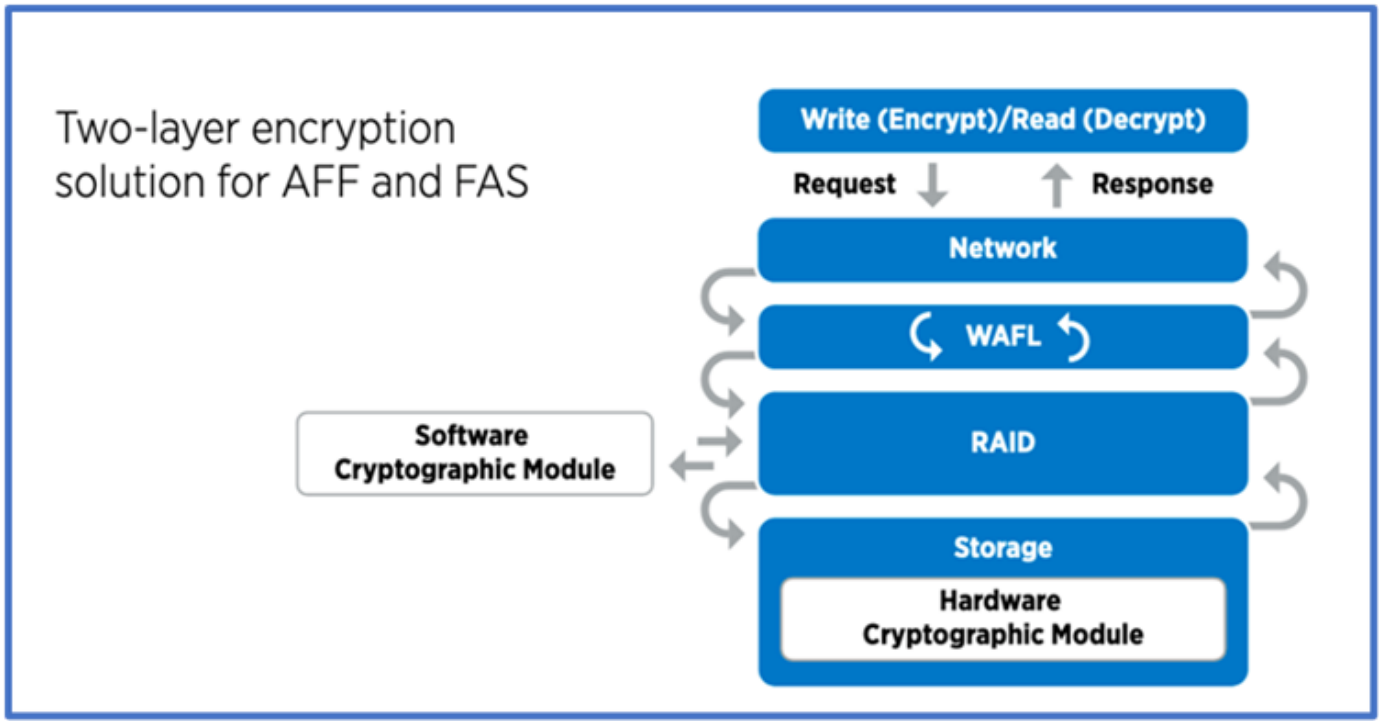
保存中のデータと転送中のデータに暗号化を使用

保存データ暗号化

組織がドライブを再利用したり、不良ドライブを返品したり、売却や下取りによってより大容量のドライブにアップグレードしたりする際には、ストレージシステムのリスクやインフラストラクチャのギャップを軽減するための新たな要件が日々発生します。ストレージエンジニアは、データの管理者および運用者として、データのライフサイクル全体を通してデータを安全に管理・維持することが求められます。 "NetAppストレージ暗号化（NSE）；NetAppボリューム暗号化（NVE）；およびNetAppアグリゲート暗号化"有害なデータであろうとなかろうと、保存されているすべてのデータを常に暗号化し、日常業務に影響を与えることなく、データ保護を支援します。 "NSE"はONTAPハードウェア"保存データ"FIPS 140-2レベル2認証済みの自己暗号化ドライブを利用した暗号化ソリューションです。 "NVE および NAE"はONTAPソフトウェア"保存データ" "FIPS 140-2レベル1認定NetApp暗号モジュール"を活用した暗号化ソリューションです。NVEとNAEでは、ハードディスクドライブまたはソリッドステートドライブのどちらでも、保存データの暗号化に使用できます。さらに、NSEドライブを使用することで、暗号化の冗長性と追加のセキュリティを提供するネイティブの階層型暗号化ソリューションを実現できます。1つの層が侵害されても、2つ目の層がデータを引き続き保護します。これらの機能により、ONTAPは "Quantum対応の暗号化"に適した位置づけとなっています。

NVEには、機密ファイルが分類されていないボリュームに書き込まれたときに、暗号化によってデータ流出から有害なデータを削除するという機能もあります。 "セキュアパージ"

ONTAPに組み込まれているキー管理ツールであるを "オンボードキーマネージャ（ OKM ）"使用するか、 "承認済み" またはサードパーティ製品 "カイフキカンリツル" をNSEおよびNVEと併用して、キー情報をセキュアに格納できます。



上の図に示すように、ハードウェアベースとソフトウェアベースの暗号化を組み合わせることができます。この機能により、ではトップシークレットデータの保存が可能になり "分類されたプログラムのためのNSAの商用ソリューションへのONTAPの検証" ました。

転送中データの暗号化

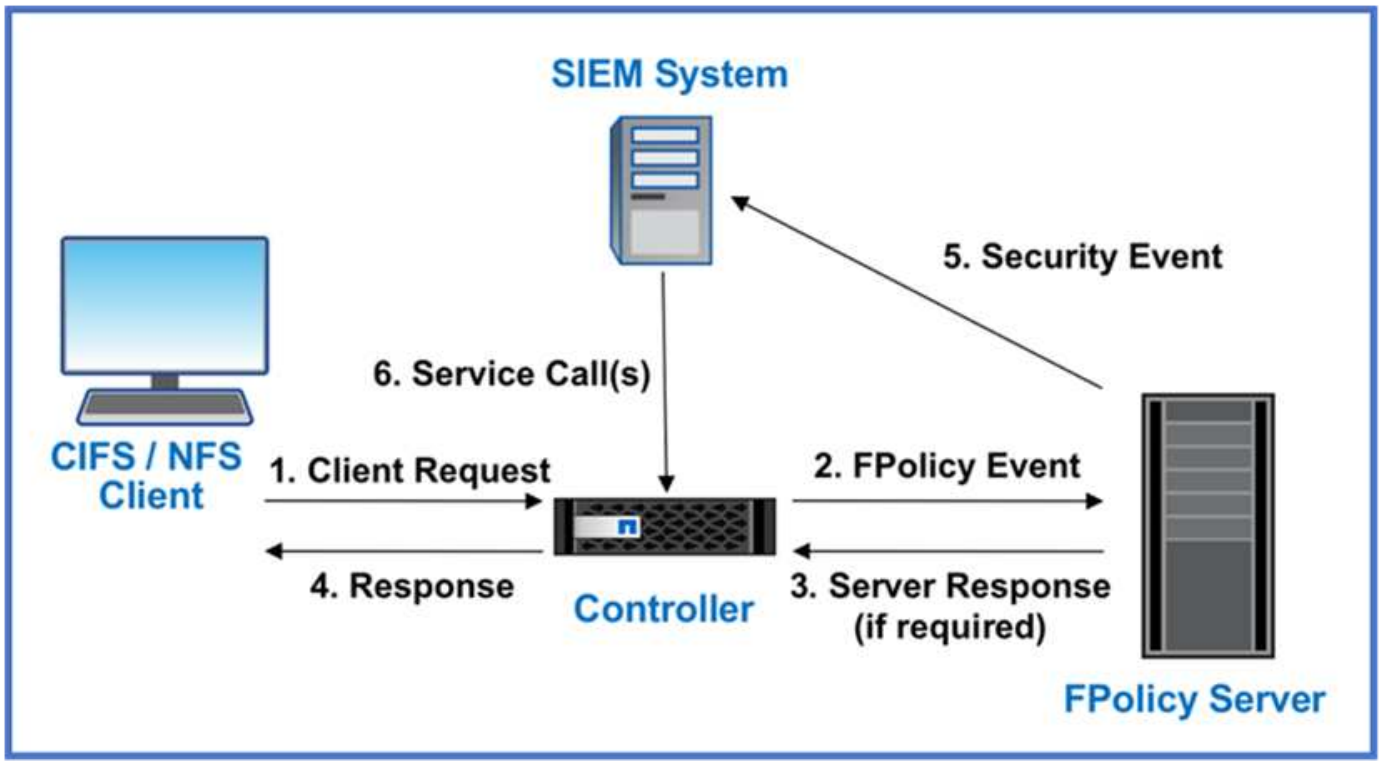
ONTAPの転送中データ暗号化により、ユーザデータアクセスとコントロールプレーンアクセスが保護されます。ユーザデータアクセスは、Microsoft CIFS共有アクセスの場合はSMB 3.0暗号化、NFS Kerberos 5の場合はkrb5pによって暗号化できます。ユーザデータアクセスは、を使用してCIFS、NFS、iSCSIの暗号化することもできます "IPSec" 。コントロールプレーンアクセスは、Transport Layer Security（TLS）で暗号化されます。ONTAPには、コントロールプレーンアクセスのコンプライアンスモードが用意されて"FIPS"います。このモードでは、FIPS承認のアルゴリズムが有効になり、FIPS承認でないアルゴリズムが無効になります。データレプリケーションはで暗号化され "クラスタピア暗号化"ます。これにより、ONTAP SnapVaultテクノロジとSnapMirrorテクノロジが暗号化されます。

すべてのアクセスを監視してログに記録

RBACポリシーを設定したら、アクティブな監視、監査、アラートを導入する必要があります。NetApp ONTAPのFPolicyゼロトラストエンジンとを組み合わせること "NetApp FPolicyパートナーエコシステム"で、データ主体のゼロトラストモデルに必要な制御を実現できます。NetApp ONTAPは、セキュリティが充実したデータ管理ソフトウェアであり "FPolicy" 、きめ細かなファイルベースのイベント通知インターフェイスを提供する、業界をリードするONTAP機能です。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。ONTAPのFPolicy機能とFPolicyパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザの行動分析を使用すると、通常のパターンから外れた不審なデータアクセスや異常なデータアクセスをアラートで通知し、必要に応じてアクセスを拒否するアクションを実行できます。

FPolicyパートナーは、ユーザ行動分析にとどまらず、機械学習（ML）や人工知能（AI）に移行しつつあります。これにより、イベントの忠実度が向上し、誤検出があった場合にはそれを減らすことができます。すべてのイベントは、syslogサーバ、またはMLやAIを使用できるセキュリティ情報イベント管理（SIEM）システム

に記録する必要があります。



NetAppの "DII ストレージ ワークロード セキュリティ"クラウドとオンプレミスの両方のONTAPストレージ システムで FPolicy インターフェイスとユーザー行動分析を利用して、悪意のあるユーザー行動に関するリアルタイムのアラートを提供します。また、高度な機械学習と異常検出機能により、悪意のあるユーザやセキュリティ侵害を受けたユーザが組織のデータを不正利用できないよう保護します。ストレージ ワークロード セキュリティは、ランサムウェア攻撃やその他の不正行為を識別し、スナップショットを呼び出して悪意のあるユーザーを隔離できます。また、フォレンジック機能により、ユーザとエンティティのアクティビティを詳細に把握できます。ストレージ ワークロード セキュリティは、 NetApp Data Infrastructure Insightsの一部です。

ONTAPには、ストレージワークロードのセキュリティに加えて、（ARP）と呼ばれるランサムウェア検出機能が搭載され "自律型ランサムウェア対策" ています。ARPは機械学習を使用して、ランサムウェア攻撃が進行中であることを示す異常なファイルアクティビティがないかどうかを判断し、スナップショットを呼び出して管理者にアラートを送信します。Storage Workload Securityは、ONTAPと統合してARPイベントを受信し、追加の分析機能と自動応答レイヤを提供します。

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ONTAPの外部にあるNetAppセキュリティの自動化とオーケストレーションの制御

自動化を使用すると、最小限の人間の支援でプロセスや手順を実行できます。自動化により、組織はゼロトラスト環境を手動の手順をはるかに超えて拡張し、自動化された不正なアクティビティから保護できます。

Ansibleは、オープンソースのソフトウェアプロビジョニング、構成管理、およびアプリケーション展開ツールです。このソフトウェアは多くのUnix系システムで動作し、Unix系システムとMicrosoft Windowsの両方を構成できます。システム構成を記述するための独自の宣言型言語が含まれています。AnsibleはMichael DeHaanによって開発され、2015年にRed Hatに買収されました。Ansibleはエージェントレスでありまたはwindows Remote Management（リモートのPowerShell実行を可能にする）を介して一時的にリモート接続

し、タスクを実行します。NetAppは "ONTAPソフトウェア向け150個のAnsibleモジュール"以上を開発しており、Ansible自動化フレームワークとのさらなる統合を実現しています。NetApp向けAnsibleモジュールは、望ましい状態を定義してターゲットのNetApp環境に伝達する方法に関する一連の手順を提供します。モジュールは、ライセンスの設定、アグリゲートやストレージ仮想マシンの作成、ボリュームの作成、スナップショットの復元など、さまざまなタスクをサポートするように構築されています。Ansibleロールは "GitHubで公開"、NetApp DoD Unified Capabilities （UC） Deployment Guideに特化して作成されています。

利用可能なモジュールのライブラリを使用することで、Ansibleプレイブックを簡単に開発し、独自のアプリケーションやビジネスニーズに合わせてカスタマイズして、日常的なタスクを自動化できます。作成したプレイブックを実行して指定したタスクを実行することで、時間を節約し、生産性を向上させることができます。NetAppでは、サンプルのプレイブックを作成して共有しています。プレイブックは直接使用することも、ニーズに合わせてカスタマイズすることもできます。

Data Infrastructure Insightsは、インフラストラクチャ全体の可視性を提供するインフラストラクチャ監視ツールです。 Data Infrastructure Insightsを使用すると、パブリック クラウド インスタンスやプライベート データ センターを含むすべてのリソースを監視、トラブルシューティング、最適化できます。 Data Infrastructure Insights を使用すると、平均解決時間を 90% 短縮し、クラウドの問題の 80% がエンド ユーザーに影響を与えるのを防ぐことができます。クラウド インフラのコストを平均で33%削減可能なほか、実用的なインテリジェンスによりデータを保護し、内部の脅威に対するリスクも軽減できます。 Data Infrastructure Insightsのストレージ ワークロード セキュリティ機能により、AI と ML を使用したユーザー行動分析が可能になり、内部脅威によって異常なユーザー行動が発生したときに警告を発することができます。ONTAPの場合、Storage Workload SecurityではゼロトラストFPolicyエンジンを使用します。

ゼロトラストとハイブリッドクラウド環境

NetAppは、ハイブリッド クラウドのデータに関するオーソリティです。NetAppは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud、その他の主要なクラウド プロバイダーを使用して、オンプレミスのデータ管理システムをハイブリッド クラウドに拡張するためのさまざまなオプションを提供しています。NetAppのハイブリッド クラウド ソリューションは、オンプレミスのONTAPシステムおよびONTAP Select Software-Defined Storageで採用されているものと同じゼロ トラスト セキュリティ対策に対応しています。

AWS (FSxN)、Google Cloud (GCNV)、および Microsoft Azure 向けAzure NetApp Files向けのエンタープライズ クラスのクラウドネイティブ ファイル サービスを使用することで、一般的な CAPEX 制約なしにパブリック クラウドの容量を簡単に拡張できます。これらは分析やDevOpsなど、データを大量に使用するワークロードに最適なクラウド データ サービスであり、NetAppの柔軟性のあるオンデマンド ストレージ サービスと、ONTAPデータ管理機能をフルマネージド形式で組み合わせて利用できます。

ONTAP は、 NetApp SnapMirrorデータ レプリケーション ソフトウェアを使用して、オンプレミスのONTAPシステムと AWS、Google Cloud、または Azure ストレージ環境間でデータを移動できるようにします。

属性ベースのアクセス制御

ONTAPによる属性ベースのアクセス制御

9.12.1以降では、NFSv4.2セキュリティラベルおよび拡張属性（xattrs）を使用してONTAPを設定し、属性および属性ベースアクセス制御（ABAC）を使用したロールベースアクセス制御（RBAC）をサポートできます。

ABACは、ユーザ属性、リソース属性、および環境条件に基づいて権限を定義する認可戦略です。ONTAPとNFS v4.2セキュリティラベルおよびxattrsの統合は、NIST Special Publication 800-162に規定されているABACソリューションのNIST標準に準拠しています。

NFS v4.2セキュリティラベルとxattrsを使用して、ファイルにユーザ定義の属性とラベルを割り当てることができます。ONTAPは、ABAC指向のIDおよびアクセス管理ソフトウェアと統合して、これらの属性とラベルに基づいてきめ細かなファイルおよびフォルダのアクセス制御ポリシーを適用できます。

関連情報

- "ONTAPを使用したABACへのアプローチ"
- "NetApp ONTAPのNFS：ベストプラクティスおよび実装ガイド"

ONTAPでの属性ベースアクセス制御（ABAC）のアプローチ

ONTAPには、NFS v4.2セキュリティラベルやNFSを使用した拡張属性（xattrs）など、ファイルレベルの属性ベースアクセス制御（ABAC）を実現するために使用できるいくつかのアプローチが用意されています。

NFS v4.2セキュリティラベル

ONTAP 9.9.1以降では、NFS v4.2の「ラベル付きNFS」機能がサポートされます。

NFS v4.2セキュリティラベルは、SELinuxラベルとMandatory Access Control（MAC；強制アクセス制御）を使用して、ファイルやフォルダへのきめ細かなアクセスを管理する方法です。これらのMACラベルはファイルとフォルダに格納され、UNIX権限およびNFS v4.x ACLと連携して機能します。

NFS v4.2セキュリティラベルがサポートされたことで、ONTAPはNFSクライアントのSELinuxラベル設定を認識して認識できるようになりました。NFS v4.2セキュリティラベルはRFC-7204で規定されています。

NFS v4.2セキュリティラベルのユースケースには、次のようなものがあります。

- 仮想マシン（VM）イメージのMACラベル付け
- 公共機関のデータセキュリティ分類（シークレット、トップシークレット、その他の分類）
- セキュリティコンプライアンス
- ディスクレス Linux

NFS v4.2セキュリティラベルを有効にする

NFS v4.2セキュリティラベルを有効または無効にするには、次のコマンドを使用します（advanced権限が必要）。

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

の詳細については `vserver nfs modify`、を"ONTAPコマンド リファレンス"参照してください。

NFS v4.2セキュリティラベルの適用モード

ONTAP 9.9.1以降では、ONTAPで次の強制モードがサポートされています。

- 制限付きサーバーモード：ONTAPはラベルを強制できませんが、ラベルを保存および送信できます。

  MACラベルを変更する機能は、強制するクライアントによって異なります。

- ゲストモード：クライアントにNFS対応（v4.1以前）のラベルが付けられていない場合、MACラベルは送信されません。

  ONTAPは現在、フルモード（MACラベルの保存と適用）をサポートしていません。

NFS v4.2セキュリティラベルの例

次の設定例は、Red Hat Enterprise Linuxリリース9.3（Plow）を使用した概念を示しています。

このユーザ `jrsmith`は、John R. Smithのクレデンシャルに基づいて作成され、次のアカウントPrivilegesを持ちます。

- ユーザ名= `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

ロールには2つあります。管理者アカウントは、次のMLS Privilegesの表で説明されているように、特権ユーザおよびユーザ `jrsmith`です。

ユーザ	ロール	タイプ	レベル
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

この例の環境では、ユーザー `jrsmith`はに `s3`あるレベルのファイルにアクセスできます `s0`。以下に概説する既存のセキュリティ分類を強化して、管理者がユーザー固有のデータにアクセスできないようにすることができます。

- S0 =権限管理者ユーザデータ
- S0 =未分類データ
- S1 =社外秘
- S2 =シークレットデータ
- S3 =トップシークレットデータ

MCSヲシヨウシタNFS v4.2セキュリティラベルノレイ

マルチレベルセキュリティ（MLS）に加えて、マルチカテゴリセキュリティ（MCS）と呼ばれる別の機能を使用すると、プロジェクトなどのカテゴリを定義できます。

NFSセキュリティラベル	値
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

拡張属性（**xattrs**）

ONTAP 9.12.1以降では、ONTAPはxattrs.xattrsをサポートしています。xattrsを使用すると、アクセス制御リスト(ACL)やユーザ定義属性など、システムによって提供されるもの以外のファイルやディレクトリにメタデータを関連付けることができます。

xattrsを実装するには、Linuxでと `getfattr`コマンドラインユーティリティを使用できます `setfattr`。これらのツールを使用すると、ファイルやディレクトリの追加メタデータを強力に管理できます。不適切な使用は予期しない動作やセキュリティ上の問題につながる可能性があるため、注意して使用する必要があります。使用方法の詳細については、および `getfattr`のマニュアルページを参照するか、信頼性の高いその他のドキュメントを参照して `setfattr`ください。

ONTAPファイルシステムでxattrsが有効になっている場合'ユーザーはファイルの任意の属性を設定'変更'取得できますこれらの属性は、アクセス制御情報など、標準のファイル属性セットではキャプチャされないファイルに関する追加情報を格納するために使用できます。

ONTAPでxattrsを使用するには、いくつかの要件と制限があります。

- Red Hat Enterprise Linux 8.4以降
- Ubuntu 22.04以降
- 各ファイルには最大128個のxattrsを含めることができます。
- xattrキーは255バイトに制限されています
- キーまたは値の合計サイズは'xattrごとに1,729バイトです
- ディレクトリとファイルはxattrsを持つことができる
- xattrsを設定および取得するには、ユーザおよびグループに対して書き込みモードビットが有効になっている必要があります。 `w`

Xattrsはユーザーネームスペース内で使用され、ONTAP自体に本質的な意味を持たない。代わりに、それらの実用的なアプリケーションは、ファイルシステムとやり取りするクライアント側のアプリケーションによって排他的に決定され、管理されます。

xattrの使用例：

- ファイルの作成を担当するアプリケーションの名前の記録
- ファイルの取得元の電子メールメッセージへの参照の維持
- ファイルオブジェクトを整理するための分類フレームワークの確立
- 元のダウンロード元のURLを使用したファイルのラベル付け

xattrsの管理用コマンド

- `setfattr`ファイルまたはディレクトリの拡張属性を設定します。

```
setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
```

コマンド例：

```
setfattr -n user.comment -v test example.txt
```

- `getfattr`特定の拡張属性の値を取得するか、ファイルまたはディレクトリのすべての拡張属性を一覧表示します。

  特定の属性：
  `getfattr -n <attribute_name> <file or directory name>`

  すべての属性：
  `getfattr <file or directory name>`

  コマンド例：

```
getfattr -n user.comment example.txt
```

xattrキーと値のペアの例

次の表に、2つのxattrキー値ペアの例を示します。

xattr	値
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

xattrsのACEを使用したユーザー権限

Access Control Entry（ACE；アクセス制御エントリ）は、ファイルやディレクトリなどの特定のリソースに対して個 々 のユーザまたはユーザグループに付与されるアクセス権または権限を定義するACL内のコンポーネントです。各ACEは、許可または拒否されるアクセスのタイプを指定し、特定のセキュリティプリンシパル（ユーザまたはグループのID）に関連付けます。

xattrsに必要なアクセス制御エントリ（ACE）

- Retrieve xattr：ユーザがファイルまたはディレクトリの拡張属性を読み取るために必要な権限。「R」は、読み取り権限が必要であることを示します。
- set xattrs：拡張属性を変更または設定するために必要な権限。"A"、"w"、"T"は、append、write、xattrsに関連する特定のパーミッションなど、パーミッションの異なる例を表しています。
- ファイル:拡張属性を設定するには、追加、書き込み、およびxattrsに関連する特別な権限が必要です。
- ディレクトリ:拡張属性を設定するには、特定の権限「T」が必要です。

ファイルタイプ	**xattr**の取得	**xattrs**の設定
ファイル	R	A、w、T
ディレクトリ	R	T

ABAC IDおよびアクセス制御ソフトウェアとの統合

ABACの機能を最大限に活用するために、ONTAPはABAC指向のIDおよびアクセス管理ソフトウェアと統合できます。

ABACシステムでは、Policy Enforcement Point (PEP)とPolicy Decision Point (PDP)が重要な役割を果たす。PEPはアクセス制御ポリシーの適用を担当し、PDPはポリシーに基づいてアクセスを許可するか拒否するかを決定します。

実際的な設定では、NFSセキュリティラベルとxattrsを組み合わせて使用します。これらは、分類、セキュリティ、アプリケーション、コンテンツなど、さまざまなメタデータを表すために使用されます。これらはすべてABACの決定を行うのに役立ちます。xattrsは、PDPが意思決定プロセスに使用するリソース属性を格納するために使用できます。属性は、ファイルの分類レベルを表すように定義できます（「未分類」、「機密」、「シークレット」、「トップシークレット」など）。その後、PDPはこの属性を使用して、ユーザーがクリアランスレベル以下の分類レベルを持つファイルのみにアクセスするように制限するポリシーを適用できます。

> このコンテンツでは、お客様のID、認証、およびアクセスサービスに、ファイルシステムへのアクセスの仲介者として機能するPEPおよびPDPが少なくとも1つ含まれていることを前提としています。

ABACのプロセスフローの例

1. ユーザは、PEPへのシステムアクセスにクレデンシャル（PKI、OAuth、SAMLなど）を提示し、PDPから結果を取得します。

   PEPの役割は、ユーザのアクセス要求を代行受信してPDPに転送することです。

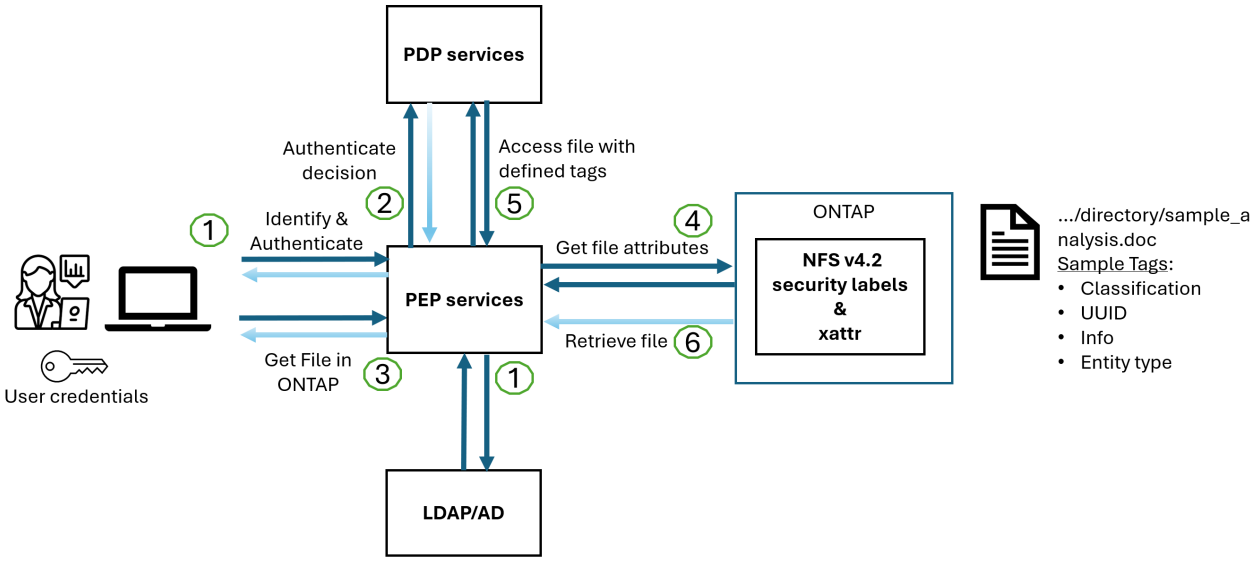
2. PDPは、確立されたABACポリシーに照らしてこの要求を評価します。

   これらのポリシーでは、ユーザー、問題のリソース、および周囲の環境に関連するさまざまな属性が考慮されます。これらのポリシーに基づいて、PDPはアクセスを許可するか拒否するかを決定し、その決定をPEPに伝えます。

   PDPはPEPにポリシーを提供して実施します。PEPはこの決定を実行し、PDPの決定に従ってユーザーのアクセス要求を許可または拒否します。

3. 要求が成功すると、ユーザはONTAPに格納されているファイル（AFF、AFF -Cなど）を要求します。
4. 要求が成功すると、PEPはドキュメントから詳細なアクセス制御タグを取得します。
5. PEPは、そのユーザの証明書に基づいてユーザのポリシーを要求します。
6. ユーザがファイルにアクセスできる場合、PEPはポリシーとタグに基づいて決定を行い、ユーザがファイルを取得できるようにします。

> 実際のアクセスはトークンを使用して行われる場合があります。



ONTAPクローニングと**SnapMirror**

ONTAPのクローニングおよびSnapMirrorテクノロジは、効率的で信頼性の高いデータレプリケーションおよびクローニング機能を提供するように設計されています。xattrsは、ファイルに関連付けられた追加のメタデータ（セキュリティラベル、アクセス制御情報、ユーザ定義データなど）を保存するため、ファイルのコンテキストと整合性の維持に不可欠です。xattrsは重要です。

ONTAPのFlexCloneテクノロジを使用してボリュームをクローニングすると、ボリュームの完全な書き込み可能なレプリカが作成されます。このクローニングプロセスは瞬時に実行されるスペース効率に優れており、すべてのファイルデータとメタデータが含まれているため、xattrsを完全にレプリケートできます。同様に、SnapMirrorでは、データが完全に忠実にセカンダリシステムにミラーリングされます。これにはxattrsも含まれます。xattrsは、このメタデータに依存するアプリケーションが正しく機能するために非常に重要です。

NetApp ONTAPでは、クローニング処理とレプリケーション処理の両方にxattrsを含めることで、プライマリストレージシステムとセカンダリストレージシステム全体で、すべての特性を含む完全なデータセットを使用して一貫性を確保します。この包括的なデータ管理アプローチは、一貫したデータ保護、迅速なリカバリ、コンプライアンスと規制基準への準拠を必要とする組織にとって不可欠です。また、オンプレミスでもクラウドでも、さまざまな環境にわたってデータの管理が簡易化されるため、ユーザはプロセス中もデータが完全で変更されていないという安心感を得ることができます。

NFS v4.2セキュリティラベルには、に定義された注意事項NFS v4.2セキュリティラベルがあります。

ラベルに対する変更の監査

xattrsまたはNFSセキュリティラベルに対する変更の監査は、ファイルシステムの管理とセキュリティの重要な側面です。標準のファイルシステム監査ツールを使用すると、xattrsやセキュリティラベルの変更など、ファイルシステムに対するすべての変更を監視およびロギングできます。

Linux環境では、 `auditd`ファイルシステムイベントの監査を確立するために一般にデーモンが使用されます。管理者は、`xattr`の変更（、 `lsetxattr`など）に関連する特定のシステムコールを監視し、 `fsetxattr`属性と、 `lremovexattr`fremovexattr`の設定、および`removexattr`属性の削除を監視するルールを設定でき`setxattr`ます。

ONTAP FPolicyは、ファイル操作をリアルタイムで監視および制御するための堅牢なフレームワークを提供することで、これらの機能を拡張します。FPolicyは、さまざまな属性xattrイベントをサポートするように設定できます。これにより、ファイル操作をきめ細かく制御したり、包括的なデータ管理ポリシーを適用したりできます。

xattrsを使用するユーザ、特にNFS v3およびNFS v4環境では、監視対象としてサポートされるファイル操作とフィルタの特定の組み合わせのみが対象となります。FPolicyによるNFS v3およびNFS v4のファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを次に示します。

サポートされているファイル操作	サポートされているフィルタ
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

属性設定操作の**auditd**ログスニペットの例：

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

ユーザがxattrsを使用できるようにする"ONTAP FPolicy"と、ファイルシステムの整合性とセキュリティを維持するために不可欠な可視性と制御のレイヤが提供されます。FPolicyの高度な監視機能を活用することで、組織はxattrsに対するすべての変更を追跡、監査し、セキュリティおよびコンプライアンス基準に準拠させることができます。ファイルシステム管理に対するこのプロアクティブなアプローチが、データガバナンスと保護戦略を強化したいと考えている組織にとって、ONTAP FPolicyを有効にすることが強く推奨される理由です。

データアクセスの制御例

John R. SmithのPKI証明書に格納されているデータの次のエントリ例は、NetAppのアプローチをファイルに適用し、きめ細かなアクセス制御を提供する方法を示しています。

これらの例は説明を目的としたものであり、NFS v4.2セキュリティラベルおよびxattrsに関連付けられているメタデータはお客様の責任で確認してください。わかりやすいように更新とラベルの保持の詳細は省略しています。

- PKI証明書値の例*

キー	値
entitySecurityMark	T：S01 =未分類

情報	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

仕様	"DoD"
UUID	b4111349-7875-4115-AD30-0928565f2e15

管理組織	{
	"value": "DoD"
	}

キー	値

ブリーフィング	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

市民権ステータス	{
	"value": "US"
	}

クリアランス	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

加盟国	[
	{
	"value": "USA"
	}
	]

キー	値

デジタル識別子	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

転送先	<pre>{
	  "value": "DoD"
	}</pre>

DutyOrganization	<pre>{
	  "value": "DoD"
	}</pre>

エンティティタイプ	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControls	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

これらのPKIエンタイトルメントには、データ型やアトリビューションによるアクセスなど、John R. Smithのアクセスの詳細が表示されます。

IC-TDFメタデータがファイルとは別に格納されているシナリオでは、NetAppは詳細なアクセス制御レイヤを追加することを推奨しています。これには、アクセス制御情報がディレクトリレベルおよび各ファイルに関連付けられて格納されることが含まれます。例として、次のタグがファイルにリンクされているとします。

- NFS v4.2セキュリティラベル：セキュリティの決定に使用
- xattrs：ファイルおよび組織のプログラム要件に関連する補足情報を提供します。

次のキーと値のペアは、xattrsとして保存できるメタデータの例であり、ファイルの作成者と関連するセキュリティ分類に関する詳細情報を提供します。クライアントアプリケーションでこのメタデータを使用すると、十分な情報に基づいてアクセスに関する意思決定を行い、組織の標準や要件に従ってファイルを整理できます。

- xattrキーと値のペアの例*

キー	値
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

キー	値

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

キー	値
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

関連情報

- "NetApp ONTAPのNFS：ベストプラクティスおよび実装ガイド"
- "ONTAPコマンド リファレンス"
- コメント要求（RFC）
  - "RFC 7204:ラベル付きNFSの要件"
  - "RFC 2203：RPCSEC_GSS Protocol Specification"
  - "RFC 3530：Network File System (NFS) Version 4 Protocol"

セキュリティの強化

ONTAPセキュリティ強化ガイド

これらのテクニカルレポートには、NetApp ONTAPおよび他のNetApp製品を強化する方法に関するガイダンスが記載されています。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"ONTAPセキュリティとデータ暗号化"ています。

硬化ガイド

"TR-4569：『Security Hardening Guide for NetApp ONTAP』" 情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を組織が達成できるようにNetApp ONTAPを構成する方法について説明します。

"ONTAP tools for VMware vSphere向けセキュリティ強化ガイド" 組織が情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成できるように、VMware vSphere用のONTAPツールを構成する方法について説明します。

"TR-4957：『Security Hardening Guide for NetApp SnapCenter』"
組織が情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成できるようにNetApp SnapCenterソフトウェアを構成する方法について説明します。

"TR-4963: セキュリティ強化ガイド: NetApp Backup and Recovery"組織が情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を達成できるように、 NetApp Cloud Backup for Applications を構成する方法を学習します。

"TR-4943：『Security Hardening Guide for NetApp Active IQ Unified Manager』"
情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を組織が達成できるようにNetApp Active IQ Unified Managerを構成する方法について説明します。

"TR-4945：『Security Hardening Guide for NetApp Manageability SDK』"
NetApp Manageability SDK(NMSDK)を構成して、組織が情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成できるようにする方法について説明します。

