aws

ONTAP のユーザーガイド

FSx for ONTAP

FSx for ONTAP: ONTAP のユーザーガイド

Table of Contents

Amazon FSx for NetApp ONTAP とは

Amazon FSx for NetApp ONTAP は、 NetAppの人気のある ONTAP ファイルシステム上に構築された、信頼性、スケーラビリティ、高性能、機能豊富なファイルストレージを提供するフルマネージドサービスです。FSx for ONTAP は、 NetApp ファイルシステムの使い慣れた機能、パフォーマンス、機能、API オペレーションと、フルマネージド の俊敏性、スケーラビリティ、シンプルさを組み合わせます AWS のサービス。

FSx for ONTAP は、 AWS またはオンプレミスで実行されている Linux、Windows、macOS コンピューティングインスタンスから幅広くアクセスできる、機能豊富で高速、かつ柔軟な共有ファイルストレージを提供します。FSx for ONTAP は、ミリ秒未満のレイテンシーを備えた高性能なソリッドステートドライブ (SSD) ストレージを提供します。FSx for ONTAP では、ごく一部のデータに対して SSD ストレージの費用を支払う一方で、ワークロードに対して SSD レベルのパフォーマンスを実現することができます。

ボタンをクリックするだけでファイルのスナップショット、クローン作成、およびレプリケーションができるため、FSx for ONTAP を使用したデータの管理が簡単になります。さらに FSx for ONTAP では、データを低コストで伸縮性のあるストレージに自動的に階層化することで、容量のプロビジョニングや管理の必要性を軽減します。

FSx for ONTAP は、フルマネージド型バックアップとリージョン間の災害対策サポートを備えた高可用性で耐久性のあるストレージも提供します。データの保護と保護を容易にするために、FSx for ONTAP は一般的なデータセキュリティおよびウイルス対策アプリケーションをサポートしています。

NetApp ONTAP をオンプレミスで使用するお客様にとって、FSx for ONTAP は、アプリケーションコードやデータの管理方法を変更 AWS することなく、ファイルベースのアプリケーションをオンプレミスから に移行、バックアップ、またはバーストするための理想的なソリューションです。

フルマネージドサービスとして、Amazon FSx for NetApp ONTAP は、クラウドでの信頼性、パフォーマンス、安全な共有ファイルストレージを簡単に起動およびスケーリングできます。FSx for ONTAP では、次のことを心配する必要がなくなります。

- ファイルサーバとストレージボリュームの設定とプロビジョニング
- データのレプリケーション
- ファイルサーバソフトウェアのインストールとパッチ適用
- ハードウェア障害の検出と対処

- フェイルオーバーとフェイルバックの管理
- バックアップの手動による実行

FSx for ONTAP は、 (IAM)、Amazon 、 AWS Key Management Service （ AWS KMS ） WorkSpaces、 などの AWS Identity and Access Management 他の AWS サービスとの豊富な統合も提供します AWS CloudTrail。

トピック

FSx for ONTAP の特徴

FSx for ONTAP では、次を備えたフルマネージド型のファイルストレージソリューションが得られます。

- 1 つの名前空間でのペタバイトスケーリングのデータセットのサポート
- ファイルシステムあたり最大数十ギガバイト/秒 (Gbps) のスループット
- ネットワークファイルシステム (NFS)、サーバーメッセージブロック (SMB)、インターネットスモールコンピュータシステムインターフェイス (iSCSI) プロトコルを使用したデータへのマルチプロトコルアクセス
- 可用性が高く耐久性に優れた、マルチ AZ およびシングル AZ デプロイのオプション
- アクセスパターンに応じて、アクセス頻度の低いデータをより低コストのストレージ階層に自動的に移行し、ストレージコストを削減する自動データ階層化機能
- データ圧縮、重複排除、圧縮によるストレージ消費の削減
- NetAppの SnapMirror レプリケーション機能のサポート
- NetAppのオンプレミスキャッシュソリューションのサポート: NetApp グローバルファイルキャッシュおよび FlexCache
- ネイティブ AWS または NetApp ツールと API オペレーションを使用したアクセスと管理のサポート

  - AWS Management Console、 AWS Command Line Interface （ AWS CLI ）、 SDKs
  - NetApp ONTAP CLI、REST API、および BlueXP
- 次のデータ保護およびセキュリティ機能のサポート。
  - を使用したファイルシステムデータと保管時のバックアップの暗号化 AWS KMS keys
  - SMB Kerberos セッションキーを使用した転送中のデータの暗号化
  - オンデマンドのアンチウイルススキャン
  - Microsoft アクティブディレクトリを使用した認証と認可
  - ファイルアクセスの監査
  - NetApp SnapLock Compliance ボリュームと Enterprise ボリュームをサポートする WORM 機能

セキュリティとデータ保護

Amazon FSx は、ユーザーのデータが確実に保護されるよう、複数のレベルのセキュリティとコンプライアンスを提供します。 AWS Key Management Service () で管理するキーを使用して、ファイルシステムおよびバックアップに保管中のデータを自動的に暗号化しますAWS KMS。Kerberos for NFS および SMB クライアントを使用して、転送中のデータを暗号化することもできます。

Amazon FSx は、次のスタンダードに準拠していると評価されています。

- 国際標準化機構 (ISO)
- ペイメントカード業界データセキュリティ基準 (PCI DSS、Payment Card Industry Data Security Standard)
- システムおよび組織管理 (SOC) 認定
- 1996 年の医療保険の相互運用性と説明責任に関する法律 (HIPAA、The Health Insurance Portability and Accountability Act of 1996)

詳細については、「Amazon FSx for NetApp ONTAP でのデータ保護」を参照してください。

Amazon FSx では、次のレベルのアクセスコントロールも提供します。

- Amazon FSx は、Amazon Virtual Private Cloud (Amazon VPC) セキュリティグループを使用して、ファイルシステムレベルでアクセスコントロールを提供します。
- API レベルでは、Amazon FSx は AWS Identity and Access Management (IAM) アクセスポリシーを使用してアクセスコントロールを提供します。

- ファイルおよびフォルダーレベルでアクセスコントロールを提供するために、Amazon FSx は、Unix アクセス許可、NFS アクセスコントロールリスト (ACL)、および NTFS ACL をサポートしています。Amazon FSx をアクティブディレクトリ (AD) に参加すると、ファイルシステムにアクセスするユーザーは、アクティブディレクトリ認証情報を使用して認証できます。

Amazon FSx リソースでユーザーが実行したアクションを確認できるように、Amazon FSx は と統合 AWS CloudTrail して Amazon FSx API コールをモニタリングおよびログに記録します。詳細については、「AWS CloudTrail での FSx for ONTAP API コールのロギング」を参照してください。

さらに、Amazon FSx は、高い耐久性ファイルシステムバックアップでデータを保護します。Amazon FSx は毎日自動バックアップを実行し、いつでも追加のバックアップを取ることができます。詳細については、「データの保護」を参照してください。

FSx for ONTAP の料金

ファイルシステムについては、次のカテゴリに基づいて請求されます。

- SSD ストレージ容量 (ギガバイト/月あたり、または GB/月あたり)
- 3 IOPS / GB 以上にプロビジョニングした SSD IOPS (IOPS / 月あたり)
- スループット容量 (メガバイト / 秒 [MBps] / 月 あたり)
- 容量プールのストレージ消費量 (GB / 月あたり)
- 容量プールリクエスト (読み取りと書き込みあたり)
- バックアップストレージの消費量 (GB / 月あたり)

サービスに関連する料金の詳細については、「Amazon FSx for NetApp ONTAP の料金」を参照してください。

FSx for ONTAP フォーラム

Amazon FSxの使用中に問題が発生した場合は、FSx for ONTAP ディスカッションフォーラムを使用して回答を得てください。

Amazon FSx を初めてご使用のユーザーですか ?

Amazon FSx を初めて使用する場合は、以下のセクションを順に読むことをお勧めします。

1. を初めて使用する場合は AWS、「」を参照して をセットアップFSx for ONTAP の設定しますAWS アカウント。
2. 最初の Amazon FSx ファイルシステムを作成する準備ができたら、Amazon FSx for NetApp ONTAP の開始方法 の手順に従います。
3. パフォーマンスの詳細については、「Amazon FSx for NetApp ONTAP のパフォーマンス」を参照してください。
4. Amazon FSx セキュリティの詳細については、「Amazon FSx for NetApp ONTAP のセキュリティ」を参照してください。
5. Amazon FSx API の詳細については、「Amazon FSx API リファレンス」を参照してください。

Amazon FSx for NetApp ONTAP の仕組み

このトピックでは、Amazon FSx for NetApp ONTAP ファイルシステムの主な機能とその仕組みを紹介します。詳細な説明、実装に関する重要な詳細、設定手順が記載されたセクションへのリンクも掲載されています。 step-by-step

トピック

- FSx for ONTAP ファイルシステム
- ストレージ仮想マシン
- ボリューム
- ストレージ階層
- ストレージ効率
- NetApp ONTAP ファイルシステムの Amazon FSx に保存されているデータへのアクセス
- FSx for ONTAP リソースの管理

FSx for ONTAP ファイルシステム

ファイルシステムは、オンプレミスの ONTAP クラスタと同様に、ONTAP のプライマリ FSx リソースです。 NetApp ファイルシステムの SSD ストレージ容量とスループットキャパシティを指定して、ファイルシステムを作成する Amazon 仮想プライベートクラウド (VPC) を選択します。詳細については、「FSx for ONTAP ファイルシステムの管理」を参照してください。

ファイルシステムには、構成に応じて 1 ～ 12 の高可用性 (HA) ペアを設定できます。HA ペアは、アクティブ/スタンバイ構成の 2 台のファイルサーバーで構成されます。HA ペアが 1 つだけのファイルシステムは、スケールアップファイルシステムと呼ばれます。HA ペアが複数のファイルシステムは、スケールアウトファイルシステムと呼ばれます。詳細については、「高可用性 (HA) ペア」を参照してください。

ストレージ仮想マシン

ストレージ仮想マシン (SVM) は、データを管理およびアクセスするための独自の管理およびデータアクセスエンドポイントを備えた分離されたファイルサーバーです。FSx for ONTAP ファイルシステムのデータにアクセスすると、クライアントとワークステーションが SVM のエンドポイント IP

アドレスを使用して SVM とインターフェイスをとります。詳細については、「SVM の管理」を参照してください。

SVM を Microsoft Active Directory に登録して、ファイルアクセスの認証と認可を行うことができます。詳細については、「FSx for ONTAP で Microsoft アクティブディレクトリの使用」を参照してください。

ボリューム

FSx for ONTAP のボリュームは、データの整理とグループ化に使用する仮想リソースです。ボリュームは SVM 上でホストされる論理コンテナであり、ボリュームに格納されたデータはファイルシステムの物理ストレージ容量を消費します。

ボリュームを作成するときは、ボリュームのサイズを設定します。これにより、データが保存されているストレージ階層に関係なく、そのボリュームに格納できる物理データの量が決まります。また、RW (読み取り/書き込み可能) または DP (データ保護) のいずれかのボリュームタイプも設定します。DP ボリュームは読み取り専用で、OR 関係のデスティネーションとして使用できます。NetApp SnapMirror SnapVault

FSx for ONTAP ボリュームはシンプロビジョニングされます。つまり、ボリュームに保存されているデータのストレージ容量しか消費しません。シンプロビジョニングされたボリュームでは、ストレージ容量は事前に予約されません。代わりに、ストレージは必要に応じて動的に割り当てられます。ボリュームまたは LUN 内のデータが削除されると、空き領域が解放されてファイルシステムに戻されます。たとえば、10 TiB の空きストレージ容量を設定したファイルシステムに 10 TiB のボリュームを 3 つ作成できます。ただし、3 つのボリュームに格納されているデータの合計量が常に 10 TiB を超えないことが条件です。1 つのボリュームに物理的に保存されているデータ量は、ストレージ容量全体の消費量にカウントされます。詳細については、「FSx for ONTAP ボリュームの管理」を参照してください。

ストレージ階層

FSx for ONTAP ファイルシステムには、プライマリストレージと容量プールストレージという 2 つの storage tiers (ストレージ階層) があります。プライマリストレージは、データセットのアクティブな部分に合わせて設計された、プロビジョニングされ、スケーラブルでハイパフォーマンスな SSD ストレージです。容量プールストレージは、ペタバイトサイズまで拡張できる完全に伸縮性のあるストレージ階層で、アクセス頻度の低いに対してコストが最適化されます。ボリュームに書き込むデータは、ストレージ階層の容量を消費します。詳細については、「FSx for ONTAP ストレージ階層」を参照してください。

データ階層化

データ階層化は、Amazon FSx for NetApp ONTAP が SSD とキャパシティプールのストレージ階層間でデータを自動的に移動するプロセスです。各ボリュームには、非アクティブ (コールド) になったときにデータをキャパシティ階層に移動するかどうかを制御する階層化ポリシーがあります。ボリュームの階層化ポリシーの冷却期間によって、データが非アクティブ (コールド) になる時期が決まります。詳細については、「ボリュームデータの階層化」を参照してください。

ストレージ効率

Amazon FSx for NetApp ONTAP は、ONTAP のブロックレベルのストレージ効率化機能 (圧縮、圧縮、重複排除) をサポートしているため、データが消費するストレージ容量を削減できます。ストレージ効率の機能により、SSD ストレージ、容量プールストレージ、およびバックアップにおけるデータのフットプリントを削減できます。パフォーマンスを犠牲にすることなく、汎用ファイル共有ワークロードの一般的なストレージ容量の削減効果は、SSD と容量プールの両方のストレージ階層で圧縮、重複排除、および圧縮による 65% です。詳細については、「FSx for ONTAP ストレージの効率化」を参照してください。

NetApp ONTAP ファイルシステムの Amazon FSx に保存されているデータへのアクセス

NFS (v3、v4、v4.1、v4.2) と SMB プロトコルを介して複数の Linux、Windows、または macOS クライアントから同時に ONTAP ボリュームのデータにアクセスすることができます。iSCSI (ブロック) プロトコルを使用してデータにアクセスすることもできます。詳細については、「データへのアクセス」を参照してください。

FSx for ONTAP リソースの管理

FSx for ONTAP ファイルシステムと相互作用して、そのリソースを管理することができるいくつかの方法があります。FSx for ONTAP リソースは、と ONTAP AWS NetApp 管理ツールの両方を使用して管理できます。

- AWS 管理ツール
  - ザ・ AWS Management Console
  - ザ・ AWS Command Line Interface (AWS CLI)
  - Amazon FSx API と SDK

    - AWS CloudFormation
- NetApp 管理ツール:
    - NetApp ブルーXP
    - NetApp ONTAP CLI
    - NetApp ONTAP REST API

詳細については、「リソースの管理」を参照してください。

FSx for ONTAP の設定

Amazon FSx を初めて使用する場合は、事前に以下のタスクを実行してください。

1. にサインアップする AWS アカウント
2. 管理アクセスを持つユーザーを作成する

トピック

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール) 」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルへのサインイン」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

次のステップ

FSx for ONTAP の使用をスタートするには、Amazon FSx for NetApp ONTAP の開始方法 Amazon FSx リソースの作成手順を参照してください。

Amazon FSx for NetApp ONTAP の開始方法

Amazon FSx for NetApp ONTAP の使用を開始する方法について説明します。この入門演習では、次のステップが含まれます。

トピック

ステップ 1: Amazon FSx for NetApp ONTAP ファイルシステムを作成する

Amazon FSx コンソールには、ファイルシステムを作成するために、[Quick create] (クイック作成) オプションと [Standard create] (標準作成) オプションの 2 つのオプションがあります。サービス推奨設定で Amazon FSx for NetApp ONTAP ファイルシステムを迅速かつ簡単に作成するには、クイック作成オプションを使用します。

[クイック作成] オプションでは、1 つの高可用性ペア (HA)、1 つのストレージ仮想マシン (SVM)、および 1 つのボリュームを持つファイルシステムが作成しされます。[Quick create] (クイック作成) オプションを使用すると、ネットワークファイルシステム (NFS) プロトコル経由の Linux インスタンスからのデータアクセスを許可するように、このファイルシステムが設定されます。ファイルシステムを作成したら、必要に応じて追加の SVM とボリュームを作成できます。これには、サーバーメッセージブロック (SMB) プロトコル経由で Windows および macOS クライアントからのアクセスを許可するアクティブディレクトリに参加している SVM も含まれます。

標準作成オプションを使用してカスタマイズされた設定でファイルシステムを作成する方法、および AWS CLI と API を使用する方法については、「」を参照してくださいFSx for ONTAP ファイルシステムの作成。

ファイルシステムを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ダッシュボードで ファイルシステムの作成 を選択し、ファイルシステム作成ウィザードを起動します。

3. ファイルシステムタイプの選択ページで、Amazon FSx for NetApp ONTAP を選択し、次へ を選択します。[Create ONTAP file system] (ONTAP ファイルシステムを作成する) ページが表示されます。
4. [Creation method] (作成方法) については、[Quick create] (クイック作成) を選択します。
5. [Quick configuration] (クイック設定) セクションで、[File system name - optional] (ファイルシステム名-オプション) ごとに、ファイルシステムの名前を入力します。ファイルシステムに名前を付けると、ファイルシステムを簡単に検索および管理できます。最大 256 の Unicode 文字、ホワイトスペース、数字、および特殊文字を使用できます。+- (ハイフン) =。_ (下線) :/
6. [Deployment type] (デプロイタイプ) では [Multi-AZ] (マルチ AZ) または [Single-AZ] (シングル AZ) を選択します。

   - Multi-AZ (マルチ AZ) ファイルシステムは、データをレプリケートし、同じ AWS リージョン内の複数のアベイラビリティーゾーンにまたがるフェイルオーバーをサポートします。
   - [Single-AZ] (シングル AZ) ファイルシステムでは、データをレプリケートし、単一のアベイラビリティーゾーン内で自動フェイルオーバーを行います。

   詳細については、「可用性と耐久性」を参照してください。
7. SSD ストレージ容量 の場合、ファイルシステムのストレージ容量をギビバイト (GiB) で指定します。1,024 ~ 196,608 の範囲の任意の整数を入力します。SSD ストレージ容量がさらに必要な場合は、[スタンダード作成] を使用できます。詳細については、「ファイルシステムの作成方法 (コンソール)」を参照してください。

   ファイルシステムの作成後でも、いつでも必要に応じてストレージ容量を増やすことができます。詳細については、「ストレージ容量の管理」を参照してください。
8. スループットキャパシティについては、Amazon FSx は SSD ストレージに基づいて自動的にスループットキャパシティを推奨します。ファイルシステムのスループット (最大 4,096 MBps) を選択することもできます。さらにスループットキャパシティが必要な場合は、標準作成 を使用できます。
9. [Virtual Private Cloud (VPC)] (仮想プライベートクラウド (VPC)) については、ファイルシステムに関連付ける Amazon VPC を選択します。
10. ストレージ効率 については、[Enabled] (有効) を選択し、ONTAP ストレージ効率機能 (圧縮、重複排除、コンパクション) をオンにするか [Disabled] (無効) を選択してそれらをオフにします。
11. (マルチ AZ のみ) [Endpoint IP address range] (エンドポイント IP アドレスの範囲) で、ファイルシステムにアクセスするためのエンドポイントが作成され、IP アドレスの範囲を指定します。

エンドポイント IP アドレス範囲の [Quick create] (クイック作成) オプションを選択します：

- [Unallocated IP address range from your VPC] (VPC からの未割り当ての IP アドレス範囲) — このオプションを選択すると、Amazon FSx は VPC のプライマリ CIDR 範囲の最後の 64 個の IP アドレスを、ファイルシステムのエンドポイント IP アドレス範囲として使用します。このオプションを複数回選択すると、この範囲は複数のファイルシステムで共有されることに注意してください。

  > **Note**
  >
  > - 作成する各ファイルシステムは、この範囲から 2 つの IP アドレスを消費します。1 つはクラスター用、もう 1 つは最初の SVM 用です。最初と最後の IP アドレスも予約されます。SVM を追加するたびに、ファイルシステムは別の IP アドレスを使用します。例えば、10 個の SVM をホストするファイルシステムは、11 個の IP アドレスを使用します。他のファイルシステムも同様に動作します。2 つの初期 IP アドレスと追加の SVM ごとに 1 つずつ使用します。同じ IP アドレス範囲を使用し、それぞれが単一の SVM を使用するファイルシステムの最大数は 31 です。
  > - VPC のプライマリ CIDR 範囲の最後の 64 個の IP アドレスのいずれかがサブネットで使用されている場合、このオプションはグレー表示されます。

- [Floating IP address range outside your VPC] (VPC 外のフローティング IP アドレス範囲) — Amazon FSx が、同じ VPC とルートテーブルを持つ他のファイルシステムでまだ使用されていない 198.19.x.0/24 アドレス範囲を使用するようにするには、このオプションを選択します。

[Standard create] (標準作成) オプションで独自の IP アドレス範囲を指定することもできます。

12. [Next] (次へ) を選択して、[Create ONTAP file system] (ONTAP ファイルシステムの作成) ページでファイルシステムの構成を確認します。ファイルシステムの作成後に変更可能なファイルシステム設定を書き留めておきます。
13. [Create ONTAP file system] (ファイルシステムを作成する) を選択します。

[Quick create] (クイック作成) は 1 つの SVM (`fsx` という名前) とボリューム (`vol1` という名前) を作成します。ボリュームには、`/vol1` のジャンクションパスと [Auto] (自動) の容量プールの階層化ポリシー (自動的に 31 日間アクセスされていないデータを階層化して容量プールストレージコストを軽減する) があります。デフォルトのスナップショットポリシーがデフォルトのボリュームに割り

当てられます。ファイルシステムデータは、保管時にデフォルトのサービスマネージド AWS KMS キーを使用して暗号化されます。

ステップ 2: Amazon EC2 Linux インスタンスからファイルシステムをマウントする

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスからファイルシステムをマウントできます。この手順では、Amazon Linux 2 を実行しているインスタンスを使用します。

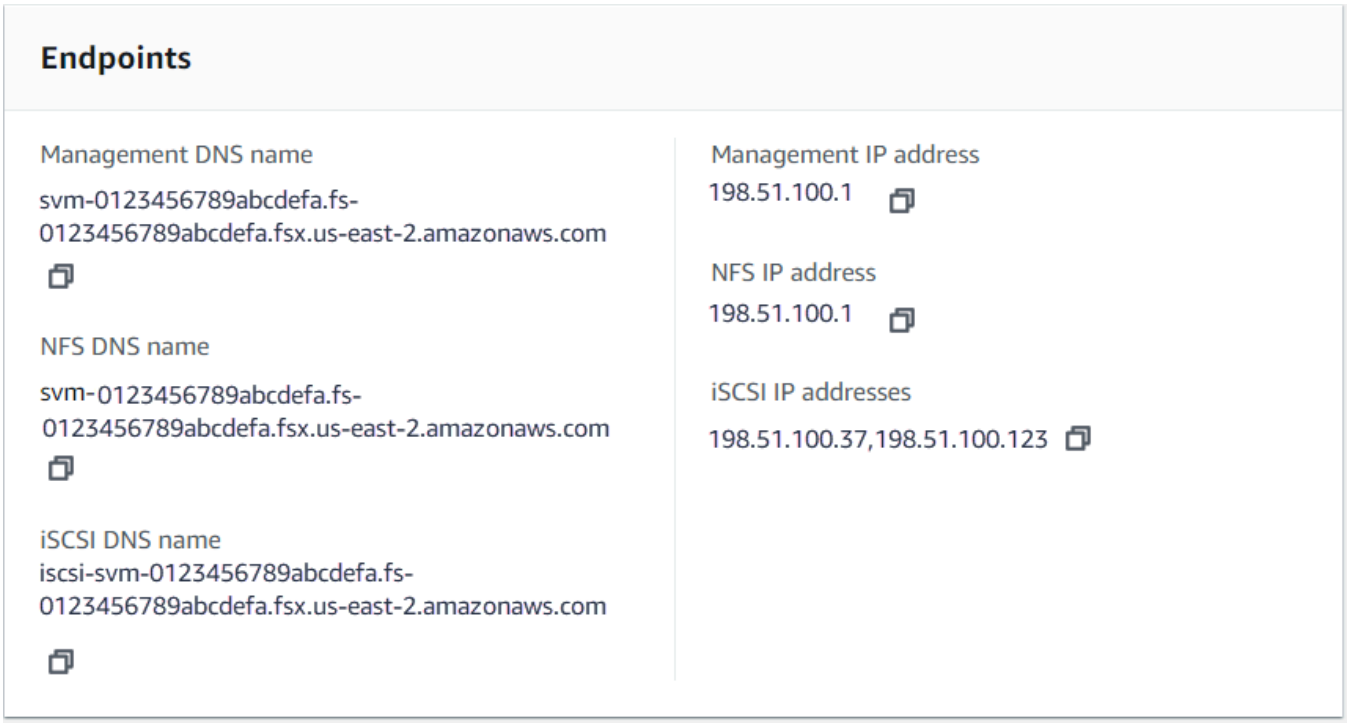
Amazon EC2 からファイルシステムをマウントするには

1. https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. ファイルシステムと同じ仮想プライベートクラウド (VPC) にある Amazon Linux 2 を実行する Amazon EC2 インスタンスを作成または選択します。インスタンスの起動の詳細については、Amazon EC2 ユーザーガイド」の「ステップ 1: インスタンスを起動する」を参照してください。
3. Amazon EC2 Linux インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2
4. Amazon EC2 インスタンスでセキュアシェル (SSH) を使用してターミナルを開き、適切な認証情報を使用してログインします。
5. 次のコマンドを使用して、Amazon EC2 インスタンスでボリュームのマウントポイントとして使用するディレクトリを作成します。次の例では、`########` を独自の情報に置き換えます。

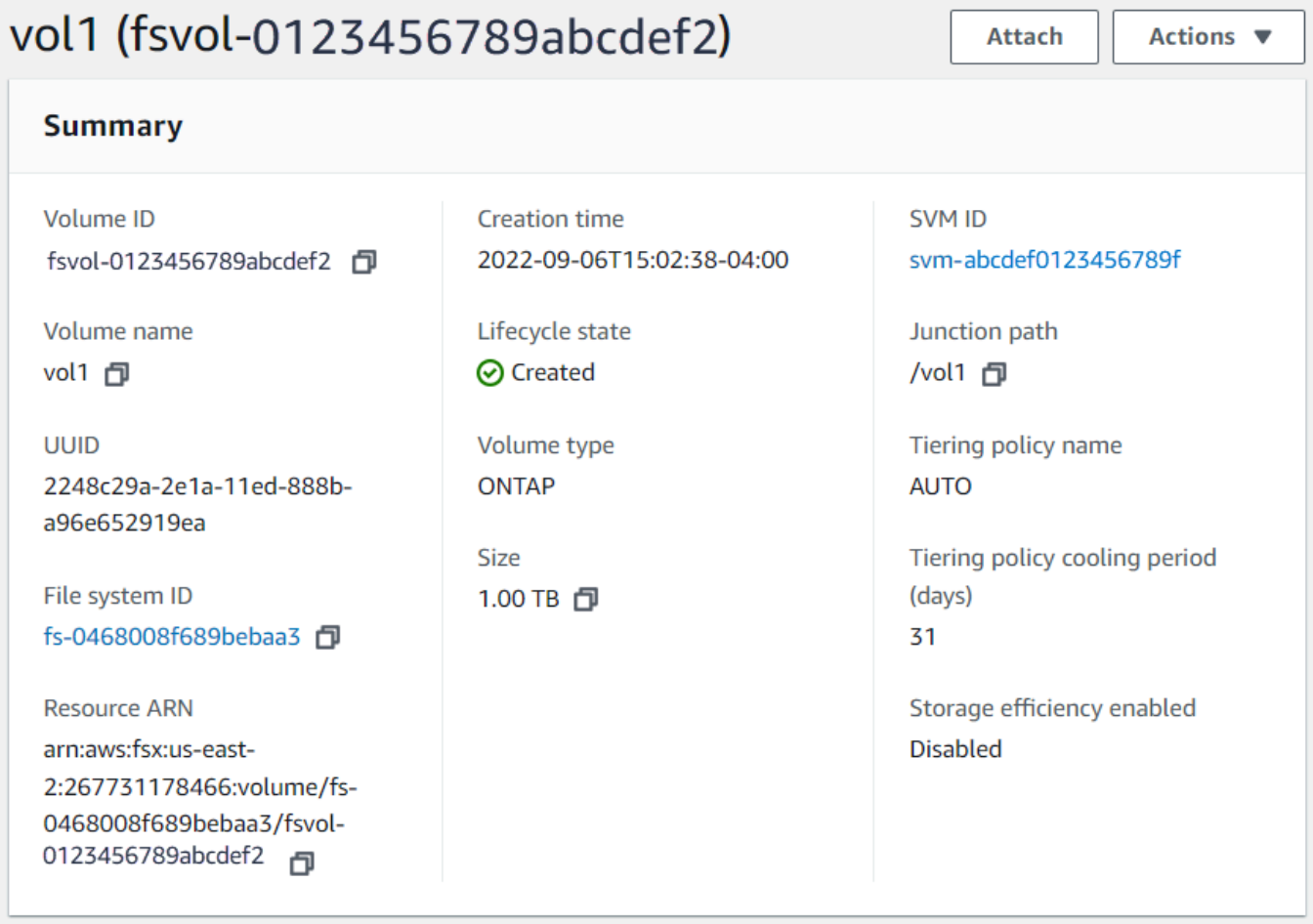
   ```
   $ sudo mkdir /mount-point
   ```

6. Amazon FSx for NetApp ONTAP ファイルシステムを、作成したディレクトリにマウントします。次の例と類似する `mount` コマンドを使用します。次の例では、次のプレースホルダ値を独自の情報に置き換えます。

   - *`nfs_version`* — 使用している NFS バージョンである FSx for ONTAP は、バージョン 3、4.0、4.1、および 4.2 をサポートします。
   - *`nfs-dns-name`* — マウントするボリュームがあるストレージ仮想マシン (SVM) の NFS DNS 名です。Amazon FSx コンソールで NFS DNS 名を確認するには、[Storage virtual machines] (ストレージ仮想マシン) を選択し、マウントするボリュームが存在する SVM を選択します。NFS DNS 名は、次の図に示すように [Endpoints] (エンドポイント) パネルにあります。



- *volume-junction-path* — マウントするボリュームの接続パスです。ボリュームのジャンクションパスは、以下の画像に示すように、Amazon FSx コンソールのボリューム詳細ページの [Summary] (概要) パネルで確認できます。



- *mount-point* — EC2 インスタンスにボリュームのマウントポイント用に作成したディレクトリの名前です。

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

次のコマンドでは、値の例を使用しています。

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Amazon EC2 インスタンスに問題がある場合 (接続のタイムアウトなど)、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのトラブルシューティング」を参照してください。 Amazon EC2

ステップ 3: リソースをクリーンアップする

この演習が完了したら、以下の手順に従ってリソースをクリーンアップし、 AWS アカウントを保護します。

リソースをクリーンアップするには

1. Amazon EC2 コンソールで、インスタンスを終了します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」を参照してください。 Amazon EC2
2. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
3. Amazon FSx コンソールで、SVM のルートボリュームではないすべての FSx for ONTAP ボリュームを削除します。詳細については、「ボリュームの削除」を参照してください。
4. FSx for ONTAP SVM をすべて削除します。詳細については、「ストレージ仮想マシン (SVM) の削除」を参照してください。
5. Amazon FSx コンソールで、ファイルシステムを削除します。ファイルシステムを削除すると、すべての自動バックアップが自動的に削除されます。ただし、手動で作成したバックアップは削除する必要があります。次のステップでこのプロセスを示します。

    a. コンソールダッシュボードから、この演習用に作成したファイルシステムの名前を選択します。

    b. [Actions] (アクション) で、[Delete file system] (ファイルシステムの削除) を選択します。

    c. [Delete file system] (ファイルシステムの削除) ダイアログボックスに、[File system ID] (ファイルシステム ID) ボックスで削除するファイルシステムの ID を入力します。

    d. [Delete file system] (ファイルシステムの削除) を選択します。

    e. Amazon FSx がファイルシステムを削除する間、ダッシュボードの状態が [DELETING] (削除中) に変更されます。ファイルシステムが削除されると、そのファイルシステムはダッシュボードに表示されなくなります。自動バックアップは、ファイルシステムとともに削除されます。

    f. これで、ファイルシステムに対して手動で作成されたバックアップを削除できます。左側のナビゲーションから、[Backups] (バックアップ) を選択します。

    g. ダッシュボードから、選択したファイルシステムと同じ [File system ID] (ファイルシステム ID) を持つバックアップをし、[Delete backup] (バックアップの削除) を選択します。最終的なバックアップを作成した場合は、必ず最終バックアップを保持してください。

h. [Delete backup] (バックアップの削除) ダイアログボックスが開きます。削除するバックアップの ID のチェックボックスをオンにし、[Delete backup] (バックアップの削除) を選択します。

これで、Amazon FSx ファイルシステムと関連する自動バックアップが、削除することを選択した手動バックアップとともに削除されます。

データへのアクセス

Amazon FSx ファイルシステムには、 環境とオンプレミス環境の両方でサポートされているさまざまなクライアント AWS クラウド とメソッドを使用してアクセスできます。

各 SVM には、 NetApp ONTAP CLI または REST API を使用してデータにアクセスしたり、SVM を管理するために使用される 4 つのエンドポイントがあります。

- `Nfs` - ネットワークファイルシステム (NFS、Network File System) プロトコルを使用して接続する場合
- `Smb` - サービスメッセージブロック (SMB、Service Message Block) プロトコルを使用して接続する場合 (SVM がアクティブディレクトリに参加している場合、またはワークグループを使用している場合)
- `Iscsi` — Internet Small Computer Systems Interface (iSCSI) プロトコル (スケールアップファイルシステムのみ) を使用して接続する場合。
- `Management` – NetApp ONTAP CLI、API、または NetApp BlueXP を使用して SVMs を管理する場合

トピック

サポートされているクライアント

FSx for ONTAP ファイルシステムは、さまざまなコンピューティングインスタンスおよびオペレーティングシステムからのデータへのアクセスをサポートしています。これは、ネットワークファイルシステム (NFS) プロトコル (v3、v4.0、v4.1、v4.2)、サーバーメッセージブロック (SMB) プロトコルのすべてのバージョン (2.0、3.0、3.1.1 を含む)、およびインターネットスモールコンピュータシステムインターフェイス (iSCSI) プロトコルを使用したアクセスをサポートします。

> **Important**
>
> Amazon FSxは、公開インターネットからのファイルシステムへのアクセスをサポートしていません。Amazon FSx は、インターネットから到達可能なパブリック IP アドレスである Elastic IP アドレスを自動的にデタッチして、ファイルシステムの Elastic Network Interface にアタッチします。

FSx for ONTAP では、次の AWS コンピューティングインスタンスがサポートされています。

- NFS または SMB をサポートする Linux、Microsoft Windows、および MacOS を実行する Amazon Elastic Compute Cloud (Amazon EC2) インスタンス。詳細については、「ボリュームをマウントする」を参照してください。
- Amazon EC2 Windows および Linux インスタンス上の Amazon Elastic Container Service (Amazon ECS) Docker コンテナ。詳細については、「FSx for ONTAP で Amazon Elastic Container Service を使用する」を参照してください。
- Amazon Elastic Kubernetes Service – 詳細については、「Amazon EKS ユーザーガイド」の「Amazon FSx for NetApp ONTAP CSI ドライバー」を参照してください。
- Red Hat OpenShift Service on AWS (ROSA) – 詳細については、「Red Hat OpenShift Service on ユーザーガイド」の「Red Hat Service on AWSとは」を参照してください。 OpenShift AWS
- Amazon WorkSpaces インスタンス。詳細については、「FSx for ONTAP での Amazon WorkSpaces の使用」を参照してください。
- Amazon AppStream 2.0 インスタンス。
- AWS Lambda – 詳細については、 AWS ブログ記事「Amazon FSx によるサーバーレスワークロードの SMB アクセスの有効化」を参照してください。
- VMware Cloud on AWS 環境で実行されている仮想マシン (VMs)。詳細については、「Configure Amazon FSx for NetApp ONTAP as External Storage」およびVMware Cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide」を参照してください。

マウントされると、FSx for ONTAP ファイルシステムは、NFS および SMB 上のローカルディレクトリまたはドライブ文字として表示されます。これにより、最大数千のクライアントから同時にアクセスできる、フルマネージド型共有ネットワークファイルストレージが提供されます。iSCSI LUN は、iSCSI 上にマウントすると、ブロックデバイスとしてアクセスできます。

内からのデータへのアクセス AWS

Amazon FSx の各ファイルシステムは、仮想プライベートクラウド (VPC) に関連付けられています。FSx for ONTAP ファイルシステムには、アベイラビリティーゾーンに関係なく、ファイルシステムの VPC 内の任意の場所からアクセスできます。異なる AWS アカウントまたは にある他の VPCs からファイルシステムにアクセスすることもできます AWS リージョン。以降のセクションで説明する FSx for ONTAP リソースへのアクセスの要件に加えて、データと管理トラフィックがファイルシステムとクライアントの間を移動できるようファイルシステムの VPC セキュリティグループが設定されていることを確認する必要もあります。必要なポートでのセキュリティグループの設定の詳細については、「Amazon VPC セキュリティグループ」を参照してください。

トピック

- 同じ VPC 内からデータへのアクセス
- デプロイ用の VPC の外部からのデータへのアクセス

同じ VPC 内からデータへのアクセス

Amazon FSx for NetApp ONTAP ファイルシステムを作成するときは、そのファイルシステムが存在する Amazon VPC を選択します。Amazon FSx for NetApp ONTAP ファイルシステムに関連付けられているすべての SVMs とボリュームも同じ VPC にあります。ボリュームをマウントするときに、ファイルシステムとボリュームをマウントするクライアントが同じ VPC と にある場合は AWS アカウント、クライアントに応じて SVM の DNS 名とボリュームジャンクションまたは SMB 共有を使用できます。詳細については、「ボリュームをマウントする」を参照してください。

クライアントとボリュームがファイルシステムのサブネットまたはマルチ AZ ファイルシステムの優先サブネットと同じアベイラビリティーゾーンにある場合、最適なパフォーマンスを実現できます。ファイルシステムのサブネットまたは優先サブネットを識別するには、Amazon FSx コンソールで [ファイルシステム] を選択し、マウントしているボリュームがある ONTAP ファイルシステムを選択します。サブネットまたは優先サブネット (マルチ AZ) が [サブネット] または [優先サブネット] に表示されます。

デプロイ用の VPC の外部からのデータへのアクセス

このセクションでは、ファイルシステムのデプロイ VPC 外の AWS 場所から FSx for ONTAP ファイルシステムのエンドポイントにアクセスする方法について説明します。

マルチ AZ ファイルシステム上の NFS、SMB、ONTAP 管理エンドポイントにアクセスする

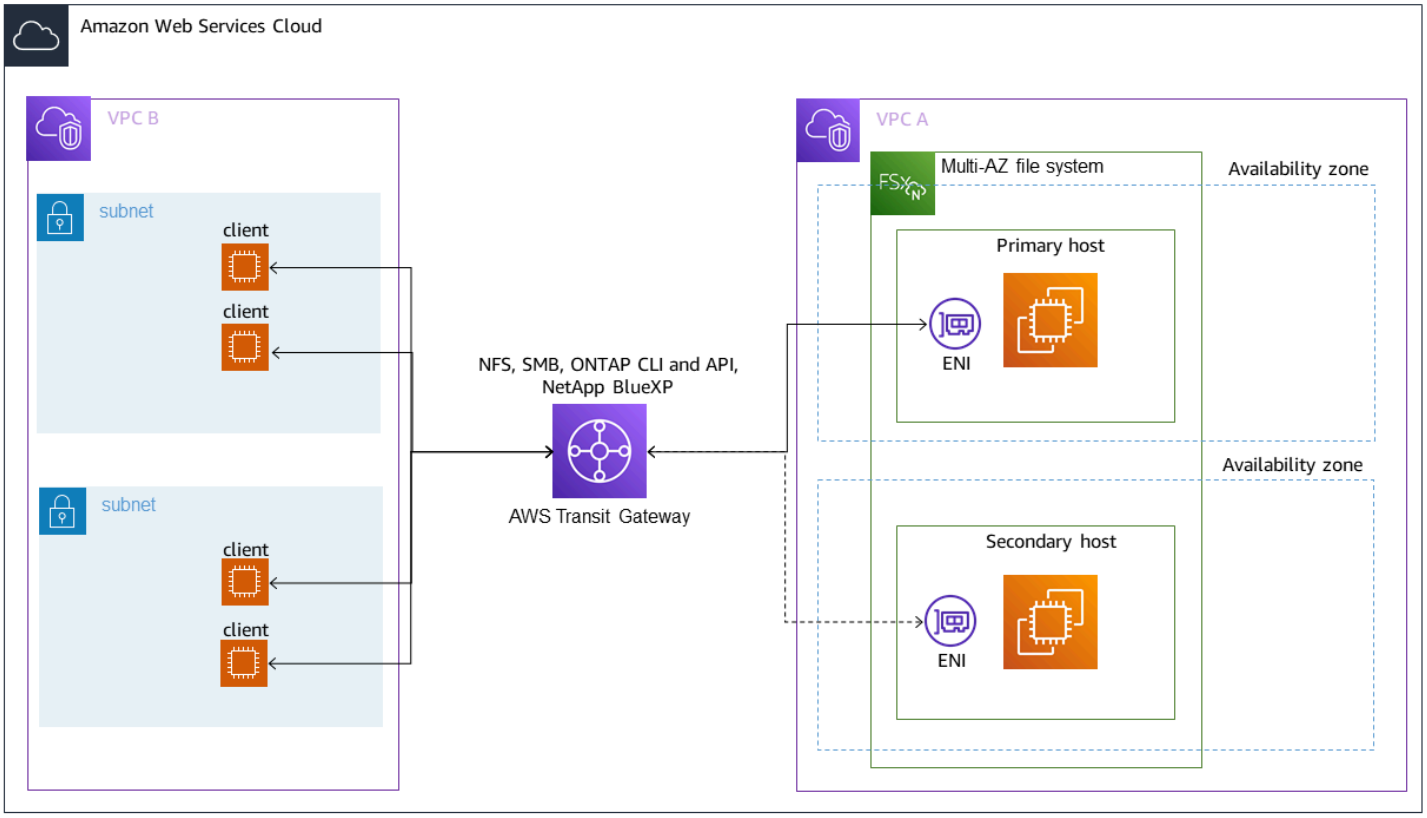
Amazon FSx for ONTAP マルチ AZ ファイルシステムの NFS、SMB、 NetApp ONTAP 管理エンドポイントは、フローティングインターネットプロトコル (IP) アドレスを使用するため、接続されたクライアントはフェイルオーバーイベント中に優先ファイルサーバーとスタンバイファイルサーバー間でシームレスに移行できます。フェイルオーバーについての詳細は、「FSx for ONTAP のフェイルオーバープロセス」を参照してください。

これらのフローティング IP アドレスは、ファイルシステムに関連付けられた VPC ルートテーブルに作成され、作成時に指定できるファイルシステムの `EndpointIpAddressRange` 内にあります。`EndpointIpAddressRange` は、ファイルシステムの作成方法に応じて、以下のアドレス範囲を使用します。

- Amazon FSx コンソールを使用して作成されたマルチ AZ ファイルシステムは、デフォルトでは、ファイルシステムの `EndpointIpAddressRange` に対して VPC のプライマリ CIDR 範囲の末尾 64 個の IP アドレスを使用します。
- AWS CLI または Amazon FSx API を使用して作成されたマルチ AZ ファイルシステムは、`EndpointIpAddressRange`デフォルトで のアドレスブロック内の IP `198.19.0.0/16` アドレス範囲を使用します。

フローティング IP アドレスをサポートするのは AWS Transit Gateway だけです。これは推移的なピアリング接続とも呼ばれます。VPC ピアリング AWS Direct Connect、、 は推移的なピアリングをサポート AWS VPN していません。そのため、ファイルシステムの VPC の外部にあるネットワークからこれらのインターフェイスにアクセスするには、Transit Gateway を使用する必要があります。

下の図は、アクセス元のクライアントとは別の VPC にあるマルチ AZ ファイルシステムに対する NFS、SMB、または管理アクセスに Transit Gateway を使用する方法を示しています。



> **Note**
>
> 使用しているすべてのルートテーブルがマルチ AZ ファイルシステムに関連付けられていることを確認します。これにより、フェイルオーバー中に使用できなくなるのを防ぐことができます。Amazon VPC ルートテーブルとファイルシステムの関連付けの詳細については、「ファイルシステムの更新」を参照してください。

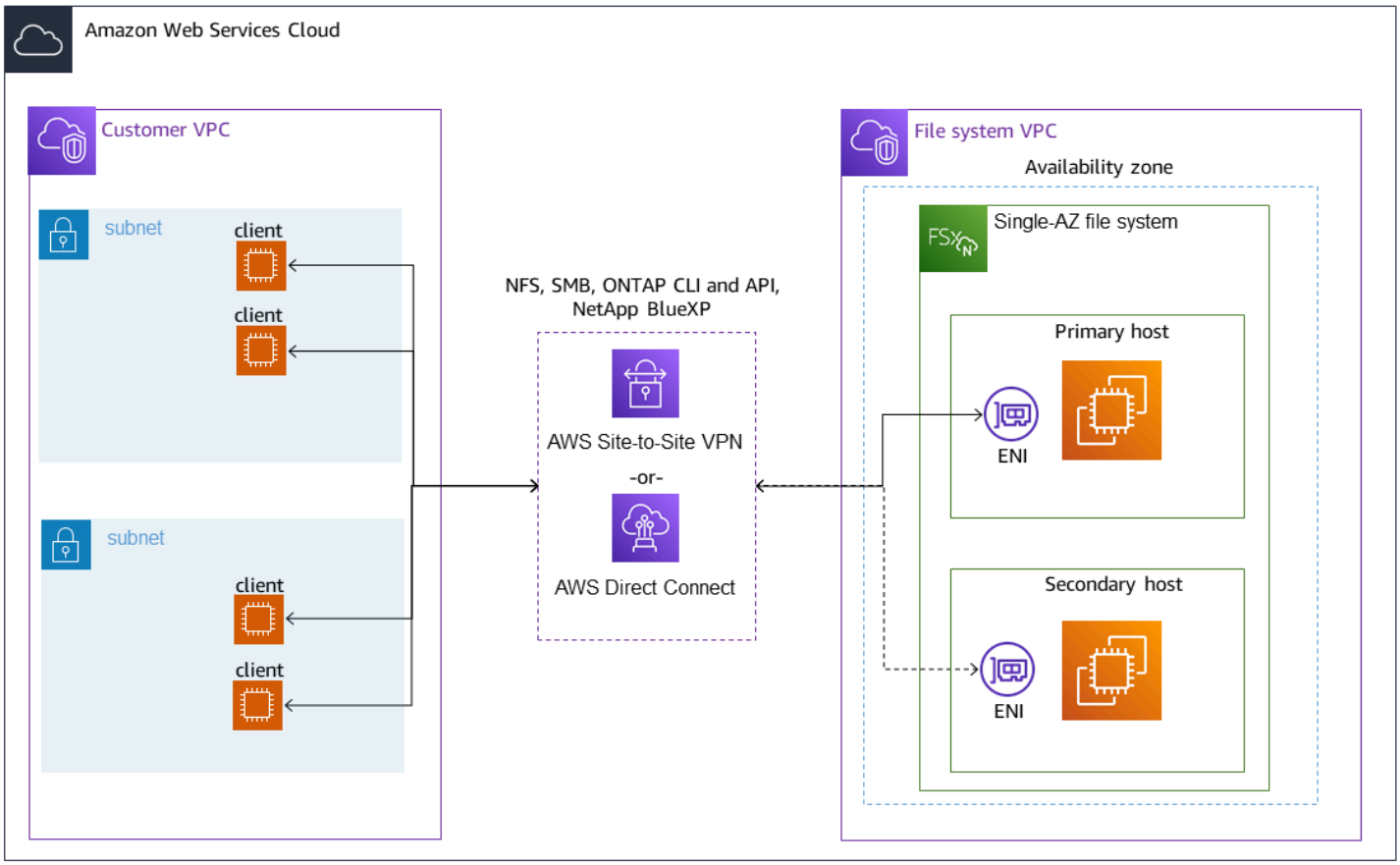
FSx for ONTAP ファイルシステムにアクセスするために Transit Gateway を使用する必要がある場合の詳細については、「Transit Gateway はどのような場合に必要ですか。」を参照してください。

シングル AZ ファイルシステムの NFS、SMB、または ONTAP CLI と API にアクセスする

NFS または SMB 経由の FSx for ONTAP のシングル AZ ファイルシステムへのアクセス、および ONTAP CLI または REST API を使用したファイルシステムの管理に使用されるエンドポイントは、アクティブなファイルサーバーの ENI 上のセカンダリ IP アドレスです。セカンダリ IP アドレスは VPC の CIDR 範囲内にあるため、クライアントは VPC ピアリングを使用するか AWS Direct

Connect、 を必要と AWS VPN せずにデータおよび管理ポートにアクセスできます AWS Transit Gateway。

次の図は、NFS、SMB、またはシングル AZ ファイルシステムにアクセスするクライアントとは異なる VPC にある管理アクセス AWS Direct Connect に AWS VPN または を使用する方法を示しています。



Transit Gateway はどのような場合に必要ですか。

マルチ AZ ファイルシステムに Transit Gateway が必要かどうかは、ファイルシステムのデータへのアクセスに使用する方法によって異なります。シングル AZ ファイルシステムには、Transit Gateway は必要ありません。次の表は、マルチ AZ ファイルシステムへのアクセスに AWS Transit Gateway 使用する必要がある場合を示しています。

データアクセス	Transit Gateway は必要ですか。
NFS、SMB、または NetApp ONTAP REST API、CLI、または BlueXP を介した FSx へのアクセス	次の場合のみ必要です。

データアクセス	Transit Gateway は必要ですか。
	• ピアリング接続されたネットワーク (オンプレミスなど) からアクセスし、 • FlexCache またはグローバルファイルキャッシュインスタンスを介して NetApp FSx にアクセスしていない
iSCSI 経由でデータにアクセスする	いいえ
SVM をアクティブディレクトリに結合する	いいえ
SnapMirror	いいえ
FlexCache キャッシュ	いいえ
グローバルファイルキャッシュ	いいえ

AWS Transit Gatewayを使用してルーティングを設定する

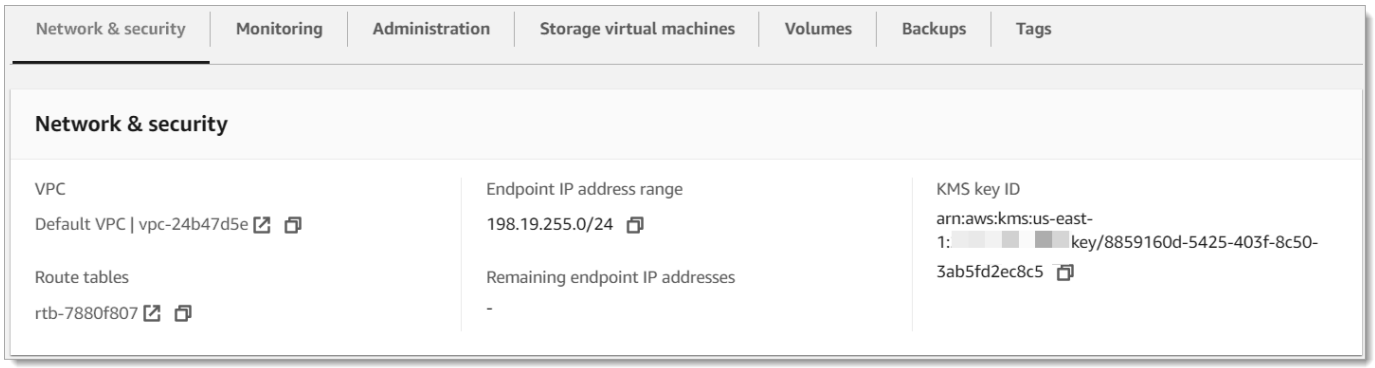
`EndpointIPAddressRange` VPC の CIDR 範囲外の を持つマルチ AZ ファイルシステムがある場合は、ピア接続ネットワークまたはオンプレミスネットワークからファイルシステムにアクセス AWS Transit Gateway するために、 で追加のルーティングを設定する必要があります。

> **Important**
>
> Transit Gateway を使用してマルチ AZ ファイルシステムにアクセスするには、ルートテーブルがファイルシステムに関連付けられているサブネットにトランジットゲートウェイの各アタッチメントを作成する必要があります。

> **Note**
>
> VPC の IP アドレス範囲内にある `EndpointIPAddressRange` を持つシングル AZ ファイルシステムまたはマルチ AZ ファイルシステムでは、中継ゲートウェイの設定は必要ありません。

を使用してルーティングを設定するには AWS Transit Gateway

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ピアリングされた接続ネットワークからのアクセスを設定する FSx for ONTAP ファイルシステムを選択します。
3. [Network & security] (ネットワークとセキュリティ) で [Endpoint IP address range] (エンドポイント IP アドレス範囲) をコピーします。



4. この IP アドレス範囲宛てのトラフィックをファイルシステムの VPC にルーティングするルートを Transit Gateway に追加します。詳細については、「Amazon VPC Transit Gateways」にある「トランジットゲートウェイの使用」を参照してください。
5. ピアリングされたネットワークから FSx for ONTAP ファイルシステムにアクセスできることを確認します。

ルートテーブルをファイルシステムに追加するには、「ファイルシステムの更新」を参照してください。

> **Note**
>
> 管理、NFS、および SMB エンドポイントの DNS レコードは、ファイルシステムと同じ VPC 内からのみ解決できます。ボリュームをマウントしたり、別のネットワークから管理ポートに接続したりするには、エンドポイントの IP アドレスを使用する必要があります。これらの IP アドレスは、時間の経過とともに変化しません。

デプロイ用 VPC の外部の iSCSI またはクラスター間エンドポイントにアクセスする

VPC ピアリングまたは を使用して AWS Transit Gateway 、ファイルシステムのデプロイ VPC の外部からファイルシステムの iSCSI エンドポイントまたはクラスター間エンドポイントにアクセスで

きます。VPC ピアリングを使用して、VPC 間で iSCSI とクラスター間トラフィックをルーティングできます。VPC ピアリング接続は 2 つの VPC の間のネットワーキング接続で、プライベート IPv4 アドレスを使用して 2 つの VPC 間でトラフィックをルーティングするために使用されます。VPC ピアリングを使用して、同じ 内 AWS リージョン または異なる 間で VPCs を接続できます AWS リージョン。詳細については、Amazon VPC ピアリング接続ガイドの「VPC ピア機能とは」を参照してください。

オンプレミスからデータにアクセスする

AWS VPN および AWS Direct Connect を使用して、オンプレミスから FSx for ONTAP ファイルシステムにアクセスできます。より具体的なユースケースのガイドラインについては、以下のセクションを参照してください。オンプレミスから異なる FSx for ONTAP リソースにアクセスするための以下の要件に加えて、ファイルシステムの VPC セキュリティグループがファイルシステムとクライアント間でデータをフローできるようにする必要があります。必要なポートのリストについては、「Amazon VPC セキュリティグループ」を参照してください。

オンプレミスから NFS、SMB、ONTAP CLI または REST API エンドポイントにアクセスする

このセクションでは、オンプレミスネットワークから FSx for ONTAP ファイルシステム上の NFS、SMB、ONTAP 管理ポートにアクセスする方法について説明します。

マルチ AZ ファイルシステムにアクセスする

Amazon FSx では、オンプレミスネットワークからマルチ AZ ファイルシステムにアクセス NetApp FlexCache するために、 NetAppまたはリモートグローバルファイルキャッシュ AWS Transit Gateway を使用するか、設定する必要があります。Amazon FSx は、マルチ AZ ファイルシステムで複数のアベイラビリティーゾーンにわたるフェイルオーバーをサポートするために NFS、SMB、ONTAP 管理エンドポイントに使用されるインターフェイスにフローティング IP アドレスを使用します。NFS、SMB、および管理エンドポイントはフローティング IPsを使用するため、を AWS Direct Connect または AWS Transit Gatewayと組み合わせて使用 AWS VPN して、オンプレミスネットワークからこれらのインターフェイスにアクセスする必要があります。これらのインターフェイスで使用するフローティング IP アドレスは、マルチ AZ ファイルシステムの作成時に指定した `EndpointIpAddressRange` 内にあります。Amazon FSx コンソールでファイルシステムを作成する場合、基本的に Amazon FSx は、ファイルシステムのエンドポイント IP アドレスの範囲として使用する VPC の基本 CIDR 範囲の最後の 64 個の IP アドレスを選択します。 AWS CLI または Amazon FSx API からファイルシステムを作成する場合、デフォルトでは、Amazon FSx は IP アド

レス範囲内の 198.19.0.0/16 IP アドレス範囲を選択します。フローティング IP アドレスを使用すると、フェイルオーバーが必要な場合にはクライアントをスタンバイファイルシステムへシームレスに移行できます。詳細については、「FSx for ONTAP のフェイルオーバープロセス」を参照してください。

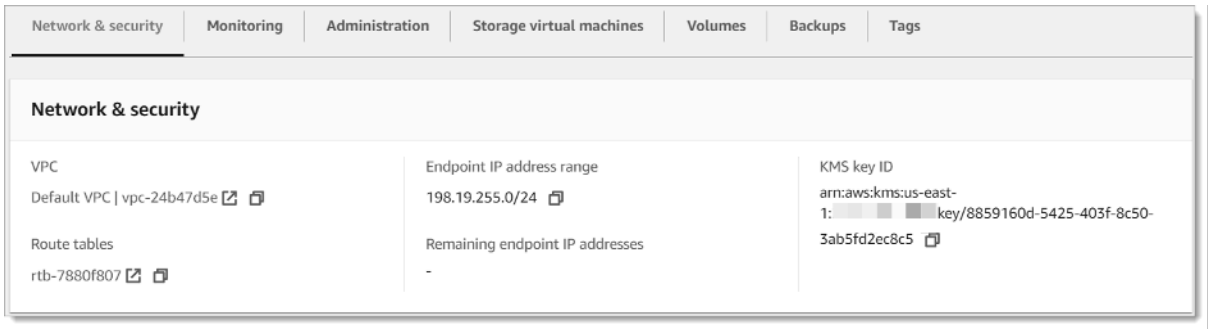
> **Important**
>
> Transit Gateway を使用してマルチ AZ ファイルシステムにアクセスするには、ルートテーブルがファイルシステムに関連付けられているサブネットにトランジットゲートウェイの各アタッチメントを作成する必要があります。

VPC の外部からアクセス AWS Transit Gateway するように を設定するには

EndpointIPAddressRange VPC の CIDR 範囲外の を持つマルチ AZ ファイルシステムがある場合は、ピア接続ネットワークまたはオンプレミスネットワークからファイルシステムにアクセス AWS Transit Gateway するために、 で追加のルーティングを設定する必要があります。

> **Note**
>
> VPC の IP アドレス範囲内にある EndpointIPAddressRange を持つシングル AZ ファイルシステムまたはマルチ AZ ファイルシステムでは、中継ゲートウェイの設定は必要ありません。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ピアリングされた接続ネットワークからのアクセスを設定する FSx for ONTAP ファイルシステムを選択します。
3. [Network & security] (ネットワークとセキュリティ) で [Endpoint IP address range] (エンドポイント IP アドレス範囲) をコピーします。



4. この IP アドレス範囲宛てのトラフィックをファイルシステムの VPC にルーティングするルートを Transit Gateway に追加します。詳細については、「Amazon VPC Transit Gateway ユーザーガイド」の「Transit Gateway の使用」を参照してください。
5. ピアリングされたネットワークから FSx for ONTAP ファイルシステムにアクセスできることを確認します。

> **Important**
>
> Transit Gateway を使用してマルチ AZ ファイルシステムにアクセスするには、ルートテーブルがファイルシステムに関連付けられているサブネットにトランジットゲートウェイの各アタッチメントを作成する必要があります。

ルートテーブルをファイルシステムに追加するには、「ファイルシステムの更新」を参照してください。

シングル AZ ファイルシステムにアクセスする

AWS Transit Gateway を使用してオンプレミスネットワークからデータにアクセスする要件は、シングル AZ ファイルシステムには存在しません。シングル AZ ファイルシステムは単一のサブネットにデプロイされ、ノード間のフェイルオーバーを提供するためにフローティング IP アドレスは必要ありません。代わりに、シングル AZ ファイルシステムでアクセスする IP アドレスは、ファイルシステムの VPC CIDR 範囲内のセカンダリ IP アドレスとして実装されるため、 AWS Transit Gateway を必要とせずに別のネットワークからデータにアクセスできるようになります。

オンプレミスからクラスター間エンドポイントにアクセスする

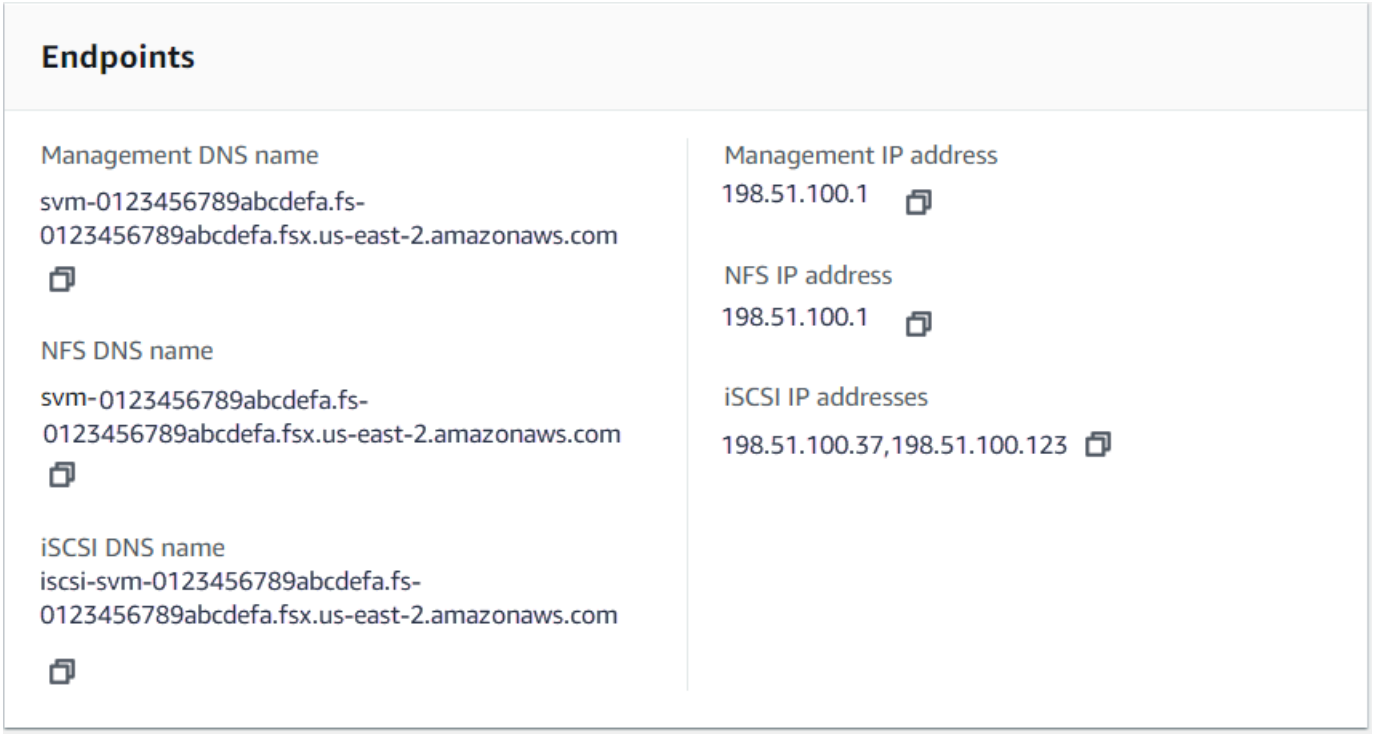
FSx for ONTAP のクラスター間エンドポイントは、オンプレミス NetApp デプロイと FSx for NetApp ONTAP 間を含む ONTAP ファイルシステム間のレプリケーショントラフィック専用です。レプリケーショントラフィックには SnapMirror、 FlexCache、、ストレージ FlexClone仮想マシン (SVMsと異なるファイルシステム間のボリューム間の関係、および NetApp グローバルファイルキャッシュが含まれます。クラスター間エンドポイントは、アクティブディレクトリのトラフィックにも使用されます。

ファイルシステムのクラスター間エンドポイントは FSx for ONTAP ファイルシステムを作成する際にユーザーが提供した VPC の CIDR 範囲内にある IP アドレスを使用するので、オンプレミスと AWS クラウドの間でクラスター間トラフィックをルーティングするために Transit Gateway を使用

する必要はありません。ただし、オンプレミスクライアントは引き続き AWS VPN または を使用して VPC への安全な接続 AWS Direct Connect を確立する必要があります。

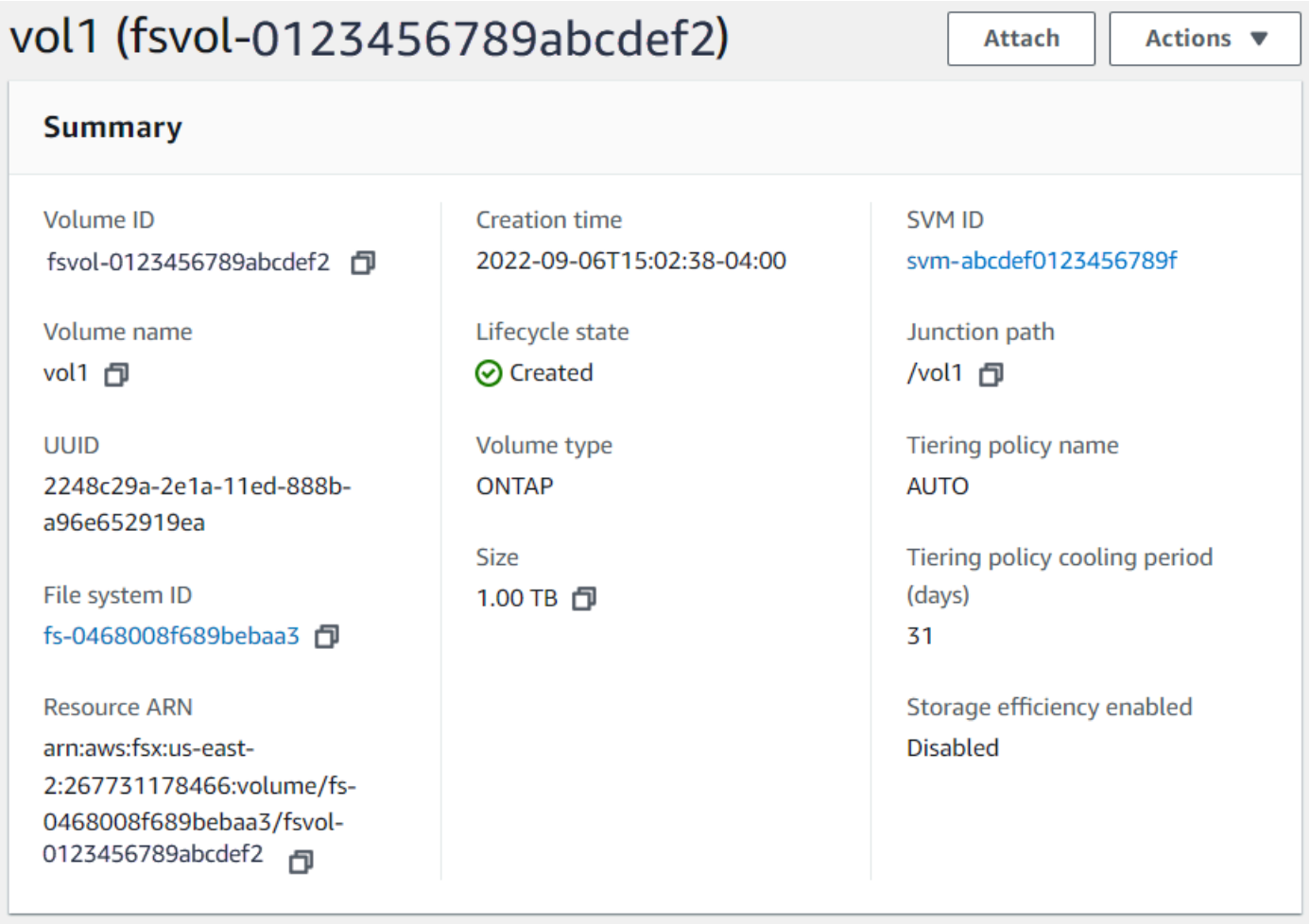
ボリュームをマウントする

FSx for ONTAP のデータにアクセスするには、クライアントにボリュームをマウントします。このセクションのコマンドは、ボリュームをマウントまたはアタッチするためにボリュームが作成される SVM の DNS 名または IP アドレスを使用します。次の図に示すように、SVM の DNS 名と IP アドレスは、Amazon FSx コンソールで [ONTAP > Storage virtual machines] (ONTAP > ストレージ仮想マシン) を選択するか、ファイルシステムの [File system details] (ファイルシステムの詳細) ページの [Storage virtual machine] (ストレージ仮想マシン) タブで確認できます。



または、DescribeStorageVirtualMachinesAPI オペレーションのレスポンスで確認できます。

ボリュームのジャンクションパスは、以下の画像に示すように、Amazon FSx コンソールのボリューム詳細ページの [Summary] (概要) パネルで確認できます。



トピック

- Linux クライアントでのマウント
- Microsoft Windows クライアントでのマウント
- macOS クライアントでのマウント

Linux クライアントでのマウント

Linux クライアントをアタッチしている SVM ボリュームには、UNIX または mixed のセキュリティスタイル設定をお勧めします。詳細については、「FSx for ONTAP ボリュームの管理」を参照してください。

> **Note**
>
> デフォルトでは、FSx for ONTAP NFS マウントは `hard` マウントです。フェイルオーバーが発生した場合にスムーズなフェイルオーバーを実現するには、デフォルトの `hard` マウントオプションの使用をお勧めします。

ONTAP ボリュームを Linux クライアントにマウントするには

1. https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. ファイルシステムと同じ VPC にある Amazon Linux 2 を実行する Amazon EC2 インスタンスを作成または選択します。

   EC2 Linux インスタンスの起動の詳細については、Amazon EC2 ユーザーガイド」の「ステップ 1: インスタンスを起動する」を参照してください。
3. Amazon EC2 Linux インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2
4. Secure Shell (SSH) を使用して EC2 インスタンスでターミナルを開き、適切な認証情報でログインします。
5. 次のように、SVM ボリュームをマウントするための EC2 インスタンス上にディレクトリを作成します。

   ```
   sudo mkdir /fsx
   ```
6. 次のコマンドを使用して、作成したディレクトリにボリュームをマウントします。

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   次の例は、サンプル値を使用しています。

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   また、DNS 名の代わりに SVM の IP アドレス SVM を使用できます。DNS 名を使用してクライアントをスケールアウトファイルシステムにマウントして、クライアントがファイルシステムの高可用性 (HA) ペアにバランスよく配置されるようにすることをお勧めします。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> スケールアウトファイルシステムでは、パラレル NFS (pNFS) プロトコルがデフォルトで有効になっており、NFS v4.1 以降でボリュームをマウントするすべてのクライアントにデフォルトで使用されます。

/etc/fstab を使用したインスタンスリブートへの自動マウント

Amazon EC2 Linux インスタンスの再起動時に FSx for ONTAP ボリュームを自動的に再マウントするには、/etc/fstab ファイルを使用します。/etc/fstab ファイルには、ファイルシステムに関する情報が含まれています。インスタンスの起動中に実行される mount -a コマンドは、/etc/fstab に示されているファイルシステムをマウントします。

> **Note**
>
> FSx for ONTAP ファイルシステムは、Amazon EC2 Mac インスタンスの /etc/fstab を使用した自動マウントをサポートしていません。

> **Note**
>
> EC2 インスタンスの /etc/fstab ファイルを更新する前に、FSx for ONTAP ファイルシステムがすでに作成済みであることを確認してください。詳細については、「FSx for ONTAP ファイルシステムの作成」を参照してください。

EC2 インスタンスで / etc / fstab ファイルを更新するには

1. EC2 インスタンスに接続します。

   - macOS または Linux が稼働しているコンピュータからインスタンスに接続するには、SSH コマンドで .pem ファイルを指定します。これを行うには、-i オプションとプライベートキーへのパスを使用します。

- Windows を実行しているコンピュータからインスタンスに接続するには、 MindTerm または PuTTY を使用できます。PuTTY を使用するには、PuTTY をインストールし、.pem ファイルを .ppk ファイルに変換します。

詳細については、Amazon EC2 ユーザーガイド」の以下のトピックを参照してください。

- [Connecting to your Linux instance using SSH] (SSH を使用した Linux インスタンスへの接続)
- [Connecting to your Linux instance from Windows using PuTTY] (PuTTY を使用した Windows から Linux インスタンスへの接続)

2. SVM ボリュームのマウントに使用するローカルディレクトリを作成します。

```
sudo mkdir /fsx
```

3. 適切なエディタで、/etc/fstab ファイルを開きます。
4. 次の行を /etc/fstab ファイルに追加します。各パラメータの間にタブ文字を挿入します。改行のない行として表示されるはずです。

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

ボリュームの SVM の IP アドレスを使用することもできます。最後の 3 つのパラメータは、NFS オプション (デフォルトに設定)、ファイルシステムおよびファイルシステムチェックのダンプ (通常は使用されないため、0 に設定) を示します。

5. 変更をファイルに保存します。
6. 次のコマンドを使用して、ファイルシェアをマウントします。次回システムがスタートすると、フォルダは自動的にマウントされます。

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

EC2 インスタンスは、再起動するたびに ONTAP ボリュームをマウントするように設定されました。

Microsoft Windows クライアントでのマウント

このセクションでは、Microsoft Windows オペレーティングシステムを実行しているクライアントを使用して FSx for ONTAP ファイルシステムのデータにアクセスする方法について説明します。使用しているクライアントのタイプに関係なく、次の要件を確認してください。

この手順では、クライアントとファイルシステムが同じ VPC と AWS アカウントにあると想定しています。クライアントがオンプレミスまたは別の VPC、、 AWS アカウントまたは にある場合 AWS リージョン、この手順では、 または を使用する専用ネットワーク接続、 AWS Transit Gateway または を使用するプライベート AWS Direct Connect で安全なトンネルをセットアップしていることも前提としています AWS Virtual Private Network。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

SMB プロトコルを使用して Windows クライアントにボリュームをアタッチすることをお勧めします。

前提条件

Microsoft Windows クライアントを使用して ONTAP ストレージボリュームにアクセスするには、次の前提条件を満たす必要があります。

- 添付するボリュームの SVM が組織の Active Directory に参加しているか、ユーザーがワークグループを使用している必要があります。アクティブディレクトリへの SVM への参加方法の詳細については、「FSx for ONTAP ストレージ仮想マシンの管理」を参照してください。ワークグループの使用の詳細については、「 NetApp ドキュメントセンター」の「ワークグループの概要で SMB サーバーを設定する」を参照してください。
- 添付するボリュームは、NTFS または `mixed` のセキュリティスタイルの設定です。詳細については、「FSx for ONTAP ボリュームの管理」を参照してください。

SMB と Active Directory を使用して Windows クライアントに ONTAP ボリュームをアタッチするには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ファイルシステムと同じ VPC にあり、ボリュームの SVM と同じ Microsoft アクティブディレクトリに参加している Microsoft Windows を実行している Amazon EC2 インスタンスを作成または選択します。

   インスタンスの起動の詳細については、Amazon EC2 ユーザーガイド」の「ステップ 1: インスタンスを起動する」を参照してください。

アクティブディレクトリへの SVM への参加方法の詳細については、「FSx for ONTAP ストレージ仮想マシンの管理」を参照してください。

3. Amazon EC2 Windows インスタンスに接続します。詳細については、Amazon EC2 ユーザーガイド」の「Windows インスタンスへの接続」を参照してください。
4. コマンドプロントを開きます。
5. 以下のコマンドを実行します。以下に置き換えます:

   - `Z:` を使用可能なドライブ文字に置き換えます。
   - `DNS_NAME` をボリュームの SVM 用の SMB エンドポイントの DNS 名または IP アドレスに置き換えます。
   - を SMB 共有の名前`SHARE_NAME`に置き換えます。 `C$`は SVM の名前空間のルートにあるデフォルトの SMB 共有ですが、ストレージがルートボリュームに公開され、セキュリティとサービスの中断を引き起こす可能性があるため、マウントしないでください。の代わりにマウントする SMB 共有名を指定する必要がありますC$。SMB 共有を作成する方法の詳細については、「SMB 共有の管理」を参照してください。

```
net use Z: \\DNS_NAME\SHARE_NAME
```

次の例は、サンプル値を使用しています。

```
net use Z: \\corp.example.com\group_share
```

DNS 名の代わりに SVM の IP アドレスを使用することもできます。DNS 名を使用してクライアントをスケールアウトファイルシステムにマウントして、クライアントがファイルシステムの高可用性 (HA) ペアにバランスよく配置されるようにすることをお勧めします。

```
net use Z: \\198.51.100.5\group_share
```

macOS クライアントでのマウント

このセクションでは、macOS オペレーティングシステムを実行しているクライアントを使用して FSx for ONTAP ファイルシステムのデータにアクセスする方法について説明します。使用しているクライアントのタイプに関係なく、次の要件を確認してください。

この手順では、クライアントとファイルシステムが同じ VPC と AWS アカウントにあると想定しています。クライアントがオンプレミス、別の VPC、 AWS アカウント または にある場合は AWS リージョン、 または を使用する専用ネットワーク接続、 AWS Transit Gateway または を使用するプライベート AWS Direct Connect で安全なトンネルをセットアップします AWS Virtual Private Network。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

SMB プロトコルを使用して Mac クライアントにボリュームをアタッチすることをお勧めします。

SMB を使用して MacOS クライアントに ONTAP ボリュームをマウントするには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ファイルシステムと同じ VPC にある macOS を実行する Amazon EC2 Mac インスタンスを作成または選択します。

   インスタンスの起動の詳細については、Amazon EC2 ユーザーガイド」の「ステップ 1: インスタンスを起動する」を参照してください。
3. Amazon EC2 Mac インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2
4. Secure Shell (SSH) を使用して EC2 インスタンスでターミナルを開き、適切な認証情報でログインします。
5. EC2 インスタンスに、ボリュームをマウントするためのディレクトリを、次のように作成します。