"MetroCluster Tiebreakerホストおよびデータベースのセキュリティ強化ガイド"組織が情報システムの機密性、整合性、可用性に関して規定されたセキュリティ目標を達成できるように、NetApp MetroCluster Tiebreakerのホストとデータベースを構成する方法について説明します。

ONTAPセキュリティ強化ガイドライン

ONTAPセキュリティ強化の概要

ONTAPには、業界をリードするデータ管理ソフトウェアであるONTAPストレージオペレーティングシステムを強化するための一連の制御機能が用意されています。ONTAPのガイダンスと構成設定を使用して、組織が情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成できるようにします。

現在、進化を続ける脅威から最も価値のある資産であるデータと情報を保護するため、組織は今までに経験したことのない課題に直面しています。日々進化する脅威や脆弱性はますます洗練され、潜在的な侵入者による難読化と偵察の手法の有効性が向上すると同時に、システム管理者はデータと情報のセキュリティにプロアクティブに対処する必要があります。

2024年7月以降、以前にPDFとして公開されていたテクニカルレポート_TR-4569：ONTAPのセキュリティ強化ガイドの内容がdocs.netapp.comで公開されました。

ONTAP画像検証

ONTAPには、アップグレード時およびブート時にONTAPイメージが有効であることを確認するメカニズムが用意されています。

アップグレードイメージの検証

コード署名は、無停止イメージ更新または自動無停止イメージ更新、CLI、またはONTAP APIによってインストールされたONTAPイメージがNetAppによって正式に生成され、改ざんされていないことを確認するのに役立ちます。アップグレードイメージの検証はONTAP 9.3で導入されました。

ONTAPのアップグレード時またはリバート時に自動的に適用されます。ユーザは、オプションでトップレベルシグネチャを検証する以外は、別の方法で処理する必要はありません `image.tgz` 。

ブート時イメージの検証

ONTAP 9.4以降では、NetApp AFF A800、AFF A220、FAS2750、FAS2720システム、およびUEFI BIOSを採用する後続の次世代システムで、Unified Extensible Firmware Interface（UEFI）セキュアブートが有効になります。

電源投入時、ブートローダーによってセキュア ブート キーのホワイトリスト データベースとロードする各モジュールに関連付けられた署名が照合されて検証されます。各モジュールが検証されてロードされると、ONTAPの初期化が実行されます。モジュールが1つでも署名の検証に失敗した場合、システムはリブートします。

これらの項目は、ONTAPイメージおよびプラットフォームBIOSに適用されます。

ローカルストレージ管理者アカウント

ONTAPのロール、アプリケーション、認証

ONTAPは、セキュリティを重視する企業に、さまざまなログインアプリケーションやログイン方法を使用して、さまざまな管理者にきめ細かくアクセスできる機能を提供します。これにより、お客様はデータ中心のゼロトラストモデルを構築できます。

管理者とStorage Virtual Machine管理者が使用できるロールです。ログインアプリケーション方式とログイン認証方式が指定されています。

役割

Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用すると、ユーザは自分のジョブロールと機能に必要なシステムとオプションにのみアクセスできます。ONTAPのRBACソリューションではユー

ザの管理アクセスがそのユーザのロールに付与されたレベルに制限されるため、管理者は割り当てられたロールに基づいてユーザを管理できます。ONTAPには、複数の事前定義されたロールが用意されています。オペレータや管理者はカスタムのアクセス制御ロールを作成、変更、削除したり、特定のロールに対してアカウント制限を指定したりできます。

クラスタ管理者の事前定義されたロール

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します
`admin`	すべて	すべてのコマンドディレクトリ(`DEFAULT`)
`admin-no-fsa`（ONTAP 9.12.1以降で使用可能）	読み取り / 書き込み	• すべてのコマンドディレクトリ(`DEFAULT`) • `security login rest-role` • `security login role`
読み取り専用です	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	なし
`volume file show-disk-usage`	`autosupport`	すべて

• set • system node autosupport	なし	その他すべてのコマンドディレクトリ(DEFAULT)
backup	すべて	vserver services ndmp
読み取り専用です	volume	なし
その他すべてのコマンドディレクトリ(DEFAULT)	readonly	すべて
• security login password 自分のユーザアカウントのローカルパスワードとキーの情報のみを管理する場合 • set	なし	security
読み取り専用です	その他すべてのコマンドディレクトリ(DEFAULT)	none

autosupport`ロールは事前定義されたアカウントに割り当てられ `autosupport、AutoSupport OnDemandで使用されます。ONTAPでは、アカウントを変更または削除することはできません autosupport。また、ONTAPでは、他のユーザアカウントにロールを割り当てることもできません autosupport。

Storage Virtual Machine（SVM）管理者の事前定義されたロール

ロール名	機能

`vsadmin`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルを管理します。 • LUNの管理 • SnapLock処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
`vsadmin-volume`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルを管理します。 • LUNの管理 • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • ネットワーク インターフェイスの監視 • SVMの健全性の監視
`vsadmin-protocol`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • LUNの管理 • ネットワーク インターフェイスの監視 • SVMの健全性の監視

vsadmin-backup	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • NDMP処理を管理します。 • リストアしたボリュームを読み取り/書き込み可能にします。 • SnapMirror関係とSnapshotを管理します。 • ボリュームとネットワーク情報の表示
vsadmin-snaplock	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshot、およびファイルを管理します。 • privileged deleteなどのSnapLock処理の実行 • プロトコルの設定：NFSとSMB • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視
vsadmin-readonly	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • SVMの健全性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

アプリケーションメソッド

Application Methodはログイン方法のアクセス タイプを指定します。指定できる値は `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 、および `telnet`です。

このパラメータをに設定すると `service-processor` 、サービスプロセッサへのアクセスがユーザに付与されます。サービスプロセッサでは認証のみがサポートされるため、このパラメータを `service-processor-authentication-method` に設定する必要があります `password` 。 `password`SVMユーザ アカウントではサービス プロセッサにアクセスできません。したがって、このパラメータがに設定されている場合、オペレータや管理者はパラメータを使用できません `-vserver service-processor`。

へのアクセスをさらに制限するには `service-processor` 、コマンドを使用し `system service-processor ssh add-allowed-addresses`ます。コマンドを `system service-processor api-service` 使用すると、設定と証明書を更新できます。

セキュリティ上の理由から、NetAppはセキュアなリモートアクセスにセキュアシェル（SSH）を推奨しているため、Telnetとリモートシェル（RSH）はデフォルトで無効になっています。要件や独自のニーズに従ってTelnetまたはRSHを使用する必要がある場合は、それらを有効にする必要があります。

コマンドは `security protocol modify` 、クラスタ全体のRSHおよびTelnetの既存の設定を変更します。[Enabled]フィールドをに設定して、クラスタでRSHとTelnetを有効にします `true`。

ニンショウホウ

Authentication Methodパラメータは、ログインに使用する認証方式を指定します。

認証方式	説明
`cert`	SSL証明書認証
`community`	SNMPコミュニティ ストリング
`domain`	Active Directory認証
`nsswitch`	LDAP認証またはNIS認証
`password`	パスワード
`publickey`	公開鍵認証
`usm`	SNMPユーザ セキュリティ モデル

NISプロトコルはセキュリティが脆弱であるため、推奨されません。

ONTAP 9.3以降では、ローカルSSHアカウントに対して、およびを2つの認証方式として使用して、チェーン型の2要素認証を使用でき `admin` `publickey` `password` ます。コマンドのフィールドに加えて `-authentication-method` `security login` 、という名前の新しいフィールドが `-second-authentication-method` 追加されました。またはは、 `publickey` または `password` として指定できます `-authentication-method` `-second-authentication-method`。ただし、SSH認証では、常に部分認証で順序が変更さ `publickey` れ、その後に完全認証のためのパスワードプロンプトが表示されます。

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

ONTAP 9.4以降では、を `nsswitch` 使用して2つ目の認証方式として使用できます `publickey`。

ONTAP 9.12.1以降では、YubiKeyハードウェア認証デバイスまたは他のFIDO2互換デバイスを使用したSSH認証にもFIDO2を使用できます。

ONTAP 9.13.1以降：

- `domain` アカウントは、を使用して2番目の認証方法として使用でき `publickey`ます。
- 時間ベースのワンタイムパスワード (`totp`）は、現在の時刻を2番目の認証方法の認証要素の1つとして使用するアルゴリズムによって生成される一時パスコードです。

- 公開鍵の失効は、SSH公開鍵と、SSH中に有効期限や失効がチェックされる証明書でサポートされます。

ONTAP System Manager、Active IQ Unified Manager、およびSSHの多要素認証（MFA）の詳細については、"TR-4647：『Multifactor Authentication in ONTAP 9』"を参照してください。

デフォルトノカンリアカウント

管理者ロールにはすべてのアプリケーションを使用したアクセスが許可されているため、adminアカウントは制限する必要があります。diagアカウントはシステムシェルへのアクセスを許可します。テクニカルサポートがトラブルシューティングタスクを実行する場合にのみ使用してください。

デフォルトの管理アカウントには、との2つがあります。 `admin` `diag`

アカウントの孤立は重大なセキュリティ ベクターで、権限の昇格などの脆弱性を招くことが珍しくありません。孤立したアカウントとは、ユーザ アカウント リポジトリに残っている使用されていない不要なアカウントのことです。孤立したアカウントの多くは、使用されたことがないかパスワードが更新または変更されていないデフォルト アカウントです。この問題に対処するために、ONTAPではアカウントの削除と名前変更がサポートされています。

組み込みアカウントを削除したり名前を変更したりすることはできません。管理者がアカウントを削除した場合、再起動時に組み込みアカウントが再作成されます。**NetApp**では、不要な組み込みアカウントはlockコマンドを使用してロックすることを推奨します。

孤立したアカウントは重大なセキュリティ問題ですが、*NetApp は*ローカル アカウント リポジトリからアカウントを削除した場合の影響をテストすることを*強く推奨*します。

ローカルアカウントをリスト表示

ローカルアカウントを一覧表示するには、コマンドを実行し `security login show` ます。

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------ -----------
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
6 entries were displayed.
```

診断（**diag**）アカウントのパスワードを設定する

ストレージシステムには、という名前の診断アカウントが `diag` 用意されています。アカウントを使用して、でトラブルシューティングタスクを実行できます `diag systemshell`。 `diag`システムシェルへのアクセスに使用できるアカウントはアカウントだけです。アクセスには、特権コマンドを使用し `diag systemshell` ます。

> システムシェルと関連する `diag` アカウントは、簡単な診断を目的としています。このアクセスにはdiagnostic権限レベルが必要で、テクニカルサポートからの指示に従ってトラブルシューティングタスクを実行する場合にのみ使用されます。アカウントとは、いずれも `diag systemshell` 一般的な管理目的で使用するものではありません。

開始する前に

にアクセスする前に `systemshell`、コマンドを使用してアカウントパスワードを設定する必要があります `diag security login password`。強力なパスワード原則を使用し、定期的にパスワードを変更する必要があります `diag`。

手順

1. アカウントのユーザパスワードを設定し `diag` ます。

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

マルチ管理者認証

ONTAP 9.11.1以降では、Multi-Admin Verification（MAV；マルチ管理者認証）を使用して、ボリュームやスナップショットの削除などの特定の処理を、指定した管理者の承認後にのみ実行できます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。

MAVの設定は、次の内容で構成されます。

- "1つ以上の管理者承認グループの作成"です。

- "マルチ管理者検証機能の有効化"です。
- "ルールの追加または変更"です。

初期設定後は、MAV承認グループの管理者（MAV管理者）のみがこれらの要素を変更できます。

MAVがイネーブルの場合、保護されたすべての動作を完了するには、次の3つのステップが必要です。

1. ユーザが処理を開始すると、が"要求が生成されました"表示されます。
2. 実行する前に、必要な数のを指定します"MAV管理者は承認する必要があります"。
3. 承認後、ユーザーは操作を完了します。

MAVは、高度な自動化を伴うボリュームやワークフローでは使用しません。自動化された各タスクは、操作を完了する前に承認を必要とするためです。自動化とMAVを一緒に使用する場合はNetApp、特定のMAV操作にクエリを使用することをお勧めします。たとえば、自動化が関係していないボリュームにのみMAVルールを適用し `volume delete` 、特定の命名規則を使用してそれらのボリュームを指定できます。

MAVの詳細については、を参照してください "ONTAPのマルチ管理者認証に関するドキュメント"。

Snapshotロック

Snapshotロックは、ボリュームSnapshotポリシーの保持期間に応じて手動または自動でSnapshotを消去できないようにするSnapLock機能です。Snapshotロックの目的は、不正な管理者や信頼されていない管理者がプライマリまたはセカンダリのONTAPシステムでSnapshotを削除するのを防ぐことです。

スナップショットロックはONTAP 9.12.1で導入されました。スナップショットロックは、改ざん防止スナップショットロックとも呼ばれます。SnapLockライセンスとコンプライアンスクロックの初期化が必要ですが、SnapshotロックはSnapLock ComplianceやSnapLock Enterpriseとは関係ありません。SnapLock Enterpriseのように信頼できるストレージ管理者は存在せず、SnapLockコンプライアンスのように基盤となる物理ストレージインフラを保護することもできません。これは、Snapshotをセカンダリシステムにバックアップする場合に比べて改善された機能です。プライマリシステム上のロックされたSnapshotの迅速なリカバリを実現して、ランサムウェアによって破損したボリュームをリストアできます。

詳細については、を参照して"Snapshotロックのドキュメント"ください。

証明書ベースの**API**アクセスのセットアップ

REST APIまたはNetApp Manageability SDK APIによるONTAPへのアクセスでは、ユーザIDとパスワード認証の代わりに、証明書ベースの認証を使用する必要があります。

REST APIの証明書ベースの認証の代わりにを使用し "OAuth 2.0トークンベースの認証"ます）。

次の手順の説明に従って、自己署名証明書を生成してONTAPにインストールできます。

手順

1. OpenSSLを使用して、次のコマンドを実行して証明書を生成します。

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

このコマンドは、というパブリック証明書とという名前の秘密鍵を生成します `test.pem` `key.out`。共通名CNは、ONTAPユーザIDに対応します。

2. 次のコマンドを実行し、プロンプトが表示されたら証明書の内容をONTAPに貼り付けて、パブリック証明書の内容をPrivacy Enhanced Mail（PEM）形式でインストールします。

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. ONTAPがSSL経由のアクセスをクライアントに許可し、APIアクセスに使用するユーザIDを定義できるようにします。

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

次の例では、証明書で認証されたAPIアクセスの使用をユーザIDで `cert_user` 有効にしています。ONTAPのバージョンを表示するためにを使用する簡単なManageability SDK Pythonスクリプトは `cert_user` 、次のようになります。

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

スクリプトからONTAPのバージョンが出力されます。

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. ONTAP REST APIを使用して証明書ベースの認証を実行するには、次の手順を実行します。
   a. ONTAPで、httpアクセスのユーザIDを定義します。

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. Linuxクライアントで、次のコマンドを実行してONTAPバージョンを出力します。

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

詳細情報

- "NetApp Manageability SDK for ONTAPを使用した証明書ベースの認証"です。

REST APIのONTAP OAuth 2.0トークンベース認証

証明書ベースの認証の代わりに、REST APIにOAuth 2.0トークンベースの認証を使用できます。

ONTAP 9.14.1以降では、Open Authorization（OAuth 2.0）フレームワークを使用してONTAPクラスタへのアクセスを制御するオプションが用意されています。この機能は、ONTAP CLI、System Manager、REST APIなど、ONTAP管理インターフェイスを使用して設定できます。ただし、OAuth 2.0の承認とアクセス制御の決定は、クライアントがREST APIを使用してONTAPにアクセスする場合にのみ適用できます。

OAuth 2.0トークンは、ユーザーアカウント認証用のパスワードを置き換えます。

OAuth 2.0の使用方法の詳細については、を参照してください "OAuth 2.0を使用した認証と許可に関するONTAPドキュメント"。

ログインとパスワードのパラメータ

セキュリティ体制は、組織が規定したポリシーやガイドライン、および組織に適用されるガバナンスや標準に準拠していなければ効果的とはいえません。例としては、ユーザ名の有効期間、パスワードの長さ、使用できる文字、アカウントの保存などの要件があります。ONTAPソリューションには、これらのセキュリティ要素に対応する機能が用意されています。

新しいローカルアカウント機能

組織のユーザーアカウントポリシー、ガイドライン、またはガバナンスを含む標準をサポートするために、ONTAPでは次の機能がサポートされています。

- パスワード ポリシーを設定して最小文字数や大文字小文字の条件を適用する
- ログインに失敗したあとに遅延させる
- アカウントがアクティブでない状態を維持できる最大期間を定義する
- ユーザ アカウントを期限切れにする
- パスワード失効の警告メッセージを表示する
- 無効なログインを通知する

設定可能な設定は、security login role config modifyコマンドを使用して管理します。

SHA-512のサポート

パスワードのセキュリティを強化するために、ONTAP 9ではSHA-2パスワード ハッシュ関数をサポートしており、新規作成または変更されたパスワードのハッシュ化にSHA-512をデフォルトで使用します。必要に応じて、オペレータや管理者がアカウントを期限切れにしたり、ロックしたりすることもできます。

パスワードが変更されていない既存のONTAP 9ユーザアカウントでは、ONTAP 9.0以降へのアップグレード後も引き続きMD5ハッシュ関数が使用されます。ただし、のNetAppでは、これらのユーザアカウントをより安全なSHA-512ソリューションに移行し、ユーザにパスワードを変更させることを強く推奨しています。

パスワード ハッシュ機能を使用して、次の作業を実行できます。

- 指定したハッシュ関数に一致するユーザアカウントを表示します。

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 指定したハッシュ関数（MD5など）を使用するアカウントを期限切れにします。これにより、ユーザは次回のログイン時にパスワードを変更する必要があります。

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 指定したハッシュ関数を使用するパスワードでアカウントをロックします。

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

クラスタの管理SVMにある内部ユーザのパスワードハッシュ関数が不明 `autosupport` です。これは問題のない問題です。この内部ユーザにはデフォルトでパスワードが設定されていないため、ハッシュ関数は不明です。

- ユーザのパスワードハッシュ関数を表示するには `autosupport` 、次のコマンドを実行します。

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- パスワードハッシュ関数（デフォルト：SHA512）を設定するには、次のコマンドを実行します。

```
::> security login password -username autosupport
```

パスワードが何に設定されているかは関係ありません。

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

パスワードパラメータ

ONTAPでは、組織のポリシーやガイドラインに対応するパスワード パラメータをサポートしています。

9.14.1以降では、ONTAPの新規インストールにのみ適用されるパスワードの複雑さとロックアウトルールが追加されています。

すべてのパスワードをユーザ名と区別する必要があります。

属性	説明	デフォルト	範囲
`username-minlength`	ユーザ名の最小文字数	3	3-16
`username-alphanum`	ユーザ名のアルファベットと数字の混在	無効	enabled / disabled
`passwd-minlength`	パスワードの最大文字数	8	3-64
`passwd-alphanum`	パスワードのアルファベットと数字の混在	有効	enabled / disabled
`passwd-min-special-chars`	パスワードに必要な特殊文字の最小数	0	0-64
`passwd-expiry-time`	パスワードの有効期限（日数）	unlimited（パスワードは失効しない）	0 -無制限 0 == 直ちに失効
`require-initial-passwd-update`	初回ログイン時に初期パスワードの更新が必要	無効	enabled / disabled コンソールまたはSSHから変更可能
`max-failed-login-attempts`	最大失敗回数	0（アカウントをロックしない）	-

属性	説明	デフォルト	範囲
lockout-duration	最大ロックアウト期間（日数）	0（アカウントをその日だけロックする）	-
disallowed-reuse	直近のN個のパスワードを許可しない	6	6以上
change-delay	次回のパスワード変更までに必要な間隔（日数）	0	-
delay-after-failed-login	失敗したログイン後の再試行間隔（秒数）	4	-
passwd-min-lowercase-chars	パスワードに必要な小文字の最小数	0（小文字は不要）	0-64
passwd-min-uppercase-chars	パスワードに必要な大文字の最小数	0（大文字は不要）	0-64
passwd-min-digits	パスワードに必要な数字の最小数	0（数字は不要）	0-64
passwd-expiry-warn-time	パスワードの失効何日前に警告を表示するか（日数）	unlimited（パスワードの失効について警告しない）	0（ログインのたびにパスワードの失効について警告）
account-expiry-time	N日後にアカウントの有効期限が切れます	unlimited（アカウントは失効しない）	アクティブでないアカウントが失効となるまでの期間よりも長くする必要がある
account-inactive-limit	アクティブでないアカウントが失効となるまでの期間（日数）	unlimited（アクティブでないアカウントは失効しない）	アカウントの有効期間よりも短くする必要がある

例

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

システムカンリホウホウ

これらは、ONTAPシステム管理を強化するための重要なパラメータです。

コマンドラインアクセス

ソリューションの安全性を守るには、システムとの間にセキュアなアクセスを確立することが重要です。コマンドライン アクセスの最も一般的なオプションとしては、SSH、Telnet、RSHがあります。このうちで最も安全なのがSSHであり、リモート コマンドライン アクセス用の業界標準のベストプラクティスとなっています。ONTAPソリューションへのコマンドライン アクセスにはSSHを使用することを強く推奨します。

SSHセツテイ

`security ssh show`コマンドは、クラスタおよびSVMの
SSH鍵交換アルゴリズム、暗号、およびMACアルゴリズムの設定を表示します。鍵交換方式は、これらのアルゴリズムと暗号を使用して、暗号化や認証用の1回限りのセッション
キーの生成方法、およびサーバ認証の実行方法を指定します。

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

ロクインハナ

ログイン バナーを使用すると、すべてのオペレータと管理者、さらには不正ユーザにも、システムの利用条件を提示することができます。また、誰がシステムへのアクセスを許可されているかを伝えることもできます。ログイン バナーは、システムに求められるアクセス方法や使用方法を確立するのに役立ちます。 `security login banner modify`コマンドは、ログインバナーを変更します。ログイン バナーは、SSHおよびコンソール デバイスのログイン プロセスで認証ステップの直前に表示されます。バナーテキストは、次の例に示すように、二重引用符（""）で囲む必要があります。

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

ログインバナーのパラメータ

パラメータ	説明
`vserver`	このパラメータを使用して、バナーを変更するSVMを指定します。クラスタ レベルのメッセージを変更する場合は、クラスタ管理SVMの名前を使用します。クラスタ レベルのメッセージは、メッセージが定義されていないデータSVM用のデフォルトとして使用されます。

パラメータ	説明
`message`	（オプション）このパラメータは、ログインバナーメッセージを指定します。クラスタにログイン バナー メッセージが設定されている場合、データSVMにもクラスタのログイン バナーが使用されます。データSVMのログインバナーを設定すると、クラスタのログインバナーは表示されません。データSVMのログインバナーでクラスタのログインバナーを使用するようにリセットするには、このパラメータに値を指定します。 このパラメータを使用する場合、ログイン バナーに改行（EOL）を含めることはできません。改行付きのログインバナーメッセージを入力する場合は、パラメータを指定しないでください。そうすると、メッセージを入力するためのプロンプトが表示されます。対話形式で入力されたメッセージには改行を含めることができます。 非ASCII文字にはUnicode UTF-8形式を使用する必要があります。
`uri`	`(ftp
http):///(hostname	IPv4` このパラメータを使用して、ログイン バナーのダウンロード元のURIを指定します。 メッセージの長さは2048バイトを超えてはなりません。ASCII以外の文字はUnicode UTF-8で指定する必要があります。

Message Of The Day

コマンドは、 `security login motd modify` Message Of The Day（MOTD；本日のメッセージ）を更新します。

MOTDには、クラスタ レベルのMOTDとデータSVMレベルのMOTDの2種類があります。データSVMのクラスタシェルにログインしたユーザには、クラスタレベルのMOTDに続いて、そのSVMに対するSVMレベルのMOTDが表示されることがあります。

クラスタ管理者は、クラスタ レベルのMOTDを必要に応じてSVM単位で有効または無効にできます。クラスタ管理者がSVMでクラスタ レベルのMOTDを無効にした場合、そのSVMにログインしたユーザにはクラスタレベルのメッセージは表示されません。クラスタレベルのメッセージを有効または無効にできるのは、クラスタ管理者だけです。

MOTDパラメータ	説明
SVM	このパラメータを使用して、MOTDを変更するSVMを指定します。クラスタ レベルのメッセージを変更する場合は、クラスタ管理SVMの名前を使用します。

MOTDパラメータ	説明
メッセージ	（オプション）このパラメータを使用すると、メッセージを指定できます。このパラメータを使用する場合、MOTDに改行を含めることはできません。パラメータ以外のパラメータを指定しない場合は `-vserver` 、メッセージを対話型モードで入力するように求められます。対話形式で入力されたメッセージには改行を含めることができます。ASCII以外の文字はUnicode UTF-8で指定する必要があります。メッセージには、次のエスケープ シーケンスを使用して、動的に生成される内容を含めることもできます。 • `\\` - 1つのバックスラッシュ文字 • `\b` -出力なし（Linuxとの互換性のためのみサポート） • `\C` -クラスタ名 • `\d` -ログインしたノードの現在の日付 • `\t` -ログインしたノードの現在の時刻 • `\I` -受信LIFのIPアドレス（ログインの場合は「console」と出力 `console` ） • `\l` -ログインしたデバイス名（ログインの場合はconsoleと出力 `console` ） • `\L` -ユーザによるクラスタ内のノードへの前回のログイン • `\m` -マシンアーキテクチャ • `\n` -ノードまたはデータSVMの名前 • `\N` -ログインしているユーザの名前 • `\o` -\Oと同じ。Linuxとの互換性を考慮して提供 • `\O` -ノードのDNSドメイン名。出力はネットワーク構成によって異なり、空になる場合もあり • `\r` -ソフトウェアリリース番号 • `\s` -オペレーティングシステム名 • `\u` -ローカルノードのアクティブなクラスタシェルセッションの数。クラスタ管理者の場合：すべてのクラスタシェルユーザ。データSVM管理の場合はそのデータSVMのアクティブなセッションのみが含まれる • `\U` -と同じ `\u` `` ですが、またはが付加されています。 `user users` • `\v` -有効なクラスタバージョン文字列 • `\W` -ログインしているユーザのクラスタ全体でのアクティブなセッション (`who`)

ONTAPでのMessage Of The Dayの設定の詳細については、を参照してください "Message Of The Dayに関するONTAPのドキュメント"。

CLIセツシヨンタイムアウト

CLIセッションのデフォルトのタイムアウトは30分です。タイムアウトは古いセッションやセッションのピギーバックを防ぐために重要です。

現在のCLIセッションタイムアウトを表示するには、コマンドを使用し `system timeout show` ます。タイムアウト値を設定するには、コマンドを使用し `system timeout modify -timeout <minutes>` ます。

NetApp ONTAP System ManagerによるWebアクセス

ONTAP管理者がCLIではなくグラフィカル インターフェイスを使用してクラスタにアクセスして管理するには、NetApp ONTAP System Managerを使用します。System ManagerはWebサービスとしてONTAPに搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。DNSまたはIPv4またはIPv6アドレスを使用している場合は、ブラウザでホスト名を指定し `https://cluster-management-LIF`ます。

自己署名デジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを示す警告がブラウザに表示されることがあります。危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をクラスタにインストールしてサーバを認証します。

ONTAP 9.3以降では、Security Assertion Markup Language（SAML）認証はONTAP System Managerのオプションです。

ONTAP System ManagerのSAML認証

SAML 2.0は広く採用されている業界標準で、SAMLに準拠したサードパーティのアイデンティティプロバイダ（IdP）が、企業が選択したIdP固有のメカニズムを使用してシングルサインオン（SSO）のソースとしてMFAを実行できるようにします。

SAML仕様では、プリンシパル、IdP、サービスプロバイダの3つのロールが定義されています。ONTAP環境の場合、プリンシパルは、ONTAP System ManagerまたはNetApp Active IQ Unified Managerを通じてONTAPにアクセスするクラスタ管理者です。IdPはサードパーティのIdPソフトウェアです。ONTAP 9.3以降では、Microsoft Active Directoryフェデレーションサービス（ADFS）とオープンソースのシボレスIdPがサポートされます。ONTAP 9.12.1以降では、Cisco Duoがサポートされます。サービスプロバイダは、ONTAPに組み込まれているSAML機能で、ONTAP System ManagerまたはActive IQ Unified Manager Webアプリケーションで使用されます。

SSHの2要素設定プロセスとは異なり、SAML認証をアクティブ化すると、ONTAP System ManagerまたはONTAPサービス プロセッサのアクセスでは既存のすべての管理者にSAML IdPによる認証が要求されます。クラスタ ユーザ アカウントへの変更は必要ありません。SAML認証を有効にすると、およびアプリケーションの管理者ロールを持つ既存のユーザに新しい認証方式が `saml` 追加され `http` `ontapi` ます。

SAML認証を有効にしたあとに、アプリケーションおよびアプリケーションに対して、SAML IdPアクセスを必要とする追加のアカウントを管理者ロールとSAML認証方式でONTAPで定義する必要があります `http` `ontapi` 。ある時点でSAML認証が無効になった場合、これらの新しいアカウントに、およびアプリケーション用の管理者ロールを指定した認証方式を定義し、ローカルのONTAP認証用のアプリケーションをONTAP System Managerに追加する必要があります `password` `http` `ontapi` `console` 。

SAML IdPを有効にすると、IdPは、Lightweight Directory Access Protocol（LDAP）、Active Directory（AD）、Kerberos、パスワードなど、IdPで使用可能な方式を使用してONTAP System Managerへのアクセスの認証を実行します。使用可能な方式はIdPごとに異なります。ONTAPで設定したアカウントのユーザIDがIdPの認証方式に対応していることが重要になります。

NetAppによって検証されたIdPは、Microsoft ADFS、Cisco Duo、およびオープンソースのShibboleth IdPである。

ONTAP 9.14.1以降では、Cisco DuoをSSHの2番目の認証要素として使用できます。

ONTAP System Manager、Active IQ Unified Manager、およびSSHのMFAの詳細については、"TR-4647

：『Multifactor Authentication in ONTAP 9』"を参照してください。

ONTAP System Managerの分析情報

ONTAP 9.11.1以降のONTAP System Managerには、クラスタ管理者が日常的なタスクを合理化するための分析情報が用意されています。セキュリティに関する分析情報は、このテクニカルレポートの推奨事項に基づいています。

セキュリティインサイト	決定
Telnetが有効	NetAppでは、セキュアなリモートアクセスにセキュアシェル（SSH）を推奨しています。
Remote Shell（RSH；リモートシェル）が有効	NetAppでは、セキュアなリモートアクセスにSSHを推奨しています。
AutoSupportでセキュアでないプロトコルが使用されています	AutoSupportは、LINK:HTTPS経由で送信されるように設定されていません。
クラスタレベルでログインバナーが設定されていません	警告：クラスタにログインバナーが設定されていません。
SSH でセキュアでない暗号を使用	SSHでセキュアでない暗号が使用されている場合の警告。
設定されているNTPサーバが少なすぎます	Warning：設定されているNTPサーバの数が3つ未満の場合。
デフォルトの管理ユーザがロックされていない	デフォルトの管理アカウント（adminまたはdiag）を使用してSystem Managerにログインしない場合、それらのアカウントがロックされていないときは、ロックすることを推奨します。
ランサムウェア対策：ボリュームにSnapshotポリシーがない	適切なSnapshotポリシーが1つ以上のボリュームに関連付けられていません。
ランサムウェア対策：Snapshotの自動削除を無効にする	Snapshotの自動削除が1つ以上のボリュームに対して設定されています。
ボリュームはランサムウェア攻撃に対して監視されていない	自律型ランサムウェア対策は複数のボリュームでサポートされますが、まだ設定されていません。
SVMは自律型ランサムウェア対策用に設定されていない	自律型ランサムウェア対策は複数のSVMでサポートされますが、まだ設定されていません。
ネイティブFPolicyが設定されていない	NAS SVMに対してはFPolicyが設定されません。
自律型ランサムウェア対策アクティブモードを有効にする	複数のボリュームがラーニングモードを完了しました。アクティブモードをオンにすることができます。
FIPS 140-2へのグローバルな準拠が無効になっている	グローバルなFIPS 140-2準拠が有効になっていません。
通知用のクラスタが設定されていません	Eメール、Webhook、またはSNMPトラップホストは、通知を受信するように設定されていません。

ONTAP System Managerのインサイトの詳細については、を参照して "ONTAP System Managerインサイトドキュメント"ください。

System Managerノセッションタイムアウト

System Managerセッションの非アクティブ時のタイムアウトを変更できます。デフォルトの非アクティブ時

のタイムアウトは30分です。タイムアウトは、古いセッションやセッションのピギーバックを防ぐために重要です。

SAMLが設定されている場合は、非アクティブ時のタイムアウトはIdPの設定で制御されます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [UI settings]*で、を選択します 。
3. [非アクティブ時のタイムアウト]ボックスに、2～180の分値を入力するか、「0」を入力してタイムアウトを無効にします。
4. [保存（ Save ）] を選択します。

ONTAP自律型ランサムウェア対策

ONTAPの自律型ランサムウェア対策は、ストレージワークロードのセキュリティに関するユーザ行動分析を補完するために、ボリュームのワークロードとエントロピーを分析してランサムウェアを検出し、Snapshotを作成して攻撃の疑いがある場合に管理者に通知します。

ONTAP 9.10.1 では、 NetApp Data Infrastructure Insights Storage Workload Security とNetApp FPolicy パートナー エコシステムによる外部 FPolicy ユーザー行動分析 (UBA) を使用したランサムウェアの検出と防止に加えて、自律的なランサムウェア保護が導入されています。ONTAP自律型ランサムウェア対策は、ボリューム ワークロード アクティビティとデータのエントロピーを監視する標準搭載の機械学習（ML）機能を使用して、ランサムウェアを自動的に検出します。UBAとは異なるアクティビティを監視し、UBAではない攻撃を検出できるようにします。

この機能の詳細については"ランサムウェア向けNetAppソリューション"、またはを参照して"ONTAP自律型ランサムウェア対策に関するドキュメント"ください。

ストレージ管理システムの監査

ONTAPイベントをリモートsyslogサーバにオフロードして、イベント監査の整合性を確保します。このサーバは、Splunkなどのセキュリティ情報イベント管理システムである可能性があります。

syslogを送信

ログや監査情報は、サポートやシステム可用性の観点から組織に欠かせません。また、ログ（syslog）や監査レポート、出力結果には、通常、取り扱いに注意を要する情報が含まれています。セキュリティのコントロールと体制を維持するためには、ログと監査データをセキュアな方法で管理することが必要です。

違反の範囲やフットプリントを単一のシステムまたはソリューションに限定するには、syslog情報のオフロードが必要です。そのため、NetAppでは、syslog情報を安全なストレージまたは保持場所に安全にオフロードすることを推奨しています。

ログの転送先を作成する

リモートロギングのログ転送先を作成するには、コマンドを使用し `cluster log-forwarding create` ま

す。

パラメータ

コマンドを設定するには、次のパラメータを使用し `cluster log-forwarding create` ます。

- *デスティネーションホスト*ログの転送先サーバのホスト名、IPv4アドレス、またはIPv6アドレスを指定します。

```
-destination <Remote InetAddress>
```

- *宛先ポート*転送先サーバがリスンするポートを指定します。

```
[-port <integer>]
```

- *ログ転送プロトコル。*転送先へのメッセージの送信に使用するプロトコルを指定します。

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  ログ転送プロトコルには、次のいずれかの値を指定できます。

  ◦ `udp-unencrypted`です。User Datagram Protocol、セキュリティなし。

  ◦ `tcp-unencrypted`です。TCP、セキュリティなし。

  ◦ `tcp-encrypted`です。TCP、Transport Layer Security（TLS）を使用。

- *宛先サーバーIDを確認します。*このパラメータをtrueに設定すると、証明書を検証してログの転送先の識別情報が確認されます。この値をtrueに設定できるのは、protocolフィールドで値が選択されている場合だけ `tcpencrypted` です。

```
[-verify-server \{true|false}]
```

- * Syslogファシリティ。*転送対象のログに使用するsyslog機能を指定します。

```
[-facility <Syslog Facility>]
```

- *接続テストをスキップします。*通常、この `cluster log-forwarding create` コマンドは、Internet Control Message Protocol（ICMP）pingを送信して宛先に到達できるかどうかを確認し、到達できない場合は失敗します。この値をに設定する `true` と、pingチェックが省略され、到達不能なデスティネーションを設定できるようになります。