   ```
   sudo mkdir /fsx
   ```
6. 次のコマンドを使用して、ボリュームをマウントします。

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   次の例は、サンプル値を使用しています。

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   DNS 名の代わりに SVM の IP アドレスを使用することもできます。DNS 名を使用してクライアントをスケールアウトファイルシステムにマウントして、クライアントがファイルシステムの高可用性 (HA) ペアにバランスよく配置されるようにすることをお勧めします。

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

C$ は、SVM の名前空間のルートを表示するためにマウントできるデフォルトの SMB 共有です。SVM にサーバーメッセージブロック (SMB) 共有を作成した場合は、C$ の代わりに SMB 共有名を指定します。SMB 共有を作成する方法の詳細については、「SMB 共有の管理」を参照してください。

NFS を使用して MacOS クライアントに ONTAP ボリュームをマウントするには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ファイルシステムと同じ VPC にある Amazon Linux 2 を実行する Amazon EC2 インスタンスを作成または選択します。

   EC2 Linux インスタンスの起動の詳細については、Amazon EC2 ユーザーガイド」の「ステップ 1: インスタンスを起動する」を参照してください。
3. Amazon EC2 Linux インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスに接続する」を参照してください。 Amazon EC2
4. インスタンスの起動時にユーザーデータスクリプトを使用するか、次のコマンドを実行して、FSx for ONTAP ボリュームを Linux EC2 インスタンスにマウントします。

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   次の例は、サンプル値を使用しています。

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   また、DNS 名の代わりに SVM の IP アドレス SVM を使用できます。DNS 名を使用してクライアントをスケールアウトファイルシステムにマウントして、クライアントがファイルシステムの HA ペアにバランスよく配置されるようにすることをお勧めします。

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```
5. 次のコマンドを使用して、作成したディレクトリにボリュームをマウントします。

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

次の例は、サンプル値を使用しています。

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

また、DNS 名の代わりに SVM の IP アドレス SVM を使用できます。DNS 名を使用してクライアントをスケールアウトファイルシステムにマウントして、クライアントがファイルシステムの高可用性 (HA) ペアにバランスよく配置されるようにすることをお勧めします。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

iSCSI LUN のマウント

Amazon FSx for NetApp ONTAP は、iSCSI (Internet Small Computer Systems Interface) プロトコルを介した共有ブロックストレージサポートを提供します。LUN (論理的なユニット番号) をプロビジョニングしてイニシエーターグループ (igroup) にマッピングし、ブロックストレージを Linux および Windows ホストに公開することで、iSCSI ストレージを有効にできます。

> **Note**
>
> iSCSI プロトコルは、FSx for ONTAP スケールアウトファイルシステム (ファイルサーバーの高可用性 (HA) ペアが複数あるファイルシステム) ではサポートされていません。

トピック

- Linux クライアントへの iSCSI LUN のマウント
- Windows クライアントへの iSCSI LUN のマウント

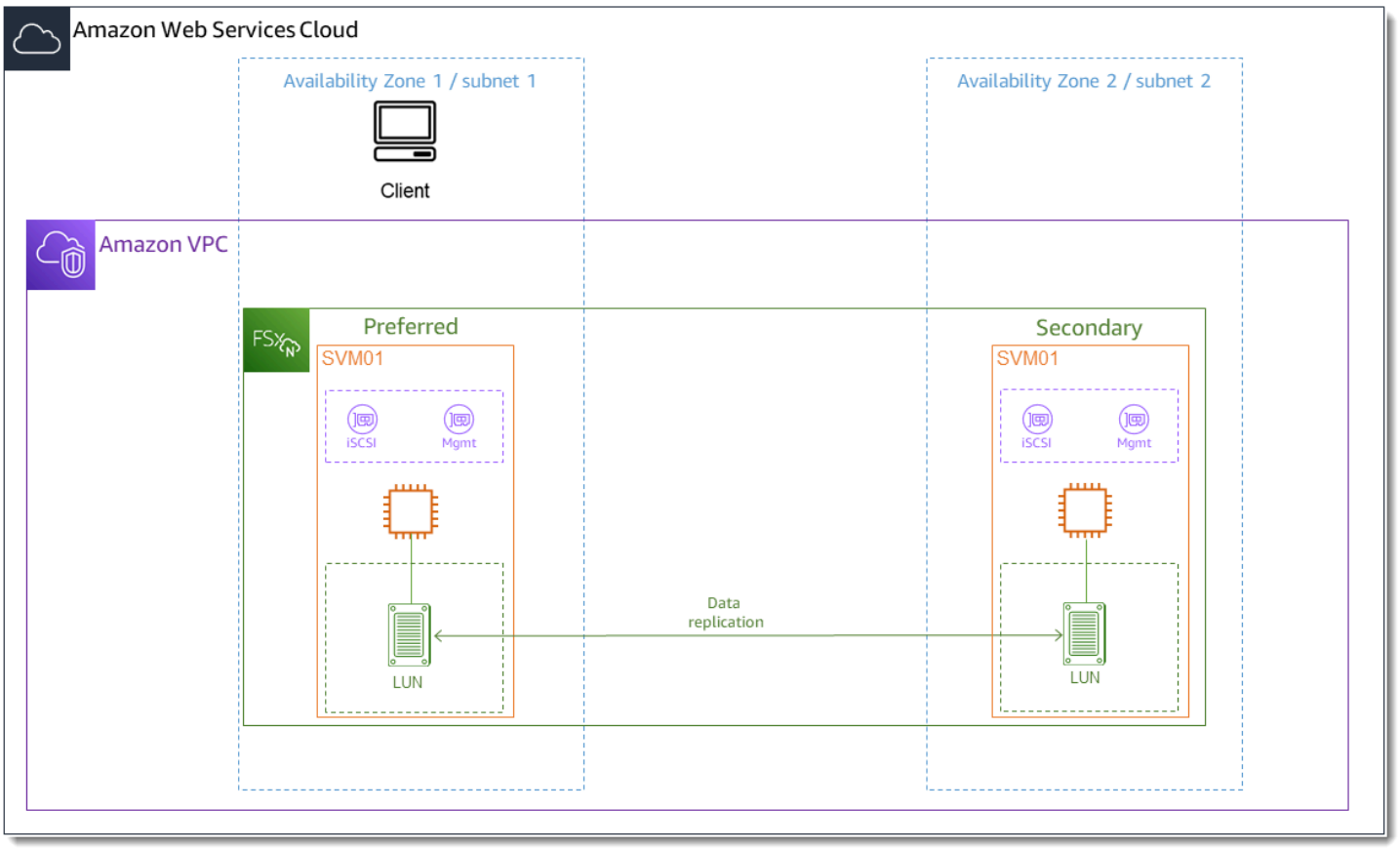
Linux クライアントへの iSCSI LUN のマウント

手順で示されている例では、次の設定を使用しています。

- Linux ホストにマウントされる iSCSI LUN はすでに作成されています。詳細については、「iSCSI LUN の作成」を参照してください。
- iSCSI LUN をマウントしている Linux ホストは、Amazon Linux 2 Amazon マシンイメージ (AMI) を実行している Amazon EC2 インスタンスです。Amazon VPC によるファイルシステムアクセスコントロール で説明されているように、インバウンドトラフィックとアウトバウンドトラフィックを許可するように設定された VPC セキュリティグループがあります。
- Linux ホストと FSx for ONTAP ファイルシステムは、同じ VPC と AWS アカウントにあります。ホストが別の VPC にある場合は、VPC ピアリングまたは を使用して AWS Transit Gateway 、ボリュームの iSCSI エンドポイントへのアクセス権を他の VPCs に付与できます。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

  別の Linux AMI を実行している EC2 インスタンスを使用している場合、ホストにインストールされるユーティリティの一部がプリインストールされている可能性があり、別のコマンドを使用して必要なパッケージをインストールする可能性があります。パッケージのインストールを除いて、このセクションで使用されるコマンドは他の EC2 Linux AMI で有効です。

  次の図に示すように、EC2インスタンスはファイルシステムの優先サブネットと同じアベイラビリティーゾーンにあることをお勧めします。



トピック

- Linux クライアントに iSCSI をインストールして設定する
- FSx for ONTAP ファイルシステムで iSCSI を設定する
- Linux クライアントにiSCSI LUN をマウントします

Linux クライアントに iSCSI をインストールして設定する

iSCSI クライアントをインストールするには

1. Linux デバイスに `iscsi-initiator-utils` と `device-mapper-multipath` がインストールされていることを確認します。SSH クライアントを使用して Linux インスタンスに接続します。詳細については、「SSH を使用した Linux インスタンスへの接続」を参照してください。
2. 次のコマンドを使用して、`multipath` と iSCSI クライアントをインストールします。ファイルサーバー間で自動的にフェイルオーバーしたい場合は、`multipath` をインストールする必要があります。

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. multipath の使用時にファイルサーバー間で自動的にフェイルオーバーする際のレスポンスを高速化するには、デフォルト値の 120 を使用する代わりに、/etc/iscsi/iscsid.conf ファイルの置換タイムアウト値を 5 の値に設定します。

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. iSCSI サービスをスタートします。

```
~$ sudo service iscsid start
```

お使いの Linux のバージョンによっては、代わりにこのコマンドを使用しなければならない場合があります。

```
~$ sudo systemctl start iscsid
```

5. 次のコマンドを使用して、サービスが実行されていることを確認します。

```
~$ sudo systemctl status iscsid.service
```

システムは次の出力でレスポンスします。

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Linux クライアントで iSCSI を設定するには

1. クライアントがファイルサーバー間で自動的にフェイルオーバーできるようにするには、マルチパスを設定する必要があります。以下のコマンドを使用します。

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. 次のコマンドを使用して、Linux ホストのイニシエーター名を確認します。イニシエーター名の場所は、iSCSI ユーティリティによって異なります。`iscsi-initiator-utils` を使用している場合、イニシエーター名はファイル `/etc/iscsi/initiatorname.iscsi` にあります。

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

システムはイニシエーター名でレスポンスします。

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

FSx for ONTAP ファイルシステムで iSCSI を設定する

1. 次のコマンドを使用して、iSCSI NetApp LUN を作成した FSx for ONTAP ファイルシステムの ONTAP CLI に接続します。詳細については、「NetApp ONTAP CLI の使用」を参照してください。

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. NetApp ONTAP CLI lun igroup create コマンドを使用してイニシエータグループ (`igroup`) を作成します。イニシエーターグループは iSCSI LUN にマッピングし、どのイニシエーター (クライアント) が LUN にアクセスできるかをコントロールします。`host_initiator_name` を、前の手順で取得した Linux ホストのイニシエーター名に置き換えます。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

この igroup にマップされた LUN を複数のホストで使用できるようにする場合は、コンマで区切って複数のイニシエーター名を指定できます。詳細については、NetApp ONTAP ドキュメントセンターの「lun igroup create」を参照してください。

3. 次の lun igroup show コマンドを使用して、`igroup` が存在することを確認します。

```
::> lun igroup show
```

システムは次の出力でレスポンスします。

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. このステップは、iSCSI LUN がすでに作成されていることを前提としています。まだ行っていない場合は、「」で step-by-step その手順iSCSI LUN の作成を確認してください。

   次の属性を指定して、作成した LUN から作成した igroup へのマッピングを lun mapping create を使用して作成します。

   - *svm_name* - iSCSI ターゲットを提供するストレージ仮想マシンの名前。ホストはこの値を使用して LUN に到達します。
   - *vol_name* - LUN をホストしているボリュームの名前。
   - *lun_name* - LUN に割り当てた名前。
   - *igroup_name* - イニシエーターグループの名前。
   - *lun_id* - LUN ID 整数は、LUN 自体ではなく、マッピングに固有です。これは、論理的なユニット番号がストレージにアクセスするときにイニシエーターにこの値を使用するため、igroup のイニシエーターによって使用されます。

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. lun show -path コマンドを使用して、LUN が作成され、オンラインになり、マッピングされていることを確認します。

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

システムは次の出力でレスポンスします。

```
 Vserver    Path                            serial-hex              state    mapped
 --------- ------------------------------- ----------------------- --------
 --------
```

```
svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

serial_hex 値 (この例では 6c5742314e5d52766e796150) を保存します。これは後のステップ、ブロックデバイスのわかりやすい名前を作成する際に使用します。

6. network interface show -vserver コマンドを使用して、iSCSI LUNを作成した SVM の iscsi_1 および iscsi_2 インターフェイスのアドレスを取得します。

```
::> network interface show -vserver svm_name
```

システムは次の出力でレスポンスします。

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

この例では、iscsi_1 の IP アドレスは 172.31.0.143 で、iscsi_2 は 172.31.21.81 です。

Linux クライアントにiSCSI LUN をマウントします

1. Linux クライアントで、次のコマンドを使用して、iscsi_1 の IP アドレス *iscsi_1_IP* を使用してターゲット iSCSI ノードを検出します。

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

この例で
は、iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3 は優先アベイラビリティーゾーンの iSCSI LUN の target_initiator に対応します。

2. (オプション) target_initiator との追加セッションを確立できます。Amazon EC2 のシングルフロートラフィックの帯域幅制限は 5 Gb/秒 (〜625 MB / 秒) ですが、複数のセッションを作成して、単一のクライアントからファイルシステムに高レベルのスループットをもたらすことができます。詳細については、「Linux インスタンスの Amazon Elastic Compute Cloud ユーザーガイドの「 Amazon EC2 インスタンスネットワーク帯域幅」を参照してください。

   次のコマンドは、各アベイラビリティーゾーンの ONTAP ノードごとに、イニシエーターごとに 8 つのセッションを確立し、クライアントが最大 40 Gb/秒 (5,000 MB / 秒) の集約スループットを iSCSI LUN に駆動できるようにします。

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. ターゲットイニシエーターにログインします。iSCSI LUN は、使用可能なディスクとして表示されます。

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

上記の出力は切り捨てられます。各ファイルサーバーのセッションごとに 1 つの Logging in と 1 つの Login successful レスポンスが表示されます。ノードごとに 4 つのセッションの場合、8 つの Logging in および 8 つの Login successful レスポンスがあります。

4. 次のコマンドを使用して、dm-multipath が複数のポリシーを持つ単一の LUN を表示することにより、iSCSI セッションを識別してマージしたことを確認します。active としてリストされているデバイスと enabled としてリストされているデバイスの数は同じである必要があります。

```
~$ sudo multipath -ll
```

出力では、ディスク名は dm-xyz としてフォーマットされます。ここで、xyz は整数です。他にマルチパスディスクがない場合、この値は dm-0 です。

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

これで、ブロックデバイスが Linux クライアントに接続されました。パス /dev/*dm-xyz* の下にあります。このパスを管理目的で使用しないでください。代わりに、パス /dev/mapper/*wwid* の下にあるシンボリックリンクを使用します。*wwid* は、デバイス間で一貫している LUN の一意の識別子です。次のステップでは、*wwid* にわかりやすい名前を付けて、他のマルチパスディスクと区別できるようにします。

ブロックデバイスにフレンドリ名を付けるには

1. デバイスにわかりやすい名前を付けるには、/etc/multipath.conf ファイルにエイリアスを作成します。これを行うには、好みのテキストエディタを使用してファイルに次のエントリを追加し、次のプレースホルダーを置き換えます。

   - serial_hex を FSx for ONTAP ファイルシステムで iSCSI を設定する の手順で保存した値に置き換えます。

- 例に示すように、プレフィックス 3600a0980 を serial_hex 値に追加します。これは、Amazon FSx for NetApp ONTAP が使用する NetApp ONTAP ディストリビューションの一意のプリアンブルです。
- device_name をデバイスに使用するわかりやすい名に置き換えます。

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

別の方法として、次のスクリプティングを multipath_alias.sh などの bash ファイルとしてコピーして保存することもできます。スクリプティングは sudo 許可で実行でき、*serial_hex* (3600a0980 プレフィックスなし) と *device_name* をそれぞれのシリアル番号と目的のフレンドリ名に置き換えます。このスクリプティングは、/etc/multipath.conf ファイル内のコメントされていない multipaths セクションを検索します。もしそれが存在する場合は、そのセクションに multipath エントリを追加します。それ以外の場合は、ブロックデバイスの multipath エントリを含む新しい multipaths セクションが作成されます。

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. /etc/multipathd.conf への変更を有効にするには、multipathd サービスを再起動します。

```
~$ systemctl restart multipathd.service
```

LUN をパーティション分割するには

次のステップでは、fdisk を使用して LUN をフォーマットおよびパーティション分割すします。

1. 次のコマンドを使用して、device_name へのパスが存在することを確認します。

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. fdisk を使用してディスクをパーティション分割します。インタラクティブなプロンプトを入力します。表示されている順序でオプションを入力します。Last sector 値は、iSCSI LUN のサイズ (この例では 10GB) によって異なることに注意してください。最後のセクター (この例では 20971519) よりも小さい値を使用して、複数のパーティションを作成できます。

```
~$ sudo fdisk /dev/mapper/device_name
```

fsdisk インタラクティブプロンプトが起動します。

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519
```

```
Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

w を入力すると、新しいパーティション /dev/mapper/*partition_name* が使用可能になります。*partition_name* の形式は *<device_name><partition_number>*です。前のステップの fdisk コマンドで使用されたパーティション番号として、1 が使用されました。

3. パスとして /dev/mapper/*partition_name* を使用してファイルシステムを作成します。

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

システムは次の出力でレスポンスします。

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Linux クライアントに LUN をマウントするには

1. ファイルシステムのマウントポイントとしてディレクトリ *directory_path* を作成します。

```
~$ sudo mkdir /directory_path/mount_point
```

2. 次のコマンドを使用してファイルシステムをマウントします。

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (オプション) マウントディレクトリの所有権をユーザーに変更できます。*username* を自分のユーザーネームに置き換えます。

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (オプション) ファイルシステムとの間でデータの読み取りと書き込みができることを確認します。

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

これで、Linux クライアントに iSCSI LUN が正常に作成されてマウントされました。

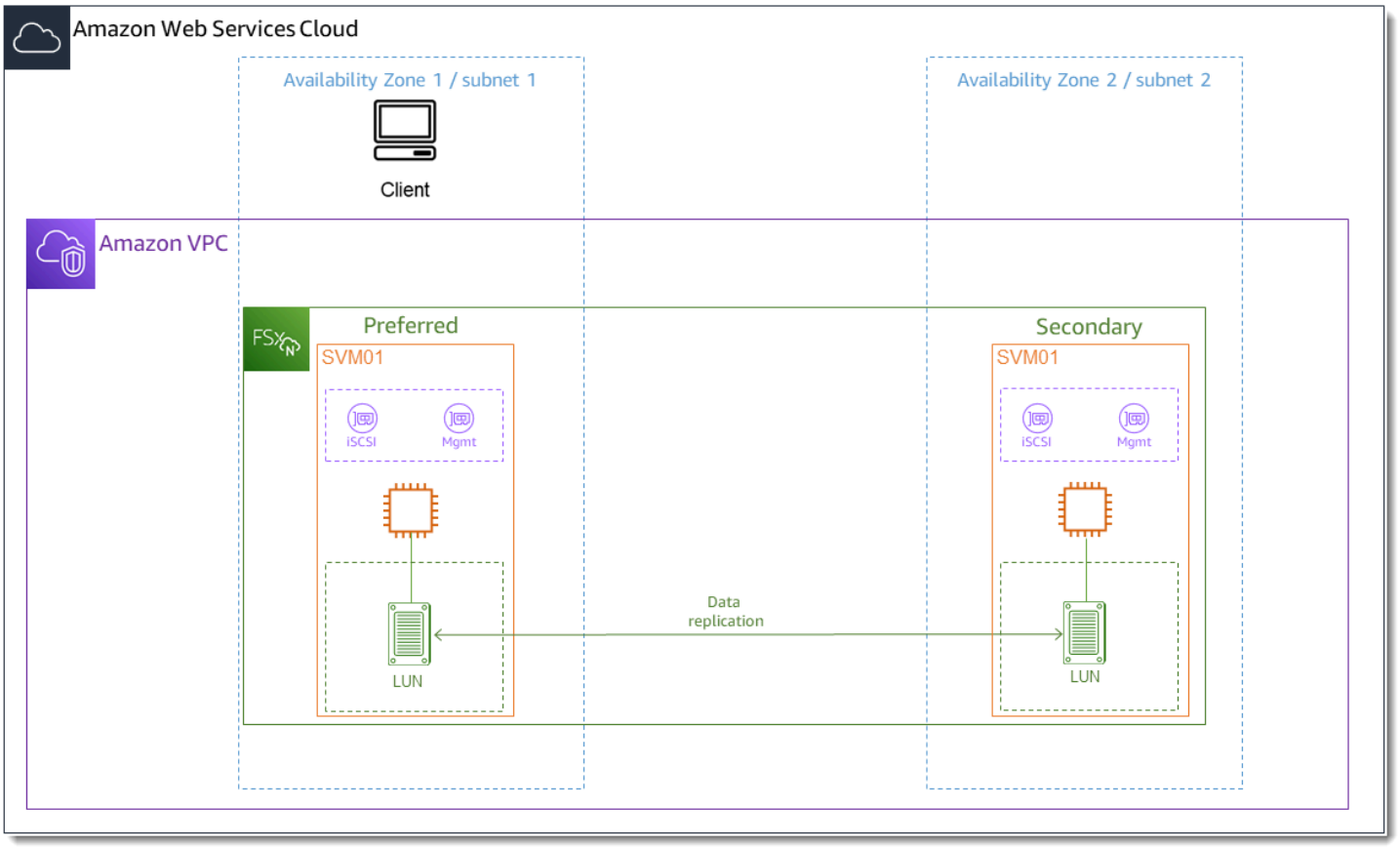
Windows クライアントへの iSCSI LUN のマウント

手順で示されている例では、次の設定を使用しています。

- Windows ホストにマウントされる iSCSI LUN はすでに作成されています。詳細については、「iSCSI LUN の作成」を参照してください。
- iSCSI LUN をマウントしている Microsoft Windows ホストは、Microsoft Windows Server 2019 Amazon マシンイメージ (AMI) を実行している Amazon EC2 インスタンスです。Amazon VPC によるファイルシステムアクセスコントロール で説明されているように、インバウンドトラフィックとアウトバウンドトラフィックを許可するように設定された VPC セキュリティグループがあります。

  セットアップで別の Microsoft Windows AMI を使用している可能性があります。
- クライアントとファイルシステムは同じ VPC と AWS アカウントにあります。クライアントが別の VPC にある場合は、VPC ピアリングまたは AWS Transit Gateway を使用して、他の VPCs に iSCSI エンドポイントへのアクセスを許可できます。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

次の図に示すように、EC2インスタンスはファイルシステムの優先サブネットと同じアベイラビリティーゾーンにあることをお勧めします。



トピック

- Windows クライアントで iSCSI を設定する
- FSx for ONTAP ファイルシステムで iSCSI を設定する
- Windows クライアントに iSCSI LUN をマウントします
- iSCSI 設定の検証

Windows クライアントで iSCSI を設定する

1. Windows リモートデスクトップを使用して、iSCSI LUN をマウントする Windows クライアントに接続します。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「RDP を使用して Windows インスタンスに接続する」を参照してください。

2. 管理者 PowerShell として Windows を開きます。次のコマンドを使用して、Windows インスタンスで iSCSI を有効にし、iSCSI サービスが自動的にスタートするように設定します。

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Windows インスタンスのイニシエーター名を取得します。この値は、ONTAP CLI を使用して FSx for ONTAP ファイルシステムで iSCSI NetApp を設定するときに使用します。

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

システムはイニシエーターポートでレスポンスします。

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. クライアントがファイルサーバー間で自動的にフェイルオーバーできるようにするには、Windows インスタンスに `Multipath-IO` (MPIO) をインストールする必要があります。以下のコマンドを使用します。

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. `Multipath-IO` のインストールが完了したら、Windows インスタンスを再起動します。次のセクションで iSCSI LUN をマウントする手順を実行するには、Windows インスタンスを開いたままにします。

FSx for ONTAP ファイルシステムで iSCSI を設定する

1. 次のコマンドを使用して、iSCSI NetApp LUN を作成した FSx for ONTAP ファイルシステムの ONTAP CLI に接続します。詳細については、「NetApp ONTAP CLI の使用」を参照してください。

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. NetApp ONTAP CLI を使用してlun igroup create、イニシエータグループ または を作成しますigroup。イニシエータグループは iSCSI LUN にマップし、どのイニシエーター (クライアント) が LUN にアクセスできるかをコントロールします。`host_initiator_name` を、前の手順で取得した Windows ホストのイニシエーター名に置き換えます。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

この igroup にマッピングされた LUN を複数のホストで使用できるようにする場合は、複数のコンマ区切りのイニシエーター名を指定できます。詳細については、ONTAP ドキュメントセンターlun igroup createの「」を参照してください。 NetApp

3. 次のコマンドを使用して、igroup が正常に作成されたことを確認します。

```
::> lun igroup show
```

システムは次の出力でレスポンスします。

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

igroup を作成したら、LUN を作成して igroup にマッピングする準備が整います。

4. このステップは、iSCSI LUN がすでに作成されていることを前提としています。まだ行っていない場合は、「」で step-by-step その手順iSCSI LUN の作成を確認してください。

LUN から新しい igroup への LUN マッピングを作成します。

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. 次のコマンドを使用して、LUN が作成され、オンラインになり、マッピングされていることを確認します。

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

これで、Windows インスタンスに iSCSI ターゲットを追加する準備が整いました。

6. 次のコマンドを使用して、SVM の iscsi_1 および iscsi_2 インターフェイスの IP アドレスを取得します。

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

この例では、iscsi_1 の IP アドレスは 172.31.0.143 で、iscsi_2 は 172.31.21.81 です。

Windows クライアントに iSCSI LUN をマウントします

1. Windows インスタンスで、管理者として PowerShell ターミナルを開きます。
2. 次のことを行う .ps1 スクリプティングを作成します。

   - 各ファイルシステムの iSCSI インターフェイスに接続します。
   - iSCSI 用の MPIO を追加および設定します。
   - iSCSI 接続ごとに 8 つのセッションを確立します。これにより、クライアントは最大 40 Gb/秒 (5,000 MB/秒) の集約スループットを iSCSI LUN に駆動できます。セッションが 8 つあるため、ONTAP スループットキャパシティで最高レベルの FSx である、4,000 MB/秒のスループット容量をフルに駆動することができます。また、#Establish iSCSI connection ステップのスクリプトの for-loop を、1..8 から別の上限に変更することで、セッション数を増減することもできます (各セッションのスループットは最大 625 MB/秒)。詳細については、「Windows インスタンスの Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon EC2 インスタンスネットワーク帯域幅」を参照してください。

   次の一連のコマンドをファイルにコピーして、.ps1 スクリプトを作成します。

   - iscsi_1 と iscsi_2 を、前のステップで取得した IP アドレスに置き換えます。

- ec2_ip を Windows インスタンスの IP アドレスに置き換えます。

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

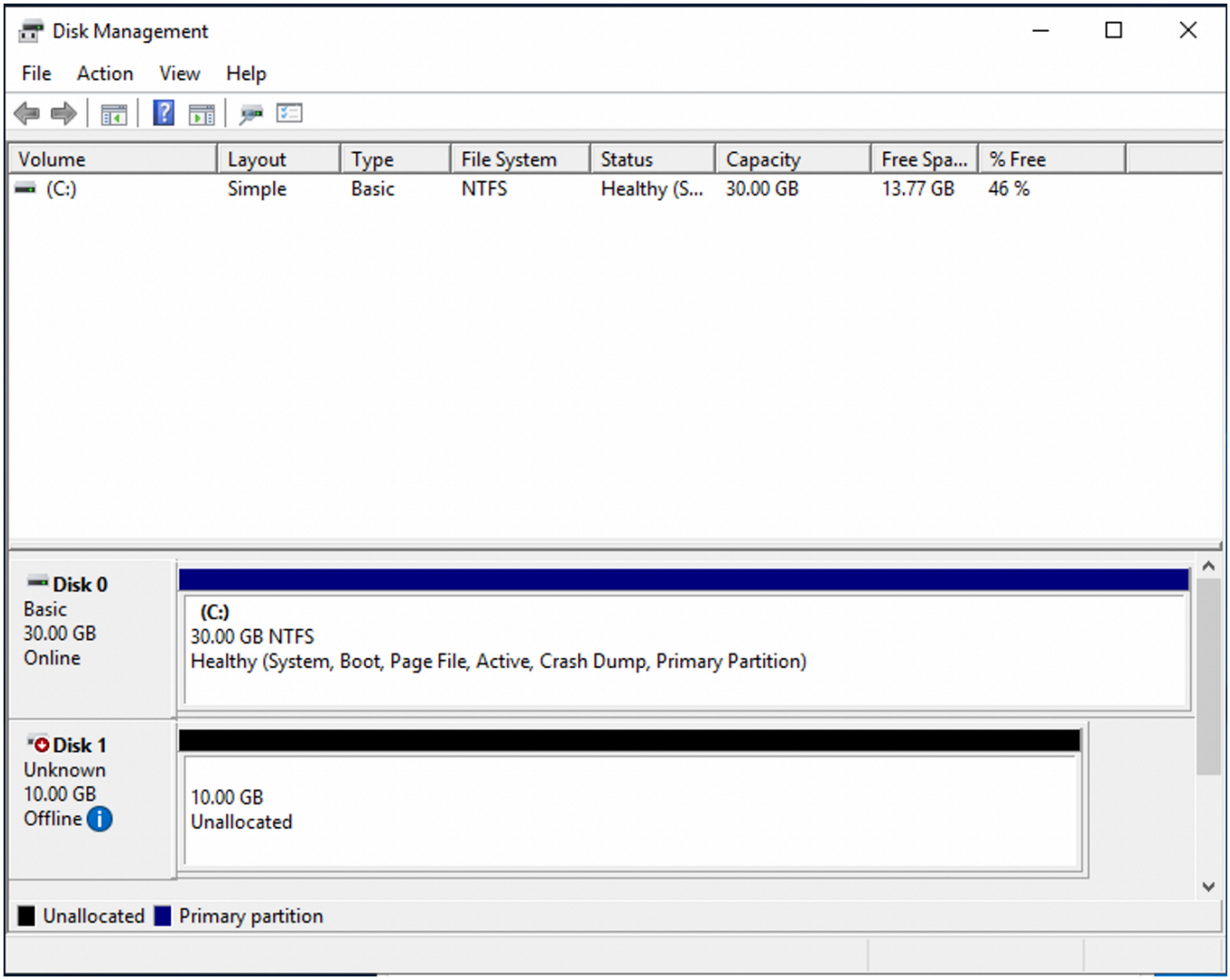
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

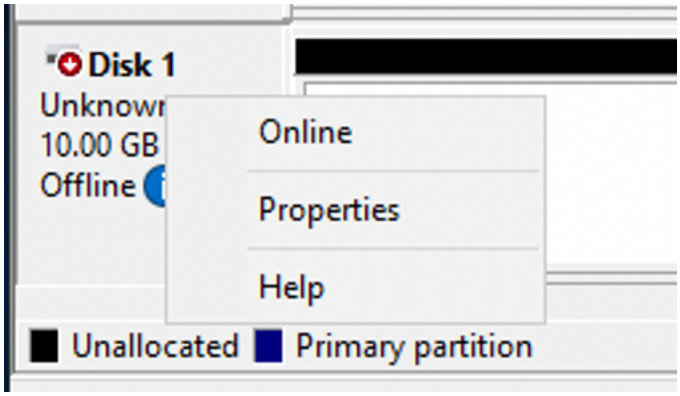
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Windows ディスク管理アプリケーションを起動します。Windows の実行ダイアログボックスを開き、diskmgmt.msc と入力して、[Enter] を押します。ディスク管理アプリケーションが開きます。



4. 未割り当てのディスクを見つけます。これは iSCSI LUN です。この例では、ディスク 1 が iSCSI ディスクです。オフラインです。



ディスク 1 にカーソルを合わせてボリュームをオンラインにし、右クリックして [Online] (オンライン) を選択します。

> **Note**
>
> ストレージエリアネットワーク (SAN) ポリシーを変更して、新しいボリュームが自動的にオンラインになるようにすることができます。詳細については、「Microsoft Windows Server コマンドリファレンス」の「SAN ポリシー」を参照してください。

5. ディスクを初期化するには、カーソルをディスク 1 の上に置いて右クリックし、[Initialize] (初期化) を選択します。初期化ダイアログが表示されます。[OK] を選択してディスクを初期化します。
6. 通常どおりにディスクをフォーマットします。フォーマットが完了すると、iSCSI ドライブは Windows クライアントで使用可能なドライブとして表示されます。

iSCSI 設定の検証

iSCSI 設定が正しく設定されていることを確認するスクリプトを用意しました。このスクリプトは、セッション数、ノード分散、マルチパス I/O (MPIO) ステータスなどのパラメータを調べます。次のタスクでは、 スクリプトをインストールして使用する方法について説明します。

iSCSI 設定を検証するには

1. Windows PowerShell ウィンドウを開きます。
2. 次のコマンドを使用してスクリプトをダウンロードします。

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. 次のコマンドを使用して zip ファイルを展開します。

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. 次のコマンドを使用してスクリプトを実行します。

```
PS C:\> ./CheckiSCSI.ps1
```

5. 出力を確認して、設定の現在の状態を理解します。次の例は、iSCSI 設定が成功したことを示しています。

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

他の AWS サービスで FSx for ONTAP を使用する

Amazon EC2 に加えて、ボリュームで他の AWS サービスを使用してデータにアクセスできます。

トピック

- FSx for ONTAP での Amazon WorkSpaces の使用
- FSx for ONTAP で Amazon Elastic Container Service を使用する
- FSx for ONTAP で VMware Cloud を使用する

FSx for ONTAP での Amazon WorkSpaces の使用

FSx for ONTAP を Amazon WorkSpaces と共に使用して、共有ネットワーク添付ドストレージ (NAS) を提供したり、Amazon WorkSpaces アカウントのローミングプロファイルを保存したりできます。WorkSpace インスタンスで SMB ファイル共有に接続した後、ユーザーはファイル共有でファイルを作成および編集できます。

次の手順は、Amazon FSx と Amazon WorkSpaces を使用して、移動プロファイルとホームフォルダへのアクセスに一貫したエクスペリエンスを提供し、Windows および Linux WorkSpace ユーザーに共有チームフォルダを提供する方法を示しています。Amazon WorkSpaces を初めて使用する場合は、「Amazon WorkSpaces 管理ガイド」の「WorkSpaces Quick Setup を開始する」手順に従って、最初の Amazon WorkSpaces 環境を作成できます。

トピック

- ローミングプロファイルのサポートを提供
- 共通ファイルにアクセスするための共有フォルダを指定する

ローミングプロファイルのサポートを提供

Amazon FSx を使用して、組織内のユーザーにローミングプロファイルのサポートを提供できます。ユーザーは、自分のローミングプロファイルのみにアクセスする許可があります。フォルダは、アクティブディレクトリのグループポリシーを使用して自動的に接続されます。ローミングプロファイルで、Amazon FSx ファイル共有をログオフすると、ユーザーのデータとデスクトップ設定が保存され、ドキュメントと設定を異なる WorkSpace インスタンス間で共有し、Amazon FSx の自動の日次バックアップを使用して自動的にバックアップされます。

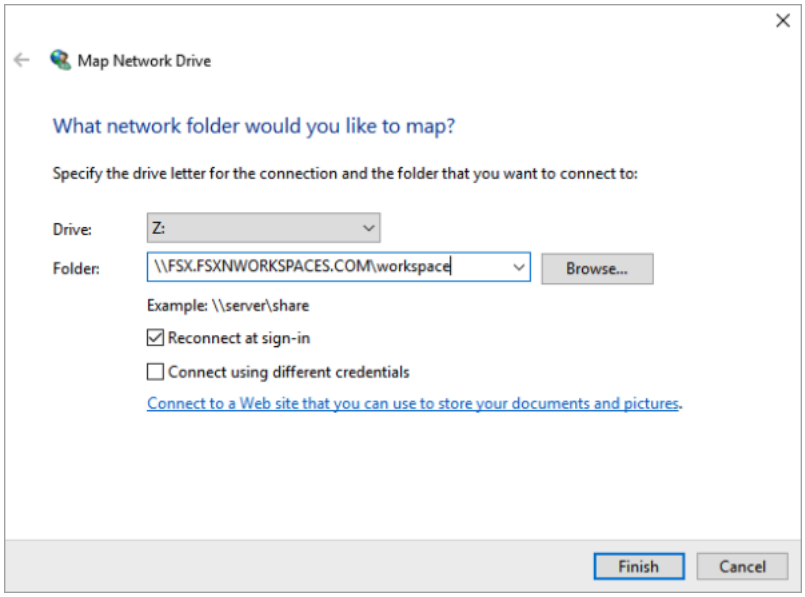
ステップ 1: Amazon FSx を使用してドメインユーザー用のプロファイルフォルダの場所を作成する

1. Amazon FSx コンソールを使用して FSx for ONTAP ファイルシステムを作成します。詳細については、「ファイルシステムの作成方法 (コンソール)」を参照してください。

   > **Important**
   >
   > 各 FSx for ONTAP ファイルシステムには、ファイルシステムに関連付けられたエンドポイントが作成されるエンドポイント IP アドレス範囲があります。マルチ AZ ファイルシステムの場合、FSx for ONTAP は、エンドポイント IP アドレス範囲として、デフォルトの 198.19.0.0/16 からの未使用の IP アドレス範囲を選択します。この IP アドレス範囲は、「Amazon WorkSpaces 管理ガイド」の「WorkSpace の IP アドレスとポートの要件」で説明するように、WorkSpace でも管理トラフィック範囲に使用されます。その結果、WorkSpace からマルチ AZ FSx for ONTAP ファイルシステムにアクセスするには、198.19.0.0/16 と重複しないエンドポイント IP アドレス範囲を選択する必要があります。

2. アクティブディレクトリに参加しているストレージ仮想マシン (SVM) がない場合は、ここで作成します。例えば、`fsx` という名前の SVM をプロビジョニングして、セキュリティスタイルを NTFS に設定することができます。詳細については、「ストレージ仮想マシンを作成するには (コンソール)」を参照してください。
3. SVM のボリュームを作成します。例えば、SVM ルートボリュームのセキュリティスタイルを継承する `fsx-vol` という名前のボリュームを作成できます。詳細については、「FlexVol ボリュームを作成するには (コンソール)」を参照してください。

4. ボリュームに SMB 共有を作成します。例えば、`fsx-vol` という名前のボリュームに `workspace` という名前の共有を作成し、その中に `profiles` という名前のフォルダーを作成できます。詳細については、「SMB 共有の管理」を参照してください。
5. Windows Server を実行する Amazon EC2 インスタンスまたは WorkSpace から Amazon FSx SVM にアクセスします。詳細については、「データへのアクセス」を参照してください。
6. Windows WorkSpace インスタンスで `Z:\` に共有をマッピングします。



ステップ 2: FSx for ONTAP ファイル共有をユーザーアカウントにリンクする

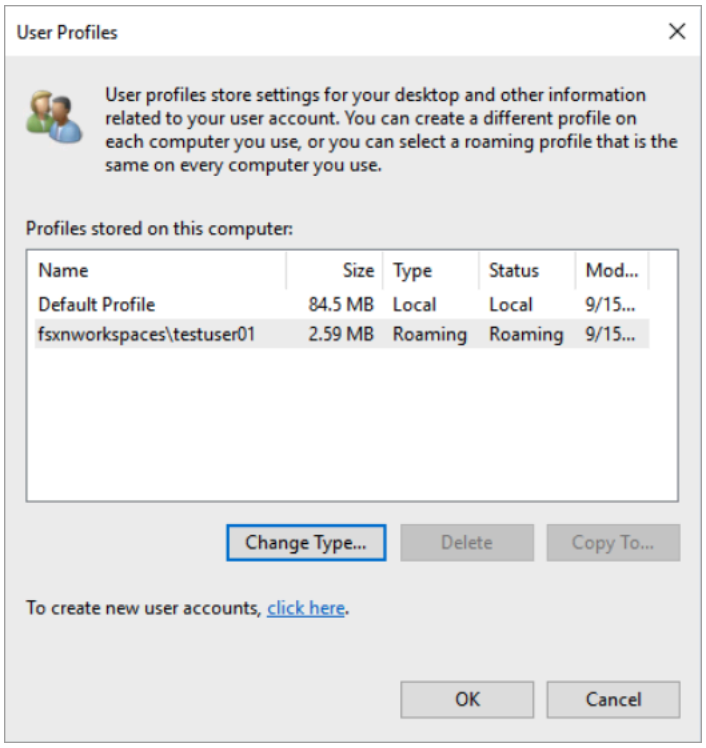
1. テストユーザーの WorkSpace で、Windows > システム > システムの詳細設定 を選択します。
2. [System Properties] (システムプロパティ) で、[Advanced] (詳細設定) タブを選択し、[User Profiles] (ユーザープロファイル) セクションの [Settings] (設定) ボタンを押します。ログインしているユーザーのプロファイルタイプは `Local` になります。
3. WorkSpace からテストユーザーをログアウトします。
4. Amazon FSx ファイルシステム上にローミングプロファイルを配置するようにテストユーザーを設定します。管理者 WorkSpace で、PowerShell コンソールを開き、(ステップ 1 で作成した `profiles` フォルダを使用した) 次の例のようなコマンドを使用します。

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

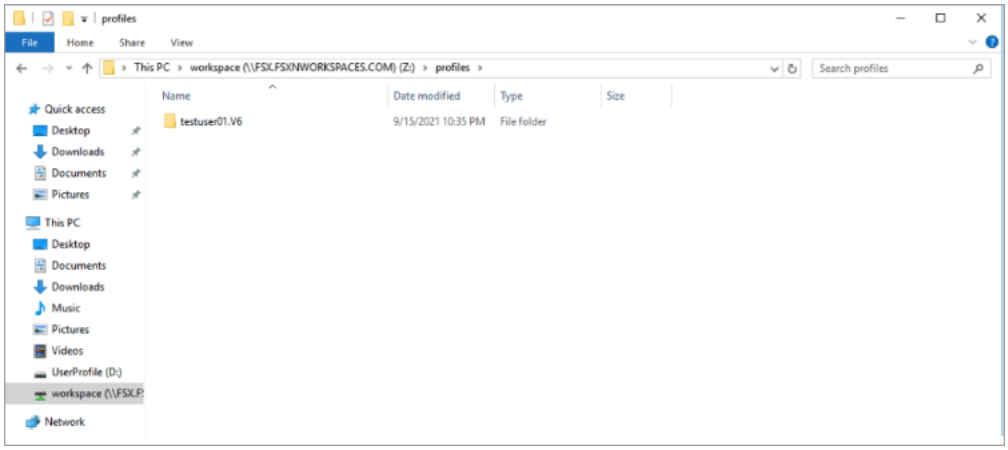
例:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

5. テストユーザー WorkSpace にログオンします。
6. [System Properties] (システムプロパティ) で、[Advanced] (詳細設定) タブを選択し、[User Profiles] (ユーザープロファイル) セクションの [Settings] (設定) ボタンを押します。ログインしているユーザーのプロファイルタイプは `Roaming` になります。

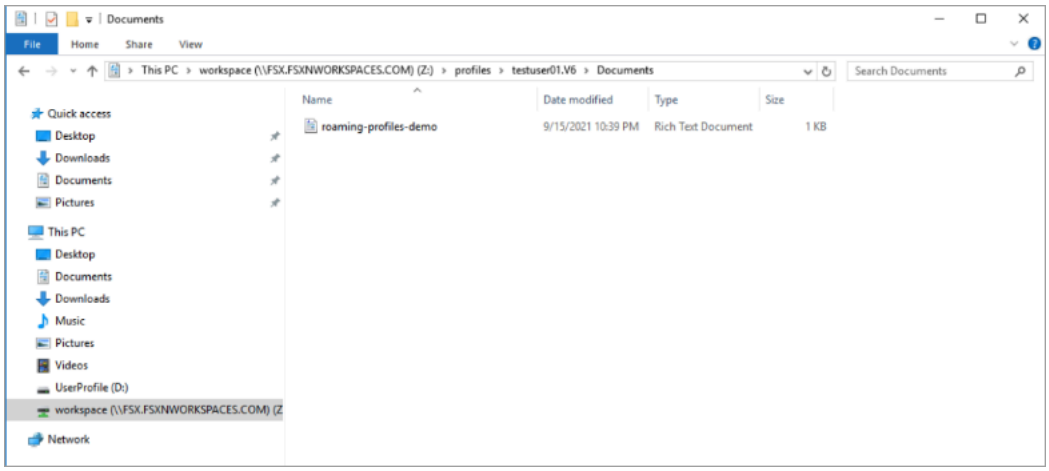


7. FSx for ONTAP 共有フォルダを参照します。`profiles` フォルダにユーザーのフォルダが表示されます。



8. テストユーザーの `Documents` フォルダでドキュメントを作成する

9. WorkSpace からテストユーザーをログアウトします。
10. テストユーザーとして再度ログオンし、プロファイルストアを参照すると、作成したドキュメントが表示されます。

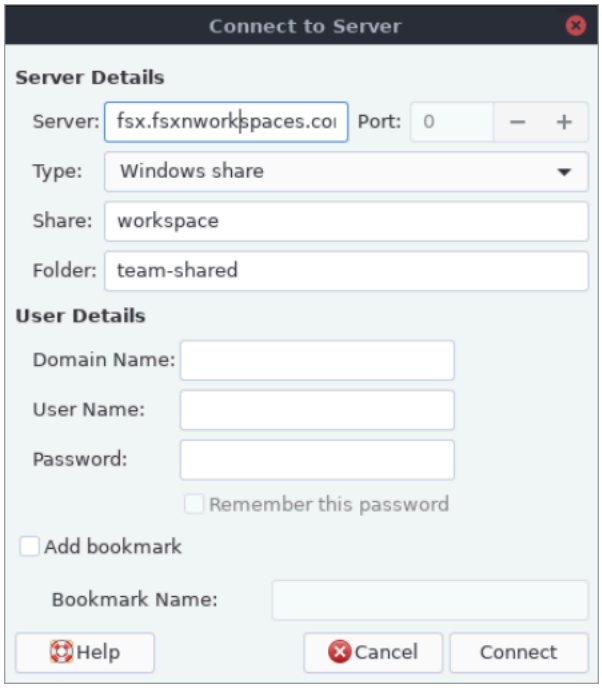


共通ファイルにアクセスするための共有フォルダを指定する

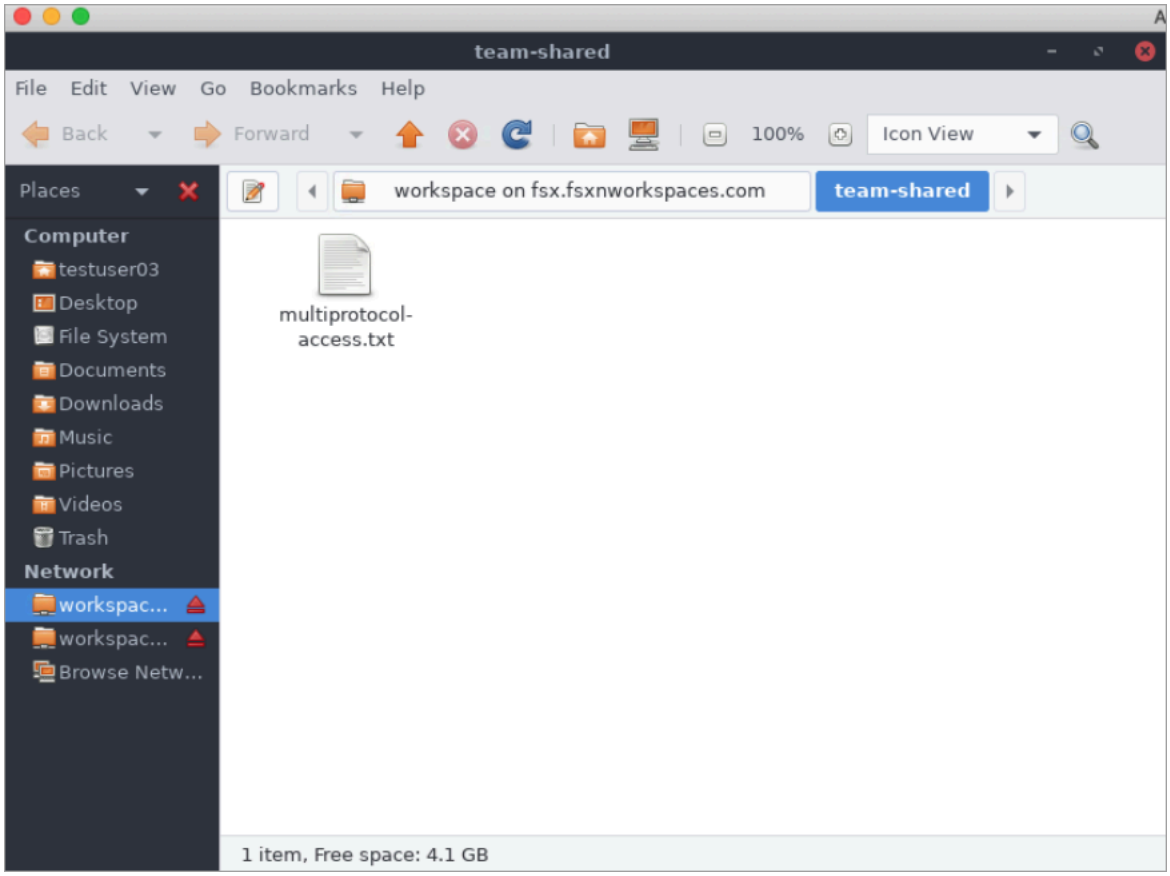
Amazon FSx を使用して、組織内のユーザーに共有フォルダを提供できます。共有フォルダは、デモファイル、コード例、すべてのユーザーが必要とする取扱説明書など、ユーザーコミュニティが使用するファイルを保存するために使用できます。通常、共有フォルダ用にドライブがマッピングされていますが、マッピングされたドライブには文字が使用されるため、使用できる共有数には制限があります。この手順では、ドライブの文字なしで利用可能な Amazon FSx 共有フォルダが作成されるため、チームへの共有の割り当てをより柔軟に行うことができます。

Linux と Windows WorkSpace の両方からクロスプラットフォームアクセスの共有フォルダをマウントするには

1. タスクバーで、場所 > サーバーに接続を選択します。
   a. [Server] (サーバー) に「*`file-system-dns-name`*」と入力します。
   b. タイプを `Windows share` に設定します。
   c. 共有を `workspace` などの SMB 共有の名前に設定します。
   d. フォルダは `/` のままにするか、`team-shared` という名前のフォルダなどのフォルダに設定することができます。
   e. Linux WorkSpace の場合、Linux WorkSpace が Amazon FSx 共有と同じドメインにあれば、ユーザーの詳細を入力する必要はありません。
   f. [Connect] (接続) を選択します。



2. 接続が確立されると、workspace という名前の SMB 共有に共有フォルダが表示されます (この例では team-shared という名前)。



FSx for ONTAP で Amazon Elastic Container Service を使用する

Amazon FSx for NetApp ONTAP ファイルシステムには、Amazon EC2 Linux または Windows インスタンスの Amazon Elastic Container Service (Amazon ECS) Docker コンテナからアクセスできます。

Amazon ECS Linux コンテナでのマウント

1. Linux コンテナ用の EC2 Linux + ネットワーククラスターテンプレートを使用して、ECS クラスターを作成します。詳細については、[Amazon Elastic Container Service Developer Guide] (Amazon Elastic Container Service デベロッパーガイド) の クラスターの作成 を参照してください。
2. 次のように、SVM ボリュームをマウントするための EC2 インスタンス上にディレクトリを作成します。

   ```
   sudo mkdir /fsxontap
   ```

3. インスタンスの起動時にユーザーデータスクリプトを使用するか、次のコマンドを実行して、FSx for ONTAP ボリュームを Linux EC2 インスタンスにマウントします。

   ```
   sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
   ```

4. 次のコマンドを使用して、ボリュームをマウントします。

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
   fsxontap
   ```

   次の例は、サンプル値を使用しています。

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   また、DNS 名の代わりに SVM の IP アドレス SVM を使用できます。

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```

5. Amazon ECS タスク定義を作成する場合、JSON コンテナの定義に以下の volumes と mountPoints コンテナプロパティを追加します。sourcePath を FSx for ONTAP ファイルシステム内のマウントポイントとディレクトリに置き換えます。

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Amazon ECS Windows コンテナへのマウント

1. Windows コンテナ用の EC2 Windows + ネットワーククラスターテンプレートを使用して、ECS クラスターを作成します。詳細については、「Amazon Elastic Container Service デベロッパーガイド」の クラスターの作成 を参照してください。
2. ドメインに参加している Windows EC2 インスタンスを ECS Windows クラスターに追加し、SMB 共有をマッピングします。

   アクティブディレクトリドメインに参加している ECS 最適化された Windows EC2 インスタンスを起動し、次のコマンドを実行して ECS エージェントを初期化します。

```
PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
EnableTaskIAMRole
```

   次のように、スクリプト内の情報をユーザーデータテキストフィールドに渡すこともできます。

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
</powershell>
```

3. SMB 共有をドライブにマッピングできるように、EC2 インスタンスで SMB グローバルマッピングを作成します。FSx ファイルシステムと共有名の netbios または DNS 名の下の値を置き換えます。Linux EC2 インスタンスにマウントされた NFS ボリューム vol1 は、FSx ファイルシステム上の CIFS 共有 fsxontap として設定されます。

```
vserver cifs share show -vserver svm08 -share-name fsxontap


                                    Vserver: svm08
                                      Share: fsxontap
                    CIFS Server NetBIOS Name: FSXONTAPDEMO
                                       Path: /vol1
                             Share Properties: oplocks
                                               browsable
                                               changenotify
                                               show-previous-versions
                           Symlink Properties: symlinks
                    File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                                Share Comment: -
                                    Share ACL: Everyone / Full Control
               File Attribute Cache Lifetime: -
                                  Volume Name: vol1
                                Offline Files: manual
               Vscan File-Operations Profile: standard
          Maximum Tree Connections on Share: 4294967295
                  UNIX Group for File Create: -
```

4. 次のコマンドを使用して、EC2 インスタンスに SMB グローバルマッピングを作成します。

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Amazon ECS タスク定義を作成する場合、JSON コンテナの定義に以下の volumes と mountPoints コンテナプロパティを追加します。sourcePath を FSx for ONTAP ファイルシステム内のマウントポイントとディレクトリに置き換えます。

```
{
```

```
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

FSx for ONTAP で VMware Cloud を使用する

FSx for ONTAP は、VMware Cloud on AWS Software-Defined Data Center (SDDCs) の外部データストアとして使用できます。詳細については、「Configure Amazon FSx for NetApp ONTAP as External Storage」およびVMware Cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide」を参照してください。

可用性と耐久性

Amazon FSx for NetApp ONTAP は、シングル AZ とマルチ AZ の 2 つのデプロイタイプを使用します。これは、さまざまなレベルの可用性と耐久性を提供します。このトピックでは、ワークロードに適したデプロイを選択する際の参照となるよう、各デプロイタイプの可用性と耐久性の機能について説明します。サービスの可用性の SLA (サービスレベルアグリーメント) については、「Amazon FSx Service Level Agreement」(Amazon FSx サービスレベルアグリーメント) を参照してください。

トピック

ファイルシステムのデプロイタイプを選択

シングル AZ およびマルチ AZ のファイルシステムのデプロイタイプの可用性と耐久性の機能については、以降のセクションを参照してください。

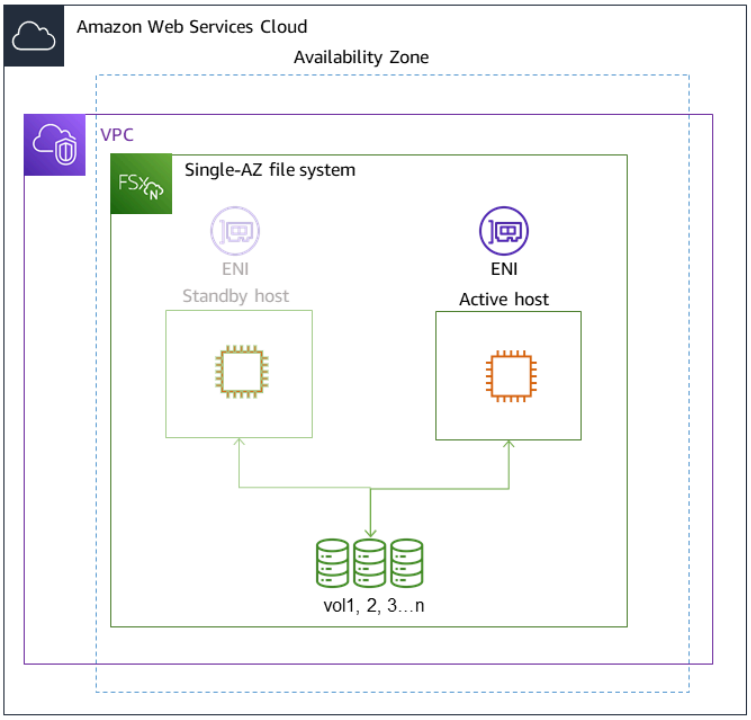
シングル AZ デプロイデプロイタイプ

シングル AZ ファイルシステムを作成すると、Amazon FSx はアクティブ/スタンバイ設定で 1 ~ 12 のファイルサーバーのペアを自動的にプロビジョニングします。各ペアのアクティブファイルサーバーとスタンバイファイルサーバーは、 の 1 つのアベイラビリティーゾーン内の個別の障害ドメインに配置されます AWS リージョン。予定されたファイルシステムのメンテナンス中、またはアクティブファイルサーバーの予定外のサービス中断中に、Amazon FSx は、通常数秒以内に、その高可用性 (HA) ペアをスタンバイファイルサーバーに自動的かつ個別にフェイルオーバーします。フェイルオーバー中も、手動による介入なしで引き続きデータにアクセスできます。

高い可用性を維持するため、Amazon FSx はハードウェア障害を継続的にモニタリングし、障害発生時にはインフラストラクチャのコンポーネントを自動的に置き換えます。高い耐久性を実現するために、Amazon FSx は、アベイラビリティーゾーン内のデータを自動的にレプリケートし、コンポーネントの障害からデータを保護します。さらに、ファイルシステムデータの自動日次バックアップを設定することもできます。これらのバックアップは複数のアベイラビリティーゾーンに保存され、すべてのバックアップデータに対してマルチ AZの回復性を提供します。

シングル AZ ファイルシステムは、マルチ AZ ファイルシステムのデータ回復モデルを必要としないユースケース向けに設計されています。開発環境やテスト環境などのユースケースや、単一のアベイラビリティーゾーン内のデータをレプリケートするだけで AWS リージョン、オンプレミスまたは他の にすでに保存されているデータのセカンダリコピーを保存するための、コスト最適化ソリューションを提供します。

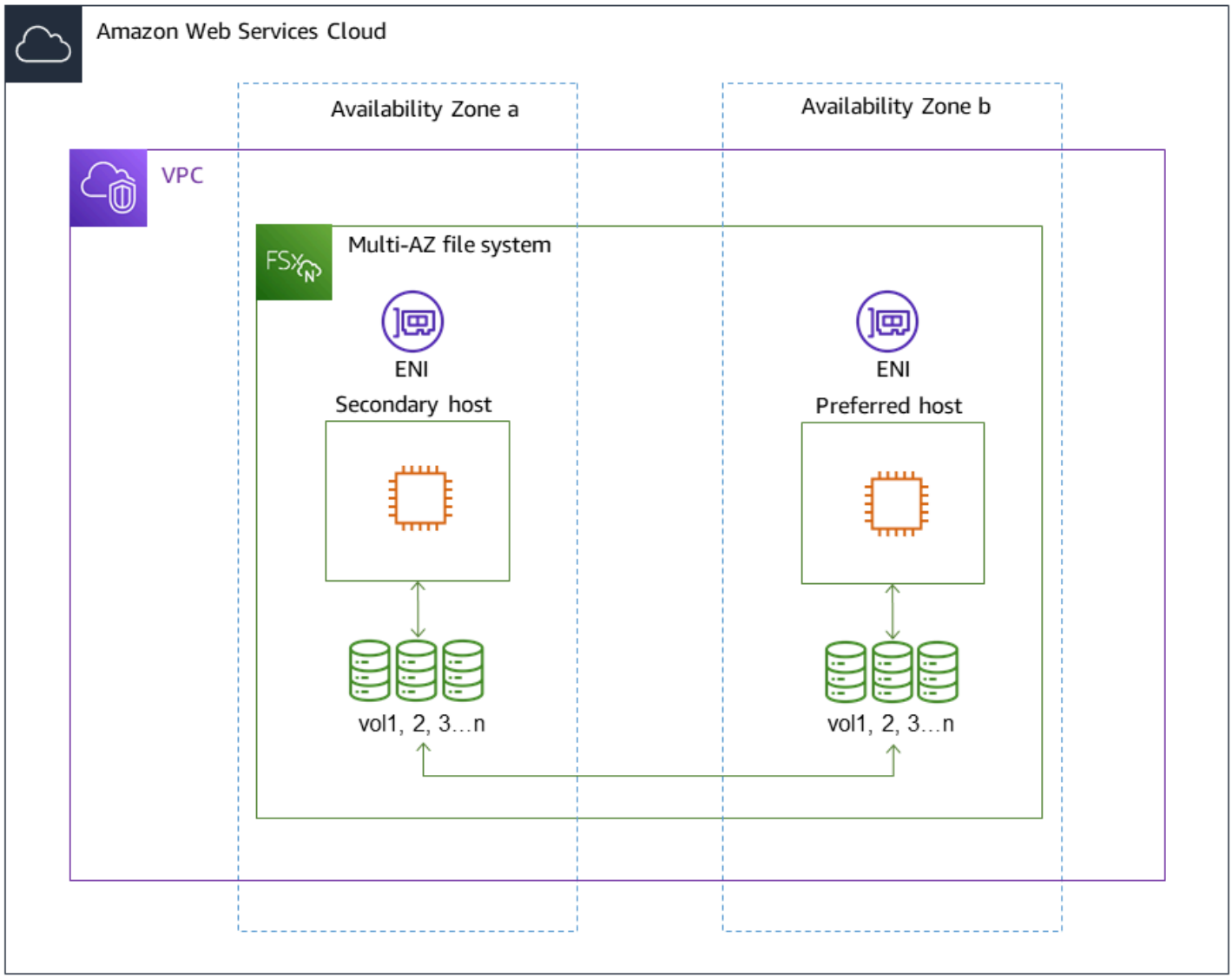
下の図は、FSx for ONTAP のシングル AZ ファイルシステムのアーキテクチャを示します。



マルチ AZ デプロイのタイプ

マルチ AZ ファイルシステムは、シングル AZ ファイルシステムの可用性と耐久性の機能をすべてサポートしています。さらに、アベイラビリティーゾーンが利用できない場合でも、データに継続的な可用性を提供するように設計されています。マルチ AZ 配置では、ファイルサーバーの HA ペアは 1 つで、スタンバイファイルサーバーは同じ AWS リージョン内のアクティブなファイルサーバーとは異なるアベイラビリティーゾーンにデプロイされます。ファイルシステムに書き込まれるすべての変更は、アベイラビリティーゾーン間で同期的にスタンバイにレプリケートされます。

マルチ AZ ファイルシステムは、共有された ONTAP ファイルデータに高い可用性を要求し、アベイラビリティーゾーン間でのレプリケーションが組み込まれたストレージを必要とする、ビジネスクリティカルなプロダクションワークロードなどのユースケース向けに設計されています。下の図は、FSx for ONTAP のマルチ AZ ファイルシステムのアーキテクチャを示します。



FSx for ONTAP のフェイルオーバープロセス

シングル AZ とマルチ AZ のファイルシステムは、以下のいずれかの条件が発生した場合、特定の HA ペアを優先またはアクティブファイルサーバーからスタンバイファイルサーバーに自動的にフェイルオーバーします。

- 優先またはアクティブファイルサーバーは使用できなくなります
- ファイルシステムのスループットキャパシティが変更されました
- 優先またはアクティブファイルサーバーでは、予定されているメンテナンスが実行されます
- アベイラビリティーゾーンが停止します (マルチ AZ ファイルシステムのみ)

> **Note**
>
> スケールアウトファイルシステムでは、各 HA ペアのフェイルオーバー動作は独立しています。ある HA ペアの優先ファイルサーバーが使用できない場合、その HA ペアだけがスタンバイファイルサーバーにフェイルオーバーします。

あるファイルサーバーから別のファイルサーバーにフェイルオーバーすると、新しいアクティブファイルサーバーは、その HA ペアに対するすべてのファイルシステムの読み取りおよび書き込みリクエストを自動的に処理し始めます。マルチ AZ ファイルシステムの場合、優先ファイルサーバーが完全に復旧して利用可能になると、Amazon FSx は自動的にそのサーバーにフェイルバックします。通常、フェイルバックは 60 秒以内に完了します。シングル AZ とマルチ AZ のファイルシステムの場合、アクティブファイルサーバーでの障害検出からスタンバイファイルサーバーのアクティブステータスへの昇格までのフェイルオーバーの処理は、通常 60 秒以内に完了します。クライアントが NFS または SMB 経由でデータにアクセスするために使用するエンドポイント IP アドレスは同じであるため、フェイルオーバーは Linux、Windows、および macOS アプリケーションに対して透過的であり、手動による介入なしにファイルシステムオペレーションが再開されます。

FSx for ONTAP のシングル AZ とマルチ AZ のファイルシステムに接続されたクライアントに対してフェイルオーバーを透過的に行うには、「内からのデータへのアクセス AWS」を参照してください。

ファイルシステムでフェイルオーバーをテストする

スループットキャパシティを変更することにより、スケールアップファイルシステムでフェイルオーバーをテストできます。ファイルシステムのスループットキャパシティを変更すると、Amazon FSx はファイルシステムのファイルサーバーを順次切り替えます。ファイルシステムはセカンダリサーバーに自動的にフェイルオーバーし、Amazon FSx は優先ファイルサーバーを最初に置き換えます。更新されると、ファイルシステムは自動的に新しいプライマリサーバーにフェイルバックし、Amazon FSx がセカンダリファイルサーバーを置き換えます。

Amazon FSx コンソール、CLI、および API で、スループットキャパシティ更新リクエストの進行状況をモニタリングできます。ファイルシステムのスループットキャパシティの変更、およびリクエストの進行状況のモニタリングに関する詳細については、「スループット容量の管理」を参照してください。

ネットワークリソース

このセクションでは、シングル AZ とマルチ AZ のファイルシステムによって消費されるネットワークリソースについて説明します。

サブネット

シングル AZ ファイルシステムを作成する際は、ファイルシステムに対して単一のサブネットを指定します。選択したサブネットは、ファイルシステムが作成されるアベイラビリティーゾーンを定義します。マルチ AZ ファイルシステムを作成する場合、2 つのサブネットを指定します。1 つは優先ファイルサーバー用、もう 1 つはスタンバイファイルサーバー用です。選択する 2 つのサブネットは、同じ AWS リージョン内の異なるアベイラビリティーゾーンに存在している必要があります。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「Amazon VPC とは?」を参照してください。

> **Note**
>
> 指定したサブネットに関係なく、ファイルシステムの VPC 内の任意のサブネットからファイルシステムにアクセスできます。

ファイルシステム Elastic Network Interface

シングル AZ ファイルシステムの場合、Amazon FSx は、ファイルシステムに関連付けられているサブネットに 2 つの Elastic Network Interface (ENI) をプロビジョニングします。マルチ AZ ファイルシステムの場合、Amazon FSx は、ファイルシステムに関連付けられている各サブネットに 1 つずつ、2 つの ENI をプロビジョニングします。クライアントは、ENI を使用して Amazon FSx ファイルシステムと通信します。このネットワークインターフェイスは、アカウントの VPC の一部であるにもかかわらず、Amazon FSx のサービス範囲内であると見なされます。マルチ AZ ファイルシステムは、フローティングインターネットプロトコル (IP) アドレスを使用しています。これにより、接続しているクライアントがフェイルオーバーイベント中に優先ファイルサーバーとスタンバイファイルサーバー間をシームレスに移行できるようにします。

> **Warning**
>
> - ファイルシステムに関連付けられている Elastic Network Interface は、変更または削除しないでください。このネットワークインターフェイスを変更または削除すると、VPC とファイルシステムとの間の接続が完全に失われる可能性があります。

- ファイルシステムに関連付けられた伸縮自在なネットワークインターフェイスには、ルートが自動的に作成され、デフォルトの VPC とサブネットのルートテーブルに追加されます。これらのルートを変更または削除すると、ファイルシステムクライアントの接続が一時的または永続的に失われる可能性があります。

以下の表は、FSx for ONTAP ファイルシステムの各デプロイタイプのサブネット、Elastic Network Interface および IP アドレスリソースの概要を示したものです。

	シングル AZ (スケールアップ)	シングル AZ (スケールアウト)	マルチ AZ (スケールアップ)
サブネット数	1	1	2
Elastic Network Interface 数	2	HA ペアあたり 2	2
ENI あたりの IP アドレス番号	1 + ファイルシステム内のファイルの数	HA ペア数 + HA ペア数にファイルシステム内の SVM の数を掛けた数	1 + ファイルシステム内のファイルの数
VPC のルートテーブルのルート数	該当なし	該当なし	1 + ファイルシステム内のファイルの数

ファイルシステムまたは SVM が作成されると、ファイルシステムが削除されるまでその IP アドレスは変更されません。

Important

Amazon FSx は、パブリックインターネットからのファイルシステムへのアクセス、またはファイルシステムへの公開をサポートしていません。Amazon FSx は、インターネットから到達可能なパブリック IP アドレスである Elastic IP アドレスを自動的にデタッチし、ファイルシステムの Elastic Network Interface に接続します。

ストレージ容量の管理

Amazon FSx for NetApp ONTAP には、ファイルシステムのストレージ容量を管理するために使用できるストレージ関連の機能が多数用意されています。

トピック

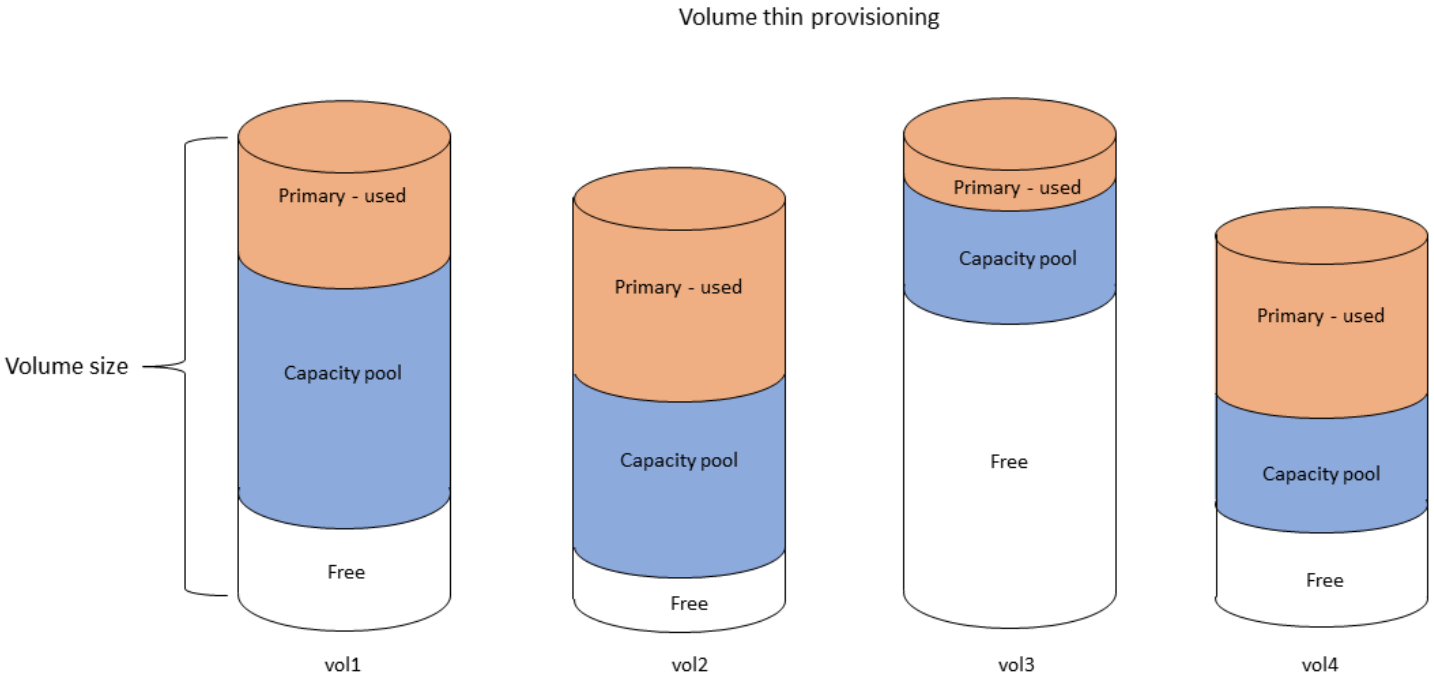
FSx for ONTAP ストレージ階層

ストレージ階層は、Amazon FSx for NetApp ONTAP ファイルシステムの物理ストレージメディアです。FSx for ONTAP は、次のストレージ階層を提供します。

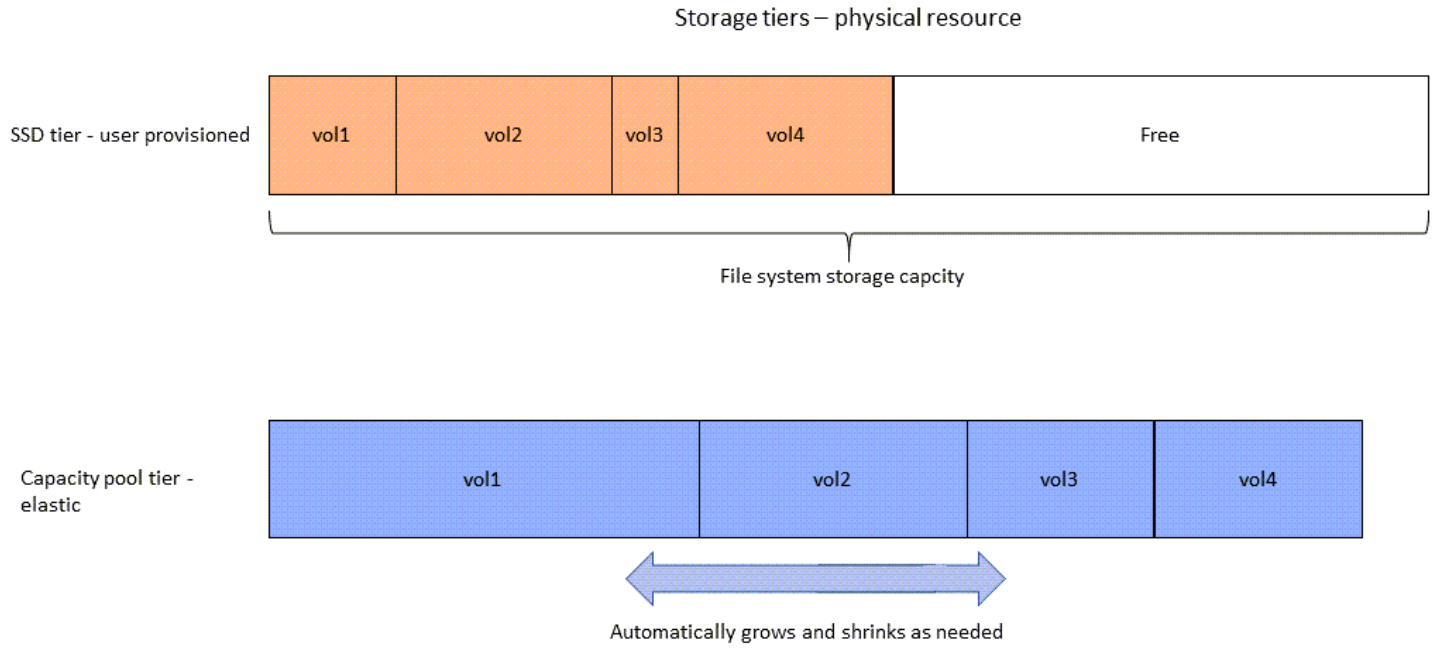
- SSD 階層 — データセットのアクティブな部分専用に設計された、ユーザーがプロビジョニングする高性能ソリッドステートドライブ (SSD) ストレージです。
- 容量プール層 — ペタバイト規模まで自動的に拡張する、伸縮自在なストレージで、アクセス頻度の低いデータに対してコストを最適化します。

FSx for ONTAP ボリュームは、フォルダと同様にストレージ容量を消費しない仮想リソースです。保存するデータ、そして物理的なストレージを消費するデータは、ボリューム内に格納されます。ボリュームの作成時に、サイズを指定します。サイズは、作成後に変更できます。FSx for ONTAP ボリュームはシンプロビジョニングされ、ファイルシステムストレージは事前に予約されません。代わりに、SSD と容量プールのストレージは必要に応じて動的に割り当てられます。ボリュームレベルで構成する階層化ポリシーは、SSD 階層に保存されているデータを容量プール階層に移行するかどうか、いつ移行するかを決定します。

次の図は、ファイルシステム内の複数の FSx for ONTAP ボリュームにまたがって配置されたデータの例を示しています。



次の図は、前の図の 4 つのボリューム内のデータによって、ファイルシステムの物理ストレージ容量が、どのように消費されるかを示しています。



ファイルシステムの各ボリュームの要件に最適な階層化ポリシーを選択することで、ストレージコストを削減できます。詳細については、「ボリュームデータの階層化」を参照してください。

適切な量のファイルシステム SSD ストレージを選択する

FSx for ONTAP ファイルシステムの SSD ストレージ容量を選択する際には、データの保存に使用できる SSD ストレージの容量に影響する次の項目を考慮する必要があります。

- NetApp ONTAP ソフトウェアのオーバーヘッド用に予約されたストレージ容量。
- ファイルメタデータ
- 最近書き込まれたデータ
- SSD ストレージに保存する予定のファイルです (冷却期間に達していないデータや、最近読み込んで SSD に取り出したデータなど)。

SSD ストレージの使用方法

ファイルシステムの SSD ストレージは、 NetApp ONTAP ソフトウェア (オーバーヘッド) 、ファイルメタデータ、およびデータの組み合わせに使用されます。

NetApp ONTAP ソフトウェアのオーバーヘッド

他の NetApp ONTAP ファイルシステムと同様に、ファイルシステムの SSD ストレージ容量の最大 16% は ONTAP オーバーヘッド用に予約されています。つまり、ファイルを保存することはできません。ONTAP オーバーヘッドは次のように割り当てられます。

- 11% は NetApp ONTAP ソフトウェア用に予約されています。30 テビバイト (TiB) を超える SSD ストレージ容量を持つファイルシステムでは、6% が予約されています。
- 5% は、ファイルシステムの両方のファイルサーバ間でデータを同期させるために必要な、集約スナップショット用に確保されています。

ファイルメタデータ

ファイルメタデータは、通常、ファイルが消費するストレージ容量の 3～7% を消費します。この割合は、平均ファイルサイズ (平均ファイルサイズが小さいほど多くのメタデータが必要になります) と、ファイルのストレージ効率化で、どれだけ節約できるかによって異なります。ファイルメタデータはストレージ効率化による節約の恩恵を受けないことに注意してください。ファイルシステム上のメタデータに使用される SSD ストレージの容量を見積もるには、次のガイドラインが使用できます。

平均ファイルサイズ	ファイルデータに対する、メタデータサイズの割合
4 KB	7%
8 KB	3.5%
32 KB 以上	1 ~ 3%

容量プール階層に保存する予定のファイルのメタデータに必要な SSD ストレージ容量をサイジングする際には、容量プール階層に保存する予定のデータ 10 GiB ごとに 1 GiB の SSD ストレージという控えめな比率を使用することをお勧めします。

SSD 階層に保存されているファイルデータ

アクティブなデータセットとすべてのファイルメタデータに加えて、ファイルシステムに書き込まれたすべてのデータは、容量プールストレージに階層化される前に、最初に SSD 階層に書き込まれます。これは、 を使用してすべてのデータ階層化ポリシーで設定されたボリューム SnapMirror にデータを転送することを除いて、ボリュームの階層化ポリシーに関係なく当てはまります。

容量プール階層からのランダムリードは、SSD 階層の使用率が 90% 未満であれば、SSD 階層にキャッシュされます。詳細については、「ボリュームデータの階層化」を参照してください。

SSD 容量の推奨使用率

SSD 層の使用率が継続的に 80% を超えないようにすることをお勧めします。スケールアウトファイルシステムでは、ファイルシステムのアグリゲートの使用率が継続的に 80% を超えないようにすることをお勧めします。これらの推奨事項は、ONTAP に関する NetAppの推奨事項と一致しています。ファイルシステムの SSD 階層は、容量プール階層への書き込みのステージングや容量プール階層からのランダムリードにも使用されるため、アクセスパターンが突然変化すると、SSD 階層の使用率がすぐに上昇する可能性があります。

SSD の使用率が 90% になると、容量プール階層から読み取られたデータは SSD 階層にキャッシュされなくなるため、残りの SSD 容量はファイルシステムに書き込まれる新しいデータ用に保持されます。これにより、容量プール階層から同じデータを繰り返し読み込むと、SSD 階層からキャッシュされて読み取られるのではなく、容量プールストレージから読み取られるようになり、ファイルシステムのスループット容量に影響する可能性があります。

SSD 階層の使用率が 98% 以上になると、すべての階層化機能が停止します。詳細については、「階層化のしきい値」を参照してください。

FSx for ONTAP ストレージの効率化

NetApp ONTAP は、圧縮、圧縮、重複排除などのブロックレベルのストレージ効率機能を提供し、パフォーマンスを犠牲にすることなく、一般的なファイル共有のストレージ容量を最大 65% 節約できます。

Amazon FSx for NetApp ONTAP は、スナップショット、シンプロビジョニング、 FlexClone ボリュームなど、スペースを節約する他の ONTAP 機能もサポートしています。

ストレージ効率の機能はデフォルトでは有効になっていません。以下の手順で、有効にできます。

- ファイルシステムを作成する 場合、SVM のルートボリュームで。
- 新しいボリュームを作成する 場合。
- 既存のボリュームを変更する 場合。

ストレージ効率が有効になっているファイルシステムのストレージ削減額を確認するには、「」を参照してくださいストレージ効率の節約の表示。

ストレージ効率の節約の計算

`LogicalDataStored` および `StorageUsed`FSx for ONTAP CloudWatch ファイルシステムメトリクスを使用して、圧縮、重複排除、圧縮、スナップショット、および によるストレージの節約を計算できますFlexClones。これらのメトリクスのディメンションは 1 つで、`FileSystemId` です。詳細については、「ファイルシステムのメトリクス」を参照してください。

- ストレージ効率の節約をバイト単位でコンピューティングするには、特定の期間の `StorageUsed` の平均を取得し、同じ期間の `LogicalDataStored` の平均から減算します。
- 合計論理的なデータサイズのパーセンテージとしてストレージ効率の節約をコンピューティングするには、特定の期間の `StorageUsed` の `Average` を取得し、同じ期間の `LogicalDataStored` の `Average` から減算します。次に、同じ期間の `LogicalDataStored` の `Average` で差を割ります。

SSD のサイジングの例

データのうち 80% へのアクセス頻度が低いアプリケーション用に 100 TiB のデータを保存するとします。このシナリオでは、データの 80% (80 TB) が自動的に容量プール階層に階層化され、残りの 20% (20 TB) は SSD ストレージに残ります。汎用のファイル共有ワークロードで、65% という一般的なストレージ効率の節約に基づいた場合、7 TiB のデータ量に相当します。SSD の使用率を 80% に維持するには、20 TiB のアクティブアクセスデータに対して 8.75 TiB の SSD ストレージ容量が必要です。次の計算に示すように、プロビジョニングする SSD ストレージの量も ONTAP ソフトウェアのストレージオーバーヘッドの 16% を考慮する必要があります。

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

そのため、この例では、少なくとも 10.42 TiB の SSD ストレージをプロビジョニングする必要があります。また、アクセス頻度の低い残りの 80 TiB のデータには、28 TiB の容量プールストレージを使用します。

ファイルシステムのストレージ容量と IOPS

FSx for ONTAP ファイルシステムを作成するときは、SSD 階層のストレージ容量を指定します。スケールアウトファイルシステムでは、指定したストレージ容量は各高可用性 (HA) ペアのストレージプールに均等に分散されます。これらのストレージプールはアグリゲートと呼ばれます。

プロビジョニングした SSD ストレージの GiB ごとに、Amazon FSx はファイルシステムに対して 3 SSD 1 秒あたりの入出力オペレーション (IOPS) を自動的にプロビジョニングします。ファイルシステムあたり最大 160,000 SSD IOPS です。スケールアウトファイルシステムでは、SSD IOPS はファイルシステムの各アグリゲートに均等に分散されます。プロビジョニングされた SSD IOPS のレベルを、1 GiB あたり自動 3 SSD IOPS を超えるように指定することもできます。FSx for ONTAP ファイルシステムにプロビジョニングできる SSD IOPS の最大数の詳細については、スループット容量がパフォーマンスに与える影響 を参照してください。

トピック

- ファイルシステムの SSD ストレージと IOPS の更新
- SSD ストレージ使用率のモニタリング
- ファイルシステムストレージ容量使用率アラームの作成
- ストレージ効率の節約の表示

- SSD ストレージ容量とプロビジョンド IOPS の変更
- ストレージ容量と IOPS アップデートのモニタリング
- SSD ストレージ容量を動的に増やす

ファイルシステムの SSD ストレージと IOPS の更新

データセットのアクティブな部分にストレージを追加する必要がある場合は、Amazon FSx for NetApp ONTAP ファイルシステムの SSD ストレージ容量を増やすことができます。SSD ストレージ容量を増やすには、Amazon FSx コンソール、Amazon FSx API、または AWS Command Line Interface （ AWS CLI) を使用します。詳細については、「SSD ストレージ容量とプロビジョンド IOPS の変更」を参照してください。

Amazon FSx ファイルシステムの SSD ストレージ容量を増やすと、通常、新しい容量は数分以内に使用できます。新しい SSD ストレージ容量は、使用可能になった後に請求されます。料金の詳細については、「Amazon FSx for NetApp ONTAP の料金」を参照してください。

ストレージ容量を増やすと、Amazon FSx はストレージ最適化プロセスをバックグラウンドで実行してデータのバランスを再調整します。ほとんどのファイルシステムでは、ストレージの最適化には数時間かかり、ワークロードのパフォーマンスへの影響は最小限に抑えられます。

Amazon FSx コンソール、CLI、および API を使用して、ストレージ最適化の進捗状況をいつでも追跡できます。詳細については、「ストレージ容量と IOPS アップデートのモニタリング」を参照してください。

考慮事項

ファイルシステムの SSD ストレージ容量とプロビジョンド IOPS を変更するときに考慮すべき重要な項目を以下に示します。

- ストレージ容量増量のみ - ファイルシステムのストレージ容量を増加することのみできます。ストレージ容量を減らすことはできません。
- ストレージ容量増量の最小値 – 各 SSD ストレージ容量の増加は、ファイルシステムの現在の SSD ストレージ容量の 10% 以上で、ファイルシステム構成の最大 SSD ストレージ容量以下である必要があります。
- (スケールアウトのみ) ストレージ容量の分散 – ファイルシステム用に選択した新しいストレージ容量や SSD IOPS は、ファイルシステムの各アグリゲートに均等に分散されます。
- 増加の間隔 — ファイルシステムの SSD ストレージ容量、プロビジョンド IOPS、スループットキャパシティのいずれかを変更した後に、同じファイルシステムで再度これらの構成のいずれかを

変更するときは、6 時間以上待機する必要があります。これは、クールダウン期間と呼ばれることもあります。

- プロビジョンド IOPS モード - プロビジョンド IOPS の変更については、2 つの IOPS モードのうち、いずれかを指定する必要があります。
  - 自動モード – Amazon FSx は、SSD IOPS を自動的にスケールして、SSD ストレージ容量 1 GiB ごとに 3 つのプロビジョニングされた SSD IOPS を維持します。上限は、ファイルシステム構成の最大 SSD IOPS です。

    > **Note**
    >
    > FSx for ONTAP ファイルシステムにプロビジョニングできる SSD IOPS の最大数の詳細については、スループット容量がパフォーマンスに与える影響 を参照してください。

  - [User-provisioned] (ユーザープロビジョニング) モード - SSD IOPS の数を指定します。これは、SSD ストレージ容量の GiB あたり 3 IOPS 以上である必要があります。より高いレベルの IOPS のプロビジョニングを選択した場合は、その月のインクルードレートを上回ってプロビジョニングされた平均 IOPS に対して支払います。これは、IOPS 月単位で測定されます。

料金の詳細については、「Amazon FSx for NetApp ONTAP の料金」を参照してください。

SSD ストレージ容量を増やすタイミング

使用可能な SSD 階層ストレージが不足している場合は、ファイルシステムのストレージ容量を増やすことをお勧めします。ストレージが不足すると、データセットのアクティブな部分の SSD 階層のサイズが小さくなることを示します。

ファイルシステムで使用可能な空きストレージの量をモニタリングするには、ファイルシステムレベル`StorageCapacity`と `StorageUsed` Amazon CloudWatch メトリクスを使用します。メトリクスに CloudWatch アラームを作成し、特定のしきい値を下回ったときに通知を受け取ることができます。詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。

> **Note**
>
> データ階層化、スループットスケーリング、他のメンテナンス用アクティビティが適切に機能し、追加のデータに使用できる容量を確保するために、SSD ストレージの容量使用率が 80% を超えないようにすることをお勧めします。スケールアウトファイルシステムの場合、

この推奨事項はファイルシステムのすべてのアグリゲートの平均使用率と個々のアグリゲートの両方に適用されます。

ファイルシステムの SSD ストレージの使用方法、およびファイルメタデータとオペレーティングソフトウェア用に SSD ストレージがどれだけ確保されているかについては、適切な量のファイルシステム SSD ストレージを選択する を参照してください。

SSD ストレージ使用率のモニタリング

さまざまな AWS およびNetAppツールを使用して、ファイルシステムの SSD ストレージ容量の使用率をモニタリングできます。Amazon CloudWatch を使用すると、ストレージ容量の使用率をモニタリングし、ストレージ容量の使用率がカスタマイズ可能なしきい値に達したときに警告するアラームを設定できます。

> **Note**
>
> SSD ストレージ層のストレージ容量使用率が 80% を超えないようにすることをお勧めします。これにより、階層化が適切に機能し、新しいデータのオーバーヘッドが発生します。SSD ストレージ層のストレージ容量使用率が一貫して 80% を上回っている場合は、SSD ストレージ層の容量を増やすことができます。詳細については、「ファイルシステムの SSD ストレージと IOPS の更新」を参照してください。

Amazon FSx コンソールで、ファイルシステムの使用可能な SSD ストレージと全体的なストレージディストリビューションを表示できます。[Available SSD storage capacity] (利用可能な SSD ストレージ容量) グラフには、ファイルシステムで利用可能な SSD ベースのストレージ容量が時系列で表示されます。[Storage distribution] (ストレージ分布) グラフは、ファイルシステム全体のストレージ容量が現在、次の 3 つのカテゴリにどのように分布しているか示しています。

- 容量プール層
- SSD 階層 - 利用可能
- SSD 階層 - 使用済み

次の手順を使用して AWS Management Console、ファイルシステムの SSD ストレージ容量の使用率を でモニタリングできます。

ファイルシステムの使用可能な SSD 階層ストレージ容量をモニタリングするには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーション列でファイルシステムを選択し、ストレージ容量情報を表示するONTAP ファイルシステムを選択します。ファイルシステムの詳細ページが表示されます。
3. 2 番目のパネルで、モニタリングとパフォーマンスタブを選択し、ストレージ を選択します。集約グラフあたりの使用可能なプライマリストレージ容量とストレージ容量使用率が表示されます。

ファイルシステムストレージ容量使用率アラームの作成

SSD ストレージ容量の平均使用率が一貫して 80% を超えないようにすることをお勧めします。SSD ストレージの使用率が 80% を超える場合もあるのは許容範囲です。平均使用率を 80% 未満に維持することで、問題なくストレージを増やすことができる十分な容量が確保できます。次の手順は、ファイルシステムの SSD ストレージ使用率が 80% に近づいたときに警告する CloudWatch アラームを作成する方法を示しています。

ファイルシステム SCU アラームを作成するには

`StorageCapacityUtilization` メトリクスを使用して、1 つ以上の FSx for ONTAP ファイルシステムがストレージ使用率のしきい値に達したときにトリガーされるアラームを作成できます。

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. 左側のナビゲーションペインのアラーム で、すべてのアラーム を選択します。次に、アラームの作成 を選択します。アラームの作成ウィザードで、メトリクスの選択 を選択します。
3. グラフエクスプローラー で、マルチソースクエリタブを選択します。
4. クエリビルダー で、以下を選択します。
   - 名前空間 で、AWS/FSx > 詳細なファイルシステムメトリクス を選択します。
   - メトリクス名 で、MAX(StorageCapacityUtilization) を選択します。
   - によるフィルタリングでは、オプションで ID で特定のファイルシステムを含めたり除外したりできます。Filter by empty のままにすると、ファイルシステムがアラームのストレージ容量使用率のしきい値を超えると、アラームがトリガーされます。
   - 残りのオプションは空のままにして、グラフクエリ を選択します。
5. [メトリクスの選択] を選択します。ウィザードのメトリクスセクションに戻り、メトリクスにラベル を付けます。期間を 5 分にしておくことをお勧めします。

6. 条件 で、メトリクスが 80 より大きい/等しい場合は常に、静的しきい値タイプ を選択します。
7. 次へ を選択して、「アクションの設定」ページに移動します。

アラームアクションを設定するには

アラームが設定したしきい値に達したときにトリガーするように、さまざまなアクションを設定できます。この例では、Simple Notification Service (SNS) トピックを選択しますが、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch アラームの使用」で他のアクションについて学ぶことができます。

1. 通知セクションで、アラームが ALARM状態になったときに通知する SNS トピックを選択します。既存のトピックを選択するか、新しいトピックを作成できます。E メールアドレスへのアラーム通知を受信する前に確認する必要があるサブスクリプション通知が送信されます。
2. [次へ] をクリックします。

アラームを終了するには

以下の手順に従って、 CloudWatch アラームを作成するプロセスを完了します。

1. 「名前と説明を追加」ページで、アラームに名前を付け、オプションで説明を指定して、次へ を選択します。
2. プレビューと作成ページで設定した内容をすべて確認し、アラームの作成 を選択します。

ストレージ効率の節約の表示

を有効にする CloudWatch と、Amazon FSx コンソール、Amazon コンソール、および ONTAP CLI で保存しているストレージ容量を確認できます。

ストレージ効率の節約を表示するには (コンソール)

FSx for ONTAP ファイルシステムの Amazon FSx コンソールに表示されるストレージ効率の節約には、 FlexClones および からの節約が含まれます SnapShots。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [File systems] (ファイルシステム) のリストから、ストレージ効率の節約をモニタリングする FSx for ONTAP ファイルシステムを選択します。

3. ファイルシステムの詳細ページの 2 番目のパネルの「モニタリングとパフォーマンス」タブで「概要」を選択します。
4. [Storage efficiency savings] (ストレージ効率の節約グラフ) には、論理データサイズに対するスペースの節約率と物理バイト数が表示されます。

ストレージ効率の節約を表示するには (ONTAP CLI)

ONTAP CLI を使用して `storage aggregate show-efficiency` コマンドFlexClonesを実行すると、スナップショットや の影響なしに、圧縮、圧縮、重複排除のストレージ効率を節約できます。詳細については、「 NetApp ONTAPドキュメントセンター」の「ストレージ集計の show-efficiency」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. storage aggregate show-efficiency コマンドは、すべてのアグリゲートのストレージ効率に関する情報を表示します。ストレージ効率は 4 つの異なるレベルで表示されます。

   - 合計
   - 集計
   - ボリューム
   - スナップショットと FlexClone ボリューム

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   Total Storage Efficiency Ratio:         4.29:1
   ```

```
Aggregate: aggr2
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                     2.39:1
Total Storage Efficiency Ratio:                 4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:                5.03:1
Compression Efficiency:                         1.00:1

Snapshot Volume Storage Efficiency:             8.81:1
FlexClone Volume Storage Efficiency:            1.00:1
Number of Efficiency Disabled Volumes:          1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                     2.39:1
Total Storage Efficiency Ratio:                 4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:                5.03:1
Compression Efficiency:                         1.00:1

Snapshot Volume Storage Efficiency:             8.81:1
FlexClone Volume Storage Efficiency:            1.00:1
Number of Efficiency Disabled Volumes:          1
```

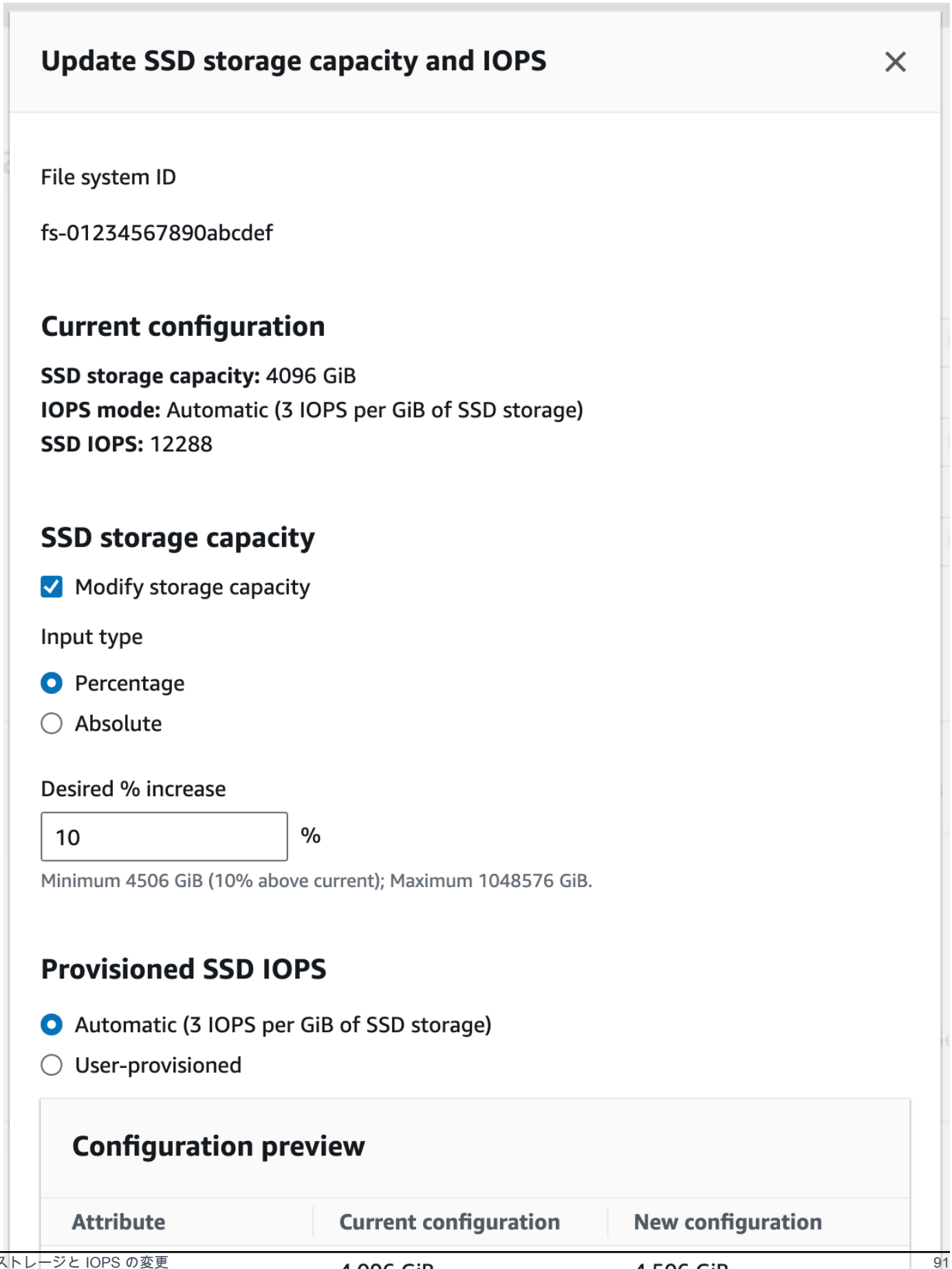
SSD ストレージ容量とプロビジョンド IOPS の変更

ファイルシステムの SSD ベースのストレージを増やすことができ、Amazon FSx コンソール、、および API を使用して AWS CLI、プロビジョニングされた SSD IOPS の量を増減できます。

ファイルシステムの SSD ストレージ容量またはプロビジョンド IOPS を更新するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左のナビゲーションペインで [File system] (ファイルシステム) を選択します。[File system] (ファイルシステム) リストで、SSD ストレージ容量と SSD IOPS を更新する FSx for ONTAP ファイルシステムを選択します。
3. [Action] (アクション) > [Update storage capacity] (ストレージ容量をアップデート) を選択します。または、[Summary] (概要) パネルで、ファイルシステムの横にある [SSD storage capacity] (ストレージ容量) の [Update] (更新) を選択します。

   [Update SSD storage capacity and IOPS] (SSD ストレージ容量と IOPS をアップデートする) ダイアログボックスが表示されます。



Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. SSD ストレージ容量を増やすには、[Modify storage capacity] (ストレージ容量の変更) を選択します。
5. [Input type] (入力タイプ) で、以下のいずれかを選択します。
   - 新しい SSD ストレージ容量を現在の値からの変化率として入力するには、[Percentage] (割合 (%) を選択します。
   - 新しい値を GiB に入力するには、[Absolute] (絶対) を選択します。
6. 入力タイプに応じて、[Desired % increase] (希望する % 増加) の値を入力します。
   - [Percentage] (割合 (%) で、増加率の値を入力します。この値は、現在の値より 10% 以上大きい値である必要があります。
   - [Absolute] (絶対) を使用する場合、新しい値を GiB に入力します。最大許容値 196,608 GiB までです。
7. [Provisioned SSD IOPS] (プロビジョンド SSD IOPS) で、ファイルシステムの IOPS 数をプロビジョニングするには、次の 2 つのオプションがあります。
   - Amazon FSx が SSD IOPS を自動的にスケーリングして、SSD ストレージのストレージ容量 GiB あたり 3 プロビジョンド SSD IOPS (最大 160,000 まで) を維持する場合は、[Automatic] (自動) を選択します。
   - IOPS の数を指定する場合は、[User-provisioned] (ユーザープロビジョニング) を選択します。SSD ストレージ階層の GiB の 3 倍以上、160,000 以下である IOPS の絶対数を入力します。

> **Note**
>
> FSx for ONTAP ファイルシステムにプロビジョニングできる SSD IOPS の最大数の詳細については、スループット容量がパフォーマンスに与える影響 を参照してください。

8. [更新] を選択します。

> **Note**
>
> プロンプトの下部に、新しい SSD ストレージ容量と SSD IOPS の設定プレビューが表示されます。スケールアウトファイルシステムでは、HA ペアあたりの値も表示されます。

SSD ストレージ容量とファイルシステム用にプロビジョニングされた IOPS を更新するには (CLI)

FSx for ONTAP ファイルシステムの SSD ストレージ容量とプロビジョンド IOPS を更新するには、AWS CLI コマンドupdate-file-systemまたは同等の UpdateFileSystem API アクションを使用します。以下のパラメータを値で設定します。

- `--file-system-id` を更新するファイルシステムの ID に設定します。
- SSD ストレージ容量を増やすには、 `--storage-capacity`をターゲットストレージ容量値に設定します。この値は、現在の値よりも 10% 以上大きくする必要があります。
- プロビジョンド SSD IOPS を変更するには、`--ontap-configuration DiskIopsConfiguration` プロパティを使用します。このプロパティには、`Iops` と `Mode` の 2 つのパラメータがあります。
  - プロビジョンド IOPS の数を指定する場合は、`Iops=`*`number_of_IOPS`* (最大 160,000 まで) と `Mode=USER_PROVISIONED` を使用します。IOPS 値は、リクエストされた SSD ストレージ容量の 3 倍以上にする必要があります。ストレージ容量を増やさない場合、IOPS 値は現在の SSD ストレージ容量の 3 倍以上である必要があります。
  - Amazon FSx で SSD IOPS を自動的に増加させたい場合は、`Mode=AUTOMATIC` を使用し、`Iops` パラメータは使用しないでください。Amazon FSx は、プロビジョニングされた SSD ストレージ容量の GiB あたり 3 SSD IOPS を自動的に維持します (最大 160,000)。

> **Note**
>
> FSx for ONTAP ファイルシステムにプロビジョニングできる SSD IOPS の最大数の詳細については、スループット容量がパフォーマンスに与える影響 を参照してください。

次の例では、ファイルシステムの SSD ストレージを 2000 GiB に増やし、ユーザープロビジョニングされた SSD IOPS の量を 7000 に設定します。

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

更新の進行状況をモニタリングするには、 describe-file-systems AWS CLI コマンドを使用します。出力で `AdministrativeActions` セクションを探します。

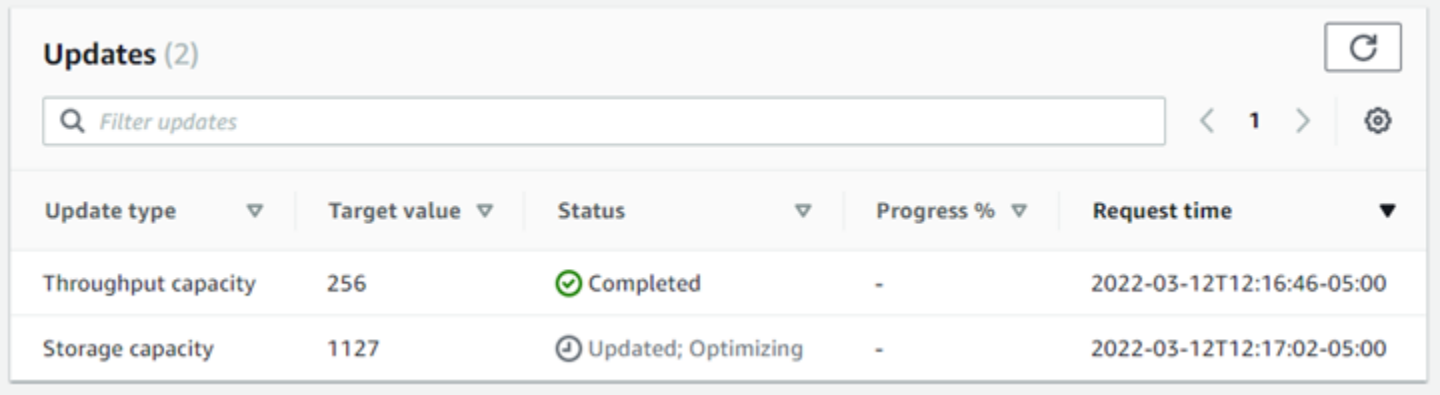
詳細については、AdministrativeAction「Amazon FSx for NetApp ONTAP API リファレンス」の「」を参照してください。

ストレージ容量と IOPS アップデートのモニタリング

Amazon FSx コンソール、CLI、および API を使用して、SSD ストレージ容量と IOPS 更新の進行状況をモニタリングできます。

ストレージと IOPS の更新をモニタリングするには (コンソール)

FSx for ONTAP ファイルシステムの [File system details] (ファイルシステムの詳細) ページの [Update] (更新) タブで、各更新タイプの最新の 10 件の更新ケースを表示できます。



ストレージ容量の更新については、次の情報を表示できます。

[Update type] (更新タイプ)

サポートされているタイプは次のとおりです。[Storage capacity] (ストレージ容量)、[Mode] (モード)、および IOPS です。[Mode] (モード) と IOPS の値は、すべてのストレージ容量と IOPS スケーリングリクエストについて一覧表示されます。

[Target value] (ターゲット値)

ファイルシステムの SSD ストレージ容量または IOPS を更新するために指定した値です。

[Status] (ステータス)

更新の現在のステータス。指定できる値は次のとおりです。

- [Pending] (保留中) - Amazon FSx は更新リクエストを受信しましたが、処理を開始していません。
- [In progress] (進行中) - Amazon FSx が更新リクエストを処理しています。

- [Updated; Optimizing] (更新済み、最適化) - Amazon FSx により、ファイルシステムのストレージ容量が増加されました。ストレージ最適化プロセスでは、バックグラウンドでデータの再バランシングが行われています。
- [Completed] (完了) - 更新は正常に終了しました。
- [Failed] (失敗) - 更新リクエストが失敗する。詳細を見るには、疑問符 ([?]) を選択します。

[Progress %] (進行 %)

ストレージ最適化プロセスの進行状況を、完了率として表示します。

[Request time] (リクエスト時間)

Amazon FSx が更新アクションリクエストを受信した時刻。

ストレージと IOPS の更新をモニタリングするには (CLI)

describe-file-systems AWS CLI コマンドと DescribeFileSystems API オペレーションを使用して、ファイルシステムの SSD ストレージ容量の増加リクエストを表示およびモニタリングできます。`AdministrativeActions` 配列には、管理アクションタイプごとに最新の更新アクションが 10 件を表示されます。ファイルシステムのストレージ容量を増やすと、`FILE_SYSTEM_UPDATE` および `STORAGE_OPTIMIZATION` アクションの 2 つの `AdministrativeActions` が生成されます。

次の例は、`describe-file-systems` CLI コマンドのレスポンスの抜粋を示しています。ファイルシステムには、SSD ストレージ容量を 2000 GiB に、プロビジョンド SSD IOPS を 7000 に増やすための保留中の管理アクションがあります。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
```

```
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx はまず FILE_SYSTEM_UPDATE アクションを処理し、新しい大きなストレージディスクをファイルシステムに追加します。新しいストレージがファイルシステムで使用可能になると、FILE_SYSTEM_UPDATE ステータスが UPDATED_OPTIMIZING に変わります。ストレージ容量は新しい大きな値を示し、Amazon FSx は STORAGE_OPTIMIZATION 管理アクションの処理を開始します。この動作は、describe-file-systems CLI コマンドのレスポンスの次の抜粋を示しています。

ProgressPercent プロパティには、ストレージ最適化プロセスの進行状況が表示されます。ストレージ最適化プロセスが正常に完了すると、FILE_SYSTEM_UPDATE アクションが COMPLETED に変更され、STORAGE_OPTIMIZATION アクションは表示されなくなります。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

ストレージ容量または IOPS 更新リクエストが失敗した場合、次の例に示すように、FILE_SYSTEM_UPDATE アクションが FAILED に変更されます。FailureDetails プロパティでは、障害に関する情報が表示されます。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

SSD ストレージ容量を動的に増やす

次のソリューションを使用すると、使用している SSD ストレージ容量が指定したしきい値を超えた場合に、FSx for ONTAP ファイルシステムの SSD ストレージ容量を動的に増やすことができます。この AWS CloudFormation テンプレートは、ストレージ容量のしきい値、このしきい値に基づく Amazon CloudWatch アラーム、ファイルシステムのストレージ容量を増やす AWS Lambda 関数を定義するために必要なすべてのコンポーネントを自動的にデプロイします。

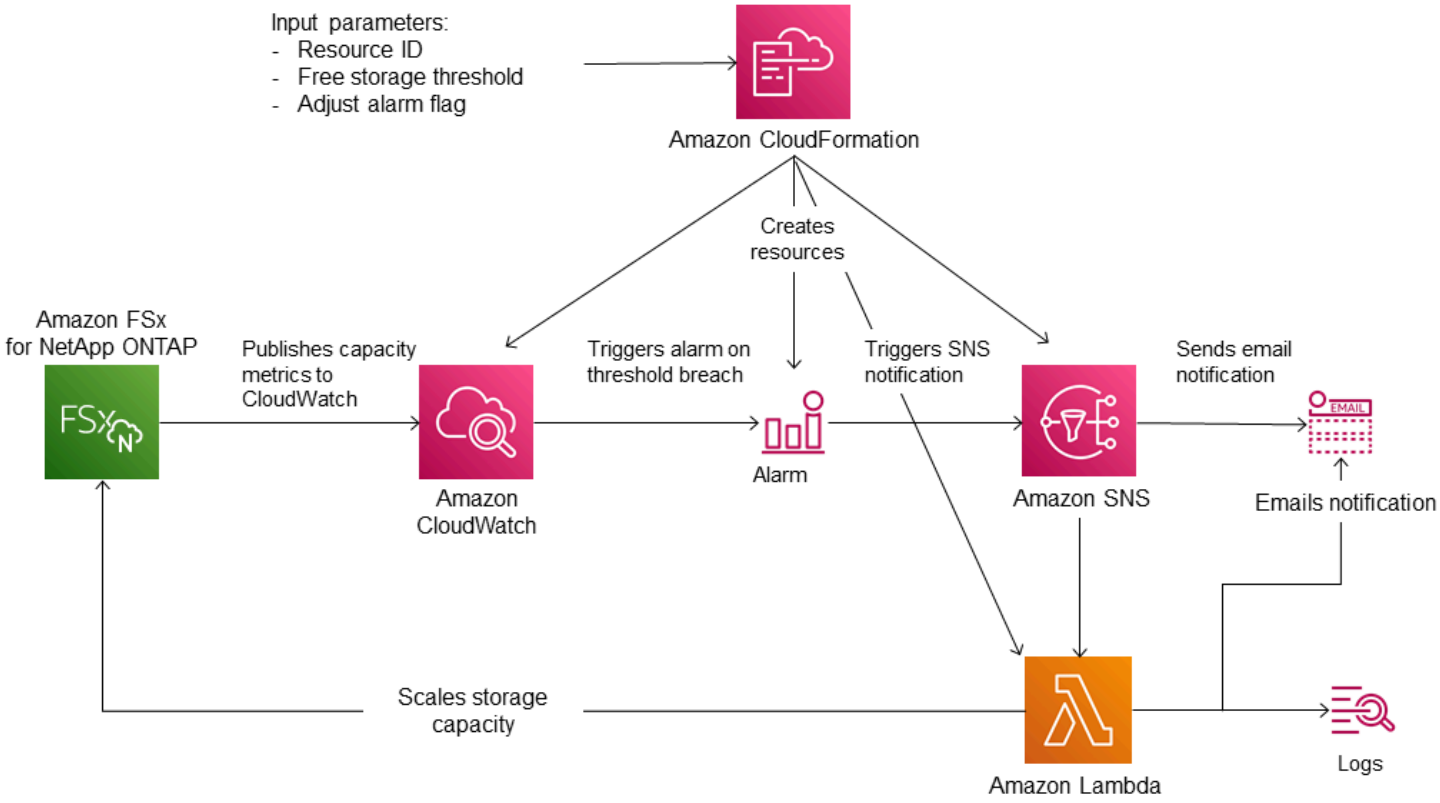
このソリューションは、必要なすべてのコンポーネントを自動的にデプロイし、以下のパラメータを使用します。

- FSx for ONTAP ファイルシステム ID。
- 使用している SSD ストレージ容量のしきい値 (数値)。これは、 CloudWatch アラームがトリガーされる割合です。
- ストレージ容量の増加率 (%)。
- スケーリング通知の受信に使用する E メールアドレス。

トピック

アーキテクチャの概要

このソリューションをデプロイすると、 AWS クラウドに以下のリソースが構築されます。



この図表は以下のステップを示しています。

1. AWS CloudFormation テンプレートは、 CloudWatch アラーム、 AWS Lambda 関数、Amazon Simple Notification Service (Amazon SNS) キュー、および必要なすべての (IAM) ロールをデプロイします。 AWS Identity and Access Management IAM ロールは、Amazon FSx API オペレーションを呼び出すためのアクセス許可を Lambda 関数に付与します。
2. CloudWatch は、ファイルシステムの使用済みストレージ容量が指定されたしきい値を超えたときにアラームをトリガーし、Amazon SNS キューにメッセージを送信します。アラームは、ファイルシステムの使用している容量が 5 分間、継続的にしきい値を超えた場合にのみトリガーされます。

3. ソリューションによって、この Amazon SNS トピックに登録されている Lambda 関数がトリガーされます。
4. Lambda 関数は、指定された増加率の値に基づいて新しいファイルシステムのストレージ容量を計算し、新しいファイルシステムのストレージ容量を設定します。
5. Lambda 関数オペレーションの元の CloudWatch アラーム状態と結果は、Amazon SNS キューに送信されます。

CloudWatch アラームへの応答として実行されたアクションに関する通知を受信するには、サブスクリプション確認 E メールに記載されているリンクに従って Amazon SNS トピックサブスクリプションを確認する必要があります。

AWS CloudFormation テンプレート

このソリューションでは AWS CloudFormation 、 を使用して、FSx for ONTAP ファイルシステムのストレージ容量を自動的に増やすために使用されるコンポーネントのデプロイを自動化します。このソリューションを使用するには、FSxOntapDynamicStorageScaling AWS CloudFormation テンプレートをダウンロードします。

テンプレートは、次のように説明されている パラメータ を使用します。テンプレートパラメータとそのデフォルト値を確認し、ファイルシステムのニーズに合わせて変更します。

FileSystemId

デフォルト値はありません。ストレージ容量を自動的に拡張したいファイルシステムの ID。

LowFreeDataStorageCapacityThreshold

デフォルト値はありません。使用しているストレージ容量のしきい値を、ファイルシステムの現在のストレージ容量のパーセンテージ (%) で指定します。このしきい値で、アラームがトリガーされ、ファイルシステムのストレージ容量が自動的に拡張されます。使用しているストレージがこのしきい値を超えると、ファイルシステムの空きストレージ容量が低いと見なされます。

EmailAddress

デフォルト値はありません。SNS サブスクリプションに使用するメールアドレスを指定して、ストレージ容量のしきい値アラートを受信します。

PercentIncrease

デフォルトは、20% です。現在のストレージ容量のパーセンテージとして表される、ストレージ容量を増やす量を指定します。

> **Note**
>
> ストレージスケーリングは、 CloudWatch アラームが ALARM状態になるたびに 1 回試行されます。ストレージのスケーリングオペレーションが試行された後でも SSD ストレージ容量の使用率がしきい値を超えている場合、ストレージスケーリングオペレーションは再度試行されません。

MaxFSxSizeinGi B

デフォルトは、196608 です。SSD ストレージでサポートされる最大ストレージ容量を指定します。

による自動デプロイ AWS CloudFormation

次の手順では、FSx for ONTAP ファイルシステムのストレージ容量を自動的に増やすように AWS CloudFormation スタックを設定してデプロイします。デプロイには、数分かかります。CloudFormation スタックの作成の詳細については、「 ユーザーガイド」の「 AWS CloudFormation コンソールでのスタックの作成AWS CloudFormation 」を参照してください。

> **Note**
>
> このソリューションを実装すると、関連する AWS サービスの料金が発生します。詳細については、それらのサービスの料金詳細ページを参照してください。

開始する前に、 の Amazon Virtual Private Cloud (Amazon VPC) で実行されている Amazon FSx ファイルシステムの ID が必要です AWS アカウント。Amazon FSx リソースの作成の詳細については、「Amazon FSx for NetApp ONTAP の開始方法」を参照してください。

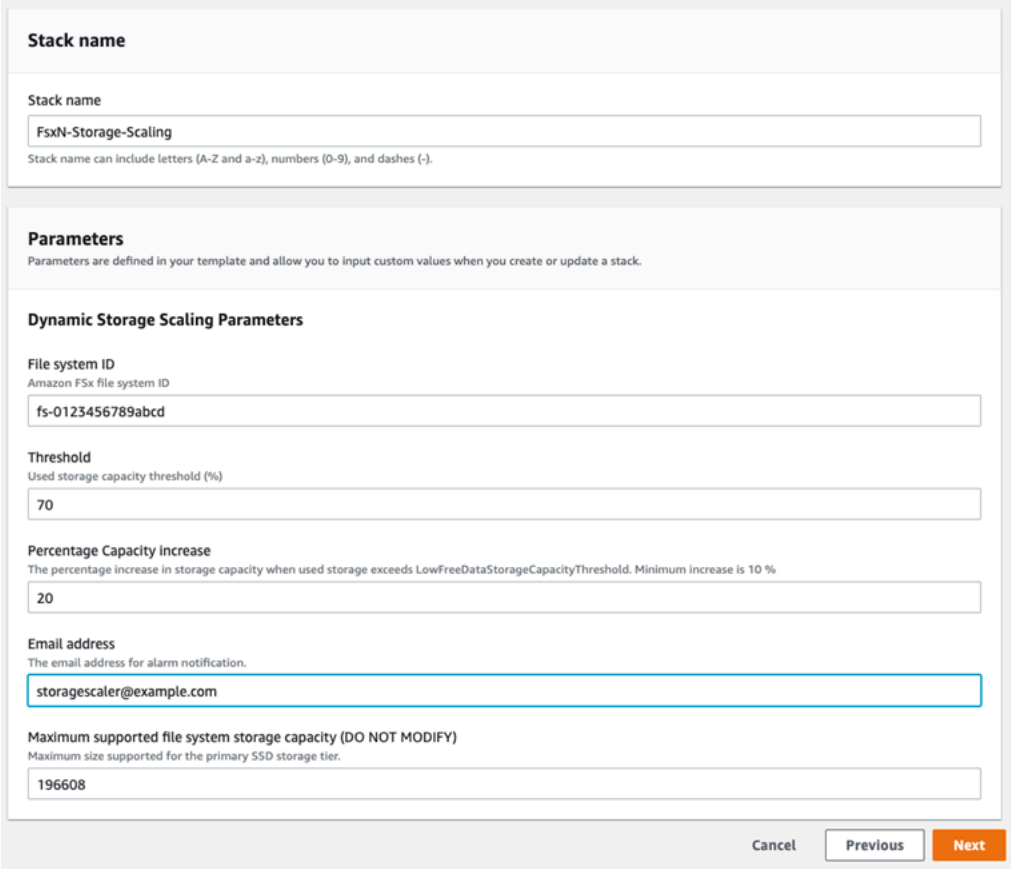
自動ストレージ容量拡張ソリューションスタックを起動するには

1. FSxOntapDynamicStorageScaling AWS CloudFormation テンプレートをダウンロードします。

   > **Note**
   >
   > Amazon FSx は現在、特定の AWS リージョンでのみ利用可能です。このソリューションは、Amazon FSx が利用可能な AWS リージョンで起動する必要があります。詳細

については、「AWS 全般のリファレンス」の「Amazon FSx エンドポイントとクォータ」を参照してください。

2. AWS CloudFormation コンソールから、スタックの作成 > 新しいリソース を選択します。
3. [Template is ready] (テンプレートの準備完了) を選択します。[Specify template] (テンプレートの指定) セクションで、[Upload a template file] (テンプレートファイルをアップロード) を選択し、ダウンロードしたテンプレートをアップロードします。
4. [Specify stack details] (スタック詳細の指定) では、自動ストレージ容量増加ソリューションの値を入力します。



5. [Stack name] (スタック名) を入力します。
6. [Parameters] (パラメータ) については、テンプレートのパラメータを確認し、ファイルシステムのニーズに合わせて変更します。次いで、[次へ] を選択します。

> **Note**
>
> この CloudFormation テンプレートでスケーリングが試行されたときに E メール通知を受信するには、テンプレートのデプロイ後に受信する SNS サブスクリプション E メールを確認します。

7. カスタムソリューションに必要な [Options] (オプション) 設定を入力し、[Next] (次へ) を選択します。
8. [Review] (確認) では、ソリューション設定を確認して確定します。テンプレートが IAM リソースを作成することを認めるチェックボックスを選択します。
9. [Create] (作成) を選択してスタックをデプロイします。

スタックのステータスは、 AWS CloudFormation コンソールの ステータス 列で表示できます。数分で [CREATE_COMPLETE] (作成完了) のステータスが表示されます。

スタックの更新

スタックの作成後、同じテンプレートを使用してパラメータに新しい値を指定することで、スタックを更新できます。詳細については、「AWS CloudFormation ユーザーガイド」の「スタックの直接更新」を参照してください。

ボリュームストレージ容量

FSx for ONTAP ボリュームは、データをグループ化し、データの保存方法を決定し、データへのアクセスの種類を決定するために使用する仮想リソースです。ボリュームは、フォルダと同様に、ファイルシステムのストレージ容量自体を消費しません。ボリュームに保存されているデータのみが SSD ストレージを消費し、ボリュームの階層化ポリシー によっては容量プールストレージも消費します。ボリュームのサイズは作成時に設定し、後でサイズを変更できます。、、API AWS Management Console、 AWS CLI ONTAP CLI を使用して、FSx for ONTAP ボリュームのストレージ容量をモニタリングおよび管理できます。

トピック

- ボリュームデータの階層化
- スナップショットとボリュームストレージ容量
- ボリュームファイル容量
- ボリュームのストレージ容量の更新

- ボリュームの自動サイズ調整の有効化
- ボリュームストレージ容量のモニタリング
- ボリュームの階層化ポリシーの設定
- 最低冷却日数の設定
- ボリュームのクラウド検索ポリシーの設定
- ボリュームのファイル容量を表示する
- ボリューム上の最大ファイル数を増やす
- ボリュームのクラウド書き込みモードの有効化

ボリュームデータの階層化

Amazon FSx for NetApp ONTAP ファイルシステムには、プライマリストレージと容量プールストレージの 2 つのストレージ階層があります。プライマリストレージは、データセットのアクティブな部分に合わせて設計された、プロビジョニングされ、スケーラブルでハイパフォーマンスな SSD ストレージです。容量プールストレージは、ペタバイトサイズまで拡張できる完全に伸縮性のあるストレージ階層で、アクセス頻度の低いに対してコストが最適化されます。

各ボリュームのデータは、ボリュームの階層化ポリシー、冷却期間、しきい値の設定に基づいて、キャパシティプールストレージ階層に自動的に階層化されます。以下のセクションでは、ONTAPボリューム階層化ポリシーと、データが容量プールに階層化されるタイミングを決定するために使用されるしきい値について説明します。

ボリューム階層化ポリシー

FSx for ONTAP ファイルシステムのストレージ階層の使用方法を決めるには、ファイルシステム上の各ボリュームの階層化ポリシーを選択します。ボリュームの作成時に階層化ポリシーを選択し、Amazon FSx コンソール、、API AWS CLI、または NetApp 管理ツール を使用していつでも変更できます。どのデータを容量プールのストレージに階層化するかは (階層化するデータがある場合) 、以下のポリシーから選択できます。

> **Note**
>
> 階層化により、ファイルデータとスナップショットデータを容量プール階層に移動できます。ただし、ファイルメタデータは常に SSD 階層に残ります。詳細については、「SSD ストレージの使用方法」を参照してください。

- [Auto] (自動) — このポリシーは、すべてのコールドデータ (ユーザーデータとスナップショット) を容量プール階層に移動します。データの冷却速度は、ポリシーの冷却期間 (デフォルトは 31 日間) によって決定され、2〜183 日の間で設定できます。基盤となるコールドデータブロックが (一般的なファイルアクセスのように) ランダムに読み取られると、ホットになり、プライマリストレージ層に書き込まれます。コールドデータブロックが (ウイルス対策スキャンなどで) 順番に読み取られると、コールドデータブロックはコールドのまま容量プールのストレージ階層に残ります。これは、Amazon FSx コンソールを使用してボリュームを作成するときのデフォルトポリシーです。
- [Snapshot Only] (スナップショットのみ) — このポリシーは、スナップショットデータのみを容量プールのストレージ階層に移動します。スナップショットが容量プールに階層化される速度は、ポリシーの冷却期間によって決まります。冷却期間は、デフォルトで 2 日間に設定され、2 ~ 183 日の間で設定できます。コールドスナップショットデータが読み取られると、ホットになり、プライマリストレージ階層に書き込まれます。これは、、Amazon FSx API AWS CLI、または NetApp ONTAP CLI を使用してボリュームを作成するときのデフォルトポリシーです。
- [All] (すべて) — このポリシーは、すべてのユーザーデータとスナップショットデータをコールドとしてマークし、容量プール階層に保存します。データブロックが読み込み時には、コールド状態のまま、プライマリストレージ階層には書き込まれません。[All] (すべて) の階層化 ポリシーを使用してボリュームにデータを書き込むと、最初は SSD ストレージ階層に書き込まれ、バックグラウンドプロセスによって容量プールに階層化されます。ファイルのメタデータは常に SSD 階層に残っていることに注意してください。
- [None] (なし) — このポリシーは、ボリュームのすべてのデータをプライマリストレージ層に保持し、キャパシティプールストレージに移動できないようにします。他のポリシーを使用した後、ボリュームをこのポリシーに設定した場合、容量プールストレージにあったボリューム内の既存のデータは、SSD の使用率が 90% 未満であれば、バックグラウンドプロセスによって SSD ストレージに移動されます。このバックグラウンドプロセスは、意図的にデータを読み取るか、ボリュームのクラウド検索ポリシーを変更することで高速化できます。詳細については、「クラウド取得ポリシー」を参照してください。

ベストプラクティスとして、容量プールストレージに長期的に保存する予定のデータを移行する場合は、ボリュームで [自動] 階層化ポリシーを使用することをお勧めします。[自動] 階層化を使用すると、データは SSD ストレージ階層に最低 2 日間 (ボリュームの冷却期間に基づく) 保存された後、容量プール階層に移動します。SSD ストレージにデータを 2 日間以上保持すると、ONTAP はデータにポストプロセス圧縮と重複除外を実行するため、データを節約できます。これは、データを容量プールに階層化したときにも保持されます。ONTAP は SSD ストレージ上のデータに対してのみポストプロセス圧縮と重複除外を実行するため、このポリシーを選択すると、長期的なストレージ節約

率を最大化できます。また、バックアップされるデータは SSD ストレージ上にあるため、ボリュームの最初に作成するバックアップの転送速度を最大化することもできます。

ボリュームの階層化ポリシーの設定または変更の詳細については、ボリュームの階層化ポリシーの設定 を参照してください。

階層化の冷却期間

ボリュームの階層化冷却期間は、SSD 階層内のデータがコールドとしてマークされるまでにかかる時間を設定します。冷却期間は、`Auto` や `Snapshot-only`、および階層化ポリシーに適用されます。冷却期間は 2～183 日の範囲の値に設定できます。冷却期間の設定の詳細については、最低冷却日数の設定 を参照してください。

データは、冷却期間が終了してから 24～48 時間後に階層化されます。階層化はネットワークリソースを消費するバックグラウンドプロセスであり、クライアント側のリクエストよりも優先度が低くなります。クライアント側のリクエストが続いている場合、階層化アクティビティは制限されます。

クラウド取得ポリシー

ボリュームのクラウド検索ポリシーは、容量プール階層から読み取られたデータを SSD 階層に昇格させるタイミングを指定するための条件を設定します。クラウド検索ポリシーを `Default` 以外に設定すると、このポリシーがボリュームの階層化ポリシーの取得動作よりも優先されます。ボリュームには、次のいずれかのクラウド検索ポリシーがあります。

- [Default] (デフォルト) — このポリシーは、ボリュームの基礎となる階層化ポリシーに基づいて階層化されたデータを取得します。これはすべてのボリュームのデフォルトのクラウド検索ポリシーです。
- [Never] (なし) — このポリシーは、読み取りがシーケンシャルかランダムかに関係なく、階層化されたデータを取得しません。これは、ボリュームの階層化ポリシーを [All] (すべて) に設定するのと似ていますが、他のポリシー - [Auto] (自動)、[Snapshot-only] (スナップショットのみ) - と併用することで、データを即時ではなく、最小冷却期間に従って階層化することができます。
- [On-read] (読み取り時) — このポリシーは、クライアント主導のすべてのデータ読み取りに対して、階層化されたデータを取得します。このポリシーは、[All] (すべての) 階層化ポリシーを使用している場合は効果がありません。
- [Promote] (プロモート) — このポリシーは、容量プールにあるボリュームのすべてのデータを SSD 階層に取得対象としてマークします。データは、日次バックグラウンド階層化スキャナーが、次回実行されたときにマークされます。このポリシーは、頻繁には実行されない周期的なワークロードがあるが、実行時には SSD 階層のパフォーマンスが必要なアプリケーションにとって有

益です。このポリシーは、[All] (すべての) 階層化ポリシーを使用している場合は効果がありません。

ボリュームのクラウド検索ポリシーの設定については、ボリュームのクラウド検索ポリシーの設定を参照してください。

階層化のしきい値

ファイルシステムの SSD ストレージ容量使用率によって、 がすべてのボリュームの階層化動作 ONTAPを管理する方法が決まります。ファイルシステムの SSD ストレージ容量の使用状況に基づいて、以下のしきい値によって階層化の動作が説明どおりに設定されます。ボリュームの SSD ストレージ階層の容量使用率を監視する方法については、ボリュームストレージ容量のモニタリング を参照してください。

> **Note**
>
> SSD ストレージ層のストレージ容量使用率が 80% を超えないようにすることをお勧めします。スケールアウトファイルシステムの場合、この推奨事項は、ファイルシステムのすべてのアグリゲートの合計平均使用率と、個々のアグリゲートの使用率の両方に適用されます。これにより、階層化が適切に機能し、新しいデータのオーバーヘッドが発生します。SSD ストレージ層のストレージ容量使用率が一貫して 80% を上回っている場合は、SSD ストレージ層の容量を増やすことができます。詳細については、「ファイルシステムの SSD ストレージと IOPS の更新」を参照してください。

FSx for ONTAP では、次のストレージ容量のしきい値を使用してボリュームの階層化を管理します。

- SSD ストレージ階層の使用率が 50% 以下 — このしきい値では、SSD ストレージ階層は十分に活用されていないと見なされ、[All] (すべての) 階層化ポリシーを使用しているボリュームのみが容量プールストレージにデータを階層化しています。[Auto] (自動) ポリシーと [Snapshot-only] (Snapshot 専用) ポリシーが適用されているボリュームでは、このしきい値ではデータが階層化されません。
- SSD ストレージ階層の使用率が 50% を超える — [Auto] (自動) および [Snapshot-only] (Snapshot 専用) の階層化ポリシーが適用されたボリュームでは、階層化の最小冷却日数設定に基づいてデータが階層化されます。デフォルト設定は 31 日間。

- SSD ストレージ階層の使用率が 90% 以上 – このしきい値では、Amazon FSx は SSD ストレージ階層のスペース確保を優先します。[Auto] (自動) および [Snapshot-only] (Snapshot 専用) ポリシーを使用するボリュームを読み取る場合、容量プール階層のコールドデータが SSD ストレージ層に移動されなくなりました。
- SSD ストレージ階層の使用率が 98% 以上 – SSD ストレージ階層の使用率が 98% 以上になると、すべての階層化機能が停止します。ストレージ階層からの読み取りは引き続き可能ですが、階層への書き込みはできません。

スナップショットとボリュームストレージ容量

スナップショットは、特定の時点における Amazon FSx for NetApp ONTAP ボリュームの読み取り専用イメージです。スナップショットは、ボリューム内のファイルの間違った削除や変更からの保護を提供します。スナップショットで、ユーザーは以前のスナップショットから個々のファイルやフォルダを簡単に表示および復元できます。

スナップショットはファイルシステムのデータと一緒に保存されるため、ファイルシステムのストレージ容量が消費されます。ただし、スナップショットは、前回のスナップショット以降に変更されたファイルの部分に対してのみストレージ容量を消費します。スナップショットは、ファイルシステムボリュームのバックアップには含まれません。

スナップショットは、デフォルトのスナップショットポリシーを使用して、ボリューム上でデフォルトで有効になります。スナップショットはボリュームのルート内の `.snapshot` ディレクトリに保存されます。スナップショットのボリュームストレージ容量を管理できます。

- 「Snapshot policies」 (スナップショットポリシー) — 組み込みのスナップショットポリシーを選択するか、ONTAP CLI または REST API で作成したカスタムポリシーを選択します。
- 「Manually delete snapshots」(スナップショットの手動削除) — スナップショットを手動で削除してストレージ容量を再利用します。
- 「Create a snapshot autodelete policy」(スナップショット自動削除ポリシーの作成) — デフォルトのスナップショットポリシーよりも多くのスナップショットを削除するポリシーを作成します。
- 「Turn off automatic snapshots」(自動スナップショットをオフにする) — 自動スナップショットをオフにしてストレージ容量を節約します。

詳細については、「スナップショットの使用」を参照してください。

ボリュームファイル容量

Amazon FSx for NetApp ONTAP ボリュームには、ファイル名、最終アクセス時間、アクセス許可、サイズなどのファイルメタデータを保存し、データブロックへのポインタとして機能するファイルポインタがあります。これらのファイルポインタは inode と呼ばれ、各ボリュームには inode の数に対する有限の容量があり、これをボリュームファイル容量と呼びます。ボリュームの容量が少なくなったり、使用可能なファイル (inode) を使い果たしたりすると、そのボリュームに追加のデータを書き込むことはできません。

ボリュームに格納できるファイルシステムオブジェクト (ファイル、ディレクトリ、スナップショットコピー) の数は、その inode の数によって決まります。ボリューム内の inode の数は、ボリュームのストレージ容量 (および FlexGroup ボリュームの構成ボリューム数) に応じて増加します。デフォルトでは、648 GiB 以上のストレージ容量を持つ FlexVol ボリューム (または FlexGroup 構成要素) は、すべて同じ数 (21,251,126) の inode を持ちます。648 GiB を超えるボリュームを作成し、21,251,126 以上の inode ををを含める場合は、ボリューム上のファイルの最大数を手動で増やす必要があります。ボリュームの最大ファイル数の表示の詳細については、「」を参照してくださいボリュームのファイル容量を表示する。

ボリューム上の inode のデフォルトの数は、ボリュームストレージ容量の 32 KiB ごとに 1 つの inode で、ボリュームサイズは 648 GiB までとされています。1 GiB ボリュームの場合:

ボリュームサイズ (バイト単位)×(1 ファイル÷バイト単位の inode サイズ)=ファイルの最大数

1,073,741,824 バイト×(1 ファイル÷32,768 バイト)=32,768 ファイル

ボリュームに含めることができる inode の最大数は、ストレージ容量 4 KiB ごとに最大 1 つの inode まで増やすことができます。1 GiB ボリュームの場合、inode またはファイルの最大数が 32,768 から 262,144 に増加します:

1,073,741,824 バイト×(1 ファイル÷ 4096 バイト)=262,144 ファイル

FSx for ONTAP には、最大 20 億の inode を含めることができます。

ボリュームが保存できるファイルの最大数の変更については、「」を参照してくださいボリューム上の最大ファイル数を増やす。

ボリュームのストレージ容量の更新

ボリュームストレージ容量は、、、 API AWS Management Console、 AWS CLI および ONTAP CLI を使用して、ボリュームサイズを手動で増減することで管理できます。ボリュームの自動サイズ設定

を有効にすることで、使用済みストレージ容量のしきい値に達すると、ボリュームサイズが自動的に拡大または縮小されます。ONTAP CLI を使用してボリュームの自動サイズ設定を管理します。

ボリュームのストレージ容量を変更するには (コンソール)

- Amazon FSx コンソール、および API を使用して AWS CLI、ボリュームのストレージ容量を増減できます。詳細については、「ボリュームの更新」を参照してください。

CLI ONTAP を使用して、 volume modify コマンドを使用してボリュームのストレージ容量を変更することもできます。

ボリュームのサイズを変更するには (ONTAP CLI)

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. volume modify ONTAP CLI コマンドを使用して、ボリュームのストレージ容量を変更します。次の値の代わりにデータを使用して、次のコマンドを実行します。

   - *svm_name* をボリュームが作成されているストレージ仮想マシン (SVM) の名前に置き換えます。
   - を、サイズを変更するボリュームの名前*vol_name*に置き換えます。
   - *vol_size* を *integer*[KB|MB|GB|TB|PB] 形式のボリュームの新しいサイズに置き換えます。(例えば、ボリュームサイズを 100 ギガバイトに増やすには 100GB です)。

   ```
   ::> volume modify -vserver svm_name -volume vol_name -size vol_size
   ```

ボリュームの自動サイズ調整の有効化

ボリュームの自動サイズ調整により、使用済みスペースのしきい値に達すると、ボリュームが指定されたサイズに自動的に拡大されます。これは、volume autosizeONTAP CLI コマンドを使用して

FlexVol 、ボリュームタイプ (FSx for ONTAP のデフォルトのボリュームタイプ) に対して実行できます。

ボリュームの自動サイズ調整を有効にするには (ONTAP CLI)

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. 以下のように `volume autosize` コマンドを使用して、次の値を置き換えます。

   - *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
   - *vol_name* をサイズを変更するボリュームの名前に置き換えます。
   - *grow_threshold* を、ボリュームのサイズが自動的に引き上げられる (最大 *max_size* 値まで) 使用済みスペースのパーセンテージ値 (`90` など) に置き換えます。
   - *max_size* を、ボリュームを増やせる最大サイズに置き換えます。*integer*`[KB|MB|GB|TB|PB]` 形式を使用します。例えば、`300TB` です。最大サイズは 300 TB です。デフォルトはボリュームサイズの 120% です。
   - *min_size* をボリュームが縮小する最小サイズに置き換えます。*max_size* と同じ形式を使用してください。
   - *shrink_threshold* は使用済みスペースのパーセンテージに置き換えます。このパーセンテージに達すると、ボリュームのサイズが自動的に縮小されます。

   ```
   ::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
   grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
   percent shrink_threshold -minimum-size min_size
   ```

ボリュームストレージ容量のモニタリング

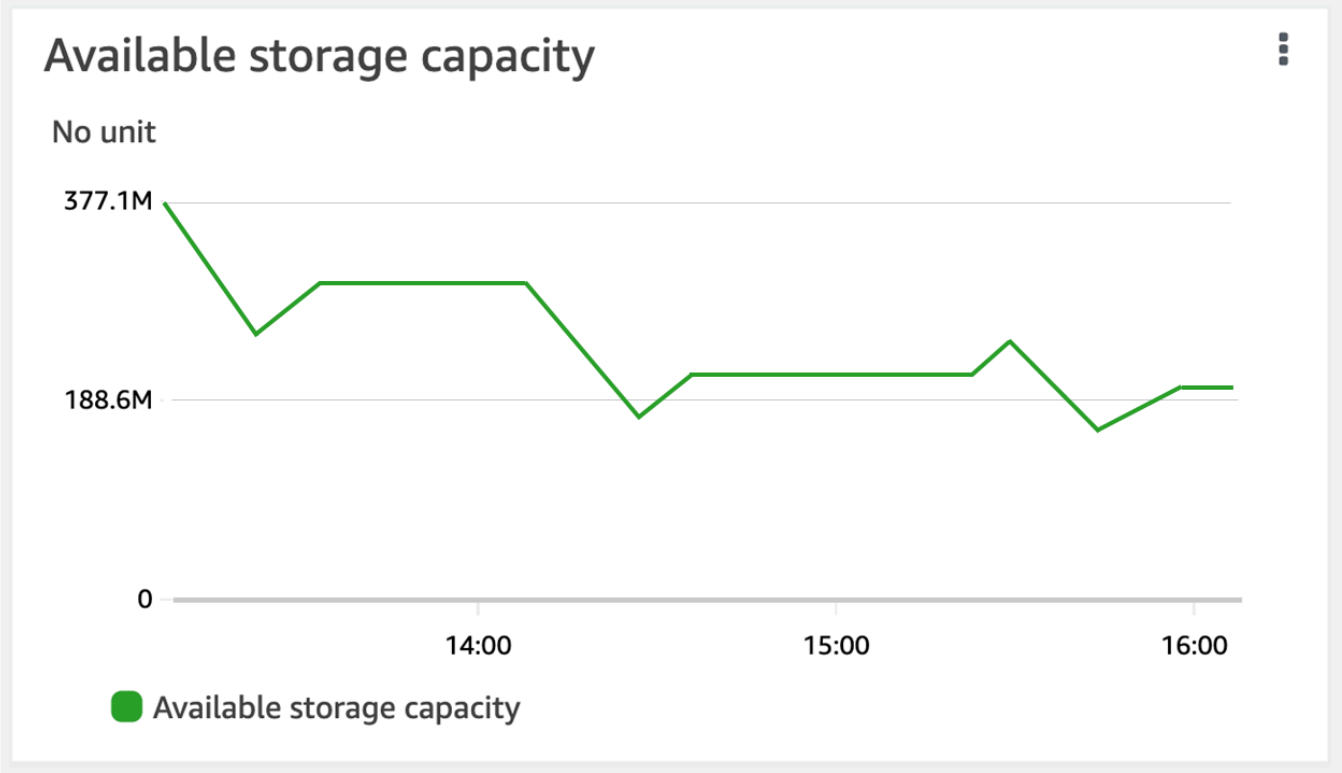
ボリュームの使用可能なストレージとそのストレージディストリビューションは AWS Management Console、、 AWS CLIおよび NetApp ONTAP CLI で表示できます。

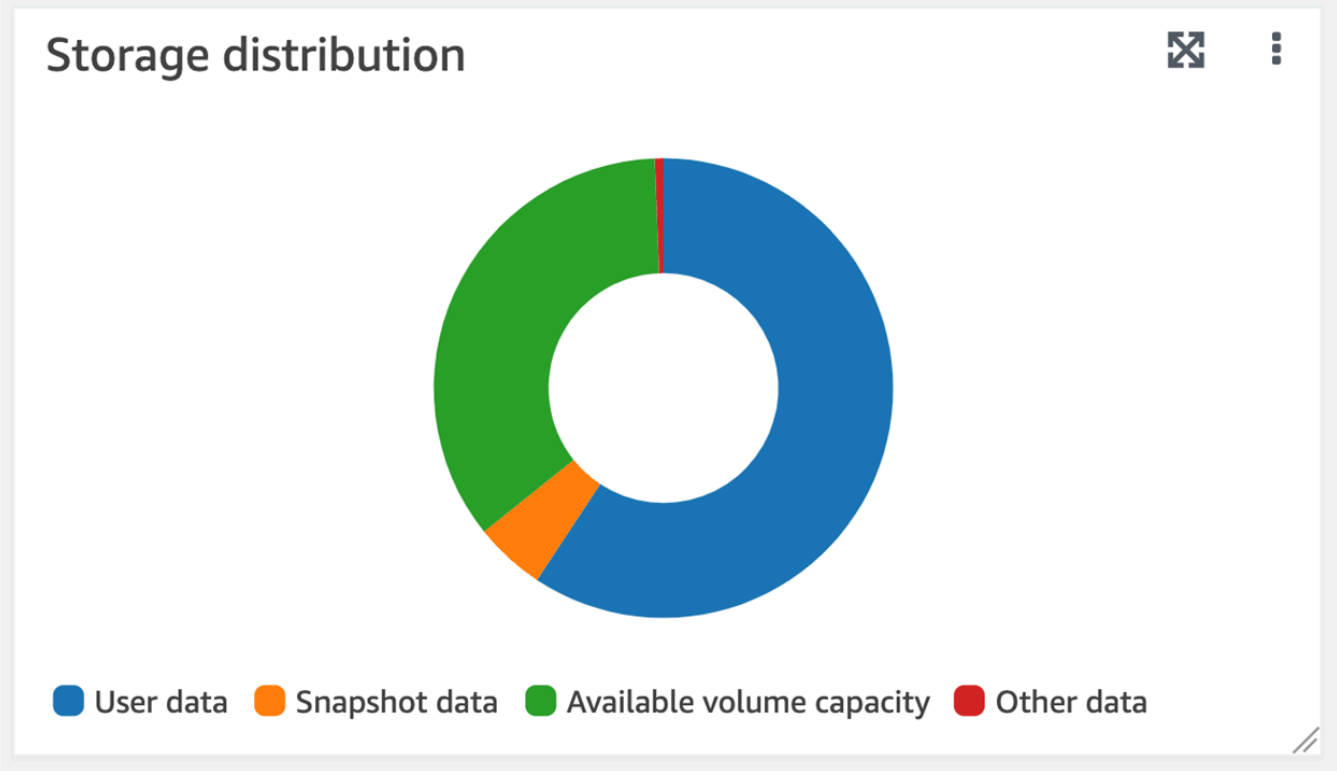
ボリュームのストレージ容量をモニタリングするには (コンソール)

[Available Storage] (使用可能なストレージ) グラフには、ボリュームの空きストレージ容量が時系列で表示されます。[Storage distribution] (ストレージ分布) グラフには、ボリュームのストレージ容量が現在 4 つのカテゴリにどのように分布しているかが表示されます。

- ユーザーデータ
- スナップショットデータ
- 使用可能なボリューム容量
- その他のデータ

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーション列で [Volumes] (ボリューム) を選択し、ストレージ容量情報を表示する ONTAP ボリュームを選択します。ボリュームの詳細ページが表示されます。
3. 2 つ目のパネルで、[Monitoring] (モニタリング) タブを選択します。[Available storage] (使用可能なストレージ) と [Storage distribution] (ストレージ分布) のグラフが、他のいくつかのグラフとともに表示されます。





ボリュームのストレージ容量をモニタリングするには (ONTAP CLI)

`volume show-space` ONTAP CLI コマンドを使用して、ボリュームのストレージ容量の消費状況をモニタリングできます。詳細については、 NetApp ONTAPドキュメントセンター`volume show-space`の「」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. 次のコマンドを実行し、ボリュームのストレージ容量使用量を表示します。

   - *`svm_name`* をボリュームが作成されている SVM の名前に置き換えます。
   - *`vol_name`* を、データ階層化ポリシーを設定するボリュームの名前に置き換えます。

```
::> volume show-space -vserver svm_name -volume vol_name
```

コマンドが成功した場合は、以下のような出力が表示されます。

```
Vserver : svm_name
Volume  : vol_name
Feature                                     Used      Used%
--------------------------------     ----------     ------
User Data                                  140KB         0%
Filesystem Metadata                      164.4MB         1%
Inodes                                   10.28MB         0%
Snapshot Reserve                         563.2MB         5%
Deduplication                              12KB         0%
Snapshot Spill                           9.31GB        85%
Performance Metadata                       668KB         0%

Total Used                               10.03GB        91%

Total Physical Used                      10.03GB        91%
```

このコマンドの出力には、このボリュームで異なるタイプのデータが占める物理領域の量が表示されます。また、各タイプのデータが消費する総ボリューム容量の割合も表示されます。この例では、Snapshot Spill および Snapshot Reserve がボリュームの容量の 合計 90% を消費します。

Snapshot Reserve は、スナップショットコピーの保存用に確保されているディスク容量を表示します。スナップショットコピーのストレージがリザーブスペースを超えると、ファイルシステムにオーバーフローし、この量が Snapshot Spill の下に表示されます。

使用可能な領域を増やすには、次の手順に示すように、ボリュームのサイズを大きくするか、使用していないスナップショットを削除します。

FlexVol ボリュームタイプ (FSx for ONTAP ボリュームのデフォルトのボリュームタイプ) では、ボリュームの自動サイズ設定を有効にすることもできます。自動サイズ調整を有効にすると、特定のしきい値に達した場合にボリュームサイズが自動的に増加します。自動スナップショットを無効化することもできます。これらの機能については、以降のセクションで説明します。

ボリュームの階層化ポリシーの設定

ボリュームの階層化ポリシーは AWS Management Console、、 AWS CLI 、 API、および ONTAP CLI を使用して変更できます。

ボリュームのデータ階層化ポリシーを変更するには (コンソール)

次の手順に従って、 AWS Management Consoleを使用して、ボリュームのデータ階層化ポリシーを変更します。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーションペインで [Volumes] (ボリューム) を選択し、データ階層化ポリシーを変更する ONTAP ボリュームを選択します。
3. [Actions] (アクション) ドロップダウンメニューから、[Update volume] (ボリュームの更新) を選択します。[Update volume] (ボリュームの更新) ウィンドウが表示されます。
4. [Capacity pool tiering policy] (容量プールの階層化ポリシー) では、ボリュームの新しいポリシーを選択します。詳細については、「ボリューム階層化ポリシー」を参照してください。
5. [Update] (更新) を選択して、新しいポリシーをボリュームに適用します。

ボリュームの階層化ポリシーを設定するには (CLI)

- update-volume CLI コマンドを使用してボリュームの階層化ポリシーを変更します (UpdateVolume は同等の Amazon FSx API アクションです)。次の CLI コマンド例では、ボリュームのデータ階層化ポリシーを SNAPSHOT_ONLY に設定します。

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

リクエストが成功すると、システムはボリュームの説明を応答します。

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
```

```
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

ボリュームの階層化ポリシーを変更するには (ONTAP CLI)

`volume modify` ONTAP CLI コマンドを使用して、ボリュームの階層化ポリシーを設定します。詳細については、 NetApp ONTAP ドキュメントセンター`volume modify`の「」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. 次のコマンドを使用して ONTAP CLI アドバンスドモードを開始します。

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   ```

```
Do you want to continue? {y|n}: y
```

3. 次のコマンドを使用して、ボリュームデータ階層化のポリシーを変更します。

   - *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
   - *vol_name* を、データ階層化ポリシーを設定するボリュームの名前に置き換えます。
   - *tiering_policy* を、目的のポリシーに置き換えます。有効な値は snapshot-only、auto、all、または none です。詳細については、「ボリューム階層化ポリシー」を参照してください。

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
policy tiering_policy
```

最低冷却日数の設定

ボリュームの最小冷却日数は、どのデータがワームで、どのデータがコールドかを決定するための閾値を設定します。ボリュームの最小冷却日数は、 AWS CLI と API、および ONTAP CLI を使用して設定できます。

ボリュームの最小冷却日数を設定するには (CLI)

- update-volume CLI コマンドを使用してボリューム設定を変更します (UpdateVolume は同等の Amazon FSx API アクションです)。次の CLI コマンド例では、ボリュームの CoolingPeriod を 104 日に設定しています。

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

システムは、リクエストが成功すると、ボリュームの説明を応答します。

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
```

```
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

ボリュームの最小冷却日数を設定するには (ONTAP CLI)

`volume modify` ONTAP CLI コマンドを使用して、既存のボリュームの最小冷却日数を設定します。詳細については、 NetApp ONTAP ドキュメントセンター`volume modify`の「」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. 次のコマンドを使用して ONTAP CLI アドバンスドモードを開始します。

```
FSx::> set adv

Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. 次のコマンドを使用して、ボリュームの階層化の最小冷却日数を変更します。

   - *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
   - *vol_name* を、冷房日数を設定するボリュームの名前に置き換えてください。
   - *cooling_days* を、希望する 2～183 の整数に置き換えます。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
   days cooling_days
   ```

   リクエストが成功すると、システムは次のように応答します。

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

ボリュームのクラウド検索ポリシーの設定

volume modify ONTAP CLI コマンドを使用して、既存のボリュームのクラウド検索ポリシーを設定します。詳細については、 NetApp ONTAP ドキュメントセンターvolume modifyの「」を参照してください。

ボリュームのクラウド検索ポリシーを設定するには (ONTAP CLI)

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. 次のコマンドを使用して ONTAP CLI アドバンスドモードを開始します。

```
FSx::> set adv

Warning: These advanced commands are potentially dangerous; use them only when
     directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. 次のコマンドを使用して、ボリュームのクラウド検索ポリシーを設定します。

   - *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
   - *vol_name* を、クラウド検索ポリシーを設定するボリュームの名前に置き換えてください。
   - *retrieval_policy* を、default、on-read、never または promote のいずれか希望の値に置き換えます。

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
policy retrieval_policy
```

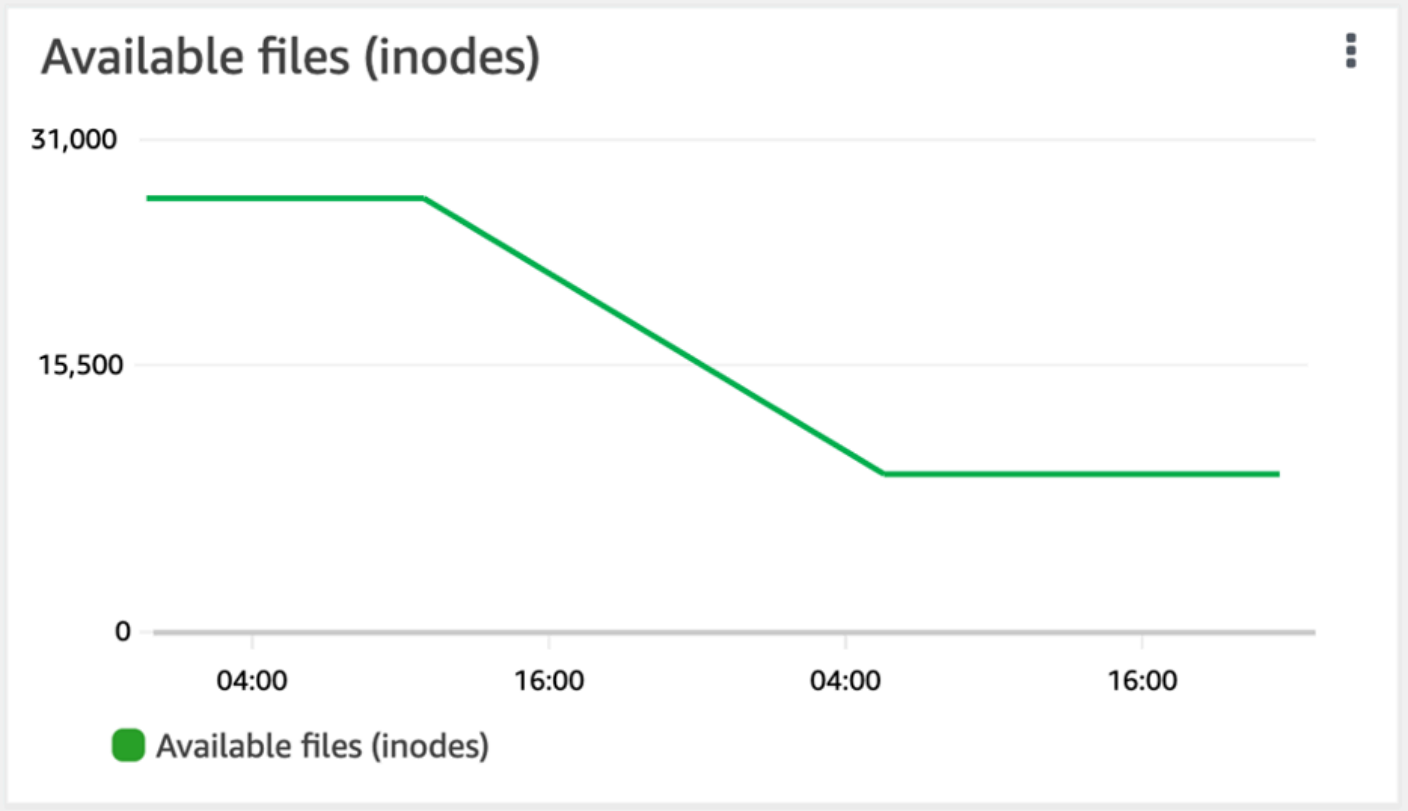
   リクエストが成功すると、システムは次のように応答します。

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

ボリュームのファイル容量を表示する

次のいずれかの方法を使用すると、ボリュームで許可されているファイルの最大数と、既に使用されているファイルの数を表示できます。

- CloudWatch ボリュームメトリクス FilesCapacityおよび FilesUsed。
- Amazon FSx コンソールで、ボリュームの[Monitoring] (モニタリング) タブにある [Available files (inodes)] (使用可能なファイル (inode)) チャートに移動します。次の画像は、時間の経過とともに減少するボリューム上の [Available files (inodes)] (使用可能なファイル (inode)) を示しています。