```
[-force [true]]
```

NetAppでは、コマンドを使用してタイプへの接続を強制することを推奨しています `cluster log-forwarding -tcp-encrypted` 。

イベント通知

システムから送信される情報とデータを保護することは、システムのセキュリティ体制を維持および管理するために不可欠です。ONTAPソリューションで生成されるイベントは、ソリューションで発生している状況や処理されている情報など、豊富な情報を提供します。このデータは非常に重要なものであり、安全な方法で管理および移行する必要があります。

コマンドは `event notification create` 、イベントフィルタで定義した一連のイベントの新しい通知を1つ以上の通知先に送信します。次の例は、イベント通知の設定と、設定されているイベント通知フィルタと送信先を表示するコマンドを示して `event notification show` います。

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

ONTAPでのストレージ暗号化

ディスクが盗難、返却、転用された場合に機密データを保護するには、ハードウェアベースのNetAppストレージ暗号化またはソフトウェアベースのNetAppボリューム暗号化/NetAppアグリゲート暗号化を使用してください。どちらのメカニズムもFIPS-140-2検証済みであり、ハードウェアベースのメカニズムとソフトウェアベースのメカニズムを使用する場合、このソリューションはCommercial Solutions for Classified（CSfC）Programの対象となります。ハードウェアレイヤとソフトウェアレイヤの両方に保存されている機密データと最高機密データのセキュリティ保護を強化できます。

保管データの暗号化は、ディスクが盗難、返却、転用された場合に機密データを保護するために重要です。

ONTAP 9には、連邦情報処理標準（FIPS）140-2に準拠した保管データ暗号化ソリューションが3つあります。

- NetAppストレージ暗号化（NSE）は、自己暗号化ドライブを使用するハードウェアソリューションです。
- NetApp Volume Encryption（NVE）は、ボリュームごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。
- NetApp Aggregate Encryption（NAE）は、アグリゲートごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。

NSE、NVE、NAEは、外部キー管理またはオンボードキーマネージャ（OKM）のいずれかを使用できます。NSE、NVE、およびNAEを使用しても、ONTAPのストレージ効率化機能には影響はありません。ただし、NVEボリュームはアグリゲート重複排除の対象外です。NAEボリュームはアグリゲート重複排除の対象

であり、重複排除のメリットが得られます。

OKMは、NSE、NVE、またはNAEを使用した保存データに対する自己完結型の暗号化ソリューションです。

NVE、NAE、OKMでは、ONTAP CryptoModが使用されます。CryptoModは、CMVP FIPS 140-2の検証済みモジュールのリストに表示されています。を参照して "FIPS 140-2証明書番号4144"

OKMの設定を開始するには、コマンドを使用し `security key-manager onboard enable` ます。外部のKey Management Interoperability Protocol（KMIP）キー管理ツールを設定するには、コマンドを使用し `security key-manager external enable` ます。ONTAP 9.6以降では、外部キー マネージャでマルチテナンシーがサポートされます。パラメータを使用し `-vserver <vserver name>` て、特定のSVMで外部キー管理を有効にします。9.6より前のバージョンでは `security key-manager setup` 、コマンドを使用してOKMと外部キーマネージャの両方を設定していました。オンボード キー管理の場合、オペレータや管理者は、このコマンドの指示に従ってパスフレーズやOKMのその他のパラメータを順に設定できます。

以下はその一部です。

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

ONTAP 9.4以降では、でtrueオプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができます `-enable-cc-mode` `security key-manager setup` 。ONTAP 9.6以降では、コマンド構文はです `security key-manager onboard enable -cc-mode-enabled yes`。

ONTAP 9.4以降では、advanced権限で機能を使用して、NVE対応ボリュームのデータを無停止で「スクラビ

ング」でき secure-purge ます。暗号化されたボリュームのデータをスクラビングすると、物理メディアからもリカバリできなくなります。次のコマンドは、SVM vs1のvol1にある削除済みファイルを安全にパージします。

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

ONTAP 9.7以降では、VEライセンスが設定されていて、OKMまたは外部キー管理ツールが設定されていてNSEが使用されていない場合、NAEとNVEがデフォルトで有効になります。NAEアグリゲートにはNAEボリュームがデフォルトで作成され、NAE以外のアグリゲートにはNVEボリュームがデフォルトで作成されます。これを無効にするには、次のコマンドを入力します。

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

ONTAP 9.6以降では、SVMスコープを使用して、クラスタ内のデータSVMに対して外部キー管理を設定できます。この方法は、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。詳細については、ONTAPのドキュメントのを参照してください "ONTAP 9.6以降で外部キー管理を有効にする" 。

ONTAP 9.11.1以降では、SVMでプライマリキーサーバとセカンダリキーサーバを指定することで、クラスタ化された外部キー管理サーバへの接続を設定できます。詳細については、ONTAPのドキュメントのを参照してください "クラスタ化された外部キーサーバの設定" 。

ONTAP 9.13.1以降では、System Managerで外部キー管理サーバを設定できます。詳細については、ONTAPのドキュメントのを参照してください "外部キー管理ツールを管理します。" 。

データレプリケーションの暗号化

保存データの暗号化を補うために、SnapMirror、SnapVault、またはFlexCacheの事前共有キーを使用したTLSによるクラスタ間のONTAPデータレプリケーショントラフィックを暗号化できます。

ディザスタリカバリ、キャッシュ、またはバックアップのためにデータをレプリケートする場合は、ONTAPクラスタ間でネットワークを介して転送するときに、そのデータを保護する必要があります。これにより、転送中の機密データに対する悪意のある中間者攻撃を防ぐことができます。

ONTAP 9.6以降、クラスタピアリング暗号化により、SnapMirror、SnapVault、FlexCacheなどのONTAPデータレプリケーション機能に対してTLS 1.2 AES-256 GCM暗号化がサポートされます。暗号化は、2つのクラスタピア間の事前共有キー（PSK）によって設定されます。

ONTAP 9.15.1以降、クラスタピアリング暗号化により、SnapMirror、SnapVault、FlexCacheなどのONTAPデータレプリケーション機能に対してTLS 1.3 AES-256 GCM暗号化がサポートされます。暗号化は、2つのクラスタピア間の事前共有キー（PSK）によってセットアップされます。

NSE、NVE、NAEなどの技術を使用して保存データを保護しているお客様は、ONTAP 9.6以降にアップグレードしてクラスタピアリング暗号化を使用することで、エンドツーエンドのデータ暗号化も使用できます。

クラスター ピアリングは、クラスター ピア間のすべてのデータを暗号化します。例えば、SnapMirrorを使用する場合、すべてのピアリング情報とソースとデスティネーション クラスタ ピア間のすべてのSnapMirror関

係が暗号化されます。クラスタ ピアリング暗号化が有効になっているクラスタ ピア間でクリアテキスト データを送信することはできません。

ONTAP 9.6 以降では、新しいクラスタピア関係ではデフォルトで暗号化が有効になっています。ONTAP 9.6 より前に作成されたクラスタピア関係で暗号化を有効にするには、ソースクラスタとデスティネーション クラスタを 9.6 にアップグレードする必要があります。さらに、 `cluster peer modify`コマンドを使用して、ソースクラスタピアとデスティネーション クラスタピアの両方がクラスタピアリング暗号化を使用するように変更する必要があります。

ONTAP 9.6では、次の例に示すように、既存のピア関係をクラスタピアリング暗号化を使用するように変換できます：

```
On the destination cluster peer:

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the source cluster peer:

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

IPSec転送中データの暗号化

データレプリケーショントラフィックにNetApp Storage Encryption（NSE）やNetApp Volume Encryption（NVE）やクラスタピアリング暗号化（CPE）などの保存データ暗号化テクノロジを使用しているお客様は、ONTAP 9.8以降にアップグレードして次を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間でエンドツーエンドの暗号化を使用できるようになりました。 IPSec：IPSecは、NFS暗号化またはSMB / CIFS暗号化の代替手段であり、iSCSIトラフィックの唯一の転送中暗号化オプションです。

状況によっては、ネットワークを介してONTAP SVMに転送される（または転送中の）すべてのクライアントデータの保護が必要になることがあります。これにより、転送中の機密データに対するリプレイや悪意のある中間者攻撃を防ぐことができます。

ONTAP 9.8以降では、インターネットプロトコルセキュリティ（IPsec）で、クライアントとONTAP SVMの間のすべてのIPトラフィックをエンドツーエンドで暗号化できます。すべてのIPトラフィックのIPSecデータ暗号化には、NFS、iSCSI、SMB / CIFSの各プロトコルが含まれます。IPSecは、iSCSIトラフィックに対して唯一の転送中暗号化オプションを提供します。

ネットワークを介したNFS暗号化は、IPsecの主なユースケースの1つです。ONTAP 9.8より前のバージョンでは、ネットワーク上でのNFS暗号化では、krb5pを使用して転送中のNFSデータを暗号化するようにKerberosをセットアップして設定する必要がありました。これは、すべてのお客様の環境で、必ずしも簡単ではありま

せん。

データレプリケーショントラフィックにNetApp Storage Encryption（NSE）やNetApp Volume Encryption（NVE）やクラスタピアリング暗号化（CPE）などの保存データ暗号化テクノロジを使用しているお客様は、ONTAP 9.8以降にアップグレードして次を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間でエンドツーエンドの暗号化を使用できるようになりました。
IPSec：

IPSecはIETF標準です。ONTAPはトランスポートモードでIPsecを使用します。また、Internet Key Exchange（IKE;インターネットキー交換）プロトコルバージョン2も利用します。IKEプロトコルバージョン2では、事前共有キー（PSK）を使用して、クライアントとONTAP間でIPv4またはIPv6のいずれかでキー素材をネゴシエートします。デフォルトでは、IPsecはSuite-B AES-GCM 256ビット暗号化を使用します。Suite-B AES-GMAC256およびAES-CBC256（256ビット暗号化）もサポートされています。

IPSec機能はクラスタで有効にする必要がありますが、Security Policy Database（SPD；セキュリティポリシーデータベース）エントリを使用して個 々 のSVMのIPアドレスに適用されます。ポリシー（SPD）エントリには、クライアントIPアドレス（リモートIPサブネット）、SVM IPアドレス（ローカルIPサブネット）、使用する暗号スイート、およびIKEv2を介した認証とIPsec接続の確立に必要な事前共有シークレット（PSK）が含まれます。IPsecポリシーエントリに加えて、トラフィックがIPsec接続を通過する前に、クライアントに同じ情報（ローカルおよびリモートIP、PSK、および暗号スイート）を設定する必要があります。ONTAP 9.10.1以降では、IPsec証明書認証のサポートが追加されています。これにより、IPsecポリシーの制限がなくなり、Windows OSでIPsecがサポートされるようになります。

クライアントとSVMのIPアドレスの間にファイアウォールがある場合は、IKEv2ネゴシエーションが成功し、IPsecトラフィックが許可されるように、ESPおよびUDP（ポート500および4500）プロトコル（インバウンド（入力）とアウトバウンド（出力）の両方）を許可する必要があります。

NetApp SnapMirrorおよびクラスタピアリングトラフィックの暗号化では、引き続きIPSecよりもクラスタピアリング暗号化（CPE）を推奨します。これにより、ネットワークを介してセキュアに転送されます。CPEは、IPsecよりもこれらのワークロードに対して優れたパフォーマンスを発揮します。IPsecのライセンスは必要ありません。また、輸出入に関する制限もありません。

次の例に示すように、クラスタでIPSecを有効にし、単一のクライアントおよび単一のSVM IPアドレスに対してSPDエントリを作成できます。

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

関連情報

"ONTAPネットワークでIPセキュリティを使用するための準備"

ONTAPでのFIPSモードとTLSとSSLの管理

FIPS 140-2規格は、コンピュータおよび通信システムの機密情報を保護するセキュリテ

ィシステム内の暗号モジュールのセキュリティ要件を規定しています。FIPS 140-2標準は、製品、アーキテクチャ、データ、エコシステムではなく、_specificate__を暗号化モジュールに適用します。暗号モジュールは、NISTが承認したセキュリティ機能を実装する特定のコンポーネント（ハードウェア、ソフトウェア、ファームウェア、またはこれら3つの組み合わせ）です。

FIPS 140-2への準拠を有効にすると、ONTAP 9内外の他のシステムや通信に影響します。コンソール アクセスが可能な非本番環境のシステムで、これらの設定をテストすることを強く推奨します。

ONTAP 9.11.1およびTLS 1.3のサポート以降では、FIPS 140-3を検証できます。

FIPSの設定は、ONTAPとプラットフォームBMCに適用されます。

NetApp ONTAPのFIPSモード設定

NetApp ONTAPにはFIPSモード構成があり、コントロールプレーンにセキュリティレベルを追加できます。

- ONTAP 9.11.1以降では、FIPS 140-2準拠モードが有効になっている場合、TLSv1、TLSv1.1、およびSSLv3は無効になり、TSLv1.2とTSLv1.3のみが引き続き有効になります。ONTAP 9の内部および外部にある他のシステムおよび通信に影響します。FIPS 140-2準拠モードを有効にしたあとに無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効なままになります。以前の設定に応じて、TLSv1.2またはTLSv1.3のいずれかが有効なままになります。
- 9.11.1より前のバージョンのONTAPでFIPS 140-2準拠モードが有効になっている場合、TLSv1とSSLv3の両方が無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAPでは、FIPS 140-2準拠モードが有効な場合、TLSv1とSSLv3の両方を有効にすることはできません。FIPS 140-2準拠モードを有効にしたあとに無効にした場合、TLSv1とSSLv3は無効なままですが、以前の設定に応じてTLSv1.2またはTLSv1.1とTLSv1.2の両方が有効になります。
- "NetApp暗号セキュリティモジュール（NCSM）"はFIPS 140-2レベル1に準拠しており、ソフトウェアベースのコンプライアンスを実現します。

NISTはFIPS-140-3規格を提出しており、NCSMはFIPS-140-2およびFIPS-140-3の検証を受ける予定です。すべてのFIPS 140-2検証は、新しい証明書の提出の最終日から5年後の2026年9月21日に履歴ステータスに移行します。

FIPS-140-2および**FIPS-140-3**準拠モードの有効化

ONTAP 9以降では、クラスタ全体のコントロールプレーンインターフェイスに対してFIPS-140-2およびFIPS-140-3準拠モードを有効にすることができます。

- "FIPS を有効にする"
- "FIPSステータスの表示"

FIPSの有効化とプロトコル

`security config modify`コマンドを使用すると、クラスタ全体の既存のセキュリティ設定を変更できます。FIPS準拠モードを有効にすると、自動的にTLSプロトコルのみが選択されます。

- パラメータを使用する `-supported-protocols` と、FIPSモードとは関係なくTLSプロトコルを追加または除外できます。デフォルトでは、FIPSモードは無効になっており、TLSv1.3（ONTAP 9.11.1以降）およびTLSv1.2プロトコルが有効になっています。
- 以前のONTAPリリースでは、次のTLSプロトコルがデフォルトで有効になっていました。
  - TLSv1.1（ONTAP 9.12.1以降ではデフォルトで無効）
  - TLSv1（ONTAP 9.8以降ではデフォルトで無効）
- 下位互換性を維持するために、ONTAPでは、FIPSモードが無効な場合にsupported-protocolsのリストにSSLv3を追加できます。

FIPSの有効化と暗号

- パラメータを使用し `-supported-cipher-suites` て、Advanced Encryption Standard（AES）またはAESと3DESのみを設定します。
- を指定すると、RC4などの弱い暗号を無効にできます `!RC4`。デフォルトでは、サポートされる暗号設定はです `ALL:!LOW:!aNULL:!EXP:!eNULL`。この設定は、プロトコルでサポートされるすべての暗号スイートが有効になっていることを意味します。ただし、認証、暗号化、エクスポート、および低暗号化暗号スイートを使用しない64ビットまたは56ビットの暗号アルゴリズムを使用している暗号スイートは除きます。
- 選択したプロトコルで使用可能な暗号スイートを選択してください。設定が無効な場合、一部の機能が適切に動作しなくなる可能性があります。
- 正しい暗号文字列構文については、『 "[Ciphersページ"^]on OpenSSL』（OpenSSLソフトウェア財団が公開）を参照してください。ONTAP 9.9.1以降のリリースでは、セキュリティ設定の変更後にすべてのノードを手動でリブートする必要がなくなりました。

SSHと**TLS**のセキュリティ強化

ONTAP 9のSSH管理には、OpenSSHクライアント5.7以降が必要です。SSHクライアントは、接続を成功させるために、Elliptic Curve Digital Signature Algorithm（ECDSA）公開鍵アルゴリズムとネゴシエートする必要があります。

TLSセキュリティを強化するには、TLS 1.2のみを有効にし、Perfect Forward Secrecy（PFS）に対応した暗号スイートを使用します。PFSは鍵交換の方法で、TLS 1.2などの暗号化プロトコルと組み合わせて使用すると、攻撃者がクライアントとサーバ間のすべてのネットワークセッションを復号化するのを防ぐことができます。

TLSv1.2および**PFS**対応の暗号スイートを有効にする

TLS 1.2およびPFS対応の暗号スイートのみを有効にするには `security config modify`、advanced権限レベルでコマンドを使用します。

SSLインターフェイス設定を変更する前に、ONTAPとの接続を維持するためにONTAPに接続するときに、クライアントが暗号DHEおよびECDHEをサポートしていることを確認してください。

例

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

プロンプトごとに確認し `y` ます。PFSの詳細については、こちらを参照して "ネットアップのブログ"ください。

関連情報

"Federal Information Processing Standard（FIPS）パブリケーション140"

CA署名デジタル証明書の作成

ONTAP Webアクセス用の自己署名デジタル証明書が、組織の情報セキュリティ ポリシーに準拠していないことは珍しくありません。本番用システムでは、NetAppのベストプラクティスとしてCA署名デジタル証明書をインストールし、クラスタまたはSVMをSSLサーバとして認証する際に使用することを推奨します。

コマンドを使用して証明書署名要求（CSR）を生成し、コマンドを使用してCAから返された証明書をインストールできます `security certificate generate-csr` `security certificate install` 。

手順

1. 組織のCAによって署名されたデジタル証明書を作成するには、次の手順を実行します。
   a. CSRを生成します。
   b. 組織の手順に従って、組織のCAからCSRを使用してデジタル証明書を要求します。たとえば、Microsoft Active Directory証明書サービスWebインターフェイスを使用してに移動し `<CA_server_name>/certsrv` 、証明書を要求します。
   c. デジタル証明書をONTAPにインストールします。

オンライン証明書ステータスプロトコル

Online Certificate Status Protocol（OCSP）を有効にすると、TLS通信（LDAP、TLSなど）を使用するONTAPアプリケーションがデジタル証明書のステータスを受信できるようになります。アプリケーションは、要求した証明書が「有効」、「失効」、「不明」のどのステータスであるかを示す署名済みの応答を受け取ります。

OCSPを使用すると、証明書失効リスト（CRL）がなくてもデジタル証明書の現在のステータスを特定することができます。

デフォルトでは、OCSPによる証明書のステータスチェックは無効になっています。オンにするには、コマンドを使用し `security config ocsp enable -app name`ます。アプリケーション名は `autosupport`、、 `audit_log` `fabricpool`、、 `ems` `kmip`、、 `ldap_ad` `ldap_nis_namemap`、、または `all`。このコマンドにはadvanced権限レベルが必要です。

SSHv2の管理

コマンドは `security ssh modify` 、クラスタまたはSVMのSSH鍵交換アルゴリズム、暗号、またはMACアルゴリズムの既存の設定を、指定した設定で置き換えます。

NetAppの推奨事項は次のとおりです。

- ユーザ セッションにはパスワードを使用する。
- マシン アクセスには公開鍵を使用する。

サポートされる暗号とキー交換

暗号	キー交換
aes256-ctr	diffie-hellman-group-exchange-sha256（SHA-2）
aes192-ctr	diffie-hellman-group-exchange-sha1（SHA-1）
aes128-ctr	diffie-hellman-group14-sha1（SHA-1）
aes256-cbc	diffie-hellman-group1-sha1（SHA-1）
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

サポートされる**AES**および**3DES**対称暗号化

ONTAPでは、次のタイプのAESおよび3DESの対称暗号化（暗号）もサポートしています。

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm

- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

SSH管理設定は、ONTAPおよびプラットフォームBMCに適用されます。

NetApp AutoSupport

ONTAPのAutoSupport機能を使用すると、システムの健全性をプロアクティブに監視し、NetAppテクニカルサポート、組織内のサポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。ストレージシステムの初回設定時には、NetAppテクニカルサポートへのAutoSupportメッセージがデフォルトで有効になります。また、AutoSupportは有効になってから24時間後にNetAppテクニカルサポートへのメッセージ送信を開始します。この24時間という設定は変更可能です。組織の社内サポートチームとのコミュニケーションを活用するには、メールホストの設定が完了している必要があります。

AutoSupportを管理（設定）できるのはクラスタ管理者だけです。SVM管理者にはAutoSupportへのアクセス権はありません。AutoSupport機能は無効にできます。ただし、のNetAppでは、AutoSupportを有効にすることを推奨しています。これは、ストレージシステムで問題が発生した場合に、迅速に問題を特定して解決できるためです。デフォルトでは、AutoSupportを無効にした場合でも、AutoSupport情報は収集されてローカルに格納されます。

さまざまなメッセージに含まれる内容や、さまざまな種類のメッセージが送信される場所など、AutoSupportメッセージの詳細については、ドキュメントを参照して "NetAppデジタルアドバイザ" ください。

AutoSupportメッセージには、次のような機密データが含まれます。

- ログファイル
- 特定のサブシステムについての状況に応じたデータ
- 設定データとステータスデータ
- パフォーマンスデータ

AutoSupportでは、転送プロトコルとしてHTTPSとSMTPがサポートされます。AutoSupportメッセージは機密性が高いため、NetAppでは、AutoSupportメッセージをNetAppサポートに送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。

また、コマンドを使用して、AutoSupportデータのターゲット（NetAppテクニカルサポート、組織内の業務、パートナーなど）を指定する必要があります `system node autosupport modify` 。このコマンドでは、AutoSupportで送信する内容（パフォーマンス データやログ ファイルなど）も指定できます。

AutoSupportを完全に無効にするには、コマンドを使用し `system node autosupport modify -state disable` ます。

ネットワークタイムプロトコル

ONTAPではクラスタのタイムゾーン、日付、および時刻を手動で設定できますが、クラスタ時間を3つ以上の外部NTPサーバと同期するようにネットワークタイムプロトコル（NTP）サーバを設定する必要があります。

クラスタ時間が不正確だと問題が発生する可能性があります。ONTAPではクラスタのタイム ゾーン、日付、時刻を手動で設定できますが、ネットワーク タイム プロトコル（NTP）サーバを設定してクラスタ時間を外部のNTPサーバと同期する必要があります。

ONTAP 9.5以降では、対称認証を使用してNTPサーバを設定できます。

コマンドを使用すると、最大10台の外部NTPサーバを関連付けることができます `cluster time-service ntp server create`。タイムサービスの冗長性と品質を高めるには、少なくとも3台の外部NTPサーバをクラスタに関連付ける必要があります。

ONTAPでのNTPの設定の詳細については、を参照してください "クラスタ時間の管理（クラスタ管理者のみ）"。

NASファイルシステムのローカルアカウント（CIFSワークグループ）

ワークグループによるクライアント認証は、従来のドメイン認証の仕組みに反しないセキュリティ レイヤをONTAPソリューションに追加します。IP情報、認証メカニズム、プロトコルバージョン、認証タイプなど、ポスチャ関連の詳細情報を多数表示するには、コマンドを使用し `vserver cifs session show` ます。

ONTAP 9以降では、ローカルで定義されたユーザとグループを使用してサーバに認証するCIFSクライアントを含むワークグループ内にCIFSサーバを設定できます。ワークグループによるクライアント認証は、従来のドメイン認証の仕組みに反しないセキュリティ レイヤをONTAPソリューションに追加します。CIFSサーバを設定するには、コマンドを使用し `vserver cifs create` ます。CIFSサーバを作成したら、CIFSドメインに追加するかワークグループに追加できます。ワークグループに参加するには、パラメータを使用し `-workgroup` ます。次に設定例を示します。

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

ワークグループ モードのCIFSサーバでは、Windows NT LAN Manager（NTLM）認証のみがサポートされ、Kerberos認証はサポートされません。

NetAppでは、組織のセキュリティ体制を維持するために、CIFSワークグループでNTLM認証機能を使用することを推奨しています。NetAppでは、CIFSのセキュリティ体制を検証するために、コマンドを使用して、IP情報、認証メカニズム、プロトコルバージョン、認証タイプなど、ポスチャ関連の詳細を表示することを推奨してい `vserver cifs session show` ます。

NASフアイルシステムノカンサ

NASファイル・システムは'今日の脅威の状況で使用量が増加しています監査機能は'可視性をサポートするために不可欠です

セキュリティには検証が必要です。ONTAPは、ソリューション全体にわたって監査イベントと詳細情報の拡充を提供します。今日の脅威環境においてNASファイルシステムの占有率が高まっているため、可視性をサポートするには監査機能が不可欠です。ONTAPの監査機能の強化により、CIFSの監査詳細情報はこれまで以上に充実しました。以下の重要な詳細情報は、作成されたイベントと共に記録されます：

- ファイル、フォルダ、共有へのアクセス
- ファイルの作成、変更、削除
- ファイル読み取りアクセスの成功
- ファイルの読み取りまたは書き込みの失敗
- フォルダ権限の変更

監査設定を作成します。

監査イベントを生成するには、CIFS監査を有効にする必要があります。監査設定を作成するには、コマンドを使用し `vserver audit create` ます。デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。ローテーション パラメータのフィールドにオプションを指定すれば、時間に基づくローテーションも使用できます。監査ログのローテーション設定には、ローテーションのスケジュール、ローテーション上限、実行する曜日、サイズなどの詳細を指定できます。次のテキストは、すべての曜日の12：30にスケジュールされた月単位の時間ベースのローテーションを使用した監査設定の例を示しています。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS監査イベント

CIFS監査イベントは次のとおりです。

- ファイル共有：関連するコマンドを使用してCIFSネットワーク共有が追加、変更、または削除されたときに監査イベントを生成します `vserver cifs share` 。
- 監査ポリシーの変更：関連するコマンドを使用して監査ポリシーが無効化、有効化、または変更された場合に、監査イベントを生成します `vserver audit` 。
- ユーザアカウント：ローカルのCIFSまたはUNIXユーザが作成または削除されたとき、ローカルユーザアカウントが有効化、無効化、変更されたとき、パスワードがリセットまたは変更されたときに監査イベントを生成します。このイベントは、コマンドまたは関連するコマンドを使用し `vserver cifs users-and-groups local-group` `vserver services name-service unix-user` ます。
- セキュリティグループ：コマンドまたは関連するコマンドを使用してローカルのCIFSまたはUNIXセキュリティグループが作成または削除されたときに監査イベントを生成します `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- 認証ポリシーの変更：コマンドを使用してCIFSユーザまたはCIFSグループの権限が付与または取り消されたときに、監査イベントを生成します `vserver cifs users-and-groups privilege` 。

これはシステムの監査機能に基づく機能であり、管理者は、システムが何を許可および実行しているかをデータ ユーザの視点で確認することができます。

NASノカンサヘノRESTAPIノエイキヨウ

ONTAPには、管理者アカウントがREST APIを使用してSMB / CIFSまたはNFSファイルにアクセスして操作する機能が含まれています。REST APIはONTAP管理者のみが実行できますが、REST APIコマンドはシステムNAS監査ログをバイパスします。また、ONTAP管理者がREST APIを使用する際にファイル権限をバイパスすることもできます。ただし、ファイルに対するREST APIを使用した管理者の操作は、システムコマンド履歴ログに記録されます。

アクセスなしREST APIロールの作成

RESTを使用してONTAPボリュームにアクセスできないREST APIロールを作成することで、ONTAP管理者がREST APIをファイルアクセスに使用できないようにすることができます。このロールをプロビジョニングするには、次の手順を実行します。

/api/storage/volumes REST APIは、ファイルアクセス以外にも様々な用途で使用されます。System Managerやその他のGUIインターフェースでは、ボリュームの作成、表示、変更に使用されます。

手順

1. ストレージボリュームへのアクセスは許可されず、他のすべてのREST APIアクセスを許可する新しいRESTロールを作成します。

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 前の手順で作成した新しいREST APIロールに管理者アカウントを割り当てます。

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

組み込みのONTAPクラスタ管理者アカウントがREST APIをファイルアクセスに使用しないようにするには、まずを実行する必要があり "新しい管理者アカウントを作成し、組み込みアカウントを無効化または削除する"ます。

CIFS SMBの署名と封印の設定と有効化

ストレージシステムとクライアント間のトラフィックがリプレイ攻撃や中間者攻撃によって危険にさらされないようにすることで、データファブリックのセキュリティを保護するSMB署名を設定して有効にすることができます。SMB署名は、SMBメッセージに有効な署名があることを確認することで保護します。

タスクの内容

ファイルシステムやアーキテクチャの代表的な脅威ベクターは、SMBプロトコルです。このベクターに対処するために、ONTAP 9は業界標準のSMB署名と封印を使用します。SMB署名は、ストレージシステムとクライ

アント間のトラフィックがリプレイ攻撃や中間者攻撃によって危険にさらされないようにすることで、データファブリックのセキュリティを保護します。具体的には、SMBメッセージに有効な署名があることが確認されます。

パフォーマンス上の理由からSMB署名はデフォルトでは無効になっていますが、NetAppでは有効にすることを強く推奨します。さらに、ONTAPではSMB暗号化（封印）もサポートしています。SMB暗号化は共有単位でのセキュアなデータ転送を実現します。デフォルトでは、SMB暗号化は無効になっています。ただし、NetAppではSMB暗号化を有効にすることを推奨します。

SMB 2.0以降ではLDAPの署名と封印がサポートされるようになりました。署名（改ざんに対する保護）と封印（暗号化）により、SVMとActive Directoryサーバ間のセキュアな通信が実現します。SMB 3.0以降では、アクセラレーション用の新しいAES命令セット（Intel AES NI）がサポートされます。Intel AES NIはAESアルゴリズムの改良版で、サポートされるプロセッサ ファミリでのデータ暗号化を加速します。

手順

1. SMB署名を設定して有効にするには、コマンドを使用し `vserver cifs security modify` て、パラメータがに設定されていることを確認し `-is-signing-required` `true`ます。次の設定例を参照してください。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. SMBの封印と暗号化を設定して有効にするには、コマンドを使用し `vserver cifs security modify` て、パラメータがに設定されていることを確認し `-is-smb-encryption-required` `true`ます。次の設定例を参照してください。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFSのセキュリティ保護

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポート ルールでは、ボリュームへのクライアント アクセス要求が設定済みの特定のパラメータと照合され、クライアント アクセス要求の処理方法が決定されます。エクスポートポリシーには、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順序で処理されます。

アクセス制御は、セキュアな体制を維持するうえで中心的な役割を果たします。そのためONTAPでは、エクスポート ポリシー機能を使用して、NFSボリュームへのアクセスを特定のパラメータに一致するクライアン

トだけに制限します。エクスポートポリシーには、各クライアントアクセス要求を処理する1つ以上のエクスポートルールが含まれています。ボリュームへのクライアント アクセスを設定するため、各ボリュームにはエクスポート ポリシーが関連付けられています。エクスポート ポリシーの結果に基づいて、クライアントにボリュームへのアクセスが許可されるか拒否されるか（「permission denied」メッセージが表示される）が決まります。また、ボリュームに対するアクセス レベルも決まります。

> クライアントがデータにアクセスするためには、エクスポート ルールを含むエクスポート ポリシーがSVMに割り当てられている必要があります。SVMには複数のエクスポート ポリシーを割り当てることができます。

ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールのアクセス権が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

エクスポート ルールは、次の条件を適用することでクライアントのアクセス権を決定します。

- クライアントが要求の送信に使用したファイル アクセス プロトコル（NFSv4やSMBなど）
- クライアント識別子（ホスト名やIPアドレスなど）
- クライアントが認証に使用したセキュリティ タイプ（Kerberos v5、NTLM、AUTH_SYSなど）

ルールに複数の条件が指定されている場合、クライアントが1つでも条件に一致しないとそのルールは適用されません。

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれているとします。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントに付与されるアクセス レベルはセキュリティ タイプで決まります。アクセスレベルには、読み取り専用、読み取り/書き込み、およびスーパーユーザ（ユーザIDを持つクライアントの場合）の3つがあります `0`。セキュリティタイプによって決定されたアクセスレベルはこの順序で評価されるため、次のルールに従う必要があります。

エクスポートルールのアクセスレベルパラメータのルール

クライアントが次のアクセスレベルを取得する場合	これらのアクセスパラメータは、クライアントのセキュリティタイプと一致している必要があります。
標準ユーザの読み取り専用	読み取り(`-rorule`専用)
標準ユーザの読み取り / 書き込み	読み取り専用(`-rorule`）および読み取り/書き込み(`-rwrule`)
スーパーユーザの読み取り専用	読み取り専用(`-rorule`）および `-superuser`

クライアントが次のアクセスレベルを取得する場合	これらのアクセスパラメータは、クライアントのセキュリティタイプと一致している必要があります。
スーパーユーザの読み取り / 書き込み	読み取り専用(`-rorule`）(`-rwrule`および `-superuser`読み取り/書き込み

これら3つの各アクセスパラメータで有効なセキュリティタイプは次のとおりです。

- 任意
- なし
- しない

次のセキュリティタイプは、パラメータでは使用できません `-superuser` 。

- krb5
- ntlm
- sys

アクセス パラメータのルール結果

クライアントのセキュリティ タイプ	そしたら...。
アクセス パラメータに指定されたセキュリティ タイプと一致する。	クライアントは、自身のユーザIDでそのレベルのアクセス権を受け取ります。
指定したセキュリティタイプと一致しないが、アクセスパラメータにオプションが指定されている `none`。	クライアントは、そのレベルのアクセス権を受け取り、パラメータで指定されたユーザIDを持つ匿名ユーザを受け取り `-anon` ます。
指定したセキュリティタイプと一致しないため、アクセスパラメータにオプションが含まれていません `none`。	クライアントは、そのレベルのアクセス権を受け取りません。 この制限はパラメータには適用され `-superuser` ません。このパラメータには、指定しなくても常にnoneが指定されるためです。

Kerberos 5とkrb5p

ONTAP 9以降では、プライバシー サービス（krb5p）を使用したKerberos 5認証がサポートされます。krbp5認証は安全で、チェックサムを使用してクライアントとサーバの間のすべてのトラフィックを暗号化することでデータの改ざんやスヌーピングを防止します。ONTAPでは、Kerberos用に128ビットおよび256ビットのAES暗号化をサポートしています。プライバシー サービスには、受信データの整合性検証、ユーザの認証、送信前のデータの暗号化が含まれます。

krb5pオプションはエクスポート ポリシー機能で最もよく使用され、暗号化オプションとして設定されます。次の例に示すように、krb5p認証方式を認証パラメータとして使用できます。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Lightweight Directory Access Protocolの署名と封印を有効にする

署名と封印は、LDAPサーバへのクエリでセッションセキュリティを有効にするためにサポートされています。これは、LDAP over TLSに代わるセッション セキュリティを提供します。

署名は、シークレット キー技術を使用してLDAPペイロード データの整合性を確保します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。SVMのセッションセキュリティ設定は、LDAPサーバで使用可能な設定に対応しています。デフォルトでは、LDAPの署名と封印は無効になっています。

手順

1. この機能を有効にするには、パラメータを指定してコマンドを実行し `vserver cifs security modify session-security-for-ad-ldap` ます。

   LDAPセキュリティ機能のオプション：

   - なし:デフォルト、署名または封印なし
   - 署名：LDAPトラフィックに署名します。
   - 封印：LDAPトラフィックの署名と暗号化

   > signとsealは累積的に適用されます。つまり、signオプションを使用した場合はLDAPが署名され、sealオプションを使用した場合は署名されたうえで封印（暗号化）されます。また、このコマンドにパラメータを指定しない場合、デフォルトはnoneです。