ボリューム上の最大ファイル数を増やす

FSx for ONTAP ボリュームは、使用可能な inode またはファイルポインタの数を使い切ると、ファイル容量が足りなくなることがあります。

ボリューム上のファイルの最大数を増やすには (ONTAP CLI)

`volume modify` ONTAP CLI コマンドを使用して、ボリューム上のファイルの最大数を増やします。詳細については、 NetApp ONTAPドキュメントセンターの`volume modify`「」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. ユースケースに応じて、以下のいずれかを実行します。*svm_name* および *vol_name* を実際の値に置き換えます。

   - 使用可能なファイル (inode) が常に最大数になるようにボリュームを設定するには、次の手順を実行します。

     1. 次のコマンドを使用して ONTAP CLI でアドバンストモードを開始します。

        ```
        ::> set adv
        ```

     2. このコマンドを実行すると、この出力が表示されます。y を入力して続行します。

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. ボリューム上のファイルの最大数を常に使用するには、次のコマンドを入力します。

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - ボリュームで許可されるファイルの総数を *max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB) を使用して手動で指定するには、使用可能な最大値である 20 億まで次のコマンドを使用します。

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

ボリュームのクラウド書き込みモードの有効化

volume modify ONTAP CLI コマンドを使用して、既存のボリュームのクラウド書き込みモードを有効または無効にします。詳細については、 NetApp ONTAP ドキュメントセンターvolume modifyの「」を参照してください。

クラウド書き込みモードを設定するための前提条件は次のとおりです。

- ボリュームは既存のボリュームである必要があります。この機能は、既存のボリュームでのみ有効にできます。

- ボリュームは読み取り/書き込み (RW) ボリュームである必要があります。
- ボリュームには、すべての階層化ポリシーが必要です。ボリュームの階層化ポリシーの変更の詳細については、「」を参照してくださいボリュームの階層化ポリシーの設定。

クラウド書き込みモードは、NFS プロトコルを使用して大量のデータがファイルシステムに転送される移行などに役立ちます。

ボリュームのクラウド書き込みモードを設定するには (ONTAP CLI)

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. 次のコマンドを使用して ONTAP CLI アドバンスドモードを開始します。

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. 次のコマンドを使用して、ボリュームのクラウド書き込みモードを設定し、次の値を置き換えます。

   - *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
   - を、クラウド書き込みモードを設定するボリュームの名前*vol_name*に置き換えます。
   - ボリュームでクラウド書き込みモードtrueを有効にするか、無効にfalseするには、 を*vol_cw_mode*に置き換えます。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   リクエストが成功すると、システムは次のように応答します。

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

データの保護

Amazon FSxは、ファイルシステムのデータを自動的にレプリケーションして高い耐久性を確保するだけでなく、ファイルシステムに保存されているデータを、さらに保護するための以下のオプションが提供されています:

- Amazon FSx のネイティブバックアップは、Amazon FSx 内のバックアップ保持およびコンプライアンスのニーズをサポートします。 AWS Backup を使用して、クラウド内の 全体の AWS のサービス バックアップを一元管理、自動化、保護することもできます。
- スナップショットは、ユーザーがファイルを以前のバージョンに復元することで、ファイルの変更を元に戻したり、ファイルのバージョンを比較したりすることを有効にします。
- 2 番目のファイルシステムに Amazon FSx ファイルシステムをレプリケーションすることで、データの保護とリカバリーが行われます。レプリケーションは、有効にすると、スケジュールに沿って自動的に実行されます。
- SnapLock は、ファイルを WORM (Write Once, Read Many) に移行することでファイルを保護します。これにより、指定した保存期間中のファイルの変更や削除を防ぐことができます。

トピック

バックアップの使用

FSx for ONTAP を使用すると、ファイルシステム上のボリュームの日次自動バックアップとユーザー開始バックアップを作成できます。FSx for ONTAP バックアップはボリューム単位で行われるため、各バックアップには特定のボリュームのデータのみが含まれます。Amazon FSx バックアップは、高い耐久性、増分的です。

Amazon FSx バックアップ (自動日次バックアップとユーザー開始バックアップ) はすべて増分バックアップです。つまり、最新のバックアップを実行した時点から、ボリューム上で変更のあるデータのみが保存されます。これにより、バックアップの作成に必要な時間とバックアップに必要なストレージが最小限に抑えられ、データが重複しないためストレージコストを節約できます。バックアッ

プを削除すると、そのバックアップに固有のデータのみが削除されます。Amazon FSx の各バックアップには、バックアップから新しいボリュームを作成するのに必要な情報がすべて含まれており、point-in-time ファイルシステムボリュームのスナップショットを効果的に復元できます。

ボリュームの定期的なバックアップを作成することは、データ保持とコンプライアンスのニーズを満たすのに役立つベストプラクティスです。Amazon FSx バックアップの操作は、バックアップの作成、バックアップからの復元、またはバックアップの削除のいずれであっても、簡単です。

Amazon FSx は、ONTAPFlexVolボリューム (すべてのファイルシステム上) と `OntapVolumeType` of `RW` (読み取り/書き込み) FlexGroup によるボリュームのバックアップをサポートしています。

> **Note**
>
> Amazon FSx は、データ保護 (DP) ボリューム、負荷分散 (LS) ボリューム、またはデスティネーションボリュームのバックアップをサポートしていません。FlexCache

ファイルシステム 1 つおよびボリュームごとに保存できるバックアップの数には制限があります。詳細については、「増やすことができるクォータ」および「ファイルシステムあたりのリソースクォータ」を参照してください。

トピック

- バックアップの仕組み
- ストレージの要件
- 自動の日次バックアップの操作
- ユーザー主導のバックアップ機能
- バックアップへのタグのコピー
- Backup とリストアのパフォーマンス
- Amazon AWS Backup FSx との併用
- バックアップを新しいボリュームに復元する
- バックアップの削除
- バックアップとオフラインボリューム
- ユーザー主導のバックアップの作成
- バックアップを新しいボリュームに復元する。
- バックアップの削除

バックアップの仕組み

Amazon FSx point-in-time バックアップでは、スナップショット (ボリュームの読み取り専用イメージ) を使用してバックアップ間の増分を維持します。バックアップを作成するたびに、Amazon FSx はまずボリュームのスナップショットを取ります。バックアップスナップショットはボリュームに保存され、SSD ストレージ層の容量を消費します。次に、Amazon FSx は、このスナップショットを以前のバックアップスナップショット (存在する場合) と比較し、変更されたデータのみをバックアップにコピーします。

以前のバックアップスナップショットが存在しない場合は、最新のバックアップスナップショットの内容全体がバックアップにコピーされます。最新のバックアップスナップショットが正常に作成されると、Amazon FSx は以前のバックアップスナップショットを削除します。プロセスが繰り返される場合、最新のバックアップに使用されたスナップショットは、次のバックアップが作成されるまで、ボリュームに残ります。バックアップストレージコストを最適化するために、ONTAPボリュームのストレージ効率の節約分をバックアップ時に維持します。

Amazon FSx はオフラインのボリュームをバックアップできません。

ストレージの要件

ボリュームのバックアップを取るには、ボリュームとファイルシステムの両方に、バックアップスナップショットを保存するのに十分な SSD ストレージ容量が必要です。バックアップスナップショットを作成する場合、そのスナップショットによって消費される追加のストレージ容量によって、ボリュームの SSD ストレージ使用率が 98% を超えてはなりません。この場合、バックアップは失敗します。バックアップが中断されないように、ボリュームまたはファイルシステムの SSD ストレージをいつでも増やすことができます。

自動の日次バックアップの操作

ファイルシステムを作成すると、ファイルシステムのボリュームの自動日次バックアップはデフォルトで有効になっています。ファイルシステムの自動日次バックアップはいつでも有効または無効にできます。自動日次バックアップは、ファイルシステムの作成時に自動的に設定される日次バックアップウィンドウ中に行われます。日次バックアップウィンドウはいつでも変更できます。バックアップパフォーマンスを向上させるために、ボリュームを使用するアプリケーションの通常の営業時間外に、毎日のバックアップを行う時間帯を選択することをお勧めします。詳細については、「Backup とリストアのパフォーマンス」を参照してください。

ファイルシステムの作成時またはいつでも、コンソールで毎日の自動バックアップの保持期間を 1 日から 90 日の間で設定できます。デフォルトの日次自動バックアップ保持期間は 30 日間です。保

存期間が終了すると、サービスは自動日次バックアップを削除します。CLI または API を使用して、保持期間を 0 ~ 90 日の間で設定できます。0 に設定すると、毎日の自動バックアップが無効になります。

日次バックアップウィンドウとバックアップ保持期間は、ファイルシステム上のすべてのボリュームに適用されるファイルシステムレベルの設定です。Amazon FSx コンソール、、または API を使用して AWS CLI、ファイルシステムのバックアップウィンドウとバックアップ保持期間を変更したり、毎日の自動バックアップをオンまたはオフにしたりできます。詳細については、「ファイルシステムの更新」を参照してください。

ボリュームがオフラインの場合、ボリュームバックアップは作成できません。詳細については、「バックアップとオフラインボリューム」を参照してください。

> **Note**
>
> 毎日の自動バックアップの最大保存期間は 90 日ですが、AWS Backupを使用して作成されたバックアップを含め、ユーザーが作成したバックアップは、 AWS Backup ユーザーまたはサービスが削除しない限り永久に保持されます。

コンソール、CLI、および API を使用して、自動日次バックアップを手動で削除できます。ボリュームを削除すると、そのボリュームの日次自動バックアップも削除されます。Amazon FSx には、ボリュームを削除する前に最終バックアップを作成するオプションが用意されています。最終バックアップは、削除しない限り永久に保持されます。詳細については、を参照してくださいバックアップの削除。

ユーザー主導のバックアップ機能

Amazon FSx では、、および API を使用して AWS Management Console AWS CLI、いつでもファイルシステムのボリュームを手動でバックアップできます。ユーザー主導のバックアップは、ボリュームに対して作成された他のバックアップと比較すると増分的で、ユーザーが削除しない限り、永続的に保持されます。ユーザー主導のバックアップは、バックアップが作成されたボリュームまたはファイルシステムを削除した後でも保持されます。ユーザーが作成したバックアップは、Amazon FSx コンソール、API、または CLI を使用してのみ削除できます。Amazon FSx によって自動的に削除されることはありません。詳細については、「バックアップの削除」を参照してください。

ボリュームがオフラインの場合、ボリュームバックアップは作成できません。詳細については、「バックアップとオフラインボリューム」を参照してください。

バックアップへのタグのコピー

CLI または API を使用してボリュームを作成または更新すると、CopyTagsToBackupsボリュームのタグをそのバックアップに自動的にコピーできます。ただし、コンソールを使用するときにバックアップに名前を付けるなど、ユーザーが開始するバックアップの作成中にタグを追加した場合CopyTagsToBackups、サービスは有効になっていてもボリュームからタグをコピーしません。

Backup とリストアのパフォーマンス

バックアップと復元操作のパフォーマンスには、さまざまな要因が影響します。Backup とリストア操作はバックグラウンドプロセスであるため、クライアント IO 操作に比べて優先順位が低くなります。クライアント IO 操作には、NFS、CIFS、iSCSI データの読み取りと書き込みが含まれます。バックアップや復元操作を含むすべてのバックグラウンドプロセスは、ファイルシステムのスループット容量の未使用部分のみを使用し、バックアップのサイズとファイルシステム上の未使用のスループット容量によっては、完了するまでに数分から数時間かかる場合があります。

バックアップと復元のパフォーマンスに影響するその他の要因には、データが保存されているストレージ階層やデータセットプロファイルがあります。データの大部分が SSD ストレージにあるときに、ボリュームの最初のバックアップを作成することをお勧めします。大部分が小さいファイルを含むデータセットは、大部分が大きなファイルを含む同じサイズのデータセットと比べると、通常はパフォーマンスが低下します。これは、小さなファイルを多数処理するほうが、大きなファイルを少数処理するよりも、CPU サイクルとネットワークオーバーヘッドを多く消費するためです。

一般に、SSD ストレージ層に保存されているデータをバックアップする場合、次のバックアップ速度が期待できます。

- 大きなファイルが大部分を占める複数の同時バックアップで 750 MBps。
- 小さなファイルが大部分を占める複数の同時バックアップで 100 Mbps。

一般に、次の復元速度が期待できます。

- 大きなファイルが大部分を占める複数の同時復元で 250 MBps。
- 小さなファイルが大部分を占める複数の同時復元で 100 MBps。

Amazon AWS Backup FSx との併用

AWS Backup は、Amazon FSx for NetApp ONTAP ボリュームをバックアップすることでデータを保護するシンプルで費用対効果の高い方法です。 AWS Backup は、バックアップの作成、復元、削除

を簡素化すると同時に、レポートと監査を強化するように設計された統合バックアップサービスです。 AWS Backup 法律、規制、職業上のコンプライアンスに対応するための一元的なバックアップ戦略を簡単に策定できます。 AWS Backup また、次のことを一元的に行えるため、 AWS ストレージボリューム、データベース、ファイルシステムの保護がより簡単になります。

- AWS バックアップするリソースの設定と監査を行います。
- バックアップのスケジューリングの自動化。
- 保持ポリシーの設定。
- 最近のすべてのバックアップ、コピー、および復元アクティビティのモニタリング。

AWS Backup Amazon FSx の組み込みバックアップ機能を使用します。 AWS Backup コンソールを使用して作成されたバックアップは、ファイルシステムの一貫性とパフォーマンスが同じレベルで、ボリュームから取得する他の Amazon FSx バックアップ (ユーザー開始または自動) と比較して段階的にバックアップされ、Amazon FSx コンソールから作成されたバックアップと同じ復元オプションを提供します。 AWS Backup を使用してこれらのバックアップを管理すると、1 時間ごとにスケジュールされたバックアップを作成できるなど、追加機能を利用できるようになります。バックアップをVaultに保存することで、バックアップを不注意や悪意による削除から保護する防御を強化できます。 AWS Backup

AWS Backup によって作成されたバックアップはユーザー開始バックアップと見なされ、Amazon FSx のユーザー開始バックアップクォータにカウントされます。詳細については、「増やすことができるクォータ」を参照してください。Amazon FSx コンソール、CLI、および API AWS Backup で作成したバックアップを表示および復元できます。ただし、Amazon FSx コンソール、CLI、または API AWS Backup で作成されたバックアップは削除できません。詳細については、『AWS Backup 開発者ガイド』の「AWS Backupはじめに」を参照してください。

AWS Backup オフラインのボリュームはバックアップできません。

バックアップを新しいボリュームに復元する

ボリュームバックアップを新しいボリュームに復元し、コンソール、CLI、または API point-in-time を使用してボリュームのスナップショットを効果的に復元できます。。

バックアップを復元すると、サービスが復元されたボリュームに設定した階層化ポリシーに従って容量プールストレージへのデータの階層化を開始する前に、すべてのデータが最初に SSD ストレージ階層に書き込まれます。階層化ポリシー `All` を使用してボリュームにバックアップを復元すると、定期的なバックグラウンドプロセスによってデータが容量プールに階層化されます。階層化ポリシー

Snapshot Only または Auto を使用してボリュームにバックアップを復元する場合、ファイルシステムの SSD 使用率が 50% を超えると、データは容量プールに階層化されますが、冷却速度は階層化ポリシーの冷却期間によって決まります。

元のファイルシステムとは異なる数の高可用性 (HA) ペアを持つファイルシステムで FlexGroup ボリュームバックアップを復元する場合、Amazon FSx は、構成要素が均等に分散されるように、構成ボリュームを追加する場合があります。

step-by-step バックアップを新しいボリュームに復元する手順については、を参照してください。バックアップを新しいボリュームに復元する。

> **Note**
>
> 復元されたボリュームは、常に元のボリュームと同じボリュームスタイルになります。復元時にボリュームスタイルを変更することはできません。

バックアップの削除

ボリュームの日次自動バックアップとユーザーが開始したバックアップは削除できます。バックアップの削除は、永久的で回復不能なアクションです。削除されたバックアップ内のデータもすべて削除されます。今後そのバックアップが必要でないということが確かでない限り、バックアップを削除しないでください。バックアップを削除する方法の説明については、を参照してください。バックアップの削除

Amazon FSx コンソール、CLI AWS Backup、または API で作成されたAWS Backup、タイプ付きのバックアップは削除できません。で作成したバックアップの削除については AWS Backup、『 AWS Backup 開発者ガイド』の「バックアップの削除」を参照してください。

ボリュームがオフラインの場合、そのボリュームのバックアップは削除できません。詳細については、「バックアップとオフラインボリューム」を参照してください。

> **Important**
>
> ボリューム上の共通スナップショットは、バックアップ間の増分を維持するために使用されるため、削除しないでください。ボリューム上の共通スナップショットを削除すると、次回のバックアップは単なる増分バックアップではなく、ボリューム全体のバックアップになります。

バックアップとオフラインボリューム

ボリュームがオフラインの場合、ボリュームバックアップを作成または削除することはできません。volume showONTAPCLI コマンドを使用して、ボリュームの現在の状態とステータスを確認します。

オフラインのボリュームをオンラインに戻すには、次の例のように volume onlineONTAPCLI コマンドを使用します。

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

ユーザー主導のバックアップの作成

以下の手順では、Amazon FSx コンソールを使用して、ユーザーが開始するボリュームのバックアップを作成する方法について説明します。

ボリュームがオフラインの場合、ボリュームバックアップは作成できません。詳細については、「バックアップとオフラインボリューム」を参照してください。

ユーザーが開始するボリュームのバックアップを作成するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [ファイルシステム] に移動し、ONTAPボリュームをバックアップしたいファイルシステムを選択します。
3. ボリュームタブを選択します。
4. バックアップするボリュームを選択します。
5. [Actions] (アクション) で、[Create backup] (バックアップの作成) を選択します。
6. [Create backup] (バックアップの作成) ダイアログボックスが表示されますので、バックアップ名を入力します。バックアップ名は、英字、空白、数字、特殊文字. + - = _ : / を含む最大 256 の Unicode 文字を使用できます。
7. [Create backup] (バックアップを作成) を選択します。

これで、ファイルシステムのボリュームの 1 つのバックアップが作成されました。左側のナビゲーションで、[Backups] (バックアップ を選択すると、Amazon FSx コンソールにすべてのバックアッ

プの表を見つけることができます。バックアップに付けた名前と、一致する結果のみを表示するようにテーブルフィルターを検索できます。

この手順で説明したようにユーザーが開始するバックアップを作成すると、タイプは `USER_INITIATED` になり、完全に使用可能になるまで `CREATING` ステータスになります。

バックアップを新しいボリュームに復元する。

以下の手順では、とを使用して FSx for ONTAP バックアップを新しいボリュームにリストアする方法について説明します。 AWS Management Console AWS CLI

ボリュームバックアップを新しいボリュームにリストアするには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ナビゲーションペインで、[バックアップ] を選択して、復元する FSx for ONTAP ボリュームバックアップを選択します。
3. 右上の [アクション] メニューで、[バックアップの復元] を選択します。[バックアップからボリュームを作成] ページが表示されます。
4. ドロップダウンメニューから、バックアップの復元先となる FSx for ONTAP ファイルシステムとストレージ仮想マシンを選択します。
5. [ボリュームの詳細] には、いくつかの選択肢があります。まず、[ボリューム名] に入力します。英数字とアンダースコア (_) で最大 203 文字まで使用できます。
6. [ボリュームサイズ] に、20～314572800 の範囲で任意の整数を入力し、サイズをメビバイト (MiB) 単位で指定します。
7. [ボリュームタイプ] では、読み取りと書き込みが可能なボリュームを作成するには [Read-Write (RW)] を選択し、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用できる読み取り専用のボリュームを作成するには [Data Protection (DP)] を選択します。詳細については、「ボリュームの種類」を参照してください。
8. [Junction path] (ジャンクションパス) で、ボリュームをマウントするファイルシステム内の場所を入力します。`/vol3` のように、名前の先頭にスラッシュを付ける必要があります。
9. ストレージ効率を高めるには、「有効」ONTAP を選択してストレージ効率化機能 (重複排除、圧縮、圧縮) を有効にします。詳細については、「FSx for ONTAP ストレージの効率化」を参照してください。
10. [ボリュームのセキュリティスタイル] には、[UNIX (Linux)]、[NTFS]、または [混合] のいずれかを選択します。ボリュームのセキュリティスタイルによって、マルチプロトコルアクセスで

NTFS ACL と UNIX ACL のどちらを優先するかが決まります。MIXED モードはマルチプロトコルアクセスには必要なく、上級ユーザーにのみ推奨されます。

11. [Snapshot policy] (スナップショットポリシー) で、ボリュームのスナップショットポリシーを選択します。スナップショットポリシーの詳細については、スナップショットポリシー を参照してください。

    [Custom policy] (カスタムポリシー) を選択した場合は、[custom-policy] (カスタムポリシー) フィールドにポリシーの名前を指定する必要があります。カスタムポリシーは SVM またはファイルシステムにすでに存在している必要があります。ONTAPCLI または REST API を使用してカスタムスナップショットポリシーを作成できます。詳細については、NetApp ONTAP製品ドキュメントの「スナップショットポリシーの作成」を参照してください。

12. [階層化ポリシーの冷却期間] の有効値は 2 ~ 183 日です。ボリュームの階層化ポリシーの冷却期間は、アクセスされていないデータがコールドとしてマークされ、容量プールストレージに移動されるまでの日数を定義します。この設定は `Auto` ポリシーと `Snapshot-only` ポリシーにのみ影響します。

13. 「SnapLock詳細設定」セクションの「設定」では、デフォルトの「無効」設定のままにするか、「有効」SnapLock を選択してボリュームを設定できます。SnapLock Complianceボリュームまたはボリュームの設定について詳しくは、「」SnapLock Compliance ボリュームの作成 と「」を参照してくださいSnapLock Enterprise ボリュームの作成。SnapLock EnterpriseSnapLock の詳細については、「によるデータの保護 SnapLock」を参照してください。

14. [確認] を選択してボリュームを作成します。

ボリュームバックアップを新しいボリュームに復元するには (CLI)

create-volume-from-backupCLI コマンドまたは同等の CreateVolumeFromBackupAPI コマンドを使用して、ボリュームバックアップを新しいボリュームに復元します。

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```

  リクエストが成功した場合のシステム応答は次のとおりです。

  ```
  {
        "Volume": {
  ```
  ```

```
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",

        }
    }
```


バックアップの削除

以下の手順で説明するように、Amazon FSx コンソール、CLI、および API を使用して、自動日次バックアップとユーザー開始バックアップを削除できます。

を使用して作成したバックアップを削除するには AWS Backup、『開発者ガイド』の「AWS Backup バックアップの削除」を参照してください。

バックアップを削除するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. コンソールダッシュボードで、左側のナビゲーションから [Backups] (バックアップ) を選択します。
3. [Backups] (バックアップ) テーブルから削除するバックアップを選択してから、[Delete backup] (バックアップの 削除) を選択します。

4. 開いた Delete backups ダイアログボックスで、表示されているバックアップの ID が削除するバックアップであることを確認します。
5. 削除するバックアップのチェックボックスがチェックされていることを確認します。
6. バックアップの削除を選択します。

バックアップとそれに含まれるすべてのデータが恒久的に、回復不能な形で削除されます。

バックアップを削除するには (CLI)

- 次の例に示すように、delete-backup CLI DeleteBackup コマンドまたは同等の API アクションを使用して、ONTAP ボリュームバックアップ用の FSx を削除します。

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

システムレスポンスには、削除されるバックアップの ID とライフサイクルステータスが含まれており、DELETEDリクエストが成功したことが示されます。

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

スナップショットの使用

スナップショットは、特定の時点における Amazon FSx for NetApp ONTAP ボリュームの読み取り専用イメージです。スナップショットは、ボリューム内のファイルの間違った削除や変更からの保護を提供します。スナップショットを使用すると、ユーザーは以前のスナップショットから個々のファイルまたはフォルダを簡単に表示および復元して、変更を元に戻したり、削除されたコンテンツを復元したり、ファイルバージョンを比較したりできます。

スナップショットには、ファイルシステムの SSD ストレージ容量を消費する最後のスナップショット以降に変更されたデータが含まれます。スナップショットは、ボリュームバックアップ には含まれていません。スナップショットは、スナップショットdefaultポリシーを使用してボリュームでデフォルトで有効になっています。スナップショットはボリュームのルート内の .snapshot ディレクトリに保存されます。ボリュームごとに最大 1,023 個のスナップショットを任意の時点で保存できます。この制限に達したら、ボリュームの新しいスナップショットを作成する前に、既存のスナップショットを削除する必要があります。

トピック

スナップショットポリシー

スナップショットポリシーは、システムがボリュームのスナップショットを作成する方法を定義します。ポリシーは、スナップショットを作成する時期、保持するコピーの数、および命名方法を指定します。FSx for ONTAP には、次の 3 つの基本的なスナップショットポリシーがあります:

- `default`
- `default-1weekly`
- `none`

デフォルトで、すべてのボリュームはファイルシステムの `default` スナップショットポリシーに関連付けられます。ほとんどのワークロードでは、このポリシーを使用することを推奨します。

`default` ポリシーは、次のスケジュールでスナップショットを自動的に作成し、最も古いスナップショットコピーを削除して、新しいコピーの空き領域を確保します。

- 時間の 5 分後に撮影された最大 6 つの 1 時間単位のスナップショット。
- 月曜日から土曜日の午前 0 時から 10 分後に撮影される最大 2 つの日次スナップショット。
- 毎週日曜日の午前 0 時から 15 分後に撮影される最大 2 つの週次スナップショット。

> **Note**
>
> スナップショット時間は、デフォルトで協調ユニバーサルタイム (UTC) に設定されているファイルシステムの時間帯に基づきます。タイムゾーンの変更については、 NetApp サポートドキュメントの「システムタイムゾーンの表示と設定」を参照してください。

`default-1weekly` ポリシーは、週間スケジュールのスナップショットを 1 つだけ保持する点を除いて、`default` ポリシーと同じ方法で動作します。

none ポリシーは、スナップショットを作成しません。このポリシーをボリュームに割り当てると、自動スナップショットが作成されないようにすることができます。

ONTAP CLI または REST API を使用してカスタムスナップショットポリシーを作成することもできます。詳細については、NetApp ONTAP 製品ドキュメントの「スナップショットポリシーの作成」を参照してください。Amazon FSx コンソール、、または Amazon FSx API でボリュームを作成または更新するときに AWS CLI、スナップショットポリシーを選択できます。詳細については、「ボリュームの作成」および「ボリュームの更新」を参照してください。

個々のファイルとフォルダの復元

Amazon FSx ファイルシステム上のスナップショットを使用して、ユーザーは個々のファイルまたはフォルダーの以前のバージョンをすばやく復元できます。これにより、共有ファイルシステムに保存されている削除または変更されたファイルをリカバリできます。管理者の手を借りずに、デスクトップ上で直接セルフサービス方式で行うことができます。このセルフサービスアプローチにより、生産性が向上し、管理のワークロードが軽減されます。

Linux および macOS クライアントはスナップショットをボリュームのルートにある `.snapshot` ディレクトリに表示することができます。Windows クライアントはスナップショットを Windows エクスプローラのタブ (ファイルまたはフォルダを右クリック) の `Previous Versions` タブに表示することができます。

スナップショットからファイルを復元する

スナップショットからファイルを復元するには (Linux および macOS クライアント)

1. 元のファイルがまだ存在し、スナップショット内のファイルによって上書きしたくない場合は、Linux または macOS クライアントを使用して元のファイルの名前を変更するか、別のディレクトリに移動します。

2. .snapshot ディレクトリで、復元するファイルのバージョンを含むスナップショットを見つけます。
3. .snapshot ディレクトリからファイルが元々存在していたディレクトリにファイルをコピーします。

スナップショットからファイルを復元するには (Windows クライアント)

Windows クライアント上のユーザーは、使い慣れた Windows ファイルエクスプローラーインターフェイスを使用して、ファイルを以前のバージョンに復元できます。

1. ファイルを復元するには、復元するファイルを選択し、コンテキスト (右クリック) メニューから [Restore previous versions] (以前のバージョンの復元) を選択します。
2. その後、ユーザーは [Previous Versions] (以前のバージョン) リストから以前のバージョンを表示および復元できます。

スナップショットのデータは読み取り専用です。[Previous Versions] (以前のバージョン) タブにリストされているファイルおよびフォルダに変更を加える場合、変更するファイルとフォルダのコピーを書き込み可能な場所に保存し、そのコピーを変更する必要があります。

スナップショットの削除

スナップショットは、前回のスナップショット以降に変更されたボリューム上のデータに対してのみストレージ容量を消費します。このため、ワークロードがデータを迅速に書き込む場合、古いデータのスナップショットはボリュームのストレージ容量の大部分を占める可能性があります。

例えば、 volume show-space ONTAP CLI コマンド出力には 140 KB の が表示されますUser Data。しかし、ユーザーデータが削除される前は、ボリュームには 9.8 GB の User Data がありました。ボリュームからファイルを削除した場合でも、スナップショットは以前のユーザーデータを参照している可能性があります。このため、前の例の Snapshot Reserve および Snapshot Spill は、ボリュームにユーザーデータがほとんどないにもかかわらず、合計 9.8 GB の容量を使用します。

ボリュームの領域を解放するには、不要になった古いスナップショットを削除できます。これを行うには、スナップショットの自動削除ポリシーを作成するか、スナップショットを手動で削除します。スナップショットを削除すると、スナップショットに保存されている変更されたデータが削除されます。

スナップショットの自動削除ポリシーを作成する

ボリューム内の使用可能な領域が少なくなっているときに、スナップショットを自動的に削除するポリシーを作成できます。ボリュームスナップショットの自動削除変更 ONTAP CLI コマンドを使用して、ボリュームの自動削除ポリシーを確立します。

このコマンドを使用する場合は、データを使用して次のプレースホルダー値を置き換えます。

- *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
- *vol_name* をボリュームの名前に置き換えます。

-trigger には、次のいずれかの値を割り当てます。

- volume - スナップショットが削除されるしきい値を使用済みボリューム容量合計のしきい値に対応させる場合は、volume を使用します。スナップショットの削除をトリガーする使用済みボリューム容量のしきい値は、ボリュームのサイズによって決まります。使用される容量のしきい値は 85 ~ 98% です。ボリュームが小さいほどしきい値が小さくなり、ボリュームが大きいほどしきい値が大きくなります。
- snap_reserve - スナップショット予約に保持できる内容に基づいてスナップショットを削除する場合は、snap_reserve を使用します。

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

詳細については、NetApp ONTAP ドキュメントセンターのボリュームスナップショット自動削除変更コマンドを参照してください。

スナップショットを削除する

volume snapshot delete ONTAP CLI コマンドを使用してスナップショットを手動で削除し、次のプレースホルダー値をデータに置き換えます。

- *svm_name* をボリュームが作成されている SVM の名前に置き換えます。
- *vol_name* をボリュームの名前に置き換えます。
- *snapshot_name* をスナップショットの名前に置き換えます。このコマンドは、*snapshot_name* のワイルドカード文字 (*) をサポートしています。したがって、例えば、hourly* を使用して時間単位のスナップショットをすべて削除できます。

> **Important**
>
> Amazon FSx バックアップが有効になっている場合、Amazon FSx は各ボリュームの最新の Amazon FSx バックアップのスナップショットを保持します。これらのスナップショットは、バックアップ間の増分を維持するために使用され、この方法を使用して削除することはできません。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

自動スナップショットの無効化

自動スナップショットは、FSx for ONTAP ファイルシステム内のボリュームのデフォルトのスナップショットポリシーによって有効になります。データのスナップショットが必要ない場合 (テストデータを使用している場合など) 、次の手順で説明するように、ボリュームのスナップショットポリシーを 、 、API、および CLI を使用して に設定することで、スナップショットを無効にすることができます。 none AWS Management Console AWS CLI ONTAP

自動スナップショットを無効にするには (AWS コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [File systems] (ファイルシステム) に移動してボリュームを更新する ONTAP ファイルシステムを選択します。
3. [Volumes] (ボリューム) タブを選択します。
4. 更新するボリュームを選択します。
5. [Action] (アクション) で、[Update volume] (ボリュームの更新) を選択します。

   [Update volume] (ボリュームの更新) ダイアログボックスに、現在のボリューム設定が表示されます。
6. スナップショットポリシー で、なし を選択します。
7. [Update] (更新) をクリックして、ボリュームを更新します。

自動スナップショットを無効にするには (AWS CLI)

- 次の例に示すように、update-volume AWS CLI コマンド (または同等の UpdateVolume API コマンド) を使用してnone、 を SnapshotPolicy に設定します。

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

自動スナップショットを無効にするには (ONTAP CLI)

ボリュームのスナップショットポリシーを設定して、noneデフォルトのポリシーを使用して自動スナップショットをオフにします。

1. volume snapshot policy show ONTAP CLI コマンドを使用してnoneポリシーを表示します。

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                             0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                 SnapMirror Label
    ---------------------- -----     ---------------------- -------------------
    -                          -     -                      -
```

2. volume modify ONTAP CII コマンドを使用して、ボリュームのスナップショットポリシーをに設定noneし、自動スナップショットを無効にします。次のプレースホルダー値をデータに置き換えます。

   - *svm_name* — SVM の名前を使用します。
   - *vol_name* — ボリュームの名前を使用します。

   続行するかどうかを確認するメッセージが表示されたら、**y** を入力します。

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none
```

```
Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

スナップショット予約

スナップショットコピー予約は、スナップショットコピーを保存するためのボリュームのストレージ容量の特定の割合を設定し、デフォルト値は 5% です。スナップショットコピー予約には、ボリュームバックアップ を含め、スナップショットコピーに十分なスペースを割り当てる必要があります。スナップショットコピーがスナップショット予約領域を超える場合は、アクティブなファイルシステムから既存のスナップショットコピーを削除して、ファイルシステムを使用するためのストレージ容量を回復する必要があります。スナップショットコピーに割り当てられているディスク容量の割合を変更することもできます。

スナップショットがスナップショット予約の 100% 以上を消費するたびに、プライマリ SSD ストレージ領域を占有し始めます。このプロセスはスナップショットスピルと呼ばれます。スナップショットがアクティブなファイルシステムスペースを占有し続けると、ファイルシステムがいっぱいになるリスクがあります。スナップショットの流出によりファイルシステムがいっぱいになった場合は、十分なスナップショットを削除した後にのみファイルを作成できます。

スナップショットリザーブのスナップショットに十分なディスク容量がある場合、プライマリ SSD 階層からファイルを削除すると、新しいファイルのディスク容量が解放されます。一方、これらのファイルを参照するスナップショットコピーは、スナップショットコピーリザーブの領域のみを消費します。

スナップショットがリザーブド量 (スナップショットリザーブ) を超えるディスク容量を消費するのを防ぐ方法がないため、プライマリ SSD 階層に新しいファイルを作成したり、既存のファイルを変更したりするために常に使用可能な容量を確保するために、スナップショットに十分なディスク容量を予約することが重要です。

ディスクがいっぱいになったときにスナップショットが作成された場合、プライマリ SSD 階層からファイルを削除しても、そのデータはすべて新しく作成されたスナップショットからも参照される

ため、空き領域は作成されません。ファイルを作成または更新するためにストレージを解放するには、スナップショットを削除する必要があります。

NetApp ONTAP CLI を使用して、ボリュームのスナップショット予約の量を変更できます。詳細については、「ボリュームのスナップショット予約の更新」を参照してください。

ボリュームのスナップショット予約の更新

次の手順で説明するように、CLI または API NetApp ONTAP を使用してボリュームのスナップショット予約の量を変更できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. `snap reserve` ONTAP CLI コマンドを使用して、スナップショットのコピー予約に使用されるディスク容量の割合を変更します。をボリュームの名前*vol_name*に置き換え、 *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

   次の例では、vol1 のスナップショット予約をボリュームストレージ容量の 25% に変更します。

   ```
   ::> snap reserve vol1 25
   ```

を使用したスケジュールされたレプリケーション NetApp SnapMirror

を使用して NetApp SnapMirror 、2 番目のファイルシステムとの間で FSx for ONTAP ファイルシステムの定期的なレプリケーションをスケジュールできます。この機能は、リージョン内とクロスリージョンデプロイの両方で使用できます。

NetApp SnapMirror はデータを高速でレプリケートするため、 の 2 つの Amazon FSx ファイルシステム間、またはオンプレミスから へレプリケートする場合にも AWS、ONTAP システム間で高いデータ可用性と高速データレプリケーションを実現できます AWS。レプリケーションは 5 分ごとにスケジュールできますが、RPO (目標復旧時点)、RTO (目標復旧時間)、パフォーマンスに関する考慮事項に基づいて間隔を慎重に選択する必要があります。

データを NetApp ストレージシステムにレプリケートし、セカンダリデータを継続的に更新すると、データは最新の状態に保たれ、必要なときにいつでも利用可能な状態に保たれます。外部レプリケーションサーバーは必要ありません。を使用してデータをレプリケート NetApp SnapMirror する方法の詳細については、NetApp BlueXP ドキュメントの「レプリケーションサービスについて学ぶ」を参照してください。

NetApp ONTAP CLI および REST API に加えて、Amazon FSx コンソール、 AWS CLI、および Amazon FSx API を使用して、 の NetApp SnapMirrorデータ保護 (DP) 送信先ボリュームを作成できます。Amazon FSx コンソールと を使用して送信先ボリュームを作成する方法については AWS CLI、「」を参照してくださいボリュームの作成。

NetApp BlueXP または NetApp ONTAP CLI を使用して、ファイルシステムのレプリケーションをスケジュールできます。

> **Note**
>
> SnapMirror レプリケーションには次の 2 つのタイプがあります。ボリュームレベル SnapMirror と SVM ディザスタリカバリ(SVMDR)。FSx for ONTAP では、ボリュームレベルの SnapMirror レプリケーションのみがサポートされています。

NetApp BlueXP を使用してレプリケーションをスケジュールする

NetApp BlueXP を使用して、FSx for ONTAP ファイルシステムで SnapMirror とのレプリケーションを設定できます。詳細については、「BlueXP ドキュメント」の「システム間でのデータのレプリケーション」を参照してください。 NetApp BlueXP

NetApp ONTAP CLI を使用してレプリケーションをスケジュールする

NetApp ONTAP CLI を使用して、スケジュールされたボリュームレプリケーションを設定できます。詳細については、NetApp ONTAP ドキュメントセンターの SnapMirror 「ボリュームレプリケーションの管理」を参照してください。

によるデータの保護 SnapLock

SnapLock は、ファイルを Write Once, Read Many (WORM) に移行して保護する機能で、これを使うことにより、指定した保持期間中はファイルの変更や削除を防ぐことができます。SnapLock を使用することで、規制を順守したり、ビジネスに不可欠なデータをランサムウェアによる攻撃から保護したり、セキュリティを強化して改ざんや削除からデータを保護したりすることができます。

Amazon FSx for NetApp ONTAP は、 での Compliance モードと Enterprise モードの保持をサポートしていますSnapLock。詳細については、「SnapLock Compliance と SnapLock Enterprise」を参照してください。

SnapLock ボリュームは、2023 年 7 月 13 日以降に作成された FSx for ONTAP ファイルシステムで作成できます。既存のファイルシステムでは、今後予定されている週次メンテナンス期間中に SnapLock のサポートを受けることになります。

トピック

SnapLock の働き

SnapLock を使うと、ファイルが削除、変更されたり、その名前が変更されたりするのを防ぐことにより、規制やガバナンス上の目的を満たすことができます。SnapLock ボリュームを作成する際は、ファイルを WORM (Write Once, Read Many) ストレージにコミットし、データの保持期間を設定します。ファイルは、指定した期間だけ、または無期限に、消去不可または書き込み不可の状態で保存できます。

> **Important**
>
> ボリュームの作成時に、SnapLock の設定を使用するかどうかを指定する必要があります。作成後は、SnapLock ではないボリュームを SnapLock に変換することはできません。

リテンションモード

SnapLock には、Compliance と Enterprise という 2 種類の保持モードがあります。Amazon FSx for NetApp ONTAP は、両方をサポートしています。これらはユースケースが異なり、機能も一部異なりますが、どちらも WORM モデルを使うことでデータを変更または削除から保護します。以下の表は、両方の保持モードの類似点と相違点をまとめたものです。

SnapLock 機能	SnapLock Compliance	SnapLock Enterprise
説明	Compliance ボリューム上の WORM に移行したファイルは、保持期間が終了するまで削除することはできません。	Enterprise ボリューム上の WORM に移行したファイルは、権限を持つユーザーが特権削除を使用すると、保持期間の終了前に削除することができます。
ユースケース	• 政府または業界に固有の指令 (SEC 規則 17a-4 (f)、FINRA 規則 4511、CFTC 規制 1.31 など) に対応するため。 • ランサムウェア攻撃から防御するため。	• 組織内のデータ整合性と内部コンプライアンスを強化するため。 • SnapLock Compliance を使用する前に保持設定をテストするため。
自動コミット	はい	はい
イベントベースの保持 (EBR)*	はい	はい
リーガルホールド*	はい	いいえ
特権削除	いいえ	はい
ボリューム付加モード	はい	はい
SnapLock 監査ログボリューム	はい	はい

* EBR およびリーガルホールドのオペレーションは、ONTAP CLI と REST API でサポートされています。

SnapLock 管理者

SnapLock ボリュームで特定のアクションを実行するときは、SnapLock 管理者権限が必要になります。SnapLock 管理者権限は、ONTAP CLI の `vsadmin-snaplock` のロールで定義されます。SnapLock 管理者ロールを持つ、ストレージ仮想マシン (SVM) 管理者アカウントを作成できるのは、クラスター管理者です。

次のアクションは、ONTAP CLI の `vsadmin-snaplock` のロールを使用することで実行できます。

- 自分のユーザーアカウント、ローカルパスワード、キー情報を管理する
- ボリュームを管理する (ボリュームの移動は除く)
- クォータ、qtree、スナップショットのコピー、ファイルを管理する
- 特権削除やリーガルホールドなど、SnapLock のアクションを実行する
- ネットワークファイルシステム (NFS) とサーバーメッセージブロック (SMB) プロトコルを設定する
- ドメインネームシステム (DNS)、Lightweight Directory Access Protocol (LDAP)、Network Information Service (NIS) の各サービスを設定する
- ジョブをモニタリングする

以下の手順では、ONTAP CLI で SnapLock 管理者を作成する方法について説明します。このタスクを実行するには、Secure Shell Protocol (SSH) などの安全な接続で、クラスター管理者としてログインする必要があります。

ONTAP CLI で vsadmin-snaplock ロールを持つ SVM 管理者アカウントを作成するには

- 以下のコマンドを実行します。*SVM_name* と をユーザー自身の情報*SnapLockAdmin*に置き換えます。

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLock 監査ログボリューム

SnapLock 監査ログボリュームには SnapLock 監査ログが含まれ、監査ログには、SnapLock 管理者が作成された日時、特権削除が実行された日時、ファイルにリーガルホールドが適用された日時などの、イベントのタイムスタンプが含まれています。SnapLock 監査ログのボリュームは、消去できないイベントの記録です。

以下のアクションを行うには、SnapLock 監査ログボリュームを SnapLock ボリュームと同じ SVM に作成する必要があります。

- 特権削除を SnapLock Enterprise ボリュームで有効または無効にするには
- リーガルホールドを SnapLock Compliance ボリューム内のファイルに適用するには

> **Warning**
>
> - SnapLock 監査ログボリュームの最小保持期間は 6 か月間です。この保持期間が終了しないと、SnapLock 監査ログボリュームが SnapLock Enterprise モードで作成されている場合であっても、そのボリュームとそれに関連付けられている SVM およびファイルシステムは削除できません。
> - 特権削除を使用してファイルを削除した際に、ファイルの保持期間がボリュームの保持期間よりも長い場合、監査ログボリュームはファイルの保持期間を継承します。例えば、特権削除を使用して、保持期間が 10 か月のファイルを削除した際に、監査ログボリュームの保持期間が 6 か月の場合、この監査ログボリュームの保持期間は 10 か月に延長されます。

SVM で使用できるアクティブな SnapLock 監査ログボリュームは 1 つのみですが、これは SVM 内の複数の SnapLock ボリュームで共有できます。SnapLock 監査ログボリュームを正常にマウントするには、ジャンクションパスを `/snaplock_audit_log` に設定します。このジャンクションパスは、監査ログボリュームではないボリュームを含め、他のボリュームが使用することはできません。

SnapLock 監査ログは、監査ログボリュームのルートの下にある `/snaplock_log` ディレクトリにあります。特権削除のオペレーションは、`privdel_log` サブディレクトリに口グ記録されます。リーガルホールドの開始および終了オペレーションは、`/snaplock_log/legal_hold_logs/` に口グ記録されます。それ以外のログはすべて、`system_log` サブディレクトリに保存されます。

SnapLock 監査ログボリュームは、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API を使って作成できます。

> **Note**
>
> データ保護 (DP) ボリュームを SnapLock 監査ログボリュームとして使用することはできません。

以下の手順では、Amazon FSx コンソールで SnapLock 監査ログボリュームを作成する方法について説明します。

Amazon FSx コンソールで SnapLock 監査ログボリュームを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [監査ログボリューム] で [有効] を選択します。

   [ジャンクションパス] が `/snaplock_audit_log` に設定されていることを確認します。
5. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
6. [確認] を選択してボリュームを作成します。

Amazon FSx API を使用して SnapLock 監査ログボリュームをオンにするには、`CreateSnaplockConfiguration` で `AuditLogVolume` を使用します。

SnapLock ボリューム内のデータへのアクセス

SnapLock ボリューム内のデータには、NFS や SMB など、オープンファイルのプロトコルを使用することでアクセスできます。SnapLock ボリュームにデータを書き込んだり、WORM で保護されたデータを読み込んだりしても、パフォーマンスには影響しません。

NFS や SMB を使うことで SnapLock ボリューム間でファイルをコピーできます。ただし、元の WORM プロパティはコピー先の SnapLock ボリュームでは保持されません。コピーしたファイルの

変更または削除を防ぐには、コピーしたファイルを WORM に再コミットする必要があります。詳細については、「ファイルを WORM 状態にコミットする」を参照してください。

また、SnapMirror を使って SnapLock データをレプリケートすることも可能ですが、レプリケート元のボリュームとレプリケート先のボリュームは同じ保持モードの SnapLock ボリュームでなければなりません (共に Compliance モードまたは Enterprise モードであるなど)。

SnapLock Compliance

Amazon FSx for NetApp ONTAP は SnapLock Compliance ボリュームをサポートしています。

SnapLock Compliance の使用

このセクションでは、Compliance 保持モードのユースケースと考慮事項について説明します。

SnapLock Compliance のユースケース

以下のユースケースでは、Compliance 保持モードを選択できます。

- 政府または業界に固有の指令 (SEC 規則 17a-4 (f)、FINRA 規則 4511、CFTC 規制 1.31 など) に対応する必要がある場合に、SnapLock Compliance を使用できます。Amazon FSx for NetApp ONTAP のコンプライアンスは、 によってこれらの義務と規制について評価されましたCohasset Associates。詳細については、「Amazon FSx for NetApp ONTAP のコンプライアンス評価レポート」を参照してください。
- SnapLock Compliance を使用すれば、ランサムウェア攻撃に対抗するための包括的なデータ保護戦略を、補完または強化できます。

SnapLock Compliance の考慮事項

Compliance 保持モードについて考慮すべき重要な点をいくつか紹介します。

- ファイルを SnapLock Compliance ボリュームで Write Once, Read Many (WORM) 状態に移行させると、保持期間が終了するまで、いずれのユーザーもこれを削除することはできなくなります。
- SnapLock Compliance ボリュームを削除できるのは、ボリューム上のすべての WORM ファイルの保持期間が終了し、ボリュームから WORM ファイルが削除された場合のみです。
- SnapLock Compliance ボリュームの名前は、作成後は変更できません。
- SnapMirror を使用して WORM ファイルをレプリケートできますが、レプリケート元ボリュームとレプリケート先ボリュームは同じ保持モードである必要があります (たとえば、両方とも Compliance である必要があります) 。

- SnapLock Compliance ボリュームを SnapLock Enterprise ボリュームに変換することはできません。その逆の変換もできません。

SnapLock Compliance ボリュームの作成

SnapLock Compliance ボリュームは、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API を使って作成できます。

Amazon FSx API を使用して SnapLock Compliance ボリュームを作成するには、`CreateSnaplockConfiguration` で `SnaplockType` を使用します。

以下の手順では、Amazon FSx コンソールで SnapLock Compliance ログボリュームを作成する方法について説明します。

Amazon FSx コンソールで SnapLock Compliance ボリュームを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [保持モード] で [Compliance] を選択します。
5. [監査ログボリューム] で、[有効] または [無効] を選択します。

   [有効] を選択した場合は、[ジャンクションパス] が `/snaplock_audit_log` に設定されていることを確認します。

   詳細については、「SnapLock 監査ログボリューム」を参照してください。
6. [保持期間] で、[デフォルトの保持期間]、[最小保持期間]、[最大保持期間] の値を入力します。次に、[ユニット] でそれぞれに対応する単位を選択します。

   詳細については、「SnapLock の保持期間の設定」を参照してください。
7. [自動コミット] で、[有効] または [無効] を選択します。

   [有効] を選択した場合は、[自動コミット期間] に値を入力し、対応する[自動コミット単位] を選択します。

   値は 5 分から 10 年までの間で指定できます。

詳細については、「自動コミット」を参照してください。

8. [ボリューム付加モード] で、[有効] または [無効] を選択します。

   詳細については、「ボリューム付加モード」を参照してください。

9. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
10. [確認] を選択してボリュームを作成します。

SnapLock Enterprise

Amazon FSx for NetApp ONTAP はSnapLock、Enterprise ボリュームをサポートしています。

SnapLock Enterprise を使う

このセクションでは、Enterprise 保持モードのユースケースと考慮事項について説明します。

SnapLock Enterprise のユースケース

以下のユースケースでは、Enterprise 保持モードを選択できます。

- SnapLock Enterprise を使用すると、特定のユーザーのみにファイルを削除する権限を付与できます。
- SnapLock Enterprise を使用すると、組織のデータ整合性と内部コンプライアンスとを向上させることができます。
- SnapLock Enterprise を使用すると、SnapLock Compliance を使用する前に保持設定をテストできます。

SnapLock Enterprise を使用する際の考慮事項

Enterprise 保持モードについて考慮すべき重要な点をいくつか紹介します。

- SnapMirror を使用すると WORM ファイルをレプリケートできますが、レプリケート元のボリュームとレプリケート先のボリュームは、同じ保持モードである必要があります (共に Enterprise モードであるなど)。
- SnapLock ボリュームは、Enterprise から Compliance に、または Compliance からEnterprise に変換することはできません。
- SnapLock Enterprise は、リーガルホールドをサポートしていません。

特権削除

SnapLock Enterprise と SnapLock Compliance の大きな違いの 1 つは、SnapLock Enterprise ボリュームでは、SnapLock 管理者が特権削除を有効にして、保持期間が終了する前にファイルを削除することができるという点です。SnapLock 管理者は、有効な保持ポリシーが適用されている SnapLock Enterprise ボリュームから、ファイルを削除することができる唯一のユーザーです。詳細については、「SnapLock 管理者」を参照してください。

特権削除は、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API から、有効または無効にすることができます。特権削除を有効にするには、先に、SnapLock ボリュームと同じ SVM に SnapLock 監査ログボリュームを作成する必要があります。詳細については、「SnapLock 監査ログボリューム」を参照してください。

Amazon FSx API で特権削除を有効にするには、`CreateSnaplockConfiguration` で `PrivilegedDelete` を使用します。

以下の手順では、Amazon FSx コンソールで特権削除を有効にする方法について説明します。

Amazon FSx コンソールで SnapLock Enterprise ボリュームの特権削除を有効にするには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [保持モード] は、[Enterprise] を選択します。
5. [特権削除] は、[有効] を選択します。
6. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
7. [確認] を選択してボリュームを作成します。

> **Note**
>
> 保持期間が終了した Write Once, Read Many (WORM) ファイルを削除するために、特権削除コマンドを発行することはできません。保持期間の終了後は、通常の削除オペレーションを発行dできます。

特権削除は完全に無効にすることができますが、このアクションは元に戻せません。特権削除を完全に無効にしたときは、SnapLock 監査ログボリュームを SnapLock Enterprise ボリュームに関連付ける必要はありません。

Amazon FSx API を使って特権削除を有効にするときは、`CreateSnaplockConfiguration` で `PrivilegedDelete` を使用します。

Amazon FSx コンソールで SnapLock Enterprise ボリュームの特権削除を無効にするには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [保持モード] は、[Enterprise] を選択します。
5. [特権削除] は、[完全に無効] を選択します。
6. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
7. [確認] を選択してボリュームを作成します。

SnapLock Enterprise ボリュームの作成

SnapLock Enterprise ボリュームは、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API を使って作成できます。

Amazon FSx API を使用して SnapLock Enterprise ボリュームを作成するには、`CreateSnaplockConfiguration` で `SnaplockType` を使用します。

Amazon FSx コンソールで SnapLock Enterprise ボリュームを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [保持モード] は、[Enterprise] を選択します。

5. [監査ログボリューム] で、[有効] または [無効] を選択します。

   [有効] を選択した場合は、[ジャンクションパス] が /snaplock_audit_log に設定されていることを確認します。

   詳細については、「SnapLock 監査ログボリューム」を参照してください。
6. [保持期間] で、[デフォルトの保持期間]、[最小保持期間]、[最大保持期間] の値を入力します。次に、[ユニット] でそれぞれに対応する単位を選択します。

   詳細については、「SnapLock の保持期間の設定」を参照してください。
7. [自動コミット] で、[有効] または [無効] を選択します。

   [有効] を選択した場合は、[自動コミット期間] に値を入力し、対応する[自動コミット単位] を選択します。

   値は 5 分から 10 年までの間で指定できます。

   詳細については、「自動コミット」を参照してください。
8. [特権削除] で、[有効]、[無効]、[完全に無効] のいずれかを選択します。

   詳細については、「特権削除」を参照してください。
9. [ボリューム付加モード] で、[有効] または [無効] を選択します。

   詳細については、「ボリューム付加モード」を参照してください。
10. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
11. [確認] を選択してボリュームを作成します。

Enterprise モードをバイパスする

Amazon FSx コンソールか Amazon FSx API を使用する場合は、IAM `fsx:BypassSnapLockEnterpriseRetention` アクセス権限を使って、有効な保持ポリシーを持つ WORM ファイルを含む、SnapLock Enterprise ボリュームを削除する必要があります。

詳細については、「SnapLock ボリュームの削除」を参照してください。

SnapLock の保持期間の設定

SnapLock ボリュームを作成するときは、ボリュームのデフォルトの保持期間を設定することもできますが、Write Once, Read Many (WORM) ファイル用に明示的に保持期間を設定することもでき

ます。この保持期間中は、WORM で保護されたファイルを削除または変更することはできません。保持期間は、保持時間の計算に使用されます。例えば、2023 年 7 月 14 日の午前 0 時にファイルを WORM に移行して、保持期間を 5 年に設定した場合、保持時間は 2028 年 7 月 14 日の午前 0 時までになります。

WORM の詳細については、「ファイルを WORM 状態にコミットする」を参照してください。

保持期間ポリシー

保持期間は、以下のパラメータに割り当てる値によって決まります。

- デフォルトの保持 — WORM ファイルに保持期間を明示的に指定しなかった場合に割り当てられる、デフォルトの保持期間です。
- 最小保持期間 — WORM ファイルに割り当てることができる最短の保持期間です。
- 最大保持期間 — WORM ファイルに割り当てることができる最長の保持期間です。

> **Note**
>
> 保持期間が終了しても、WORM ファイルを変更することはできません。ファイルを削除するか、新たに保持期間を設定し、WORM の保護を再度有効にします。

保持期間は、複数の異なる時間単位を使用して指定できます。以下の表は、サポートされている具体的な範囲のリストです。

タイプ	値	メモ
[Seconds] (秒)	0 ~ 65,535	
分	0 ~ 65,535	
時間	0 ~ 24	
日間	0 ~ 365	
か月	0 ~ 12	
年間	0 ~ 100	

タイプ	値	メモ
無制限	-	ファイルを永久に保持します。 [デフォルトの保持期間]、[最大保持期間]、[最小保持期間] で使用できます。
未指定*	-	保持期間が設定されるまでファイルを保持します。 [デフォルトの保持期間] のみで使用できます。

* ファイルを、保持期間が指定されていない WORM に移行すると、ファイルにはその SnapLock ボリュームに設定されている最小保持期間が付与されます。WORM で保護されたファイルを絶対保持時間に移行する場合、新しい保持期間は、そのファイルで以前に設定された最小期間よりも長くする必要があります。

期限の切れた保持期間

WORM ファイルの保持期間が終了すると、ファイルを削除するか、新しい保持期間を設定して WORM 保護を再度有効にすることができます。WORM ファイルは、保持期間の終了後は、自動的に削除されることはありません。保持期間が終了しても、引き続き、WORM ファイルの内容を変更することはできません。

SnapLock ボリュームの保持期間の設定

SnapLock ボリュームの保持期間は、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API を使って設定できます。

Amazon FSx API を使って保持期間を設定するには、`SnaplockRetentionPeriod` 設定を使用します。

以下の手順では、Amazon FSx コンソールで保持期間を設定する方法について説明します。

Amazon FSx コンソールで SnapLock ボリュームの保持期間を設定するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。

2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [保持期間] で、[デフォルトの保持期間]、[最小保持期間]、[最大保持期間] の値を入力します。次に、[ユニット] でそれぞれに対応する単位を選択します。
5. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
6. [確認] を選択してボリュームを作成します。

ファイルを WORM 状態にコミットする

このセクションでは、ファイルを Write Once, Read Many (WORM) 状態に移行する方法について説明します。また、WORM で保護されたファイルに段階的にデータを書き込んでいく方法である、ボリューム付加モードについても取り上げます。

自動コミット

ファイルが指定した期間、変更されなかった場合は、自動コミットを使用して WORM に移行することができます。自動コミットは、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API から、有効にすることができます。

自動コミットの期間は、5 分から 10 年の間で指定できます。以下の表は、サポートされている具体的な範囲のリストです。

単位	値
分	5 ~ 65,535
時間	1 ~ 65,535
日間	1 ~ 3,650
か月	1 ~ 120
年間	1 ~ 10

Amazon FSx API を使って自動コミットを有効にするには、CreateSnaplockConfiguration で AutocommitPeriod を使用します。

以下の手順では、Amazon FSx コンソールで自動コミットを有効にする方法について説明します。

Amazon FSx コンソールで自動コミットを有効にするには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [自動コミット] は、[有効] を選択します。
5. [自動コミット期間] に値を入力し、対応する[自動コミット単位] を選択します。

   値は 5 分から 10 年までの間で指定できます。
6. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
7. [確認] を選択してボリュームを作成します。

ボリューム付加モード

WORM で保護されたファイルにある既存のデータは変更できません。ただし、SnapLock では、WORM に付加可能なファイルを使って既存データの保護を継続することができます。例えば、ログファイルを生成したり、データをファイルに段階的に書き込みながら音声や映像のストリーミングデータを保存したりできます。ボリューム付加モードは、Amazon FSx コンソール、AWS CLI、Amazon FSx API、ONTAP CLI と REST API から、有効または無効にすることができます。

ボリューム付加モードの更新要件

- SnapLock ボリュームは、必ずアンマウントします。
- SnapLock ボリュームから、スナップショットのコピーとユーザーデータをすべて削除します。

Amazon FSx API を使用してボリューム付加モードを有効にするには、CreateSnaplockConfiguration で VolumeAppendModeEnabled を使用します。

以下の手順では、Amazon FSx コンソールでボリューム付加モードを有効にする方法について説明します。

Amazon FSx コンソールでボリューム付加モードを有効にするには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「ボリュームの作成」にある新しいボリュームの作成手順に従います。
3. 詳細セクションのSnapLock 「設定」で、「有効化」を選択します。

   ボリュームで SnapLock を有効化することについての警告に同意するには、チェックボックスを選択します。
4. [ボリューム付加モード] で[有効] を選択します。
5. 「ボリュームの作成」にある、新しいボリュームを作成する手順の続きに従います。
6. [確認] を選択してボリュームを作成します。

イベントベースの保持 (EBR)

イベントベースの保持 (EBR) を使用すると、関連する保持期間を含むカスタムポリシーを作成できます。例えば、指定したパスに含まれるすべてのファイルを WORM に移行し、`snaplock event-retention policy create` および `snaplock event-retention apply` コマンドを使用して保持期間を 1 年間に設定できます。EBR を使用する場合は、ボリューム、ディレクトリ、ファイルのいずれかを指定する必要があります。EBR ポリシーを作成するときに選択した保持期間は、指定したパスに含まれるすべてのファイルに適用されます。

EBR は ONTAP CLI と REST API でサポートされています。

> **Note**
>
> ONTAP は、 FlexGroup ボリュームでの EBR をサポートしていません。

以下の手順では、EBR ポリシーを作成、適用、変更、削除する方法について説明します。ONTAP CLI でこれらのタスクを実行するには、SnapLock 管理者である (`vsadmin-snaplock` 権限を持つ人である) 必要があります。詳細については、「SnapLock 管理者」を参照してください。

ONTAP CLI で EBR ポリシーを作成するには

以下のコマンドを実行します。*p1* と *"10 years"* を自分の情報に置き換えます。

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

ONTAP CLI で EBR ポリシーを適用するには

以下のコマンドを実行します。*p1* と *slc* を自分の情報に置き換えます。EBR ポリシーに特定のパスを指定するときは、フォワードスラッシュ (/) の後にパスを追加できます。それ以外の場合、このコマンドは、ボリューム上のすべてのファイルに EBR ポリシーを適用します。

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

ONTAP CLI で EBR ポリシーを修正するには

以下のコマンドを実行します。*p1* と *"5 years"* を自分の情報に置き換えます。

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

ONTAP CLI で EBR ポリシーを削除するには

以下のコマンドを実行します。*p1* を自分の情報に置き換えます。

```
vs1::> snaplock event-retention policy delete -name p1
```

NetApp Documentation Center の関連コマンド:

- snaplock event-retention abort
- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

リーガルホールド

リーガルホールドを使用すると、WORM ファイルを無期限に保持できます。リーガルホールドは通常、訴訟目的で使用されます。リーガルホールドの対象となっている WORM ファイルは、リーガルホールドが解除されるまで削除することはできません。

リーガルホールド は、ONTAP CLI と REST API でサポートされています。

> **Note**
>
> ONTAP は、 FlexGroup ボリュームでのリーガルホールドをサポートしていません。

以下の手順では、リーガルホールドを開始および終了する方法について説明します。ONTAP CLI でこれらのタスクを実行するには、SnapLock 管理者である (vsadmin-snaplock 権限を持つ人である) 必要があります。詳細については、「SnapLock 管理者」を参照してください。

ONTAP CLI を使用して SnapLock Compliance ボリューム内のファイルでリーガルホールドを開始するには

以下のコマンドを実行します。*litigation1*、*slc_vol1*、*file1* を自分の情報に置き換えます。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

ONTAP CLI を使用して SnapLock Compliance ボリューム内のすべてのファイルでリーガルホールドを開始するには

以下のコマンドを実行します。*litigation1* と *slc_vol1* を自分の情報に置き換えます。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

ONTAP CLI を使用して SnapLock Compliance ボリューム内のファイルでリーガルホールドを終了するには

以下のコマンドを実行します。*litigation1*、*slc_vol1*、*file1* を自分の情報に置き換えます。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

ONTAP CLI を使用して SnapLock Compliance ボリューム内のすべてのファイルでリーガルホールドを終了するには

以下のコマンドを実行します。*litigation1* と *slc_vol1* を自分の情報に置き換えます。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> リーガルホールドを発行するときは、`snaplock legal-hold show` コマンドを使用して `-operation-status` をモニタリングし、失敗していないことを確認することが推奨されます。

NetApp Documentation Center の関連コマンド:

- snaplock legal-hold abort
- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

SnapLock ボリュームのバックアップ

SnapLock ボリュームをバックアップすればデータ保護を強化できます。SnapLock ボリュームを復元すると、デフォルトの保持期間、最小保持期間、最大保持期間など、ボリュームの元の設定が維持されます。Write Once, Read Many (WORM) 設定やリーガルホールドも維持されます。

> **Note**
>
> SnapLock FlexGroup ボリュームはバックアップできません。

SnapLock ボリュームのバックアップを SnapLock またはそれ以外の SnapLock ボリュームとして復元できます。ただし、それ以外の SnapLock ボリュームのバックアップを SnapLock ボリュームとして復元できません。

バックアップの詳細については、「バックアップの使用」を参照してください。

SnapLock ボリュームの削除

SnapLock Compliance ボリューム上のすべての Write Once, Read Many (WORM) ファイルの保持期間が過ぎている場合、この Compliance ボリュームは削除できます。

> **Note**
>
> SnapLock Enterprise または Compliance ボリュームを含む AWS アカウント を閉じると、AWS と FSx for ONTAP はデータをそのまま維持してアカウントを 90 日間停止します。アカウントを 90 日以内に再開しなければ、AWS は保存設定に関係なく、SnapLock ボリューム内のデータを含むすべてのデータを削除します。

適切な権限を持っていれば、SnapLock Enterprise ボリュームはいつでも削除できます。Amazon FSx 管理者である必要があります。また、Amazon FSx コンソールか Amazon FSx API を使用する場合は、IAM `fsx:BypassSnapLockEnterpriseRetention` IAM アクセス権限を使って、有効な保持ポリシーを持つ WORM ファイルを含む、SnapLock Enterprise ボリュームを削除する必要があります。

> **Warning**
>
> SnapLock 監査ログボリュームの最小保持期間は 6 か月間です。この保持期間が終了するまでは、SnapLock 監査ログボリューム、ストレージ仮想マシン (SVM)、SVM に関連付けられたファイルシステムは、ボリュームが SnapLock Enterprise モードで作成された場合であっても、削除することはできません。詳細については、「SnapLock 監査ログボリューム」を参照してください。

Amazon FSx コンソールで SnapLock Enterprise ボリュームを削除するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ナビゲーションペインで [ボリューム] を選択します。
3. 削除するボリューム を選択します。
4. [アクション] で [ボリュームを削除] を選択します。
5. SnapLock 「エンタープライズ保持をバイパスする」で、「はい」を選択します。
6. 確認のダイアログボックスで、[最終バックアップを作成] の、次のいずれかのオプションを選択します。

   - [はい] を選択してボリュームの最終バックアップを作成します。最終バックアップの名前が表示されます。
   - ボリュームの最終バックアップが必要ない場合は [No] (なし) を選択します。ボリュームを削除すると、自動バックアップは使用できなくなることを確認するよう求められます。

7. [削除の確認] フィールドに **delete** と入力し、ボリュームの削除を確定します。
8. [Delete volume] (ボリュームの削除) を選択します。

FSx for ONTAP で Microsoft アクティブディレクトリの使用

Amazon FSx は Microsoft Active Directory と連携して、既存の環境と統合します。アクティブディレクトリは、ネットワーク上のオブジェクトに関する情報を保存し、管理者とユーザーがこの情報を見つけて使用できるようにするために使用される Microsoft のディレクトリサービスです。これらのオブジェクトには、通常、ファイルサーバー、ネットワークユーザーおよびコンピュータアカウントなどの共有リソースが含まれます。

オプションで、FSx for ONTAP ストレージ仮想マシン (SVMsをアクティブディレクトリドメインに結合して、ユーザー認証とファイルレベルおよびフォルダレベルのアクセスコントロールを提供できます。その後、サーバーメッセージブロック (SMB) クライアントは、アクティブディレクトリ内の既存のユーザー ID を使用して自分自身を認証し、SVM ボリュームにアクセスできます。ユーザーは、既存の ID を使用し、個々のファイルやフォルダへのアクセスをコントロールすることができます。さらに、既存のファイル、フォルダ、これらのセキュリティアクセスコントロールリスト (ACL) の設定を Amazon FSx に移行でき、一切変更する必要はありません。

Amazon FSx for NetApp ONTAP をアクティブディレクトリに参加させると、ファイルシステムの SVMs をアクティブディレクトリに個別に参加させることができます。つまり、アクティブディレクトリに参加している一部の SVMs と、そうでない他の SVMs を持つファイルシステムを持つことができます。

SVM がアクティブディレクトリに接続したら、次のアクティブディレクトリ設定プロパティを更新できます。

- DNS サーバーの IP アドレス
- セルフマネージド Active Directory サービスアカウントのユーザー名とパスワード

トピック

SVM をセルフマネージド Microsoft AD に接続させるための前提条件

FSx for ONTAP SVM をセルフマネージド Microsoft AD ドメインに接続させる前に、アクティブディレクトリとネットワークが次のセクションに説明されている要件を満たしていることを確認してください。

トピック

オンプレミスのアクティブディレクトリ要件

SVM が接続できるオンプレミスまたはその他のセルフマネージド Microsoft AD が既にあることを確認してください。この Active Directory には、次の設定が必要です。

- Active Directory ドメインコントローラードメインの機能レベルは Windows Server 2000 以降です。
- Active Directory は、単一ラベルドメイン (SLD) 形式ではないドメイン名を使用します。Amazon FSx は SLD ドメインをサポートしていません。
- Active Directory サイトが定義されている場合は、FSx for ONTAP ファイルシステムに関連付けられている VPC 内のサブネットが同じ Active Directory サイトで定義されていること、および VPC サブネットと Active Directory サイトのサブネットの間に競合が存在しないことを確認します。

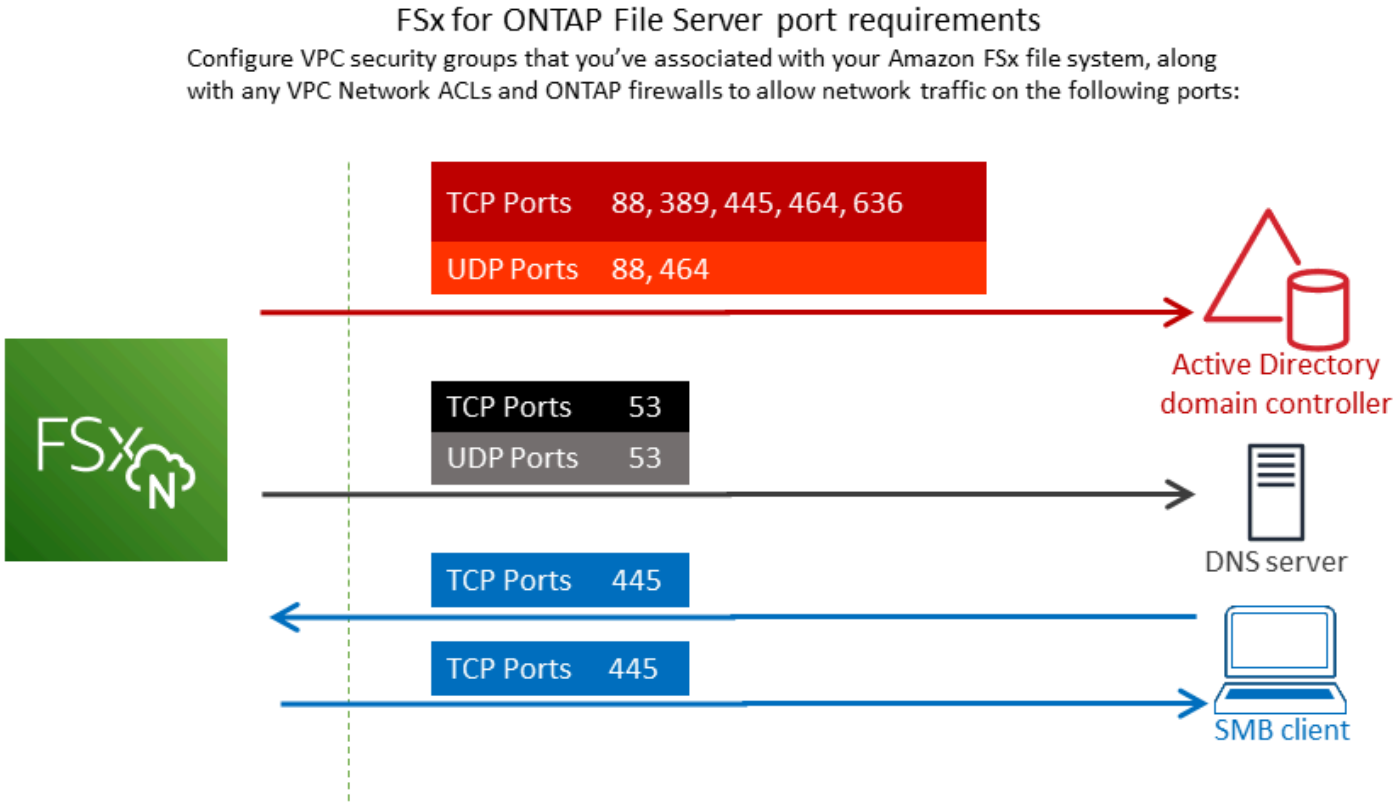
> **Note**
>
> を使用している場合 AWS Directory Service、FSx for ONTAP は SVMs を Simple Active Directory に接続させることをサポートしていません。

ネットワークの設定要件

次のネットワーク設定が適切であり、関連情報が手元にあることを確認してください。

> **Important**
>
> SVM をアクティブディレクトリに接続するには、このトピックに記載されているポートが、すべてのアクティブディレクトリドメインコントローラと SVM 上の両方の iSCSI IP アドレス (iscsi_1 と iscsi_2 の論理インターフェイス (LIF)) 間のトラフィックを許可していることを確認する必要があります。

- DNS サーバーと Active Directory ドメインコントローラーの IP アドレス。
- ファイルシステムを作成する Amazon VPC と、「AWS Direct Connect」、「AWS VPN」、「AWS Transit Gateway」を使用しているセルフマネージドアクティブディレクトリ間の接続。
- ファイルシステムを作成しているサブネットのセキュリティグループおよび VPC ネットワーク ACL で、次の図面に示されているポートとトラフィック方向でトラフィックを許可する必要があります。



各ポートの役割は、次の表に示されています。

プロトコル	ポート	ロール
TCP / UDP	53	ドメインネームシステム (DNS)
TCP / UDP	88	Kerberos 認証
TCP / UDP	389	Lightweight Directory Access プロトコル (LDAP)
TCP	445	Directory Services SMB ファイル共有
TCP / UDP	464	パスワードを変更 / 設定する
TCP	636	TLS/SSL (LDAPS) を介した Lightweight Directory Access Protocol (LDAPS)

- これらのトラフィックルールは、各 Active Directory ドメインコントローラー、DNS サーバー、FSx クライアント、FSx 管理者に適用されるファイアウォールにもミラーリングする必要があります。

> **Important**
>
> Amazon VPC セキュリティグループでは、ネットワークトラフィックが開始される方向でのみポートを開く必要がありますが、ほとんどの Windows ファイアウォールとおよび VPC ネットワーク ACL では両方向にポートを開く必要があります。

アクティブディレクトリサービスアカウントの要件

コンピュータをドメインに接続させる権限を委任されたサービスアカウントが、セルフマネージド Microsoft AD にあることを確認してください。サービスアカウントは、特定のタスクを委任されたセルフマネージド Active Directory のユーザーアカウントです。

サービスアカウントには最低でも、SVM を接続させる OU で次の許可が委任されている必要があります。

- パスワードをリセットする機能
- アカウントのデータの読み取りと書き込みを制限する機能

- コンピュータオブジェクトに `msDS-SupportedEncryptionTypes` プロパティを設定する機能
- DNS ホスト名への書き込み許可
- サービスプリンシパル名への書き込みを許可
- コンピュータオブジェクトを作成および削除する権限
- アカウント制限の読み書きを検証する機能

これらは、コンピュータオブジェクトをアクティブディレクトリに参加させるために必要な最小限のアクセス許可セットを表します。詳細については、Windows Server のドキュメントトピック、「エラー: コントロールを委任された管理者以外のユーザーが、コンピュータをドメインコントローラーに接続させようとすると、アクセスが拒否される」を参照してください。

適切なアクセス許可を使用したサービスアカウントの作成の詳細については、「Amazon FSx サービスアカウントにアクセス許可を委任する」を参照してください。

> **Important**
>
> Amazon FSx では、Amazon FSx ファイルシステムの存続期間中、有効なサービスアカウントが必要です。Amazon FSx は、ファイルシステムを完全に管理し、Active Directory ドメインへのリソースの結合解除と再結合を必要とするタスクを実行できる必要があります。これらのタスクには、障害が発生したファイルシステムまたは SVM の交換、 NetApp ONTAP ソフトウェアのパッチ適用が含まれます。サービスアカウントの認証情報など、Amazon FSx で Active Directory の設定情報を最新の状態に保ちます。詳細については、「Amazon FSx でアクティブディレクトリ設定を最新の状態に保つ」を参照してください。