   次に、設定例を示します。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

NetApp FPolicyの作成と使用

ONTAPソリューションのインフラコンポーネントであるFPolicyを作成して使用できます。FPolicyを使用すると、パートナーアプリケーションからファイルアクセス権限を監視および設定できます。その中でも強力なアプリケーションの1つが、NetApp SaaSアプリケーションであるストレージワークロードセキュリティです。ハイブリッドクラウド環境全体にわたるすべての企業データアクセスを一元的に可視化して制御できるため、セキュリティとコンプライアンスの目標を確実に達成できます。

アクセス制御はセキュリティの中核をなす概念です。ファイルアクセスやファイル操作を可視化し、応答でき

るようにすることは、セキュリティ体制の維持に欠かせません。可視性とファイルアクセス制御を提供するために、ONTAPソリューションではNetApp FPolicy機能を使用しています。

ファイル ポリシーはファイル タイプに基づいて設定できます。FPolicyは、ファイルを作成する、開く、名前を変更する、削除するといった、個々のクライアント システムからの操作の要求をストレージ システムがどのように処理するかを決定します。ONTAP 9以降ではFPolicyのファイル アクセス通知フレームワークが強化され、フィルタによる制御および短時間のネットワーク停止に対する耐障害性が追加されました。

手順

1. FPolicy機能を利用するには、まずコマンドを使用してFPolicyポリシーを作成する必要があります `vserver fpolicy policy create` 。

   FPolicyを使用してイベントを表示したり収集したりする場合は、パラメータも使用し `-events` ます。ONTAPには、フィルタ処理やアクセスをユーザ名レベルで制御するより細かな機能が用意されています。ユーザ名で権限とアクセスを制御するには、パラメータを指定します `-privilege-user-name` 。

   次にFPolicyの作成例を示します。

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. FPolicyポリシーを作成したら、コマンドを使用して有効にする必要があります `vserver fpolicy enable` 。このコマンドではFPolicyエントリの優先度（順序）も設定します。

   同じファイル アクセス イベントに複数のポリシーが割り当てられている場合、優先度に基づいてアクセスが許可または拒否される順序が決まるため、FPolicyのシーケンスが重要になります。

   次のテキストは、コマンドを使用してFPolicyポリシーを有効にし、その設定を検証する設定例を示してい `vserver fpolicy show` ます。

   ```
   cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
   vs2_pol -sequence-number 5

   cluster1::> vserver fpolicy show
   Vserver                 Policy Name                     Sequence  Status
   Engine
   ----------------------- ------------------------------- --------  -------
   -------
   vs1.example.com         vs1_pol
   vs2.example.com         vs2_pol
    external
   2 entries were displayed.
   ```

FPolicyの機能拡張

以降のセクションで、ONTAP 9で強化されたFPolicyの機能について説明します。

フィルタリングコントロール

ディレクトリアクティビティに関する通知を削除するための新しいフィルタが追加されました `SetAttr` 。

非同期の耐障害性

非同期モードで動作しているFPolicyサーバでネットワーク停止が発生した場合、停止中に生成されたFPolicy通知がストレージ ノードに保存されます。FPolicyサーバがオンラインに戻ると、サーバは格納された通知に関するアラートを受け取り、ストレージ ノードから通知を読み込むことができます。停止中に通知を格納できる期間は、10分までの範囲で設定可能です。

ONTAPでのLIFロールのセキュリティ特性

LIFは、ロール、ホームポート、ホームノード、フェイルオーバー先のポートのリスト、ファイアウォールポリシーなどの特性が関連付けられているIPアドレスまたはWorld Wide Port Name（WWPN）です。LIFは、クラスタでネットワーク経由の通信の送受信に使用するポートに設定できます。LIFの各ロールのセキュリティ特性を理解することが重要です。

LIFロール

LIFのロールは次のとおりです。

- *データLIF *：SVMに関連付けられ、クライアントとの通信に使用されるLIFです。
- *クラスタLIF *：クラスタ内のノード間のトラフィックの伝送に使用されるLIFです。
- *ノード管理LIF *：クラスタ内の特定のノードを管理するための専用IPアドレスを提供するLIFです。
- *クラスタ管理LIF *：クラスタ全体に対して単一の管理インターフェイスを提供するLIFです。
- *クラスタ間LIF *：クラスタ間の通信、バックアップ、およびレプリケーションに使用されるLIFです。

各LIFロールのセキュリティ特性

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
プライベートIPサブネットが必要	いいえ	はい	いいえ	いいえ	いいえ
セキュアなネットワークが必要	いいえ	はい	いいえ	いいえ	はい
デフォルトのファイアウォールポリシー	非常に厳しい	完全にオープン	中	中	非常に厳しい
ファイアウォールをカスタマイズ可能	はい	いいえ	はい	はい	はい

- クラスタLIFは完全にオープンで設定可能なファイアウォール ポリシーがないため、分離されたセキュアなネットワークのプライベートIPサブネットに配置する必要があります。
- LIFのロールをインターネットに公開しないでください。

LIFのセキュリティ保護の詳細については、以下を参照してください。 "LIFのファイアウォールポリシーを設定する"。このページでは、 ONTAP 9.10.1 以降の LIF サービス ポリシーの詳細も説明します。

新しいサービスポリシーを作成する方法の詳細については、 `network interface service-policy create` コマンドの "コマンドリファレンス。"

プロトコルおよびポートセキュリティ

ソリューションのセキュリティを強化するには、組み込みのセキュリティ処理や機能に加え、外部のセキュリティ メカニズムも必要になります。ファイアウォール、不正侵入防御（IPS）、その他のセキュリティ デバイスなど、追加のインフラ デバイスを利用してONTAPへのアクセスをフィルタおよび制限することで、厳しいセキュリティ体制を効果的に確立して維持することができます。この情報は、環境とそのリソースへのアクセスをフィルタリングおよび制限するための重要なコンポーネントです。

よく使用されるプロトコルとポート

サービス	ポート / プロトコル	説明
SSH	22 / TCP	SSHロクイン
telnet	23 / TCP	リモートログイン
Domain	53 / TCP	ドメイン ネーム サーバ
HTTP	80 / TCP 80 / UDP	HTTP
rpcbind	111 / TCP 111 / UDP	リモートプロシージャコール
NTP	123 / UDP	ネットワークタイムプロトコル
msrpc	135 / TCP	Microsoftリモート プロシージャ コール
Netbios-name	137 / TCP 137 / UDP	NetBIOSネームサービス
netbios-ssn	139 / TCP	NetBIOSサービスセッション
SNMP	161 / UDP	SNMP
HTTPS	443 / TCP	セキュアリンク：http
microsoft-ds	445 / TCP	Microsoftディレクトリ サービス
IPsec	500 / UDP	インターネットプロトコルセキュリティ
mount	635/UDP	NFSマウント

サービス	ポート / プロトコル	説明
named	953 / UDP	名前デーモン
NFS	2049 / UDP 2049 / TCP	NFSサーバデーモン
nrv	2050 / TCP	NetAppリモート ボリューム プロトコル
iscsi	3260 / TCP	iSCSIターゲットポート
Lockd	4045 / TCP 4045 / UDP	NFSロックデーモン
NFS	4046 / TCP	NFS mountdプロトコル
acp-proto	4046 / UDP	アカウント プロトコル
rquotad	4049/UDP	NFS rquotadプロトコル
krb524	4444 / UDP	Kerberos 524
IPsec	4500/UDP	インターネットプロトコルセキュリティ
acp	5125 / UDP 5133 / UDP 5144 / TCP	ディスク用の代替制御ポート
Mdns	5353 / UDP	マルチキャストDNS
HTTPS	5986/UDP	HTTPSポート：バイナリ プロトコルをリスン
TELNET	8023 / TCP	ノードを対象としたTelnet
HTTPS	8443 / TCP	7MTT GUIツール（リンク経由）：HTTPS
RSH	8514 / TCP	ノードを対象としたRSH
KMIP	9877 / TCP	KMIPクライアント ポート（内部ローカル ホストのみ）
ndmp	10000 / TCP	NDMP
cifs 監視ポート	40001 / TCP	CIFS監視ポート
TLS	50000 / TCP	トランスポートレイヤセキュリティ
Iscsi	65200 / TCP	iSCSIポート
SSH	65502 / TCP	セキュアシェル
vsun	65503 / TCP	vsun

NetApp内部ポート

ポート / プロトコル	説明
900	NetAppクラスタRPC
902	NetAppクラスタRPC
904	NetAppクラスタRPC
905	NetAppクラスタRPC

ポート / プロトコル	説明
910	NetAppクラスタRPC
911	NetAppクラスタRPC
913	NetAppクラスタRPC
914	NetAppクラスタRPC
915	NetAppクラスタRPC
918	NetAppクラスタRPC
920	NetAppクラスタRPC
921	NetAppクラスタRPC
924	NetAppクラスタRPC
925	NetAppクラスタRPC
927	NetAppクラスタRPC
928	NetAppクラスタRPC
929	NetAppクラスタRPC
931	NetAppクラスタRPC
932	NetAppクラスタRPC
933	NetAppクラスタRPC
934	NetAppクラスタRPC
935	NetAppクラスタRPC
936	NetAppクラスタRPC
937	NetAppクラスタRPC
939	NetAppクラスタRPC
940	NetAppクラスタRPC
951	NetAppクラスタRPC
954	NetAppクラスタRPC
955	NetAppクラスタRPC
956	NetAppクラスタRPC
958	NetAppクラスタRPC
961	NetAppクラスタRPC
963	NetAppクラスタRPC
964	NetAppクラスタRPC
966	NetAppクラスタRPC
967	NetAppクラスタRPC
7810	NetAppクラスタRPC

ポート / プロトコル	説明
7811	NetAppクラスタRPC
7812	NetAppクラスタRPC
7813	NetAppクラスタRPC
7814	NetAppクラスタRPC
7815	NetAppクラスタRPC
7816	NetAppクラスタRPC
7817	NetAppクラスタRPC
7818	NetAppクラスタRPC
7819	NetAppクラスタRPC
7820	NetAppクラスタRPC
7821	NetAppクラスタRPC
7822	NetAppクラスタRPC
7823	NetAppクラスタRPC
7824	NetAppクラスタRPC

ONTAP NASテクニカルレポート

NetApp NASソリューションはデータ管理を簡素化し、コストを最適化しながら成長ペースに対応できるよう支援します。

ONTAP S3の略

"TR-4814：『S3 in ONTAP best practices』" Amazon Simple Storage Service（S3）をONTAPソフトウェアで使用するための推奨されるプラクティス、およびONTAPをネイティブのS3アプリケーションを使用するオブジェクトストアとして、またはFabricPoolの階層化のデスティネーションとして使用するための機能と設定について説明します。

ONTAP SMBの技術レポート

NetApp NASソリューションはデータ管理を簡素化し、コストを最適化しながら成長ペースに対応できるよう支援します。

SMB

"TR-4740：『SMB 3.0 multichannel』"
Microsoftは、SMB1およびSMB2のパフォーマンスと信頼性の制限に対処することでSMB3プロトコルを改善することを目的として、SMB 3.0プロトコルにマルチチャネルを導入しました。ONTAPのマルチチャネル機能の機能、推奨される方法、パフォーマンステストの結果などについて説明します。

マルチプロトコル

"TR-4887：『Multiprotocol NAS in ONTAP Overview and Best Practices』"
ONTAPでのマルチプロトコルNASアクセスの仕組みと、マルチプロトコル環境の推奨事項について説明します。

ストレージ システム

AFX

NetApp AFXの概要：NetApp AFXについて学ぶ

NetApp AFXは引き続きONTAPです。ONTAPのメリットを活用するための別の方法にすぎません。NetApp AFXは、NASおよびオブジェクトワークロード向けに分散型アーキテクチャを提供しながら、お客様がよく知っていて信頼している機能豊富なONTAPソフトウェアを提供します。

イノベーションの進化：NetApp ONTAP

NetApp ONTAPは、複数のクライアントにNFSワークロードを提供する新しい方法として1992年に開発され、パフォーマンス、データの回復力、特定時点のコピーなどにおいて革新的な進歩をもたらしました。当初はNFSv2のみをサポートしていましたが、新しいNFSバージョン、他のデータプロトコル、より多くのデータ保護機能に対する需要が高まるにつれて、NetApp ONTAPは進化せざるを得ませんでした。

以下は、過去30年以上にわたって起こった主要なONTAPの進化の簡略化されたタイムラインです。

NetApp ONTAP の進化

10年	機能
1990sを使用したチャンク アップロード署名要求がサポートされるようになりました。	NFSv2、NFSv3、CIFS、スナップショット、WAFL ファイルシステム、AutoSupport、SnapMirror
2000sを使用したチャンク アップロード署名要求がサポートされるようになりました。	SnapVault、SnapLock、NFSv4、ブロックプロトコル、FlexVols、FlexClone、GX/スケールアウト、重複排除、ファイルクローン
2010sを使用したチャンク アップロード署名要求がサポートされるようになりました。	クラスタ ONTAP、インライン ストレージ効率化機能、NFSv4.1/pNFS、NVMe、RAID-TEC、FlexGroup ボリューム、ボリューム暗号化、AFF、Cloud Volumes ONTAP、QoS、FabricPool、Azure NetApp Files（ANF）、Google Cloud NetApp Volumes（GCNV）、All SAN Array（ASA）
2020sを使用したチャンク アップロード署名要求がサポートされるようになりました。	SnapMirror Business Continuity、FlexCache 、ONTAP S3、IPsec、Autonomous Ransomware Protection、SnapMirror in and out of ANF and GCNV、Amazon FSxN、ASAr2、NetApp AFX you are here

NetApp ONTAP パーソナリティ

長年にわたり、ONTAPはファイル、ブロック、オブジェクトを単一のシステムに統合した、単一の統合プラットフォームとして動作してきました。これにより、ONTAPはデータセンターにおけるスイスアーミーナイフのような存在——つまり、どんな要求にも応えられるプラットフォームとして位置付けられました。

しかし、アプリケーションが進化し、IT業界の一連の変化に伴いデータセンターの要件が変化するにつれて、特定の機能を実行できるプラットフォームへの需要が高まった。その結果、現在では ONTAP を利用するいく

つかの異なる方法が存在する。

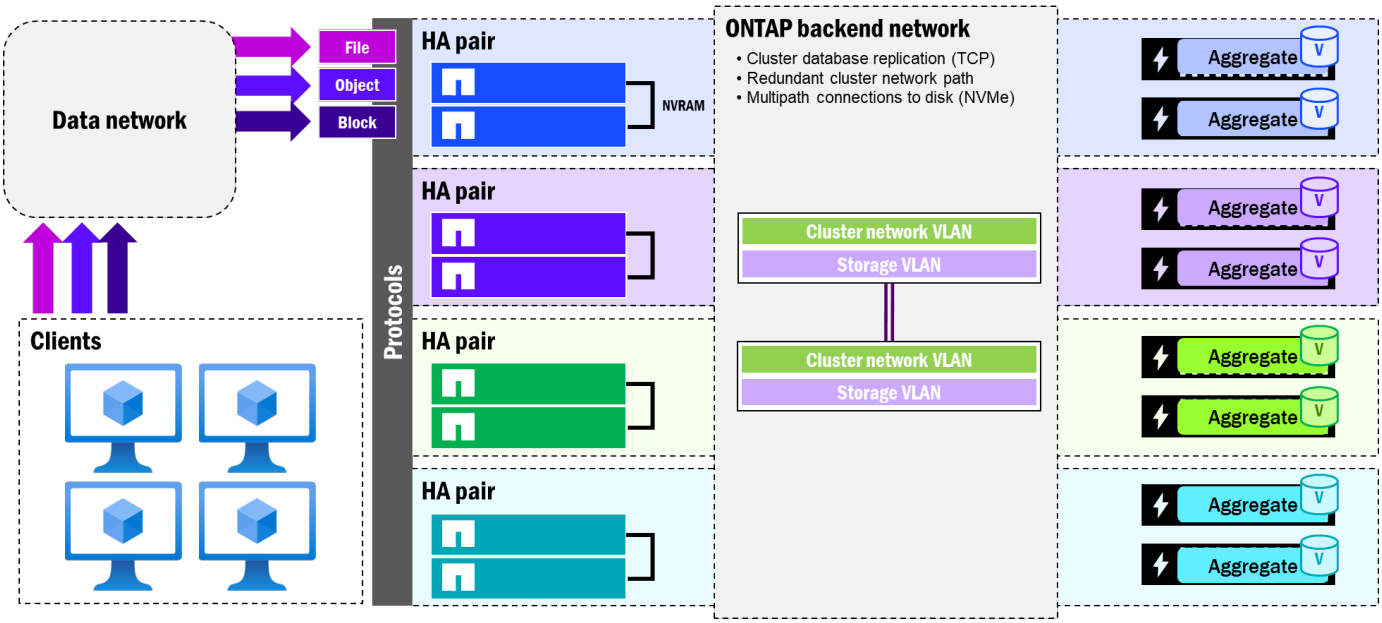
NetApp ONTAPパーソナリティ

ONTAPパーソナリティ	説明
ユニファイド ONTAP	これまでと同じONTAPであり、現在も活発に開発と改善が続けられています。
すべての SAN アレイ	iSCSI、FCP、FC/TCP 経由の NVMe のみをサポートし、アクティブ / アクティブ コントローラ機能と ASAr2 における分散型コンセプトを提供する ONTAP。
クラウド常駐 ONTAP	クラウド上で動作する ONTAP 。クラウドデータセンターに設置されたベアメタルシステム、または仮想化された ONTAP インスタンスのいずれか。
ディスアグリゲーテッド ONTAP/AFX	ONTAP は、高性能 NAS およびオブジェクト ワークロード向けに分離型アーキテクチャを使用しています。

統合 **ONTAP** アーキテクチャの概要

次の図は、統合 ONTAP の一般的なアーキテクチャを示しており、その下にすべてがどのように組み合わさるかの説明が記載されています。

一般的な**ONTAP**アーキテクチャ



ONTAP アーキテクチャの主な特徴：

- ファイル、オブジェクト、ブロックのサポート
- プロトコルはフロントエンド クライアント データ ネットワーク経由で提供されます
- 複数の独立したノードをまとめてクラスタ化できます

- 各ノードは、データおよび管理のユースケース向けに独立したフローティング IP アドレスを提供できます
- クラスタ化されたノードは、クラスタVLAN経由でNetApp提供のバックエンドスイッチに接続されます
- ノードは、ハードウェア障害や停電が発生した場合に備えて、HAペアとして提供されます
- HAペアには、書き込みを保護するためにレプリケートする直接接続されたNVRAMカードがあります
- 各ノードには少なくとも 1 つのアグリゲートが割り当てられ、ディスク総数の一部を所有します。
- フェイルオーバー時には、ノードのディスクはHAパートナー（かつHAパートナーのみ）に再割り当てされます。
- ディスクシェルフは通常、マルチパスケーブルを介してノードに直接接続されますが、ハイエンドシステムでは、同じバックエンドクラスタスイッチ上にストレージネットワークの概念が導入されています。
- ボリューム（FlexVolsおよびFlexGroupボリューム）は、データアクセス用のストレージへのエントリポイントを提供します

NetApp AFXとは

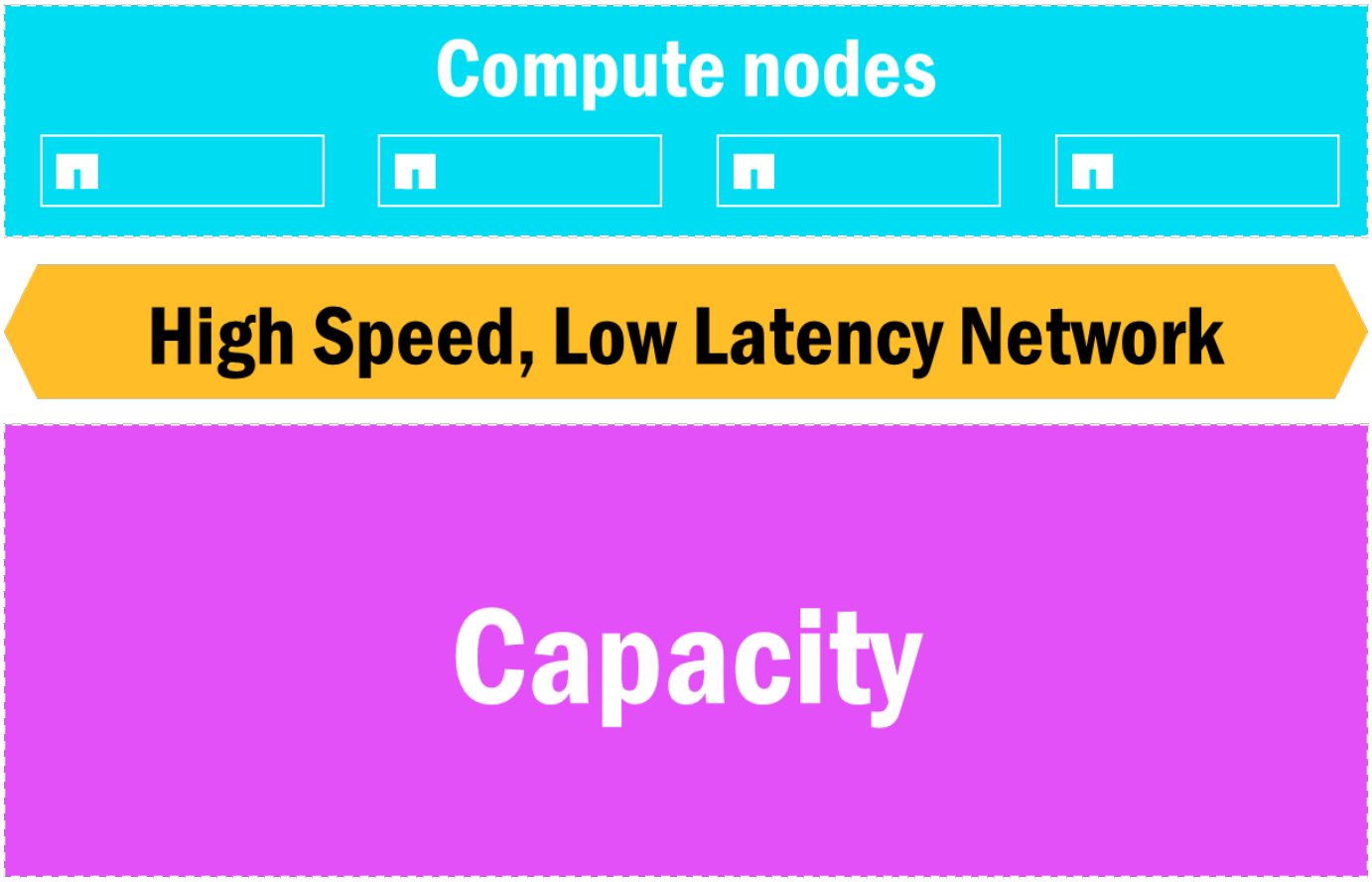
ここで留意すべき点は、NetApp AFF は引き続き ONTAP であるということです。

これは単に、ONTAPのメリットを活用するための別の方法です。Unified ONTAPまたはAll SAN Arrayシステムにインストールするのと同じイメージが、NetApp AFXでも使用されます。コードベースは同一ですが、システムの起動方法によって、実行されるコードパス、バックエンドストレージの表示方法、サポートされる機能やプロトコルが決まります。

NetApp AFXは、使い慣れた機能豊富なONTAPソフトウェアを提供しながら、NASおよびオブジェクト ワークロード向けの分離型アーキテクチャを提供します。分離型ONTAPとは、冗長ネットワーク スイッチと高速で低レイテンシのネットワークを介して、すべてのNetAppコントローラ ノードが同じ容量を認識するストレージ アーキテクチャを指します。このアプローチにより、コントローラ ノードとストレージ容量を互いに独立して拡張し、さまざまなハイパフォーマンス ワークロードのニーズにより的確に対応できるようになります。つまり、追加のパフォーマンスが必要な場合は、コントローラ ノードを追加するだけです。追加の容量が必要な場合は、シェルフ エンクロージャを追加します。これにより、ストレージ管理者は、より対費用効果の高いストレージ ソリューションをエンド ユーザーに提供できる柔軟性を得ることができます。

コントローラノードはそれぞれ独立してディスクを所有していないため、容量やパフォーマンスに制約のある物理アグリゲートも存在しません。その代わりに、容量はすべてのノードが相互作用できる共有モデルとして提示され、ONTAPが自動的に管理できます。

ディスアグリゲーテッド **ONTAP**



主要な用語と概念

以下は AFX に直接関連する用語です。ONTAP 固有の用語については、製品ドキュメントを参照してください。

"ONTAP 製品ドキュメント".

ディスアグリゲーテッド **ONTAP**

ONTAPを基盤とする新しいアーキテクチャを指し、コンピューティング能力と容量を互いに独立して拡張することが可能になります。「Disaggregated ONTAP」という用語は製品名ではなく、統合されたONTAPとNetApp AFXアーキテクチャを区別するための手段です。

NetApp AFX

NetApp AFXは、ディスアグリゲーテッドONTAPアーキテクチャの正式な製品名であり、NetApp Insight 2025で発表されました。

コンピューティング ノード

NetApp AFXの計算ノードは、ストレージコントローラノードを指します（ドキュメントでは同義語として使用されることがよくあります）。これらのノードにはオンボードディスクがなく、完全にモジュール化されており、分散型ONTAPアーキテクチャが提供する独立したスケールを可能にするように設計されています。

ストレージ可用性ゾーン（SAZ）は、NetApp AFXクラスタ内の単一の容量プールであり、すべてのディスクがすべてのノード間で共有されます。SAZは、共有容量、パフォーマンスの向上、グローバル重複排除などの機能を実現します。

NetApp AFXの新機能

このセクションでは、NetApp AFXの最新のアップデートについて説明します。新しいリリースごとに更新されます。最新情報については定期的にこのページをご確認ください。また、バージョンリリースノートも併せてご確認ください。

AFX向けのNetApp ONTAPの最新リリースの新機能

最新リリース：

ONTAP 9.19.1RC1（2026年5月時点）

NetApp AFXの新機能：

- グローバル重複排除
- 動的なストレージ効率
- 高度な先読み
- 32ノード対応
- 32PBのサポート
- FlexGroupボリュームあたり512個の構成ボリューム

バージョン履歴

version	日付	ドキュメントのバージョン履歴
バージョン1.0	2026年6月	初版リリース

NetApp AFX アーキテクチャと統合 ONTAP の違い

NetApp AFXは、統合型ONTAPとは大きく異なるアーキテクチャを採用しています。ストレージの提供方法、ノードとディスクの相互作用方法、および容量管理方法において。

以前は、統一されたONTAPアーキテクチャが、直接接続されたHAペアを介してファイル、オブジェクト、およびブロックデータのストレージを提供する方法の全体像を示しました。HAペアはそれぞれ独自のディスクセットを所有し、ディスクの集合体を介して物理容量を提供します。このセクションでは、統合されたONTAPとNetApp AFXアーキテクチャの主な違いについて、さらに詳しく説明します。

システムが NetApp AFX を実行しているかどうかを確認する方法

システムが NetApp AFX を実行しているかどうかを確認する主な方法は、次のコマンドを実行することです：

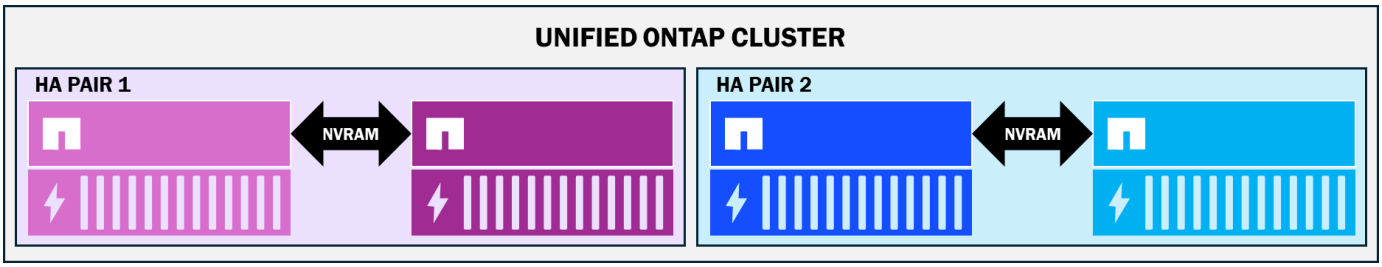
```
AFX::> node show -fields personality
node              personality
----------------- -----------
afx-01            AFX
afx-02            AFX
```

もう1つの手がかりは新しいストレージ可用性ゾーンですが、これもまたNetAppオールSANアレイ（ASA）で利用可能な概念です。そのコマンドを使えば、容量を確認できます。

```
AFX::> storage availability-zone show
                     Availability Zone Name: storage_availability_zone_0
                     Availability Zone UUID: 545cb59f-32e9-11f1-a2f5-
d039eabdd925
                                 Total Size: 69.59TB
                              Physical Used: 837.1GB
                       Physical Used Percent: 1%
                                  Available: 68.77TB
                              Metadata Used: 837.1GB
                  Log and Recovery Metadata: 834.6GB
                              Delayed Frees: 2.50GB
 Physical User Data Without Snapshot Copies: 17.24MB
  Logical User Data Without Snapshot Copies: 17.24MB
   Efficiency Ratio Without Snapshot Copies: 1.00:1
              Space Full Threshold Percent: 98%
        Space Nearly Full Threshold Percent: 95%
```

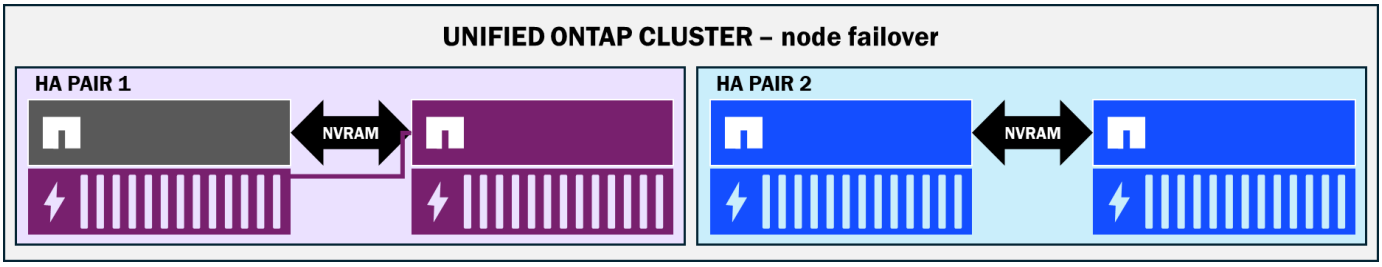
ノードとディスクの関係

統一された ONTAP アーキテクチャでは、読み取りと書き込みは特定のディスクのサブセットに振り分けられます。つまり、24 ノードのクラスタに 24 個のディスク シェルフ（ノードごとに 1 つのシェルフ）があったとしても、各ノードが直接アクセスできるのは一度に 1 つのディスク シェルフのみであり、クラスタで利用可能な容量とパフォーマンスが制限されることになります。



さらに、NVRAMはHAペア間で直接接続されているため、ノードは物理的に隣接している必要があり、フェイルオーバーのターゲットとしてより密接に結合されています。例えば、あるノードがパートナーノードにフェイルオーバーした場合、物理的にアクセスできるディスクは、HAペアドメイン内のディスクのみとなります。

HAフェイルオーバー中の統一ONTAPクラスタ

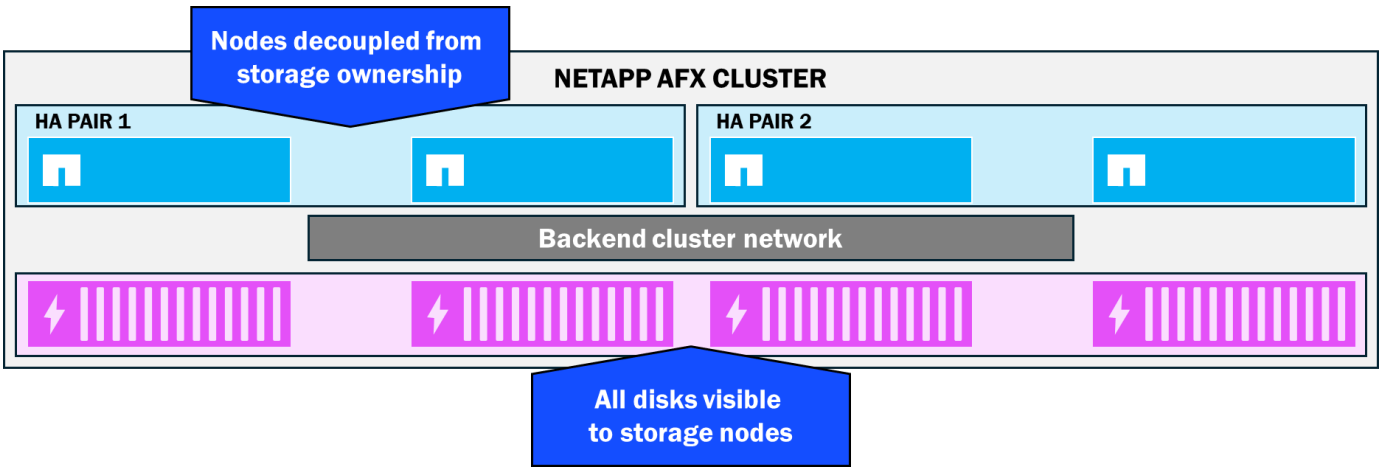


NetApp AFXでは、ディスクがコンピュートノードに提示される方法にいくつかの大きな変化があります。

すべてのディスクはすべてのストレージノードから参照可能—ディスクの所有権なし

NetApp AFXでは、ノードとシェルフがすべて同じバックエンドスイッチに接続されているため、ONTAPはディスクの全体的な可視性ドメインをスタック全体に拡張できます。その結果、どのノードも特定のディスクを所有しません。むしろ、すべてのディスクはStorage Availability Zoneと呼ばれる単一の容量プールに参加し、容量管理の簡素化とパフォーマンスの向上（利用可能なディスクが多いほど、利用可能なパフォーマンスも向上する）を実現します。

NetApp AFXストレージアベイラビリティゾーン

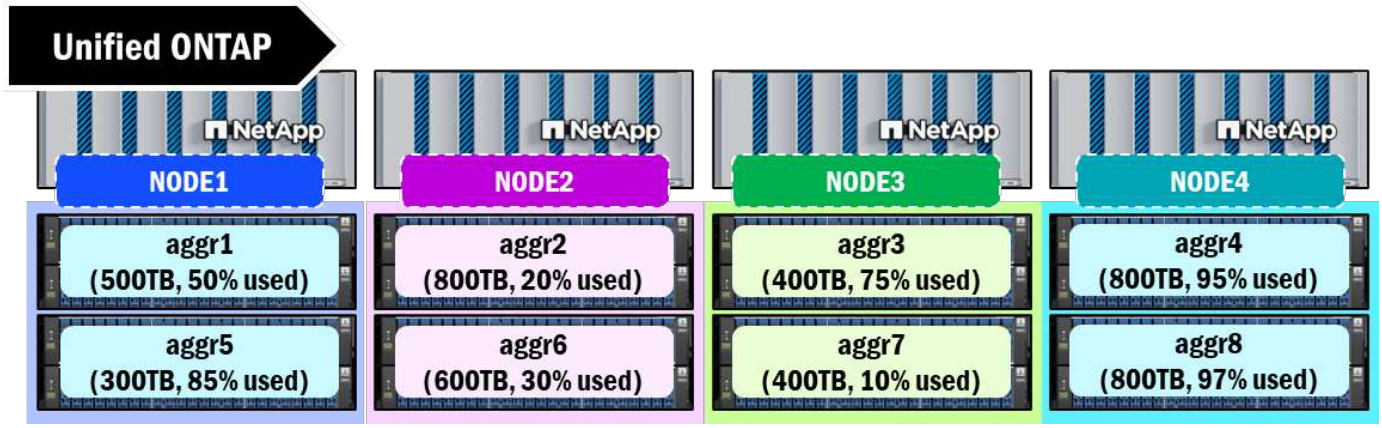


物理アグリゲートは不要

統合 ONTAP は、ディスクを RAID グループにまとめ、それらをアグリゲートと呼ばれる容量構造に結合します。このアグリゲートは、ストレージに対して物理的な容量を提示する方法であり、エンドユーザーにデータを提供するボリュームを作成するために利用可能なスペースの境界となります。各ノードには少なくとも 1 つのアグリゲートが割り当てられている必要があり、これらのアグリゲートの現在の制限は 800TB です。その制限に達すると、それ以上の書き込みのための空き容量はなくなります。