AWS と FSx for ONTAP を初めて使用する場合は、Active Directory 統合を開始する前に、必ず初期セットアップ手順を完了してください。詳細については、「FSx for ONTAP の設定」を参照してください。

> **Important**
>
> SVMs の作成後に Amazon FSx が OU に作成するコンピュータオブジェクトを移動したり、SVM が接続している間にアクティブディレクトリを削除したりしないでください。移動した場合、SVM が誤設定される原因となります。

アクティブディレクトリを使用する際のベストプラクティス

Amazon FSx for NetApp ONTAP SVM をセルフマネージド Microsoft アクティブディレクトリに接続させる際に考慮するべき提案事項やガイドラインについていくつか説明します。これらはベストプラクティスとして推奨されていますが、必須ではないことに注意してください。

Amazon FSx サービスアカウントにアクセス許可を委任する

Amazon FSx に提供するサービスアカウントは、少なくとも必要最低限のアクセス許可を持つように設定してください。さらに、組織単位 (OU) を他のドメインコントローラーから分離します。

Amazon FSx SVM をドメインに接続させるには、サービスアカウントに委任された許可があることを確認してください。[ドメイン管理者] グループのメンバーには、このタスクを実行するための十分な許可があります。ただし、ベストプラクティスとして、これを実行するために必要最小限の許可のみ付与したサービスアカウントを使用してください。次の手順は、FSx for ONTAP SVM をドメインに接続させるために必要な許可のみを委任する方法を示しています。

この手順は、ディレクトリに接続し、かつ Active Directory User and Computers MMC スナップインがインストールされているマシンで実行します。

Microsoft Active Directory ドメインのサービスアカウントを作成するには

1. Microsoft Active Directory ドメインのドメイン管理者としてログインしていることを確認してください。
2. アクティブディレクトリユーザーとコンピュータ MMC スナップインを開きます。
3. タスクペインで、ドメインノードを展開します。
4. 変更する OU のコンテキスト (右クリック) メニューを見つけて開き、[Delegate Control] (コントロールの委任) を選択します。
5. [Delegation of Control Wizard] (コントロールウィザードの委任) ページで、[Next] (次へ) を選択します。
6. [Selected users and groups] (選択したユーザーとグループ) に特定のユーザーまたは特定のグループを追加するには、[Add] (追加) を選択してから、[Next] (次へ) を選択します。
7. [Tasks to Delegate] (委任するタスク) ページで、[Create a custom task to delegate] (委任するカスタムタスクの作成) を選択し、[Next (次へ) を選択します。
8. [Only the following objects in the folder] (フォルダー内の以下のオブジェクトのみ) を選択してから、[Computer objects] (コンピュータオブジェクト) を選択します。

9. [Create selected objects in this folder] (このフォルダー内に選択したオブジェクトを作成する) を選択してから、[Delete selected objects in this folder] (このフォルダー内の選択したオブジェクトを削除する) を選択します。続いて、[Next] (次へ) を選択します。
10. [これらのアクセス許可を表示] で、[一般] と [プロパティ固有] が選択されていることを確認します。
11. [Permissions] (アクセス許可) を使用する場合、以下を選択します。
    - [Reset Password] (パスワードのリセット)
    - [Read and write Account Restriction] (読み取りおよび書き込み、アカウントの制限)
    - [Validated write to DNS host name] (DNS ホスト名への書き込みの検証)
    - [Validated write to service principal name] (サービスプリンシパル名への書き込みの検証)
    - [msDS-SupportedEncryptionTypes の書き込み]
12. [Next] (次へ) を選択し、[Finish] (完了) を選択します。
13. アクティブディレクトリユーザーとコンピュータ MMC スナップインを閉じます。

> **Important**
>
> SVM が作成された後に Amazon FSx が OU で作成するコンピュータオブジェクトを移動しないでください。移動した場合、SVM が誤設定される原因となります。

Amazon FSx でアクティブディレクトリ設定を最新の状態に保つ

Amazon FSx SVM の中断されない可用性を確保するには、セルフマネージド AD 設定を変更する際、SVM のセルフマネージドアクティブディレクトリ(AD) の設定を更新してください。

例えば、AD が時間ベースのパスワードリセットポリシーを使用しているとします。この場合、パスワードがリセットされたらすぐに、Amazon FSx でサービスアカウントのパスワードを更新してください。これを行うには、Amazon FSx コンソール、Amazon FSx API、または AWS CLI を使用します。同様に、アクティブディレクトリドメインの DNS サーバーの IP アドレスが変更された場合、変更が発生したらすぐに DNS サーバーの IP アドレスを Amazon FSx で更新します。

更新されたセルフマネージド AD 設定に問題がある場合、SVM の状態は [Misconfigured] (誤設定) に変わります。この状態では、コンソール、API、CLI の SVM 説明の横にエラーメッセージと推奨アクションが表示されます。SVM の AD 設定に問題が発生した場合は、設定プロパティに推奨された

是正処置を必ず実行してください。問題が解決した場合は、SVM の状態が [Created] (作成済み) に変わっていることを確認します。

詳細については、、 AWS Management ConsoleAWS CLI、および API を使用した既存の SVM アクティブディレクトリ設定の更新 および ONTAP CLI を使用してアクティブディレクトリの設定を変更する を参照してください。

セキュリティグループを使用して VPC 内のトラフィックを制限する

仮想プライベートクラウド (VPC) のネットワークトラフィックを制限するために、VPC に最小特権のプリンシパルを実装できます。言い換えると、許可を必要最低限に制限することができます。これを行うには、セキュリティグループルールを使用します。詳細については、「Amazon VPC セキュリティグループ」を参照してください。

ファイルシステムのネットワークインターフェイス用のアウトバウンドセキュリティグループルールの作成

セキュリティを強化するには、アウトバウンドトラフィックルールを使用したセキュリティグループの設定を検討してください。これらのルールは、セルフマネージド AD ドメインコントローラー、あるいはサブネットまたはセキュリティグループ内へのアウトバウンドトラフィックのみを許可する必要があります。このセキュリティグループを Amazon FSx ファイルシステムの Elastic Network Interface に関連付けられた VPC に適用します。詳細については、「Amazon VPC によるファイルシステムアクセスコントロール」を参照してください。

SVM を Microsoft アクティブディレクトリに接続する

組織は、オンプレミスかクラウドかにかかわらず、Active Directory を使用して ID とデバイスを管理している場合があります。FSx for ONTAP を使用すると、次の方法で SVMs を既存のアクティブディレクトリドメインに直接結合できます。

- 作成時に新しい SVMs をアクティブディレクトリに接続する：
  - Amazon FSx コンソールの標準作成オプションを使用して新しい FSx for ONTAP ファイルシステムを作成すると、デフォルトの SVM をセルフマネージドアクティブディレクトリに参加させることができます。詳細については、「ファイルシステムの作成方法 (コンソール)」を参照してください。
  - Amazon FSx コンソール AWS CLI、または Amazon FSx API を使用して、既存の FSx for ONTAP ファイルシステムに新しい SVM を作成します。詳細については、「ストレージ仮想マシンの作成」を参照してください。

- 既存の SVMs をアクティブディレクトリに接続する：
  - AWS Management Console AWS CLI、、および API を使用して SVM をアクティブディレクトリに接続させ、最初の参加に失敗した場合は SVM をアクティブディレクトリに再度接続してみてください。既にアクティブディレクトリに接続している SVMs の一部のアクティブディレクトリ設定プロパティを更新することもできます。詳細については、「SVM アクティブディレクトリ設定の管理」を参照してください。
  - NetApp ONTAP CLI または REST API を使用して、SVM アクティブディレクトリ設定の参加、再試行、および参加解除を行います。詳細については、「 NetApp CLI を使用した SVM アクティブディレクトリ設定の管理」を参照してください。

> **Important**
>
> - Amazon FSx は、Microsoft DNS をデフォルトの DNS サービスとして使用する場合にのみ、SVM の DNS レコードを登録します。サードパーティー DNS を使用する場合、作成後に Amazon FSx SVM の DNS エントリを手動で設定する必要があります。
> - を使用する場合は AWS Managed Microsoft AD、 AWS が委任した FSx 管理者、 AWS が委任した管理者などのグループ、または OU に委任されたアクセス許可を持つカスタムグループを指定する必要があります。

FSx for ONTAP SVM をセルフマネージド Active Directory に直接結合すると、SVM は同じ Active Directory フォレスト (ドメイン、ユーザー、コンピュータを含む Active Directory 設定内の最上位の論理コンテナ) と、既存のファイルサーバーを含むユーザーおよび既存のリソースと同じ Active Directory ドメインに存在します。

SVM をアクティブディレクトリに接続するときに必要な情報

選択した API オペレーションに関係なく、SVM をアクティブディレクトリに接続させるときは、アクティブディレクトリに関する次の情報を指定する必要があります。

- SVM 用に作成するアクティブディレクトリコンピュータオブジェクトの NetBIOS 名。これはアクティブディレクトリ内の SVM の名前であり、アクティブディレクトリ内で一意である必要があります。ホームドメインの NetBIOS 名は使用しないでください。NetBIOS 名は 15 文字を超えてはいけません。
- アクティブディレクトリの[完全修飾ドメイン名 (FQDN)]。FQDN は 255 文字を超えることはできません。

> **Note**
>
> FQDN をシングルラベルドメイン (SLD) 形式にすることはできません。Amazon FSx は SLD ドメインをサポートしていません。

- ドメインの DNS サーバーまたはドメインホストの IP アドレスは最大 3 つまで。

  DNS サーバの IP アドレスとアクティブディレクトリドメインコントローラーの IP アドレスは、以下の場合を除き、任意の IP アドレス範囲内に指定できます。

  - AWS リージョン で Amazon Web Services 所有の IP アドレスと競合する IP アドレス。リージョン別の AWS IP アドレスのリストについては、AWS 「 IP アドレスの範囲」を参照してください。
  - 以下の CIDR ブロック範囲内の IP アドレス: 198.19.0.0/16
- Amazon FSx が SVM をアクティブディレクトリドメインに参加させるときに使用するアクティブディレクトリドメインのサービスアカウントのユーザー名とパスワード。サービスアカウント要件の詳細については、アクティブディレクトリサービスアカウントの要件 を参照してください。
- (オプション) SVM に接続させたドメイン内の組織単位 (OU)。

> **Note**
>
> SVM を AWS Directory Service アクティブディレクトリに参加させる場合は、 に関連するディレクトリオブジェクト用に が AWS Directory Service 作成するデフォルトの OU 内にある OU を指定する必要があります AWS。これは、 AWS Directory Service が Active Directory のデフォルト OU `Computers` へのアクセスを提供しないためです。例えば、Active Directory ドメインが の場合`example.com`、次の OU を指定できます: `OU=Computers,OU=example,DC=example,DC=com`。

- (オプション) ファイルシステム上で管理アクションを実行する権限を委任するドメイングループ。例えば、このドメイングループが Windows SMB ファイル共有を管理したり、ファイルやフォルダの所有権を取得したりします。このグループを指定しない場合は、Amazon FSx はデフォルトでこの許可を Active Directory ドメインの Domain Admins グループに委任します。

SVM アクティブディレクトリ設定の管理

このセクションでは、 AWS Management Console、、FSx API、ONTAP AWS CLICLI を使用して以下を実行する方法について説明します。

- 既存の SVM をアクティブディレクトリに接続する
- 既存の SVM アクティブディレクトリ設定の変更
- アクティブディレクトリからの SVMs の削除

SVM をアクティブディレクトリから削除するには、 NetApp ONTAP CLI を使用する必要があります。

トピック

- AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する
- 、 AWS Management ConsoleAWS CLI、および API を使用した既存の SVM アクティブディレクトリ設定の更新
- NetApp CLI を使用した SVM アクティブディレクトリ設定の管理

AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する

既存の SVM をアクティブディレクトリに接続するには、次の手順に従います。この手順では、SVM はまだアクティブディレクトリに参加していません。

SVM をアクティブディレクトリ (AWS Management Console) に接続するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. アクティブディレクトリに結合する SVM を選択します。
   - 左のナビゲーションペインで、[ファイルシステム] を選択し、次に更新する ONTAP ファイルシステムを SVM で選択します。
   - ストレージ仮想マシン タブを選択します。

     -または-
   - 利用可能なすべての SVM のリストを表示するには、左側のナビゲーションペインで [ONTAP] を展開し、[ストレージ仮想マシン] を選択します。のアカウント内のすべての SVMs のリスト AWS リージョン が表示されます。

   リストからアクティブディレクトリに結合する SVM を選択します。

3. SVM の[概要]パネルの右上で、[アクション] > [アクティブディレクトリに接続/更新] を選択します。[SVM をアクティブディレクトリに接続する]ウィンドウが表示されます。
4. SVM を接続させるアクティブディレクトリの次の情報を入力します。

   - SVM 用に作成するアクティブディレクトリコンピュータオブジェクトの NetBIOS 名。これはアクティブディレクトリ内の SVM の名前であり、アクティブディレクトリ内で一意である必要があります。ホームドメインの NetBIOS 名は使用しないでください。NetBIOS 名は 15 文字を超えてはいけません。
   - アクティブディレクトリの[完全修飾ドメイン名 (FQDN)]。ドメイン名は 255 文字を超えてはいけません。
   - DNS サーバーの IP アドレス - ドメインの DNS サーバーの IPv4 アドレス。
   - サービスアカウントのユーザー名 - 既存のアクティブディレクトリのサービスアカウントのユーザー名。ドメインのプレフィックスまたはサフィックスを含めないでください。たとえば、`EXAMPLE\ADMIN` には `ADMIN` のみを使用します。
   - サービスアカウントのパスワード - サービスアカウントのパスワード。
   - パスワードの確認 - サービスアカウントのパスワード。
   - (オプション) [組織単位 (OU)] - SVM に接続させる組織単位の識別パス名。
   - 委任されたファイルシステム管理者グループ - ファイルシステムを管理できる Active Directory 内のグループ名。

     を使用している場合は AWS Managed Microsoft AD、 AWS が委任した FSx 管理者、 AWS が委任した管理者などのグループ、または OU に委任されたアクセス許可を持つカスタムグループを指定する必要があります。

     セルフマネージド Active Directory に参加している場合は、Active Directory 内のグループの名前を使用します。デフォルトのグループは `Domain Admins` です。
5. 「アクティブディレクトリの結合」を選択し、指定した設定を使用して SVM をアクティブディレクトリに結合します。

SVM をアクティブディレクトリ (AWS CLI) に接続するには

- FSx for ONTAP SVM をアクティブディレクトリに結合するには、次の例に示すようにupdate-storage-virtual-machine、 CLI コマンド (または同等の UpdateStorageVirtualMachine API オペレーション) を使用します。

```
aws fsx update-storage-virtual-machine \
```

```
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

ストレージ仮想マシンが正常に作成されると、次の例で示すように、Amazon FSx はその説明を JSON 形式で返します。

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
```

```
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

、 AWS Management ConsoleAWS CLI、および API を使用した既存の SVM アクティブディレクトリ設定の更新

次の手順を使用して、既にアクティブディレクトリに接続している SVM のアクティブディレクトリ設定を更新します。

SVM アクティブディレクトリ設定を更新するには (AWS Management Console)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 更新する SVM を次のように選択します。

   - 左のナビゲーションペインで、[ファイルシステム] を選択し、次に SVM を更新する ONTAP ファイルシステムを選択します。
   - ストレージ仮想マシン タブを選択します。

     -または-

   - 利用可能なすべての SVM のリストを表示するには、左側のナビゲーションペインで [ONTAP] を展開し、[ストレージ仮想マシン] を選択します。

更新する SVM をリストから選択します。

3. SVM の [概要] パネルで、[アクション] > [アクティブディレクトリに接続/更新] を選択します。[SVM アクティブディレクトリ設定の更新]ウィンドウが表示されます。
4. このウィンドウで、次の Active Directory 設定プロパティを更新できます。
   - [DNS サーバーの IP アドレス] - ドメインの DNS サーバーの IPv4 アドレス。
   - サービスアカウントのユーザー名 - 既存のアクティブディレクトリのサービスアカウントのユーザー名。ドメインのプレフィックスまたはサフィックスを含めないでください。`EXAMPLE\ADMIN` の場合は、`ADMIN` を使用します。
   - サービスアカウントのパスワード – Active Directory サービスアカウントのパスワード。
5. 更新内容を入力した後、[アクティブディレクトリの更新] を選択して変更を加えます。

次の手順を使用して、既にアクティブディレクトリに接続している SVM のアクティブディレクトリ設定を更新します。

SVM アクティブディレクトリ設定を更新するには (AWS CLI)

- AWS CLI または API を使用して SVM のアクティブディレクトリ設定を更新するには、次の例に示すようにupdate-storage-virtual-machine、 CLI コマンド (または同等の UpdateStorageVirtualMachine API オペレーション) を使用します。

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

NetApp CLI を使用した SVM アクティブディレクトリ設定の管理

NetApp ONTAP CLI を使用して、SVM をアクティブディレクトリに接続および接続解除したり、既存の SVM アクティブディレクトリ設定を変更したりできます。

ONTAP CLI を使用して SVM をアクティブディレクトリに接続する

次の手順で説明するように、ONTAP CLI を使用して既存の SVMs をアクティブディレクトリに接続できます。これは、SVM がすでにアクティブディレクトリに参加している場合でも実行できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. 完全なディレクトリ DNS 名 (corp.example.com) と少なくとも 1 つの DNS サーバーの IP アドレスを指定して、Active Directory の DNS エントリを作成します。

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

   DNS サーバーへの接続を検証するには、次のコマンドを実行します。*svm_name* を自分の情報に置き換えます。

   ```
   FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                               Name Server
   Vserver       Name Server     Status       Status Details
   ------------- --------------- ------------ --------------------------
   svm_name      172.31.14.245   up           Response time (msec): 0
   svm_name      172.31.25.207   up           Response time (msec): 1
   2 entries were displayed.
   ```

3. SVM を Active Directory に参加させるには、次のコマンドを実行します。アクティブディレクトリにまだ存在しない computer_name を指定し、-domain のディレクトリ DNS 名を指定する必要があることに注意してください。-OU には、SVM を参加させる OU と、DC 形式の完全な DNS 名を入力します。

   ```
   ::>vserver cifs create -vserver svm_name -cifs-server computer_name -
   domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
   ```

Active Directory 接続のステータスを確認するには、次のコマンドを実行します。

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
                    Cifs NetBIOS Name : svm_netBIOS_name
                          Cifs Status : Running
                                 Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. この参加後に共有にアクセスできない場合は、共有にアクセスするために使用しているアカウントにアクセス許可が付与されていることを確認してください。例えば、 AWS マネージド Active Directory でデフォルトAdminアカウント (委任管理者) を使用している場合は、ONTAP で次のコマンドを実行する必要があります。netbios_domain は Active Directory のドメイン名に対応します (corp.example.com の場合、ここで使用される netbios_domain は example です)。

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

ONTAP CLI を使用してアクティブディレクトリの設定を変更する

ONTAP CLI を使用して、既存の Active Directory 設定を変更できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. 次のコマンドを実行して、SVM の CIFS サーバーを一時的に停止します。

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Active Directory の DNS エントリを変更する必要がある場合は、次のコマンドを実行します。

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

vserver services name-service dns check -vserver svm_name コマンドを使用して、Active Directory の DNS サーバーへの接続ステータスを検証できます。

```
::>vserver services name-service dns check -vserver svm_name
                             Name Server
Vserver       Name Server    Status       Status Details
------------- -------------- ------------ --------------------------
svmciad       dns_ip_1       up           Response time (msec): 1
svmciad       dns_ip_2       up           Response time (msec): 1
2 entries were displayed.
```

4. Active Directory の設定自体を変更する必要がある場合は、次のコマンドを使用して既存のフィールドを変更できます。

   - *computer_name* (SVM の NetBIOS (マシンアカウント) 名を変更する場合)。
   - *domain_name* (ドメインの名前を変更する場合)。これは、このセクションのステップ 3 に記載されている DNS ドメインエントリに対応している必要があります (corp.example.com)。
   - organizational_unit (OU (OU=Computers,OU=example,DC=corp,DC=example,DC=com) を変更する場合)。

   このデバイスを Active Directory に参加させるために使用した Active Directory 認証情報を再入力する必要があります。

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

`vserver cifs check -vserver svm_name` コマンドを使用して、Active Directory 接続の接続ステータスを確認できます。

5. Active Directory と DNS の設定の変更が完了したら、次のコマンドを実行して CIFS サーバーをバックアップします。

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

NetApp ONTAP CLI を使用して SVM からアクティブディレクトリの接続を解除する

NetApp ONTAP CLI は、以下の手順に従って SVM をアクティブディレクトリから接続解除するためにも使用できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. 次のコマンドを実行して、Active Directory からデバイスの接続を解除した CIFS サーバーを削除します。ONTAP が SVM のマシンアカウントを削除するには、SVM をアクティブディレクトリに接続させるために最初に使用した認証情報を指定します。

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Active Directory の DNS エントリを変更する必要がある場合は、次のコマンドを実行します。

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:
```

```
Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. 次のコマンドを実行して、Active Directory の DNS サーバーを削除します。

```
::vserver services name-service dns delete -vserver svm_name
```

を として削除dnsする必要があることを示す次のような警告が表示されns-switch、このデバイスを Active Directory に再結合する予定がない場合は、ns-switchエントリを削除できます。

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (オプション) 以下のコマンドを実行して、dns の ns-switch エントリを削除します。ソースの順序を確認し、リストされている他のソースのみが含まれるように sources を変更して、hosts データベースの dns エントリを削除します。この例では、他のソースは files のみです。

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (オプション) データベースホストが files のみを含むように sources を変更して dns エントリを削除します。

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx for NetApp ONTAP のパフォーマンス

Amazon FSx for NetApp ONTAP ファイルシステムのパフォーマンスの概要を以下に示します。使用可能なパフォーマンスとスループットのオプション、および便利なパフォーマンスのヒントについて説明します。

トピック

FSx for ONTAP ファイルシステムのパフォーマンスの測定方法

ファイルシステムのパフォーマンスは、レイテンシー、スループット、1 秒あたりの I / O オペレーション (IOPS) によって測定されます。

レイテンシー

Amazon FSx for NetApp ONTAP は、ソリッドステートドライブ (SSD) ストレージでミリ秒未満のファイルオペレーションレイテンシーを提供し、容量プールストレージでは数十ミリ秒のレイテンシーを提供します。さらに、Amazon FSx では、各ファイルサーバーに、NVMe (non-volatile memory express) ドライブとインメモリの 2 レイヤーのリードキャッシュがあり、最も頻繁に読み取られるデータにアクセスする場合のレイテンシーがさらに低くなります。

スループットと IOPS

各 Amazon FSx ファイルシステムは、最大、数十 GB/秒 のスループットと数百万の IOPS を提供します。ファイルシステム上でワークロードが駆動できるスループットと IOPS の具体的な量は、ファイルシステムの合計スループットキャパシティとストレージ容量の設定、およびワークロードの性質 (アクティブなワーキングセットのサイズなど) によって異なります。

SMB マルチチャネルおよび NFS nconnect のサポート

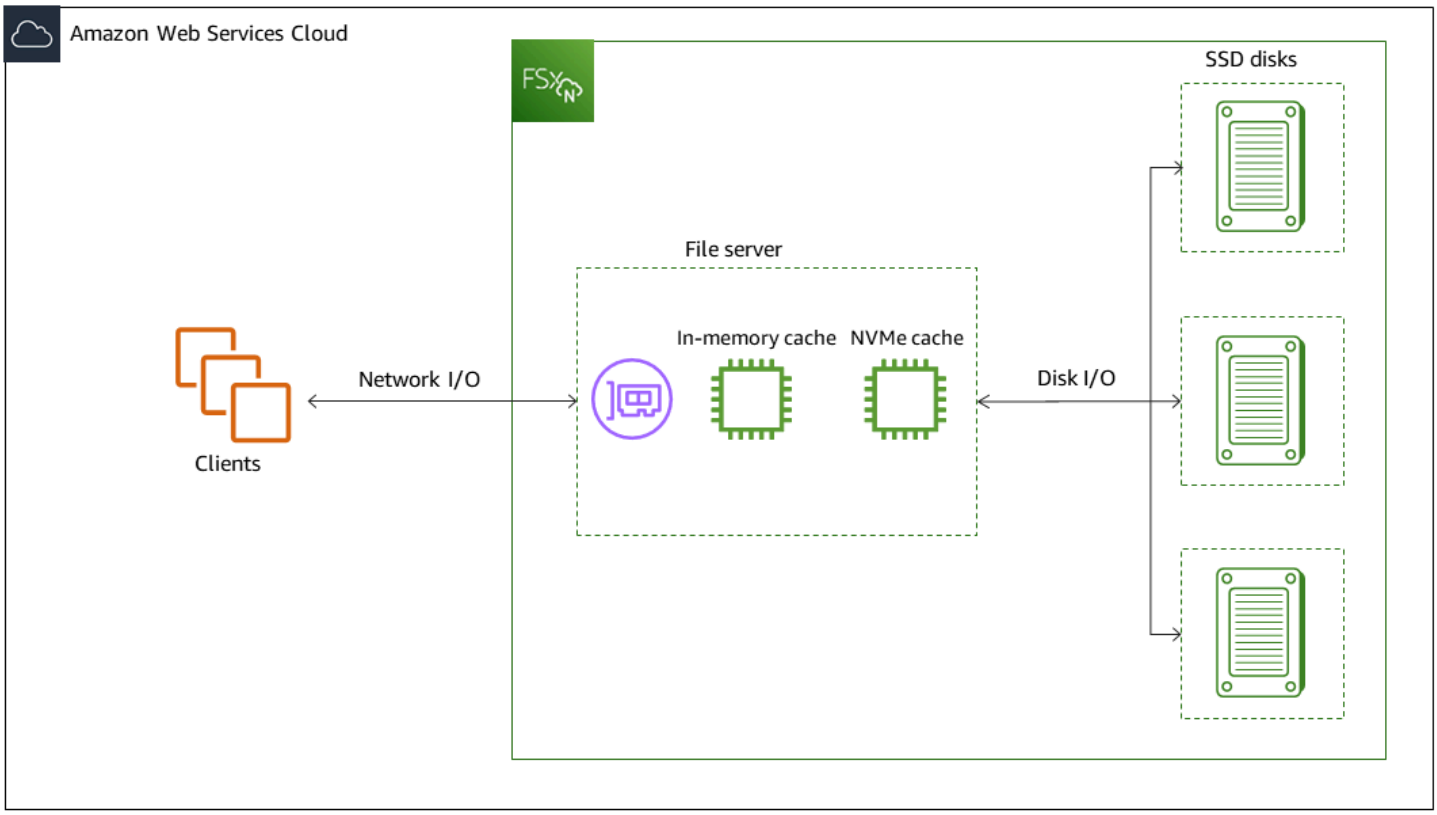
Amazon FSx では、1 つの SMB セッションで ONTAPとクライアント間に複数の接続を提供するように SMB マルチチャネルを設定できます。SMB マルチチャネルは、クライアントとサーバ間の複数のネットワーク接続を同時に使用して、ネットワーク帯域幅を集約し、最大限の利用率を実現します。NetApp ONTAP CLI を使用して SMB マルチチャネルを設定する方法については、「パフォーマンスと冗長性のための SMB マルチチャネルの設定」を参照してください。

NFS クライアントは、nconnect マウントオプションを使用して、単一の NFS マウントに関連付けられた複数の TCP 接続 (最大 16) を持つことができます。このような NFS クライアントは、ラウンドロビン方式でファイル操作を複数の TCP 接続に多重化するため、使用可能なネットワーク帯域幅から高いスループットが得られます。NFSv3 と NFSv4.1+ は nconnect をサポートします。「Amazon EC2 instance network bandwidth」(Amazon EC2 インスタンスのネットワーク帯域幅) に、ネットワークフローあたりの全二重 5 Gbps の帯域幅制限を示します。nconnect または SMB マルチチャネルで複数のネットワークフローを使用することにより、この制限を克服できます。クライアントバージョンで nconnect がサポートされているかどうかを確認するには、NFS クライアントのドキュメントを参照してください。NetApp ONTAP のサポートの詳細についてはnconnect、ONTAPNFSv4.1 のサポート」を参照してください。

パフォーマンスの詳細

Amazon FSx for NetApp ONTAP のパフォーマンスモデルについて詳しく理解するには、Amazon FSx ファイルシステムのアーキテクチャコンポーネントを調べることができます。クライアントコンピューティングインスタンスは、 AWS に存在するかオンプレミスに存在するかにかかわらず、1 つ以上の Elastic Network Interface (ENI) を介してファイルシステムにアクセスします。ネットワークインターフェイスは、ファイルシステムに関連付ける Amazon VPC に存在します。各ファイルシステムの ENI の背後には、ネットワーク経由でNetApp ONTAPファイルシステムにアクセスするクライアントにデータを提供するファイルサーバーがあります。Amazon FSx は、各ファイルサーバーで高速なインメモリキャッシュと NVMe キャッシュを提供し、最も頻繁にアクセスされるデータのパフォーマンスを向上させます。各ファイルサーバには、ファイルシステムデータをホストする SSD ディスクが添付されます。

これらのコンポーネントを次の図表で説明します。



ネットワークインターフェイス、インメモリキャッシュ、NVMe キャッシュ、ストレージボリュームなどのアーキテクチャコンポーネントに対応するのが、全体的なスループットと IOPS パフォーマンスを決定する Amazon FSx for NetApp ONTAP ファイルシステムの主なパフォーマンス特性です。

- ネットワーク I / O パフォーマンス:クライアントとファイルサーバー間のリクエストのスループット / IOPS (集計)
- ファイルサーバー上のインメモリおよび NVMe キャッシュサイズ: キャッシュに対応できるアクティブなワーキングセットのサイズ
- ディスク I / O パフォーマンス:ファイルサーバーとストレージディスク間のリクエストのスループット / IOPS

ファイルシステムのパフォーマンス特性を決定する要因として、SSD IOPS の合計量と、それに設定するスループットキャパシティの 2 つがあります。最初の 2 つのパフォーマンス特性 (ネットワーク I/O パフォーマンス、インメモリ、NVMe キャッシュサイズ) はスループットキャパシティによってのみ決定され、3 番目のパフォーマンス特性 (ディスク I / O パフォーマンス) はスループットキャパシティと SSD IOPS の組み合わせによって決まります。

ファイルベースのワークロードは通常、スパイクであり、バースト間のアイドル時間が長い I / O が短く、強烈な期間によって特徴付けられます。スパイクの多いワークロードをサポートするために、ファイルシステムが 24 時間年中無休で維持できるベースライン速度に加えて、Amazon FSx は、ネットワーク I / O とディスク I / O の両方のオペレーションで一定期間より高速にバーストする機能を提供します。Amazon FSx は、ネットワーク I / O クレジットメカニズムを使用して、平均使用率に基づいてスループットと IOPS を割り当てます。ファイルシステムでは、スループットと IOPS 使用率がベースライン制限を下回るとクレジットが計上され、I / O 操作の実行時にこれらのクレジットを使用できます。

書き込み操作は、読み取り操作の 2 倍のネットワーク帯域幅を使用します。書き込み操作はセカンダリファイルサーバー上でレプリケートされる必要があるため、1 回の書き込み操作で 2 倍のネットワークスループットが発生します。

デプロイタイプがパフォーマンスに与える影響

FSx for ONTAP では、2 種類のファイルシステムを作成できます。ファイルサーバーの高可用性 (HA) ペアが 1 つだけのファイルシステムは、スケールアップファイルシステムと呼ばれます。HA ペアが複数のファイルシステムは、スケールアウトファイルシステムと呼ばれます。詳細については、「高可用性 (HA) ペア」を参照してください。

FSx for ONTAP マルチ AZ とシングル AZ ファイルシステムでは、一貫してサブミリ秒のレイテンシーで SSD ストレージ内のファイル操作を可能にし、さらに容量プールストレージ内のデータには数十ミリ秒のレイテンシーでアクセスできます。さらに、次の要件を満たすファイルシステムは、読み取り遅延を低減し、頻繁に読み取りされるデータの IOPS を向上させる次のような NVMe 読み取りキャッシュを提供します：

- マルチ AZ ファイルシステム
- 2022 年 11 月 28 日以降に作成された、スループットキャパシティが少なくとも 2 GBps のシングル AZ スケールアップファイルシステム

次の表は、高可用性 (HA) ペアの数や可用性などの要因に応じて、ファイルシステムがスケールアップできるスループット容量を示しています AWS リージョン 。

Scale-up

これらの性能仕様は、スケールアップファイルシステムに適用されます。

スケールアップファイルシステムの HA ペアあたりの SSD ストレージの最大スループット

	米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、欧州 (アイルランド)		FSx for ONTAP AWS リージョン が利用可能なその他すべての	
	読み込みスループット (MBps)	書き込みスループット (MBps)	読み込みスループット (MBps)	書き込みスループット (MBps)
シングル AZ	4,096*	1,000	2,048	750
マルチ AZ	4,096*	1,800	2,048	1,300

> **Note**
>
> * 4 GBps のスループットキャパシティをプロビジョニングするには、ファイルシステムに最低 5,120 GiB の SSD ストレージ容量と 160,000 の SSD IOPS を設定する必要があります。

Scale-out

これらの性能仕様は、スケールアウトファイルシステムに適用されます。

スケールアウトファイルシステムの HA ペアあたりの SSD ストレージの最大スループット

	読み込みスループット (MBps)	書き込みスループット (MBps)
シングル AZ スケールアウト	6,144*	1,100*

> **Note**
>
> * HA ペアごと (最大 12)。詳細については、「高可用性 (HA) ペア」を参照してください。

ストレージ容量のパフォーマンスへの影響

ファイルシステムが達成できる最大ディスクスループットと IOPS レベルは、次のうち低くなります。

- ファイルシステム用に選択したスループットキャパシティに基づく、ファイルサーバーによって提供されるディスクパフォーマンスレベル
- ファイルシステム用にプロビジョニングした SSD IOPS の数によって提供されるディスクパフォーマンスレベル

デフォルトでは、ファイルシステムの SSD ストレージは、最大次のレベルのディスクスループットと IOPS を提供します。

- ディスクスループット (ストレージの TiB あたり MBps): 768
- ディスク IOPS (ストレージの TiB あたりの IOPS): 3,072

スループット容量がパフォーマンスに与える影響

すべての Amazon FSx ファイルシステムには、ファイルシステムの作成時に設定するスループットキャパシティがあります。ファイルシステムのスループットキャパシティによって、ネットワーク I/O パフォーマンスのレベル、つまりファイルシステムをホストする各ファイルサーバーが、ファイルシステムにアクセスするクライアントにネットワーク経由でファイルデータを提供できる速度が決まります。スループットキャパシティが高くなると、各ファイルサーバーでデータをキャッシュするためのメモリと不揮発性メモリエクスプレス (NVMe) ストレージが増え、各ファイルサーバーでサポートされるディスク I/O パフォーマンスが向上します。

オプションで、ファイルシステムを作成するときに、より高いレベルの SSD IOPS をプロビジョニングできます。ファイルシステムが達成できる SSD IOPS の最大レベルは、追加の SSD IOPS をプロビジョニングする場合でも、ファイルシステムのスループットキャパシティによって決定されます。

次の表に、スループットキャパシティの完全な仕様と、ベースライン、バーストレベル、および対応する AWS リージョンのファイルサーバでのキャッシュのメモリ量を示します。

Single-AZ (scale-up)

これらの性能仕様は、指定した AWS リージョンで 2022 年 11 月 28 日以降に作成されたシングル AZ スケールアップファイルシステムに適用されます。

米国東部 (バージニア北部) 、 AWS リージョン米国東部 (オハイオ) 、米国西部 (オレゴン) 、欧州 (アイルランド) の におけるファイルシステムのパフォーマンス仕様

FSx スループットキャパシティ (MBps)	ネットワークスループットキャパシティ (MBps)		ネットワーク IOPS	インメモリキャッシュ (GB)	NVMe 読み取りキャッシュ (GB)	ディスクスループット (MBps)		SSD ドライブ IOPS *	
	[Baseline] (ベースライン)	[Burst] (バースト)				[Baseline] (ベースライン)	[Burst] (バースト)	[Baseline] (ベースライン)	[Burst] (バースト)
128	188	1,500	数万、ベースライン	16	–	128	1,250	6,000	40,000
256	375	1,500		32	–	256	1,250	12,000	40,000
512	750	1,500	数十万、ベースライン	64	–	512	1,250	20,000	40,000
1,024	1,500	–		128	–	1,024	1,250	40,000	–
2,048	3,125	–		256	1,900	2,048	–	80,000	–
4,096	6,250	–		512	5,400	4,096	–	160,000	–

> **Note**
>
> * SSD IOPS は、ファイルサーバーのインメモリキャッシュまたは NVMe キャッシュにキャッシュされていないデータにアクセスするときにのみ使用されます。

これらのパフォーマンス仕様は、FSx for ONTAP AWS リージョン が利用可能な他のすべての のシングル AZ スケールアップファイルシステムに適用されます。

FSx for ONTAP AWS リージョン が利用可能な他のすべての のファイルシステムのパフォーマンス仕様

FSx スループットキャパシティ (MBps)	ネットワークスループットキャパシティ (MBps)		ネットワーク IOPS	インメモリキャッシュ (GB)	ディスクスループット (MBps)		SSD ドライブ IOPS *	
	[Baseline] (ベースライン)	[Burst] (バースト)			[Baseline] (ベースライン)	[Burst] (バースト)	[Baseline] (ベースライン)	[Burst] (バースト)
128	150	1,250	数万、ベースライン	16	128	600	6,000	18,750
256	300	1,250		32	256	600	12,000	18,750
512	625	1,250	数十万、ベースライン	64	512	600	18,750	–
1,024	1,500	–		128	1,024	–	40,000	–
2,048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * SSD IOPS は、ファイルサーバーのインメモリキャッシュまたは NVMe キャッシュにキャッシュされていないデータにアクセスするときにのみ使用されます。

Single-AZ (scale-out)

これらの性能仕様は、スケールアウトファイルシステムに適用されます。

スケールアウトファイルシステムの性能仕様

FSx スループットキャパシティ (MBps)	ネットワークスループットキャパシティ (MBps)		ネットワーク IOPS	インメモリキャッシュ (GB)	ディスクスループット (MBps)		SSD ドライブ IOPS *	
	[Baseline] (ベースライン)	[Burst] (バースト)			[Baseline] (ベースライン)	[Burst] (バースト)	[Baseline] (ベースライン)	[Burst] (バースト)
3,072**	6,250	–	数十万、ベースライン	128	3,072	–	100,000	–
6,144**	12,500	–		256	6,144	–	200,000 件の	–

> **Note**
>
> * SSD IOPS は、ファイルサーバーのインメモリキャッシュまたは NVMe キャッシュにキャッシュされていないデータにアクセスするときにのみ使用されます。
> ** HA ペアあたり (最大 12)。詳細については、「高可用性 (HA) ペア」を参照してください。

Multi-AZ (scale-up)

これらの性能仕様は、指定した AWS リージョンで 2022 年 11 月 28 日以降に作成されたマルチ AZ スケールアップファイルシステムに適用されます。

米国東部 (バージニア北部) 、 AWS リージョン米国東部 (オハイオ) 、米国西部 (オレゴン) 、欧州 (アイルランド) の におけるファイルシステムのパフォーマンス仕様

FSx スループットキャパシティ (MBps)	ネットワークスループットキャパシティ (MBps)		ネットワーク IOPS	インメモリキャッシュ (GB)	NVMe キャッシュ (GB)	ディスクスループット (MBps)		SSD ドライブ IOPS *	
	[Baseline] (ベースライン)	[Burst] (バースト)				[Baseline] (ベースライン)	[Burst] (バースト)	[Baseline] (ベースライン)	[Burst] (バースト)
128	188	1,500	数万、ベースライン	16	238	128	1,250	6,000	40,000
256	375	1,500		32	475	256	1,250	12,000	40,000
512	750	1,500	数十万、ベースライン	64	950	512	1,250	20,000	40,000
1,024	1,500	–		128	1,900	1,024	1,250	40,000	–
2,048	3,125	–		256	3,800	2,048	–	80,000	–
4,096	6,250	–		512	7,600	4,096	–	160,000	–

> **Note**
>
> * SSD IOPS は、ファイルサーバーのインメモリキャッシュまたは NVMe キャッシュにキャッシュされていないデータにアクセスするときにのみ使用されます。

これらのパフォーマンス仕様は、FSx for ONTAP AWS リージョン が利用可能な他のすべての のマルチ AZ スケールアップファイルシステムに適用されます。

FSx for ONTAP AWS リージョン が利用可能な他のすべての のファイルシステムのパフォーマンス仕様

FSx スループットキャパシティ (MBps)	ネットワークスループットキャパシティ (MBps)		ネットワーク IOPS	インメモリキャッシュ (GB)	NVMe キャッシュ (GB)	ディスクスループット (MBps)		SSD ドライブ IOPS *	
	[Baseline] (ベースライン)	[Burst] (バースト)				[Baseline] (ベースライン)	[Burst] (バースト)	[Baseline] (ベースライン)	[Burst] (バースト)
128	150	1,250	数万、ベースライン	16	150	128	600	6,000	18,750
256	300	1,250		32	300	256	600	12,000	18,750
512	625	1,250	数十万、ベースライン	64	600	512	600	18,750	–
1,024	1,500	–		128	1,200	1,024	–	40,000	–
2,048	3,125	–		256	2,400	2,048	–	80,000	–

> **Note**
>
> * SSD IOPS は、ファイルサーバーのインメモリキャッシュまたは NVMe キャッシュにキャッシュされていないデータにアクセスするときにのみ使用されます。

例: ストレージ容量とスループットキャパシティ

次の例は、ストレージ容量とスループットキャパシティがファイルシステムのパフォーマンスに与える影響を示しています。

2 TiB の SSD ストレージ容量と 512 MBps のスループットキャパシティで設定されたスケールアップファイルシステムには、次のスループットレベルがあります。

- ネットワークスループット - 625 MBps のベースラインと 1,250 MBps バースト (スループットキャパシティ表を参照)
- ディスクスループット - 512 MBps のベースラインと 600 MBps のバーストです。

したがって、ファイルシステムにアクセスするワークロードは、ファイルサーバーのインメモリキャッシュおよび NVMe キャッシュにキャッシュされたアクティブにアクセスされたデータに対して実行されるファイルオペレーションに対して、最大 625 MBps のベースラインと 1,250 MBps のバーストスループットを駆動できます。

FSx for ONTAP リソースの管理

AWS Management Console、 AWS CLI、ONTAP CLI および API を使用して、FSx for ONTAP リソースに対して次の管理アクションを実行できます。

- ファイルシステム、ストレージ仮想マシン (SVMs)、ボリューム、バックアップ、タグの作成、一覧表示、更新、削除。
- アクセスの管理、管理アカウントとパスワード、パスワード要件、SMB と iSCSI プロトコル、既存のファイルシステムのマウントターゲットのネットワークアクセシビリティ

トピック

FSx for ONTAP ファイルシステムの管理

ファイルシステムは オンプレミス ONTAP クラスターに類似した Amazon FSx のプライマリリソースです。ファイルシステムの SSD ストレージ容量とスループットキャパシティを指定し、ファイルシステムが作成される仮想プライベートクラウド (VPC) を選択します。各ファイルシステムに

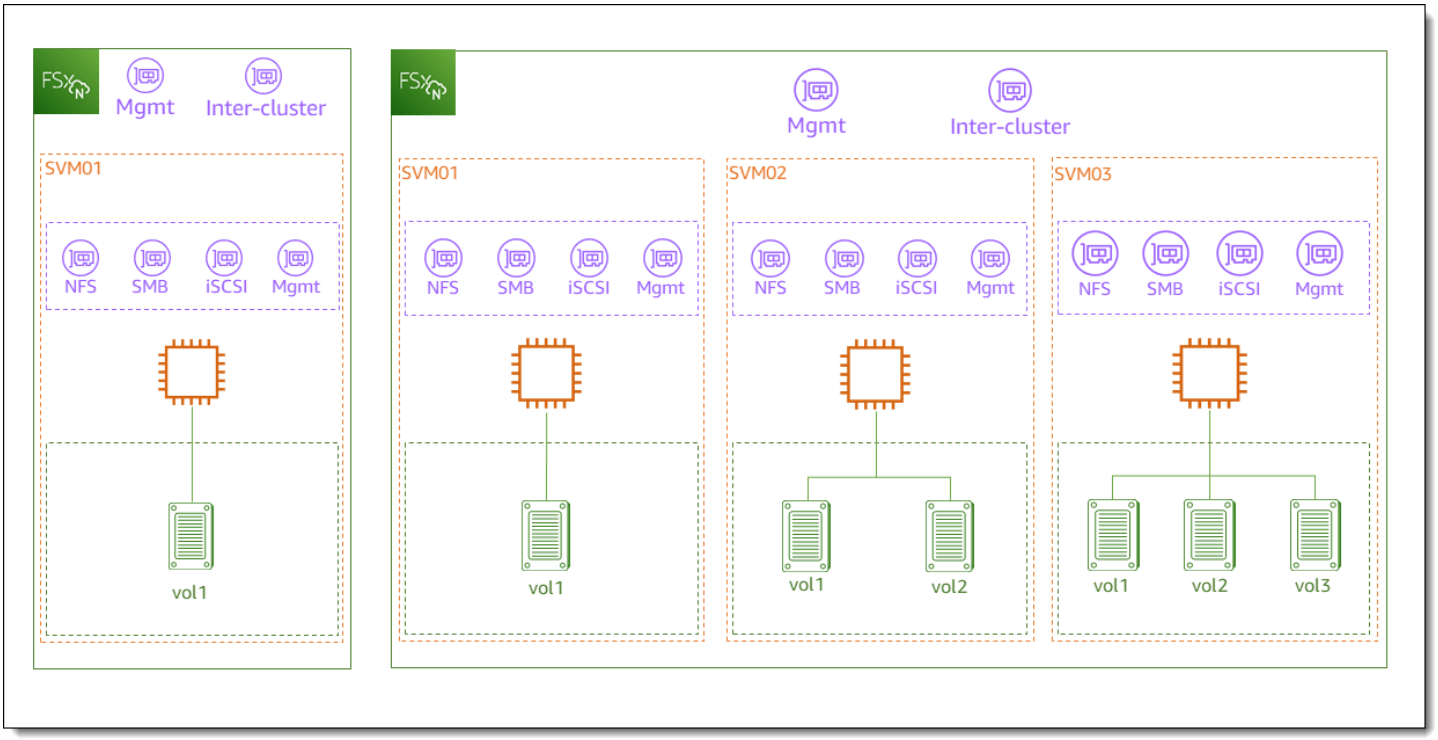
は、ONTAP CLI または REST API を使用してリソースとデータを管理するために使用できる管理エンドポイントがあります。

ファイルシステムリソース

Amazon FSx for NetApp ONTAP ファイルシステムは、次のプライマリリソースで構成されます。

- ファイルシステム自体の物理的なハードウェアで、ファイルサーバーや記憶媒体などが含まれる。
- ストレージ仮想マシン (SVM) をホストする 1 つまたは複数の高可用性 (HA) ファイルサーバーペア。スケールアップファイルシステムには 1 つの HA ペアがあり、スケールアウトファイルシステムには 2 つ以上の HA ペアがあります。各 HA ペアにはアグリゲートと呼ばれるストレージプールがあります。すべての HA ペアにわたるアグリゲートの集合が SSD ストレージ階層を構成します。
- ファイルシステムボリュームをホストし、独自の認証情報とアクセス管理を行う 1 つ以上のストレージ仮想マシン (SVM)。
- データを仮想的に整理し、クライアントによってマウントされる 1 つ以上のボリューム。

次の図は、1 つの HA ペアを持つスケールアップ FSx for ONTAP ファイルシステムのアーキテクチャと、そのプライマリリソース間の関係を示しています。左側の FSx for ONTAP ファイルシステムは、1 つの SVM と 1 つのボリュームを備えた最も単純なファイルシステムです。右側のファイルシステムには複数の SVM があり、一部の SVM には複数のボリュームがあります。ファイルシステムと SVMs にはそれぞれ複数の管理エンドポイントがあり、SVMs にもデータアクセスエンドポイントがあります。



FSx for ONTAP ファイルシステムを作成するときに、次のプロパティを定義します。

- デプロイタイプ — ファイルシステムのデプロイタイプ (マルチ AZ またはシングル AZ)。シングル AZ ファイルシステムは、データをレプリケートし、単一のアベイラビリティーゾーン内で自動フェイルオーバーを行い、スケールアウトファイルシステムを提供します。マルチ AZ ファイルシステムは、こちらもデータをレプリケートし、同じ AWS リージョン内の複数のアベイラビリティーゾーンにまたがるフェイルオーバーをサポートすることによって、回復力を高めます。
- ストレージ容量 – これは SSD ストレージの量で、スケールアップファイルシステムでは最大 192 テビバイト (TiB)、スケールアウトファイルシステムでは最大 1 ペビバイト (PiB) です。
- SSD IOPS – デフォルトでは、SSD ストレージにはギガバイトあたり 3 つの SSD IOPS が含まれます (ファイルシステムの設定でサポートされている最大値まで)。必要に応じて、追加の SSD IOPS をプロビジョンすることもできます。
- スループットキャパシティ - ファイルサーバがデータを処理できる持続速度。
- ネットワーク - ファイルシステムが作成する管理エンドポイントとデータアクセスエンドポイントの VPC とサブネット。マルチ AZ ファイルシステムの場合、IP アドレスの範囲とルートテーブルも定義します。
- 暗号化 — 保管中のファイルシステムデータを暗号化するために使用される AWS Key Management Service （ AWS KMS) キー。

- 管理者アクセス - `fsxadmin` ユーザーのパスワードを指定できます。このユーザーを使用して、NetApp ONTAP CLI と REST API を使用してファイルシステムを管理できます。

ONTAP CLI または REST API を使用して、FSx for NetApp ONTAP ファイルシステムを管理できます。Amazon FSx ファイルシステムと別の ONTAP デプロイ (別の Amazon FSx ファイルシステムを含む) の間に SnapMirror または の SnapVault 関係を設定することもできます。各 FSx for ONTAP ファイルシステムには、 NetApp アプリケーションへのアクセスを提供する次のファイルシステムエンドポイントがあります。

- 管理 – このエンドポイントを使用して、セキュアシェル (SSH) 経由で ONTAP CLI にアクセスする NetAppか、ファイルシステムで NetApp ONTAP REST API を使用します。
- クラスター間 — を使用してレプリケーションを設定する場合、 NetApp SnapMirror または を使用してキャッシュする場合は、このエンドポイントを使用します NetApp FlexCache。

詳細については、「NetApp アプリケーションを使用した FSx for ONTAP リソースの管理」および「を使用したスケジュールされたレプリケーション NetApp SnapMirror」を参照してください。

高可用性 (HA) ペア

各 FSx for ONTAP ファイルシステムには、アクティブ/スタンバイ構成のファイルサーバーの 1 つまたは複数の高可用性 (HA) ペアが搭載されています。この構成では、トラフィックをアクティブに処理する優先ファイルサーバーと、アクティブサーバーが使用できない場合に処理を引き継ぐセカンダリファイルサーバーがあります。FSx for ONTAP スケールアップファイルシステムには 1 つの HA ペアが搭載されており、最大 4 GBps のスループットキャパシティと 160,000 SSD IOPS を実現します。FSx for ONTAP スケールアウトファイルシステムは、最大 12 個の HA ペアを搭載しており、最大 72 GBps のスループットキャパシティと 2,400,000 SSD IOPS (HA ペアあたり 6 GBps のスループットキャパシティと 200,000 SSD IOPS) を提供します。

Amazon FSx コンソールからファイルシステムを作成する場合、Amazon FSx は、必要な SSD ストレージに基づいて使用すべき HA ペアの数を推奨します。ワークロードとパフォーマンス要件に基づいて、HA ペアの数を手動で選択することもできます。ファイルシステム要件が最大 4 GBps のスループットキャパシティと 160,000 SSD IOPS で満たされる場合は 1 つの HA ペアを使用し、ワークロードに高いレベルのパフォーマンススケーラビリティが必要な場合は複数の HA ペアを使用することをお勧めします。

各 HA ペアには、物理ディスクの論理セットである 1 つのアグリゲートがあります。

> **Note**
>
> HA ペアを既存のファイルシステムに追加することはできません。代わりに、 を使用するかSnapMirror、バックアップから新しいファイルシステムにデータを復元することで AWS DataSync、ファイルシステム間で (異なる HA ペアで) データを移行できます。

FSx for ONTAP ファイルシステムの作成

このセクションでは、Amazon FSx コンソールまたは Amazon FSx API を使用して AWS CLI FSx for ONTAP ファイルシステムを作成する方法について説明します。ファイルシステムは、所有している Virtual Private Cloud (VPC) または別の が共有している VPC AWS アカウント で作成できます。参加者が属する VPC でマルチ AZ ファイルシステムを作成する際には、考慮事項があります。これらの考慮事項については、このトピックで説明します。

デフォルトでは、Amazon FSx コンソールから新しいファイルシステムを作成すると、Amazon FSx は自動的に単一のストレージ仮想マシン (SVM) と 1 つのボリュームを持つファイルシステムを作成し、ネットワークファイルシステム (NFS) プロトコル経由で Linux インスタンスからデータにすばやくアクセスできるようにします。ファイルシステムの作成時に、オプションで SVM をアクティブディレクトリに結合させて、サーバーメッセージブロック (SMB) プロトコル経由で Windows および macOS クライアントからのアクセスを有効にすることもできます。ファイルシステムの作成後、必要に応じて追加の SVM とボリュームを作成できます。

ファイルシステムの作成方法 (コンソール)

この手順では、必要に応じてカスタマイズした設定で スタンダードの作成 を使用して、FSx for ONTAP ファイルシステムを作成します。クイック作成 オプションを使用してデフォルトの設定パラメータセットを持つファイルシステムを迅速に作成する方法については、「ステップ 1: Amazon FSx for NetApp ONTAP ファイルシステムを作成する」を参照してください。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ダッシュボードから、[ファイルシステムを作成] を選択します。
3. ファイルシステムタイプの選択ページで、ファイルシステムオプション で Amazon FSx for NetApp ONTAP を選択し、次へ を選択します。
4. [作成方法] セクションで、[スタンダード作成] を選択します。
5. [ファイルシステムの詳細] セクションで、以下の情報を入力します。

- ファイルシステム名 - オプション にファイルシステム名を入力します。ファイルシステムに名前を付けると、ファイルシステムを簡単に検索および管理できます。最大 256 文字の Unicode 文字、空白、数字、および特殊文字 (+ - = . _ : /) を使用できます。
- [Deployment type] (デプロイタイプ) では [Multi-AZ] (マルチ AZ) または [Single-AZ] (シングル AZ) を選択します。
  - Multi-AZ (マルチ AZ) ファイルシステムは、データをレプリケートし、同じ AWS リージョン内の複数のアベイラビリティーゾーンにまたがるフェイルオーバーをサポートします。
  - [Single-AZ] (シングル AZ) ファイルシステムでは、データをレプリケートし、単一のアベイラビリティーゾーン内で自動フェイルオーバーを行います。

  > **Note**
  >
  > 2 つ以上の高可用性 (HA) ペア (最大 12) を持つファイルシステムを作成する場合は、シングル AZ を選択します。詳細については、「高可用性 (HA) ペア」を参照してください。

  詳細については、「可用性と耐久性」を参照してください。
- [Storage capacity] (ストレージ容量) では、ファイルシステムのストレージ容量を GiB 単位で入力します。1,024 ~ 1,048,576 GiB (最大 1 ペビバイト [PiB]) の範囲の任意の整数を入力します。

  ファイルシステムの作成後でも、いつでも必要に応じてストレージ容量を増やすことができます。詳細については、「ストレージ容量の管理」を参照してください。
- Provisioned SSD IOPS でファイルシステムの IOPS 数をプロビジョニングするには、2 つのオプションがあります。
  - Amazon FSx で SSD ストレージの GiB あたり 3 IOPS を自動的にプロビジョニングする場合は、[Automatic] (自動) (デフォルト) を選択します。
  - IOPS の数を指定する場合は、[User-provisioned] (ユーザープロビジョニング) を選択します。ファイルシステムごとに最大 200,000 SSD IOPS をプロビジョニングできます。

  > **Note**
  >
  > プロビジョニングされた SSD IOPS は、ファイルシステムの作成後、増やすことができます。ファイルシステムで達成できる SSD IOPS の最大レベルは、追加の SSD IOPS をプロビジョニングする場合でも、ファイルシステムのスループットキャパシ

ティによって決まることに注意してください。詳細については、「スループット容量がパフォーマンスに与える影響」および「ストレージ容量の管理」を参照してください。

- [スループットキャパシティ] については、1 秒あたりのメガバイト数 (MBps) でスループットキャパシティを決定する方法が 2 つあります。
  - 選択したストレージ容量に基づいて Amazon FSx でスループットキャパシティを自動的に選択するように設定するには、[推奨されるスループット容量] を選択します。
  - スループットキャパシティの値を指定する場合は、[スループット容量を指定] を選択します。このオプションを選択すると、選択したデプロイタイプに基づいて入力される [スループットキャパシティ] ドロップダウンが表示されます。HA ペアの数 (最大 12) を選択することもできます。詳細については、「高可用性 (HA) ペア」を参照してください。

  [Throughput capacity] (スループットキャパシティ) は、ファイルシステムをホストするファイルサーバがデータを提供できる持続速度です。詳細については、「Amazon FSx for NetApp ONTAP のパフォーマンス」を参照してください。

6. [ネットワーク] セクションで、次の情報を入力します。

   - [Virtual Private Cloud (VPC)] (仮想プライベートクラウド (VPC)) で、ファイルシステムに関連付ける VPC を選択します。
   - [VPC セキュリティグループ] では、ファイルシステムのネットワークインターフェイスに関連付けるセキュリティグループを選択できます。指定しない場合、Amazon FSx は VPC のデフォルトセキュリティグループをファイルシステムに関連付けます。
   - ファイルサーバ用の [Subnet] (サブネット) を指定します。マルチ AZ ファイルシステムを作成する場合は、スタンバイファイルサーバーの [Standby subnet] (スタンバイサブネット) も選択します。
   - (マルチ AZ のみ) [VPC route tables] (VPC ルートテーブル) で、ファイルシステムのエンドポイントを作成する VPC ルートテーブルを指定します。クライアントが配置されているサブネットに関連付けられている、すべての VPC ルートテーブルを選択します。デフォルトでは、Amazon FSx は VPC のデフォルトルートテーブルを選択します。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

     Note

     Amazon FSx は、タグベースの認証を使用してマルチ AZ ファイルシステムのこれらのルートテーブルを管理します。これらのルートテーブルには `Key: AmazonFSx;`

`Value: ManagedByAmazonFSx` のタグが付けられています。を使用して FSx for ONTAP マルチ AZ ファイルシステムを作成する場合は、 `Key: AmazonFSx; Value: ManagedByAmazonFSx` タグを手動で追加 AWS CloudFormation することをお勧めします。

- (マルチ AZ のみ) [Endpoint IP address range] (エンドポイント IP アドレスの範囲) で、ファイルシステムにアクセスするためのエンドポイントが作成され、IP アドレスの範囲を指定します。

  エンドポイント IP アドレスの範囲には、次の 3 つのオプションがあります。

  - [Unallocated IP address range from your VPC] (VPC からの未割り当ての IP アドレス範囲) – Amazon FSx は、ファイルシステムのエンドポイント IP アドレス範囲として使用するため、VPC のプライマリ CIDR 範囲から最後の 64 個の IP アドレスを選択します。このオプションを複数回選択すると、この範囲は複数のファイルシステムで共有されます。

    > **Note**
    >
    > VPC のプライマリ CIDR 範囲の最後の 64 個の IP アドレスのいずれかがサブネットで使用されている場合、このオプションはグレー表示されます。この場合でも、[Enter an IP address range] (IP アドレス範囲を入力) オプションを選択することで、VPC 内のアドレス範囲 (つまり、プライマリ CIDR 範囲の最後にない範囲、または VPC のセカンダリ CIDR にある範囲) を選択できます。

  - [優先サブネット] には、ファイルサーバーのサブネットを指定します。マルチ AZ ファイルシステムを作成する場合は、スタンバイファイルサーバーの [Standby subnet] (スタンバイサブネット) も選択します。
  - (マルチ AZ のみ) [VPC route tables] (VPC ルートテーブル) で、ファイルシステムのエンドポイントを作成する VPC ルートテーブルを指定します。クライアントが配置されているサブネットに関連付けられている、すべての VPC ルートテーブルを選択します。デフォルトでは、Amazon FSx は VPC のデフォルトルートテーブルを選択します。
  - (マルチ AZ のみ) [Endpoint IP address range] (エンドポイント IP アドレスの範囲) で、ファイルシステムにアクセスするためのエンドポイントが作成され、IP アドレスの範囲を指定します。

    エンドポイント IP アドレスの範囲には、次の 3 つのオプションがあります。

    - [Unallocated IP address range from your VPC] (VPC からの未割り当ての IP アドレス範囲) – Amazon FSx は、ファイルシステムのエンドポイント IP アドレス範囲として使用す

るため、VPC のプライマリ CIDR 範囲から最後の 64 個の IP アドレスを選択します。このオプションを複数回選択すると、この範囲は複数のファイルシステムで共有されます。

> **Note**
>
> VPC のプライマリ CIDR 範囲の最後の 64 個の IP アドレスのいずれかがサブネットで使用されている場合、このオプションはグレー表示されます。この場合でも、[Enter an IP address range] (IP アドレス範囲を入力) オプションを選択することで、VPC 内のアドレス範囲 (つまり、プライマリ CIDR 範囲の最後にない範囲、または VPC のセカンダリ CIDR にある範囲) を選択できます。

- [Floating IP address range outside your VPC] (VPC 外のフローティング IP アドレス範囲) — Amazon FSx は、同じ VPC とルートテーブルを持つ他のファイルシステムでまだ使用されていない 198.19.x.0/24 のアドレス範囲を選択します。
- IP アドレス範囲を入力 — 任意の CIDR 範囲を指定できます。選択する IP アドレス範囲は、サブネットと重複しない限り VPC の IP アドレス範囲の内側でも外側でも可能です。

> **Note**
>
> 次の CIDR 範囲に該当するものは、 FSx for ONTAP と互換性がないため選択しないでください。
>
> - 0.0.0.0/8
> - 127.0.0.0/8
> - 198.19.0.0/20
> - 224.0.0.0/4
> - 240.0.0.0/4
> - 255.255.255.255/32

7. [Security & encryption] (セキュリティと暗号化) セクションの [Encryption key] (暗号化キー) で、保管中のファイルシステムのデータを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。
8. [File system administrative password] (ファイルシステム管理パスワード) には、`fsxadmin` ユーザー用の安全なパスワードを入力します。パスワードを確認します。

このユーザーを使用して、fsxadmin ONTAP CLI および REST API を使用してファイルシステムを管理できます。fsxadmin ユーザー の詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

9. [Default storage virtual machine configuration] (デフォルトのストレージ仮想マシンの設定) セクションで、次の情報を入力します。

   - [Storage virtual machine name] (ストレージ仮想マシン名) フィールドに、ストレージ仮想マシンの名前を入力します。最大 47 文字の英数字とアンダーバー (_) の特殊文字を使用できます。
   - [SVM administrative password] (SVM 管理パスワード) には、オプションで [Specify a password] (パスワードを指定する) を選択し、SVM の vsadmin ユーザーのパスワードを入力できます。この vsadmin ユーザーを使用して、ONTAP CLI または REST API を使用して SVM を管理できます。vsadmin ユーザー の詳細については、「CLI SVMs ONTAP の管理」を参照してください。

     パスワードを指定しない (デフォルト)を選択すると、ファイルシステムの fsxadmin ユーザーを使用して ONTAP CLI または REST API を使用することでファイルシステムを管理できますが、同様のことを行うために SVM vsadmin ユーザーを使用することはできません。
   - アクティブディレクトリ セクションでは、アクティブディレクトリを SVM に結合させることができます。詳細については、「FSx for ONTAP で Microsoft アクティブディレクトリの使用」を参照してください。

     SVM をアクティブディレクトリに結合させたくない場合は、アクティブディレクトリに参加しない を選択してください。

     SVM をセルフマネージドアクティブディレクトリドメインに結合させる場合は、 [Join an Active Directory] (アクティブディレクトリに参加する) をクリックし、アクティブディレクトリに関する以下の詳細を入力します。
     - SVM 用に作成するアクティブディレクトリコンピュータオブジェクトの NetBIOS 名。NetBIOS 名は 15 文字を超えてはいけません。
     - アクティブディレクトリの完全修飾ドメイン名。ドメイン名は 255 文字を超えてはいけません。
     - DNS サーバーの IP アドレス - ドメインのドメインネームシステム (DNS) サーバーの IPv4 アドレス。
     - サービスアカウントのユーザー名 - 既存のアクティブディレクトリのサービスアカウントのユーザー名。ドメインのプレフィックスやサフィックスを含めないでください。

- サービスアカウントのパスワード - サービスアカウントのパスワード。
- パスワードの確認 - サービスアカウントのパスワード。
- (オプション)組織単位 (OU) - ファイルシステムに結合させる組織単位の識別パス名。
- 委任されたファイルシステム管理者グループ - ファイルシステムを管理できる Active Directory 内のグループ名。

  を使用している場合は AWS Managed Microsoft AD、 AWS 委任された FSx 管理者、 AWS 委任された管理者、または OU に委任されたアクセス許可を持つカスタムグループなどのグループを指定する必要があります。

  自己管理型 AD に参加している場合は、AD でのグループ名を使用してください。デフォルトのグループは `Domain Admins` です。

10. [デフォルトのボリューム設定] セクションで、ファイルシステムで作成されたデフォルトボリュームの以下の情報を入力します。

    - [Volume name] (ボリューム名) フィールドに、ボリュームの名前を入力します。英数字とアンダースコア (_) で最大 203 文字まで使用できます。
    - (スケールアップファイルシステムのみ) [ボリュームスタイル] では、[FlexVol] または [FlexGroup] を選択します。FlexVol ボリュームはサイズが最大 300 TiB の汎用ボリュームです。FlexGroup ボリュームは高性能のワークロードを対象としており、サイズは最大 20 PiB です。
    - [ボリュームサイズ] に、800 ギビバイト (GiB) ~ 2,000 ペビバイト (PiB) の範囲で任意の整数を入力します。
    - [ボリュームタイプ] では、読み取りと書き込みが可能なボリュームを作成するには [Read-Write (RW)] を選択し、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用できる読み取り専用のボリュームを作成するには [Data Protection (DP)] を選択します。詳細については、「ボリュームの種類」を参照してください。
    - [Junction path] (ジャンクションパス) で、ボリュームをマウントするファイルシステム内の場所を入力します。`/vol3` のように、名前の先頭にスラッシュを付ける必要があります。
    - [Storage efficiency] (ストレージ効率) で、[Enabled] (有効) ONTAP ストレージ効率機能 (重複排除、圧縮、コンパクト化) を有効にします。詳細については、「FSx for ONTAP ストレージの効率化」を参照してください。
    - [ボリュームのセキュリティスタイル] では、ボリュームに対して、[Unix (Linux)]、[NTFS]、[混合] から選択します。詳細については、「ボリュームセキュリティスタイル」を参照してください。

- [Snapshot policy] (スナップショットポリシー) で、ボリュームのスナップショットポリシーを選択します。スナップショットポリシーの詳細については、スナップショットポリシー を参照してください。

  [Custom policy] (カスタムポリシー) を選択した場合は、[custom-policy] (カスタムポリシー) フィールドにポリシーの名前を指定する必要があります。カスタムポリシーは SVM またはファイルシステムにすでに存在している必要があります。ONTAP CLI または REST API を使用して、カスタムスナップショットポリシーを作成することができます。詳細については、「NetApp ONTAP 製品ドキュメント」の「スナップショットポリシーを作成する」を参照してください。

11. [デフォルトのボリュームストレージの階層化] セクションの [容量プールの階層化ポリシー] で、ボリュームのストレージプール階層化ポリシーを選択します。[自動] (デフォルト)、[スナップショットのみ]、[すべて]、[なし] のいずれかになります。容量ープールの階層化ポリシーの詳細については、「ボリューム階層化ポリシー」を参照してください。

    [階層化ポリシーの冷却期間] については、ストレージ階層化を `Auto` ポリシーと `Snapshot-only` ポリシーのどちらかに設定している場合、有効な値は 2～183 日です。ボリュームの階層化ポリシーの冷却期間は、アクセスされていないデータがコールドとしてマークされ、容量プールストレージに移動されるまでの日数を定義します。

12. バックアップとメンテナンス - オプション では、次のオプションを設定できます。

    - 毎日の自動バックアップ を使用する場合は、毎日の自動バックアップのために [Enabled] (有効) をクリックします。デフォルトでは、このオプションは有効になっています。
    - 日次自動バックアップウィンドウ で、日次自動バックアップウィンドウを開始する時刻を協定世界時 (UTC) で設定します。この指定時刻から 30 分がウインドウとなります。このウィンドウは、毎週のメンテナンスバックアップウインドウと重複させることはできません。
    - 自動バックアップ保持期間で、自動バックアップを保持する期間を 1～90 日の間で設定します。
    - 毎週のメンテナンスウィンドウ では、メンテナンスウィンドウを開始する時刻を設定できます。1 日目は月曜日、2 日目は火曜日、というように続きます。この指定された時刻から 30 分間がウインドウになります。このウィンドウは毎日の自動バックアップ時間と重複させることはできません。

13. タグ - オプション で、キーと値を入力することにより、ファイルシステムにタグを追加できます。タグは、ファイルシステムの管理、フィルタリング、および検索に便利な大文字と小文字の区別があるキーと値のペアです。

[Next] (次へ) を選択します。

14. ファイルシステムを作成する ページで表示されるファイルシステムの設定を確認します。参考までに、ファイルシステムの作成後に変更可能なファイルシステム設定を書き留めておきます。
15. ファイルシステムを作成する を選択します。

ファイルシステムを作成するには (CLI)

- FSx for ONTAP ファイルシステムを作成するには、次の例に示すように、create-file-system CLI コマンド (または同等のCreateFileシステム API オペレーション) を使用します。

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

ファイルシステムが正常に作成されると、Amazon FSx は次の例のようにファイルシステムの説明を JSON 形式で返します。

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
```

```
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> コンソールでのファイルシステムの作成プロセスとは異なり、create-file-system CLI コマンドと CreateFileSystem API オペレーションでは、デフォルトの SVM やボリュームは作成されません。SVM を作成するには、「ストレージ仮想マシンの作成」を参照してください。ボリュームを作成するには、「ボリュームの作成」を参照してください。

共有サブネット内での FSx for ONTAP ファイルシステムの作成

VPC 共有により、複数の AWS アカウント が共有された一元管理仮想プライベートクラウド (VPCs にリソースを作成できます。このモデルでは、VPC (所有者) を所有するアカウントは、 から同じ組織に属する他のアカウント (参加者) と 1 つ以上のサブネットを共有します AWS Organizations。

参加者アカウントは、所有者アカウントが共有した VPC サブネット内に FSx for ONTAP シングル AZ ファイルシステムおよびマルチ AZ ファイルシステムを作成できます。参加者アカウントがマルチ AZ ファイルシステムを作成するには、参加者アカウントに代わって共有サブネット内のルートテーブルを変更するアクセス許可を Amazon FSx に所有者アカウントが付与する必要もあります。詳細については、「マルチ AZ ファイルシステムでの共有 VPC サポートの管理」を参照してください。

> **Note**
>
> 参加者のファイルシステムの VPC 内 CIDR と重複する後続の VPC サブネットが作成されないように、VPC 所有者と調整するのは参加者アカウントの責任です。サブネットが重複すると、ファイルシステムへのトラフィックが中断される可能性があります。

共有サブネットの要件と考慮事項

共有サブネットに FSx for ONTAP ファイルシステムを作成するときは、次の点に注意してください。

- VPC サブネットの所有者が参加者アカウントとサブネットを共有しないと、そのアカウントではそこに FSx for ONTAP file system を作成できません。
- VPC のデフォルトセキュリティグループは所有者に属しているため、デフォルトのセキュリティグループを使用してリソースを起動することはできません。さらに、参加者アカウントは、他の参加者または所有者が所有するセキュリティグループを使用してリソースを起動することはできません。
- 共有サブネットでは、参加者と所有者がそれぞれのアカウント内のセキュリティグループを個別に管理します。所有者アカウントは、参加者が作成したセキュリティグループを表示できますが、これらのグループに対してアクションを実行することはできません。所有者アカウントがこれらのセキュリティグループの削除や変更を希望する場合は、セキュリティグループを作成した参加者がそのアクションを実行する必要があります。
- 参加者アカウントは、所有者アカウントが共有したサブネット内にあるシングル AZ ファイルシステムおよび関連リソースを表示、作成、変更、および削除できます。

- 参加者アカウントは、所有者アカウントが共有したサブネット内にあるマルチ AZ ファイルシステムおよび関連リソースを作成、表示、変更、および削除できます。さらに、所有者アカウントは、参加者アカウントに代わって共有サブネットのルートテーブルを変更するアクセス許可を Amazon FSx サービスに付与する必要もあります。詳細については、「マルチ AZ ファイルシステムでの共有 VPC サポートの管理」を参照してください。
- 共有 VPC の所有者は、参加者が共有サブネット内に作成したリソースを表示、変更、削除することはできません。これは、アカウントごとに異なるアクセス権を持つ VPC リソースに加えて適用されます。詳細については、「Amazon VPC ユーザーガイド」の「所有者および参加者の責任と権限」を参照してください。

詳細については、「Amazon VPC ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。

VPC サブネットを共有する場合

共有サブネットに FSx for ONTAP ファイルシステムを作成する参加者アカウントとサブネットを共有する場合は、次のことを行う必要があります。

- VPC 所有者は を使用して AWS Resource Access Manager 、VPCsとサブネットを他の と安全に共有する必要があります AWS アカウント。詳細については、「 ユーザーガイド」の「 AWS リソースの共有 AWS Resource Access Manager 」を参照してください。
- VPC 所有者は、1 つまたは複数の VPC を参加者アカウントと共有する必要があります。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。
- 参加者アカウントが FSx for ONTAP マルチ AZ ファイルシステムを作成するには、参加者アカウントに代わって共有サブネット内のルートテーブルを作成および変更するアクセス許可を Amazon FSx サービスに所有者アカウントが付与する必要もあります。これは、接続しているクライアントがフェイルオーバーイベント中に優先ファイルサーバーとスタンバイファイルサーバー間をシームレスに移行できるようにするために、FSx for ONTAP マルチ AZ ファイルシステムがフローティング IP アドレスを使用しているためです。フェイルオーバーイベントが発生すると、Amazon FSx は、ファイルシステムに関連付けられているすべてのルートテーブルのすべてのルートを、現在アクティブなファイルサーバーを指すように更新します。

マルチ AZ ファイルシステムでの共有 VPC サポートの管理

所有者アカウントは、次のセクションで説明するように、、 AWS Management Console AWS CLI、および API を使用して、所有者が参加者と共有した VPC サブネットにマルチ AZ FSx for ONTAP ファイルシステムを作成できるかどうかを管理できます。

マルチ AZ ファイルシステムの VPC 共有を管理するには (コンソール)

https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。

1. ナビゲーションペインで [設定] を選択します。
2. [設定] ページで [マルチ AZ 共有 VPC 設定] を探します。
   - 共有する VPC サブネット内のマルチ AZ ファイルシステムの VPC 共有を有効にするには、[参加者アカウントからのルートテーブル更新を有効化] を選択します。
   - 所有するすべての VPC 内のマルチ AZ ファイルシステムの VPC 共有を無効にするには、[参加者アカウントからのルートテーブル更新を無効化] を選択します。確認画面が表示されます。

   > **Important**
   >
   > この機能を無効にする前に、共有 VPC 内の参加者が作成したマルチ AZ ファイルシステムを削除することを強くお勧めします。この機能を無効にすると、これらのファイルシステムは `MISCONFIGURED` 状態になり、使用できなくなる危険性があります。

3. 「**`confirm`**」と入力して [確認] を選択すると、この機能が無効になります。

マルチ AZ ファイルシステムの VPC 共有を管理するには (AWS CLI)

1. マルチ AZ VPC 共有の現在の設定を表示するには、次のように describe-shared-vpc-configuration CLI コマンドまたは同等の DescribeSharedVpcConfiguration API コマンドを使用します。

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   リクエストが成功すると、サービスは次のように応答します。

   ```
   {
   ```

```
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. マルチ AZ 共有 VPC 設定を管理するには、update-shared-vpc-configuration CLI コマンド、または同等の UpdateSharedVpcConfiguration API コマンドを使用します。次の例では、マルチ AZ ファイルシステムの VPC 共有を有効にします。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

リクエストが成功すると、サービスは次のように応答します。

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. この機能を無効にするには、次の例のように EnableFsxRouteTableUpdatesFromParticipantAccounts を false に設定します。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

リクエストが成功すると、サービスは次のように応答します。

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

ファイルシステムの更新

このトピックでは、更新できる既存のファイルシステムのプロパティと、コンソールと CLI を使用して更新する手順について説明します。

Amazon FSx コンソール、、 AWS CLIおよび Amazon FSx API を使用して、次の FSx for ONTAP ファイルシステムプロパティを更新できます。

- 日次自動バックアップ。日次自動バックアップをオンまたはオフにし、バックアップウィンドウとバックアップ保持期間を変更します。バックアップの詳細については、「自動の日次バックアップの操作」を参照してください。

- 週次メンテナンス時間枠。Amazon FSx がファイルシステムのメンテナンスと更新を実行する曜日と時間を設定します。メンテナンスウィンドウの詳細については、Amazon FSx メンテナンスウィンドウでのパフォーマンスの最適化 を参照してください。
- ファイルシステムの管理者パスワード。ファイルシステムの fsxadmin ユーザーのパスワードを変更します。このユーザーを使用して、fsxadmin ONTAP CLI および REST API を使用してファイルシステムを管理できます。fsxadmin ユーザー の詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
- Amazon VPC ルートテーブル。マルチ AZ の FSx for ONTAP ファイルシステムでは、NFS または SMB を介してデータにアクセスするために使用するエンドポイントおよび ONTAP CLI、API、BlueXP にアクセスする管理エンドポイントは、ファイルシステムに関連付けた Amazon VPC ルートテーブルのフローティング IP アドレスを使用します。作成した新しいルートテーブルを既存の Multi-AZ ファイルシステムに関連付けて、ネットワークが発展してもデータにアクセスできるクライアントを制御できます。既存のルートテーブルをファイルシステムから解除 (削除) することもできます。