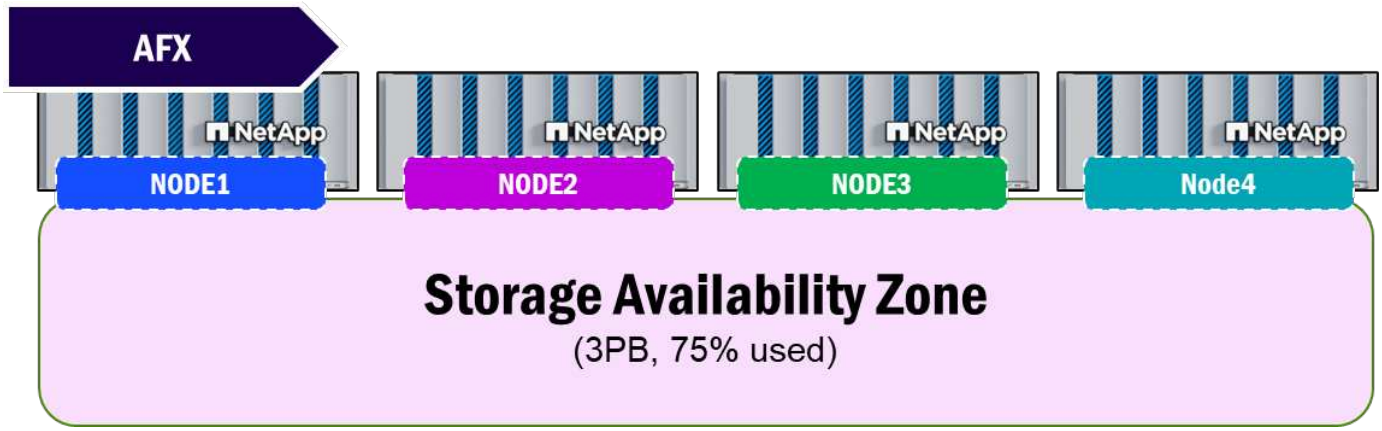
物理アグリゲートは、容量管理においていくつかの課題をもたらす可能性があります。ストレージ管理者は、クラスタノード間で容量のバランスを維持するために、ボリュームを手動で移動する必要が生じることがあります。これらの課題は、スケールアウトボリュームアーキテクチャ（FlexGroupボリュームなど）を活用する場合に、さらに大きくなる可能性があります。アグリゲートは、サイズ、ディスク数、ディスクタイプなども異なる場合があり、ノード間を移動する際にパフォーマンスの違いが生じることもあります。

統合ONTAP内のアグリゲート



NetApp AFXは、物理的なアグリゲートの概念を仮想化し、ONTAPで管理できるようにし、さらに新しいStorage Availability Zoneを介して、物理容量管理をノード単位の方法からクラスタ単位の方法へと移行します。この単一の容量プールにより、スペース管理において「見たままが得られる」というアプローチが可能になります。

NetApp AFXストレージアベイラビリティゾーン



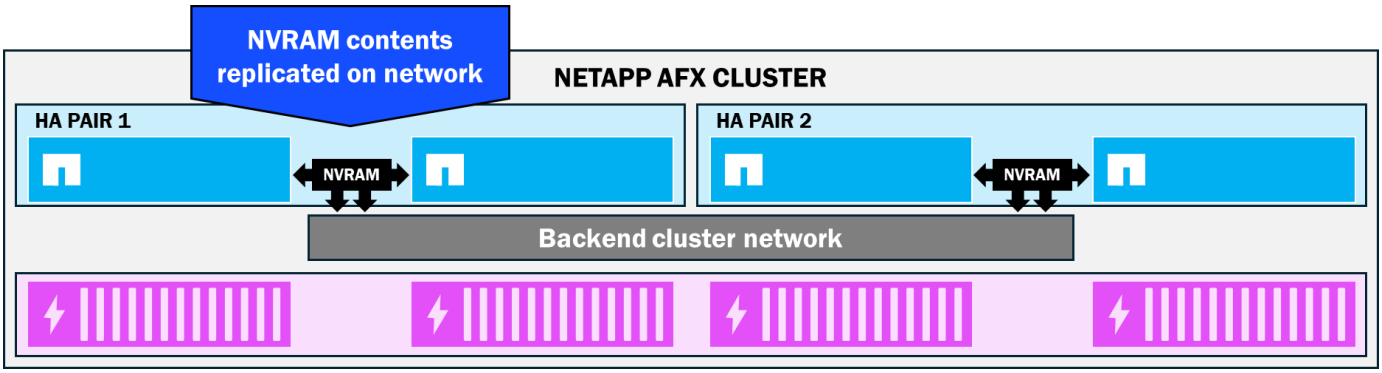
NVRAMが直接接続からスイッチド レプリケーションに移行

ONTAP は NVRAM をステージングとして使用し、クラスタへの受信書き込みを保護します。ONTAP クラスタ内の各ノードには、バッテリ バックアップ式 NVRAM カードがあります。クライアントからボリュームに書き込みが送信されると、最初に NVRAM に格納されます。NVRAM の内容は、NVRAM がいっぱいになるか、10 秒のタイマーが期限切れになると（いずれか早い方）、ディスクにフラッシュされます。これは整合性ポイントと呼ばれます。

NVRAM の内容は HA ペア間で常に複製されるため、ノード障害が発生した場合でも NVRAM の内容は存続ノードに保存されてディスクにコミットされるため、データの整合性の保護に役立ちます。

統合 ONTAP クラスタでは、HA ペア間の NVRAM カードが相互に直接接続されます。NetApp AFX は、NVRAM レプリケーションをバックエンド クラスタ ネットワークに移動します。その結果、HA パートナー ノードには、ノード間の距離に関するそれほど厳密な要件は課されません。その代わりに、HA ペアはイーサネットの最大距離まで分離することができます。

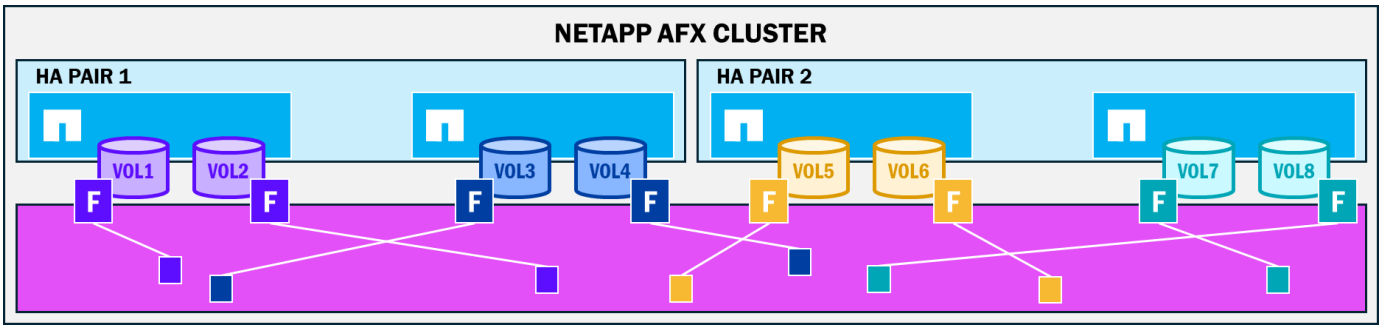
NetApp AFX NVRAM レプリケーション



アベイラビリティゾーン内の任意の（およびすべての）ディスクに書き込まれたデータ

NetApp AFXはディスク所有権の概念を排除し、物理アグリゲート構造をONTAPで管理される仮想化アプローチに移行します。これにより、クラスタ用に購入した容量はすべて、クラスタに接続されているノードで利用可能になります。AFXでは、ノード：ボリュームの所有権に関係なく、すべてのノードがStorage Availability Zone内のすべてのディスクに書き込むことができます。書き込みは依然としてNVRAMを経由するパスを通るため、ノードには依然としてボリューム所有権の概念がありますが、そのデータは利用可能な容量内のどこにでも格納される可能性があります。これは、より多くのディスクが単一のワークロードに参加できることを意味し、パフォーマンスの向上につながります。

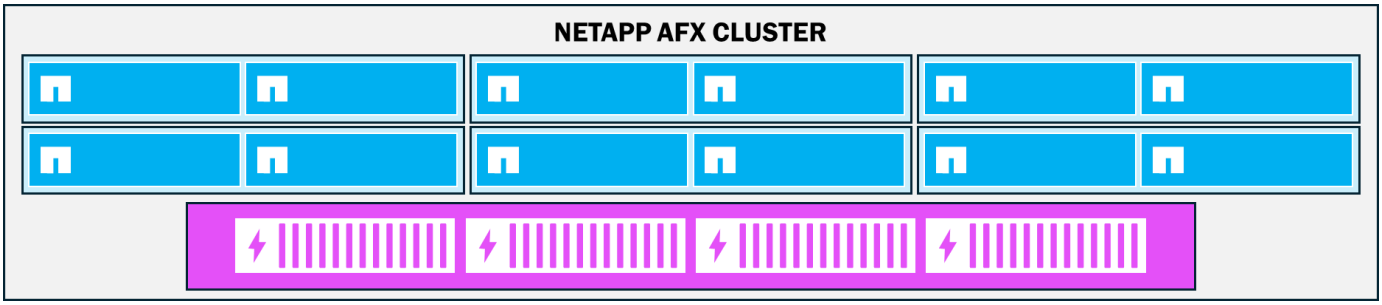
ストレージ可用性ゾーンにデータが格納される仕組み



容量ノードとコンピュート ノードの独立したスケーリング

ハードウェア リソースがNetApp AFXアーキテクチャで分離されているため、ノードに関連付けられたディスクを並行して追加する必要がなくなりました。クラスタでRAM、CPU、ネットワークスループットなどのパフォーマンス関連リソースが不足している場合は、ストレージノードのみをクラスタに追加すればよく、既存のStorage Availability Zoneを活用できます。逆に、容量が必要な場合は、シェルフを追加するだけで済みます。この柔軟性により、必要なリソースのみを購入できるため、過剰なプロビジョニングを回避できます。

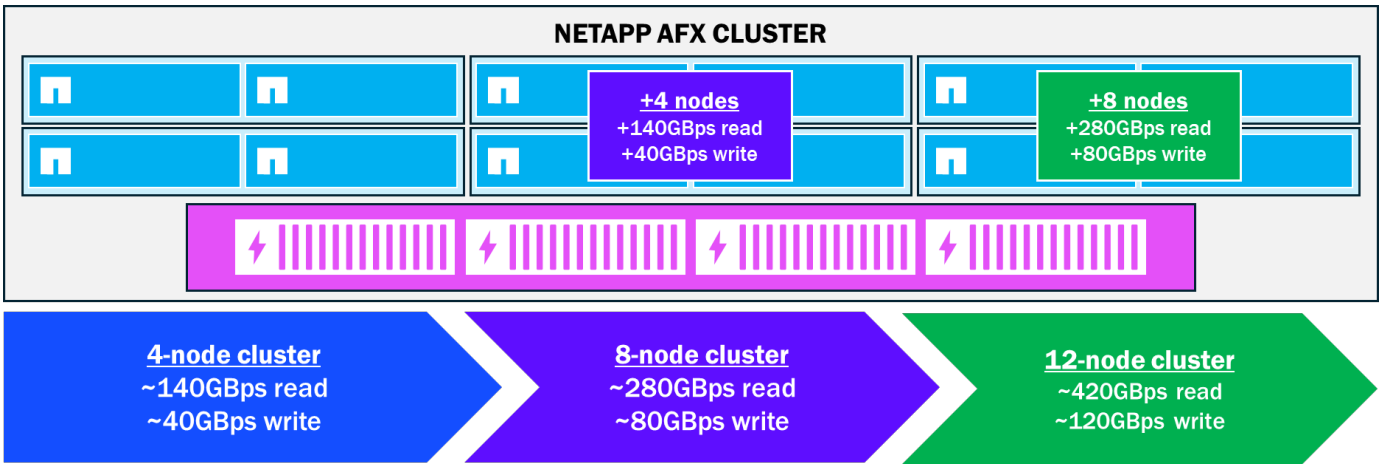
NetApp AFX – 独立スケール



ノード性能の線形スケーリング

AFX クラスタにノードが追加されると、より多くの CPU 、 RAM 、ネットワーク リソースがワークロードに導入されます。これらのリソースが環境に組み込まれると、パフォーマンスの向上は線形になります。次の図は、ノードの追加に伴ってパフォーマンスがどのように向上するかを示しています。

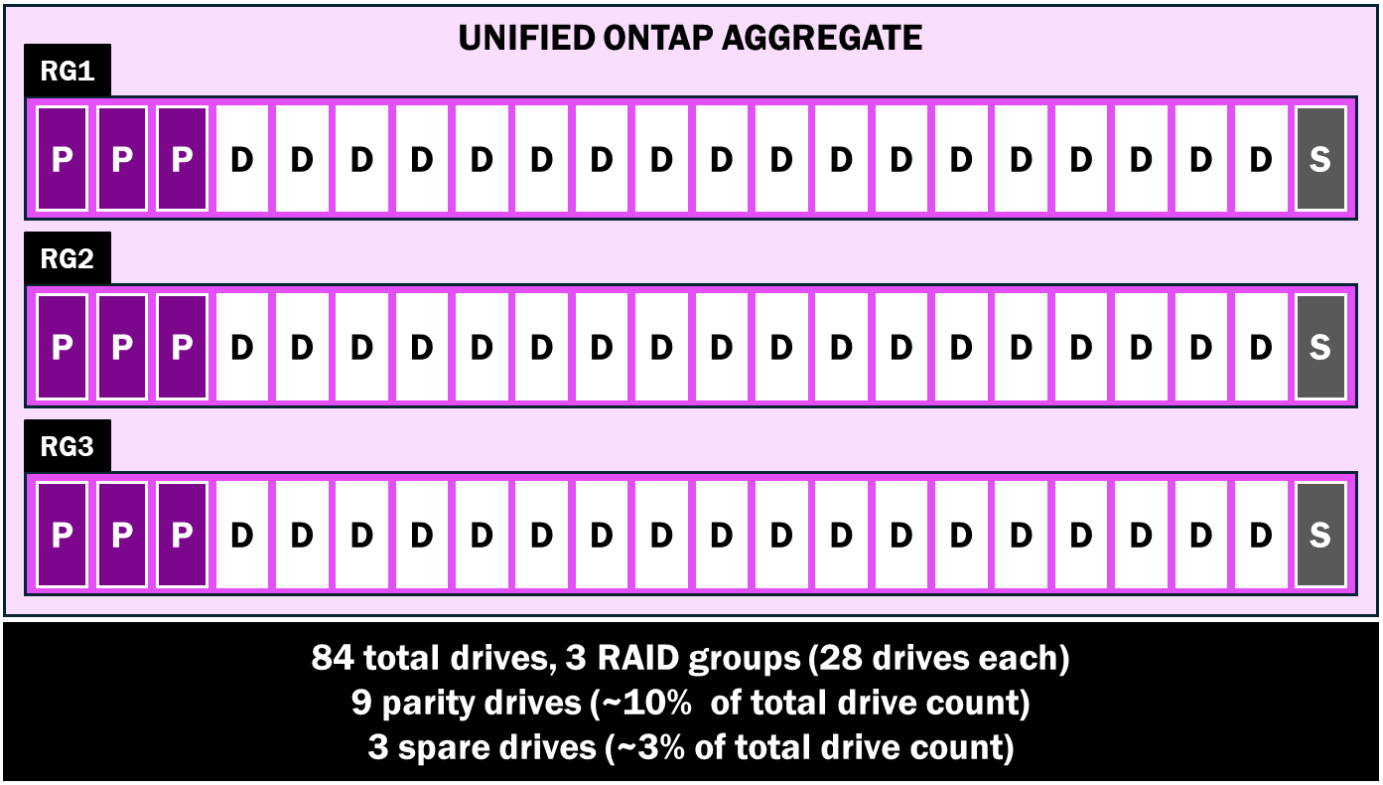
NetApp AFX ノードの追加による線形パフォーマンスの向上



RAIDグループを大きくし、パリティドライブの数を減らす

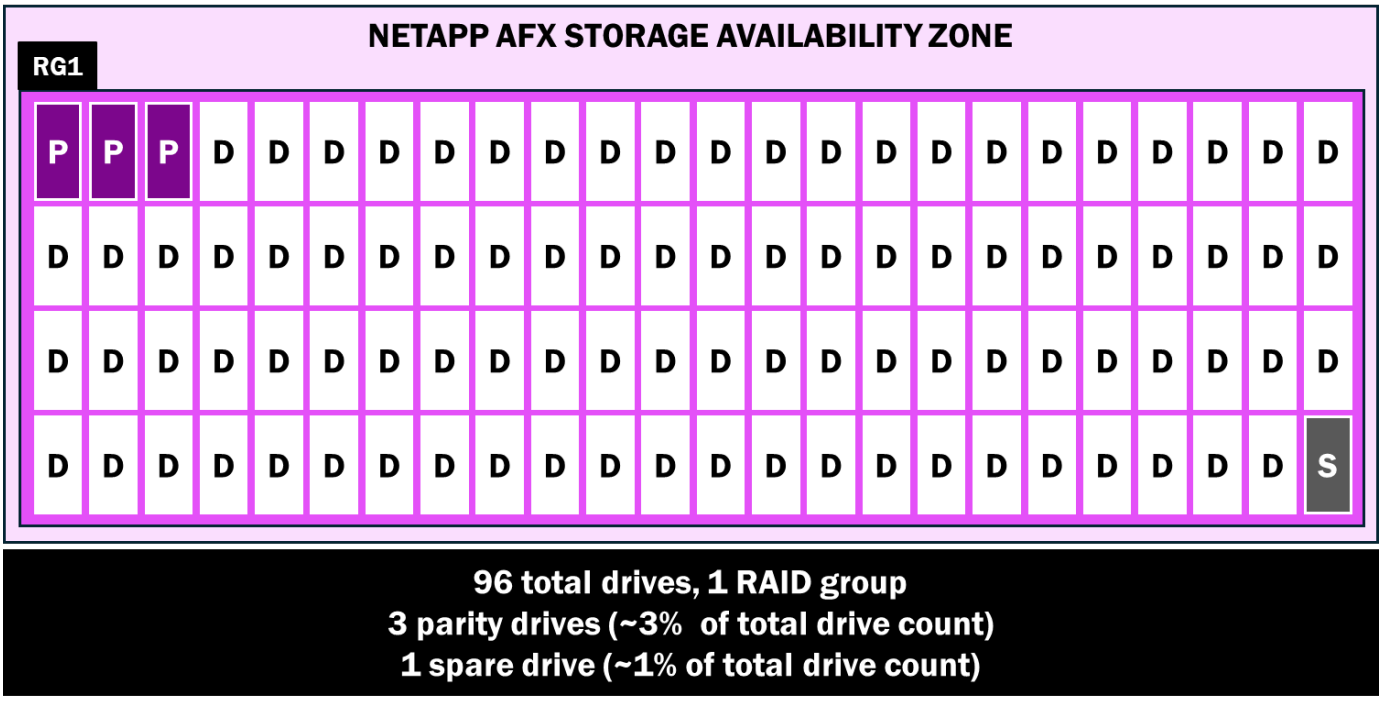
ONTAPは、RAIDグループ（特にRAID-TEC）を介してディスクのデータ保護とパフォーマンスを両立させます。RAID-TECは、ディスク障害発生時に三重パリティ保護を提供します。RAID-TECは、RAIDグループ内で最大3台のドライブが同時に故障しても耐えることができます。統合ONTAPでは、RAIDグループのディスク数は最大28台で、そのうち3台はパリティ用、1台は予備として予約されます。その結果、28台のドライブのうち24台がデータ処理/RAIDストライプに使用されます。

統一**ONTAP RAID**グループ



NetApp AFXは引き続きRAID-TECを活用しますが、必要なパリティドライブは3台、スペアドライブは1台のみでありながら、RAIDグループのサイズを96ドライブに拡張します。より大規模なRAIDグループは全体的なパフォーマンスを向上させますが、SSDの低い障害率、より多くのドライブセット全体にわたるより均等に分散された処理、およびNetApp AFXにおけるパリティからのデータドライブの再構築の改善の組み合わせにより、ドライブ障害のリスクは最小限に抑えられます。

NetApp AFX Storage Availability Zone RAIDグループ



以下の表は、統合型 ONTAP および NetApp AFX における 84 ディスクの使用可能な生容量の概算値を、ドラ

イブ サイズ別に示しています。

おおよその生容量比較、**84** 台のドライブ **– Unified ONTAP** および **NetApp AFX**

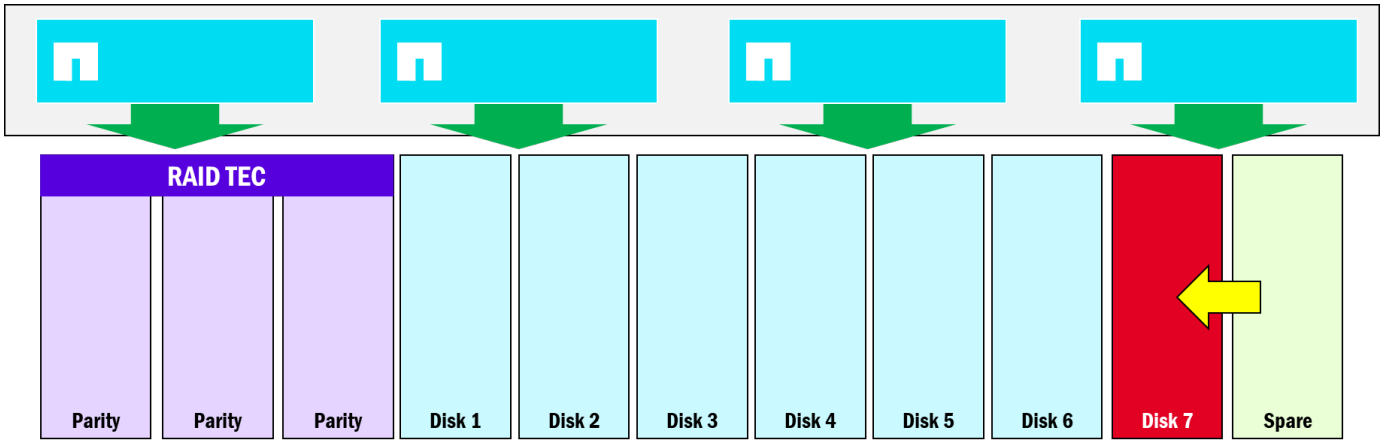
ドライブ容量	おおよその生容量（**Unified**）	概算生容量（**AFX**）
7.6 TB	~547.2TB	約608TB（+60.8TB）
15.3 TB	~1101.6TB	約1224TB（+122.4TB）
30.6 TB	~2203.2TB	約2448TB（+244.7TB）
60.1 TB	~4327.2TB	~4808TB（+480.8TB）

ディスク障害の再構築時間の短縮

統合 ONTAP では、各ノードがストレージ スタック内のディスクのサブセットを所有します。つまり、そのノードはそれらのディスクにのみ書き込みを行いますが、ディスク障害が発生した場合、ディスクの再構築は単一のノードによってのみ処理されます。

NetApp AFX はディスク所有権を必要としません。その結果、必要に応じて単一のノードからすべてのドライブに書き込みを行うことができます。つまり、ドライブをパリティから再構築する必要がある場合、クラスタ内のすべてのノードが参加するため、単一のノードが単独で行う場合よりも迅速にドライブの再構築を行うことができます。

NetApp AFX でのディスク再構築

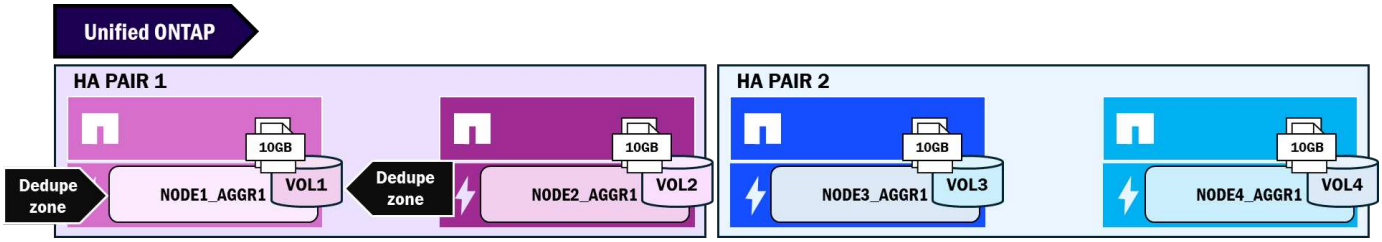


重複排除ドメイン

重複排除機能により、ストレージシステムはファイルシステム内の重複ブロックを検出し、単一のブロックへのポインタを作成することで、使用容量の総量を削減できます。統合ONTAPでは、重複排除は削減できるブロックに関して特定の境界に従います。これらの境界は、使用されている重複排除のタイプによって異なります。一般的に：

- ボリュームベースの重複排除 → ボリューム境界
- ボリューム間重複排除 → アグリゲート境界

統一 **ONTAP** 重複排除ドメイン



以下の表は、統合された ONTAP のさまざまなシナリオにおける重複データの容量挙動を示しています。ファイルコピーがノードやアグリゲート（つまり重複排除ドメイン）にまたがる場合、節約できる容量は減少します。

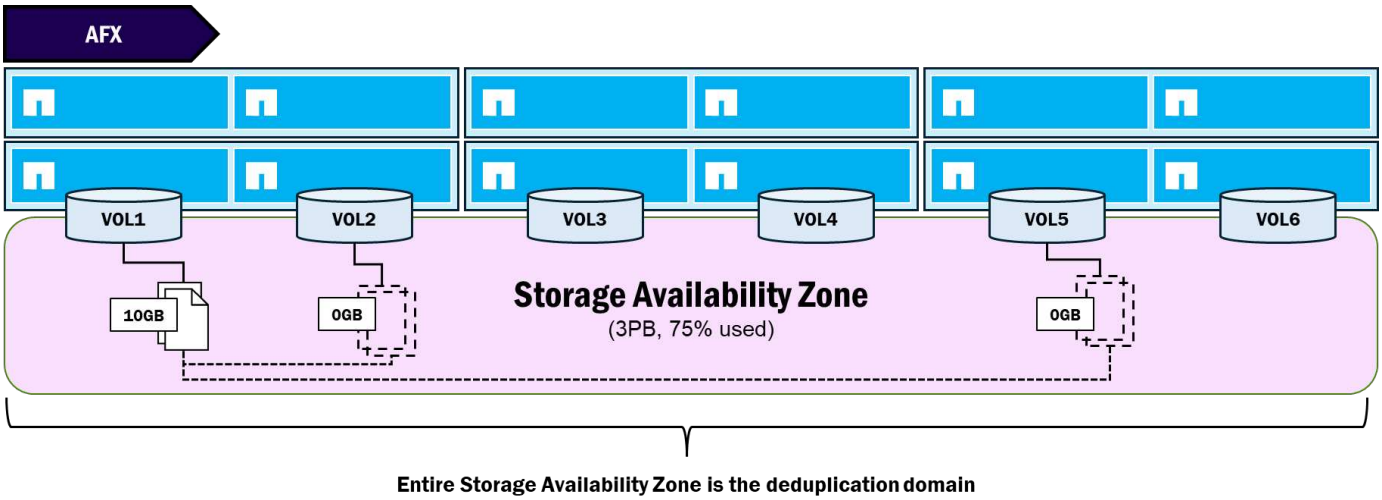
同一の**10GB**ファイルに対するさまざまなシナリオでの重複排除動作 **–** 統合**ONTAP**

シナリオ	使用済みスペース
同じ10GBファイルの4つのコピー、同じボリューム（ボリューム重複排除）	10 GB
同じ10GBファイルの4つのコピー、異なるボリューム、同じアグリゲート（ボリューム間重複排除が有効）	10 GB
同じ10GBファイルのコピーが4つ、4つの異なるボリューム、4つの異なるアグリゲート（ボリューム間重複排除が有効）	40 GB

NetApp AFXでは物理アグリゲートが削除され、容量管理が新しいStorage Availability Zoneに移行されるため、重複排除ドメインの境界も変更されます。AFXでは、重複排除ドメインはボリュームレベル（統合ONTAPと同様）および9.19.1より前のノード（アグリゲートではなく）にあります。

ONTAP 9.19.1以降、AFXはStorage Availability Zoneレベルでグローバル重複排除ドメインをサポートしているため、クラスタストレージプール内のすべての重複ブロックは同じように扱われます。

NetApp AFX – グローバル重複排除ドメイン（**ONTAP 9.19.1**）



以下の表は、NetApp AFXのさまざまなシナリオにおける重複データの容量動作を示しています。

同一の**10GB**ファイルに対するさまざまなシナリオでの重複排除動作 **– NetApp AFX**

シナリオ	使用済みスペース
同じ10GBファイルの4つのコピー、同じボリューム（ボリューム重複排除）	10GB （9.18.1） 10GB （9.19.1）
同じ10GBファイルの4つのコピー、異なるボリューム、同じノード（ボリューム間重複排除が有効）	10GB （9.18.1） 10GB （9.19.1）
同じ10GBファイルのコピーが4つ、4つの異なるボリューム、4つの異なるノード（ボリューム間重複排除が有効）	40GB（9.18.1）10GB（9.19.1）

削除された機能／サポート対象外となった機能

NetApp AFXは、ハイパフォーマンスNASおよびオブジェクトワークロード、特に（ただしこれに限定されない）AIトレーニングおよび推論領域のワークロード向けに設計されています。NetApp AFXの設計により、ONTAPの一部の機能を無効にする決定が行われました。

- ハイパフォーマンス NAS とオブジェクトに焦点を当てているため、ブロック ワークロードは NetApp AFX ソリューションから削除されました。FCP、iSCSI、NVMe のデータ プロトコルはサポートされておらず、ブロック プロトコルを追加する予定もありません。
- Disaggregated とは de-aggregated と同義であり、アグリゲート（少なくとも物理ストレージ管理の概念として）が削除されたことを意味します。物理アグリゲートを削除すると、ONTAP での容量管理が簡素化されるだけでなく、単一の容量プールを可能にするメカニズムも提供されます。
- アグリゲートが削除されるということは、アグリゲート固有の機能も削除されることを意味します。たとえば、MetroClusterは、サイトフェイルオーバー機能のために、アグリゲートレベルのミラーリングを活用しています。そのため、MetroClusterもNetApp AFXから削除されます。サイトフェイルオーバー機能は、代わりにONTAP 9.19.1GAで提供される新しいSnapMirror Active-Sync for NAS機能によって提供されます。
- FabricPoolと呼ばれるコールドデータ階層化機能も、アグリゲート固有であるため、現在NetApp AFXでは利用できません。
- 新しい容量アーキテクチャにより、NetApp AFXではコピーベースのボリューム移動も不要になりました。詳細については、[ゼロコピーボリューム移動]を参照してください。
- 機能の削除は、一部のCLI/GUI/REST APIの変更も意味するため、サポートされなくなった機能のコマンドやAPI呼び出しもすべて削除されます。
- ZAPI は現在 NetApp AFX では利用できません。
- 仮想化向けのNFSコピー オフロード（粒度データ分布のみのFlexGroupボリューム）

ONTAPの管理の変更

一般的に、NetApp AFX管理は、クラスターを管理するために使用されるメカニズムを変更するものではありません。管理者は引き続き、CLI、GUI、およびREST APIを利用してクラスターにログインし、構成を行うことができます。しかし、NetApp AFXは、ストレージ管理業務の実施方法の一部を改善する機会を提供しました。

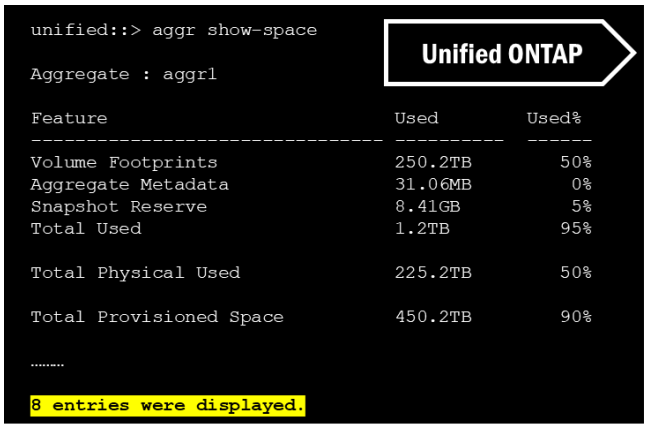
よりシンプルな容量管理

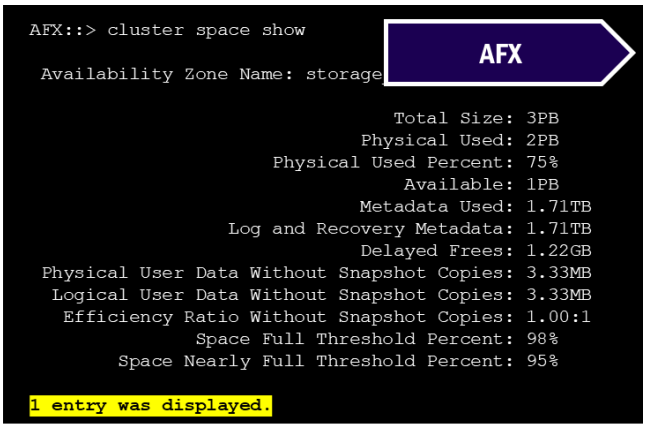
NetApp AFX Storage Availability Zoneは、管理エンドポイントをノードおよびアグリゲートベースのアプローチから、クラスタ全体で利用可能な単一の容量プールに削減します。ボリュームが拡張および縮小すると、ONTAPは自動的にStorage Availability Zoneとの間で容量を借用および返却します。

このため、ストレージ管理者は、最大24個のノードと場合によっては数百個のアグリゲートにわたる利用可能な空き容量の場所を特定し、管理する必要がなくなります。その代わりに、容量の管理と確認ができる場所は1箇所だけです。

例えば、統合された ONTAP の CLI では、クラスターの物理容量の合計情報を確認したい場合は、「`aggregate show-space`」を使用します。これにより、すべてのアグリゲートエントリが出力されます。NetApp AFX では、「`cluster space show`」というコマンドがあり、これを実行すると単一のストレージ可用性ゾーンのみが表示されます。