> **Note**
>
> Amazon FSx は、タグベースの認証を使用してマルチ AZ ファイルシステムの VPC ルートテーブルを管理します。これらのルートテーブルには Key: AmazonFSx; Value: ManagedByAmazonFSx のタグが付けられています。を使用して FSx for ONTAP マルチ AZ ファイルシステムを作成または更新する場合は、 Key: AmazonFSx; Value: ManagedByAmazonFSx タグを手動で追加 AWS CloudFormation することをお勧めします。

ファイルシステムを更新するには (コンソール)

次の手順では、 を使用して既存の FSx for ONTAP ファイルシステムを更新する方法について説明します AWS Management Console。

日次自動バックアップを更新するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ファイルシステムの詳細ページを表示するには、左のナビゲーションペインで、[File systems] (ファイルシステム) を選択し、更新する FSx for ONTAP ファイルシステムを選択します。
3. ページの 2 番目のパネルで [Backups] (バックアップ) タブを選択します。
4. [更新] を選択します。

5. このファイルシステムの日次自動バックアップの設定を変更します。
6. [保存] を選択して変更を保存します。

ウィークリーメンテナンスウィンドウを更新するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ファイルシステムの詳細ページを表示するには、左のナビゲーションペインで、[File systems] (ファイルシステム) を選択し、更新する FSx for ONTAP ファイルシステムを選択します。
3. ページの 2 番目のパネルで [Administration] (管理) タブを選択します。
4. [Maintenance] (メンテナンス) ペインで、[Update] (更新) を選択します。
5. このファイルシステムのウィークリーメンテナンスウィンドウが発生するタイミングを変更します。
6. [保存] を選択して変更を保存します。

ファイルシステムの管理者パスワードを変更するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ファイルシステムの詳細ページを表示するには、左のナビゲーションペインで、[File systems] (ファイルシステム) を選択し、更新する FSx for ONTAP ファイルシステムを選択します。
3. [Administration] (管理) タブを選択します。
4. [ONTAP 管理] ペインで、[ONTAP 管理者パスワード] の下の [更新] を選択します。
5. [ONTAP 管理者認証情報の更新] ダイアログボックスで、[ONTAP 管理パスワード] フィールドに新しいパスワードを入力します。
6. [Confirm password] (パスワードの確認) フィールドで、パスワードを確認します。
7. [更新] を選択して変更を保存します。

> **Note**
>
> 新しいパスワードがパスワード要件を満たしていないことを示すエラーが表示された場合は、`security login role config show` ONTAP CLI コマンドを使用してファイルシステムのパスワード要件設定を表示できます。パスワード設定を変更する方法などの詳細については、「」を参照してください[fsxadmin アカウントパスワードの更新が失敗する]。

マルチ AZ ファイルシステムの VPC ルートテーブルを更新するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ファイルシステムの詳細ページを表示するには、左のナビゲーションペインで、[File systems] (ファイルシステム) を選択し、更新する FSx for ONTAP ファイルシステムを選択します。
3. [Actions] (アクション) で、[Manage Route Tables] (ルートテーブルの管理) を選択します。このオプションは、マルチ AZ ファイルシステムでのみ使用可能です。
4. [Manage route tables] (ルートテーブルの管理) ダイアログボックスで、次のいずれかを実行します。
   - 新しい VPC ルートテーブルを関連付けるには、[Associate new route tables] (新しいルートテーブルの関連付け) ドロップダウンリストからルートテーブルを選択し、[Associate] (関連付け) を選択します。
   - 既存の VPC ルートテーブルの関連付けを解除するには、[Current route tables] (現在のルートテーブル) ペインからルートテーブルを選択し、[Disassociate] (関連付け解除) を選択します。
5. [閉じる] を選びます。

ファイルシステムを更新するには (CLI)

次の手順は、 を使用して既存の FSx for ONTAP ファイルシステムを更新する方法を示しています AWS CLI。

1. FSx for ONTAP ファイルシステムの設定を更新するには、次の例に示すように、update-file-system CLI コマンド (または同等のUpdateFileシステム API オペレーション) を使用します。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. 日次自動バックアップをしないようにするには、`AutomaticBackupRetentionDays` プロパティを 0 に設定します。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
```

```
    --ontap-configuration AutomaticBackupRetentionDays=0
```

ファイルシステムの削除

Amazon FSx コンソール、、Amazon FSx API および SDKs を使用して AWS CLI、FSx for ONTAP ファイルシステムを削除できます。

ファイルシステムを削除するには:

- コンソールの使用 - ステップ 3: リソースをクリーンアップするで説明されている手順に従います。
- CLI または API の使用 - まず、ファイルシステム上のすべてのボリュームと SVM を削除します。次に、delete-file-system CLI コマンドまたは DeleteFileSystem API オペレーションを使用します。

ファイルシステムの詳細の表示

Amazon FSx コンソール、、 AWS CLI API、およびサポートされている AWS SDKs を使用して、FSx for ONTAP ファイルシステムの詳細な設定情報を表示できます。

詳細なファイルシステム情報を表示するには

- コンソールの使用 - ファイルシステムを選択して、ファイルシステム 詳細ページを表示します。[Summary] (概要) パネルには、ファイルシステムの ID、ライフサイクルステータス、デプロイ タイプ、SSD ストレージ容量、スループットキャパシティ、プロビジョンド IOPS、アベイラビリティーゾーン、および作成時間が表示されます。

  以下のタブでは、詳細な設定情報が表示され、変更可能なプロパティは編集できます。

  - ネットワークとセキュリティ
  - モニタリングとパフォーマンス — 作成した CloudWatch アラーム、および以下のカテゴリのメトリクスと警告を表示します。
    - 概要 – ファイルシステムのアクティビティメトリクスのハイレベルの概要
    - ファイルシステムのストレージ容量
    - ファイルサーバーとディスクのパフォーマンス

    詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。

- 管理 – 以下のファイルシステム管理情報を表示します。
  - ファイルシステムの管理エンドポイントとクラスター間エンドポイントの DNS 名と IP アドレス。
  - ONTAP 管理者のユーザー名。
  - ONTAP 管理者のパスワードを更新するオプション。
- ファイルシステムの SVM のリスト
- ファイルシステムのボリュームのリスト
- バックアップ設定 – ファイルシステムの自動日次バックアップ設定を変更します。
- 更新 – ファイルシステムの設定に対してユーザーが開始した更新のステータスを表示します。
- タグ – タグのキーと値のペアを表示、編集、追加、削除します。
- CLI または API の使用 – describe-file-systems CLI コマンドまたは DescribeFileSystems API オペレーションを使用します。

FSx for ONTAP ファイルシステムのステータス

Amazon FSx ファイルシステムのステータスを表示するには、Amazon FSx コンソール、 AWS CLI コマンド describe-file-systems、または API オペレーション DescribeFileSystems を使用します。

ファイルシステムのステータス	説明
[AVAILABLE] (利用可能)	ファイルシステムが正常に作成され、使用可能になりました。
[CREATING] (作成中)	Amazon FSx は新しいファイルシステムを作成しています。
[DELETING] (削除中)	Amazon FSx は既存のファイルシステムを削除しています。
[MISCONFIGURED] (設定ミスです)	ファイルシステムが正しく設定されていませんが復旧可能な状態です。
[FAILED] (失敗)	1. ファイルシステムに障害が発生し、Amazon FSx はこれを修復できません。

ファイルシステムのステータス	説明
	2. ファイルシステムの新規作成時に、Amazon FSx はファイルシステムを新規作成できませんでした。

FSx for ONTAP ストレージ仮想マシンの管理

FSx for ONTAP では、ボリュームはストレージ仮想マシン (SVM) と呼ばれる仮想ファイルサーバでホストされます。SVM は、データを管理およびアクセスするための独自の管理者資格情報とエンドポイントを備えた分離されたファイルサーバーです。FSx for ONTAP のデータにアクセスすると、クライアントとワークステーションは SVM のエンドポイント (IP アドレス) を使用して SVM がホストするボリューム、SMB 共有、または iSCSI LUN をマウントします。

Amazon FSx は、 AWS Management Consoleを使用してファイルシステムを作成するときに、デフォルトの SVM をファイルシステム上に自動的に作成します。コンソール、または Amazon FSx API と SDKs を使用して AWS CLI、ファイルシステムに追加の SVMs をいつでも作成できます。ONTAP CLI または REST API を使用して SVM を作成することはできません。

SVM を Microsoft Active Directory に参加させることで、ファイルアクセスの認証と認可を行うことができます。詳細については、「FSx for ONTAP で Microsoft アクティブディレクトリの使用」を参照してください。

ファイルシステムあたりの SVM の最大数

次の表に、ファイルシステムに対して作成できる SVM の最大数を示します。SVM の最大数は、メガバイト / 秒 (MBps) 単位でプロビジョニングされるスループットキャパシティの量に依存します。

デプロイタイプ	スループットキャパシティ (MBps)	ファイルシステムあたりの SVM の最大数
シングル AZ (スケールアップ) とマルチ AZ (スケールアップ)	128	6
	256	6
	512	14
	1,024	14

デプロイタイプ	スループットキャパシティ (MBps)	ファイルシステムあたりの SVM の最大数
	2,048	24
	4,096	24
シングル AZ (スケールアウト)	すべて	5

トピック

- ストレージ仮想マシンの作成
- ストレージ仮想マシンの更新
- ストレージ仮想マシン (SVM) の削除
- ストレージ仮想マシン設定の詳細の表示

ストレージ仮想マシンの作成

AWS Management Console、 AWS CLI、および API を使用して FSx for ONTAP SVM を作成できます。

ファイルシステムに作成できる SVM の最大数は、ファイルシステムのデプロイタイプとプロビジョニングされるスループットキャパシティによって異なります。詳細については、「ファイルシステムあたりの SVM の最大数」を参照してください。

SVM のプロパティ

SVM の作成時に、次のプロパティを定義します。

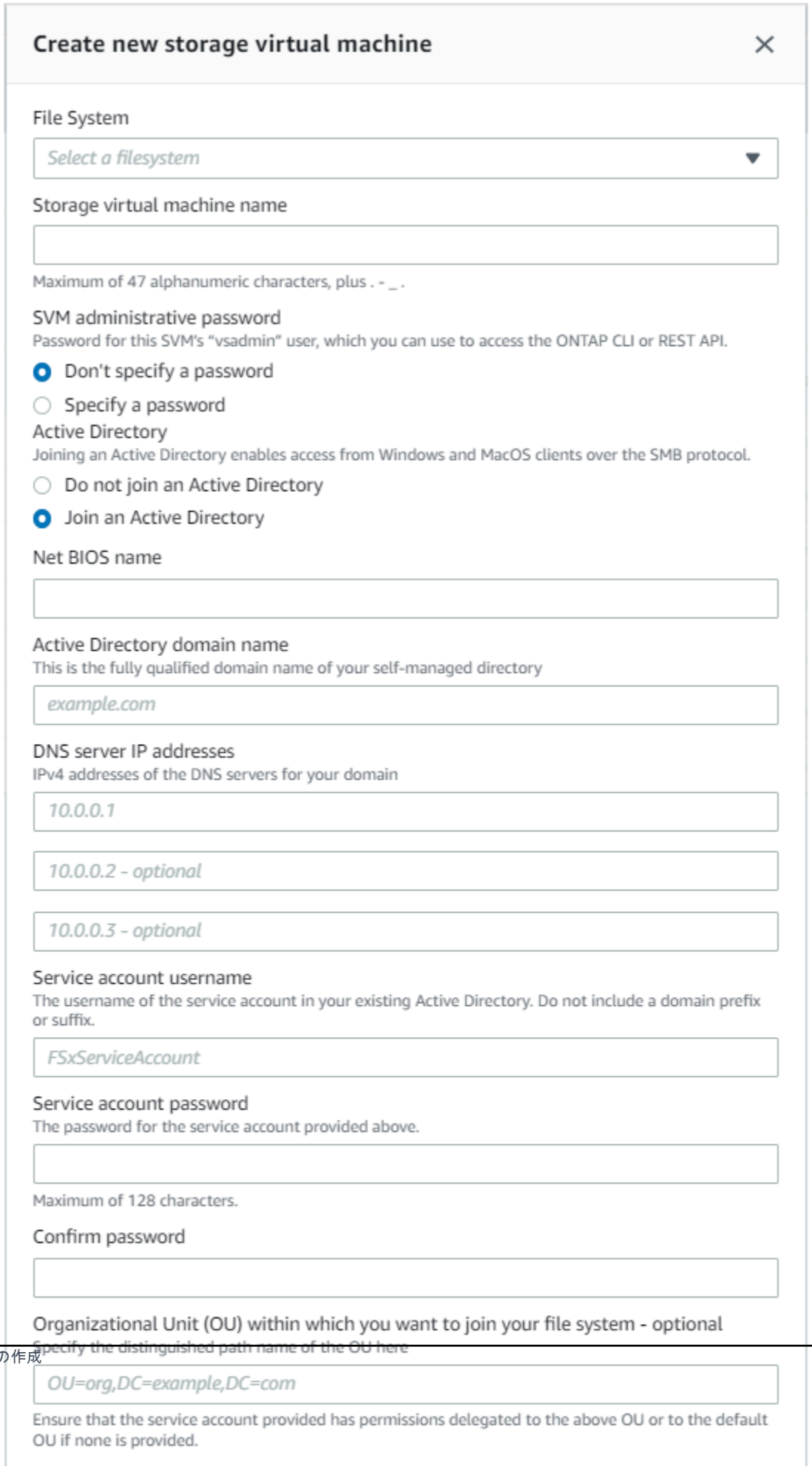
- それが属する FSx for ONTAP ファイルシステム。
- Microsoft アクティブディレクトリ(AD) の設定 - オプションとして、SVM をセルフマネージド AD に接続して、Windows および macOS クライアントの認証とアクセスコントロールを行うことができます。詳細については、「FSx for ONTAP で Microsoft アクティブディレクトリの使用」を参照してください。
- ルートボリュームセキュリティスタイル - SVM 内のデータへのアクセスに使用するクライアントのタイプに合わせて、ルートボリュームセキュリティスタイル (Unix、NTFS、または Mixed) を設定します。詳細については、「ボリュームセキュリティスタイル」を参照してください。

- SVM 管理者のパスワード — オプションとして SVM vsadmin ユーザーのパスワードを設定できます。詳細については、「CLI SVMs ONTAP の管理」を参照してください。

ストレージ仮想マシンを作成するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左のナビゲーションペインで、ストレージ仮想マシン を選択します。
3. ストレージ仮想マシンの新規作成 を選択します。

   ストレージ仮想マシンの新規作成 ダイアログボックスが表示されます。


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. [File systems] (ファイルシステム) で、ストレージ仮想マシンを作成するファイルシステムを選択します。
5. [Storage virtual machine name] (ストレージ仮想マシン名) フィールドに、ストレージ仮想マシンの名前を入力します。最大 47 文字の英数字とアンダーバー (_) の特殊文字を使用できます。
6. SVM 管理パスワード を選択した場合は、オプションで パスワードを指定する を選択して、この SVM の `vsadmin` ユーザーのパスワードを入力します。このユーザーを使用して、`vsadmin` ONTAP CLI または REST API を使用して SVM を管理できます。`vsadmin` ユーザー の詳細については、「CLI SVMs ONTAP の管理」を参照してください。

   パスワードを指定しない (デフォルト)を選択すると、ファイルシステムの `fsxadmin` ユーザーを使用して ONTAP CLI または REST API を使用することでファイルシステムを管理できますが、同様のことを行うために SVM `vsadmin` ユーザーを使用することはできません。
7. アクティブディレクトリ では、以下のオプションがあります。

   - ファイルシステムをアクティブディレクトリ(AD) に接続しない場合は、[アクティブディレクトリに接続しない] を選択してください。
   - SVM をセルフマネージド AD ドメインに接続する場合は、[アクティブディレクトリに接続する] を選択し、アクティブディレクトリに関する以下の詳細を入力します。詳細については、「SVM をセルフマネージド Microsoft AD に接続させるための前提条件」を参照してください。
     - SVM 用に作成するアクティブディレクトリコンピュータオブジェクトの NetBIOS 名。NetBIOS 名は 15 文字を超えてはいけません。これは、アクティブディレクトリ内にある SVM の名前です。
     - アクティブディレクトリの完全修飾ドメイン名 (FQDN)。FQDN は 255 文字を超えることはできません。
     - [DNS サーバーの IP アドレス] - ドメインの DNS サーバーの IPv4 アドレス。
     - [サービスアカウントのユーザー名] - 既存のアクティブディレクトリのサービスアカウントのユーザー名。ドメインのプレフィックスやサフィックスを含めないでください。`EXAMPLE\ADMIN` の場合は、`ADMIN` を使用します。
     - サービスアカウントのパスワード - サービスアカウントのパスワード。
     - パスワードの確認 - サービスアカウントのパスワード。
     - (オプション)組織単位 (OU) - ファイルシステムに結合させる組織単位の識別パス名。
     - [委任されたファイルシステム管理者グループ] - ファイルシステムを管理できる AD 内のグループ名。

を使用している場合は AWS Managed Microsoft AD、 AWS が委任した FSx 管理者、 AWS が委任した管理者などのグループ、または OU に委任されたアクセス許可を持つカスタムグループを指定する必要があります。

自己管理型 AD に参加している場合は、AD でのグループ名を使用してください。デフォルトのグループは `Domain Admins` です。

8. [SVM root volume security style] (SVM ルートボリュームセキュリティスタイル) で、データにアクセスするクライアントのタイプに応じて、SVM のセキュリティスタイルを選択します。主に Linux クライアントを使用してデータにアクセスする場合は [Unix (Linux)] を選択し、主に Windows クライアントを使用してデータにアクセスする場合は [NTFS] を選択します。詳細については、「ボリュームセキュリティスタイル」を参照してください。
9. 確認 を選択して、ストレージ仮想マシンを作成します。

更新の進捗状況は、[File systems] (ファイルシステム) 詳細ページの ストレージ仮想マシン ペインの ステータス の列でモニタリングできます。ステータスが 作成 になると、ストレージ仮想マシンが使用可能な状態になります。

ストレージ仮想マシンを作成するには (CLI)

- FSx for ONTAP ストレージ仮想マシン (SVM) を作成するには、次の例に示すようにcreate-storage-virtual-machine、 CLI コマンド (または同等の CreateStorageVirtualMachine API オペレーション) を使用します。

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

ストレージ仮想マシンが正常に作成されると、次の例で示すように、Amazon FSx はその説明を JSON 形式で返します。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
```

```
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

ストレージ仮想マシンの更新

Amazon FSx コンソール、および Amazon FSx API を使用して AWS CLI、次のストレージ仮想マシン (SVM) 設定プロパティを更新できます。

- 次のストレージ仮想マシン (SVM) の設定プロパティを更新できます。
- SVM アクティブディレクトリ(AD) 構成 - SVM を AD に接続させることも、既に AD に接続している SVM の AD 構成を変更することもできます。詳細については、「SVM アクティブディレクトリ設定の管理」を参照してください。

SVM 管理者アカウントの認証情報を更新する方法 (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 更新する SVM を次のように選択します。
   - 左のナビゲーションペインで、[ファイルシステム] を選択し、SVM を更新する ONTAP ファイルシステムを選択します。
   - ストレージ仮想マシン タブを選択します。

     -または-

   - AWS アカウント 現在の で で使用可能なすべての SVMs のリストを表示するには AWS リージョン、ONTAP を展開し、ストレージ仮想マシン を選択します。
3. 更新するストレージ仮想マシンを選択します。
4. [アクション > 管理者パスワードの更新] を選択します。[SVM 管理者認証情報の更新] ウィンドウが表示されます。
5. vsadmin ユーザーの新しいパスワードを入力し、確認します。
6. [認証情報の更新] を選択して新しいパスワードを保存します。

SVM 管理者アカウントの認証情報 (CLI) を更新する方法

- FSx for ONTAP SVM の設定を更新するには、次の例に示すようにupdate-storage-virtual-machine、 CLI コマンド (または同等の UpdateStorageVirtualMachine API オペレーション) を使用します。

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

ストレージ仮想マシンが正常に作成されると、次の例で示すように、Amazon FSx はその説明を JSON 形式で返します。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
```

```
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

ストレージ仮想マシン (SVM) の削除

FSx for ONTAP SVM を削除するには AWS CLI、Amazon FSx コンソール、、および API を使用します。SVM を削除する前に、まず SVM にアタッチされている非ルートボリュームをすべて削除する必要があります。

> **Important**
>
> NetApp ONTAP CLI または API を使用して SVM を削除することはできません。

> **Note**
>
> ストレージ仮想マシンを削除する前に、SVM 内のデータにアクセスしているアプリケーションがなく、SVM にアタッチされた非ルートボリュームがすべて削除されていることを確認してください。

ストレージ仮想マシンを削除するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 次の方法で、削除する SVM を選択します。

   - 左のナビゲーションペインで、[ファイルシステム] を選択し、SVM を削除する ONTAP ファイルシステムを選択します。
   - ストレージ仮想マシン タブを選択します。

   -または-

   - 使用可能なすべての SVM のリストを表示するには、[ONTAP] を展開して [ストレージ仮想マシン] を選択します。

   リストから削除する SVM を選択します。
3. [ボリューム] タブで、SVM にアタッチされているボリュームのリストを表示します。SVM にアタッチされた非ルートボリュームがある場合、SVM を削除する前にこれらのボリュームを削除する必要があります。詳細については、「ボリュームの削除」を参照してください。
4. [アクション] メニューで [ストレージ仮想マシンの削除] を選択します。
5. 削除確認ダイアログボックスで [ストレージ仮想マシンの削除] を選択します。

ストレージ仮想マシンを削除するには (CLI)

- FSx for ONTAP ストレージ仮想マシンを削除するには、次の例に示すようにdelete-storage-virtual-machine、 CLI コマンド (または同等の DeleteStorageVirtualMachine API オペレーション) を使用します。

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

ストレージ仮想マシン設定の詳細の表示

Amazon FSx コンソール、、および Amazon FSx API を使用して AWS CLI、現在ファイルシステム上にある FSx for ONTAP ストレージ仮想マシンを表示できます。

ファイルシステム上のストレージ仮想マシンを表示するには:

- コンソールの使用 - [File systems] (ファイルシステム) 詳細ページを表示するファイルシステムを選択します。ファイルシステム上のすべてのストレージ仮想マシンを一覧表示するには、ストレージ仮想マシン タブで、表示するストレージ仮想マシンを選択します。
- CLI または API の使用 – CLI コマンドまたは DescribeStorageVirtualMachines API describe-storage-virtual-machines オペレーションを使用します。

  システムには、その AWS リージョン のアカウント内にあるすべての SVM の詳細な説明のリストが返されます。

FSx for ONTAP ボリュームの管理

FSx for ONTAP ファイルシステム上の各ストレージ仮想マシン (SVM) には、1 つまたは複数のボリュームを含めることができます。ボリュームは、ファイル、ディレクトリ、または iSCSI 論理ストレージユニット (LUN) 用の分離されたデータコンテナです。ボリュームはシンプロビジョンされ、ストレージに格納されているデータに対してのみストレージ容量を消費します。

iSCSI LUN (共有ブロックストレージ) を作成することで、Linux、Windows、または macOS クライアントから、ネットワークファイルシステム (NFS) プロトコル、サーバーメッセージブロック (SMB) プロトコル、またはインターネットスモールコンピュータシステムインターフェイス (iSCSI) プロトコルを経由して、ボリュームにアクセスできます。FSx for ONTAP は、同じボリュームへのマルチプロトコルアクセス (同時 NFS および SMB アクセス) もサポートしています。

、 AWS Management Console、Amazon FSx API AWS CLI、または NetApp BlueXP を使用してボリュームを作成できます。また、ファイルシステムまたは SVM の管理エンドポイントを使用して、NetApp ONTAP CLI または REST API を使用してボリュームを作成、更新、削除することもできます。

> **Note**
>
> HA ペアごとに 500 個のボリュームを作成できます。すべての HA ペアで最大 1,000 個のボリュームを作成できます。 FlexGroup構成ボリュームはこの制限にカウントされます。デフォルトでは、アグリゲートごとに 8 つの構成要素ボリュームがありますFlexGroup。

ボリュームを作成するときは、次のプロパティを定義します。

- ボリュームスタイル – ボリュームスタイルは FlexVolまたは のいずれかですFlexGroup。
- ボリューム名 – ボリュームの名前。
- ボリュームタイプ – ボリュームタイプは、読み取り/書き込み (RW) またはデータ保護 (DP) のいずれかです。DP ボリュームは、読み取り専用で、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用されます。
- ボリュームサイズ – これは、ストレージ階層に関係なく、ボリュームが保存できる最大データ量です。
- ジャンクションパス - これはボリュームがマウントされる SVM の名前空間内の場所です。
- ストレージ効率 – データ圧縮、圧縮、重複排除などのストレージ効率機能により、汎用ファイル共有ワークロードの一般的なストレージコストを 65% 削減できます。
- ボリュームセキュリティスタイル (Unix、NTFS、または Mixed) – ユーザーを承認するときに、ボリュームのデータアクセスに使用されるアクセス許可のタイプを決定します。
- データ階層化 – 階層化ポリシーは、費用対効果の高いキャパシティープール階層に保存するデータを定義します。
- 階層化ポリシーの冷却期間 — データがコールドとマークされ、キャパシティープールストレージに移動されるタイミングを定義します。
- スナップショットポリシー – スナップショットポリシーは、システムがボリュームのスナップショットを作成する方法を定義します。ONTAP CLI または REST API を使用して作成した 3 つの定義済みポリシーから選択することも、カスタムポリシーを使用することもできます。
- タグをバックアップにコピーする – Amazon FSx は、このオプションを使用して、ボリュームからバックアップにタグを自動的にコピーします。このオプションは、 AWS CLI または Amazon FSx API を使用して設定できます。

トピック

- ボリュームスタイル
- ボリュームの種類
- ボリュームセキュリティスタイル
- ボリュームの作成
- ボリュームの更新
- ボリュームの削除
- ボリュームの表示

ボリュームスタイル

FSx for ONTAP には、別々の目的に使用できる 2 つのスタイルのボリュームが用意されています。Amazon FSx コンソール、、および Amazon FSx API を使用して AWS CLI、 FlexVol または FlexGroup ボリュームを作成できます。

- FlexVol ボリュームは、1 つの高可用性 (HA) ペアのファイルシステムとしては最もシンプルな操作性を実現する、スケールアップファイルシステムのデフォルトのボリュームスタイルです。FlexVol ボリュームの最小サイズは 20 メビバイト (MiB) で、最大サイズは 314,572,800 MiB です。
- FlexGroup ボリュームは複数の FlexVol ボリュームが構成要素になっているため、複数の HA ペアを持つファイルシステムの FlexVol ボリュームよりもパフォーマンスとストレージのスケーラビリティが高くなっています。FlexGroup ボリュームはスケールアウトファイルシステムのデフォルトのボリュームスタイルです。FlexGroup ボリュームの最小サイズは、構成要素あたり 100 ギビバイト (GiB) で、最大サイズは 20 ペビバイト (PiB) です。

CLI を使用すると、 FlexVol スタイルのボリュームを ONTAP FlexGroupスタイルに変換できます。これにより、単一の構成要素FlexGroupを持つ が作成されます。ただし、 AWS DataSync を使用してFlexVolボリュームと新しいFlexGroupボリューム間でデータを移動し、データがFlexGroup's構成要素間で均等に分散されるようにすることをお勧めします。詳細については、「FlexGroup 構成要素」を参照してください。

> **Note**
>
> ONTAP CLI を使用してFlexVolボリュームをFlexGroupボリュームに変換する場合は、変換する前にFlexVolボリュームのバックアップをすべて削除してください。 ONTAPは変換の一部としてデータを自動的に再調整しないため、データがFlexGroup構成要素間で不均衡になる可能性があります。

FlexGroup 構成要素

FlexGroup ボリュームは構成要素、つまり FlexVol ボリュームで構成されます。デフォルトでは、FSx for ONTAP は HA ペアごとに 1 つの FlexGroup ボリュームに 8 つの構成要素を割り当てます。

FlexGroup ボリュームを作成すると、そのサイズは構成要素間で均等に分割されます。例えば、8 つの構成要素で構成される 800 ギガバイト (GB) の FlexGroup ボリュームを作成した場合、各構成要

素のサイズは 100 GB になります。FlexGroup ボリュームのサイズは 100 GB ~ 20 PiB ですが、合計サイズは構成要素のサイズによって異なります。各構成要素の最小サイズは 100 GB、最大サイズは 300 TiB です。例えば、構成要素が 8 FlexGroup つあるボリュームの最小サイズは 800 GB、最大サイズは 20 PiB です。

ONTAP は構成要素全体にファイルレベルでデータを分散します。FlexGroup ボリュームの各構成要素には最大 20 億個のファイルを保存できます。

FlexGroup ボリュームのサイズを更新すると、新しいサイズが既存の構成要素に均等に分散されます。

ONTAP CLI または REST API を使用して、FlexGroup ボリュームにさらに構成要素を追加することもできます。ただし、追加のストレージ容量が必要で、すべての構成要素がすでに最大サイズ (構成要素あたり 300 TiB) にある場合にのみ、これを行うことをお勧めします。構成要素を追加すると、構成要素間でデータと I/O のバランスが崩れる可能性があります。構成要素のバランスが取れるまで、書き込みスループットはバランスの取れた FlexGroup ボリュームよりも 5 ~ 10% 低くなる可能性があります。新しいデータが FlexGroup ボリュームに書き込まれると、ONTAP は、構成要素のバランスが取れるまで、そのデータを新しい構成要素に優先的に分配します。新しい構成要素を追加する場合は、アグリゲートごとに 8 個を超えない偶数を選択することをお勧めします。

> **Note**
>
> 新しい構成要素を追加すると、既存のスナップショットは部分的なスナップショットになるため、FlexGroup ボリュームを以前の状態に完全に復元することはできません。新しい構成要素がまだ存在していないため、以前のスナップショットはFlexGroupボリュームの完全な point-in-time イメージを提供できません。ただし、部分スナップショットは、個々のファイルやディレクトリを復元したり、新しいボリュームを作成したり、SnapMirror でレプリケートしたりするために使用できます。

ボリュームの種類

FSx for ONTAP には、Amazon FSx コンソール、、 AWS CLIおよび Amazon FSx API を使用して作成できる 2 種類のボリュームが用意されています。

- ほとんどの場合、読み取り/書き込み (RW) ボリュームが使用されます。その名前が示すとおり、読み取りと書き込みが可能です。

- データ保護 (DP) ボリュームは、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用する、読み取り専用のボリュームです。DP ボリュームは、1 つのボリュームのデータを 移行 または 保護 する場合に使用する必要があります。

FlexVol ボリュームと FlexGroup ボリュームは RW でも DP でもかまいません。

> **Note**
>
> ボリュームの作成後に、ボリュームのタイプを更新することはできません。

ボリュームセキュリティスタイル

FSx for ONTAP は、Unix、NTFS、混合の 3 つの異なるボリュームセキュリティスタイルをサポートしています。各セキュリティスタイルは、データのアクセス許可の処理方法に異なる影響を与えます。目的に適したセキュリティスタイルを選択するには、さまざまな効果を理解する必要があります。

セキュリティスタイルは、データにアクセスできるクライアントタイプとできないクライアントタイプを決定しないことを理解することが重要です。セキュリティスタイルは、FSx for ONTAP がデータアクセスを制御するために使用するアクセス許可のタイプと、これらのアクセス許可を変更できるクライアントタイプのみを決定します。

ボリュームのセキュリティスタイルを決定するために使用する 2 つの要因は、ファイルシステムを管理する管理者のタイプと、ボリューム上のデータにアクセスするユーザーまたはサービスのタイプです。

Amazon FSx コンソール、CLI、および API でボリュームを作成する場合、セキュリティスタイルは自動的にルートボリュームのセキュリティスタイルに設定されます。ボリュームのセキュリティスタイルは、 AWS CLI または API を使用して変更できます。この設定は、ボリュームの作成後に変更できます。詳細については、「ボリュームの更新」を参照してください。

ボリュームにセキュリティスタイルを設定するときは、環境のニーズを考慮して、許可の管理に関する問題を回避するために最適なセキュリティスタイルを選択するようにしてください。セキュリティスタイルによって、データにアクセスできるクライアントタイプが決まるわけではありません。セキュリティスタイルによって、データアクセスを許可するために使用する許可およびその許可を変更できるクライアントタイプが決まります。ボリュームに対して選択するセキュリティスタイルの決定に役立つ考慮事項は、次のとおりです。

- Unix (Linux) - ファイルシステムが Unix 管理者によって管理され、大多数のユーザーが NFS クライアントであり、データにアクセスするアプリケーションが UNIX ユーザーをサービスアカウントとして使用する場合は、このセキュリティスタイルを選択します。Unix セキュリティスタイルで許可を変更できるのは Linux クライアントのみです。ファイルおよびディレクトリで使用される許可のタイプはモードビットまたは NFS v4.x ACL です。
- NTFS - ファイルシステムが Windows 管理者によって管理され、大多数のユーザーが SMB クライアントであり、データにアクセスするアプリケーションが Windows ユーザーをサービスアカウントとして使用する場合は、このセキュリティスタイルを選択します。ボリュームへの Windows アクセスが必要な場合は、NTFS セキュリティスタイルの使用をお勧めします。NTFS セキュリティスタイルでアクセス許可を変更できるのは Windows クライアントのみです。ファイルおよびディレクトリで使用されるアクセス許可の種類は NTFS ACL です。
- [Mixed] (混合) — これは高度な設定です。詳細については、「NetApp ドキュメントセンター」の「セキュリティ形式とその影響とは」を参照してください。

ボリュームの作成

ONTAP コマンドラインインターフェイス (CLI) と REST API に加えて、Amazon FSx コンソール AWS CLI、、および Amazon FSx API を使用して、FSx FSx for NetApp ONTAP FlexVolまたは FlexGroupボリュームを作成できます。

FlexVol ボリュームを作成するには (コンソール)

> **Note**
>
> ボリュームのセキュリティスタイルは、ルートボリュームのセキュリティスタイルに自動的に設定されます。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ナビゲーションペインで [ボリューム] を選択します。
3. [Create volume] (ボリュームの作成) を選択します。
4. ファイルシステムタイプ で、Amazon FSx for NetApp ONTAP を選択します。
5. [ファイルシステムの詳細] セクションで、以下の情報を入力します。
   - [File systems] (ファイルシステム) で、ボリュームを作成するファイルシステムを選択します。

- [Storage virtual machine] (ストレージ仮想マシン) で、このボリュームを作成するストレージ仮想マシン (SVM) を選択します。

6. [ボリュームスタイル] セクションで、[FlexVol] を選択します。
7. [ボリュームの詳細] セクションで、以下の情報を入力します。

   - [Volume name] (ボリューム名) フィールドに、ボリュームの名前を入力します。英数字とアンダースコア (_) で最大 203 文字まで使用できます。
   - [ボリュームサイズ] に、20～314572800 の範囲で任意の整数を入力し、サイズをメビバイト (MiB) 単位で指定します。
   - [ボリュームタイプ] では、読み取りと書き込みが可能なボリュームを作成するには [Read-Write (RW)] を選択し、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用できる読み取り専用のボリュームを作成するには [Data Protection (DP)] を選択します。詳細については、「ボリュームの種類」を参照してください。
   - [Junction path] (ジャンクションパス) で、ボリュームをマウントするファイルシステム内の場所を入力します。`/vol3` のように、名前の先頭にスラッシュを付ける必要があります。
   - [Storage efficiency] (ストレージ効率) で、[Enabled] (有効) ONTAP ストレージ効率機能 (重複排除、圧縮、コンパクト化) を有効にします。詳細については、「FSx for ONTAP ストレージの効率化」を参照してください。
   - [ボリュームのセキュリティスタイル] では、ボリュームに対して、[Unix (Linux)]、[NTFS]、[混合] から選択します。詳細については、「ボリュームセキュリティスタイル」を参照してください。
   - [Snapshot policy] (スナップショットポリシー) で、ボリュームのスナップショットポリシーを選択します。スナップショットポリシーの詳細については、スナップショットポリシー を参照してください。

     [Custom policy] (カスタムポリシー) を選択した場合は、[custom-policy] (カスタムポリシー) フィールドにポリシーの名前を指定する必要があります。カスタムポリシーは SVM またはファイルシステムにすでに存在している必要があります。ONTAP CLI または REST API を使用して、カスタムスナップショットポリシーを作成することができます。詳細については、「NetApp ONTAP 製品ドキュメント」の「スナップショットポリシーを作成する」を参照してください。

8. [ストレージの階層化] セクションで、以下の情報を入力します。

- 容量プールの階層化ポリシー で、ボリュームのストレージプール階層化ポリシーを選択し、自動 (デフォルト)、スナップショットのみ、すべて、または なし のいずれかを選択します。詳細については、「ボリューム階層化ポリシー」を参照してください。
- [自動] または [スナップショットのみ] を選択した場合は、[階層化ポリシーの冷却期間] を設定して、アクセスされていないデータがコールドとマークされて容量プールストレージに移動されるまでの日数を定義できます。2～183 日の値を指定できます。デフォルト設定は 31 日間。

9. [詳細設定] セクションの [SnapLock 設定] で、[有効] または [無効] を選択します。SnapLock の Compliance ボリュームまたは SnapLock の Enterprise ボリュームの設定の詳細については、「SnapLock Compliance ボリュームの作成」および「SnapLock Enterprise ボリュームの作成」を参照してください。SnapLock の詳細については、「によるデータの保護 SnapLock」を参照してください。
10. [Confirm] (確認) を選択してボリュームを作成します。

更新の進捗状況は、[Status] (ステータス) の列にある [Volumes] (ボリューム) ペインの [File systems] (ファイルシステム) 詳細ページでモニタリングできます。ステータスが [Created] (作成) になったら、ボリュームが使用可能な状態になります。

FlexGroup ボリュームを作成するには (コンソール)

> **Note**
>
> Amazon FSx コンソールを使用して作成できるのは、スケールアウトファイルシステム用の FlexGroup ボリュームのみです。スケールアウトファイルシステムのFlexVolボリュームを作成するには、 AWS CLI、Amazon FSx API、または NetApp 管理ツールを使用します。

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ナビゲーションペインで [ボリューム] を選択します。
3. [Create volume] (ボリュームの作成) を選択します。
4. ファイルシステムタイプ で、Amazon FSx for NetApp ONTAP を選択します。
5. [ファイルシステムの詳細] セクションで、以下の情報を入力します。
   - [File systems] (ファイルシステム) で、ボリュームを作成するファイルシステムを選択します。

- [Storage virtual machine] (ストレージ仮想マシン) で、このボリュームを作成するストレージ仮想マシン (SVM) を選択します。

6. ボリュームスタイル セクションで、 を選択しますFlexGroup。
7. [ボリュームの詳細] セクションで、以下の情報を入力します。

- [Volume name] (ボリューム名) フィールドに、ボリュームの名前を入力します。英数字とアンダースコア (_) で最大 203 文字まで使用できます。
- [ボリュームサイズ] に、800 ギビバイト (GiB) ~ 2,000 ペビバイト (PiB) の範囲で任意の整数を入力します。
- [ボリュームタイプ] では、読み取りと書き込みが可能なボリュームを作成するには [Read-Write (RW)] を選択し、NetApp SnapMirror または SnapVault 関係のデスティネーションとして使用できる読み取り専用のボリュームを作成するには [Data Protection (DP)] を選択します。詳細については、「ボリュームの種類」を参照してください。
- [Junction path] (ジャンクションパス) で、ボリュームをマウントするファイルシステム内の場所を入力します。`/vol3` のように、名前の先頭にスラッシュを付ける必要があります。
- [Storage efficiency] (ストレージ効率) で、[Enabled] (有効) ONTAP ストレージ効率機能 (重複排除、圧縮、コンパクト化) を有効にします。詳細については、「FSx for ONTAP ストレージの効率化」を参照してください。
- [ボリュームのセキュリティスタイル] では、ボリュームに対して、[Unix (Linux)]、[NTFS]、[混合] から選択します。詳細については、「ボリュームセキュリティスタイル」を参照してください。

  > **Note**
  >
  > ボリュームのセキュリティスタイルは、ルートボリュームのセキュリティスタイルに自動的に設定されます。

- [Snapshot policy] (スナップショットポリシー) で、ボリュームのスナップショットポリシーを選択します。スナップショットポリシーの詳細については、スナップショットポリシー を参照してください。

  [Custom policy] (カスタムポリシー) を選択した場合は、[custom-policy] (カスタムポリシー) フィールドにポリシーの名前を指定する必要があります。カスタムポリシーは SVM またはファイルシステムにすでに存在している必要があります。ONTAP CLI または REST API を使用して、カスタムスナップショットポリシーを作成することができます。詳細については、

「NetApp ONTAP 製品ドキュメント」の「スナップショットポリシーを作成する」を参照してください。

8. [ストレージの階層化] セクションで、以下の情報を入力します。
   - 容量プールの階層化ポリシー で、ボリュームのストレージプール階層化ポリシーを選択し、自動 (デフォルト)、スナップショットのみ、すべて、または なし のいずれかを選択します。詳細については、「ボリューム階層化ポリシー」を参照してください。
   - [自動] または [スナップショットのみ] を選択した場合は、[階層化ポリシーの冷却期間] を設定して、アクセスされていないデータがコールドとマークされて容量プールストレージに移動されるまでの日数を定義できます。2 ~ 183 日の値を入力できます。デフォルト設定は 31 日間。
9. [詳細設定] セクションの [SnapLock 設定] で、[有効] または [無効] を選択します。SnapLock の Compliance ボリュームまたは SnapLock の Enterprise ボリュームの設定の詳細については、「SnapLock Compliance ボリュームの作成」および「SnapLock Enterprise ボリュームの作成」を参照してください。SnapLock の詳細については、「によるデータの保護 SnapLock」を参照してください。
10. [Confirm] (確認) を選択してボリュームを作成します。

更新の進捗状況は、[Status] (ステータス) の列にある [Volumes] (ボリューム) ペインの [File systems] (ファイルシステム) 詳細ページでモニタリングできます。ステータスが [Created] (作成) になったら、ボリュームが使用可能な状態になります。

ボリュームを作成するには (CLI)

- FSx for ONTAP ボリュームを作成するには、次の例に示すように、create-volume CLI コマンド (または同等の CreateVolume API オペレーション) を使用します。

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

ボリュームが正常に作成されると、Amazon FSx は、次の例に示すように、その説明を JSON 形式で返します。


```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```


ボリュームのバックアップを新しいボリュームに復元して、新しいボリュームを作成することもできます。詳細については、「バックアップを新しいボリュームに復元する」を参照してください。

ボリュームの更新

ONTAP コマンドラインインターフェイス (CLI) と REST API に加えて、Amazon FSx コンソール AWS CLI、、および Amazon FSx API を使用して、FSx FSx for NetApp ONTAP ボリュームの設定を更新できます。既存の FSx for ONTAP ボリュームの次のプロパティを変更できます。

- ボリューム名
- ジャンクションパス
- ボリュームサイズ
- ストレージ効率
- 容量プールの階層化ポリシー
- ボリュームセキュリティスタイル
- スナップショットポリシー
- 階層化ポリシーの冷却期間
- タグをバックアップにコピーする (AWS CLI および Amazon FSx API を使用)

詳細については、「FSx for ONTAP ボリュームの管理」を参照してください。

ボリューム設定を更新するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [File systems] (ファイルシステム) に移動してボリュームを更新する ONTAP ファイルシステムを選択します。
3. [Volumes] (ボリューム) タブを選択します。
4. 更新するボリュームを選択します。
5. [Action] (アクション) で、[Update volume] (ボリュームの更新) を選択します。

   [Update volume] (ボリュームの更新) ダイアログボックスに、現在のボリューム設定が表示されます。
6. [Junction path] (ジャンクションパス) で、ボリュームをマウントするファイルシステム内の既存の場所を入力します。名前の先頭には `/vol15` のようにスラッシュが入らなければなりません。
7. [ボリュームサイズ] については、Amazon FSx コンソールで指定された範囲内でボリュームのサイズを増減できます。FlexVol ボリュームの最大サイズは 300 TiB です。FlexGroup ボリュームの場合、最大サイズは 300 TiB に FlexGroup の構成ボリュームの総数を掛けたもので、最大は 20 PiB です。
8. ストレージ効率 で、[Enabled] (有効) ONTAP ストレージ効率化機能 (重複排除、圧縮、コンパクト化) を有効にするか、[Disabled] (無効) をクリックして無効にします。
9. 容量プールの階層化ポリシー で、[Auto] (自動) (デフォルト)、[Snapshot-only] (スナップショットのみ)、[All] (すべて)、または [None] (なし) が選択できるボリュームの新しいストレージプー

ル階層化ポリシーを選択します。容量プールの階層化ポリシーの詳細については、「ボリューム階層化ポリシー」を参照してください。

10. [ボリュームのセキュリティスタイル] には、[UNIX (Linux)]、[NTFS]、または [混合] のいずれかを選択します。ボリュームのセキュリティスタイルによって、マルチプロトコルアクセスで NTFS ACL と UNIX ACL のどちらを優先するかが決まります。MIXED モードはマルチプロトコルアクセスには必要なく、上級ユーザーにのみ推奨されます。
11. [Snapshot policy] (スナップショットポリシー) で、ボリュームのスナップショットポリシーを選択します。スナップショットポリシーの詳細については、スナップショットポリシー を参照してください。

    [Custom policy] (カスタムポリシー) を選択した場合は、[custom-policy] (カスタムポリシー) フィールドにポリシーの名前を指定する必要があります。カスタムポリシーは SVM またはファイルシステムにすでに存在している必要があります。ONTAP CLI または REST API を使用して、カスタムスナップショットポリシーを作成することができます。詳細については、「NetApp ONTAP 製品ドキュメント」の「スナップショットポリシーを作成する」を参照してください。
12. [階層化ポリシーの冷却期間] の有効値は 2～183 日です。ボリュームの階層化ポリシーの冷却期間は、アクセスされていないデータがコールドとしてマークされ、容量プールストレージに移動されるまでの日数を定義します。この設定は `Auto` ポリシーと `Snapshot-only` ポリシーにのみ影響します。
13. [Update] (更新) をクリックして、ボリュームを更新します。

ボリュームの設定を更新するには (CLI)

- FSx for ONTAP ボリュームの設定を更新するには、次の例に示すように、update-volume CLI コマンド (または同等の UpdateVolume API オペレーション) を使用します。

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

ボリュームの削除

ONTAP コマンドラインインターフェイス (CLI) と REST API に加えて、Amazon FSx コンソール AWS CLI、、および Amazon FSx API を使用して FSx FSx for NetApp ONTAP ボリュームを削除できます。

> **Important**
>
> ボリュームの削除は、ボリュームで Amazon FSx バックアップが有効になっている場合に、Amazon FSx コンソール、API、CLI を使用してのみ実行できます。

> **Important**
>
> Amazon FSx コンソールを使用してボリュームを削除する場合、ボリュームの最終バックアップを作成することを選択できます。バックアップから新しいボリュームを作成できます。ベストプラクティスとして、最終的なバックアップを取ることをお勧めします。一定期間後に不要になった場合は、これと他の手動で作成されたボリュームバックアップを削除できます。`delete-volume` CLI コマンドを使用してボリュームを削除する場合は、Amazon FSx はデフォルトで最終バックアップを作成します。

ボリュームを削除する前に、削除するボリューム内のデータにアクセスするアプリケーションがないことを確認します。

ボリュームを削除するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左のナビゲーションペインで、[File systems] (ファイルシステム) を選択し、ボリュームを削除する ONTAP ファイルシステムを選択します。
3. [Volumes] (ボリューム) タブを選択します。
4. 削除するボリューム を選択します。
5. [Action] (アクション) では、[Delete volume] (ボリュームの削除) を選択します。
6. 確認ダイアログボックス内の [Create final backup] (最終バックアップの作成) には、2 つのオプションがあります。

- [Yes] (はい) を選択してボリュームの最終バックアップを作成します。最終バックアップの名前が表示されます。
- ボリュームの最終バックアップが必要ない場合は [No] (なし) を選択します。ボリュームを削除すると、自動バックアップは使用できなくなることを確認するよう求められます。

7. 削除の確認 フィールドに 削除する と入力し、ボリュームの削除を確認します。
8. [Delete volume] (ボリュームの削除) を選択します。

ボリュームを削除するには (CLI)

- FSx for ONTAP ボリュームを削除するには、次の例に示すように、delete-volume CLI コマンド (または同等の DeleteVolume API オペレーション) を使用します。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

ボリュームの表示

Amazon FSx コンソール、、Amazon FSx API AWS CLIおよび SDKs を使用して、ファイルシステム上に現在ある FSx for ONTAP ボリュームを表示できます。

ファイルシステム上のボリュームを表示するには

- [Using the console] (コンソールの使用) - [File systems] (ファイルシステム) 詳細ページを表示するにはファイルシステムを選択します。[Volumes] (ボリューム) タブをクリックして、ファイルシステム上のすべてのボリュームをリスト表示し、表示するボリュームを選択します。
- CLI または API の使用 – describe-volumes CLI コマンドまたは DescribeVolumes API オペレーションを使用します。

iSCSI LUN の作成

このプロセスでは、ONTAP CLI lun create コマンドを使用して Amazon FSx for NetApp ONTAP スケールアップファイルシステムに iSCSI LUN NetApp を作成する方法について説明します。詳細については、 NetApp ONTAP ドキュメントセンターlun createの「」を参照してください。

> **Note**
>
> iSCSI プロトコルはスケールアウトファイルシステムではサポートされていません。

このプロセスは、ファイルシステム上にボリュームがすでに作成されていることを前提としています。詳細については、「ボリュームの作成」を参照してください。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
2. lun create NetApp CLI コマンドを使用して LUN を作成し、次の値を置き換えます。

   - ***svm_name*** - iSCSI ターゲットを提供するストレージ仮想マシン (SVM) の名前。ホストはこの値を使用して LUN に到達します。
   - ***vol_name*** - LUN をホストするボリュームの名前。
   - ***lun_name*** - LUN に割り当てる名前。
   - ***size*** - LUN のバイト単位のサイズ。作成できる LUN の最大サイズは 128 TB です。

     > **Note**
     >
     > LUN サイズより 5% 以上大きいボリュームを使用することをお勧めします。このマージンは、ボリュームスナップショット用のスペースを残します。

   - ***ostype*** - ホストのオペレーティングシステム (`windows_2008` または `linux`)。Windows のすべてのバージョンで `windows_2008` を使用します。これにより、LUN がオペレーティングシステムに対する適切なブロックオフセットを確保し、パフォーマンスが最適化されます。

> **Note**
>
> LUN でスペース割り当てを有効にすることをお勧めします。スペース割り当てを有効にすると、ONTAP は LUN の容量が不足したときにホストに通知し、LUNからデータを削除するときにスペースを再利用できます。

詳細については、 NetApp ONTAP CLI ドキュメントlun createの「」を参照してください。

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. LUN が作成され、オンライン、およびマッピングされていることを確認します。

```
> lun show
```

システムは次の出力でレスポンスします。

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

次のステップ

iSCSI LUN を作成したので、iSCSI LUN をブロックストレージとして使用するプロセスの次のステップは、LUN を igroup にマップすることです。詳細については、「Linux クライアントへの iSCSI LUN のマウント」または「Windows クライアントへの iSCSI LUN のマウント」を参照してください。

SMB 共有の管理

Amazon FSx ファイルシステム SMB ファイル共有を管理するには、Microsoft Windows 共有フォルダ GUI を使用できます。共有フォルダ GUI は、ストレージ仮想マシン (SVM) 内のすべての共有

フォルダを一元管理する場所を提供します。次の手順では、ファイル共有を作成、更新、削除する方法を詳しく示します。

> **Note**
>
> NetApp System Manager を使用して SMB ファイル共有を管理することもできます。詳細については、「での NetApp System Manager の使用 BlueXP」を参照してください。

共有フォルダを Amazon FSx ファイルシステムに接続するには

1. Amazon EC2 インスタンスを起動し、Amazon FSx ファイルシステムと結合している Microsoft アクティブディレクトリに接続します。これを行うには、AWS Directory Service 管理ガイドから次のいずれかの手順を選択します。
   - Windows EC2 インスタンスにシームレスに接続する
   - Windows インスタンスを手動で結合させる
2. ファイルシステム管理者グループのメンバーであるユーザーとしてインスタンスに接続します。詳細については、Amazon EC2 ユーザーガイド」の「Windows インスタンスへの接続」を参照してください。
3. [Start] (スタート) メニューを開き、[Run As Administrator] (管理者として実行) を使用して fsmgmt.msc を実行します。これにより、共有フォルダ GUI ツールが開きます。
4. [Action] (アクション) で、[Connect to another computer] (別のコンピュータに接続する) を選択します。
5. [Another computer] (別のコンピュータ) で、ストレージ仮想マシン (SVM) の DNS 名、例えば **`netbios_name.corp.example.com`** を入力します。

   Amazon FSx コンソールで SVM の DNS 名を確認するには、[Storage virtual machines] (ストレージ仮想マシン) を選択し、該当する SVM を選択してから [SMB DNS name] (SMB DNS 名) が見つかるまで [Endpoints] (エンドポイント) に向かってスクロールダウンします。DescribeStorageVirtualMachines API オペレーションのレスポンスで DNS 名を取得することもできます。
6. OK を選択します。Amazon FSx ファイルシステムのエントリが共有フォルダツールのリストに表示されます。

これで、共有フォルダが Amazon FSx ファイルシステムに接続されたので、次の操作を実行して、ファイルシステム上の Windows ファイル共有を管理できます。

> **Note**
>
> SMB 共有は、ルートボリューム以外のボリュームに配置することをお勧めします。

- ファイル共有の新規作成 - 共有フォルダツール内の左側ペインにある [Shares] (共有) を選択して、Amazon FSx ファイルシステムのアクティブな共有を表示します。ボリュームは、ボリューム作成時に選択したパスにマウントされて表示されます。[New Share] (新規共有) を選択し、共有フォルダの作成ウィザードを完了します。

  新規のファイル共有を作成する前に、ローカルフォルダを作成する必要があります。次の手順で行います。

  - 共有フォルダツールの使用:ローカルフォルダパスを指定するときは、[Browse] (ブラウズ) を選択し、ローカルフォルダを作成するときは [Make new folder] (フォルダの新規作成) を選択します。
  - コマンドラインの使用

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```

- ファイル共有の変更 - 共有フォルダツール内の右側のペインで、変更するファイル共有のコンテキスト (右クリック) メニューを開き、[Properties] (プロパティ) を選択します。プロパティを変更し、OK を選択します。
- ファイル共有を削除する - 共有フォルダツール内の右側のペインで、削除するファイル共有のコンテキスト (右クリック) メニューを開き、[Stop Sharing] (共有を停止する) を選択します。

> **Note**
>
> GUI でファイル共有を削除できるのは、Amazon FSx ファイルシステムの DNS 名を使用して fsmgmt.msc に接続したときのみです。ファイルシステムの IP アドレスまたは DNS エイリアス名を使用して接続した場合は、[Stop Sharing] (共有を停止する) オプションが機能しないため、ファイル共有は削除されません。

ファイルアクセスの監査

Amazon FSx for NetApp ONTAP は、ストレージ仮想マシン (SVM) 内のファイルやディレクトリへのエンドユーザーアクセスの監査をサポートしています。

トピック

ファイルアクセス監査の概要

ファイルアクセス監査では、定義した監査ポリシーに基づいて、エンドユーザーによる個々のファイルやディレクトリへのアクセスをレコードできます。ファイルアクセス監査は、システムのセキュリティを向上させ、システムデータへの不正アクセスのリスクを軽減するのに役立ちます。ファイルアクセス監査は、組織がデータ保護要件への準拠を維持し、潜在的な脅威を早期に特定し、データ違反のリスクを軽減するのに役立ちます。

Amazon FSx は、ファイルおよびディレクトリアクセス全体で、成功した試行 (ファイルに正常にアクセスする十分な許可を持つユーザーなど)、失敗した試行、またはその両方のロギングをサポートしています。また、ファイルアクセス監査はいつでも無効にできます。

デフォルトでは、監査イベントログは EVTX ファイル形式で保存され、Microsoft イベントビューワーを使用して表示できます。

監査できる SMB アクセスイベント

次の表は、監査できる SMB ファイルおよびフォルダアクセスイベントを示しています。

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
560/4656	オブジェクトを開く / オブジェクトを作成	オブジェクトアクセス: オブジェクト (ファイルまたはディレクトリ) を開く	ファイルアクセス

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
563/4659	削除するインテントでオブジェクトを開く	オブジェクトアクセス: オブジェクト (ファイルまたはディレクトリ) へのハンドルが削除の意図でリクエストされました	ファイルアクセス
564/4660	オブジェクトの削除	オブジェクトアクセス: オブジェクト (ファイルまたはディレクトリ) を削除します。ONTAP は、Windows クライアントがオブジェクト (ファイルまたはディレクトリ) の削除を試みるとこのイベントを生成します。	ファイルアクセス

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
567/4663	オブジェクトの読み取り / オブジェクトの書き込み / オブジェクト属性の取得 / オブジェクト属性の設定	オブジェクトアクセス: オブジェクトアクセスの試み (読み取り、書き込み、属性の取得、属性の設定)。 Note このイベントでは、ONTAP はオブジェクトに対する最初の SMB 読み取りおよび最初の SMB 書き込みオペレーション (成功または障害) のみを監査します。これにより、1 つのクライアントがオブジェクトを開き、同じオブジェクトに対して多数の連続する読み取りまたは書き込み操作を実行するときに、ONTAP による過剰な	ファイルアクセス

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
		ログエントリ作成を防ぎます。	
N / A / 4664	ハードリンク	オブジェクトアクセス: ハードリンクの作成を試みました	ファイルアクセス
N / A / N / A ONTAP イベント ID 9999	オブジェクトの名前を変更	オブジェクトアクセス: オブジェクトの名前が変更されました。これは ONTAP イベントです。現在、Windows では 1 つのイベントとしてサポートされていません。	ファイルアクセス
N / A / N / A ONTAP イベント ID 9998	オブジェクトのリンク解除	オブジェクトアクセス: オブジェクトのリンクが解除されました。これは ONTAP イベントです。現在、Windows では 1 つのイベントとしてサポートされていません。	ファイルアクセス

監査できる NFS アクセスイベント

次の NFS ファイルおよびフォルダアクセスイベントを監査できます。

- READ
- OPEN

- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

ファイルアクセス監査を設定するためのタスクの概要

ファイルアクセス監査に FSx for ONTAP を設定するには以下の高レベルのタスクが必要です。

1. ファイルアクセス監査の要件と考慮事項をよく 理解 してください。
2. 特定の SVM で 監査設定を作成する。
3. その SVM で 監査を有効化 する。
4. ファイルとディレクトリに 監査ポリシーを設定する。
5. FSx for ONTAP が放出した後、監査イベントログを表示する。

次の手順で、タスクの詳細を示します。

ファイルアクセス監査を有効にするファイルシステム上の他の SVM に対して、タスクを繰り返します。

監査要件

SVM で監査を設定および有効にする前に、次の要件と考慮事項に注意する必要があります。

- NFS 監査では、u タイプとして指定された監査アクセスコントロールエントリ (ACE) がサポートされ、オブジェクトへのアクセスの試みがあると、監査ログエントリが生成されます。NFS 監査では、モードビットと監査 ACE の間にマッピングはありません。ACL をモードビットに変換する

場合、監査 ACE はスキップされます。モードビットを ACL に変換する場合、監査 ACE は生成されません。

- 監査は、ステージングボリュームに空き領域があるかどうかによって異なります。(ステージングボリュームは、ONTAP によってステージングファイルを保存するために作成される専用ボリュームで、ステージングファイルは、EVTX または XML ファイル形式への変換前に監査レコードが格納される個々のノードの中間バイナリファイルです)。監査ボリュームを含むアグリゲート内のステージングボリュームに十分なスペースがあることを確認する必要があります。
- 監査は、変換された監査イベントログが格納されているディレクトリを含むボリューム内の使用可能な領域があるかどうかによって異なります。イベントログの保存に使用するボリュームに十分な領域があることを確認する必要があります。監査設定の作成時に `-rotate-limit` パラメータを使用することで、監査ディレクトリに保持する監査ログの数を指定できます。これは、ボリューム内の監査ログに十分な空き領域があることを確認するのに役立ちます。

SVM での監査設定の作成

ファイルおよびディレクトリイベントの監査を開始する前に、ストレージ仮想マシン (SVM) で監査設定を作成する必要があります。監査設定の作成後、SVM で有効にする必要があります。

`vserver audit create` コマンドを使用して監査設定を作成する前に、ログの宛先として使用するディレクトリを作成し、ディレクトリにシンボリックリンクがないことを確認します。`-destination` パラメータで宛先ディレクトリを指定します。

次のように、ログサイズまたはスケジュールに基づいて監査ログをローテーションする監査設定を作成できます。

- ログサイズに基づいて監査ログをローテーションするには、このコマンドを使用します。

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

次の例では、サイズベースのローテーションを使用して、ファイル操作と CIFS (SMB) のログインおよびログオフイベント (デフォルト) を監査する `svm1` という名前の SVM の監査設定を作成します。ログ形式は EVTX (デフォルト)で、ログは `/audit_log` ディレクトリに保存され、一度に 1 つのログファイル (最大サイズ 200 MB) が作成されます。

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- スケジュールに基づいて監査ログをローテーションするには、このコマンドを使用します。

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

時間ベースの監査ログローテーションを設定する場合は、-rotate-schedule-minute パラメータが必要です。

次の例では、時間ベースのローテーションを使用して、svm2 という名前の SVM の監査設定を作成します。ログ形式は EVTX (デフォルト) で、監査ログは毎月、すべての曜日の午後 12 時 30 分にローテーションされます。

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

-format パラメータを使用して、監査ログが変換された EVTX 形式 (デフォルト) または XML ファイル形式で作成されるかどうかを指定できます。EVTX 形式を使用すると、Microsoft イベントビューワーでログファイルを表示できます。

デフォルトでは、監査されるイベントのカテゴリは、ファイルアクセスイベント (SMB と NFS の両方)、CIFS (SMB) のログオンおよびログオフイベント、および認可ポリシー変更イベントです。次の形式の -events パラメータを使用して、ログに記録するイベントをより細かくコントロールできます。

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

例えば、-events file-share ファイル共有イベントの監査を有効にします。

vserver audit create コマンドの詳細については、「Create an audit configuration」(監査設定を作成する) を参照してください。

SVM での監査の有効化

監査設定の設定が完了したら、SVM で監査を有効にする必要があります。そのためには、次のコマンドを使用します。

```
vserver audit enable -vserver svm_name
```

例えば、svm1 という名前の SVM の監査を有効にするには、次のコマンドを使用します。

```
vserver audit enable -vserver svm1
```

アクセス監査の作成はいつでも無効にできます。例えば、次のコマンドを使用して、svm4 という名前の SVM の監査をオフにします。

```
vserver audit disable -vserver svm4
```

監査を無効にしても、SVM 上の監査設定は削除されません。つまり、その SVM の監査をいつでも再度有効にできます。

ファイルおよびフォルダの監査ポリシーを設定する

ユーザーアクセスの試みを監査するファイルおよびフォルダーに監査ポリシーを設定する必要があります。監査ポリシーは、アクセス試行の成功と失敗の両方を監視するように設定できます。

SMB と NFS の両方の監査ポリシーを設定できます。SMB および NFS 監査ポリシーは、ボリュームのセキュリティスタイルに基づいて、設定要件と監査機能が異なります。

NTFS セキュリティスタイルのファイルおよびディレクトリに関する監査ポリシー

NTFS 監査ポリシーは、Windows のセキュリティタブまたは ONTAP CLI を使用して設定できます。

NTFS 監査ポリシーを設定するには (Windows のセキュリティタブ)

NTFS 監査ポリシーを設定するには、NTFS セキュリティ記述子に関連付けられた NTFS SACL にエントリを追加します。その後、セキュリティ記述子は NTFS ファイルとディレクトリに適用されます。タスクは Windows GUI によって自動的に処理されます。セキュリティ記述子には、ファイルとフォルダのアクセス許可を適用するための随意アクセスコントロールリスト (DACL)、ファイルとフォルダの監査のための SACL、または SACL と DACL の両方を含めることができます。

1. Windows エクスプローラーの [Tools] (ツール) メニューから [Map network drive] (ネットワークドライブのマップ) を選択します。
2. [Map Network Drive] (ネットワークドライブのマップ) ボックスを完了します。

a. [Drive] (ドライブ) 文字を選択します。

b. [Folder] (フォルダ) ボックスに、監査するデータと共有する名前を保持している共有を含む SMB (CIFS) サーバ名を入力します。

c. [Finish] (終了) を選択します。

選択したドライブがマウントされ、共有に含まれるファイルとフォルダを表示する Windows エクスプローラウィンドウで準備ができました。

3. 監査アクセスを有効にするファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、[Properties] (プロパティ) を選択します。
5. [Security] (セキュリティ) タブを選択します。
6. [Advanced] (アドバンスト) をクリックします。
7. [Auditing] (監査) タブを選択します。
8. 目的のアクションを実行します。

目的が	次の作業を行います。
新しいユーザーまたはグループの監査を設定する	1. [Add] (追加) を選択します。 2. [Enter the object name to select] (選択するオブジェクト名を入力する) ボックスで、追加するユーザーまたはグループの名前を入力します。 3. OK を選択します。
ユーザーまたはグループから監査を削除する	1. [Enter the object name to select] ボックスで、削除するユーザーまたはグループを選択します。 2. [Remove] (削除) を選択します。 3. OK を選択します。 4. この手順の残りをスキップします。
ユーザーまたはグループの監査を変更する	1. [Enter the object name to select] ボックスで、変更するユーザーまたはグループを選択します。 2. [Edit] (編集) を選択します。 3. OK を選択します。

ユーザーまたはグループの監査を設定する場合、または既存のユーザーまたはグループの監査を変更する場合は、**######** の監査エントリ ボックスが開きます。

9. [Apply to] (適用先) ボックスで、この監査エントリの適用方法を選択します。

   単一のファイルに対して監査を設定する場合は、[Apply to] ボックスは、既定で [This object only] (このオブジェクトのみ) に設定されているため、アクティブではありません。

10. [Access] (アクセス) ボックスで、監査対象を選択し、成功イベント、障害イベント、またはその両方を監査するかどうかを選択します。

    - 成功したイベントを監査するには、[Success] (成功) ボックスを選択します。
    - 障害イベントを監査するには、[Failure] (障害) ボックスを選択します。

    セキュリティ要件を満たすために監視する必要があるアクションを選択します。監査可能なイベントの詳細については、Windows ドキュメントを参照してください。次のイベントを監査できます。

    - フルコントロール
    - トラバースフォルダー / ファイルを実行
    - フォルダの一覧表示 / データの読み取り
    - 属性の読み取り
    - 拡張属性の読み取り
    - ファイルの作成 / データの書き込み
    - フォルダの作成 / データの追加
    - 属性の書き込み
    - 拡張属性の書き込み
    - サブフォルダとファイルの削除
    - 削除
    - 読み取りアクセス許可
    - 許可の変更
    - 所有権の取得

11. 監査設定を元のコンテナの後続のファイルおよびフォルダに伝搬しない場合は、[Apply these auditing entries to objects and/or containers within this container only] (監査エントリをこのコンテナ内のオブジェクトやコンテナにのみ適用する) ボックスを選択します。
12. [Apply] (適用する) を選択します。
13. 監査エントリの追加、削除、または編集が完了したら、OK を選択します。

    ###### の監査エントリ ボックスが閉じます。
14. [Auditing] (監査) ボックスで、このフォルダの継承設定を選択します。セキュリティ要件を満たす監査イベントを提供する最小レベルのみを選択します。

    次のいずれかを選択できます。

    - [Include inheritable auditing entries from this object's parent] (このオブジェクトの親から継承可能な監査エントリを含める) ボックスを選択します。
    - [Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object] (すべての子孫にある既存の継承可能な監査エントリを、このオブジェクトの継承可能な監査エントリで置き換える) ボックスを選択します。
    - 両方のボックスを選択します。
    - どちらのボックスも選択しないでください。

    単一のファイルに SACL を設定する場合は、[Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object] ボックスは [Auditing] (監査) ボックスに存在しません。
15. OK を選択します。

NTFS 監査ポリシーを設定するには (ONTAP CLI)

ONTAP CLI を使用すると、Windows クライアントの SMB 共有を使用してデータに接続することなく、NTFS 監査ポリシーを設定できます。

- NTFS 監査ポリシーは、vserver セキュリティファイルディレクトリ コマンドファミリーを使用して設定できます。

例えば、次のコマンドは、p1 という名前のセキュリティポリシーを vs0 という名前の SVM に適用します。

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

UNIX セキュリティスタイルのファイルおよびディレクトリに関する監査ポリシー

NFS v4.x ACL (アクセスコントロールリスト) に監査 ACE (アクセスコントロール表現) を追加することにより、UNIX セキュリティスタイルのファイルとディレクトリの監査を設定します。これにより、セキュリティ上の目的で、特定の NFS ファイルおよびディレクトリアクセスイベントをモニタリングできます。

> **Note**
>
> NFS v4.x の場合、任意の ACE とシステム ACE の両方が同じ ACL に格納されます。したがって、既存の ACL に監査 ACE を追加するときは、既存の ACL を上書きして失わないように注意する必要があります。既存の ACL に監査 ACE を追加する順序は重要ではありません。

UNIX 監査ポリシーを設定するには

1. `nfs4_getfacl` または同等のコマンドを使用して、ファイルまたはディレクトリの既存の ACL を取得します。
2. 目的の監査 ACE を追加します。
3. `nfs4_setfacl` または同等のコマンドを使用して、更新された ACL をファイルまたはディレクトリに適用します。

   この例では `-a` のオプションを使用してユーザー (`testuser` という名前) に `file1` という名前のファイルに対する読み取り許可を与えます。

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

監査ログの表示

EVTX または XML ファイル形式に保存された監査イベントログを表示できます。

- EVTX ファイル形式 - Microsoft イベントビューワーを使用して、変換された EVTX 監査イベントログを保存済みファイルとして開くことができます。

イベントビューワーを使用してイベントログを表示するときに使用できるオプションは 2 つあります。

- 一般ビュー: イベントレコードのすべてのイベントに共通する情報が表示されます。イベントレコードのイベント固有のデータは表示されません。詳細ビューを使用して、イベント固有のデータを表示できます。
- 詳細表示: フレンドリービューと XML ビューを使用できます。フレンドリビューと XML ビューには、すべてのイベントに共通する情報と、イベントレコードのイベント固有のデータの両方が表示されます。

- XML ファイル形式 - XML ファイル形式をサポートするサードパーティーアプリケーションで、XML 監査イベントログを表示および処理できます。XML スキーマと XML フィールドの定義に関する情報がある場合は、XML 表示ツールを使用して監査ログを表示できます。

SSD ストレージ容量とプロビジョンド IOPS のスケーリング

データセットのアクティブな部分にストレージを追加する必要がある場合は、Amazon FSx for NetApp ONTAP ファイルシステムのソリッドステートドライブ (SSD) ストレージ容量を増やすことができます。そのためには、Amazon FSx コンソール、Amazon FSx API、または AWS Command Line Interface (AWS CLI) を使用します。

プライマリ SSD ストレージ容量を増やすとき、または独立したアクションとして、ファイルシステム用にプロビジョンド SSD IOPS を変更することもできます。ファイルシステムのプライマリ SSD ストレージ容量とプロビジョンド IOPS の量のスケーリングの詳細については、ファイルシステムの SSD ストレージと IOPS の更新 を参照してください。

スループット容量の管理

FSx for ONTAP は、ファイルシステムを作成するときのスループット容量を設定します。スケールアップファイルシステムのスループットキャパシティはいつでも変更できますが、スケールアウトファイルシステムのスループットキャパシティは変更できません。最大スループットキャパシティを実現するには、ファイルシステムに特定の設定が必要であることに注意してください。例えば、スケールアップファイルシステムに 4 GBps のスループットキャパシティをプロビジョニングするには、ファイルシステムに最低 5,120 GiB の SSD ストレージ容量と 160,000 SSD IOPS を使用する構成が必要です。詳細については、「スループット容量がパフォーマンスに与える影響」を参照してください。

スループット容量は、ファイルシステムをホストしているファイルサーバーがファイルデータを提供できる速度を決定する要素の 1 つです。スループット容量が高くなるのに伴い、ネットワーク、1 秒あたりのディスク読み取り I/O オペレーション (IOPS)、ファイルサーバーのデータキャッシュ容量、の各レベルが高くなります。詳細については、「パフォーマンス」を参照してください。

ファイルシステムのスループット容量を変更すると、Amazon FSx は、そのファイルシステムを動かしているファイルサーバーを切り替えます。このプロセス中にシングル AZ とマルチ AZ の両方のファイルシステムで自動フェイルオーバーとフェイルバックが発生します。これは通常、完了するまでに数分かかります。フェイルオーバーおよびフェイルバックプロセスは、NFS (Network File Sharing)、SMB (Server Message Block)、iSCSI (Internet Small Computer Systems Interface) クライアントに対して透過的であり、中断や手動による介入なしにワークロードの実行を継続できます。ファイルシステムで使用可能になると、新しいスループット容量が課金されます。

> **Note**
>
> メンテナンスアクティビティ中のデータの整合性を確保するために、FSx for ONTAP は、メンテナンスを開始する前に、すべての日和見ロックを閉じ、ファイルシステムをホストしている基になるストレージボリュームへの保留中の書き込みオペレーションを完了します。スケジュール設定されたファイルシステムのメンテナンスウィンドウ中に、システムの変更 (スループット容量の変更など) が遅れる場合があります。メンテナンスによって、次の処理が行われるまで、変更がキューに入れられることがあります。詳細については、「the section called “メンテナンスウィンドウ”」を参照してください。

トピック

スループット容量を変更するタイミング

Amazon FSx は Amazon CloudWatch と統合されたため、ファイルシステムの継続的なスループット使用レベルをモニタリングできます。ファイルシステムを介してドライブできるスループットと IOPS パフォーマンスは、ファイルシステムのスループット容量の他、特定のワークロードの特性によって異なります。原則として、ワークロードの読み取りスループット + ワークロードの書き込み

スループットを 2 倍以上サポートするのに十分なスループット容量をプロビジョニングする必要があります。CloudWatch メトリクスを使用して、パフォーマンスを向上させるためにディメンションを決定できます。詳細については、「the section called “FSx for ONTAP CloudWatch メトリクスの使用方法”」を参照してください。

> **Note**
>
> スケールアウトファイルシステムのスループットキャパシティは変更できません。

同時スループットおよびストレージスケーリングリクエストの処理方法

SSD ストレージ容量とプロビジョンド IOPS の更新ワークフローが開始される直前または進行中に、スループットキャパシティの更新をリクエストできます。Amazon FSx が 2 つのリクエストを処理する順序は次のとおりです。

- SSD/IOPS の更新とスループットキャパシティの更新を同時に送信すると、両方の要求が受け入れられます。SSD/IOPS の更新は、スループットキャパシティの更新よりも優先されます。
- SSD/IOPS 更新の進行中にスループットキャパシティの更新を送信すると、スループットキャパシティの更新リクエストが受け入れられ、SSD/IOPS の更新後に発生するようにキューに入れられます。スループットキャパシティの更新は、SSD/IOPS が更新された後 (新しい値が利用可能)、最適化ステップ中に開始されます。通常、これには 10 分もかかりません。
- スループットキャパシティの更新中に SSD/IOPS の更新を送信すると、SSD/IOPS ストレージの更新要求が受け入れられ、スループットキャパシティの更新が完了した後に開始するためにキューに入れられます (新しいスループット容量が利用可能になります)。これには通常 20 分かかります。

SSD ストレージとプロビジョンド IOPS の更新の詳細については、「ストレージ容量の管理」を参照してください。

スループット容量を変更する方法

Amazon FSx コンソール、AWS Command Line Interface (AWS CLI)、または Amazon FSx APIを使用して、ファイルシステムのスループット容量を変更できます。

ファイルシステムのスループット容量を変更するには (コンソール)

1. https://console.aws.amazon.com/fsx/で Amazon FSx コンソールを開きます。

2. [File systems] (ファイルシステム) に移動し、スループット容量を増やす ONTAP ファイルシステムを選択します。
3. [Actions] (アクション) の場合、[Update throughput capacity] (スループット容量の更新) を選択します。または、[Summary] (概要) パネルでファイルシステムの [Throughput capacity] (スループット容量) の横にある [Update] (更新) を選択します。
4. リストから [Throughput Capacity] (スループット容量) の新しい値を選択します。

> **Note**
>
> 任意の FSx for ONTAP ファイルシステムのスループット容量を変更できます。ただし、2021 年 12 月 9 日以降に作成されたファイルシステムだけが 128 MB / 秒または 256 MB / 秒のスループット容量をサポートできます。

5. [Update] (更新) を選択して、スループット容量の更新を開始します。
6. 更新の進捗状況は、[Updates] (更新) タブの [File systems] (ファイルシステム) 詳細ページでモニタリングできます。

   Amazon FSx コンソール、AWS CLI、および API を使用して、更新の進捗状況をモニタリングできます。詳細については、「スループット容量の変更のモニタリング」を参照してください。

ファイルシステムのスループット容量を変更するには (CLI)

ファイルシステムのスループット容量を変更するには、AWS CLI コマンド update-file-system を使用します。以下のパラメータを設定します。

- 更新するファイルシステムの ID への `--file-system-id`。
- `ThroughputCapacity` を、ファイルシステムを更新する目的の値に変更します。

Amazon FSx コンソール、AWS CLI、および API を使用して、更新の進捗状況をモニタリングできます。詳細については、「スループット容量の変更のモニタリング」を参照してください。

スループット容量の変更のモニタリング

Amazon FSx コンソール、API、および AWS CLI を使用して、スループット容量変更プロセスをモニタリングできます。

コンソールでのスループット容量の変更のモニタリング

[File system detail] (ファイルシステムの詳細) ウィンドウの [Updates] (更新) タブに、各更新アクションタイプの最新の更新アクションを 10 個表示できます。

スループット容量の更新アクションでは、次の情報を表示できます。

[Update type] (更新タイプ)

サポートされるタイプは [Throughput capacity] (スループット容量)、[Storage capacity] (ストレージ容量)、および [Storage optimization] (ストレージの最適化) です。

[Target value] (ターゲット値)

ファイルシステムのスループット容量を変更するのに望ましい値。

[Status] (ステータス)

更新の現在のステータス。スループット容量の更新では、指定できる値は次のとおりです。

- [Pending] (保留中) - Amazon FSx は更新リクエストを受信しましたが、処理を開始していません。
- [In progress] (進行中) - Amazon FSx が更新リクエストを処理しています。
- [Completed] (完了) - スループット容量の更新が正常に完了しました。
- [Failed] (失敗) - スループット容量の更新に失敗しました。疑問符 (?) を選択して、スループットの更新が失敗した理由の詳細を確認します。

[Request time] (リクエストタイム)

Amazon FSx が更新リクエストを受信した時刻。

AWS CLI と API で変更をモニタリングする

describe-file-systems CLI コマンドおよび DescribeFileSystems API アクションを使用して、ファイルシステムのスループット容量変更リクエストを表示し、モニタリングできます。`AdministrativeActions` 配列には、管理アクションタイプごとに最新の更新アクションが 10 件を表示されます。ファイルシステムのスループット容量を変更すると、`FILE_SYSTEM_UPDATE` 管理アクションが生成されます。

次の例は、`describe-file-systems` CLI コマンドのレスポンスの抜粋を示しています。ファイルシステムのスループット容量は 128 MB/秒、ターゲットスループット容量は 256 MB/秒 です。

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Amazon FSx でアクションが正常に処理されると、ステータスは COMPLETED に変更されます。新しいスループット容量がファイルシステムで使用可能になり、ThroughputCapacity プロパティで表示されます。これは、describe-file-systems CLI コマンドの次のレスポンスの抜粋に示されています。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

スループット容量の変更が失敗した場合、ステータスは FAILED に代わり、FailureDetails プロパティは障害に関する情報を提供します。

Amazon FSx メンテナンスウィンドウでのパフォーマンスの最適化

フルマネージドサービスとして、FSx for ONTAP はファイルシステムのメンテナンスと更新を定期的に実行します。このメンテナンスは、ほとんどのワークロードに影響しません。パフォーマンスに敏感なワークロードの場合、まれに、メンテナンスが行われているときにパフォーマンスに短時間 (< 60 秒) の影響があることに気付く場合があります。Amazon FSx を使用すると、メンテナンスウィンドウを使用して、このような潜在的なメンテナンスアクティビティがいつ発生するかをコントロールできます。

パッチ適用はまれで、通常は数週間に 1 回行われます。スケールアップファイルシステムの場合、パッチ適用には通常、メンテナンスウィンドウの開始から 30 分しかかかりません。スケールアウトファイルシステムの場合、パッチ適用には、メンテナンスウィンドウの開始から最長 90 分かかります。この数分間、ファイルシステムは自動的にフェイルオーバー、フェイルバックを行います。ファイルシステムの作成時にメンテナンスウィンドウを選択します。時間設定をしなかった場合は、30 分の開始時間が割り当てられます。

FSx for ONTAP では、ワークロードと運用要件に合わせて、必要に応じてメンテナンスウィンドウを調整できます。メンテナンスウィンドウが少なくとも 14 日に 1 回行われる場合は、メンテナンスウィンドウを必要な頻度で移動できます。パッチがリリースされ、メンテナンスウィンドウが 14 日以内に発生しない場合、FSx for ONTAP はファイルシステムのメンテナンスを続行して、セキュリティと信頼性を確保します。

> **Note**
>
> メンテナンスアクティビティ中のデータの整合性を確保するために、FSx for ONTAP は、メンテナンスを開始する前に、すべての日和見ロックを閉じ、ファイルシステムをホストしている基になるストレージボリュームへの保留中の書き込みオペレーションを完了します。

Amazon FSx マネジメントコンソール、 AWS CLI、 AWS API、またはいずれかの AWS SDKsを使用して、ファイルシステムのメンテナンスウィンドウを変更できます。

毎週のメンテナンスウィンドウを変更するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーション列で [File systems] (ファイルシステム) を選択します。
3. 週次のメンテナンスウィンドウを変更するファイルシステムを選択します。ファイルシステムの詳細ページ [Summary] (概要) が表示されます。

4. [Administration] (管理) を選択して、ファイルシステム管理の [Settings] (設定) パネルを表示します。
5. [Update] (更新) を選択して、[Change maintenance window] (メンテナンスウィンドウの変更) ウィンドウを表示します。
6. 週次のメンテナンスウィンドウを開始する新しい日時を入力します。
7. [Save] (保存) を選択して変更を保存します。新しいメンテナンスのスタート時刻がファイルシステム管理の [Settings] (設定) パネルに表示されます。

CLI コマンドを使用して毎週のメンテナンスウィンドウを変更するには、update-file-system「」を参照してくださいファイルシステムを更新するには (CLI)。

Amazon FSx リソースのタグ付け

ファイルシステムや Amazon FSx リソースを管理しやすくするために、タグ 形式で各リソースに独自のメタデータを割り当てることができます。タグを使用すると、AWS リソースを目的、所有者、環境などさまざまな方法で分類することができます。これは同じ型のリソースが多い場合に役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できます。このトピックでは、タグとその作成方法について説明します。

トピック

- タグの基本
- リソースのタグ付け
- バックアップへのタグのコピー
- タグの制限
- 許可とタグ

タグの基本

タグ とは、AWS リソースに付けるラベルです。各タグは、定義する 2 つの部分で設定されます。

- タグキー (例: `CostCenter`、`Environment`、または `Project`)。タグキーでは、大文字と小文字が区別されます。
- タグ値 (例: `111122223333` または `Production`)。タグキーと同様に、タグ値は大文字と小文字が区別されます。タグ値はオプションです。

タグを使用すると、AWS リソースを目的、所有者、環境などさまざまな方法で分類することができます。例えば、アカウントの各インスタンスの所有者とスタックレベルを追跡しやすくするため、Amazon FSx ファイルシステムに対して一連のタグを定義できます。

リソースタイプごとのニーズを満たす一連のタグキーを考案することをお勧めします。一貫性のあるタグキーセットを使用することで、リソースの管理が容易になります。追加したタグに基づいてリソースを検索およびフィルタリングできます。効果的なリソースのタグ付け戦略を実装する方法の詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付けのベストプラクティス」を参照してください。

留意すべきタグ付けの動作:

- Amazon FSx にとってタグは意味論的な意味はなく、完全に文字列として解釈されます。
- タグは自動的にはリソースに割り当てられません。
- タグのキーと値は編集でき、タグはリソースからいつでも削除できます。
- タグの値を空の文字列に設定することはできますが、タグの値を `null` に設定することはできません。
- 特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。
- リソースを削除すると、リソースのタグも削除されます。
- AWS Command Line Interface(AWS CLI)、または AWS SDK の Amazon FSx API を使用している場合は、以下を実行できます。
  - `TagResource` API アクションを使用して既存のリソースにタグを適用することもできます。
  - リソース作成アクションによっては、リソースの作成時にリソースのタグを指定することもできます。作成時にリソースにタグ付けすることで、リソース作成後にカスタムタグ付けスクリプトを実行する必要がなくなります。

    リソースの作成時にタグを適用できない場合、Amazon FSx はリソースの作成プロセスをロールバックします。この動作により、リソースがタグ付きで作成されるか、まったく作成されないようになるため、タグ付けされていないリソースが存在することがなくなります。

> **Note**
>
> 作成時にユーザーがリソースにタグ付けする際、特定の AWS Identity and Access Management (IAM) アクセスコントロールが必要です。詳細については、「作成中にリソースにタグを付ける許可を付与する」を参照してください。

リソースのタグ付け

アカウントに存在する Amazon FSx リソースにタグ付けできます。Amazon FSx コンソールを使用している場合、関連するリソースの [Tags] (タグ) タブを使用してリソースにタグを適用することができます。リソースを作成するときに、値を指定して [Name] (Name) キーを適用し、新しいファイルシステムを作成するときに、任意のタグを適用できます。ただし、コンソールが [Name] (名前) キーに従ってリソースを整理しても、このキーは Amazon FSx サービスに対して意味論的な意味合いをもちません。

IAM ポリシーでタグベースのリソースレベルアクセス許可を、作成時のタグ付けをサポートする Amazon FSx API アクションに適用し、作成時にリソースにタグ付けできるユーザーとグループを細かくコントロールできます。このような許可をポリシーで使用すると、次のような利点があります。

- リソースは、作成時から適切に保護されます。
- リソースは、作成時から適切に保護されます。タグはリソースに即座に適用されるため、リソースの使用をコントロールするタグベースのリソースレベルアクセス許可がただちに有効になります。
- リソースは、より正確に追跡および報告されます。
- 新しいリソースにタグ付けの使用を適用し、リソースで設定されるタグキーと値をコントロールできます。

さらに、リソースレベルのアクセス許可を IAM ポリシーの `TagResource` および `UntagResource` Amazon FSx API アクションに適用し、既存のリソースで設定されるタグキーと値をコントロールすることもできます。

作成時に Amazon FSx リソースにタグを付けるのに必要なアクセス許可の詳細については、作成中にリソースにタグを付ける許可を付与する を参照してください。

タグを使用して IAM ポリシーでの Amazon FSx リソースへのアクセスを制限する方法の詳細については、タグを使用した Amazon FSx リソースへのアクセスのコントロール を参照してください。

請求用リソースへのタグ付けの詳細については、[AWS Billing User Guide] (ユーザーガイド) の [Using cost allocation tags] (コスト配分タグの使用) を参照してください。

バックアップへのタグのコピー

Amazon FSx API または AWS CLI でボリュームを作成または更新するときに CopyTagsToBackups がボリュームの任意のタグをバックアップに自動的にコピーするように設定することができます。

> **Note**
>
> ユーザーが開始したバックアップ (Amazon FSx コンソールを使用してバックアップを作成するときの名前タグを含む) を作成するときにタグを指定すると、CopyTagsToBackups を使用するように設定した場合でも、タグはボリュームからコピーされません。

バックアップの詳細については、「バックアップの使用」を参照してください。CopyTagsToBackups を使用するように設定する方法の詳細については、「Amazon FSx for NetApp ONTAP ユーザーガイド」の ボリュームを作成するには (CLI) と ボリュームの設定を更新するには (CLI) または「Amazon FSx for NetApp ONTAP API リファレンス」の「Create Volume」(ボリュームの作成) と「Update Volume」(ボリュームの更新) を参照してください。

タグの制限

タグには以下のようなベーシック制限があります。

- リソースあたりのタグの最大数は 50 です。
- キーの最大長は UTF-8 で 128 Unicode 文字です。
- 値の最大長は UTF-8 で 256 Unicode 文字です。
- 使用できる文字は、UTF-8 で表現できる文字、数字、スペース、および次の文字です。+ - (ハイフン) = . _ (下線) : / @。
- タグキーは、リソースごとにそれぞれ一意である必要があります。また、各タグキーに設定できる値は 1 つのみです。
- タグのキーと値は大文字と小文字が区別されます。
- aws: プレフィックスは AWS の使用のために予約されています。タグにこのプレフィックスが付いたタグキーがある場合、タグのキーまたは値を編集、削除することはできません。aws: プレフィックスを持つタグは、リソースあたりのタグ数の制限時には計算されません。

タグのみに基づいてリソースを削除することはできません。リソース識別子を指定する必要があります。例えば、DeleteMe というタグキーでタグ付けしたファイルシステムを削除するには、fs-1234567890abcdef0 などのファイルシステムリソース識別子で DeleteFileSystem アクションを使用する必要があります。

公開リソースまたは共有リソースにタグを付けると、割り当てたタグは、タグ付けを行った AWS アカウント のみが使用できます。他の AWS アカウント はそれらのタグにアクセスできません。共有リソースへのタグベースのアクセスコントロールの場合、各 AWS アカウント は、リソースへのアクセスをコントロールするために独自のタグのセットを割り当てる必要があります。

許可とタグ

作成時に Amazon FSx リソースにタグを付けるのに必要なアクセス許可の詳細については、「作成中にリソースにタグを付ける許可を付与する」を参照してください。

タグを使用して IAM ポリシーで Amazon FSx リソースへのアクセスを制限する方法の詳細については、「タグを使用した Amazon FSx リソースへのアクセスのコントロール」を参照してください。

NetApp アプリケーションを使用した FSx for ONTAP リソースの管理

AWS Management Console、 AWS CLI、 AWS API および SDKs、これらのNetApp管理ツールとアプリケーションを使用して FSx for ONTAP リソースを管理することもできます。

トピック

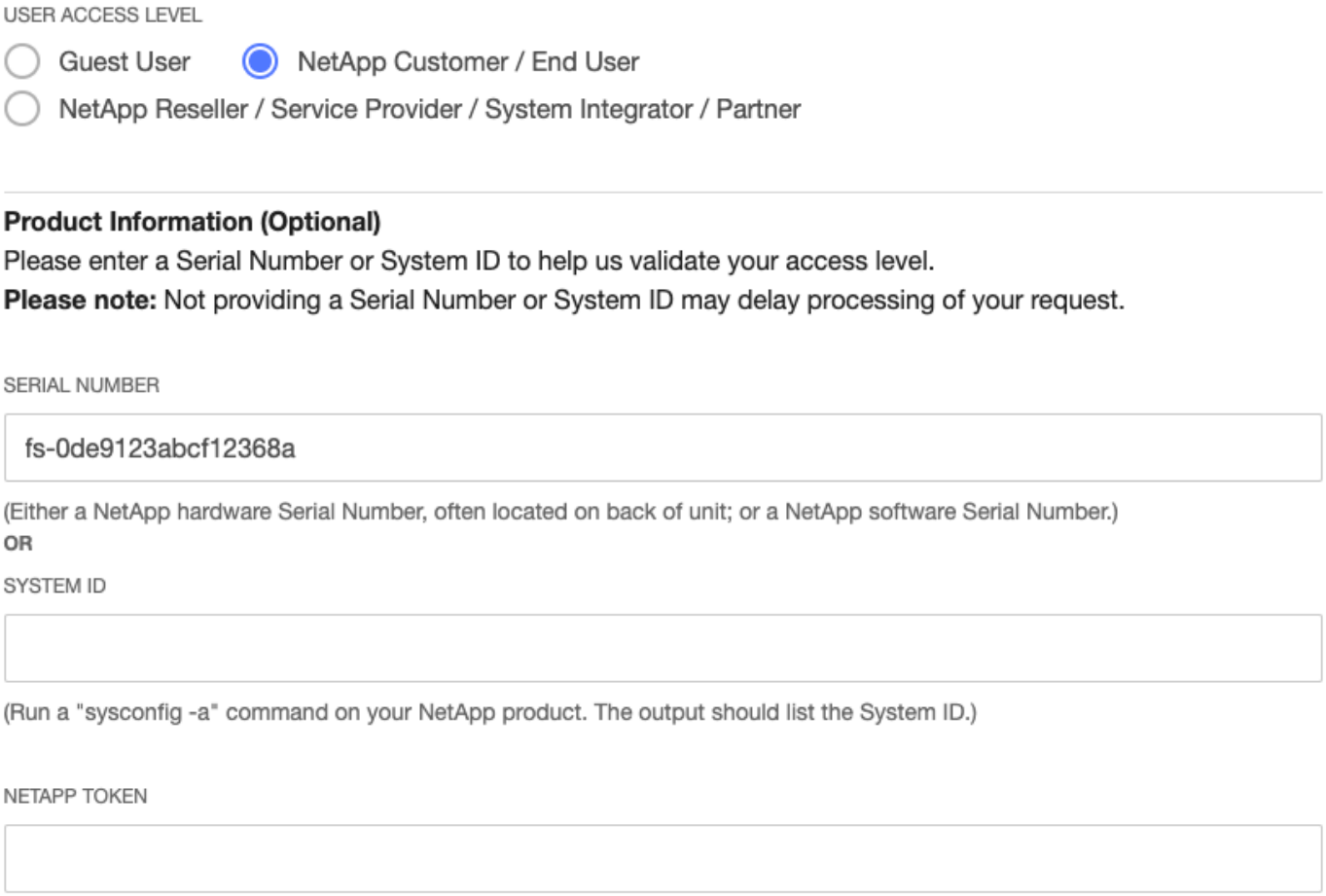
- NetApp アカウントにサインアップする
- NetApp BlueXP を使用する
- NetApp ONTAP CLI の使用
- ONTAP REST API の使用

> **Important**
>
> Amazon FSx は定期的に と同期ONTAPして整合性を確保します。NetApp アプリケーションを使用してボリュームを作成または変更する場合、これらの変更が AWS Management Console、、API AWS CLI、および SDKs に反映されるまでに数分かかることがあります。

NetApp アカウントにサインアップする

、、およびBlueXPSnapCenterONTAPウイルス対策コネクタなどのNetAppソフトウェアをダウンロードするには、 NetAppアカウントが必要です。NetApp アカウントにサインアップするには、次のステップを実行します。

1. NetApp ユーザー登録ページに移動し、新しいNetAppユーザーアカウントに登録します。
2. フォームに必要事項を入力します。必ず、NetApp顧客/エンドユーザーのアクセスレベルを選択してください。[シリアル番号] フィールドに、FSx for ONTAP ファイルシステムのファイルシステム ID をコピーして貼り付けます。次の例を参照してください。



登録後にできること

既存のNetApp製品をご利用のお客様は、1 営業日以内に NSS アカウントがカスタマーレベルアクセスにレベルアップされます。を初めてご利用になるお客様は、NSS アカウントを顧客レベルアクセスにレベルアップするだけでなく、標準的なビジネスプラクティスを使用してオンボーディング

NetAppされます。ファイルシステム ID を指定すると、このプロセスが迅速になります。NSS アカウントのステータスを確認するには、mysupport.netapp.com にログインし、「ようこそ」ページに移動します。アカウントのアクセスレベルはお客様レベルのアクセスである必要があります。

NetApp BlueXP を使用する

NetApp BlueXP は、オンプレミスおよびクラウド環境全体のストレージおよびデータサービスの管理エクスペリエンスを簡素化する統合コントロールプレーンです。BlueXP は、 およびオンプレミスでの ONTAP デプロイを管理、モニタリング AWS 、自動化するための一元化されたユーザーインターフェイスを提供します。詳細については、NetApp BlueXP ドキュメントと NetApp BlueXP for Amazon FSx for NetApp ONTAP ドキュメントを参照してください。

> **Note**
>
> NetApp BlueXP はスケールアウトファイルシステムではサポートされていません。

での NetApp System Manager の使用 BlueXP

Amazon FSx for NetApp ONTAP ファイルシステムは、 から直接 System Manager を使用して管理できますBlueXP。 BlueXPでは、使い慣れたのと同じ System Manager インターフェイスを使用できるため、ハイブリッドマルチクラウドインフラストラクチャを単一のコントロールプレーンから管理できます。また、BlueXP の他の機能にもアクセスできます。詳細については、NetAppONTAP ドキュメントの「System Manager と BlueXP の統合」トピックを参照してください。

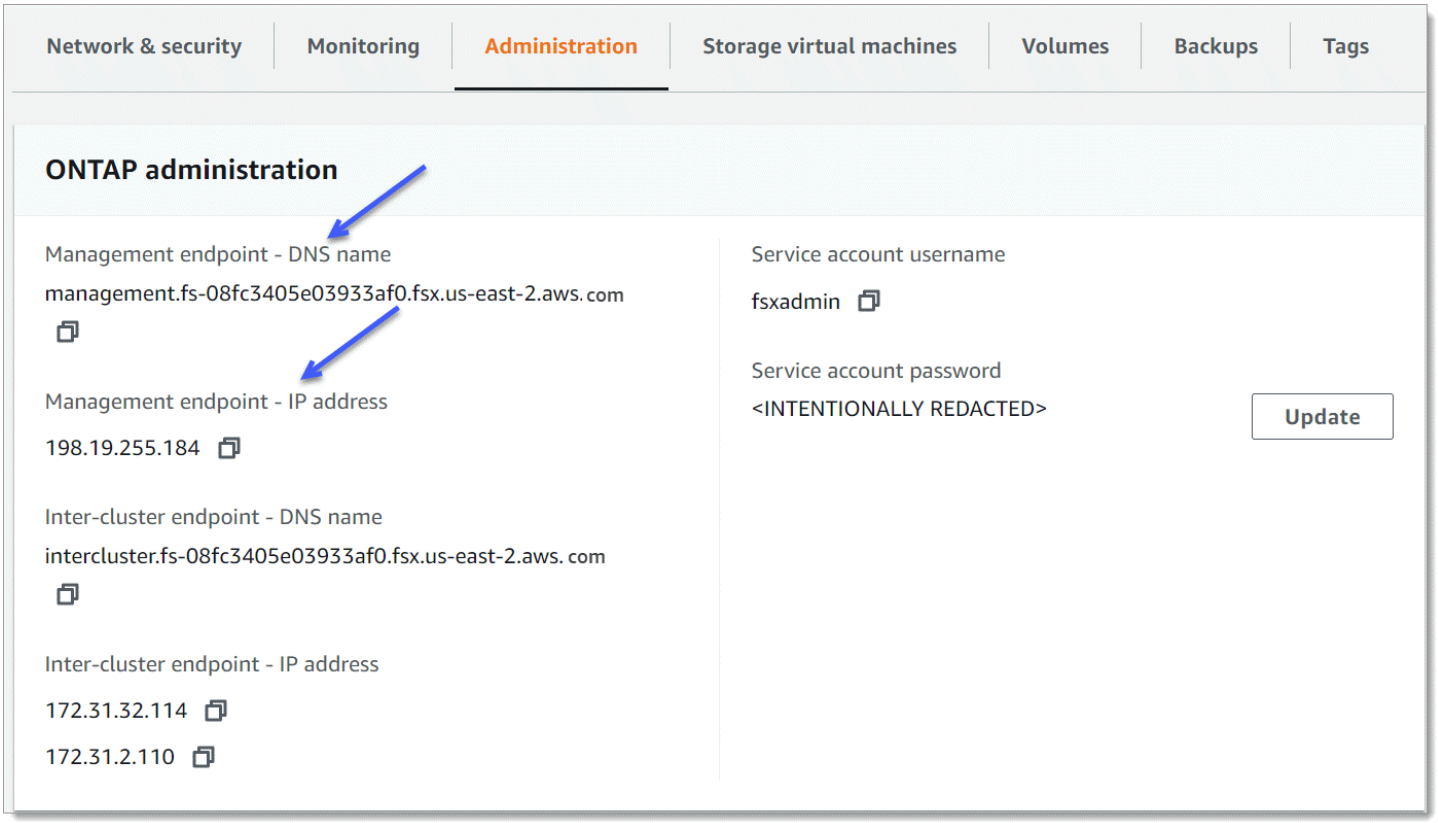
> **Note**
>
> NetApp System Manager はスケールアウトファイルシステムではサポートされていません。

NetApp ONTAP CLI の使用

CLI を使用して Amazon FSx for NetApp ONTAP NetApp ONTAP リソースを管理できます。リソースは、ファイルシステム (NetAppONTAP クラスターに類似) レベルおよび SVM レベルで管理できます。

CLI ONTAP を使用したファイルシステムの管理

FSx for ONTAP ファイルシステムで ONTAP CLI コマンドを実行できます。これは、NetApp ONTAPクラスターで実行する場合に似ています。ファイルシステムの管理エンドポイントへのセキュアシェル (SSH) 接続を確立し、`fsxadmin`ユーザー名とパスワードを使用してログインすることで、ファイルシステムの ONTAPCLI にアクセスします。カスタム作成フローまたは を使用してファイルシステムを作成するときに、パスワードを設定するオプションがあります AWS CLI。クイック作成オプションを使用してファイルシステムを作成した場合、`fsxadmin`パスワードが設定されていないため、ONTAP CLI にログインするためにパスワードを設定します。詳細については、「ファイルシステムの更新」を参照してください。ファイルシステムの管理エンドポイントの DNS 名と IP アドレスは、次の図に示すように、FSx for ONTAP ファイルシステムの詳細ページの管理タブにある Amazon FSx コンソールで確認できます。



SSH を使用してファイルシステムの管理エンドポイントに接続するには、 `fsxadmin` ユーザーとパスワードを使用します。次の例のように、ファイルシステムと同じ VPC にあるクライアントから、ファイルシステムの管理エンドポイント IP アドレスまたは DNS 名に SSH 接続できます。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

SSH コマンドとサンプル値:

```
ssh fsxadmin@198.51.100.0
```

管理エンドポイント DNS 名を使用する SSH コマンド:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

サンプル DNS 名を使用した SSH コマンド

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

で使用できる ONTAP CLI コマンドの範囲 **fsxadmin**

fsxadminの管理ビューはファイルシステムレベルにあり、ファイルシステム内のすべての SVMs とボリュームが含まれます。fsxadmin ロールは、ONTAPクラスター管理者のロールを実行します。Amazon FSx for NetApp ONTAP ファイルシステムはフルマネージド型であるため、fsxadminロールは使用可能な ONTAP CLI コマンドのサブセットを実行できます。

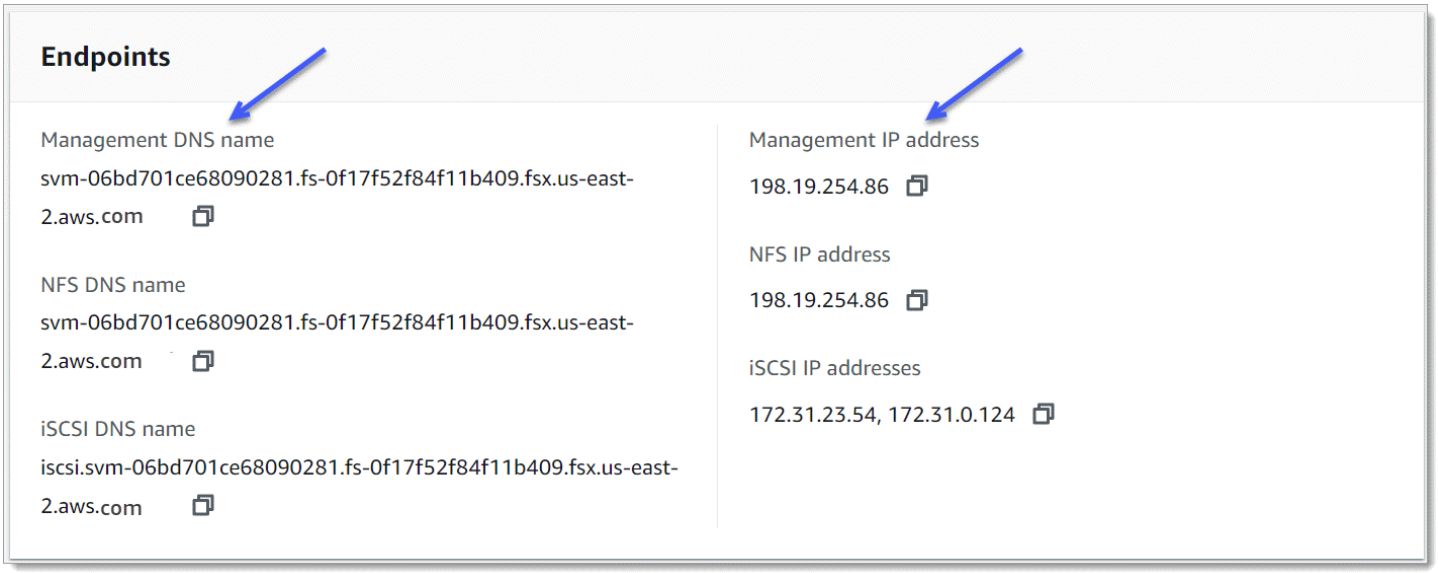
fsxadmin が実行できるコマンドのリストを表示するには、次の security login role show ONTAP CLI コマンドを使用します。

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                          Query    Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding          -port !55555  all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
```

```
                        cluster time-service ntp server create        readonly
                        cluster time-service ntp server delete        readonly
                        cluster time-service ntp server modify        readonly
                        cluster time-service ntp server show          readonly
                        debug network tcpdump       -ipspace !Cluster all
                        debug san lun                                 all
                        df         -vserver !FsxId* -vserver !Cluster readonly
                        echo                                          all
                        event catalog show                            readonly
                        event config                                  all
.
.
.
363 entries were displayed.
```

CLI SVMs ONTAP の管理

fsxadmin またはvsadminユーザー名とパスワードを使用して、SVM の管理エンドポイントへのセキュアシェル (SSH) 接続を確立することで、SVM 上の ONTAPCLI にアクセスできます。SVM の管理エンドポイントの DNS 名と IP アドレスは、次の図に示すように、ストレージ仮想マシンの詳細ページのエンドポイントパネルにある Amazon FSx コンソールにあります。



SSH を使用して SVM の管理エンドポイントに接続するには、 vsadminまたは のfsxadminユーザー名とパスワードを使用できます。SVM の作成時にvsadminユーザーのパスワードを設定しなかった場合は、いつでもvsadminパスワードを設定できます。詳細については、「ストレージ仮想マシンの更新」を参照してください。管理エンドポイントの IP アドレスまたは DNS 名を使用して、ファイルシステムと同じ VPC にあるクライアントから SVM に SSH 接続できます。

```
ssh vsadmin@svm-management-endpoint-ip-address
```

サンプル値を含むコマンド:

```
ssh vsadmin@198.51.100.10
```

管理エンドポイントの DNS 名を使用した SSH コマンド:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

サンプル DNS 名を使用した SSH コマンド

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP は NetApp ONTAP CLI コマンドをサポートしています。

NetApp ONTAP CLI コマンドの完全なリファレンスについては、「ONTAP コマンド: 手動ページリファレンス」を参照してください。

ONTAP REST API の使用

`fsxadmin` 認証情報を使用して REST API を使用して ONTAP FSx for ONTAP ファイルシステムにアクセスする場合は、次のいずれかを実行します。

- TLS 検証を無効にします。

  または

- AWS 認証機関 (CAsを信頼する – 各リージョンの CAs の証明書バンドルは、次の URLsにあります。
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle-*aws-region* .pem for Public AWS リージョン
  - リージョンの https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-aw AWS GovCloud s-region.pem

- AWS 中国リージョン用の https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-aws-region.pem

NetApp ONTAP REST API コマンドの完全なリファレンスについては、NetApp ONTAP「REST API オンラインリファレンス」を参照してください。

Amazon FSx for NetApp ONTAP のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内でのセキュリティと説明しています:

- クラウドのセキュリティ — AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 AWS また、 では、安全に使用できるサービスも提供しています。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。Amazon FSx for NetApp ONTAP に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon FSx 使用時における責任共有モデルの適用法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目標を達成するように Amazon FSx を設定する方法について説明します。また、Amazon FSx リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- Amazon FSx for NetApp ONTAP でのデータ保護
- Amazon FSx for NetApp ONTAP の Identity and Access Management
- AWS Amazon FSx の マネージドポリシー
- Amazon VPC によるファイルシステムアクセスコントロール
- Amazon FSx for NetApp ONTAP のコンプライアンス検証
- Amazon FSx for NetApp ONTAP とインターフェイス VPC エンドポイント (AWS PrivateLink)
- Amazon FSx for NetApp ONTAP の耐障害性
- Amazon FSx for NetApp ONTAP のインフラストラクチャセキュリティ
- FSx for NetApp ONTAP で ONTAP Vscan を使用する

- Amazon FSx for NetApp ONTAP のロールとユーザー

Amazon FSx for NetApp ONTAP でのデータ保護

AWS 責任共有モデル、Amazon FSx for NetApp ONTAP でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、 認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Amazon FSx AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

FSx for ONTAP でのデータ暗号化

Amazon FSx for NetApp ONTAP は、保管中のデータの暗号化と転送中のデータの暗号化をサポートしています。保管中のデータの暗号化は、Amazon FSx ファイルシステムの作成時に自動的に有効になります。Amazon FSx for NetApp ONTAP は、Active Directory または Lightweight Directory Access Protocol (LDAP) を使用してドメインに結合されている Storage Virtual Machine (SVM) 内のデータにアクセスする場合、NFS および SMB プロトコルを介した転送中の Kerberos ベースの暗号化をサポートします。

暗号化を使用するタイミング

ユーザーの組織が、保管中のデータとメタデータの暗号化が必要な企業または規制ポリシーの対象となる場合は、データは保管中に自動的に暗号化されます。また、転送中のデータの暗号化を使用してファイルシステムをマウントすることにより転送中のデータの暗号化を有効にすることも、推奨されています。

Amazon FSx for NetApp ONTAP によるデータ暗号化の詳細については、保管中のデータの暗号化「」および「」を参照してくださいEncrypting data in transit。

保管中のデータの暗号化

すべての Amazon FSx for NetApp ONTAP ファイルシステムは、 () を使用して AWS Key Management Service 管理されるキーで保管時に暗号化されますAWS KMS。データはファイルシステムに書き込まれる前に自動的に暗号化され、読み取り時に自動的に復号化されます。このプロセスは Amazon FSx で透過的に処理されるため、アプリケーションを変更する必要はありません。

Amazon FSx は、業界標準の AES-256 暗号化アルゴリズムを使用して、保存中の Amazon FSx データとメタデータを暗号化します。詳細については、「AWS Key Management Service デベロッパーガイド」の「暗号化のベーシック」を参照してください。

> **Note**
>
> AWS キー管理インフラストラクチャは、連邦情報処理規格 (FIPS) 140-2 で承認された暗号化アルゴリズムを使用します。このインフラストラクチャは、米国標準技術局 (NIST) 800-57 レコメンデーションに一致しています。

Amazon FSx が を使用する方法 AWS KMS

Amazon FSx は、キー管理 AWS KMS のために と統合されます。Amazon FSx は KMS キーを使用してファイルシステムを暗号化します。ファイルシステム (データとメタデータの両方) の暗号化と復号化に使用する KMS キーを選択します。この KMS キーの許可は、有効化、無効化、または削除することができます。この KMS キーは、以下の 2 つのタイプのいずれかになります。

- AWSマネージド KMS キー - これはデフォルトの KMS キーで、自由に使用できます。
- カスタマーマネージド CMK - これは、キーポリシーと許可を複数のユーザーまたはサービスに設定できる、最も柔軟性のある KMS キーです。KMS キーの作成の詳細については、「 AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> Amazon FSx は、KMS の対称暗号化キーのみを受け入れます。Amazon FSx では、非対称 KMS キーを使用することはできません。

顧客が管理する KMS キーをファイルデータ暗号化と復号化の KMS キーとして使用する場合は、キーローテーションを有効にできます。キーローテーションを有効にすると、 AWS KMS は、1 年に 1 回、キーを自動的にローテーションします。また、カスタマーマネージド KMS キーでは、KMS キーへのアクセスの無効化、再有効化、削除、取り消しのタイミングを随時選択できます。詳細については、「AWS Key Management Service デベロッパーガイドの ローテーション AWS KMS keys」および「キーの有効化と無効化」を参照してください。

の Amazon FSx キーポリシー AWS KMS

キーポリシーは、KMS キーへのアクセスをコントロールするための主要な方法です。キーポリシーの詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMSの キーポリシーの使用」を参照してください。次のリストは、Amazon FSx が暗号化された保管時のファイルシステムに対してサポートする AWS KMS関連のすべてのアクセス許可を示しています。

- kms:Encrypt - (オプション) プレーンテキストを暗号化テキストに暗号化します。この許可は、デフォルトのキーポリシーに含まれています。
- kms:Decrypt - (必須) 暗号化テキストを復号します。暗号文は、以前に暗号化されたプレーンテキストです。このアクセス許可は、デフォルトのキーポリシーに含まれています。

- kms:ReEncrypt – (オプション) クライアント側でデータのプレーンテキストを公開することなく AWS KMS key、サーバー側のデータを新しい で暗号化します。データは最初に復号化され、次に再暗号化されます。このアクセス許可は、デフォルトのキーポリシーに含まれています。
- kms:GenerateDataKeyWithoutPlaintext – (必須) KMS キーで暗号化されたデータ暗号化キーを返します。このアクセス許可は、kms:GenerateDataKey* のデフォルトキーポリシーに含まれています。
- kms:CreateGrant – (必須) キーを使用できるユーザーと条件を指定する権限をキーに追加します。付与は、主要なポリシーに対する代替の許可メカニズムです。許可の詳細については、「AWS Key Management Service デベロッパーガイド」の「許可の使用」を参照してください。このアクセス許可は、デフォルトのキーポリシーに含まれています。
- kms:DescribeKey – (必須) 指定された KMS キーに関する詳細情報を提供します。このアクセス許可は、デフォルトのキーポリシーに含まれています。
- kms:ListAliases – (オプション) アカウント内のすべてのキーエイリアスを一覧表示します。コンソールを使用して暗号化されたファイルシステムを作成すると、このアクセス許可が KMS キーのリストに追加されます。最高のユーザーエクスペリエンスを提供するためには、この許可の使用をお勧めします。このアクセス許可は、デフォルトのキーポリシーに含まれています。

Encrypting data in transit

このトピックでは、FSx for ONTAP ファイルシステムと接続されたクライアント間で転送されるファイルデータを暗号化するために使用できるさまざまなオプションについて説明します。また、ワークフローに最適な暗号化方法を選択するためのガイダンスも提供します。

AWS グローバルネットワーク AWS リージョン を経由するすべてのデータは、 AWS 安全な施設を離れる前に、物理レイヤーで自動的に暗号化されます。アベイラビリティーゾーン間のトラフィックは、すべて暗号化されます。追加的な暗号化レイヤーでは、このセクションに記載されているもの以外にも、保護が提供されています。 AWS が AWS リージョン、アベイラビリティーゾーン、インスタンスをまたいで流れるデータを保護する方法の詳細については、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの「転送中の暗号化」を参照してください。

Amazon FSx for NetApp ONTAP は、FSx for ONTAP ファイルシステムと接続されたクライアント間で転送中のデータを暗号化するために、次の方法をサポートしています。

- サポートされているすべてのプロトコルと、サポートされている Amazon EC2 Linux および Windows インスタンスタイプで実行されているクライアントに対して、Nitro ベースの自動暗号化を行います。
- NFS および SMB プロトコル上での Kerberos ベースの暗号化。

- NFS、iSCSI、SMB プロトコル上での IPsec ベースの暗号化

転送中のデータを暗号化するための、サポートされている方法はすべて、エンタープライズレベルの強固な暗号化を実現する業界標準、AES-256 暗号化アルゴリズムを使用しています。

トピック

転送中のデータを暗号化する方法を選ぶ

このセクションでは、サポートされている転送時の暗号化方法のどれがワークフローに最適であるかを判断する際に役立つ情報を紹介します。この後のセクションで、サポートされているオプションについて詳しく説明する際に、このセクションを再度参照します。

FSx for ONTAP ファイルシステムと接続されたクライアントとの間で転送中のデータを暗号化する方法を選ぶ際、考慮すべき要素がいくつかあります。以下のような要素です。

- AWS リージョン FSx for ONTAP ファイルシステムが実行されている 。
- クライアントが実行中のインスタンスタイプ。
- ファイルシステムにアクセスしているクライアントの場所。
- ネットワークパフォーマンスの要件。
- 暗号化しようとしているデータプロトコル。
- Microsoft Active Directory を使用している場合。

AWS リージョン

ファイルシステムが実行中の によって、Amazon Nitro ベースの暗号化を使用できるかどうか AWS リージョン が決まります。Nitro ベースの暗号化は、次の AWS リージョン で利用できます。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- 欧州 (アイルランド)

さらに、Nitro ベースの暗号化は、アジアパシフィック (シドニー) のスケールアウトファイルシステムで使用できます AWS リージョン。

クライアントのインスタンスタイプ

ファイルシステムにアクセスしているクライアントが、サポートされている Amazon EC2 Mac、Linux、Windows インスタンスタイプのいずれかで実行されており、ワークフローが Nitro ベースの暗号化を使用するためのその他すべての要件を満たしている場合、Amazon Nitro ベースの暗号化を使用できます。Kerberos または IPsec 暗号化を使用するための、クライアントインスタンスタイプの要件はありません。

クライアントロケーション

ファイルシステムの場所に対してデータにアクセスしているクライアントの場所は、使用できる転送中の暗号化の方法に影響します。クライアントとファイルシステムが同じ VPC にある場合は、サポートされている暗号化方法をどれでも使用できます。クライアントとファイルシステムが、ピア接続された VPC 内にある場合も、トラフィックが仮想ネットワークのデバイスまたはサービス (Transit Gateway など) を通過しない限り、同様です。Nitro ベースの暗号化は、クライアントが同じ VPC かピア接続された VPC にない場合、またはトラフィックが仮想ネットワークのデバイスまたはサービスを通過しない場合は、使用できません。

ネットワークパフォーマンス

Amazon Nitro ベースの暗号化を使用しても、ネットワークのパフォーマンスには影響しません。これは、サポートされている Amazon EC2 インスタンスが、基盤となる Nitro System ハードウェアのオフロード機能を使って、インスタンス間の転送中のトラフィックを自動的に暗号化するためです。

Kerberos または IPsec 暗号化を使用すると、ネットワークのパフォーマンスに影響します。これは、これらの暗号化の方法がともにソフトウェアベースであり、クライアントとサーバーが転送中のトラフィックを暗号化および復号化するためにはコンピューティングリソースを使う必要があるためです。

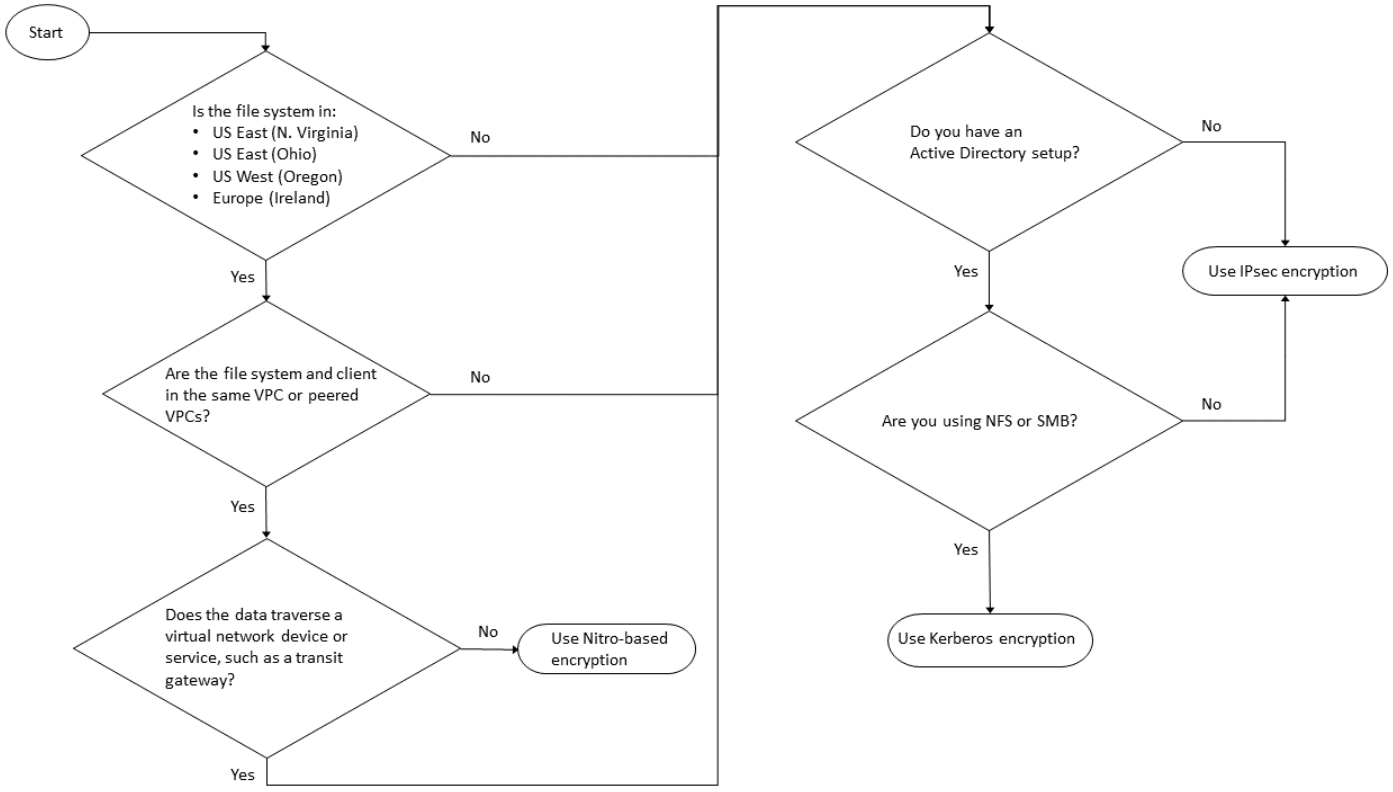
データプロトコル

Amazon Nitro ベースの暗号化と IPsec 暗号化は、サポートされているすべてのプロトコル (NFS、SMB、iSCSI) で使用することができます。Kerberos 暗号化は、NFS プロトコルと SMB プロトコル (Active Directory を使用) で使用できます。

アクティブディレクトリ

Microsoft Active Directory を使用している場合、NFS プロトコルと SMB プロトコルで Kerberos 暗号化を使用できます。

次の図は、どの転送中の暗号化方法を使用すればよいかを判断するのに役立ちます。



IPsec 暗号化は、以下のすべての条件がワークフローに当てはまる場合に使用できる、唯一の選択肢です。

- NFS、SMB、iSCSI のいずれかのプロトコルを使用している。
- ワークフローは Amazon Nitro ベースの暗号化の使用をサポートしていない。
- Microsoft アクティブディレクトリドメインを使用していない。

AWS Nitro System による転送中のデータの暗号化

Nitro ベースの暗号化を使用すると、転送中のデータは、ファイルシステムにアクセスするクライアントが、サポートされている Amazon EC2 Linux か Windows インスタンスタイプで実行されているとき、自動的に暗号化されます。

Amazon Nitro ベースの暗号化を使用しても、ネットワークのパフォーマンスには影響しません。これは、サポートされている Amazon EC2 インスタンスが、基盤となる Nitro System ハードウェアのオフロード機能を使って、インスタンス間の転送中のトラフィックを自動的に暗号化するためです。

Nitro ベースの暗号化は、サポートされているクライアントインスタンスタイプが、同じ AWS リージョン にあるか、ファイルシステムの VPC とピア接続されている同じ VPC にあるときに、自動的に有効になります。さらに、クライアントが、ピア接続された VPC 内にある場合、Nitro ベースの暗号化を自動的に有効にするために、データは、仮想ネットワークのデバイスまたはサービス (Transit Gateway など) を通過することができません。Nitro ベースの暗号化に関する詳細は、Amazon EC2 の Linux または Windows インスタンス用ユーザーガイドの「転送中の暗号化」を参照してください。

Nitro ベースの転送時の暗号化は、2022 年 11 月 28 日以降に作成されたファイルシステムで次の で使用できます AWS リージョン。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- 欧州 (アイルランド)

さらに、Nitro ベースの暗号化は、アジアパシフィック (シドニー) のスケールアウトファイルシステムで使用できます AWS リージョン。

FSx for ONTAP が利用可能な AWS リージョン の詳細については、「Amazon FSx for NetApp ONTAP の料金」を参照してください。

FSx for ONTAP ファイルシステムのパフォーマンスの仕様の詳細については、スループット容量がパフォーマンスに与える影響 を参照してください。

Kerberos ベースの暗号化を使用した転送中のデータの暗号化

Microsoft Active Directory を使用している場合は、NFS および SMB プロトコルで Kerberos ベースの暗号化を使用して、Microsoft Active Directory に参加している SVMs の子ボリュームの転送中のデータを暗号化できます。

Kerberos を使用して NFS 経由で転送中のデータを暗号化する

Kerberos を使用した転送中のデータの暗号化は、NFSv3 プロトコルと NFSv4 プロトコルでサポートされています。NFS プロトコルに Kerberos を使用して、転送中の暗号化を有効にする方法については、NetApp ONTAP ドキュメンテーションセンターの「Using Kerberos with NFS for strong security」を参照してください。

Kerberos を使用して SMB 経由で転送中のデータを暗号化する

SMB プロトコル経由の、転送中のデータの暗号化は、SMB プロトコル 3.0 以降をサポートしているコンピューティングインスタンスにマップされた、ファイル共有でサポートされています。これには、Microsoft Windows Server 2012 以降および Microsoft Windows 8 以降のすべてのMicrosoft Windowsバージョンが含まれます。有効にすると、ユーザーがアプリケーションを変更することなく、FSx for ONTAP はファイルシステムにアクセスする際にSMB 暗号化を使用して転送中のデータを自動的に暗号化します。

FSx for ONTAP SMB は 128 ビットと 256 ビットの暗号化をサポートしています。いずれになるかは、クライアントセッションのリクエストによって決まります。さまざまな暗号化レベルの詳細については、NetApp ONTAP ドキュメントセンターの「Manage SMB with the CLI」にある「Set the SMB server minimum authentication security level」のセクションを参照してください。

> **Note**
>
> 暗号化アルゴリズムはクライアントによって決まります。NTLM と Kerberos 認証は、どちらも 128 ビットと 256 ビットの両方の暗号化で動作します。FSx for ONTAP SMB Server は、すべてのスタンダード Windows クライアントリクエストを受け入れ、きめ細かいコントロールは Microsoft グループポリシーまたはレジストリ設定によって処理されます。

ONTAP CLI を使用して、ONTAP SVM およびボリュームの FSx の転送中の暗号化設定を管理します。NetApp ONTAP CLI にアクセスするには、CLI SVMs ONTAP の管理 の説明に従って、転送中の暗号化設定を行う SVM で SSH セッションを確立します。

SVM またはボリュームで SMB 暗号化を有効にする方法については、「」を参照してください転送中のデータの SMB 暗号化を有効にする。

IPsec 暗号化を使用した転送中のデータの暗号化

FSx for ONTAP は転送モード中の IPsec プロトコルの使用をサポートしているため、転送中でもデータを継続的に保護し暗号化することができます。IPsec は、NFS、iSCSI、SMB プロトコルなど、サポートされているすべての IP トラフィックについて、クライアントと FSx for ONTAP ファイルシステム間で転送中のデータを end-to-end 暗号化します。IPsec 暗号化を使用すると、IPsec が有効に設定された FSx for ONTAP SVM と、データにアクセスする接続クライアントで実行中の IPsec クライアントとの間に、IPsec トンネルが確立されます。

Nitro ベースの暗号化をサポートしていないクライアントからデータにアクセスするときや、クライアントと SVM が Active Directory (Kerberos ベースの暗号化に必要) に接続されていない場合は、IPsec を使用して NFS、SMB、iSCSI プロトコル経由で転送中のデータを暗号化することが推奨されます。iSCSI クライアントが Nitro ベースの暗号化をサポートしていない場合、iSCSI トラフィックで転送中のデータを暗号化するには、IPsec 暗号化しか使用できません。

IPsec 認証には、事前共有キー (PSK) または証明書のいずれかを使用できます。PSK を使用している場合、使用する IPsec クライアントは PSK で Internet Key Exchange バージョン 2 (IKEv2) をサポートしている必要があります。FSx for ONTAP とクライアントの両方で IPsec 暗号化を設定する手順の概要は次のとおりです。

1. ファイルシステムで IPsec を有効にし、設定します。
2. クライアントに IPsec をインストールし、設定します。
3. 複数のクライアントアクセス用に IPsec を設定します。

PSK を使用して IPsec を設定する方法の詳細については、 NetApp ONTAPドキュメントセンターの「Configure IP security (IPsec) over wire encryption」を参照してください。

証明書を使用して IPsec を設定する方法の詳細については、「」を参照してください証明書の認証を使用した IPsec の設定。

転送中のデータの SMB 暗号化を有効にする

デフォルトでは、SVM を作成すると SMB 暗号化はオフになります。個々の共有で必要な SMB 暗号化を有効にするか、SVM 上のすべての共有に対して有効にする SVM 上で有効にできます。

> **Note**
>
> SVM または共有で SMB 暗号化リクエストが有効になっている場合、暗号化をサポートしない SMB クライアントはその SVM または共有に接続できなくなります。

SVM の着信 SMB トラフィックに SMB 暗号化をリクエストするには

NetApp ONTAP CLI を使用して SVM で SMB 暗号化をリクエストするには、次の手順を実行します。

1. SVM の管理エンドポイントに SSH で接続するには、SVM の作成時に設定した vsadmin ユーザーネームと vsadmin パスワードを使用します。vsadmin パスワードを設定していない場合は、ユーザーネーム fsxadmin と fsxadmin のパスワードを使用します。管理エンドポイントの IP アドレスまたは DNS 名を使用して、ファイルシステムと同じ VPC にあるクライアントから SVM に SSH 接続できます。

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   サンプル値を含むコマンド:

   ```
   ssh vsadmin@198.51.100.10
   ```

   管理エンドポイントの DNS 名を使用した SSH コマンド:

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   サンプル DNS 名を使用した SSH コマンド

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
   east-2.aws.com
   ```

   ```
   Password: vsadmin-password

   This is your first recorded login.
   FsxIdabcdef01234567892::>
   ```

2. vserver cifs security modify NetApp ONTAP CLI コマンドを使用して、SVM への受信 SMB トラフィックに SMB 暗号化を要求します。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. 着信 SMB トラフィックに対する SMB 暗号化のリクエストを停止するには、次のコマンドを使用します。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. SVM の現在のis-smb-encryption-required設定を確認するには、vserver cifs security show NetApp ONTAP CLI コマンドを使用します。

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

SVM での SMB 暗号化の管理の詳細については、NetApp ONTAP ドキュメントセンターの「Configuring required SMB encryption on SMB servers for data transfers over SMB」を参照してください。

ボリュームで SMB 暗号化を有効にするには

NetApp ONTAP CLI を使用して共有で SMB 暗号化を有効にするには、次の手順を使用します。

1. CLI SVMs ONTAP の管理 の説明に従って、SVM の管理エンドポイントにセキュアシェル (SSH) 接続を確立します。
2. 新しい SMB 共有を作成し、この共有にアクセスするときに SMB 暗号化をリクエストするには、次の NetApp ONTAP CLI コマンドを使用します。

```
vserver cifs share create -vserver vserver_name -share-name share_name -
path share_path -share-properties encrypt-data
```

詳細については、NetApp ONTAP CLI コマンドのマニュアルページの「vserver cifs share create」を参照してください。

3. 既存の SMB 共有で SMB 暗号化をリクエストするには、次のコマンドを使用します。

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

詳細については、NetApp ONTAP CLI コマンドのマニュアルページの「vserver cifs share create」を参照してください。

4. 既存の SMB 共有で SMB 暗号化を無効にするには、次のコマンドを使用します。

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

詳細については、NetApp ONTAP CLI コマンドのマニュアルページの「vserver cifs share properties remove」を参照してください。

5. SMB 共有の現在の `is-smb-encryption-required` 設定を確認するには、次の NetApp ONTAP CLI コマンドを使用します。

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

このコマンドによって返されたプロパティの 1 つが `encrypt-data` プロパティの場合、この共有にアクセスするときに SMB 暗号化を使用する必要があることがそのプロパティによって指定されます。

詳細については、NetApp ONTAP CLI コマンドのマニュアルページの「vserver cifs share properties show」を参照してください。

PSK 認証を使用した IPsec の設定

認証に PSK を使用する場合、FSx for ONTAP とクライアントの両方で IPsec 暗号化を設定する手順は、次のとおりです。

1. ファイルシステムで IPsec を有効にし、設定します。
2. クライアントに IPsec をインストールし、設定します。
3. 複数のクライアントアクセス用に IPsec を設定します。

PSK を使用して IPsec を設定する方法の詳細については、NetApp ONTAP ドキュメンテーションセンターの「Configure IP security (IPsec) over wire encryption」を参照してください。

証明書の認証を使用した IPsec の設定

以下のトピックでは、FSx for ONTAP ファイルシステムおよび Libreswan IPsec を実行するクライアントで証明書認証を使用して IPsec 暗号化を設定する手順について説明します。このソリューションでは、 AWS Certificate Manager と AWS Private Certificate Authority を使用してプライベート認証機関を作成し、証明書を生成します。

FSx for ONTAP ファイルシステムおよび接続されたクライアントで証明書認証を使用して IPsec 暗号化を設定するための大まかな手順は次のとおりです。

1. 証明書を発行するための認証機関を用意します。
2. ファイルシステムとクライアントの CA 証明書を生成してエクスポートします。
3. クライアントインスタンスに証明書をインストールし、IPsec を設定します。
4. 証明書をインストールし、ファイルシステムに IPsec を設定します。
5. セキュリティポリシーデータベース (SPD) を定義します。
6. 複数のクライアントアクセス用に IPsec を設定します。

CA 証明書の作成とインストール

証明書の認証を行うには、認証機関の証明書を生成して、FSx for ONTAP ファイルシステムと、ファイルシステムのデータにアクセスするクライアントに、インストールする必要があります。次の例では AWS Private Certificate Authority 、 を使用してプライベート認証機関を設定し、ファイルシステムとクライアントにインストールする証明書を生成します。を使用すると AWS Private Certificate Authority、組織による内部使用のために、ルート認証機関と下位認証機関 (CAsの完全に AWS ホストされた階層を作成できます。このプロセスは、次の 5 つのステップから成ります。

1. を使用してプライベート認証機関 (CA) を作成する AWS Private CA
2. ルート証明書を発行してプライベート CA にインストールします。
3. ファイルシステムとクライアント AWS Certificate Manager 用に からプライベート証明書をリクエストする
4. ファイルシステムとクライアントの証明書をエクスポートします。

詳細については、「 ユーザーガイド」の「プライベート CA の管理 AWS Private Certificate Authority 」を参照してください。

ルートプライベート CA を作成するには

1. CA を作成するときは、指定したファイルで CA 設定を指定する必要があります。次のコマンドは、テキストエディタの nano を使用して ca_config.txt ファイルを作成します。このファイルでは以下の情報が指定されています。

   - アルゴリズムの名前
   - CA が署名に使用する署名アルゴリズム
   - X.500 件名情報

   ```
   $ > nano ca_config.txt
   ```

   テキストエディタが表示されます。

2. CA の仕様に合わせてファイルを編集します。

   ```
   {
      "KeyAlgorithm":"RSA_2048",
      "SigningAlgorithm":"SHA256WITHRSA",
      "Subject":{
         "Country":"US",
         "Organization":"Example Corp",
         "OrganizationalUnit":"Sales",
         "State":"WA",
         "Locality":"Seattle",
         "CommonName":"*.ec2.internal"
      }
   }
   ```

3. ファイルを保存て閉じ、テキストエディタを終了します。詳細については、「 ユーザーガイド」の「CA の作成手順 AWS Private Certificate Authority 」を参照してください。

4. create-certificate-authority AWS Private CA CLI コマンドを使用して、プライベート CA を作成します。

   ```
   ~/home > aws acm-pca create-certificate-authority \
        --certificate-authority-configuration file://ca_config.txt \
        --certificate-authority-type "ROOT" \
        --idempotency-token 01234567 --region aws-region
   ```

作成されると、このコマンドは CA の Amazon リソースネーム (ARN)　を出力します。

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

プライベートルート CA の証明書を作成してインストールするには (AWS CLI)

1. AWS CLI コマンドを使用して証明書署名リクエスト (CSR) get-certificate-authority-csr を生成します。

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

生成されたファイル ca.csr は base64 形式でエンコードされた PEM ファイルで、次のような外見をしています。

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

詳細については、「 ユーザーガイド」の「ルート CA 証明書のインストール」を参照してください。 AWS Private Certificate Authority

2. issue-certificate AWS CLI コマンドを使用して、ルート証明書を発行し、プライベート CA にインストールします。

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. get-certificate AWS CLI コマンドを使用してルート証明書をダウンロードします。

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. import-certificate-authority-certificate AWS CLI コマンドを使用して、プライベート CA にルート証明書をインストールします。

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

ファイルシステムとクライアント証明書を生成し、エクスポートします。

1. request-certificate AWS CLI コマンドを使用して、ファイルシステムとクライアントで使用する AWS Certificate Manager 証明書をリクエストします。

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
```

```
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

リクエストが成功すると、発行された証明書の ARN が返されます。

2. セキュリティ上の理由から、プライベートキーをエクスポートするときはパスフレーズを割り当てる必要があります。パスフレーズを作成し、passphrase.txt という名前のファイルに保存します。
3. export-certificate AWS CLI コマンドを使用して、以前に発行されたプライベート証明書をエクスポートします。エクスポートしたファイルには、証明書、証明書チェーン、証明書に埋め込まれているパブリックキーに関連付けられた、暗号化されたプライベート 2048 ビット RSA キー、が含まれています。セキュリティ上の理由から、プライベートキーをエクスポートするときはパスフレーズを割り当てる必要があります。以下は、Linux EC2 インスタンスの場合の例です。

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. 次の jq コマンドを使用して、JSON レスポンスからプライベートキーと証明書を抽出します。

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. 次の openssl コマンドを使用して、JSON レスポンスからプライベートキーを復号します。コマンドを入力すると、パスフレーズの入力を求められます。

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Libreswan IPsec を Amazon Linux 2 クライアントにインストールし、設定する

以下のセクションでは、Amazon Linux 2 を実行している Amazon EC2 インスタンスに Libreswan IPsec をインストールし、設定する方法について説明します。

Libreswan をインストールして設定するには

1. SSH を使用して EC2 インスタンスに接続します。具体的な手順については、Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイドの「SSH クライアントを使用して Linux インスタンスに接続する」を参照してください。
2. 次のコマンドを実行して `libreswan` をインストールします。

```
$ sudo yum install libreswan
```

3. (オプション) 後のステップで IPsec を検証する際、これらの設定を行っていないのにプロパティにフラグが付いていることがあります。これらの設定を行わずに、先にセットアップをテストしてみることをお勧めします。接続に問題があれば、このステップに戻って次の変更を施します。

   インストールが完了したら、任意のテキストエディタを使って次のエントリを `/etc/sysctl.conf` ファイルに追加します。

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

   変更を保存して、テキストエディタを終了します。
4. 変更を適用します。

```
$ sudo sysctl -p
```

5. IPsec の設定を確認します。

```
$ sudo ipsec verify
```

   インストールした `Libreswan` のバージョンが実行していることを確認します。
6. IPsec NSS データベースを初期化します。

```
$ sudo ipsec checknss
```

証明書をクライアントにインストールするには

1. クライアント用に生成した証明書を EC2 インスタンスの作業ディレクトリにコピーします。お客様
2. 前に生成した証明書を libreswan と互換性のある形式にエクスポートします。

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. 再フォーマットしたキーをインポートし、プロンプトが表示されたらパスフレーズを指定します。

```
$ sudo ipsec import certkey.p12
```

4. 任意のテキストエディタを使用して IPsec 設定ファイルを作成します。

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

以下のエントリを設定ファイルに追加します。

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

ファイルシステムで IPsec を設定したら、クライアントで IPsec を起動します。

ファイルシステムで IPsec を設定する

このセクションでは、FSx for ONTAP ファイルシステムに証明書をインストールし、IPsec を設定する方法について説明します。

証明書をファイルシステムにインストールするには

1. ルート証明書 (`rootCA.pem`)、クライアント証明書 (`cert.pem`)、復号されたキー (`decrypted.key`) の各ファイルをファイルシステムにコピーします。証明書のパスフレーズを書き留めておく必要があります。
2. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。
3. 各ファイルの出力をコピーし、次のステップで画面に指示が出たときに貼り付けられるよう、(ファイルシステムではなく) クライアントで cat を使用して `rootCA.pem`、`cert.pem`、`decrypted.key` ファイルの内容を一覧表示します。

   ```
   $ > cat cert.pem
   ```

   証明書の内容をコピーします。
4. すでにインストールされている場合 (ONTAP 自己署名ルート CA のケースなど) を除き、相互認証時に使用されるすべての CA 証明書を、ONTAP 側およびクライアント側両方の CA を含め、ONTAP 証明書管理にインストールする必要があります。

   `security certificate install` NetApp CLI コマンドを次のように使用して、クライアント証明書をインストールします。

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

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

前にコピーした cert.pem ファイルの内容を貼り付け、Enter キーを押します。

```
Please enter Private Key: Press <Enter> when done
```

前にコピーした decrypted.key ファイルの内容を貼り付け、Enter キーを押します。

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

n を入力し、クライアント証明書の入力を完了します。

5. SVM で使用する証明書を作成し、インストールします。この証明書の発行者 CA は、既に ONTAP にインストールされ、 IPsec に追加されている必要があります。

   以下のコマンドを使用して、ルート証明書をインストールします。

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

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

   前にコピーした rootCA.pem ファイルの内容を貼り付け、Enter キーを押します。

6. インストールされている CA が、認証中に IPsec CA 検索パス内に存在していることを確かめるには、security ipsec ca-certificate add コマンドを使って ONTAP 証明書管理 CA を IPsec モジュールに追加します。

   以下のコマンドを入力し、ルート証明書を追加します。

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. 次のコマンドを入力し、必要な IPsec ポリシーをセキュリティポリシーデータベース (SPD) に作成します。

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
```

```
ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
"CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. 次のコマンドを使用してファイルシステムの IPsec ポリシーを表示し、確認します。

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
        IKE Security Association Lifetime: 86400
      IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                        Is Policy Enabled: true
                           Local Identity: CN=*.ec2.internal
                          Remote Identity: CN=*.ec2.internal
                   Authentication Method: PKI
          Certificate for Local Identity: ipsec-client-cert
```

クライアントで IPsec を起動する

IPsec を FSx for ONTAP ファイルシステムとクライアントの両方で設定したので、これで IPsec をクライアントで起動できます。

1. SSH を使用してクライアントシステムに接続します。
2. IPsec を起動します。

```
$ sudo ipsec start
```

3. IPsec のステータスをチェックします。

```
$ sudo ipsec status
```

4. ファイルシステムにボリュームをマウントします。

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. FSx for ONTAP ファイルシステムの暗号化された接続を表示し、IPsec の設定を確認します。

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

複数のクライアントに IPsec を設定する

IPsec を使用する必要のあるクライアントが少数である場合は、各クライアントに 1 つの SPD エントリを使用すれば十分です。しかし、数百あるいは数千のクライアントで IPsec を使用する必要がある場合は、IPsec の複数クライアント構成を使用することが推奨されます。

FSx for ONTAPは、複数のネットワーク上にある複数のクライアントを IPsec が有効である 1 つの SVM IP アドレスに接続することを、サポートしています。これは、subnet 構成または Allow all clients 構成のいずれかを使用することで達成できます。その方法については、以下の手順で説明します。

サブネット構成を使用して複数のクライアント用に IPsec を構成するには

特定のサブネット (192.168.134.0/24 など) 上にあるすべてのクライアントを、1 つの SPD ポリシーエントリを使って、1 つの SVM IP アドレスに接続するには、サブネット形式で remote-ip-subnets を指定する必要があります。さらに、正しいクライアント側 ID を使って remote-identity を指定する必要があります。

> **Important**
>
> 証明書の認証を使用すると、各クライアントは、独自の証明書か共有証明書を使用して、認証を行うことができます。FSx for ONTAP IPsec は、ローカルのトラストストアにインス

トールされている CA に基づいて、証明書の有効性をチェックします。FSx for ONTAP は、証明書失効リスト (CRL) のチェックもサポートしています。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. `security ipsec policy create`NetApp ONTAP CLI コマンドを以下のように使用して、*sample* の値を特定の値に置き換えます。

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -remote-identity client_side_identity
   ```

Allow all clients 構成を使用して複数のクライアント用に IPsec を構成するには

ソース IP アドレスに関係なくすべてのクライアントに SVM IPsec 対応 IP アドレスへの接続を許可するには、`remote-ip-subnets` フィールドを指定するときに `0.0.0.0/0` ワイルドカードを使用します。

さらに、正しいクライアント側 ID を使って `remote-identity` を指定する必要があります。証明書の認証には、`ANYTHING` と入力します。

また、0.0.0.0/0 のワイルドカードを使用する場合は、使用する特定のローカルまたはリモートのポート番号を設定する必要があります。例えば、NFS ポート 2049 です。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. `security ipsec policy create`NetApp ONTAP CLI コマンドを以下のように使用して、*`sample`* の値を特定の値に置き換えます。

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -local-ports 2049 -remote-identity client_side_identity
```

Amazon FSx for NetApp ONTAP の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、Amazon FSx リソースを使用するための認証 (サインイン) および認可(許可を持つ) できるユーザーをコントロールします。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon FSx for NetApp ONTAP と IAM の連携方法
- Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例
- Amazon FSx for NetApp ONTAP のアイデンティティとアクセスのトラブルシューティング
- Amazon FSx でのタグの使用
- Amazon FSx のサービスリンクロールの使用

対象者

AWS Identity and Access Management (IAM) の使用方法は、Amazon FSx で行う作業によって異なります。

サービスユーザー - ジョブを実行するために Amazon FSx サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。さらに多くの Amazon FSx 機能を使用して作業を行うには、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切な許可をリクエストするために役に立ちます。Amazon FSx の機能にアクセスできない場合は、「Amazon FSx for NetApp ONTAP のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Amazon FSx リソースを担当している場合は、通常、Amazon FSx へのフルアクセスがあります。サービスユーザーがどの Amazon FSx 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を確認し、IAM の基本概念を理解してください。社内で Amazon FSx と IAM を併用する方法の詳細については、「Amazon FSx for NetApp ONTAP と IAM の連携方法」を参照してください。

IAM 管理者 - 管理者は、Amazon FSx へのアクセス権を管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Amazon FSx アイデンティティベースのポリシーの例を表示するには、Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例 を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『IAM ユーザーガイド』の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールが引き受けられ、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することも

できます。IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限

が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行する

ロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Amazon FSx for NetApp ONTAP と IAM の連携方法

IAM を使用して Amazon FSx へのアクセスを管理する前に、Amazon FSx で使用できる IAM 機能について理解しておく必要があります。

Amazon FSx for NetApp ONTAP で使用できる IAM の機能

IAM 機能	Amazon FSx のサポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
ポリシーリソース	Yes
ポリシー条件キー	Yes
ACL	No
ABAC (ポリシー内のタグ)	はい
一時的な認証情報	はい
転送アクセスセッション (FAS)	はい
サービスロール	いいえ
サービスリンクロール	はい

Amazon FSx およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

Amazon FSx のアイデンティティベースの ポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Amazon FSx のアイデンティティベースのポリシー例

Amazon FSx のアイデンティティベースポリシーの例を確認するには、「Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例」を参照してください。

Amazon FSx 内のリソースベースのポリシー

リソースベースのポリシーのサポート	いいえ

Amazon FSx のポリシーアクション

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

ポリシーにアクションを含めて、関連するオペレーションを実行するためのアクセス許可を付与します。

Amazon FSx アクションのリストを確認するには、サービス認可リファレンスの「Amazon FSx で定義されるアクション」を参照してください。

Amazon FSx のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
fsx
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Amazon FSx のアイデンティティベースポリシーの例を確認するには、「Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例」を参照してください。

Amazon FSx のポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

`Resource` JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource`要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの許可をサポートしないアクションの場合は、ワイルドカード (*) を使用して、ステートメントがすべてのリソースに適用されることを示します。

```
"Resource": "*"
```

Amazon FSx リソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「Amazon FSx for NetApp ONTAP で定義されるリソース」を参照してください。各リソースのARNを指定できるアクションについては、Amazon FSx で定義されているアクション を参照してください。

Amazon FSx のアイデンティティベースポリシーの例を確認するには、「Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例」を参照してください。

Amazon FSx のポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

Amazon FSx for NetApp ONTAP での条件キーの一覧については、「サービス認可リファレンス」の「Condition Keys for Amazon FSx」(Amazon FSx の条件キー) を参照してください。どのアクションおよびリソースと条件キーを使用できるかについては、「Amazon FSx で定義されるアクション」を参照してください。

Amazon FSx のアイデンティティベースポリシーの例を確認するには、「Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例」を参照してください。

Amazon FSx アクセスコントロールリスト (ACL)

ACL のサポート	いいえ

Amazon FSx での属性ベースのアクセスコントロール (ABAC)

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

Amazon FSx リソースのタグ付けの詳細については、「Amazon FSx リソースのタグ付け」を参照してください。

リソースのタグに基づいてリソースへのアクセスを制限するためのアイデンティティベースのポリシーの例を表示するには、「タグを使用した Amazon FSx リソースへのアクセスのコントロール」を参照してください。

Amazon FSx でのテンポラリ認証情報の使用

一時的な認証情報のサポート	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Amazon FSx の転送アクセスセッション

転送アクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Amazon FSx のサービスロール

サービスロールのサポート	いいえ

Amazon FSx のサービスにリンクされたロール

サービスリンクロールのサポート	はい

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集はできません。

Amazon FSx でのサービスにリンクされたロールの作成または管理の詳細については、「Amazon FSx のサービスリンクロールの使用」を参照してください。

Amazon FSx for NetApp ONTAP のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには Amazon FSx リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

Amazon FSx が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、サービス認証リファレンスの「Amazon FSx のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Amazon FSx コンソールの使用
- ユーザーが自分の許可を表示できるようにする

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウント内で誰かが Amazon FSx リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイドの「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、IAM ユーザーガイドの [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

Amazon FSx コンソールの使用

Amazon FSx for NetApp ONTAP コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Amazon FSx リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Amazon FSx コンソールを使用できるようにするには、エンティティに AmazonFSxConsoleReadOnlyAccess AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

AmazonFSxConsoleReadOnlyAccess およびその他の AWS Amazon FSx の マネージドポリシー の Amazon FSx マネージドサービスポリシーが表示されます。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon FSx for NetApp ONTAP のアイデンティティとアクセスのトラブルシューティング

Amazon FSx と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復には、次の情報を利用してください。

トピック

- Amazon FSx でアクションを実行する認可がありません
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに Amazon FSx リソース AWS アカウント へのアクセスを許可したい

Amazon FSx でアクションを実行する認可がありません

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な`fsx:`*`GetWidget`* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

この場合、fsx:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon FSx にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Amazon FSx でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Amazon FSx リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Amazon FSx が機能をサポートしているかどうかを確認するには、「Amazon FSx for NetApp ONTAP と IAM の連携方法」を参照してください。

- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Amazon FSx でのタグの使用

タグを使用すると、Amazon FSx リソースへのアクセスをコントロールしたり、属性ベースのアクセスコントロール (ABAC) を実装したりできます。作成中に Amazon FSx リソースにタグを適用するには、ユーザーは特定の AWS Identity and Access Management (IAM) 許可を持っている必要があります。

作成中にリソースにタグを付ける許可を付与する

一部のリソース作成 Amazon FSx API アクションでは、リソースの作成時にタグを指定できます。リソースタグを使用して、属性ベースのアクセスコントロール (ABAC) を実装できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

ユーザーがリソースの作成時にタグを付けるには、リソースを作成するアクション (`fsx:CreateFileSystem`、`fsx:CreateStorageVirtualMachine` や `fsx:CreateVolume` など) を使用するためのアクセス許可が必要です。リソース作成アクションでタグが指定されている場合、IAM は `fsx:TagResource` アクションに対して追加の認可を実行して、ユーザーがタグを作成する認可を持っているかどうかを確認します。そのため、ユーザーには、`fsx:TagResource` アクションを使用する明示的なアクセス許可も必要です。

次のポリシー例では、ユーザーがファイルシステムとストレージ仮想マシン (SVMsを作成し、特定の での作成時にタグを適用することを許可します AWS アカウント。

```
{
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

同様に、次のポリシーでは、ユーザーが特定のファイルシステム上でバックアップを作成し、バックアップ作成時にバックアップにタグを適用することができます。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

fsx:TagResource アクションは、タグがリソース作成アクション時に適用された場合のみ評価されます。したがって、リクエストでタグが指定されていない場合、リソースを作成するアクセス許可を持つユーザー (タグ付け条件がないと仮定) には、fsx:TagResource アクションを実行するアクセス許可は必要ありません。ただし、ユーザーがタグ付きリソースを作成しようとした場合、ユーザーが fsx:TagResource アクションを使用するアクセス許可を持っていない場合はリクエストに失敗します。

Amazon FSx リソースのタグ付けの詳細については、「Amazon FSx リソースのタグ付け」を参照してください。タグを使用して Amazon FSx リソースへのアクセスコントロールの詳細については、「タグを使用した Amazon FSx リソースへのアクセスのコントロール」を参照してください。

タグを使用した Amazon FSx リソースへのアクセスのコントロール

Amazon FSx とアクションへのアクセスをコントロールするには、タグに基づいて IAM ポリシーを使用できます。コントロールは 2 つの方法で可能です。

- それらのリソースのタグに基づいて、Amazon FSx へのアクセスをコントロールできます。
- IAM リクエストの条件でどのタグを渡すかをコントロールできます。

タグを使用してリソースへのアクセスを制御する方法については AWS 、IAM ユーザーガイドの「タグを使用したアクセスの制御」を参照してください。 作成時の Amazon FSx リソースのタグ付けの詳細については、「作成中にリソースにタグを付ける許可を付与する」を参照してください。リソースのタグ付けの詳細については、「Amazon FSx リソースのタグ付け」を参照してください

リソースのタグに基づいてアクセスのコントロール

ユーザーまたはロールが Amazon FSx リソースで実行できるアクションをコントロールするには、リソースでタグを使用できます。例えば、リソースのタグのキーバリューのペアに基づいて、ファイルシステムリソースに対する特定の API オペレーションを許可または拒否したい場合があります。

Example ポリシーの例 - 特定のタグが使用されている場合にのみファイルシステムを作成する

このポリシーにより、ユーザーは、特定のタグとキーと値のペア (この例では、`key=Department`、`value=Finance`) でタグ付けした場合にのみ、ファイルシステムを作成できます。