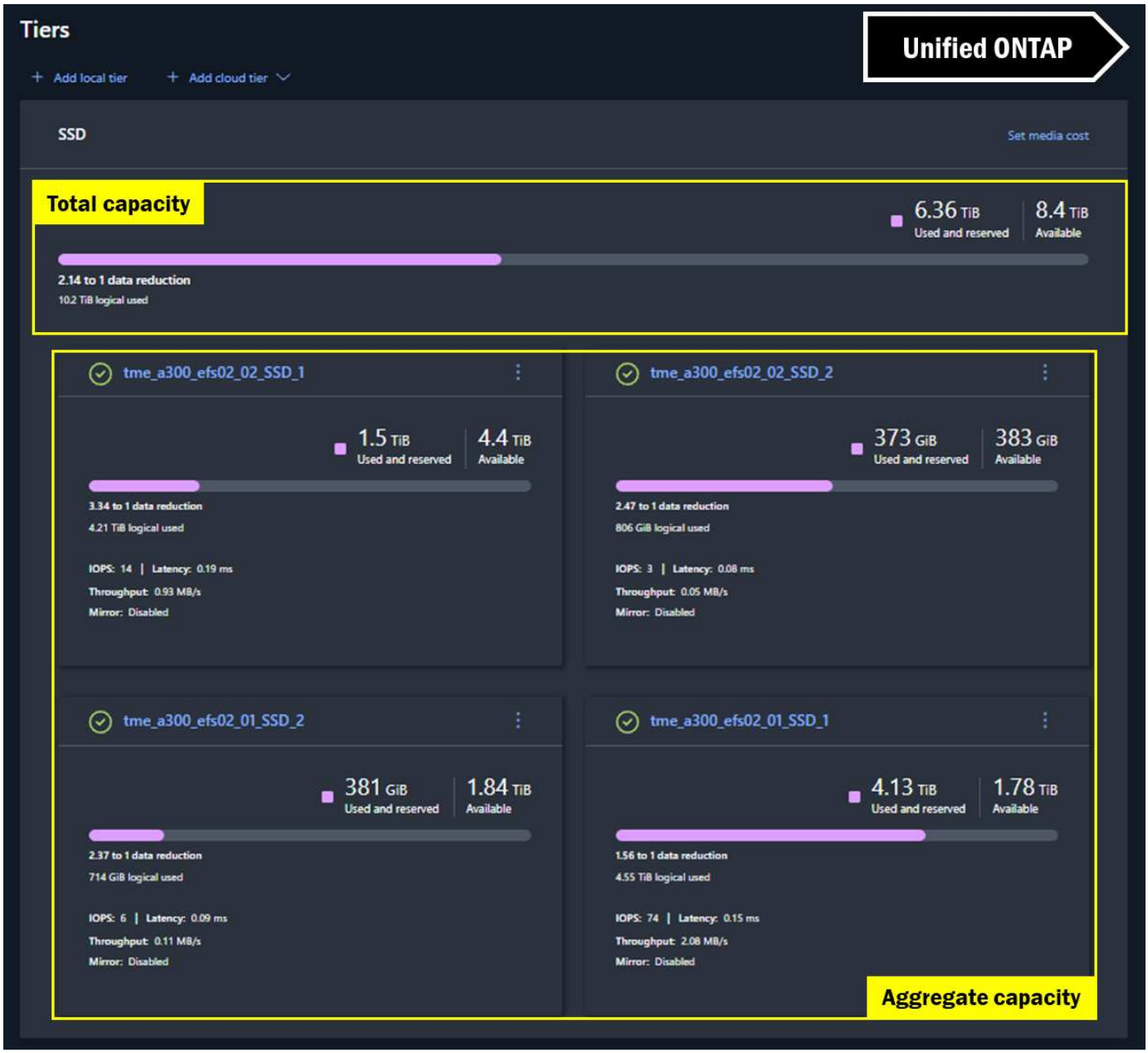
統合 **ONTAP** と **NetApp AFX** における容量 **CLI** コマンドの並列比較





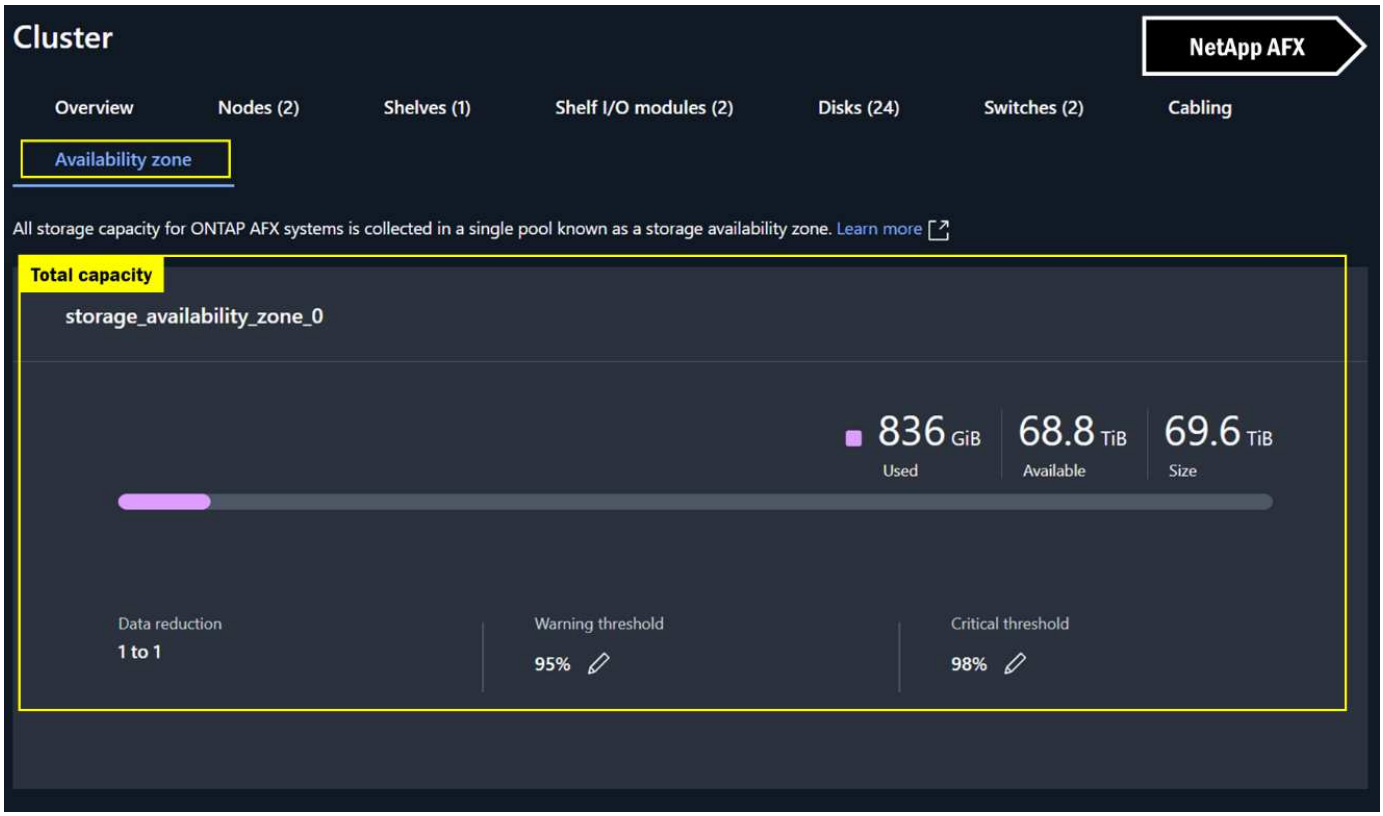
Unified ONTAP System Manager の GUI では、容量を示すために階層が使用されます。実際、GUI は合計値を算出してクラスター全体の容量を包括的に表示しようと試みていますが、それでもアグリゲート単位での全体的な使用状況が表示されます。

System Managerの容量ビュー **-** 統合**ONTAP**



NetApp AFX System Managerでは、クラスタスペースの表示はほぼ同じですが、アグリゲートがないため、追加の計算は不要です。表示されている容量が、実際に得られる容量です。

System Manager の容量ビュー **– NetApp AFX**

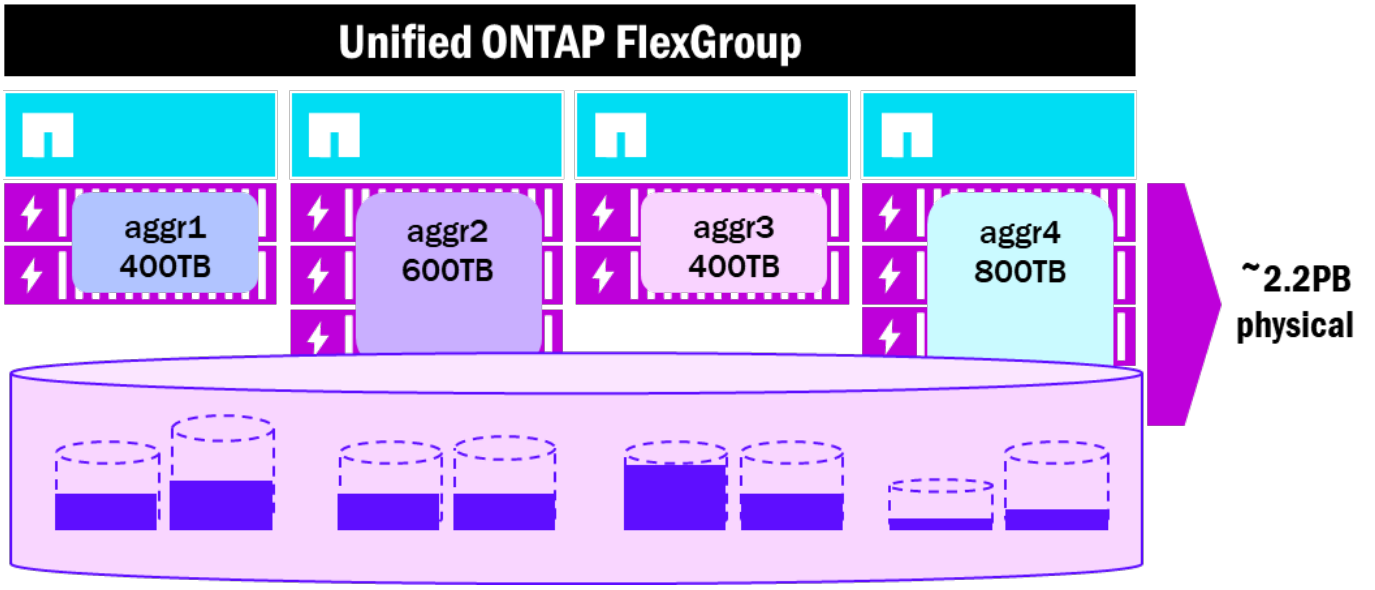


FlexGroup ボリューム管理の機能拡張

FlexGroupボリュームは、クラスター内の複数のノードとアグリゲートにまたがって作成された複数の基盤となるFlexVol構成ボリュームで構成され、NASクライアントに対して単一の大きな名前空間として提示されます。FlexGroupボリュームは、ハイパフォーマンスワークロードに対して、パフォーマンス、スケール、ロード バランシング、およびファイル数のメリットを提供します。ただし、ノードとアグリゲート間で連携するため、アグリゲートが提供する独立したファイルシステムにもそれぞれ独立した容量使用量と制限があるため、容量がいっぱいになり始めると、物理的な制約に直面することがあります。たとえば、FlexGroupボリューム構成要素を持つアグリゲートがクラスター内の他のアグリゲートよりも先にいっぱいになり始めると、FlexGroup全体が容量またはパフォーマンスの問題に直面する可能性があります。

その結果、ストレージ管理者は、基盤となるFlexGroupインフラストラクチャについて過度に心配することになり、環境の他の側面の維持への関心が低下する可能性があります。

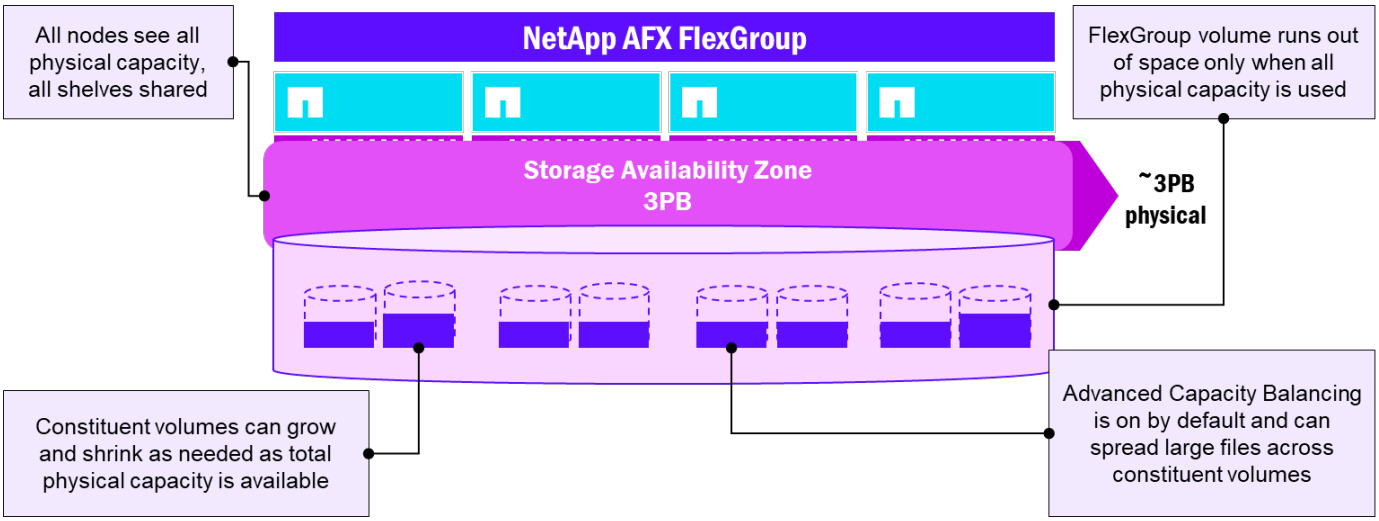
FlexGroupボリュームレイアウト **-** 統合**ONTAP**アグリゲート



NetApp AFXは単一のStorage Availability Zoneで容量を提示します。これは、FlexGroupボリュームの動作方法をより忠実に反映しています。サイズが異なる可能性のある複数の異なるアグリゲートにまたがる複数の構成ボリュームではなく、すべてのボリュームが同じ容量プールに存在するため、FlexGroupボリュームを使用する際の全体的な管理オーバーヘッドが大幅に簡素化されます。

さらに、AFXはデフォルトでFlexGroupボリュームのAdvanced Capacity Balancingを有効にし、ボリューム内の大きなファイルをより適切に分散させることができます。これにより、FlexGroupボリュームの構成要素は管理概念としての側面が薄れ、バックグラウンドで静かに機能するようになります。

FlexGroup ボリュームレイアウト **- NetApp AFX**



ストレージ管理タスクの自動化

NetApp AFX のストレージ可用性ゾーンでは、すべての容量がすべてのノード間で共有されます。ノードは引き続きボリュームを所有しますが、ONTAP は各ノードの容量使用量を、その時点での各ノードのニーズに基づいて容量を借用および解放することで自動的に管理します。つまり、ストレージ管理者は、使用可能なスペースのバランスを最適に取る方法について心配する必要がなくなります。

さらに、RAID グループ管理は ONTAP によって自動化されており、新しく追加されたディスクは、管理者の介入なしに既存または新規の RAID グループに追加されます。ONTAP は、データをコピーすることなく、ノ

ード間でのボリュームの移動も管理します。

ゼロコピーボリューム移動

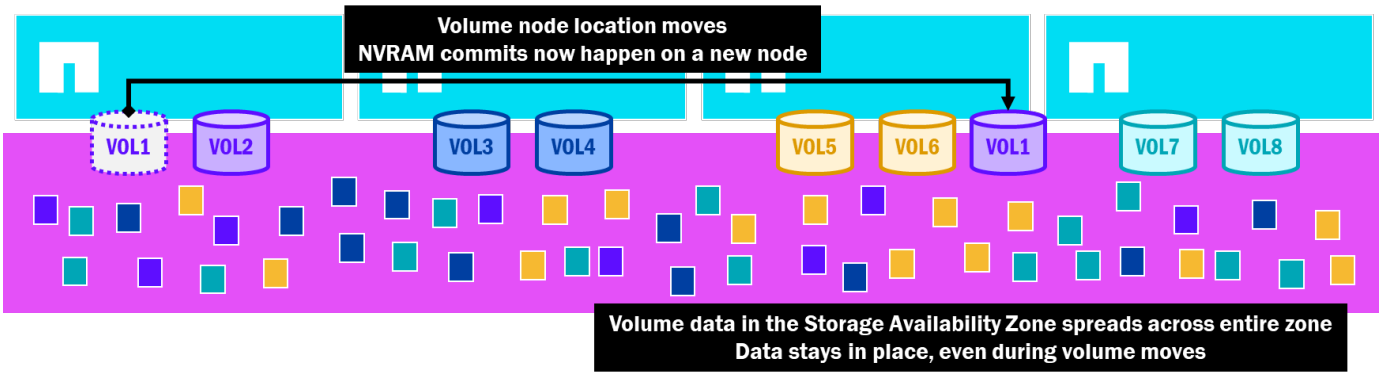
統合ONTAPは、クラスタ全体のパフォーマンスと容量使用状況を管理する方法として、ボリュームをノード間またはアグリゲート間で無停止で移動する方法を提供します。

ボリューム移動が開始されると、次のことが起こります：

- 指定されたデスティネーションアグリゲートに新しい空のボリュームが作成されます
- ボリュームメタデータ（ストレージ効率情報、ファイルハンドルなど）は、新しい宛先ボリュームに複製されます
- ボリュームデータは、SnapMirrorテクノロジを介してバックエンドクラスタネットワーク経由で宛先ボリュームにレプリケートされます。移動先のアグリゲートには移動に使用可能な空きスペースが必要です。使用可能な空きスペースがない場合、移動ジョブは失敗します
- ボリュームレプリケーションが再度実行され、両方のボリュームがデータの変更と整合していることを確認します
- カットオーバー プロセスが開始され、元のボリュームがオフラインになり、デスティネーション ボリュームがクライアントの新しいオリジン ボリュームとして昇格されます
- 切り替え中はクライアントI/Oに一時的な停止が発生しますが、再マウントは不要です

NetApp AFXでは、Storage Availability Zoneがすべての容量をすべてのノードに提供し、すべてのノードがそのプール内の任意のディスクに書き込むことができます。データが配置されると、ボリュームが移動されても、データは配置された場所に留まります。つまり、データのコピーは不要です。ボリューム移動プロセスは、SnapMirrorを介したデータのレプリケーションが不要である点を除いて、統合ONTAPと同じです。追加の容量は必要ありません。

NetApp AFX でのゼロコピーボリューム移動



軽量ボリュームモビリティにより、AFX はパフォーマンスや容量の制約なしに多くの管理タスクを自動化でき、これらのボリューム移動は、以下のトピックで説明する NetApp AFX が提供するいくつかの新機能で使用されます。

HA フェイルオーバー動作

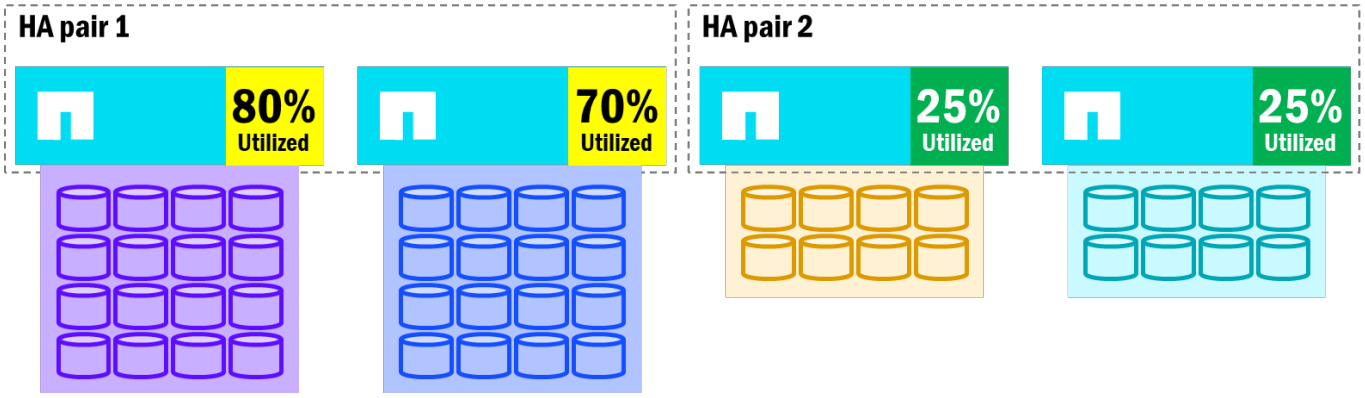
統合 ONTAP では、ノードがディスクとアグリゲートを所有し、データはボリュームを介して提供されます。書き込みは、ローカルノードの NVRAM を使用して、ノードが所有するディスクにフラッシュされます。ノードが再起動または障害が発生した場合、ONTAP は障害が発生したノードのリソースのテイクオーバーをトリガーし、ディスクとアグリゲートの所有権がパートナーノードに転送されます。ネットワークインターフェ

イスも IP スペース内のポートにフェイルオーバーされ、NVRAM の内容は HA ペア全体で常にレプリケートされているため、ノードは NVRAM の内容をフラッシュして、障害が発生したノードの書き込みをディスクにコミットします。その後、ノードのギブバックが発生するまで、存続しているノードが障害が発生したノードのアグリゲートとボリュームを所有します。つまり、フェイルオーバーの問題が解決されるまで、これらのボリュームへのすべてのトラフィック、および存続しているノードがすでに所有しているボリュームへのトラフィックは、単一のノードで処理されます。

初期の統合 ONTAP クラスタ導入の一環として、単一ノードがパートナーに過負荷をかけることを避けるために、フェイルオーバーを事前に計画しておくことを推奨します。それ自体が課題となります。なぜなら、どのボリュームがパフォーマンスの妨げになるかを予測するのは難しいからですが、無停止ボリューム移動やボリュームのサービス品質ポリシーなどの機能が緩和に役立ちます。

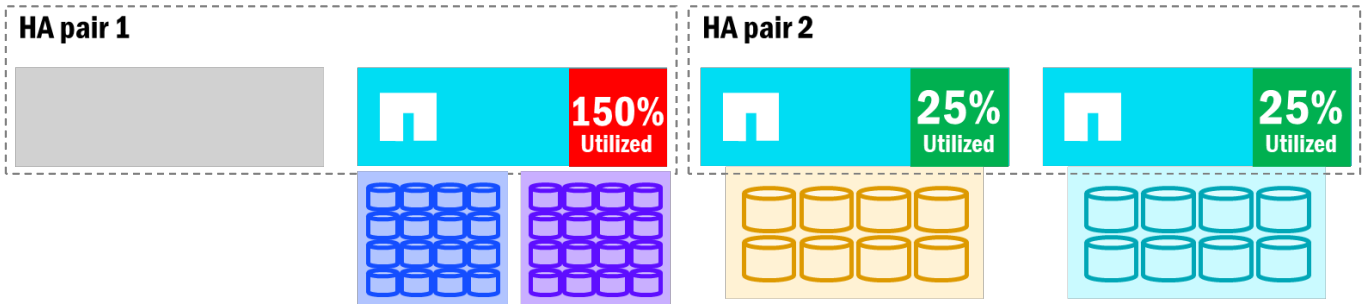
以下の画像は、統合された ONTAP クラスタでノード間のパフォーマンス バランスが不均一になる可能性があること、およびフェイルオーバーによって場合によってはパフォーマンスの低下が発生する可能性があることを示しています。

Unified ONTAP – ノード利用率の潜在的な不均衡



HA ペアのノードのボリューム数とパフォーマンス利用率のバランスが崩れると、ノードのフェイルオーバーは全体的なパフォーマンスに影響を与えます。なぜなら、生き残ったノードが、障害が発生したノードのすべてのボリュームを所有することになるからです。一方、クラスター内の他のノードには、追加の作業を引き受ける余地があるかもしれません。

統一**ONTAP –**フェイルオーバーがノード利用率に与える影響



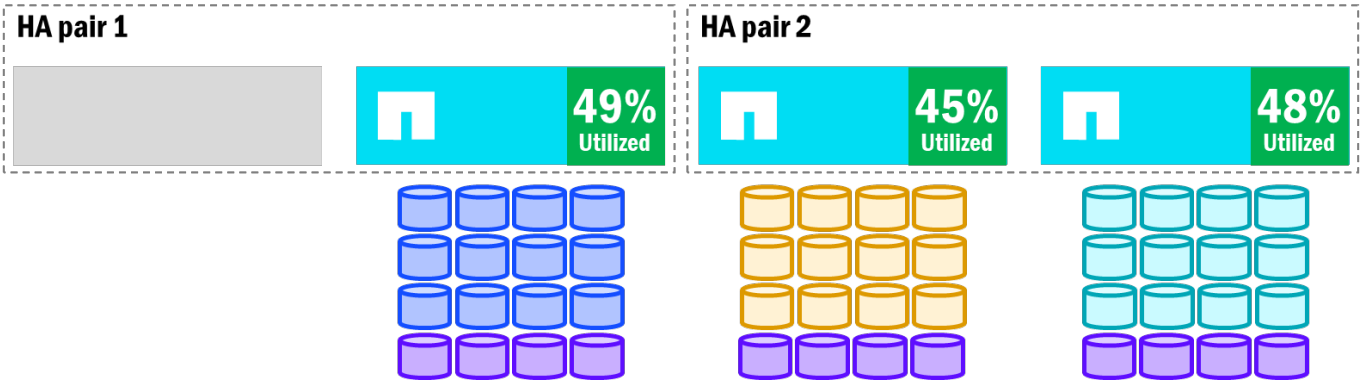
上記のように、HAパートナーが追加の作業を引き受けなければならない場合、過負荷状態になり、そのノード上のすべてのボリュームのパフォーマンスに影響を与える可能性があります。ボリュームの移動は状況の緩和に役立ちますが、これにはノード間でのコピーが必要であり（利用可能な空き容量が必要）、その所要時間はノードがフェイルバックするまでの時間を超える可能性があります。さらに、ボリュームを再配置しても、元のノードにフェイルバックすることはありません。その代わりに、移動先のノードにそのまま残ります。

NetApp AFXでは、ノードのフェイルオーバー時にいくつかの異なる動作が見られます。

- ノードはディスクを所有しておらず、物理アグリゲートも存在しないため、ノードのフェイルオーバーではこれらのリソースの転送は不要です。その代わりに、ネットワークインターフェイスとボリュームの所有権のみが他のノードに転送されます。
- NVRAMコミットは引き続き行われますが、直接接続ではなくHAネットワークを介して行われます。
- ボリュームがパートナー ノードへの初期フェイルオーバーを実行すると、AFXはクラスタ内の他の生存ノードにボリュームを再分配します。これは、ゼロコピー ボリューム移動によって可能になります。
- ノードが復旧すると、ボリュームは元のノードに戻ります。

NetApp AFXは既にクラスタ内のノード間でパフォーマンスのバランスを維持し、比較的均一な利用率を保つように設計されているため、フェイルオーバーが発生してボリュームが再バランスされると、クラスタ全体でノードの利用率はほぼ同じになるはずです。

NetApp AFX - フェイルオーバー後のボリューム再バランス



ノードの追加と削除

統合ONTAPとNetApp AFXの両方で、クラスタへのノードの追加と削除が可能です。ただし、アーキテクチャ上の違いがあるため、ノードの追加と削除のプロセスは若干異なります。

統合**ONTAP**でのノードの追加/削除

ユニファイド ONTAP では、ノードとディスクの所有権が直接結び付けられており、すべてのノードにディスクがいくつか存在し、少なくとも 1 つのアグリゲートが接続されている必要があることはすでに学習しました。これを踏まえると、追加と削除に関しては次のことが当てはまります。

- 統合されたONTAPでのノードの追加には追加の手順は必要ありませんが、すべてのノード（新しいノードを含む）でバランスの取れたパフォーマンスを実現するには、ボリュームを新しいノードに移動する必要があります。これには、既存のボリュームとそのワークロードの事前分析、移動するボリュームの決定、そして実際のボリューム移動が必要となります。そして、その移動には、バックエンドクラスタネットワーク全体にわたるデータのコピーが必要となります。
- 統合ONTAPでのノードの削除では、ノード上の既存のボリュームを手動で退避させる必要があります。つまり、均一なパフォーマンスを維持するために、どのノードがどのボリュームをホストできるかを特定し、それらのボリュームを移動するための十分な空き容量を確保する必要があります。空き容量が不足している場合は、クラスタ内でワークロードを少し再配置するために、追加のボリューム移動が必要になる場合があります。ノードの削除はHAペアの削除も伴うため、作業量は2倍になります。ノードはディスクを所有しているため、それらのノードについてもディスク全体の再初期化が必要となります。これらの要素はすべて、本来比較的簡単なはずの作業に時間と労力を追加することになります。

NetApp AFXでのノードの追加/削除

また、NetApp AFXは標準のノードとディスクの所有権を利用せず、物理アグリゲートを使用してクラスタに容量を提供しないことも学びました。そのため、ノードの追加と削除の動作は若干異なります。

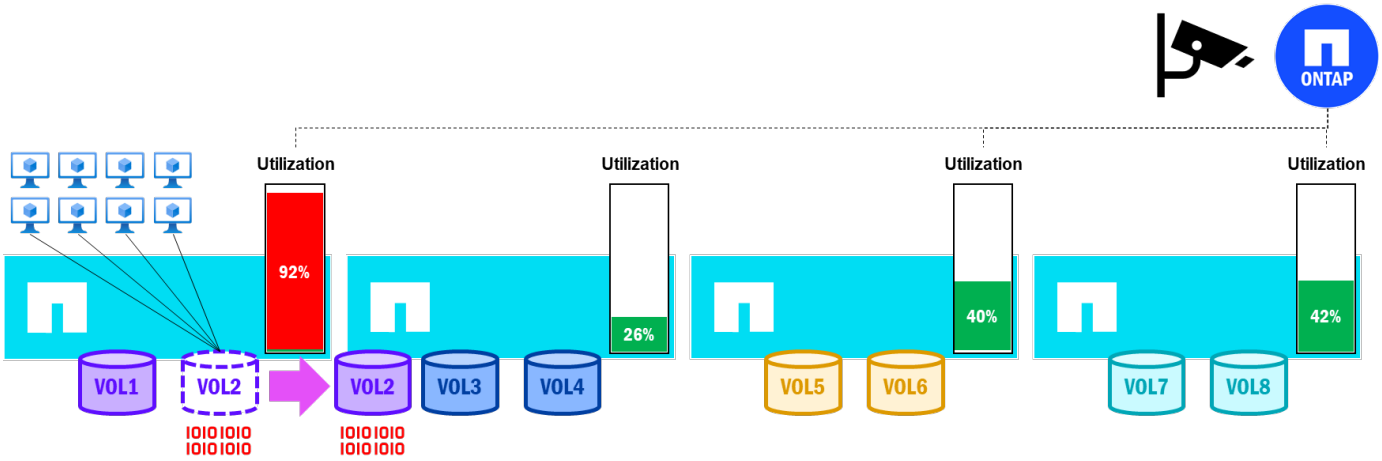
- NetApp AFXでのノード追加では、事前のボリューム分析は不要であり、各ノードのボリュームが均等になるようにするための管理上の介入も不要です。その代わり、ONTAPは新しく追加されたノード間でボリューム数を自動的にバランス調整し、比較的均一なパフォーマンスプロファイルを維持します。ONTAPはボリュームをコピーすることなくノード間で自動的に移動させるため、クラスターにノードを追加する際に必要な時間、容量、労力を削減できます。
- NetApp AFXでのノードの削除も、手動による介入をほとんど、あるいは全く必要としません。ノードが削除対象としてタグ付けされると、ONTAPは削除されるノードからデータを解放するために、ボリュームをノード間で自動的に移動します（コピーは行いません）。また、ノードが所有するディスクが存在しないため、ノードを削除した後にディスクを再初期化する必要はありません。これにより、AFXのノードはモジュール構造となり、容易にスケールアップまたはスケールダウンが可能になります。

目標達成ベースのボリューム移動

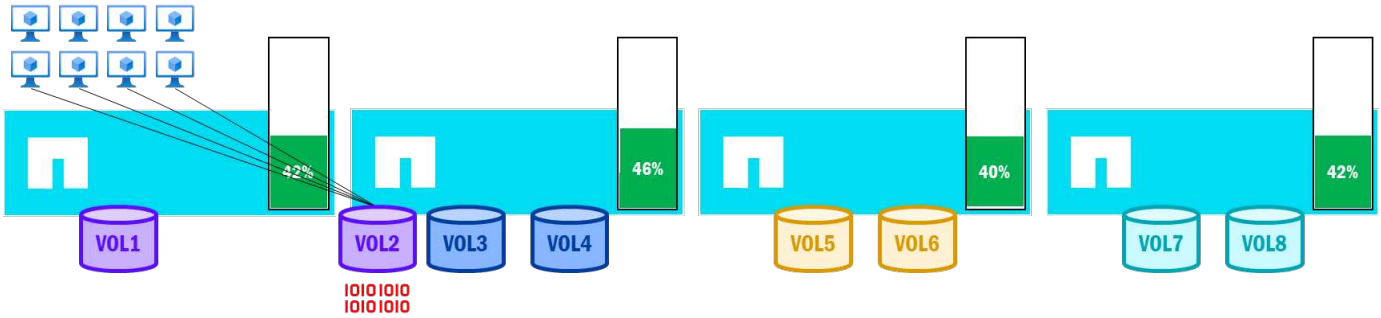
NetApp AFXのゼロコピーボリューム移動機能により、データのコピーを行わずに必要に応じてボリュームのバランス調整が可能となり、迅速な処理と追加容量を必要としない運用を実現します。これは、ボリューム移動がONTAPクラスタで利用可能な自動ロード バランシングのより大きな部分を占めることができることを意味します。ボリュームの移動にほとんどコストがかからなくなったため、ONTAPはこの貴重なツールを活用して、目標達成ベースのボリュームのロード バランシングなどの機能を組み込むことができます。

NetApp AFX で ONTAP 9.18.1 以降を実行している場合、ノード、 HA ペア、およびボリュームの使用率が継続的に監視され、パフォーマンス データが収集および分析されます。ノードの使用率が定義されたしきい値を超えた場合、 ONTAP はクラスタ全体のパフォーマンスのバランスを保つために、使用率の低いノードに移動するボリュームを自動的に選択します。

NetApp AFXにおけるパフォーマンス重視のボリューム移動 – 高い利用率がボリューム移動をトリガーする



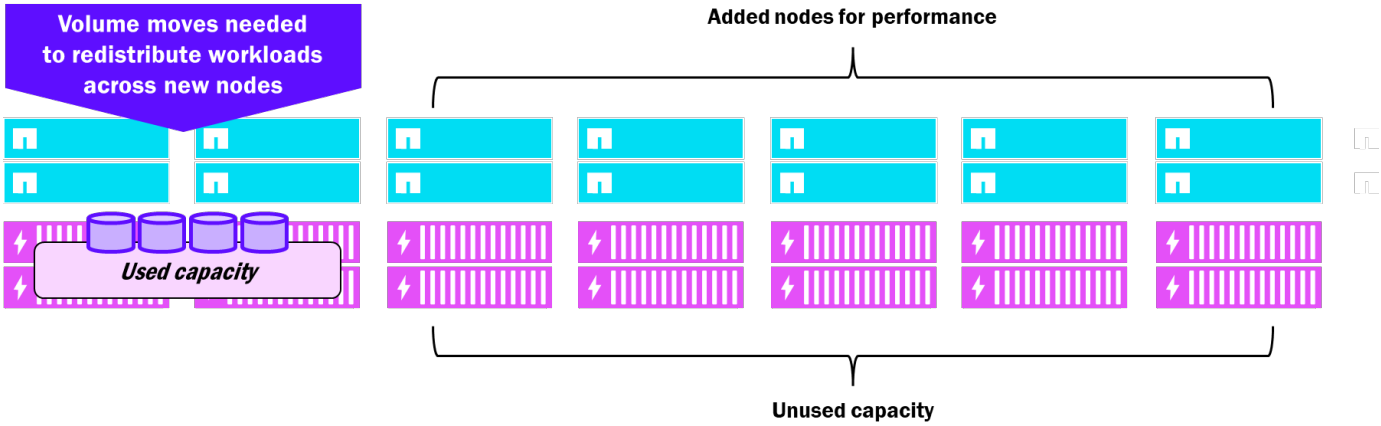
NetApp AFXにおけるパフォーマンス重視のボリューム移動 – ボリューム移動後のバランスの取れたノード利用率



クラスタの規模と拡張

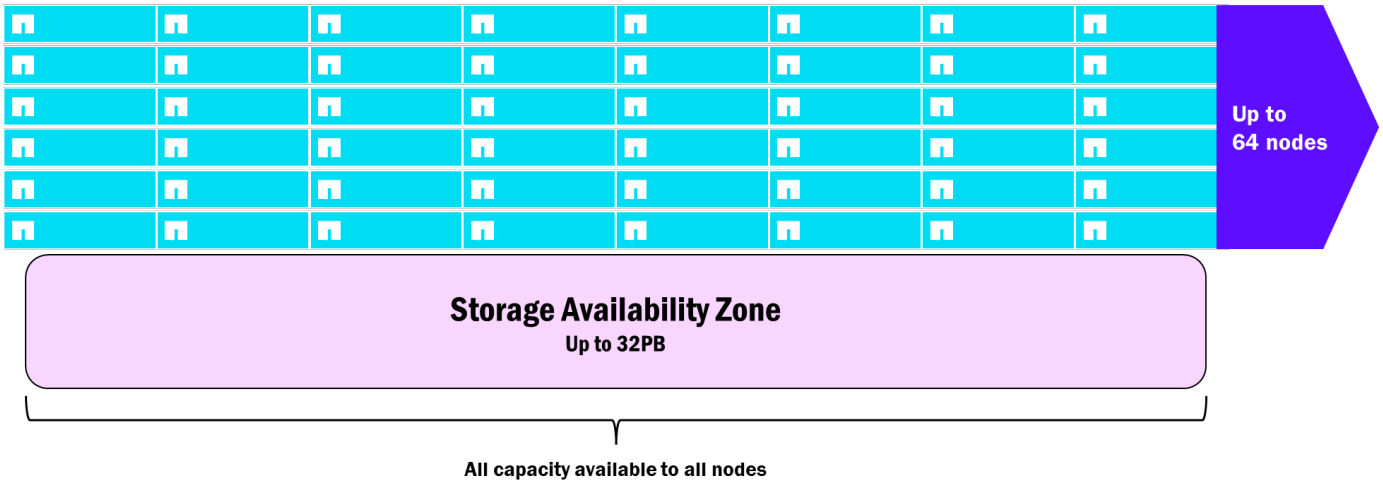
統合ONTAPクラスタは最大24ノードをサポートし、追加される各ノードにはディスク（システム機能とデータサービスの両方のため）も追加する必要があります。ディスクシェルフはクラスタに追加できますが、クラスタの規模が24ノードであっても、常に単一のHAペアに接続され、単一のノードのみが所有します。これは、パフォーマンスのみが求められる場合でもクラスタに容量が追加されることを意味し、パフォーマンスの向上は主に新しいノードが所有する特定のディスクセットに限定されます。その結果、必ずしも必要ではない余剰容量を抱えてしまう可能性があります。

Unified ONTAP – スケールに関する考慮事項を追加



NetApp AFXは、より大規模なクラスター構成に対応しています。バージョン9.19.1以降、AFXクラスターは1つのクラスター内で最大32ノードまで構成できるようになりました。すべてのノードがすべてのディスクを認識してアクセスできるため、パフォーマンスと容量（ONTAP 9.19.1時点で最大32PB）を共有できるので、リソースが無駄になることはありません。ボリューム移動にはコピーは必要ないため、ONTAPはボリュームを新しく追加されたノードに自動的に移動してノードの利用率を均等に分散させることができ、一方で容量はStorage Availability Zoneを介して均等に分散されます。

NetApp AFX – スケールに関する追加検討事項



ルートボリュームの変更

NetApp ONTAPでは、各ノードにルートボリュームが割り当てられます。このボリュームは、ログファイル、ブートイメージ、コアファイル、クラスタデータベースなど、システム固有のファイルや機能に使用されます。

統合ONTAPでは、これらのルートボリュームは物理ルートアグリゲート上に存在していました。ルートアグリゲートが使用する容量を削減するため、Advanced Disk Partitioning（ADP）を使用して、データドライブのパーティションをまたいでルートアグリゲートが作成されました。

NetApp AFXは物理アグリゲートを排除するため、ルートアグリゲートやADPを使用する必要がなくなります。ルートボリュームは依然として概念として存在しますが、現在は容量プールの仮想化領域に存在し、追加の設定は不要です。さらに、ルートボリュームの機能も変更されます。ブートイメージと複製されたクラスタデータベースは、ストレージ スタックから移動され、各AFXノードに搭載されているオンボードブートメディアに配置されます。これにより、ストレージ スタックへのアクセスが失われても、ノードは起動してクラスタの適格性を維持できるため、トラブルシューティングの複雑さが軽減されます。

オンボード ブート メディア

NetApp AFXノードは、オンボードのブートメディアとして、約3.8TBの容量を持つNVMe接続のM.2デバイスを活用します。これらのブートデバイスには、ストレージエンクロージャとは別にブートイメージファイルと複製されたデータベースが含まれており、ディスクアクセスに問題が発生した場合に冗長性を高めます。ブートメディアに障害が発生した場合、ノードはHAパートナーによって引き継がれ、ブートメディアを交換できます。交換後、新しいONTAPイメージはストレージ管理者によってデバイスにロードされ、ONTAPがクラスタデータベースを自動的に再構築し、完全な機能を復元します。

Performance

NetApp AFXは、パフォーマンスと拡張性を念頭に置いて設計されており、特に高い読み書きスループットを必要とするワークロード向けに特化しており、シンプルで線形的な拡張性を提供します。

ノードごとのパフォーマンス

各NetApp AFXストレージ ノードは、読み取りと書き込みに対して特定のスループット量を提供します。ノードがクラスタに追加されると、パフォーマンスが線形的に向上します。これについては、本書の「ノード パフォーマンスの線形スケーリング」のセクションで説明しています。

現在、ノードの種類は"AFX 1K"で、読み取りと書き込みのスループットは、おおよそ以下の値となります。新しいハードウェアがNetApp AFXで利用可能になると、これらの制限は変更される可能性があります。注：以下の「ベンチマーク結果」セクションに示すように、複数のクライアントが複数のファイルを読み書きすることで、最大のパフォーマンスが得られました。

ノードごとのパフォーマンス推定値

ノード タイプ	読み取りパフォーマンス最大	書き込みパフォーマンス最大
AFX 1K	~35GB/s	~10GB/s

最新のパフォーマンス予測については、NetApp営業チームにお問い合わせください。

シェルフごとのパフォーマンス

各シェルフには、16個の100GBイーサネットポートを備えた高性能シェルフモジュールが搭載されており、RoCEv2通信を利用して、クラスタ内のコンピューティングノードとの間で高帯域幅のストレージ通信を実現します。他の物理的な資源と同様に、これらのシェルフにも達成可能な最大値があります。特にNetApp AFXは、同じディスクセットを指す複数のノードを提示することができます。以下の表は、TLCおよびQLCドライブの場合の、単一シェルフにおける推定最大読み取りおよび書き込み性能を示しています。TLCとQLCの違いに関する詳細については、"TLCとQLC"を参照してください。

シェルフごとのパフォーマンス予測

シェルフ モジュール タイプ	読み取りパフォーマンス最大	書き込みパフォーマンス最大
NSM 140	140GB/s（TLCおよびQLC）	70GB/s TLC 35GB/s QLC

最新のパフォーマンス予測については、NetApp営業チームにお問い合わせください。

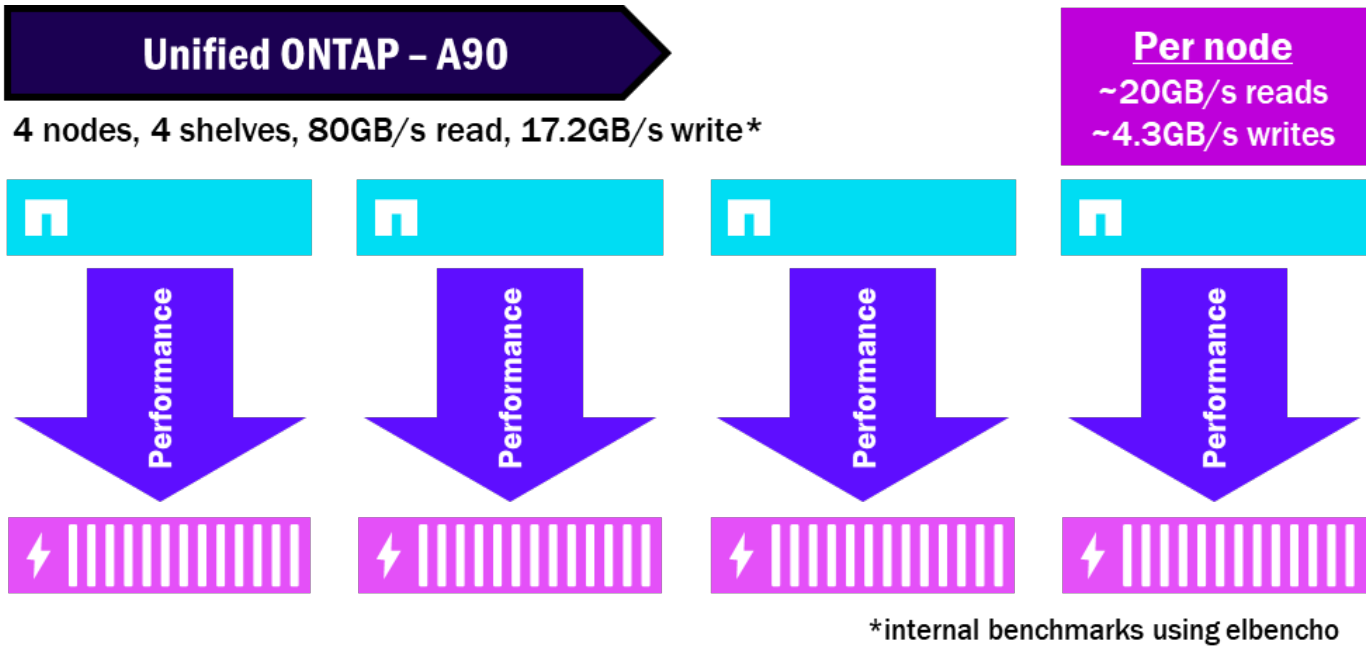
パフォーマンス密度

分散型 ONTAP アーキテクチャでストレージ ノードとシェルフを分離することで、より多くのノードがより少ないシェルフにトラフィックをプッシュできるようになり、必要な容量のみで最大のパフォーマンスを得るために必要なデータセンター全体のフットプリントを削減できます。

この「パフォーマンス密度」という概念により、ストレージ管理者はストレージ環境を過剰にプロビジョニングすることなく、既存のハードウェアを最大限に活用できるようになります。

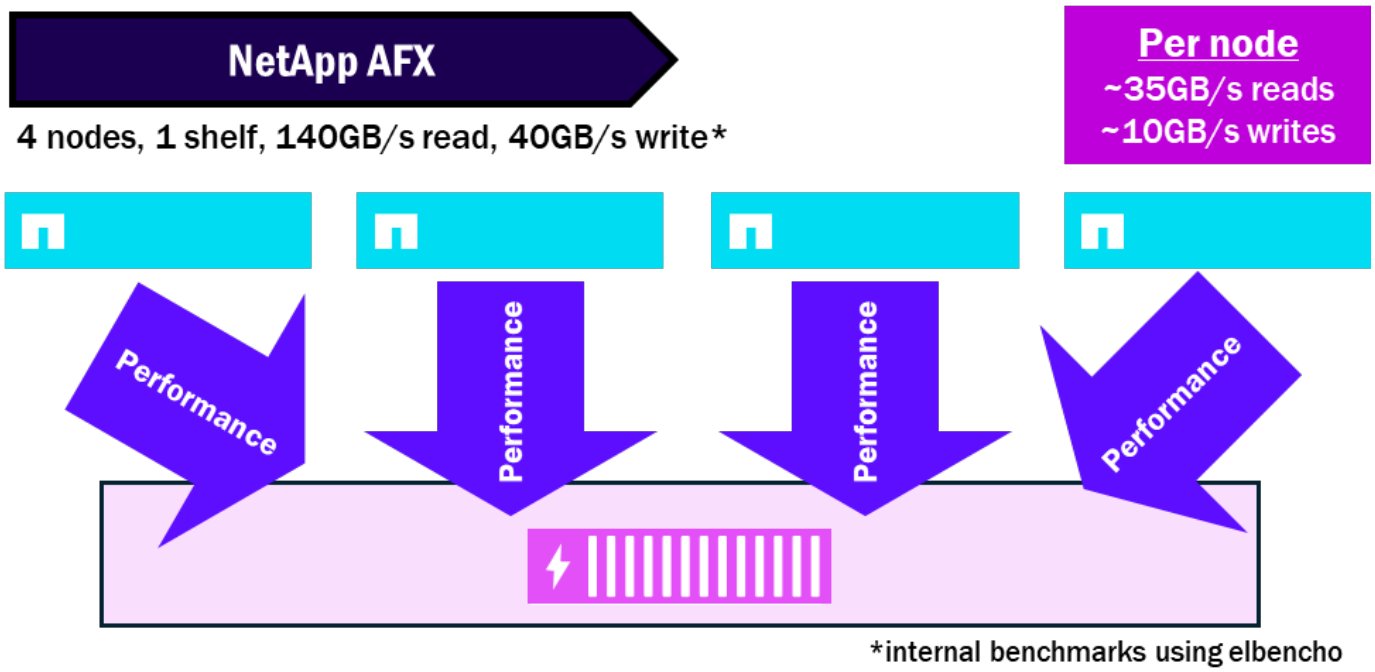
たとえば、統合ONTAPクラスタでは、各ノードに独自のディスクセットがあるため、パフォーマンスはそのノードが所有するディスクのみに向けられます。また、1つのディスクセットには1つのノードしかアクセスできないため、使用可能なディスクを必ずしも飽和状態にして最大のパフォーマンスを達成できるとは限りません。

統一 **ONTAP –** パフォーマンスの配分方法



NetApp AFXはすべてのディスクを単一のストレージ可用性ゾーンに統合するため、すべてのノードがすべてのディスクを活用できます。ディスクとノードが分離されているため、同じパフォーマンスを得るために必要なシェルフの数が少なくて済みます。これによりパフォーマンスが凝縮され、シェルフの最大パフォーマンスポテンシャルが最大限に引き出されます。

NetApp AFX – パフォーマンス密度



ノードとシェルフの比率

統合ONTAPノードには、ノードごとに少なくとも1セットのディスクが必要であり、1つのノードに複数のシェルフを接続することができる。その結果、単一ノードにおいてパフォーマンスのボトルネックが発生し、自身のディスクを飽和状態にできない可能性がある。

NetApp AFXは、すべてのディスクシェルフをすべてのノードに提示します。各シェルフには、16 x 100GB RoCE対応インターフェイスを備えたモジュールが搭載されており、シェルフあたりに許容される総パフォーマンス量を増加させます。このため、同じディスクセットに対して読み書きを行う複数のノードで単一のシェルフを飽和させることができます。

ONTAP 9.19.1の時点で、ノード：シェルフの飽和比は約4：1です。

ベンチマーク結果

次のセクションでは、以下の構成パラメータを持つNetApp AFXクラスタを使用したベンチマーク結果について説明します。

- 4ノード、4データインターフェイス
- シェルフ2台（7.6TBドライブ）
- ONTAP 9.19.1
- NFSv4.2（pNFS、セッション トランキング）
- FlexGroupボリューム
- "ElBencho" ベンチマーク
- 書き込み：elbencho --hosts=x.x.x.[y-z] -d -w -b 1M -t 80 --iodepth 1 --direct -s 600g /fio_vol1/
- 読み取り：elbencho --hosts=x.x.x.[y-z] -r -b 256k -t 80 --lat --iodepth 2 --direct -s 600g --infloop /fio_vol1/
- 4台のCisco C240 M8サーバ、2ポート×200GbE CX-7カード、80スレッド
- NFSマウントオプション：rw,vers=4.2,rsize=1048576,wsize=1048576,trunkdiscovery,proto=tcp

上記の構成では、4ノードクラスタで利用可能な最大読み取り速度（約134GB/秒）に非常に近い値を達成し、ノードあたりに許可されている最大書き込み速度（40GB/秒）にほぼ達しました。

NetApp AFX – ElBencho 読み取りパフォーマンス、**4** ノード

NetApp AFX – ElBencho 書き込みパフォーマンス、**4** ノード

積極的な先読み

メディアストリーミングのワークロードでは、4K映画はしばしば数万個のファイルに分割され、各ファイルは通常50MBから250MBのサイズになります。各ファイルはフレームを表し、アプリケーションは1回の要求

でフレーム全体を読み取ります。バッファリングが目立たず、スムーズで途切れのないストリームを維持するためには、これらのフレーム読み取りはドロップなしで完了する必要があります。

ONTAPでは、これらのワークロードを最適化するためのボリュームレベルのオプション(`-aggressive-readahead-mode`を提供しています。ONTAP 9.19.1以降、類似のファイルタイプ間で予測可能なI/Oパターンを持つワークロード（メディアレンダリングやストリーミングなど）を高速化するために、AFXでアグレッシブな先読み用の新しい `cross_file_sequential_read`モードが導入されました。

cross_file_sequential_read は、ファイル名に基づいて次に読み込むファイルを予測し、クライアントが read 呼び出しを発行する前に、それらのファイルに対して先読みを開始します。予測ロジックは、ディレクトリ内のすべてのファイルが、単調増加する数値の接尾辞（例：file1、file2、file3）を持つ命名パターンに従うことを前提としています。ディレクトリ内のすべてのファイルは、10進数または16進数のいずれかを使用して、このパターンに従う必要があります。ファイル名は最大255文字までです。このロジックは拡張子に依存せず、現在のディレクトリ内の次のファイル名セットを現在のファイル名のみに基づいて生成します。以前に10進数で生成されたファイル名がディレクトリ内に存在しない場合、ファイル名は16進数で再生成されます。生成されたファイル名がどれも存在しない場合、そのセットに対してプリフェッチは実行されません。プリフェッチは、次のクライアント読み取り要求が発行されたときに再開されます。

これらのオプションを有効にすると、"frametest"パフォーマンス ベンチマークでは、30クライアント（NFSv3およびSMB3）と34クライアント（NFSv4.1）で、30フレーム/秒で30,000個の4Kフレームを、フレーム落ちすることなく読み込むことができました。

ファイル間シーケンシャル読み取りは主にメディアワークロード向けに設計されていますが、AIのトレーニングや推論など、アクセスパターンやファイル名が予測可能な、読み取り負荷の高い他のワークロードにもメリットがあります。

考慮事項と注意点

- 共有バッファキャッシュ – アグレッシブリード先読みは、ノード上の他のボリュームと同じバッファキャッシュを使用します。これを有効にすると、そのノード上の他のボリュームの読み取りパフォーマンスに影響を与える可能性があります。
- 基盤となるストレージのパフォーマンス – ファイルの読み取り速度が十分でない場合（たとえば、HDDベースのFASシステムの場合）、キャッシュされたデータがクライアントによる読み取りが行われる前に削除される可能性があり、先読みの利点が失われる場合があります。
- アクセスパターンの要件：ワークロードの読み取りパターンがシーケンシャルでない場合、またはディレクトリ内のファイルが昇順で命名されていない場合、cross_file_sequential_read の積極的な先読みモードは、意味のあるメリットを提供しません。

NFSv4.xのパフォーマンス向上

NFSバージョン3は、1995年に初めて正式リリースされて以来、数十年にわたりNFSアプリケーションのゴールドスタンダードであり続けている。その優れた性能と堅牢性の組み合わせにより、より新しいNFSバージョンへの移行を検討することが難しいのは、それなりの理由がある。

しかし、NFSv3にも限界がないわけではない。プロトコルのステートレス性は、パフォーマンスの向上やストレージのフェイルオーバー時の障害を最小限に抑えるという点では優れているが、データの一貫性やロック管理という点では必ずしも優れているとは言えない。NFSサーバはロック状態を実際には追跡しないため、障害が発生した場合、NFSサーバはロックを解除する場合もあれば解除しない場合もあり、NFSクライアントはファイルがロックされているかどうかを認識できない場合がある。

```
 Security for NFSv3 is also a bit lacking. The protocol requires multiple
open firewall ports to function properly and numeric IDs are sent in
plaintext over the wire. Furthermore, NFS does not have robust ACL
support, and does not include native file and folder auditing. As a result
of these limitations, NFSv4 was created in 2003 via
link:https://datatracker.ietf.org/doc/html/rfc3530[RFC-3530^] (obsoleted
in 2015 by link:https://datatracker.ietf.org/doc/html/rfc7530[RFC-7530^]).
```
NFSv4.xは20年以上前から存在しているにもかかわらず、いくつかの理由からいまだに広く普及していない。

- ID管理の複雑さ：多くの環境では、NFSv4.x の名前文字列と Kerberos セキュリティ要件を適切に活用するための名前サービスインフラストラクチャが整備されていません。
- より新しいNFSクライアントの必要性：NFSv4の最初のリリース日から時間が経つにつれて、今日の最新のNFS環境ではこの懸念はそれほど切迫していません。現在使用されているほとんどすべてのOSには、NFSv4を完全にサポートするNFSクライアントが搭載されていますが、必要なNFSv4.xパッケージを備えていないレガシーシステムもまだ存在します。実際、一部のアプリケーションでは依然として古いNFSバージョンの使用が求められます。
- 「壊れていないなら直す必要はない」という考え方：企業のIT組織は、新しいテクノロジーの導入に関して非常に保守的であることで知られています。たとえ20年以上前から存在するテクノロジーであっても例外ではありません。現在のNFSバージョンが問題なく動作しているなら、なぜ変更する必要があるのでしょうか？
- パフォーマンスに関する懸念：NFSv4.xのようなステートフルなプロトコルのパフォーマンスは、過去20年間、ステートレスなNFSv3に比べて遅れをとってきました。従来は、NFSv4.xの利点よりもパフォーマンスへの影響の方が大きい場合が多かった。

ONTAP 9.18.1 における AFX を使用した NFSv4.x の改善点

ONTAP のアーキテクチャ上の変更により、NFS 全般に待望のパフォーマンス向上がもたらされ、NFSv4.x のパフォーマンス全般の改善に大きく貢献しました。

以下は、これらの変更点の概要です。

シーケンシャル読み取り性能の向上：**NFSv4.1**は**NFSv3**より**30%**向上

ONTAP 9.18.1では、NFSv4.1によるマルチパスI/Oのサポートが導入されました。WAFLファイルシステムからの読み取りを処理する代わりに、MPIOは読み取り操作をネットワークドメインに移行させ、マルチパスセーフな方法で処理できるようにします。このアプローチはコンテキストスイッチを減らし、シーケンシャル読み取りトラフィックの全体的な並列性を向上させるとともに、WAFLをバイパスすることでバッファ管理のオーバーヘッドを削減します。

FlexGroupボリュームのランダム読み取りの強化：**NFSv4.1**は**NFSv3**の**7%**以内

FlexGroupボリュームとは、複数の構成要素となるボリュームを取り込み、それらを単一の統一された名前空間として提示するボリュームのことです。AFXでは、FlexGroupボリュームにはデフォルトで高度な容量バランス機能が有効になっており、10GBを超えるファイルは複数の構成ボリュームにまたがってマルチパートファイルとして書き込まれます。これらのファイルパーツが遠隔地にあるため、従来、NFSv4.xではランダム読み取りのパフォーマンスが若干劣っていました（NFSv3より約18%低い）。ONTAP 9.18.1では、この問題に対処するため、NFSv4.xを使用したマルチパート読み取りにおけるキャッシュされたI/Oのサポートが導入されました。注：この変更はFlexVolボリュームには適用されません。

シーケンシャル書き込み：以前のリリースから**+10%**向上

HA フェイルオーバー機能に使用される NVLOG データの複製方法の改善により、NetApp AFX システムの全体的なシーケンシャル書き込みパフォーマンスが向上しました。

メタデータ操作：**EDA**ベンチマークにおいて**NFSv3**の**15%**以内のパフォーマンス

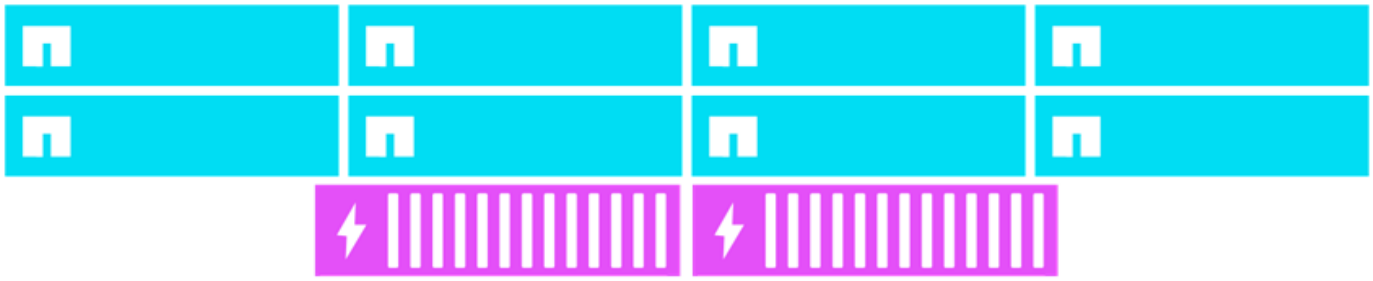
NFSv4.1 は従来、すべての OPEN および CLOSE 操作をシリアル化し、クラスタ ノードがネットワークから WAFL に送信する前に 1 つずつ処理します。ONTAP 9.18.1 では、競合状態の解決方法を変更することでネットワークの直列化を排除する Concurrent Open Close（COC）が導入され、以前のリリースで見られた OPEN/CLOSE のボトルネックが解消されます。

これらの変更はすべて、AFXで導入されたアーキテクチャの変更と相まって、ONTAP 9.18.1におけるNFSv4.1の全体的なパフォーマンスを向上させることが可能になりました。

シーケンシャル**IO**結果

若干のパフォーマンス改善が見られた分野の一つは、シーケンシャルIO（つまり、予測可能で連続して発行されるIO）でした。fioを使用した標準的なパフォーマンステストでは、ONTAP 9.18.1を実行しているAFXは、シーケンシャル読み取りパフォーマンスを約30%、シーケンシャル書き込みパフォーマンスを10%向上させました。

NetApp AFX – NFSv4.1 シーケンシャル **IO** パフォーマンス **ONTAP 9.18.1**



	AFX 9.17.1	AFX 9.18.1
Seq. reads	220GB/s	283GB/s
Seq. writes	70.6GB/s	77.7GB/s

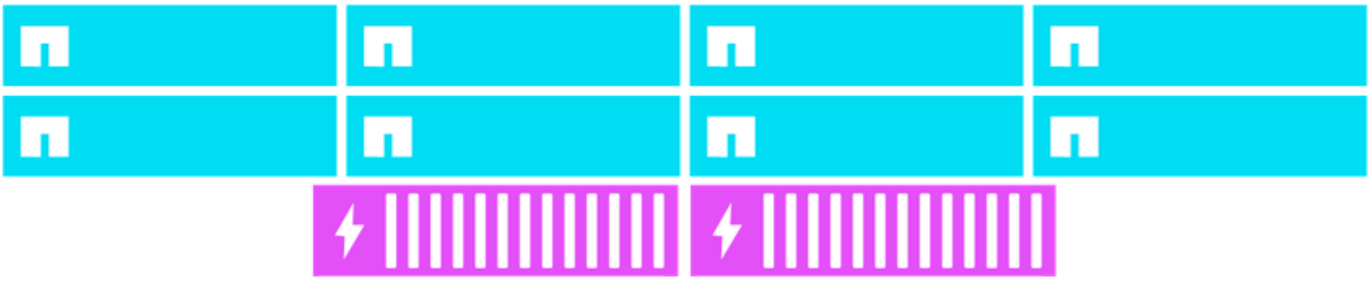
メタデータを多く含むワークロードの結果

さらに印象的なのは、NFSv4.xのパフォーマンス上の最大の課題の一つであるメタデータの改善点です。これらはランダムな入出力であり、通常は4Kバイト程度のサイズで、ファイル所有者や属性の管理、ファイルの作成や一覧表示などに使用されます。NFSv4.xはステートフルな性質を持つため、これらの操作はCPUとレイテンシのコストが高くなりがちで、結果として全体的なパフォーマンスが低下します。

AFX ONTAP 9.18.1 の変更により、これらのタイプのワークロードにおける NFSv4.x のパフォーマンスが大幅に向上し、NFSv3 のパフォーマンスとの差が（15%以内に）縮まりました。

当社のパフォーマンスエンジニアリングチームは、標準的なAI画像、EDA、およびソフトウェアビルドのベンチマークのパフォーマンスを比較し、以前のONTAPリリースから大幅な改善を発見しました。

NetApp AFX – ONTAP 9.18.1における**NFSv4.1**メタデータ**IO**パフォーマンス



	9.17.1	9.18.1	Delta
AI Image processing	209 KIOPS	239 KIOPS	+16%
Software dev	600 KIOPS	950 KIOPS	+58%
EDA	480 KIOPS	881 KIOPS	+84%

管理ツール

ストレージの提示方法にはかなり大きなアーキテクチャ上の違いがありますが、NetApp AFXの機能セットとONTAPの管理方法は実質的に変更されていません。これは完全に意図的な設計です。ONTAPはONTAPであり、可能な限り学習曲線はほとんど、あるいは全くないはずです。そしてこの場合、NetApp AFXは依然としてONTAPを実行しています。

管理 – CLI

NetApp AFXでは、CLIは統合ONTAP のCLIが提供するものとほぼ同じです。コマンドは大部分が依然としてクラスタレベルで実行されますが、ノードレベルで発行できるコマンドも依然として存在します。依然として、トップレベルのコマンドディレクトリとサブコマンド、およびコマンドのタブ補完機能が利用可能です。さらに、すべてのCLIショートカットが機能します（たとえば、 `-fields`を使用したコンテンツのフィルタリング）。

NetApp AFX CLI における唯一の実際の違いは、追加されたものと削除されたものに関係しています（このドキュメントの "" セクションで説明されています）。機能（アグリゲートや Metrocluster など）が削除された場合、対応する CLI コマンドは使用できなくなります。

さらに、NetApp AFXに新しい機能が追加された場合、新しいコマンドも利用可能になります。例えば、新しい"NetApp AI Data Engine（AIDE）"アドオンは、バックエンドクラスタネットワーク上のNetApp AFXクラスタと直接やり取りします。その結果、 `dcn`および `data-engine`コマンドディレクトリがNetApp AFX CLIに追加されます。

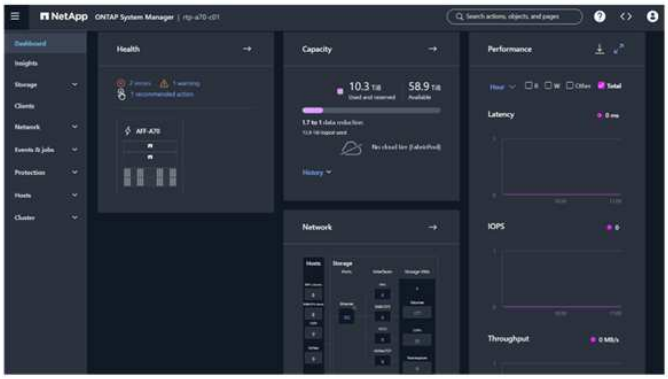
以下は、NetApp AFXクラスタで管理者権限で使用できるトップレベルのコマンドディレクトリを示しています。新しく追加されたコマンドは太字で表示されています。

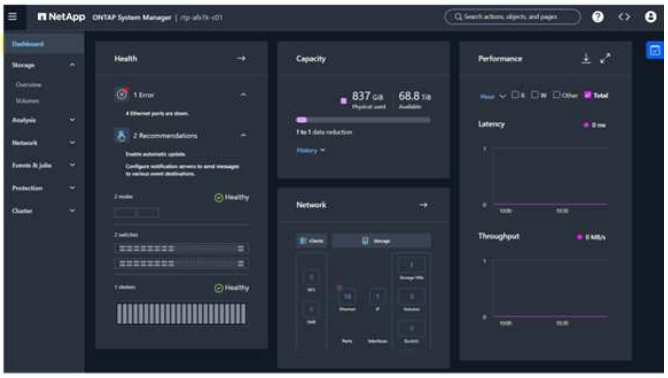
```
AFX::>
    cluster         data-engine    dcn            event          exit
    history         job            man            metrocluster   network
    qos             redo           rows           run            security
    set             snaplock       snapmirror     statistics     statistics-v1
    storage         system         top            up             volume
    vserver
```

管理 – GUI

System Managerは、リソース管理のためのNetApp AFXクラスタと対話するためのGUIインターフェイスであり、最初にログインしたときは、統合されたONTAPシステムにログインしていないことが一見してわからないでしょう。

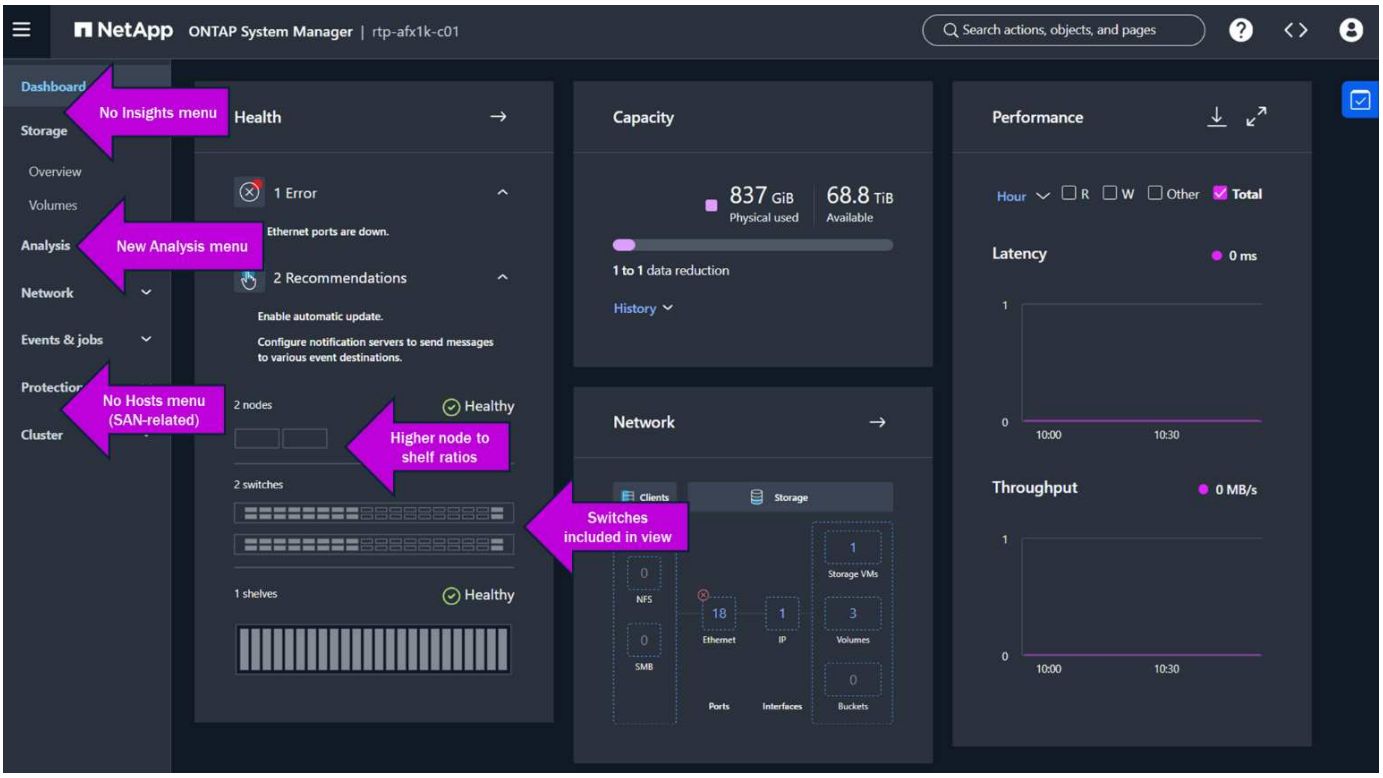
統合された **ONTAP** と **NetApp AFX System Manager** のランディングページの並列表示





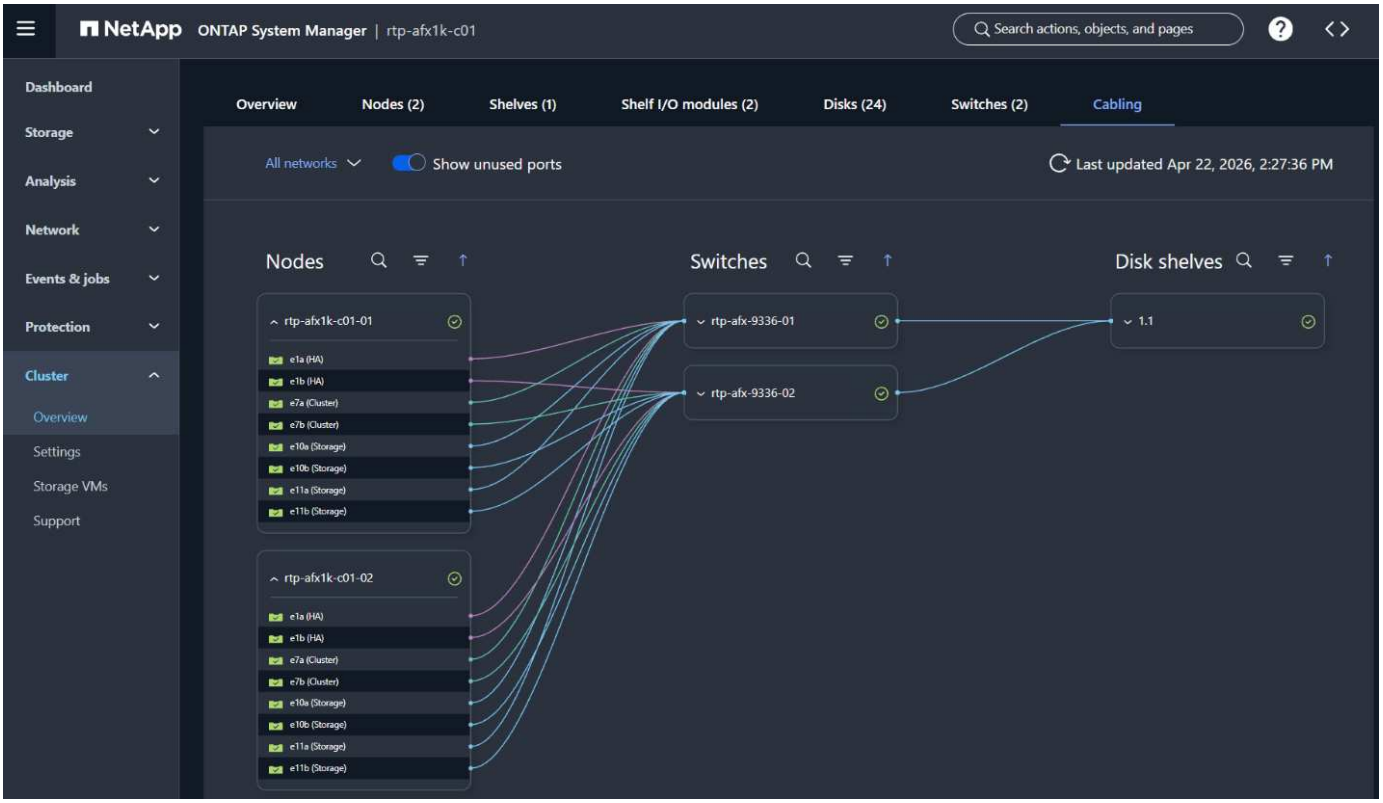
上記のとおり、統合 ONTAP と NetApp AFX の System Manager には明らかな違いはあまりありません。ただし、いくつかの兆候があります。

System Manager における **NetApp AFX** の違い



メニューやダッシュボードをドリルダウンしても、ほとんどすべてが同じままです。ボリュームには、使用済み容量と合計容量が引き続き表示されます。ネットワークインターフェイスには、ポートとIPアドレスが引き続き表示されます。SnapMirrorの保護ポリシーは引き続き設定できます。ハードウェアビューは引き続き利用できます。しかし、NetApp AFXは、新しいケーブル配線ビューを提供することでビューを少し強化しており、ドリルダウンしてストレージ スタック全体でケーブルがどこに接続されているかを確認できます。

NetApp AFXケーブル接続図



REST API

NetApp AFXは、ONTAP REST API呼び出しの大部分を保持するための協調的な取り組みも行っています。つまり、REST APIベースの自動化ツールスイートを作成している場合、ほとんどのケースで引き続き使用できるはずです。主な例外としては、アグリゲート、Metrocluster、SAN、および一部のパフォーマンスカウンタが挙げられます。完全なREST APIドキュメントは、NetApp AFXクラスタのSystem Manager で\https://clus_mgmt_ip/docs/apiに移動することで確認できます。

ONTAP外部管理ツール

NetApp AFXは、次のようなオフボックスONTAP管理ツールに対して一部のサポートを提供します：

- NetApp System Manager
- NetApp Console
- Grafana Harvest（25.11.0以降）
- NetApp Trident（25.10以降）

NetApp AFX は現在、以下の機能をサポートしていません：

- NetApp ActiveIQ Unified Manager

ネットワーク、セキュリティ、および運用

NetApp AFXは、統合ONTAPと同じネットワークスタック、セキュリティ機能、データ保護技術、無停止運用、およびボリュームタイプをサポートしていますが、分散型アーキテクチャ特有の調整がいくつか加えられています。

ネットワーキング

NetApp AFX のネットワーク スタックは、統合 ONTAP と同一です。

- データLIFは、ネットワークアドレスを内部サービスおよび外部サービスに提示するために依然として使用されています。
- 各ノードには、独自の物理ポートと仮想ポートのセットがあります。
- VLAN、ifgroup、およびBGPはすべて引き続きサポートされています。
- LIFは、クラスタ内の物理ノード間およびポート間でフェイルオーバーを行うことができます。
- IPspace／ブロードキャストドメインの設定は以前と同じです。
- 各SVMは、それぞれ専用のデータネットワークを持つことができます。
- 管理ネットワークはデータネットワークから分離できます。
- クライアントのデータネットワークは、新たに400GBのネットワークサポートが追加された以外は変更されません。
- バックエンドクラスタスイッチは、引き続きNetAppが提供する「ゴールデン構成」ファイルによって構成されます。

ネットワークの主な違いは以下のとおりです：

- バックエンドクラスタのネットワークポートは、クラスタスイッチへの100GB接続のみをサポートするようになりました。
- クラスタスイッチは400GBに対応しているため、バックエンドノード接続には4 x 100GBブレークアウトケーブルを使用して、スイッチで使用するポート数を削減します。
- NVRAMは、スイッチ上の新しいHA VLAN構成を介して、バックエンドクラスタネットワーク全体のHAペア間でミラーリングされるようになりました。
- 新しいDCNネットワークは、AI Data Engineに対してデフォルトで追加されます。これらのIPアドレスは自動的に生成され、必要に応じて変更できます。

セキュリティ

NetApp AFXはONTAPで動作します。つまり、ONTAPと同じセキュリティを使用しているということです。すべての暗号モジュールは同一であるため、認証プロセスが完了すれば、セキュリティ認証も同一になります。NetApp AFXは、統合ONTAPと同じセキュリティ暗号のサポートを活用しています。

さらに、NetApp AFXは、unified ONTAPが提供する多くのセキュリティ機能をサポートしています（ただし、これらに限定されません）：

- 自律型ランサムウェア対策
- セキュアなマルチテナンシー
- 保存時の暗号化（ボリューム暗号化）および転送時の暗号化（TLS 1.3）
- 自己暗号化ドライブ（SED）
- NFSおよびSMB Kerberos認証と暗号化
- マルチ管理者認証
- SnapLock

統合 ONTAP が取得した認証（およびその他のセキュリティ強化情報）については、以下を参照してください：

- "NetApp製品セキュリティ"
- "ONTAPセキュリティ強化の概要"

スナップショットとデータ保護

NetApp AFXは、統合型ONTAPと同じスナップショットおよびレプリケーション技術を活用しており、これらの機能の動作方法に大きな変更はありません。実際、AFXは、使い慣れた"ルールと設定"を使用して、統合型ONTAPシステムとの間でレプリケーションを行うことができます。

AFXにおけるレプリケーションの唯一の例外は、FlexGroupボリュームを統合されたONTAPシステムにレプリケートする場合です。その場合、デスティネーションの統合されたONTAPシステムは、Advanced Capacity Balancingサポートを提供するために、ONTAP 9.16.1以降を実行している必要があります。

ノンストップ オペレーション

ONTAPは、ボリュームの移動、アップグレード、クラスタのメンテナンス、ストレージのフェイルオーバーなど、無停止で運用できる操作を提供します。NetApp AFXは、若干の調整を加えて、同じ無停止運用を提供します。

- ボリュームの移動は引き続き無停止で実行できますが、コピーは不要になりました。
- ストレージのフェイルオーバーは依然としてサービスに支障をきたしませんが、最初のフェイルオーバー後、ボリュームはクラスタ内の生存しているすべてのノード間で再バランスされます。
- LIFの移行は同一です。
- ハードウェアの保守とアップグレードは同一です。

ボリューム タイプ

統合ONTAPは、以下のような複数のボリュームタイプをサポートしています。

- FlexVol
- FlexGroup ボリューム
- FlexCache
- FlexClone
- オブジェクトバケット

NetApp AFXは、これらの各ボリュームタイプを完全にサポートするだけでなく、ユニファイドONTAPシステムとのFlexCacheボリュームの完全な相互運用性も提供します。

FlexGroup ボリュームが AFX アーキテクチャからどのようなメリットを得られるかについては、"FlexGroup ボリューム管理の機能拡張"を参照してください。

ハードウェアの詳細

次のセクションでは、NetApp AFXクラスタハードウェアの詳細について説明します。NetApp AFXハードウェアの最新情報については、"https://hwu.netapp.com"を参照してください。

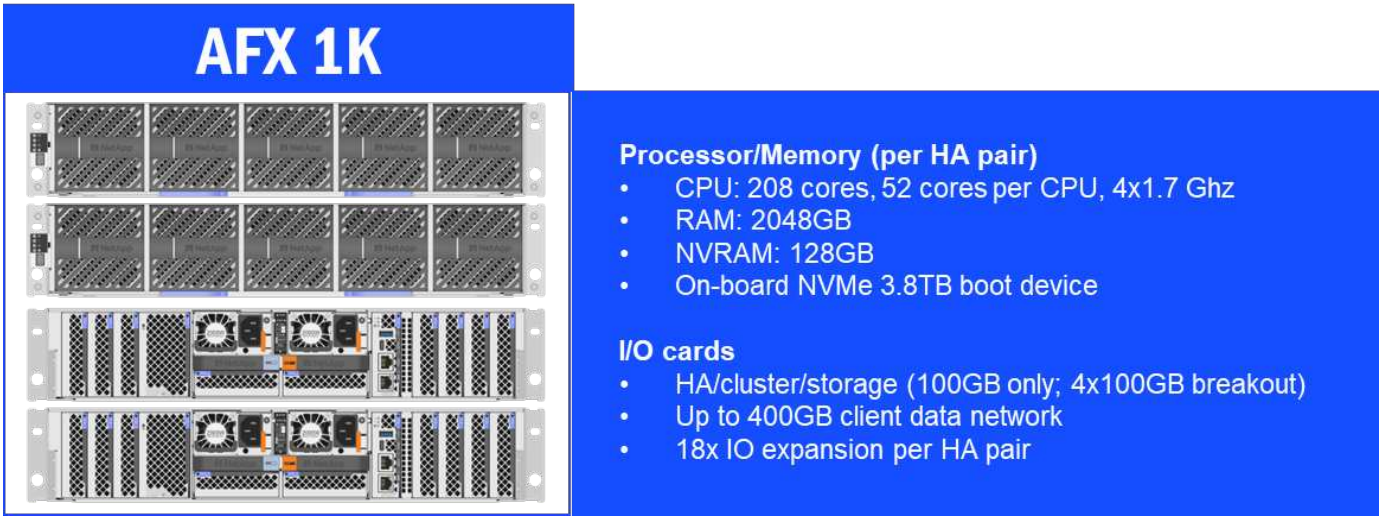
対応ハードウェア

NetApp AFX でサポートされているハードウェアに関する最新情報については、"https://hwu.netapp.com"を確認してください。

ノード

NetApp AFXノードは、統一されたONTAPクラスタ用に提供されるAFF A1Kモデルのノードをベースにしています。これらのノードにはストレージ用のオンボードディスクは搭載されておらず、パフォーマンス要件に基づいてノードを容易に追加および削除できるようにモジュール式に設計されています。各ノードは2Uのラック空間を占有し、AFXクラスタに追加されるにつれてパフォーマンスが直線的に向上します。

NetApp AFX 1K ノードの詳細



ハードウェアスロット

NetApp AFX 1K ノードでは、以下のスロット割り当てが使用されます。

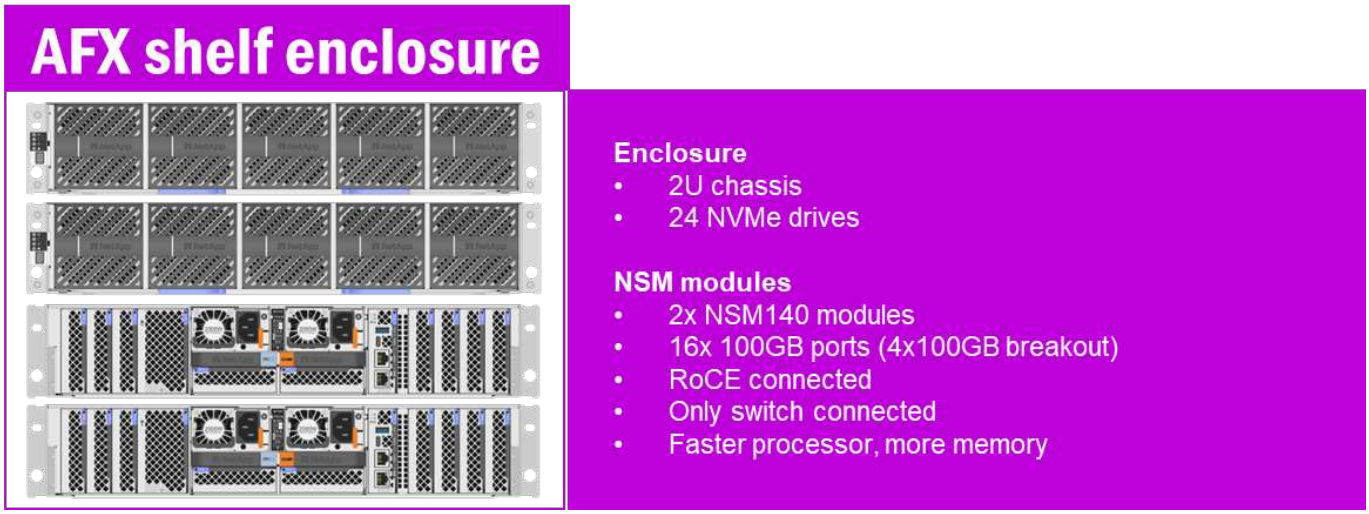
- スロット1はHAレプリケーション専用です
- スロット7はクラスタレプリケーション専用です。
- スロット10と11は、ストレージシェルフ通信専用です。

シェルフ

NetApp AFXシェルフは、AFFシステムと同じエンクロージャを使用します。AFXのシェルフの主な違いは、使用されているモジュールにあります。NSM140モジュールは、強化されたパフォーマンス機能を提供し、分散型ONTAPを可能にします。いくつかの重要な考慮事項：

- 完全に実装されたシェルフのみがサポートされます。
- シェルフは、接続するとNetApp AFXによって自動的に検出されます。
- 現在、シェルフの取り外しはサポートされていません。

NetApp AFXシェルフエンクロージャの詳細

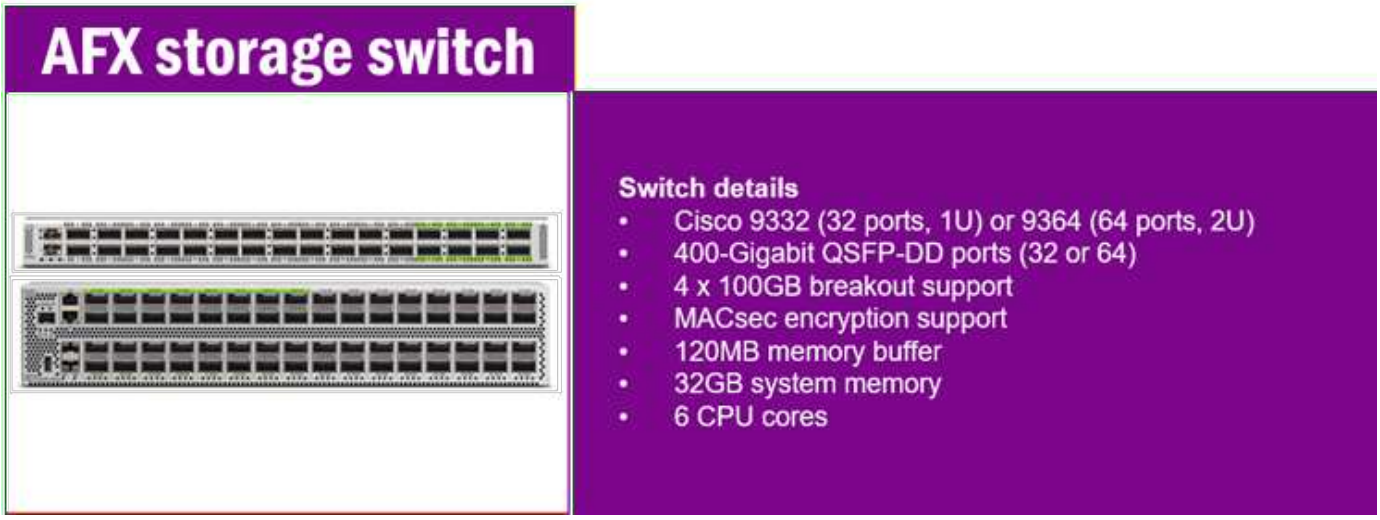


スイッチ

NetApp AFXは、クラスタデータベースのレプリケーション、リモートデータ操作、ストレージ操作、NVRAMミラーリングなどのクラスタ内通信にバックエンドクラスタスイッチを引き続き使用します。機能的には、統合ONTAPとNetApp AFXクラスタスイッチの唯一の違いは次のとおりです：

- 400GbEのサポート
- 新しいHA VLAN
- 詳細については、"Ciscoスイッチのデータシート"をご覧ください。

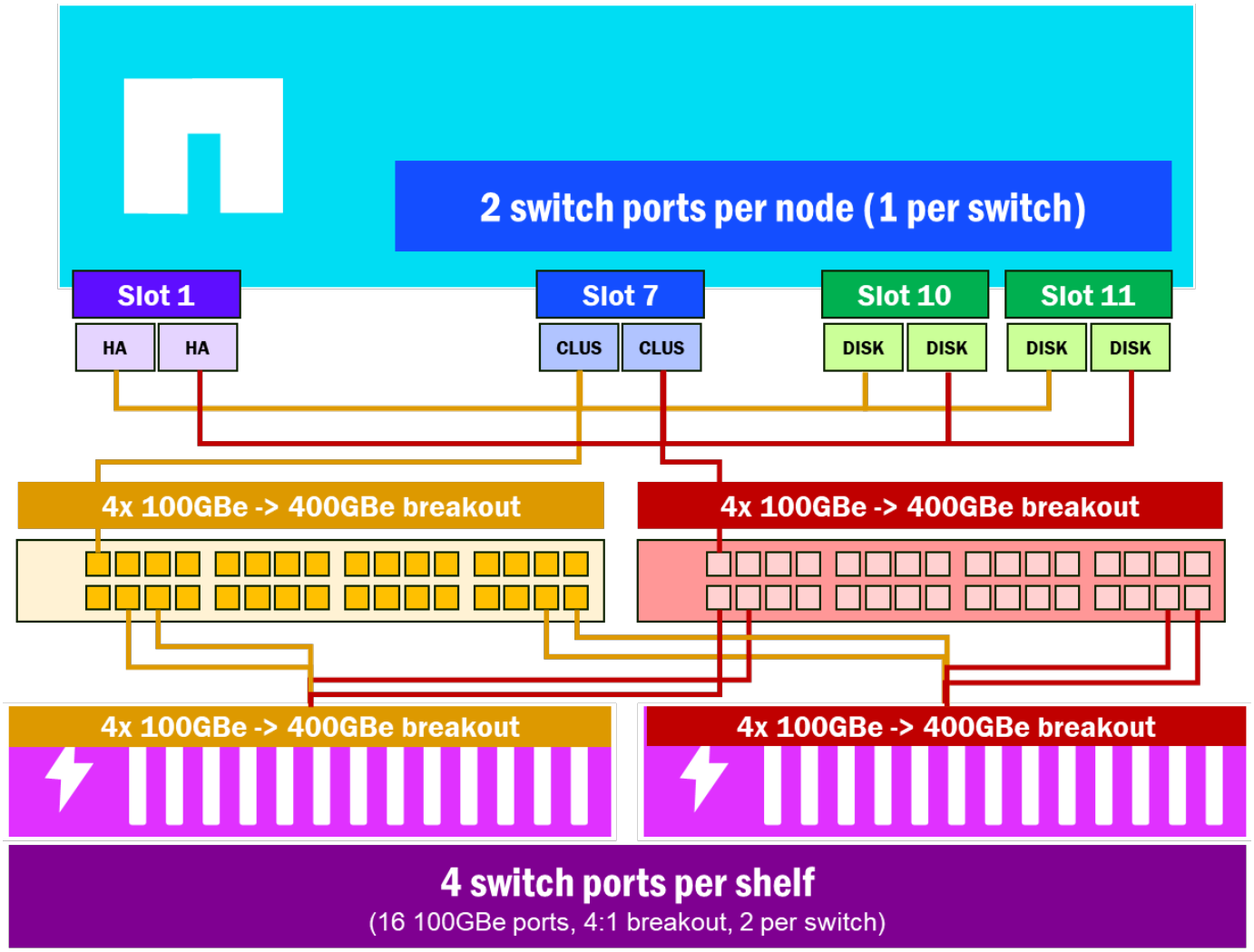
NetApp AFXクラスタスイッチ



クラスタスイッチの接続

NetApp AFXは、その主要なアーキテクチャ概念の多くにおいて、バックエンドのクラスタスイッチを多用している。例えば、クラスタインターフェイス、ストレージアダプタ、ストレージシェルフ、NVRAMカードはすべてクラスタスイッチに接続されます。現在、これらのインターフェースはすべて100GBの通信のみをサポートしていますが、スイッチは400GBをサポートしています。その結果、100GBインターフェースは、4本の100GBブレークアウトケーブルを介して、スイッチ上の400GBインターフェースに接続される。この方法により、スイッチで使用されるポート数を削減できます。例えば、16個の100GBストレージシェルフモジュールポートはスイッチの4つのポートのみを使用し、ノードの合計8つのポートはスイッチの2つのポートを使用します。

NetApp AFXスイッチのケーブル接続



ディスクのタイプとサイズ

NetApp AFX は現在、以下のサイズの NVMe 接続 SSD のみをサポートしています：

- 7.6 TB
- 15.3 TB
- 30.1 TB
- 60.6 TB

TLCとQLC

NetApp AFXはTLCとQLCの両方のフラッシュタイプを利用できます。7.6TBと15.3TBのドライブはTLCモデルで、30.1TBを超えるドライブはQLCモデルとなります。メディアの種類に関係なく、NVIDIA SuperPod認証性能基準を満たすことができます。

NetApp AFXで使用されるすべてのドライブはパフォーマンス重視のドライブであり、QLCとTLCはどちらも読み取りトラフィックに関してはほぼ同じパフォーマンスを発揮します。QLCはTLCに比べて書き込み性能がやや劣り、書き込み負荷の高いワークロードでは若干ウェアレベリングが顕著になる可能性があります。

パフォーマンス数値については、"シェルフごとのパフォーマンス"を参照してください。

使用するドライブタイプを選択する際には、ストレージがホストするワークロードと、パフォーマンス/容量密度のトレードオフを考慮してください。

最大値と制限値

次のセクションでは、NetApp AFXクラスタの最大値と最小値を統合型ONTAPと比較して説明します。

最新の制限については、"Hardware Universe"を参照してください。

NetApp AFXの最大値と最小値

上限	ユニファイド **ONTAP**	**NetApp AFX**
ボリューム数（クラスタ）	• 30,000（プラットフォームによって異なる）	• 30,000
アグリゲートサイズ	• 800 TB	• 該当なし
ノード数	• 24	• 8 (9.17.1) • 32 （9.19.1RC1）
合計容量	• ノードとドライブに依存します。詳細については、"hwu.netapp.com"を参照してください。	• 2PB （9.17.1） • 3PB（9.18.1RC1） • 16PB（9.18.1GAリリース） • 20PB（9.19.1RC0） • 32PB（9.19.1RC1）
サポートされるシェルフ数	• HAペアあたり8個 • クラスタあたり192	• クラスタあたり12（9.18.1GA） • クラスタあたり17（9.19.1RC0） • クラスタあたり25（9.19.1RC1）（HAペアの制限なし）
サポートされるドライブの総数	• HAペアあたり240 • 2880（24ノード）	• クラスタあたり288（シェルフ数の制限に基づく。HAペアの制限なし） • クラスタあたり408（9.19.1RC0） • クラスタあたり600（9.19.1RC1）

上限	ユニファイド **ONTAP**	**NetApp AFX**
ボリューム サイズ	• 300TB（FlexVol） • 60PB （FlexGroup）	• 300TB（FlexVol） • 60PB （FlexGroup）*
ボリュームあたりの最大ファイル数	• 20億（FlexVol） • 4000億（FlexGroup）	• 20億（FlexVol） • 4000億（FlexGroup）
ディレクトリあたりの最大ファイル数（デフォルトの320MB maxdirsizeの値）	• 約400万（FlexVol） • 約200万（FlexGroup）	• 約400万（FlexVol） • 約200万（FlexGroup）
SnapMirror同時転送	• 250	• 250
qtreeの数	• 4096	• 4096
ノードあたりの最大TCP接続数	• 100,000	• 100,000
ノードあたりの最大ロック数	• 3 million	• 3 million
最大データインターフェース数（クラスタ）	• 4096	• 4096
最大構成要素数 – FlexGroup	• 200	• 200 • 9.19.1 RC1で512
クラスタ間LIFの最大数	• 8	• 8
IPスペースの最大数	• 512	• 512
オリジンあたりの最大FlexCache数	• 100	• 100
FlexCacheの最大数（ノード）	• 400	• 400

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、次のドキュメントやWebサイトを参照してください：

- "Hardware Universe"
- "AFX製品ページ"
- "AIを活用した企業の構築：インフラが重要な理由"
- "ブログ：NFSv3とNFSv4.Xのどちらを選ぶべきか"
- "AFXデータシート"

ONTAP SnapCenterテクニカルレポート

SnapCenterは、アプリケーションと整合性のあるデータ保護とクローン管理を実現するユニファイドプラットフォームを提供します。SnapCenterは、アプリケーション統合ワークフローに従い、バックアップ、リストア、クローンのライフサイクル管理を簡易化します。SnapCenterは、ストレージベースのデータ管理を活用することで、パフォーマンスと可用性を向上させ、テストと開発の時間を短縮します。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載されている"SnapCenter"ています。

SnapCenter for Oracleの略

"TR-4700：『SnapCenter Plug-in for Oracle database best practices』"
NetApp SnapCenterは、Oracleと整合性のあるデータ保護を実現する、拡張性に優れたユニファイドプラットフォームです。複雑な運用を自動化し、一元的な管理と監視を実現します。SnapCenterを使用してOracleデータベースを導入する際の推奨事項について説明します。

"TR-4964：『Oracle Database backup、restore and clone with SnapCenter Services』"Amazon FSx for ONTAPストレージおよびEC2コンピューティングインスタンスに導入されたOracleデータベースをバックアップ、リストア、クローニングするために、SnapCenterサービスを設定する方法をご紹介します。セットアップと使用ははるかに簡単ですが、SnapCenterサービスは、SnapCenterインターフェイスを介して利用できる主要な機能を提供します。

SnapCenter for Microsoft SQL Serverの略

"TR-4714：『Best Practices for Microsoft SQL Server using NetApp SnapCenter』"
SnapCenterを使用してNetAppストレージにMicrosoft SQL Serverを適切に導入し、データを保護する方法について説明します。

SnapCenter for Microsoft Exchange Serverの略

"TR-4681：『Best practices for Microsoft Exchange Server using NetApp SnapCenter』"
SnapCenterを使用してNetAppストレージにMicrosoft Exchange Serverを正しく導入し、データを保護する方法について説明します。

<xmt-block0>SnapCenter</xmt-block> for SAP HANAを参照してください

"TR-4614 ：『 SAP HANA Backup and Recovery with SnapCenter 』" SnapCenterは、SAP HANAおよびその他のデータベース向けに、アプリケーションと整合性のあるデータ保護を実現する、統合された拡張性の高いプラットフォームです。SnapCenterは、集中管理と監視機能を提供すると同時に、ユーザーがアプリケーション固有のバックアップ、リストア、クローン作成ジョブを管理する権限を委任します。SnapCenterを使用することで、データベースおよびストレージ管理者は、さまざまなアプリケーションやデータベースのバックアップ、リストア、クローン作成操作を管理するための単一のツールを習得できます。

"TR-4926：『SAP HANA on Amazon FSX for NetApp ONTAP - Backup and Recovery with SnapCenter 』

"Amazon FSx for NetApp ONTAPおよびSnapCenterでSAP HANAのデータ保護を実現するための推奨プラクティスをご紹介します。SnapCenterの概念、設定の推奨事項、処理のワークフロー（設定、バックアップ処理など）などのトピックが含まれます。 リストア処理とリカバリ処理を実行できます。

"TR-4667：『Automating SAP HANA System copy and clone operations with SnapCenter』"SnapCenterストレージのクローニングと、クローニング前処理とクローニング後処理を柔軟に定義できるオプションにより、SAP Basisの管理者は、SAPシステムのコピー、クローニング、更新処理を高速化、自動化できます。詳細はこちら任意のプライマリストレージまたはセカンダリストレージに任意のSnapCenter Snapshotバックアップを選択できるため、論理的破損、ディザスタリカバリテスト、SAP QAシステムの更新など、最も重要なユースケースに対応できます。

"TR-4719：『SAP HANA system replication backup and recovery with SnapCenter』"
SAP HANAシステムレプリケーション環境で、SnapCenterテクノロジとSAP HANAプラグインを使用したバックアップとリカバリについて説明します。

"TR-4667：『Automating SAP HANA system copy and clone operations with SnapCenter』"アプリケーションと整合性のあるNetApp Snapshotバックアップをストレージレイヤに作成する機能は、システムコピー処理やシステムクローニング処理の基盤となります。ストレージベースのSnapshotバックアップは、SAP HANA用のNetApp SnapCenter プラグインと、SAP HANAデータベースが提供するインターフェイスを使用して作成します。SnapCenter は、SnapshotバックアップをSAP HANAバックアップカタログに登録して、リストアやリカバリ、クローニング処理に使用できるようにします。

SnapCenterセキュリティ強化ガイド

"TR-4957：『Security Hardening Guide for NetApp SnapCenter』"
情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を組織が達成できるようにSnapCenterを構成する方法について説明します。

ONTAP Tieringに関するテクニカルレポート

FabricPoolデータ階層化ソリューションを使用すると、企業のフラッシュシステムの全体的なユーザエクスペリエンスが向上し、アプリケーションを再設計してストレージ効率を高める手間がなくなります。FabricPoolは、システム環境のストレージフットプリントと関連コストを削減します。アクティブデータはハイパフォーマンスSSDに保持されます。アクセス頻度の低いデータは、ストレージの効率性を維持しながら、低コストのオブジェクトストレージに階層化されます。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"ONTAP FabricPool"ています。

"TR-4598：『FabricPool best bests』"
FabricPoolの機能、要件、実装、推奨されるプラクティスについて説明します。

"TR-4826：『NetApp FabricPool with StorageGRID Recommendation Guide』"
ONTAPコンポーネントのFabricPoolの大容量階層としてStorageGRIDを導入し、サイジングする際の推奨されるプラクティスについて説明します。また、StorageGRIDを使用する際のコア機能、要件、実装、推奨される方法についても説明します。

"TR-4695：『Database storage tiering with NetApp FabricPool』"
Oracle Relational Database Management System（RDBMS）など、さまざまなデータベースを使用するFabricPoolのメリットと構成オプションについて説明します。

ONTAP仮想化テクニカルレポート

NetApp仮想化ソリューションは、サーバから最大限の価値を引き出すのに役立ちます。革新的でハイパフォーマンスなONTAPフラッシュシステムを基盤に構築された、応答性に優れた仮想サーバインフラにより、データへのアクセス時間を大幅に短縮できます。仮想インフラをペタバイト規模まできめ細かく拡張でき、システムを停止することなく、複数のワークロードへの共有アクセスに必要なパフォーマンスを実現できます。ONTAPは、主要なパートナーシップ、導入ガイダンス、アプリケーション統合、優れた設計により、仮想サーバインフラの導入を合理化し、複雑さを軽減します。ONTAPは、オンプレミスとクラウドの両方で堅牢な仮想化環境を実現するための推奨事項とソリューションを多数提供しています。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"VMware vSphere 用の ONTAP ツール"ています。

"TR-4597 ：『 VMware vSphere for ONTAP 』"ONTAPは、約20年にわたってVMware vSphere環境向けの業界をリードするストレージソリューションであり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。本ドキュメントでは、導入の合理化、リスクの軽減、管理の簡易化を実現するために、最新の製品情報と推奨されるプラクティスを含むONTAP 解決策for vSphereについて説明します。

"TR-4400：『VMware vSphere Virtual Volumes（VVol）with NetApp ONTAP 』"ONTAPは、20年以上にわたってVMware vSphere環境向けの業界をリードするストレージソリューションであり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。本ドキュメントでは、VMware vSphere Virtual Volumes（VVOL）向けのONTAP機能について説明します。最新の製品情報やユースケース、導入を合理化してエラーを削減するための推奨事項などの情報を紹介します。

"TR-4900：『VMware Site Recovery Manager with NetApp ONTAP』" ONTAPは、2002年に最新のデータセンターに導入されて以来、業界をリードするVMware vSphere環境向けのストレージソリューションであり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。このドキュメントでは、業界をリードするVMwareのディザスタリカバリ（DR）ソフトウェアであるONTAP 解決策for VMware Site Recovery Manager（SRM）について説明します。このソフトウェアには、導入の合理化、リスクの軽減、継続的な管理の簡素化を実現するための最新の製品情報と推奨されるプラクティスが含まれます。

"ONTAP と vSphere の自動化の概要"VMware ESXが登場して以来、VMware環境の管理には自動化が欠かせません。インフラをコードとして導入し、手法をプライベートクラウドの運用に拡張できるため、拡張性、柔軟性、自己プロビジョニング、効率性に関する懸念を軽減できます。このドキュメントでは、ONTAPおよびVMware vSphere環境を自動化するためのONTAP 解決策 を紹介します。

"WP-7353：『ONTAP tools for VMware vSphere - Product security』"このドキュメントでは、ONTAP Tools for VMware vSphere 9.Xを製品環境の既存の脅威と新たな脅威の両方から保護するために使用される技術とテクノロジについて説明します。

"WP-7355：『SnapCenter plug-in VMware vSphere - Product security』"このドキュメントでは、NetApp SnapCenter Plug-in for VMware vSphere 4.Xを製品環境の既存の脅威と新しい脅威の両方から保護するために使用される技術とテクノロジについて説明します。

"TR-4568：『NetApp deployment guidelines and storage best practices for Windows Server』"Microsoft Windows Serverは、ネットワーク、セキュリティ、仮想化、クラウド、仮想デスクトップインフラ、アクセス保護、情報保護、Webサービス、アプリケーションプラットフォームインフラなどをカバーするエンタープライズクラスのオペレーティングシステムです。本ドキュメントでは、Microsoft Windowsに焦点を当て、特に最新の製品情報や推奨事項など、導入の合理化、リスクの軽減、管理の簡易化を実現するHyper-V仮想化テ

クノロジに重点を置いています。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

ONTAP

"ONTAP 9.16.1に関する注意事項" "ONTAP 9.16.0に関する注意事項" "ONTAP 9.15.1に関する注意事項" "ONTAP 9.15.0に関する注意事項" "ONTAP 9.14.1に関する注意事項" "ONTAP 9.14.0に関する注意事項" "ONTAP 9.13.1に関する注意事項" "ONTAP 9.12.1に関する注意事項" "ONTAP 9.12.0の注意事項" "ONTAP 9.11.1の通知です" "ONTAP 9.10.1 での通知" "ONTAP 9.10.0に関する注意事項" "ONTAP 9.9.1 に関する注意事項" "ONTAP 9.8 に関する注意事項" "ONTAP 9.7 の場合の注意事項" "ONTAP 9.6に関する注意事項" "ONTAP 9.5 では次の点に注意" "ONTAP 9.4 の注意事項" "ONTAP 9.3 での注意" "ONTAP 9.2に関する注意事項" "ONTAP 9.1に関する注意事項"

MetroCluster IP構成向けONTAPメディエーター

"9.9.1 ONTAP Mediator for MetroCluster IP構成に関する通知" "9.8 ONTAP Mediator for MetroCluster IP構成に関する通知" "9.7 ONTAP Mediator for MetroCluster IP構成に関する通知"

著作権に関する情報

商標に関する情報