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
```

```
        }
    }
}
```

Example ポリシーの例 — 特定のタグを持つ Amazon FSx for NetApp ONTAP ボリュームのバックアップのみを作成する

このポリシーでは、キーバリューのペア key=Department、value=Finance でタグ付けされた FSx for ONTAP ボリュームのバックアップのみを作成できます。バックアップは、タグ Department=Finance 付きで作成されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example ポリシーの例 - 特定のタグを持つバックアップから、特定のタグを持つボリュームを作成します。

このポリシーによりユーザーは Department=Finance タグが付けられているバックアップから Department=Finance でタグ付けされたボリュームのみを作成できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example ポリシーの例 - 特定のタグを持つファイルシステムの削除

このポリシーにより、ユーザーは Department=Finance でタグ付けされたファイルシステムのみを削除できます。最終バックアップを作成する場合は、それは Department=Finance でタグ付けされる必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example ポリシーの例 - 特定のタグを持つボリュームの削除

このポリシーにより、ユーザーは Department=Finance でタグ付けされたボリュームのみを削除できます。最終バックアップを作成する場合は、Department=Finance でタグ付けする必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
```

```
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Amazon FSx のサービスリンクロールの使用

Amazon FSx は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスリンクロールは、Amazon FSx に直接リンクされているユニークなタイプの IAM ロールです。サービスにリンクされたロールは Amazon FSx によって事前定義されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要な許可を手動で追加する必要がないため、Amazon FSx のセットアップが簡単になります。サービスリンクロールの許可は Amazon FSx が定義し、特に定義されない限り、Amazon FSx のみがそのロールを引き受けることができます。定義される許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除しなければなりません。これは、リソースにアクセスするための許可を不用意に削除できないため、Amazon FSx リソースを保護できます。

サービスリンクロールをサポートする他のサービスについては、IAM と連携するAWS るサービス を参照し、サービスリンクロール 列で はい のあるサービスを探してください。サービスリンクロールに関するドキュメントをサービスで表示するには、リンク付きの「はい」を選択します。

Amazon FSx のサービスリンクロール許可

Amazon FSx は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForAmazonFSx。これにより、VPC 内のファイルシステム用の Elastic Network Interface の作成や、 でのファイルシステムとボリュームのメトリクスの発行など、アカウントで特定のアクションを実行します CloudWatch。

このポリシーの更新については、「」を参照してください。 AmazonFSxServiceRolePolicy

許可の詳細

許可の詳細

AWSServiceRoleForAmazonFSx ロールのアクセス許可は、AmazonFSxServiceRolePolicy AWS 管理ポリシーによって定義されます。には次のアクセス許可 AWSServiceRoleForAmazonFSx があります。

> **Note**
>
> AWSServiceRoleForAmazonFSx はすべての Amazon FSx ファイルシステムタイプで使用されます。リストされているアクセス許可の一部は FSx for ONTAP には適用されません。

- ds — Amazon FSx が AWS Directory Service ディレクトリ内のアプリケーションを表示、承認、および承認解除できるようにします。
- ec2 - Amazon FSx に以下のことを許可します。
  - Amazon FSx ファイルシステムに関連付けられたネットワークインターフェイスを表示、作成、および関連付け解除します。
  - Amazon FSx ファイルシステムに関連付けられた 1 つ以上の Elastic IP アドレスを表示します。
  - Amazon FSx ファイルシステムに関連付けられている Amazon VPC、セキュリティグループ、およびサブネットを表示します。
  - VPC で使用できるすべてのセキュリティグループについて、セキュリティグループの検証を強化します。

  - ネットワークインターフェイスで特定のオペレーションを実行するための、 AWSが認可されたユーザーに対するアクセス許可を作成します。
- `cloudwatch` — Amazon FSx がメトリクスデータポイントを AWS/FSx 名前空間 CloudWatch のに発行できるようにします。
- `route53` - Amazon FSx に Amazon VPC をプライベートホストゾーンに関連付けることを許可します。
- `logs` — Amazon FSx が CloudWatch ログログストリームを記述して書き込むことを許可します。これは、ユーザーが FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを CloudWatch Logs ストリームに送信できるようにするためです。
- `firehose` — Amazon FSx が Amazon Data Firehose 配信ストリームを記述および書き込みできるようにします。これは、ユーザーが Amazon FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを Amazon Data Firehose 配信ストリームに発行できるようにするためです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
```

```
        }
    ]
}
```

本ポリシーの更新については、AWS マネージドポリシーに対する Amazon FSx の更新 に記載されています。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールのアクセス許可」を参照してください。

Amazon FSx のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。、IAM CLI AWS Management Console、または IAM API でファイルシステムを作成すると、Amazon FSx によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。サービスリンクロールは、ファイルシステムの作成時に Amazon FSx で自動的に再作成されます。

Amazon FSx のサービスにリンクされたロールの編集

Amazon FSx では、 AWSServiceRoleForAmazonFSx サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

Amazon FSx のサービスリンクロールの削除

サービスにリンクされたロールを必要とする機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。これにより、積極的にモニタリングまたは保守されない未使用の

エンティティを排除できます。ただし、サービスにリンクされたロールを手動で削除する前に、すべての ファイルシステムおよびバックアップを削除する必要があります。

> **Note**
>
> リソースを削除しようとしたときに Amazon FSx サービスがロールを使用している場合は、削除が失敗する可能性があります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、IAM CLI、または IAM API を使用して、サービスにリンクされたロールを削除します AWSServiceRoleForAmazonFSx。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

Amazon FSx サービスリンクロールがサポートされるリージョン

Amazon FSx は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「AWS リージョンとエンドポイント」を参照してください。

AWS Amazon FSx の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AmazonFSxServiceRolePolicy

Amazon FSx がユーザーに代わって AWS リソースを管理できるようにします。詳細については、「Amazon FSx のサービスリンクロールの使用」を参照してください。

AWS マネージドポリシー: AmazonFSxDeleteServiceLinkedRoleAccess

IAM エンティティに `AmazonFSxDeleteServiceLinkedRoleAccess` をアタッチすることはできません。このポリシーはサービスにリンクされ、そのサービス用のサービスにリンクされたロールでのみ使用されます。このポリシーをアタッチ、デタッチ、変更、または削除することはできません。詳細については、「Amazon FSx のサービスリンクロールの使用」を参照してください。

このポリシーは、Amazon FSx for Lustre によって Amazon FSx でのみ使用する Simple Storage Service (Amazon S3) アクセスのサービスリンクロールを削除できるようにする管理者許可を付与します。

許可の詳細

このポリシーには、Amazon FSx が Simple Storage Service (Amazon S3) アクセスの FSx サービスリンクロールの削除ステータスを表示、削除、および表示できる `iam` での許可が含まれます。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイド」の`AmazonFSxDeleteServiceLinkedRoleAccess`」を参照してください。

AWS マネージドポリシー: AmazonFSxFull Access

AmazonFSxFullAccess を IAM エンティティにアタッチできます。また、このポリシーはユーザーに代わってアクションを実行できることを Amazon FSx に許可するためのサービスロールにも添付されます。

Amazon FSx へのフルアクセスおよび関連 AWS サービスへのアクセスを提供します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `fsx` – プリンシパルに、Amazon FSx のすべてのアクション (`BypassSnaplockEnterpriseRetention` を除く) を実行するためのフルアクセスを付与します。

- ds – プリンシパルが AWS Directory Service ディレクトリに関する情報を表示できるようにします。
- ec2
  - プリンシパルが指定された条件でタグを作成できるようにします。
  - VPC で使用できるすべてのセキュリティグループのセキュリティグループ検証を強化します。
- iam - プリンシパルに、ユーザーに代わって Amazon FSx サービスにリンクされたロールを作成することを許可します。これは、Amazon FSx がユーザーに代わって AWS リソースを管理できるようにするために必要です。
- logs - プリンシパルに、ロググループ、ログストリームの作成、ログストリームへのイベントの書き込みを許可します。これは、ユーザーが監査アクセスログを CloudWatch Logs に送信して FSx for Windows File Server ファイルシステムアクセスをモニタリングできるようにするために必要です。
- firehose — プリンシパルが Amazon Data Firehose にレコードを書き込むことを許可します。これは、ユーザーが監査アクセスログを Firehose に送信して FSx for Windows File Server のファイルシステムアクセスをモニタリングできるようにするために必要です。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイド」のAmazonFSxFull Access」を参照してください。

AWS マネージドポリシー: AmazonFSxConsoleFullAccess

AmazonFSxConsoleFullAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、Amazon FSx へのフルアクセスと、 を介した関連 AWS サービスへのアクセスを許可する管理アクセス許可を付与します AWS Management Console。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- fsx – プリンシパルに、Amazon FSx マネジメントコンソールのすべてのアクション (BypassSnaplockEnterpriseRetention を除く) を実行することを許可します。
- cloudwatch — プリンシパルが Amazon FSx マネジメントコンソールで CloudWatch アラームとメトリクスを表示できるようにします。
- ds — プリンシパルが AWS Directory Service ディレクトリに関する情報を一覧表示できるようにします。

- ec2
  - プリンシパルが Amazon FSx ファイルシステムに関連付けられたルートテーブル、ネットワークインターフェイス、ルートテーブル、セキュリティグループ、サブネット、および VPC にタグを作成できるようにします。
  - VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供するには、プリンシパルに を許可します。
- kms — プリンシパルが AWS Key Management Service キーのエイリアスを一覧表示できるようにします。
- s3 - プリンシパルが、Simple Storage Service (Amazon S3) バケット内のオブジェクトの一部またはすべてを一覧表示できるようにします (最大 1000)。
- iam - Amazon FSx がユーザーに代わってアクションを実行できるようにするサービスリンクロールを作成する許可を付与します。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイド」のAmazonFSxConsoleFullAccess」を参照してください。

AWS マネージドポリシー: AmazonFSxConsoleReadOnly Access

AmazonFSxConsoleReadOnlyAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、ユーザーが でこれらの AWS サービスに関する情報を表示できるように、Amazon FSx および関連サービスへの読み取り専用アクセス許可を付与します AWS Management Console。

アクセス許可の詳細

このポリシーには、以下の許可が含まれています。

- fsx - プリンシパルが Amazon FSx マネジメントコンソールで、すべてのタグを含む Amazon FSx ファイルシステムに関する情報を表示できるようにします。
- cloudwatch — プリンシパルが Amazon FSx マネジメントコンソールで CloudWatch アラームとメトリクスを表示できるようにします。
- ds — プリンシパルが Amazon FSx マネジメントコンソールで AWS Directory Service ディレクトリに関する情報を表示できるようにします。
- ec2
  - プリンシパルが Amazon FSx マネジメントコンソールで Amazon FSx ファイルシステムに関連付けられたネットワークインターフェイス、セキュリティグループ、サブネット、および VPC を表示できるようにします。

  - VPC で使用できるすべてのセキュリティグループのセキュリティグループ検証を強化します。
- kms — プリンシパルが Amazon FSx マネジメントコンソールで AWS Key Management Service キーのエイリアスを表示できるようにします。
- log – プリンシパルがリクエストを行うアカウントに関連付けられた Amazon CloudWatch Logs ロググループを記述できるようにします。これは、プリンシパルが FSx for Windows File Server ファイルシステムの既存のファイルアクセス監査の設定を表示できるために必要です。
- firehose – プリンシパルがリクエストを行うアカウントに関連付けられた Amazon Data Firehose 配信ストリームを記述できるようにします。これは、プリンシパルが FSx for Windows File Server ファイルシステムの既存のファイルアクセス監査の設定を表示できるために必要です。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイド」のAmazonFSxConsoleReadOnly Access」を参照してください。

AWS マネージドポリシー: AmazonFSxReadOnlyAccess

AmazonFSxReadOnlyAccess ポリシーは IAM ID にアタッチできます。

このポリシーには、以下のアクセス許可が含まれています。

- fsx - プリンシパルが Amazon FSx マネジメントコンソールで、すべてのタグを含む Amazon FSx ファイルシステムに関する情報を表示できるようにします。
- ec2 – VPC で使用できるすべてのセキュリティグループのセキュリティグループ検証を強化します。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンスガイド」のAmazonFSxReadOnlyAccess」を参照してください。

AWS マネージドポリシーに対する Amazon FSx の更新

Amazon FSx の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページへの変更に関する自動アラートについては、Amazon FSx Amazon FSx for NetApp ONTAP のドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
AmazonFSxServiceRolePolicy – 既存のポリシーの更新	Amazon FSx に新しいアクセス許可が追加されました。`ec2:GetSecurityGroupsForVpc` これにより、プリンシパルは VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供できます。	2024 年 1 月 9 日
AmazonFSxReadOnlyAccess – 既存のポリシーの更新	Amazon FSx に新しいアクセス許可が追加されました。`ec2:GetSecurityGroupsForVpc` これにより、プリンシパルは VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供できます。	2024 年 1 月 9 日
AmazonFSxConsoleReadOnlyAccess – 既存のポリシーの更新	Amazon FSx に新しいアクセス許可が追加されました。`ec2:GetSecurityGroupsForVpc` これにより、プリンシパルは VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供できます。	2024 年 1 月 9 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx に新しいアクセス許可が追加されました。`ec2:GetSecurityGroupsForVpc` これにより、プリンシパルは VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供できます。	2024 年 1 月 9 日

変更	説明	日付
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx に新しいアクセス許可が追加されました。`ec2:GetSecurityGroupsForVpc` これにより、プリンシパルは VPC で使用できるすべてのセキュリティグループの拡張セキュリティグループ検証を提供できます。	2024 年 1 月 9 日
AmazonFSxFull Access – 既存のポリシーへの更新	Amazon FSx に、ユーザーが FSx for OpenZFS ファイルシステムに対してクロスリージョンおよびクロスアカウントのデータレプリケーションを実行できるようにする新しいアクセス許可が追加されました。	2023 年 12 月 20 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx に、ユーザーが FSx for OpenZFS ファイルシステムに対してクロスリージョンおよびクロスアカウントのデータレプリケーションを実行できるようにする新しいアクセス許可が追加されました。	2023 年 12 月 20 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx に、ユーザーが FSx for OpenZFS ファイルシステムに対してボリュームのオンデマンドレプリケーションを実行できるようにする新しいアクセス許可が追加されました。	2023 年 11 月 26 日

変更	説明	日付
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx に、ユーザーが FSx for OpenZFS ファイルシステムに対してボリュームのオンデマンドレプリケーションを実行できるようにする新しいアクセス許可が追加されました。	2023 年 11 月 26 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx に、ユーザーが FSx for ONTAP マルチ AZ ファイルシステムに対して共有 VPC サポートを表示、有効化、無効化できるようにする新しいアクセス許可が追加されました。	2023 年 11 月 14 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx に、ユーザーが FSx for ONTAP マルチ AZ ファイルシステムに対して共有 VPC サポートを表示、有効化、無効化できるようにする新しいアクセス許可が追加されました。	2023 年 11 月 14 日
AmazonFSxFull Access – 既存のポリシーへの更新	Amazon FSx は、Amazon FSx に FSx for OpenZFS Multi-AZ ファイルシステムのネットワーク設定を管理できるように、新しいアクセス許可を追加しました。	2023 年 8 月 9 日

変更	説明	日付
AWS マネージドポリシー: AmazonFSxServiceRolePolicy – 既存のポリシーの更新	Amazon FSx は、Amazon FSx がAWS/FSx名前空間に CloudWatch メトリクスを発行するように既存のcloudwatch:PutMetricData アクセス許可を変更しました。	2023 年 7 月 24 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx のポリシーが更新され、fsx:* アクセス権限が削除され、特定の fsx アクションが追加されました。	2023 年 7 月 13 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx のポリシーが更新され、fsx:* アクセス権限が削除され、特定の fsx アクションが追加されました。	2023 年 7 月 13 日
AmazonFSxConsoleReadOnlyAccess – 既存のポリシーの更新	Amazon FSx は、FSx for Windows File Server ファイルシステム用の強化されたパフォーマンスメトリクスと推奨アクションをユーザーが Amazon FSx コンソールで表示できるように、新しいアクセス許可を追加しました。	2022 年 9 月 21 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx は、FSx for Windows File Server ファイルシステム用の強化されたパフォーマンスメトリクスと推奨アクションをユーザーが Amazon FSx コンソールで表示できるように、新しいアクセス許可を追加しました。	2022 年 9 月 21 日

変更	説明	日付
AmazonFSxReadOnlyAccess — 追跡ポリシーを開始しました	このポリシーにより、すべての Amazon FSx のリソースと、それらに関連付けられたすべてのタグへの読み取り専用アクセスを許可します。	2022 年 2 月 4 日
AmazonFSxDeleteServiceLinkedRoleAccess — 追跡ポリシーを開始しました	このポリシーは、Amazon FSx が Simple Storage Service (Amazon S3) アクセスのサービスにリンクされたロールを削除することを許可する管理者許可を付与します。	2022 年 1 月 7 日
AmazonFSxServiceRolePolicy – 既存のポリシーの更新	Amazon FSx は、Amazon FSx が Amazon FSx for NetApp ONTAP ファイルシステムのネットワーク設定を管理できるようにする新しいアクセス許可を追加しました。	2021 年 9 月 2 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx は、Amazon FSx がスコープダウン呼び出し用の EC2 ルートテーブルにタグを作成できるように、新しいアクセス許可を追加しました。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx は、Amazon FSx が Amazon FSx for NetApp ONTAP マルチ AZ ファイルシステムを作成できるようにする新しいアクセス許可を追加しました。	2021 年 9 月 2 日

変更	説明	日付
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx は、Amazon FSx がスコープダウン呼び出し用の EC2 ルートテーブルにタグを作成できるように、新しいアクセス許可を追加しました。	2021 年 9 月 2 日
AmazonFSxServiceRolePolicy – 既存のポリシーの更新	Amazon FSx は、Amazon FSx が CloudWatch Logs ロググストリームを記述して書き込むことを許可する新しいアクセス許可を追加しました。 これは、ユーザーが Logs を使用して FSx for Windows File Server ファイルシステムのファイルアクセス監査 CloudWatch ログを表示できるようにするために必要です。	2021 年 6 月 8 日
AmazonFSxServiceRolePolicy – 既存のポリシーの更新	Amazon FSx は、Amazon FSx が Amazon Data Firehose 配信ストリームを記述して書き込むことを許可する新しいアクセス許可を追加しました。 これは、ユーザーが Amazon Data Firehose を使用して FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを表示できるようにするために必要です。	2021 年 6 月 8 日

変更	説明	日付
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx は、プリンシパルが CloudWatch ロググループを記述および作成し、ストリームをログに記録し、イベントをログストリームに書き込むことを許可する新しいアクセス許可を追加しました。 これは、プリンシパルが Logs を使用して FSx for Windows File Server ファイルシステムのファイルアクセス監査 CloudWatch ログを表示できるようにするために必要です。	2021 年 6 月 8 日
AmazonFSxFull Access – 既存のポリシーの更新	Amazon FSx は、プリンシパルがレコードを記述して Amazon Data Firehose に書き込むことを許可する新しいアクセス許可を追加しました。 これは、ユーザーが Amazon Data Firehose を使用して FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを表示できるようにするために必要です。	2021 年 6 月 8 日

変更	説明	日付
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx は、プリンシパルがリクエストを行うアカウントに関連付けられた Amazon CloudWatch Logs ロググループを記述できるようにする新しいアクセス許可を追加しました。 これは、FSx for Windows File Server ファイルシステムのファイルアクセス監査を設定するときに、プリンシパルが既存の CloudWatch Logs ロググループを選択できるようにするために必要です。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess – 既存のポリシーの更新	Amazon FSx は、プリンシパルがリクエストを行うアカウントに関連付けられた Amazon Data Firehose 配信ストリームを記述できるようにする新しいアクセス許可を追加しました。 これは、FSx for Windows File Server ファイルシステムのファイルアクセス監査を設定するときに、プリンシパルが既存の Firehose 配信ストリームを選択できるようにするために必要です。	2021 年 6 月 8 日

変更	説明	日付
AmazonFSxConsoleReadOnlyAccess – 既存のポリシーの更新	Amazon FSx は、プリンシパルがリクエストを行うアカウントに関連付けられた Amazon CloudWatch Logs ロググループを記述できるようにする新しいアクセス許可を追加しました。 これは、プリンシパルが FSx for Windows File Server ファイルシステムの既存のファイルアクセス監査の設定を表示できるために必要です。	2021 年 6 月 8 日
AmazonFSxConsoleReadOnlyAccess – 既存のポリシーの更新	Amazon FSx は、プリンシパルがリクエストを行うアカウントに関連付けられた Amazon Data Firehose 配信ストリームを記述できるようにする新しいアクセス許可を追加しました。 これは、プリンシパルが FSx for Windows File Server ファイルシステムの既存のファイルアクセス監査の設定を表示できるために必要です。	2021 年 6 月 8 日
Amazon FSx が変更の追跡をスタートしました	Amazon FSx が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 6 月 8 日

Amazon VPC によるファイルシステムアクセスコントロール

Amazon FSx for NetApp ONTAP ファイルシステムおよび SVMs にアクセスするには、アクセスのタイプに応じて、エンドポイントの DNS 名または IP アドレスを使用します。DNS 名は、VPC 内のファイルシステムまたは SVM の Elastic Network Interface プライベート IP アドレスにマッピングされます。関連付けられた VPC 内のリソース、または AWS Direct Connect または VPN によって関連付けられた VPC に接続されたリソースのみが、NFS、SMB、または iSCSI プロトコルを介してファイルシステム内のデータにアクセスできます。詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC とは」を参照してください。

> **Warning**
>
> ファイルシステムに関連付けられている Elastic Network Interface を変更または削除してはいけません。このネットワークインターフェイスを変更または削除すると、VPC とファイルシステムとの間の接続が完全に失われる可能性があります。

Amazon VPC セキュリティグループ

セキュリティグループは、FSx for ONTAP ファイルシステムの仮想ファイアウォールとして機能し、受信トラフィックと送信トラフィックをコントロールします。インバウンドルールはファイルシステムへの受信トラフィックをコントロールし、アウトバウンドルールはファイルシステムからの送信トラフィックをコントロールします。ファイルシステムを作成するときは、作成する VPC を指定するとその VPC のデフォルトのセキュリティグループが適用されます。各セキュリティグループに対してルールを追加し、関連付けられたファイルシステムおよび SVM に対するトラフィックを許可できます。セキュリティグループのルールはいつでも変更できます。新規または変更したルールは、セキュリティグループに関連付けられたすべてのリソースに自動的に適用されます。Amazon FSx は、トラフィックがリソースに到達することを許可するかどうか判断する際に、リソースに関連付けられているすべてのセキュリティグループのすべてのルールを評価します。

セキュリティグループを使用して Amazon FSx ファイルシステムへのアクセスをコントロールするには、インバウンドとアウトバウンドのルールを追加します。インバウンドルールは受信トラフィックをコントロールし、アウトバウンドルールはファイルシステムからの送信トラフィックをコントロールします。Amazon FSx ファイルシステムのファイル共有を、サポートされているコンピュートインスタンス上のフォルダーにマッピングするため、適切なネットワークトラフィックルールがセキュリティグループにあることを確認します。

セキュリティグループルールの詳細については、「Amazon EC2 ユーザーガイド」の「セキュリティグループルール」を参照してください。 Amazon EC2

VPC セキュリティグループを作成する

Amazon FSx のセキュリティグループを作成するには

1. https://console.aws.amazon.com/ec2 で Amazon EC2 コンソールを開きます。
2. ナビゲーションペインで、[セキュリティグループ] を選択します。
3. [Create Security Group] (セキュリティグループの作成) を選択します。
4. セキュリティグループの名前と説明を指定します。
5. VPC で、ファイルシステムに関連付けられている Amazon VPC を選択して、その VPC 内にセキュリティグループを作成します。
6. アウトバウンドルールについて、すべてのポート上のすべてのトラフィックを許可します。
7. セキュリティグループの着信ポートに次のルールを追加します。出典 フィールドでは [Custom] (カスタム) を選択し、FSx for ONTAP ファイルシステムにアクセスする必要があるインスタンスに関連付けられているセキュリティグループまたは IP アドレス範囲を入力する必要があります。これには、次のものが含まれます。

   - NFS、SMB、または iSCSI 経由でファイルシステム内のデータにアクセスする Linux、Windows、macOS クライアント。
   - ファイルシステムにピアリングする ONTAP ファイルシステム/クラスター (、 SnapMirror SnapVault、 など ） FlexCache。
   - ONTAP REST API、CLI、または ZAPIs へのアクセスに使用するすべてのクライアント (Harvest/Grafana インスタンス、 NetApp Connector、または NetApp BlueXP など ）。

[プロトコル]	ポート	ロール
すべての ICMP	すべて	インスタンスへの ping を実行する
SSH	22	クラスター管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	135	CIFS のリモートプロシージャコール

[プロトコル]	ポート	ロール
TCP	139	CIFS 用の NetBIOS サービスセッション
TCP	161-162	SNMP (簡易ネットワーク管理プロトコル)
TCP	443	ONTAP REST API は、クラスター管理 LIF または SVM 管理 LIF の IP アドレスにアクセスします
TCP	445	NetBIOS フレーミングを使用した Microsoft SMB / CIFS over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバーデーモン
TCP	3260	iSCSI データ LIF 経由の iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタリング
TCP	10000	ネットワークデータ管理プロトコル (NDMP) とクラスター NetApp SnapMirror 間通信
TCP	11104	クラスター NetApp SnapMirror 間通信の管理
TCP	11105	SnapMirror クラスター間 LIFs を使用したデータ転送
UDP	111	NFS のリモートプロシージャコール
UDP	135	CIFS のリモートプロシージャコール
UDP	137	CIFS の NetBIOS 名解像度
UDP	139	CIFS 用の NetBIOS サービスセッション
UDP	161-162	SNMP (簡易ネットワーク管理プロトコル)
UDP	635	NFS マウント

[プロトコル]	ポート	ロール
UDP	2049	NFS サーバーデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタリング
UDP	4049	NFS クォータプロトコル

8. ファイルシステムの Elastic Network Interface にセキュリティグループを追加します。

ファイルシステムへのアクセスを許可しない

すべてのクライアントからファイルシステムへのネットワークアクセスを一時的に無効にするには、ファイルシステムの Elastic Network Interface (複数も可) に関連付けられているすべてのセキュリティグループを削除し、インバウンド / アウトバウンドルールを持たないグループに置き換えます。

Amazon FSx for NetApp ONTAP のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon FSx for NetApp ONTAP とインターフェイス VPC エンドポイント (AWS PrivateLink)

インターフェイス VPC エンドポイントを使用するように Amazon FSx を設定することで、VPC のセキュリティ体制を強化できます。インターフェイス VPC エンドポイントは、インターネットゲートウェイAWS PrivateLink、NAT デバイス、VPN 接続、 AWS Direct Connect 接続のいずれも必要

とせずに Amazon FSx APIs にプライベートにアクセスできるテクノロジーである を利用しています。VPC のインスタンスは、パブリック IP アドレスがなくても Amazon FSx API と通信できます。VPC と Amazon FSx 間のトラフィックは、 AWS ネットワークを離れません。

各インターフェイス VPC エンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。ネットワークインターフェイスは、Amazon FSx API へのトラフィックのエントリポイントとなるプライベート IP アドレスを提供します。

Amazon FSx インターフェイス VPC エンドポイントに関する考慮事項

Amazon FSx のインターフェイス VPC エンドポイントを設定する前に、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプロパティと制限」を確認してください。

VPC から任意の Amazon FSx API オペレーションを呼び出すことができます。例えば、VPC 内から CreateFileSystem API を呼び出すことで、FSx for ONTAP ファイルシステムを作成できます。Amazon FSx API の詳細なリストについては、「Amazon FSx API Reference」(Amazon FSx API リファレンス) の「Actions」(アクション) を参照してください。

VPC ピアリングに関する考慮事項

他の VPC には、インターフェイス VPC エンドポイントを使用して、VPC ピアリングによって接続できます。VPC ピアリングは、2 つの VPC 間のネットワーク接続です。自分が所有者である 2 つの VPC 間や、他の AWS アカウントアカウント内の VPC との間で、VPC ピアリング接続を確立できます。VPCs 2 つの異なる にすることもできます AWS リージョン。

ピア接続された VPCs 間のトラフィックは AWS ネットワーク上にとどまり、パブリックインターネットを経由しません。VPC がピア接続されると、双方の VPC にある Amazon Elastic Compute Cloud (Amazon EC2) インスタンスは、いずれかの VPC で作成されたインターフェイス VPC エンドポイントを介して Amazon FSx API にアクセスできます。

Amazon FSx API 用のインターフェイス VPC エンドポイントの作成

Amazon FSx API の VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、「Amazon VPC ユーザーガイド」の「Creating an interface VPC endpoint」(インターフェイス VPC エンドポイントの作成) を参照してください。

Amazon FSx のインターフェイス VPC エンドポイントを作成するには、次のいずれかを使用します。

- **com.amazonaws.*region*.fsx** – Amazon FSx API オペレーションのエンドポイントを作成します。
- **com.amazonaws.*region*.fsx-fips** — 連邦情報処理規格 (FIPS) 140-2 に準拠した Amazon FSx API のエンドポイントを作成します。

オプションとしてプライベート DNS を使用するには、VPC の enableDnsHostnames および enableDnsSupport 属性を設定する必要があります。詳細については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性の表示と更新」を参照してください。

中国を除き、エンドポイント AWS リージョン のプライベート DNS を有効にすると、 AWS リージョンなどの のデフォルト DNS 名を使用して VPC エンドポイントで Amazon FSx に API リクエストを実行できますfsx.us-east-1.amazonaws.com。中国 (北京) と中国 (寧夏) では AWS リージョン、fsx-api.cn-northwest-1.amazonaws.com.cnそれぞれ fsx-api.cn-north-1.amazonaws.com.cnと を使用して VPC エンドポイントで API リクエストを行うことができます。

詳細については、「Amazon VPC ユーザーガイド」の「Accessing a service through an interface VPC endpoint」(インターフェイス VPC エンドポイントを介したサービスへのアクセス) を参照してください。

Amazon FSx 用の VPC エンドポイントポリシーの作成

Amazon FSx API へのアクセスを制御するには、VPC エンドポイントに AWS Identity and Access Management (IAM) ポリシーをアタッチします。本ポリシーでは、以下を規定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

Amazon FSx for NetApp ONTAP の耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、高冗長ネットワークで接続されます。アベイ

ラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Amazon FSx には、 AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能が用意されています。

バックアップと復元

Amazon FSx は、Amazon FSx for NetApp ONTAP ファイルシステムにボリュームの自動バックアップを作成して保存します。Amazon FSx は、Amazon FSx for NetApp ONTAP ファイルシステムのバックアップウィンドウ中にボリュームの自動バックアップを作成します。Amazon FSx は、指定したバックアップ保持期間に従ってボリュームの自動バックアップを保存します。また、ユーザー主導のバックアップを作成することにより、手動でボリュームをバックアップすることもできます。ボリュームバックアップは、出典として指定されたバックアップを使用して新しいボリュームを作成することで、いつでも復元できます。

詳細については、「バックアップの使用」を参照してください。

スナップショット

Amazon FSx は、Amazon FSx for NetApp ONTAP ボリュームのスナップショットコピーを作成します。スナップショットコピーは、エンドユーザーによるボリューム内のファイルの誤った削除や変更に対する保護を提供します。詳細については、「スナップショットの使用」を参照してください。

アベイラビリティーゾーン

Amazon FSx for NetApp ONTAP ファイルシステムは、サーバーに障害が発生した場合でも、データに継続的な可用性を提供するように設計されています。各ファイルシステムでは 2 つのファイルサーバーが使用され、それぞれに 1 つ以上のアベイラビリティーゾーンと独自のストレージがあります。Amazon FSx は、データを自動的にレプリケーションして、コンポーネントの障害からデータを保護し、ハードウェア障害を継続的にモニタリングし、障害が発生した場合にインフラストラクチャコンポーネントを自動的に置き換えます。ファイルシステムは必要に応じて自動的にフェイルオーバーして戻し (通常 60 秒以内)、クライアントは自動的にファイルシステムにフェイルオーバーして戻します。

マルチ AZ ファイルシステム

Amazon FSx for NetApp ONTAP ファイルシステムは、アベイラビリティーゾーン間で AWS 高い可用性と耐久性を備え、アベイラビリティーゾーンが利用できない場合でもデータに継続的な可用性を提供するように設計されています。

詳細については、「可用性と耐久性」を参照してください。

シングル AZ ファイルシステム

Amazon FSx for NetApp ONTAP ファイルシステムは、単一の AWS アベイラビリティーゾーン内で高い可用性と耐久性を備え、個々のファイルサーバーまたはディスクに障害が発生した場合に、そのアベイラビリティーゾーン内で継続的な可用性を提供するように設計されています。

詳細については、「可用性と耐久性」を参照してください。

Amazon FSx for NetApp ONTAP のインフラストラクチャセキュリティ

マネージドサービスである Amazon FSx for NetApp ONTAP は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した API コールを使用して、ネットワーク経由で Amazon FSx にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

FSx for NetApp ONTAP で ONTAP Vscan を使用する

NetApp ONTAP の Vscan 機能を使用して、サポートされているサードパーティーのウイルス対策ソフトウェアを実行できます。詳細については、サポートされているソリューション別に提供されている下記のリソースを参照してください。

- McAfee – クラスター化されたデータ ONTAP のウイルス対策ソリューションガイド： McAfee
- SentinelOne – Vscan パートナーソリューションと SentinelOne Singularity Cloud Data Security
- Symantec — Vscan パートナーソリューションと Symantec Protection Engine
- Trend Micro – 「Antivirus Solution Guide for Clustered Data ONTAP: Trend Micro」(Clustered Data ONTAP のウイルス対策ソリューション: Trend Micro)

Amazon FSx for NetApp ONTAP のロールとユーザー

NetApp ONTAP には、堅牢で拡張可能なロールベースのアクセスコントロール (RBAC) 機能が含まれています。 ONTAPロールは、 CLI ONTAP および REST API を使用するときにユーザー機能と権限を定義します。各ロールは、異なるレベルの管理機能と権限を定義します。REST API と CLI を使用するときに、FSx for ONTAP ONTAP リソースへのアクセスを制御する目的で、ユーザーにロールを割り当てます。FSx for ONTAP ファイルシステムユーザーとストレージ仮想マシン (SVM) ユーザーには、個別に使用できるONTAPロールがあります。

FSx for ONTAP ファイルシステムを作成すると、ファイルシステムレベルと SVM レベルでデフォルトのONTAPユーザーが作成されます。追加のファイルシステムと SVM ユーザーを作成し、組織のニーズに合わせて追加の SVM ロールを作成できます。この章では、ONTAPユーザーとロールについて説明し、追加のユーザーと SVM ロールを作成する詳細な手順を示します。

ファイルシステム管理者のロールとユーザー

デフォルトのONTAPファイルシステムユーザーは でfsxadmin、 fsxadminロールが割り当てられます。ファイルシステムユーザーに割り当てることができる事前定義されたロールは 2 つあり、次のようにリストされています。

- **fsxadmin**— このロールを持つ管理者は、ONTAPシステムに対する無制限の権限を持ちます。FSx for ONTAP ファイルシステムで使用できるすべてのファイルシステムと SVM レベルのリソースを設定できます。
- **fsxadmin-readonly**— このロールを持つ管理者は、ファイルシステムレベルですべてを表示できますが、変更を加えることはできません。

このロールは、使用可能なすべてのリソースとそのプロパティへの読み取り専用アクセス権があるが、変更できないNetApp Harvestため、 などのモニタリングアプリケーションでの使用に適しています。

追加のファイルシステムユーザーを作成し、 `fsxadmin`または `fsxadmin-readonly`ロールを割り当てることができます。新しいロールを作成したり、既存のロールを変更したりすることはできません。詳細については、「ファイルシステムと SVM 管理用の新しいONTAPユーザーの作成」を参照してください。

次の表は、ファイルシステム管理者ロールが CLI および ONTAP REST API コマンドとコマンドディレクトリに対して持つアクセスレベルを示しています。

ロール名	アクセスのレベル	次のコマンドまたはコマンドディレクトリへ
`fsxadmin`	すべて	FSx for ONTAP で利用可能なすべてのコマンドディレクトリ
`fsxadmin-readonly`	すべて	`security login password` 自分のユーザーアカウントのローカルパスワードとキー情報のみを管理する場合
	なし	`security`
	読み取り専用	FSx for ONTAP で利用可能な他のすべてのコマンドディレクトリ

SVM 管理者のロールとユーザー

各 SVM には個別の認証ドメインがあり、独自の管理者によって個別に管理できます。ファイルシステム上の各 SVM では、デフォルトのユーザーは vsadmin で、デフォルトで`vsadmin`ロールが割り当てられます。`vsadmin` ロールに加えて、SVM ユーザーに割り当てることができるスコープダウン

されたアクセス許可を提供する事前定義された SVM ロールもあります。また、組織のニーズに合ったアクセスコントロールのレベルを提供するカスタムロールを作成することもできます。

SVM 管理者の事前定義されたロールとその機能は次のとおりです。

ロール名	機能
`vsadmin`	• ユーザーアカウント、ローカルパスワード、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、スナップショットのコピー、ファイルの管理 • LUN の管理 • 特権削除を除く SnapLock オペレーションの実行 • プロトコルの設定: NFS、SMB、iSCSI • サービスの設定: DNS、LDAP、NIS • ジョブのモニタリング • ネットワーク接続とネットワークインターフェイスのモニタリング • SVM の正常性のモニタリング
`vsadmin-volume`	• ユーザーアカウント、ローカルパスワード、キー情報の管理 • ボリュームの管理 (ボリュームの移動を含む) • クォータ、qtree、スナップショットのコピー、ファイルの管理 • LUN の管理 • プロトコルの設定: NFS、SMB、iSCSI • 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モニタリング • SVM の正常性のモニタリング

ロール名	機能
vsadmin-protocol	• ユーザーアカウント、ローカルパスワード、キー情報の管理 • LUN の管理 • プロトコルの設定: NFS、SMB、iSCSI • 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モニタリング • SVM の正常性のモニタリング
vsadmin-backup	• ユーザーアカウント、ローカルパスワード、キー情報の管理 • NDMP オペレーションの管理 • リストアされたボリュームを読み取り/書き込み可能にする • SnapMirror リレーションシップとスナップショットコピーの管理 • ボリュームとネットワーク情報の表示
vsadmin-snaplock	• ユーザーアカウント、ローカルパスワード、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、スナップショットのコピー、ファイルの管理 • 特権削除を含む SnapLock オペレーションの実行 • プロトコルの設定: NFS、SMB • サービスの設定: DNS、LDAP、NIS • ジョブのモニタリング • ネットワーク接続とネットワークインターフェイスのモニタリング

ロール名	機能
vsadmin-readonly	• ユーザーアカウント、ローカルパスワード、キー情報の管理 • SVM の正常性のモニタリング • ネットワークインターフェイスのモニタリング • ボリュームと LUN の表示 • サービスとプロトコルの表示

新しい SVM ロールを作成する方法の詳細については、「」を参照してください新しい SVM ロールの作成。

Active Directory を使用したONTAPユーザーの認証

FSx for ONTAP ファイルシステムと SVM への Windows Active Directory ドメインユーザーのアクセスを認証できます。Active Directory アカウントがファイルシステムにアクセスする前に、次のタスクを実行する必要があります。

- SVM への Active Directory ドメインコントローラーアクセスを設定する必要があります。

  Active Directory ドメインコントローラーアクセスのゲートウェイまたはトンネルとして設定するために使用する SVM は、CIFS が有効になっているか、Active Directory に参加しているか、またはその両方である必要があります。CIFS を有効にせず、トンネル SVM をアクティブディレクトリにのみ結合する場合は、SVM がアクティブディレクトリに参加していることを確認してください。詳細については、「SVM を Microsoft アクティブディレクトリに接続する」を参照してください。
- ファイルシステムにアクセスするには、Active Directory ドメインユーザーアカウントを有効にする必要があります。

  CLI または REST API にアクセスする Windows ドメインユーザーには、パスワード認証または ONTAP SSH パブリックキー認証を使用できます。

ファイルシステムおよび SVM 管理者の Active Directory 認証の設定に を使用する手順については、「」を参照してくださいONTAP ユーザーの Active Directory 認証の設定。

ファイルシステムと SVM 管理用の新しいONTAPユーザーの作成

各ONTAPユーザーは SVM またはファイルシステムに関連付けられます。fsxadmin ロールを持つファイルシステムユーザーは、 CLI コマンドを使用して新しい SVM security login create ONTAP ロールとユーザーを作成できます。

security login create コマンドは、 管理ユーティリティのログイン方法を作成します。ログイン方法は、ユーザー名、アプリケーション (アクセス方法) 、認証方法で構成されます。ユーザー名は複数のアプリケーションに関連付けることができます。オプションで、アクセスコントロールロール名を含めることができます。Active Directory、LDAP、または NIS グループ名が使用されている場合、ログインメソッドは指定されたグループに属するユーザーにアクセス権を付与します。ユーザーがセキュリティログインテーブルでプロビジョニングされた複数のグループのメンバーである場合、ユーザーは個々のグループに対して承認されたコマンドの組み合わせリストにアクセスできます。

新しいONTAPユーザーを作成する方法については、「」を参照してください新しい ONTAP ユーザーの作成。

トピック

- 新しい ONTAP ユーザーの作成
- 新しい SVM ロールの作成
- ONTAP ユーザーの Active Directory 認証の設定
- パブリックキー認証を設定する
- ファイルシステムと SVM ロールのパスワード要件の更新
- fsxadmin アカウントパスワードの更新が失敗する

新しい ONTAP ユーザーの作成

新しい SVM またはファイルシステムユーザーを作成するには (ONTAP CLI)

fsxadmin ロールを持つファイルシステムユーザーのみが、新しい SVM およびファイルシステムユーザーを作成できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. `security login create` ONTAP CLI コマンドを使用して、FSx for ONTAP ファイルシステムまたは SVM に新しいユーザーアカウントを作成します。

   この例のプレースホルダーのデータを挿入して、次の必須プロパティを定義します。

   - `-vserver` – 新しい SVM ロールまたはユーザーを作成する SVM の名前を指定します。ファイルシステムロールまたはユーザーを作成する場合は、SVM を指定しないでください。
   - `-user-or-group-name` – ログイン方法のユーザー名または Active Directory グループ名を指定します。Active Directory グループ名は、`domain`認証方法と `ontapi`および `ssh`アプリケーションでのみ指定できます。
   - `-application` – ログイン方法のアプリケーションを指定します。指定できる値には、http、ontapi、ssh などがあります。
   - `-authentication-method` – ログインの認証方法を指定します。以下に示しているのは、可能な値です。
     - domain – Active Directory 認証に使用します。
     - password – パスワード認証に使用します。
     - publickey – パブリックキー認証用のユーザー
   - `-role` – ログインメソッドのアクセスコントロールロール名を指定します。ファイルシステムレベルで指定できるロールは、`fsxadmin` のみです。

   (オプション) コマンドでは、次のパラメータを 1 つ以上使用することもできます。

   - `[-comment]` – ユーザーアカウントの表記またはコメントを含める場合に使用します。例えば **`Guest account`** です。最大長は 128 文字です。
   - `[-second-authentication-method {none|publickey|password|nsswitch}]` — 第 2 要素認証方法を指定します。以下の方法を指定できます。
     - password – パスワード認証に使用します。
     - publickey – パブリックキー認証に使用します
     - nsswitch – NIS または LDAP 認証に使用します
     - none – 指定しない場合のデフォルト値

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

次のコマンドは、ログイン用のパスワードnew_fsxadminで SSH を使用して、 fsxadmin-readonlyロールが割り当てられた新しいファイルシステムユーザーを作成します。プロンプトが表示されたら、ユーザーのパスワードを入力します。

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. 次のコマンドは、 vsadmin_readonlyロールを持つ SVM fsx new_vsadminに新しい SVM ユーザーを作成し、SSH とパスワードを使用してログインするように設定します。プロンプトが表示されたら、ユーザーのパスワードを入力します。

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. 次のコマンドharvest2-userは、パフォーマンスと容量のメトリクスを収集するために NetApp Harvest アプリケーションで使用される新しい読み取り専用ファイルシステムユーザーを作成します。詳細については、「Harvest と Grafana を使用した ONTAP ファイルシステムの FSx のモニタリング」を参照してください。

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

すべてのファイルシステムと SVM ユーザーに関する情報を表示するには

- 次のコマンドを使用して、ファイルシステムと SVMs のすべてのログイン情報を表示します。

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none

Vserver: fsx
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

新しい SVM ロールの作成

作成する各 SVM には、事前定義されたvsadminロールが割り当てられたデフォルトの SVM 管理者があります。事前定義された SVM ロールのセットに加えて、新しい SVM ロールを作成できます。SVM の新しいロールを作成する必要がある場合は、 `security login role create` ONTAP CLI コマンドを使用します。このコマンドは、 `fsxadmin`ロールを持つファイルシステム管理者が使用できます。

新しい SVM ロールを作成するには (ONTAP CLI)

1. `security login role create` ONTAP CLI コマンドを使用して新しい SVM ロールを作成できます。

```
Fsx0123456::> security login role create -role vol_role -cmddirname volume
```

2. コマンドに以下の必須パラメータを指定します。

- `-role` – ロールの名前。
- `-cmddirname` — ロールがアクセスを許可するコマンドまたはコマンドディレクトリ。コマンドサブディレクトリ名は二重引用符で囲みます。例えば `"volume snapshot"` です。すべてのコマンドディレクトリを指定するには、`DEFAULT` と入力します。

3. (オプション) 次のいずれかのパラメータをコマンドに追加することもできます。

- `-vserver` – ロールに関連付けられた SVM の名前。
- `-access` — ロールのアクセスレベル。コマンドディレクトリの場合、アクセスレベルには以下が含まれます。
  - none — コマンドディレクトリ内のコマンドへのアクセスを拒否します。これはカスタムロールのデフォルト値です。
  - `readonly` — コマンドディレクトリとそのサブディレクトリにある show コマンドへのアクセスを許可します。
  - `all` — コマンドディレクトリとそのサブディレクトリにあるすべてのコマンドへのアクセスを許可します。組み込みコマンドへのアクセスを許可または拒否するには、コマンドディレクトリを指定する必要があります。

  非組み込みコマンド (末尾が `create`、`modify`、`delete`、または `show` 以外のコマンド) の場合:

  - none — コマンドディレクトリ内のコマンドへのアクセスを拒否します。これはカスタムロールのデフォルト値です。
  - `readonly` – 該当なし。使用不可。
  - `all` — コマンドへのアクセスを許可します。
- `-query` — アクセスレベルをフィルタリングするために使用されるクエリオブジェクト。コマンドまたはコマンドディレクトリ内のコマンドに対して有効なオプションとして指定されます。クエリオブジェクトを二重引用符で囲みます。

4. `security login role create` コマンドを実行します。

次のコマンドは、vs1.example.com Vserver の「admin」という名前のアクセスコントロールロールを作成します。ロールは「volume」コマンドにすべてアクセスできますが、「aggr0」アグリゲート内のみアクセスできます。

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

ONTAP ユーザーの Active Directory 認証の設定

ONTAP CLI を使用して、ONTAPファイルシステムおよび SVM ユーザーに対して Active Directory 認証の使用を設定します。

この手順のコマンドを使用するには、 `fsxadmin`ロールを持つファイルシステム管理者である必要があります。

ONTAP ユーザーの Active Directory 認証を設定するには (ONTAP CLI)

この手順のコマンドは、 `fsxadmin`ロールを持つファイルシステムユーザーが使用できます。

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. 次に示すように `security login domain-tunnel create` コマンドを使用して、Windows Active Directory ユーザーを認証するためのドメイントンネルを確立します。*`svm_name`* をドメイントンネルに使用している SVM の名前に置き換えます。

   ```
   FsxId0123456::> security login domain-tunnel create -vserver svm_name
   ```

3. `security login create` コマンドを使用して、ファイルシステムにアクセスする Active Directory ドメインユーザーアカウントを作成します。

   コマンドに以下の必須パラメータを指定します。

- `-vserver` – CIFS で設定され、Active Directory に結合されている SVM の名前。これは、Active Directory ドメインユーザーの をファイルシステムに対して認証するためのトンネルとして使用されます。新しいロールまたはユーザーが作成されます。
- `-user-or-group-name` — ログインに使用するユーザー名または Active Directory グループ名。Active Directory グループ名は、`domain` 認証、`ontapi`、`ssh` アプリケーションでのみ指定できます。
- `-application` — ログインに使用するアプリケーション。指定できる値には、http、ontapi、ssh などがあります。
- `-authentication-method` – ログインに使用される認証方法。以下に示しているのは、可能な値です。
  - domain – Active Directory 認証用
  - password – パスワード認証用
  - publickey – パブリックキー認証用
- `-role` — ログインに使用するアクセスコントロールのロール名。ファイルシステムレベルで指定できるロールは、`-role fsxadmin` のみです。

次の例では、`CORP\Adminfilesystem1`ファイルシステムの Active Directory ドメインユーザーアカウントを作成します。

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

次の例では、パブリックキー認証を使用して`CORP\Admin`ユーザーアカウントを作成します。

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

次のコマンドを使用して、`CORP\Admin`ユーザーのパブリックキーを作成します。

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Active Directory 認証情報で SSH を使用してファイルシステムにログインするには

- 次の例は、-application タイプで ssh を選択した場合、Active Directory の認証情報を使用してファイルシステムに SSH 接続する方法を示しています。username の形式は "domain-name\user-name" であり、アカウントの作成時に指定したドメイン名とユーザー名をバックスラッシュで区切って引用符で囲んだものです。

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  パスワードの入力を求められたら、Active Directory ユーザーのパスワードを使用してください。

パブリックキー認証を設定する

SSH パブリックキー認証を有効にするには、まず SSH キーを生成し、security login publickey create コマンドを使用してその SSH キーを管理者アカウントに関連付ける必要があります。これにより、アカウントは SVM にアクセスできるようになります。security login publickey create コマンドは、次のパラメータを承諾します。

パラメータ	説明
-vserver (オプション)	アカウントがアクセスする SVM の名前。ファイルシステムユーザーの SSH パブリックキー認証を設定する場合は、 を含めないでください-versver。
-username	アカウントのユーザー名。デフォルト値 admin は、クラスター管理者のデフォルト名です。
-index	パブリックキーのインデックス番号。キーがアカウントで最初に作成されたキーである場合、デフォルト値は 0 です。それ以外の場合、デフォルト値はアカウントの既存の最大インデックス番号より 1 つ大きい値になります。

パラメータ	説明
-publickey	OpenSSH パブリックキー。キーを二重引用符で囲みます。
-role	アカウントに割り当てられているアクセスコントロールのロール。
-comment (オプション)	パブリックキーを説明するテキスト。テキストを二重引用符で囲みます。

次の例では、パブリックキーを SVM svm01 の SVM 管理者アカウント svmadmin に関連付けています。パブリック キーにはインデックス番号 5 が割り当てられています。

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> このタスクを実行するには、SVM またはファイルシステムの管理者である必要があります。

ファイルシステムと SVM ロールのパスワード要件の更新

CLI コマンドを使用して、ファイルシステムまたは SVM security login role config modify ONTAP ロールのパスワード要件を更新できます。このコマンドは、 fsxadminロールを持つファイルシステム管理者アカウントでのみ使用できます。パスワード要件を変更すると、そのロールを持つ既存のユーザーが変更の影響を受ける場合に警告が表示されます。

次の例では、SVM で vsadmin-readonlyロールを持つユーザーのパスワードの最小長要件を 12 fsx 文字に変更します。この例では、このロールを持つ既存のユーザーがいます。

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

既存のユーザーが原因で、次の警告が表示されます。

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

fsxadmin アカウントパスワードの更新が失敗する

fsxadmin ユーザーのパスワードを更新すると、ファイルシステムに設定されているパスワード要件を満たしていない場合にエラーが表示されることがあります。CLI または security login role config show ONTAP REST API コマンドを使用して、パスワード要件を表示できます。

ファイルシステムまたは SVM ロールのパスワード要件を表示するには

1. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

2. security login role config show コマンドは、ファイルシステムまたは SVM ロールのパスワード要件を返します。

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   -fields パラメータには、次のいずれかまたはすべてを指定します。

   - passwd-minlength – パスワードの最小長
   - passwd-min-special-chars – パスワードに含まれる特殊文字の最小数
   - passwd-min-lowercase-chars — パスワードに含まれる小文字の最小数
   - passwd-min-uppercase-chars — パスワードに含まれる大文字の最小数

- passwd-min-digits — パスワードの最小桁数
- passwd-alphanum — 英数字の包含または除外に関する情報
- passwd-expiry-time – パスワードの有効期限
- passwd-expiry-warn-time — パスワード有効期限の警告時間

3. 次のコマンドを実行して、すべてのパスワード要件を確認します。

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                        0
               unlimited
```

Amazon FSx for NetApp ONTAP への移行

以下のセクションでは、既存の NetApp ONTAP ファイルシステムを Amazon FSx for NetApp ONTAP に移行する方法について説明します。

> **Note**
>
> All 階層化ポリシーを使用してデータをキャパシティプール層に移行することを計画している場合、ファイルメタデータは常に SSD 層に格納され、すべての新しいユーザーデータは最初に SSD 層に書き込まれることに注意してください。データが SSD 層に書き込まれると、バックグラウンド階層化プロセスはキャパシティプールストレージへのデータの階層化を開始しますが、階層化プロセスは即時ではなく、ネットワークリソースを消費します。キャパシティプールストレージに階層化する前に、ユーザーデータのバッファとしてファイルメタデータ (ユーザーデータサイズの 3～7%) を考慮して SSD 階層のサイズを設定する必要があります。SSD 層の使用率が 80% を超えないようにすることをお勧めします。
> データを移行する際は、CloudWatch ファイルシステムメトリクスを使用して SSD 階層をモニタリングし、階層化プロセスがデータを容量プールストレージに移動できる速度を超えないようにしてください。

トピック

- を使用した FSx for ONTAP への移行 NetApp SnapMirror
- AWS DataSync を使用した FSx for ONTAP への移行

を使用した FSx for ONTAP への移行 NetApp SnapMirror

を使用して NetApp ONTAP ファイルシステムを Amazon FSx for NetApp ONTAP に移行できます NetApp SnapMirror。

NetApp SnapMirror は、2 つの ONTAP ファイルシステム間でブロックレベルのレプリケーションを使用し、指定されたソースボリュームから宛先ボリュームにデータをレプリケートします。を使用して、オンプレミスの NetApp ONTAP ファイルシステムを FSx for ONTAP SnapMirror に移行することをお勧めします。 NetApp SnapMirrorのブロックレベルのレプリケーションは、次のファイルシステムでも迅速かつ効率的です。

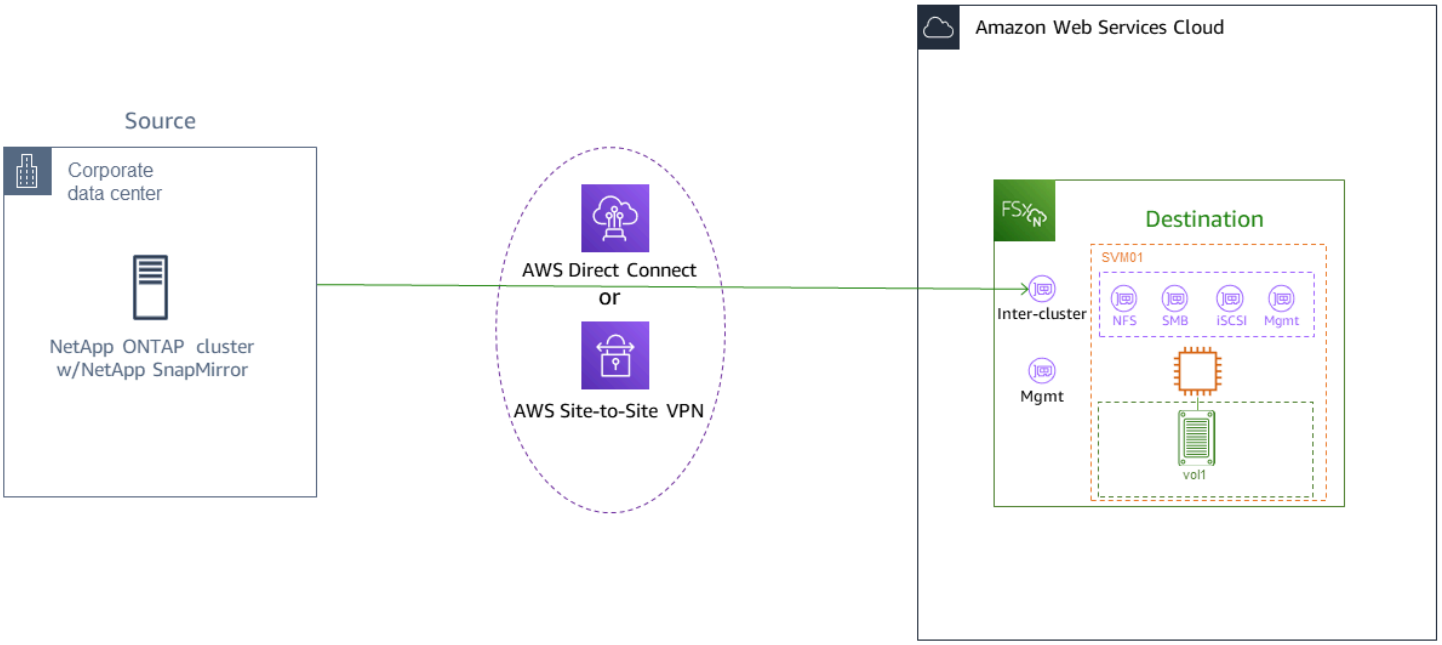
- 複雑なディレクトリ構造

- 5000 万件を超えるファイル
- 非常に小さいファイルサイズ (キロバイト単位)

SnapMirror を使用して FSx for ONTAP に移行する場合、重複排除されたデータや圧縮されたデータはこれらの状態のままになるため、転送時間が短縮され、移行に必要な帯域幅が減ります。ONTAP ボリューム出典に存在するスナップショットは、移行先ボリュームに移行しても保持されます。オンプレミスの NetApp ONTAP ファイルシステムを FSx for ONTAP に移行するには、次の高レベルのタスクが必要です。

1. Amazon FSx で宛先ボリュームを作成します。
2. 移行元と移行先の論理インターフェース (LIF) を収集します。
3. 移行元と移行先のファイルシステム間でクラスターピアリングを確立します。
4. SVM ピアリング関係を作成します。
5. SnapMirror 関係を作成します。
6. 更新された宛先クラスターを維持します。
7. FSx for ONTAP ファイルシステムにカットオーバーします。

次の図表は、このセクションで説明する移行シナリオを示しています。



トピック

- 始める前に

- 宛先ボリュームの作成
- 出典と宛先のクラスター間 LIF をレコードします
- 出典と宛先の間でクラスターピアリングを確立する
- SVM ピアリング関係を作成する
- SnapMirror 関係を作成する
- FSx for ONTAP ファイルシステムへのデータの転送
- Amazon FSx にカットオーバー

始める前に

以下のセクションで説明する手順を使用する前に、次の前提条件を満たしていることを確認してください。

- FSx for ONTAP は、データ階層化、ストレージ効率、バックアップなどのバックグラウンドタスクよりもクライアントトラフィックを優先します。データを移行するときは、一般的なベストプラクティスとして、SSD 層のキャパシティをモニタリングして、使用率が 80% を超えないようにすることをお勧めします。CloudWatch ファイルシステムメトリクス を使用して SSD 層の使用率をモニタリングできます。詳細については、「ボリュームメトリクス」を参照してください。
- データ移行時に移行先ボリュームのデータ階層化ポリシーを `All` に設定すると、すべてのファイルメタデータはプライマリ SSD ストレージ層に保存されます。ファイルメタデータは、ボリュームのデータ階層化ポリシーに関係なく、常に SSD ベースのプライマリ層に保存されます。プライマリ層とキャパシティプール層のストレージ容量の比率を 1:10 と仮定することをお勧めします。
- 出典ファイルシステムと宛先ファイルシステムは同じVPCに接続されているか、Amazon VPCピアリング、トランジットゲートウェイ、AWS Direct Connect、または AWS VPN を使用してピアリングされているネットワークにあります。詳細については、内からのデータへのアクセス AWS と [Amazon VPC Peering Guide] (Amazon VPC ピアリングガイド) の What is VPC peering? (VPC ピアリング機能とは) を参照してください。
- FSx for ONTAP ファイルシステムの VPC セキュリティグループには、クラスター間エンドポイント (LIF) のポート 443、10000、11104、および 11105 で ICMP と TCP を許可するインバウンドルールとアウトバウンドルールがあります。
- SnapMirror データ保護関係を作成する前に、ソースボリュームと宛先ボリュームで互換性のある NetApp ONTAP バージョンが実行されていることを確認します。詳細については、 NetAppの ONTAP ユーザードキュメントの SnapMirror 「関係の互換性のある ONTAP バージョン」を参照してください。ここで説明する手順では、ソースにオンプレミスの NetApp ONTAP ファイルシステムを使用します。

- オンプレミス (ソース) NetApp ONTAP ファイルシステムには SnapMirror ライセンスが含まれています。
- SVM を使用して ONTAP ファイルシステムの宛先 FSx を作成しましたが、宛先ボリュームを作成していません。詳細については、「FSx for ONTAP ファイルシステムの作成」を参照してください。

手順のコマンドは、次のクラスター、SVM、およびボリュームエイリアスを使用します。

- *FSx-Dest* – 送信先 (FSx) クラスターの ID (F SxIdabcdef1234567890a の形式) 。
- *OnPrem-Source* - 出典クラスターの ID。
- *DestSVM* - 宛先 SVM 名。
- *SourceSVM* - 出典 SVM 名。
- 出典ボリューム名と宛先ボリューム名はどちらも `vol1` です。

> **Note**
>
> FSx for ONTAP ファイルシステムは、すべての ONTAP CLI コマンドでクラスターと呼ばれます。

このセクションの手順では、次の NetApp ONTAP CLI コマンドを使用します。

- [volume create] (ボリュームの作成) コマンド
- [cluster] (クラスター) コマンド
- [vserver peer] (vserver ピア) コマンド
- [snapmirror] (スナップミラー) コマンド

NetApp ONTAP CLI を使用して、FSx for ONTAP ファイルシステム SnapMirror の設定を作成および管理します。詳細については、「NetApp ONTAP CLI の使用」を参照してください。

宛先ボリュームの作成

NetApp ONTAP CLI および REST API に加えて、Amazon FSx コンソールAWS CLI、、および Amazon FSx API を使用して、データ保護 (DP) 送信先ボリュームを作成できます。Amazon FSx コ

ンソールと AWS CLI を使用してターゲットボリュームを作成する方法の詳細については、ボリュームの作成 を参照してください。

次の手順では、 NetApp ONTAP CLI を使用して FSx for ONTAP ファイルシステムに宛先ボリュームを作成します。fsxadmin パスワードと、ファイルシステムの管理ポートの IP アドレスまたは DNS 名が必要です。

1. ユーザー fsxadmin およびファイルシステムを作成したときに設定したパスワードを使用し、宛先ファイルシステムとの SSH セッションを確立します。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 移行元ボリュームのストレージ容量と少なくとも等しいストレージ容量を持つボリュームを移行先クラスター上に作成します。を使用して-type DP、 SnapMirror 関係の送信先として指定します。

   データ階層化を使用する予定の場合は、-tiering-policy を all に設定することをお勧めします。これにより、データがすぐに容量プールストレージに転送され、SSD 階層の容量不足が防止されます。移行後、-tiering-policy を auto に切り替えることができます。

   > **Note**
   >
   > ファイルメタデータは、ボリュームのデータ階層化ポリシーに関係なく、常に SSD ベースのプライマリ層に保存されます。

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

出典と宛先のクラスター間 LIF をレコードします

SnapMirror は、それぞれに一意の IP アドレスを持つクラスター間論理インターフェイス (LIFsを使用して、送信元クラスターと送信先クラスター間のデータ転送を容易にします。

1. ONTAP ファイルシステムのデスティネーション FSx については、ファイルシステムの詳細ページの [Administration] (管理) タブを表示させることによって、Amazon FSx コンソールから [Inter-cluster endpoint - IP addresses] (クラスタ間エンドポイント - IP アドレス) を取得できます。

2. ソース NetApp ONTAP クラスターの場合は、ONTAP CLI を使用してクラスター間 LIF IP アドレスを取得します。次のコマンドを実行します。

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> スケールアウトファイルシステムでは、高可用性 (HA) ペアごとに 2 つのクラスター間 IP アドレスがあります。後で使用するためにこれらの値を保存します。

inter_1 および inter_2 IP アドレスを保存します。これらは、FSx-Dest では dest_inter_1 および dest_inter_2 として、OnPrem-Source では source_inter_1 と source_inter_2 として参照されます。

出典と宛先の間でクラスターピアリングを確立する

クラスター間 IP アドレスを指定して、宛先クラスターでクラスターピア関係を確立します。また、出典クラスターでクラスターピアリングを確立するときに入力する必要があるパスフレーズを作成する必要があります。

1. 次のコマンドを使用して宛先クラスターのピアリングを設定します。スケールアウトファイルシステムでは、クラスター間 IP アドレスをそれぞれ指定する必要があります。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. 次に、出典クラスターでクラスターピア関係を確立します。認証するには、上記で作成したパスフレーズを入力する必要があります。スケールアウトファイルシステムでは、クラスター間 IP アドレスをそれぞれ指定する必要があります。

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. 出典クラスターで次のコマンドを使用して、ピアリングが正常に完了したことを確認します。出力の内容において、Availability は Available に設定される必要があります。

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

SVM ピアリング関係を作成する

クラスターピアリングが確立されると、次のステップは SVM のピアリングです。vserver peer コマンドを使用して、宛先クラスター (FSX-deST) に SVM ピアリング関係を作成します。次のコマンドで使用される追加のエイリアスは次のとおりです。

- DestLocalName - これは、送信元 SVM で SVM ピアリングを設定するときに宛先 SVM を識別するために使用される名前です。
- SourceLocalName - これは、宛先 SVM で SVM ピアリングを設定するときに送信元 SVM を識別するために使用される名前です。

1. 次のコマンドを使用して、送信元 SVM と宛先 SVM の間に SVM ピアリング関係を作成します。

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. 出典クラスターでピアリング関係を受け入れます。

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. 次のコマンドを使用して、SVM ピアリングステータスを確認します。Peer State レスポンスの peered のように設定する必要があります。

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------- ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

SnapMirror 関係を作成する

送信元 SVM と送信先 SVMs をピアリングしたので、次のステップは送信先クラスターで SnapMirror 関係を作成して初期化することです。

> **Note**
>
> SnapMirror リレーションシップを作成して初期化すると、リレーションシップが切断されるまで、送信先ボリュームは読み取り専用になります。

- snapmirror create コマンドを使用して、送信先クラスターで SnapMirror 関係を作成します。snapmirror create コマンドは、宛先 SVM から使用する必要があります。

  オプションで、 -throttleを使用して SnapMirror 関係の最大帯域幅 (kB/秒) を設定できます。

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

FSx for ONTAP ファイルシステムへのデータの転送

SnapMirror 関係を作成したので、送信先ファイルシステムにデータを転送できます。

1. 宛先ファイルシステムで次のコマンドを実行すると、宛先ファイルシステムにデータを転送できます。

   > **Note**
   >
   > このコマンドを実行すると、 はソースボリュームから宛先ボリュームへのデータのスナップショットの転送 SnapMirror を開始します。

   ```
   FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
   path SourceLocalName:vol1
   ```

2. アクティブに使用されているデータを移行する場合は、移行元クラスターとの同期が維持されるように、移行先クラスターを更新する必要があります。宛先クラスターに対して 1 回限りの更新を実行するには、次のコマンドを実行します。

   ```
   FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
   ```

3. 移行を完了してクライアントを FSx for ONTAP に移動する前に、1 時間ごとまたは 1 日ごとの更新をスケジュールすることもできます。`snapmirror modify` コマンドを使用して SnapMirror 更新スケジュールを確立できます。

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Amazon FSx にカットオーバー

FSx for ONTAP ファイルシステムへのカットオーバーの準備を行うには、次の手順を実行します。

- 出典クラスターに書き込むすべてのクライアントを切断します。
- 最終的な SnapMirror 転送を実行して、カットオーバー時にデータが失われないようにします。
- SnapMirror 関係を解除します。
- すべてのクライアントを FSx for ONTAP ファイルシステムに接続します。

1. 出典クラスターからのすべてのデータが FSx for ONTAP ファイルシステムに確実に転送されるようにするには、最後の Snapmirror 転送を実行します。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Mirror State が Snapmirrored に設定され、Relationship Status が Idle に設定されていることを確認することにより、データ移行が完了したことを検証します。また、宛先ボリュームへの最後の転送がいつ行われたかを示すように、Last Transfer End Timestamp 日付が期待どおりであることを確認する必要があります。
3. 次のコマンドを実行して、 SnapMirror ステータスを表示します。

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. snapmirror quiesce コマンドを使用して、今後の SnapMirror 転送を無効にします。

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. snapmirror show を使用して Relationship Status が Quiesced に変更されたことを確認します。

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
Path             Path          State         Status
-----------      ------------  ------------- --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. 移行中、宛先ボリュームは読み取り専用です。読み取り/書き込みを有効にするには、SnapMirror 関係を中断し、FSx for ONTAP ファイルシステムにカットオーバーする必要があります。次のコマンドを使用して SnapMirror 関係を分割します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. SnapMirror レプリケーションが完了し、関係が SnapMirror壊れたら、ボリュームをマウントしてデータを使用可能にすることができます。

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

これで、出典ボリュームからのデータが宛先ボリュームに完全に移行された状態でボリュームが使用可能になります。このボリュームは、クライアントが読み取りおよび書き込みを行うこともできます。このボリュームの `tiering-policy` を `all` に以前に設定した場合、`auto` または `snapshot-only` に変更することが可能で、アクセスパターンに従って、データはストレージ階層間で自動的に移行します。クライアントおよびアプリケーションがこのデータにアクセスできるようにするには、「データへのアクセス」を参照してください。

AWS DataSync を使用した FSx for ONTAP への移行

FSx for ONTAP ファイルシステムと ONTAP 以外のファイルシステム (FSx for Lustre、FSx for OpenZFS、FSx for Windows File Server、Amazon EFS、Amazon S3、オンプレミスファイラーなど) の間でデータを転送するには、AWS DataSync を使用することをお勧めします。FSx for ONTAP と NetApp ONTAP の間でファイルを転送する場合は、 を使用することをお勧めしますNetApp SnapMirror。 AWS DataSyncは、インターネット経由でセルフマネージドストレージシステムとAWS ストレージサービス間のデータの移動とレプリケーションを簡素化、自動化、および高速化するデータ転送サービスですAWS Direct Connect。 DataSync は、所有権、タイムスタンプ、アクセス許可などのファイルシステムデータとメタデータを転送できます。

DataSync を使用して、2 つの FSx for ONTAP ファイルシステム間でファイルを転送したり、別の AWS リージョンまたは AWSアカウントのファイルシステムにデータを移動したりできます。DataSync FSx for ONTAP ファイルシステムで を他のタスクに使用することもできます。例えば、一度限りのデータ移行、配信ワークロード用の定期的なデータ取り込み、およびデータ保護と回復のためのレプリケーションを計画できます。

では DataSync、場所は FSx for ONTAP ファイルシステムのエンドポイントです。特定の転送シナリオに関する詳細は、「AWS DataSync ユーザーガイド」の「Working with locations」 (場所の使用) を参照してください。

> **Note**
>
> `All` 階層化ポリシーを使用してデータをキャパシティプール層に移行することを計画している場合、ファイルメタデータは常に SSD 層に格納され、すべての新しいユーザーデータ

は最初に SSD 層に書き込まれることに注意してください。データが SSD 層に書き込まれると、バックグラウンド階層化プロセスはキャパシティプールストレージへのデータの階層化を開始しますが、階層化プロセスは即時ではなく、ネットワークリソースを消費します。キャパシティプールストレージに階層化する前に、ユーザーデータのバッファとしてファイルメタデータ (ユーザーデータサイズの 3～7%) を考慮して SSD 階層のサイズを設定する必要があります。SSD の使用率が 80% を超えないようにすることをお勧めします。
データの移行中は、CloudWatch ファイルシステムメトリクスを使用して SSD 階層をモニタリングし、階層化プロセスがデータを容量プールストレージに移動できる速度を超えないようにしてください。SSD 階層の使用率が 80% を超えないように、階層化が発生しているレートよりも低いレートへの DataSync 転送を調整することもできます。例えば、スループットキャパシティが 512 MBps 以上のファイルシステムの場合、通常は 200 MBps のスロットリングでデータ転送速度とデータ階層化レートのバランスが取れます。

前提条件

FSx for ONTAP のセットアップにデータを移行するには、要件を満たすサーバーとネットワークが必要です DataSync 。詳細については、「 AWS DataSyncユーザーガイド」の「 の要件 DataSync」を参照してください。

を使用してファイルを移行するための基本的な手順 DataSync

を使用して送信元から送信先へファイルを転送する DataSync には、以下の基本的なステップを実行します。

- ご使用の環境にエージェントをダウンロードしてデプロイし、アクティブ化します (AWS のサービス 間で転送する場合は不要)。
- 送信元と送信先の場所を作成します。
- タスクを作成します。
- タスクを実行して、ソースから宛先にファイルを転送します。

詳細については、『AWS DataSync ユーザーガイド:』の以下のトピックを参照してください。

- 自己管理ストレージと AWS の間のデータ転送
- Amazon FSx for NetApp ONTAP の場所の作成

Amazon FSx for NetApp ONTAP のモニタリング

以下のサービスとツールを使用して、Amazon FSx for NetApp ONTAP の使用状況とアクティビティをモニタリングできます。

- Amazon CloudWatch – Amazon を使用してファイルシステムをモニタリングできます。Amazon は CloudWatch、FSx for ONTAP から raw データを収集して読み取り可能なメトリクスに加工します。これらの統計は 15 か月間保持されるため、履歴情報にアクセスしてファイルシステムのパフォーマンスを確認できます。また、指定した期間のメトリクスに基づいてアラームを設定し、指定したしきい値に関連するメトリクスの値に基づいて 1 つ以上のアクションを実行することもできます。
- ONTAP EMS イベント – お使いの FSx for ONTAP ファイルシステムは、ONTAP の Events Management System (EMS) が生成したイベントを使ってモニタリングできます。EMS イベントは、iSCSI LUN の作成やボリュームの自動サイズ変更など、ファイルシステム内の活動を通知する機能です。
- NetApp Cloud Insights – NetApp Cloud Insights サービスを使用して、FSx for ONTAP ファイルシステムの設定、容量、パフォーマンスメトリクスをモニタリングできます。メトリクス条件に基づいてアラートを作成することもできます。
- NetApp Harvest と NetApp Grafana – NetApp Harvest と NetApp Grafana を使用して FSx for ONTAP ファイルシステムをモニタリングできます。 NetApp Harvest は、FSx for ONTAP ファイルシステムからパフォーマンス、容量、ハードウェアメトリクスを収集することで ONTAP ファイルシステムをモニタリングします。Grafana は、収集された Harvest 指標を表示できるダッシュボードを提供します。
- AWS CloudTrail – を使用して AWS CloudTrail 、Amazon FSx のすべての API コールをイベントとしてキャプチャできます。これらのイベントは、Amazon FSx でユーザー、ロール、または AWS サービスによって実行されたアクションの記録を提供します。

トピック

Amazon によるモニタリング CloudWatch

Amazon FSx for NetApp ONTAP から raw データを収集し CloudWatch、読み取り可能なほぼリアルタイムのメトリクスに処理する Amazon を使用してファイルシステムをモニタリングできます。統計は 15 ヵ月間保持されるため、履歴情報にアクセスしてファイルシステムのパフォーマンスを判断できます。FSx for ONTAP メトリクスデータは、デフォルトで 1 分 CloudWatch 間隔で に自動的に送信されます。の詳細については CloudWatch、「Amazon ユーザーガイド」の「Amazon CloudWatchとは」を参照してください。 CloudWatch

> **Note**
>
> デフォルトでは、FSx for ONTAP は 1 分 CloudWatch 間隔で送信される以下のメトリクスを除き、1 分間隔でメトリクスデータを に送信します。
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch FSx for ONTAP の メトリクスは 4 つのカテゴリに分類され、各メトリクスのクエリに使用されるディメンションによって定義されます。ディメンションの詳細については、「Amazon CloudWatch ユーザーガイド」の「ディメンション」を参照してください。

- ファイルシステムメトリクス： F ile-system-level パフォーマンスとストレージ容量のメトリクス。
- 詳細なファイルシステムメトリクス: ile-system-level ストレージ階層 (SSD と容量プール) あたりの F ストレージメトリクス。
- [ボリュームメトリクス]: ボリュームごとのパフォーマンスおよびストレージ容量のメトリクス。
- [詳細なボリュームメトリクス]: ストレージ階層別またはデータのタイプ (ユーザー、スナップショット、その他) 別ボリュームごとのストレージ容量に関するメトリクス。

FSx for ONTAP のすべての CloudWatch メトリクスは、 `AWS/FSx`の名前空間に発行されます CloudWatch。

トピック

- FSx for ONTAP CloudWatch メトリクスの使用方法
- CloudWatch メトリクスへのアクセス

- ファイルシステムのメトリクス
- スケールアウトファイルシステムのメトリクス
- ボリュームメトリクス
- パフォーマンスの警告と推奨事項
- Amazon FSx をモニタリングする Amazon CloudWatch アラームの作成

FSx for ONTAP CloudWatch メトリクスの使用方法

Amazon FSx によってレポートされる CloudWatch メトリクスは、FSx for ONTAP ファイルシステムとボリュームに関する貴重な情報を提供します。

トピック

- Amazon FSx コンソールでファイルシステムのメトリクスをモニタリングするには
- Amazon FSx コンソールでボリュームメトリクスをモニタリングする

Amazon FSx コンソールでファイルシステムのメトリクスをモニタリングするには

Amazon FSx コンソールのファイルシステムのダッシュボードにある [モニタリングとパフォーマンス] パネルを使用して、以下の表に記載されているメトリクスを表示することができます。詳細については、「CloudWatch メトリクスへのアクセス」を参照してください。

モニタリングとパフォーマンス	方法を教えてください	チャート	関連するメトリクス
[概要]	ファイルシステムで使用可能なストレージ容量を判別するにはどうすればよいですか?	使用可能なプライマリストレージ容量 (バイト)	`StorageCapacity {SSD} - StorageUsed {SSD}`

モニタリングとパフォーマンス	方法を教えてください	チャート	関連するメトリクス
	ファイルシステムの合計スループットはどのように決定すればよいですか?	合計クライアントスループット (バイト/秒)	SUM(DataReadBytes + DataWriteBytes)/PERIOD (秒単位)
	ファイルシステムの合計クライアント IOPS はどのように決定すればよいですか?	合計クライアント IOPS (オペレーション/秒)	SUM(DataReadOperations + DataWriteOperations + MetadataOperations)/PERIOD (秒単位)
	ファイルシステムの読み取り、書き込み、メタデータオペレーションの平均レイテンシーはどのように決定すればよいですか?	平均レイテンシー (ミリ秒/オペレーション)	平均読み取りレイテンシー: DataReadOperationTime * 1000/DataReadOperations 平均書き込みレイテンシー: DataWriteOperationTime * 1000/DataWriteOperations メタデータの平均レイテンシー: MetadataOperationTime * 1000/MetadataOperations

モニタリングとパフォーマンス	方法を教えてください	チャート	関連するメトリクス
[Storage (ストレージ)]	ファイルシステム上の使用済みストレージ容量と空きストレージ容量の配分はどのように決定すればよいですか?	ストレージディストリビューション	利用可能なプライマリ階層: StorageCapacity {SSD} - StorageUsed {SSD} 使用済みプライマリ階層: StorageUsed {SSD} 使用済み容量プール: StorageUsed {StandardCapacityPool }
	ストレージ効率の節約 (圧縮、重複排除、空き領域の活用) はどのように決定すればよいですか?	ストレージ効率の節約	StorageEfficiencySavings
	使用可能なプライマリストレージの容量はどのように決定すればよいですか?	使用可能なプライマリストレージ容量 (バイト)	StorageCapacity {SSD} - StorageUsed {SSD}
	ファイルシステムのプライマリストレージの使用率はどのように決定すればよいですか?	プライマリストレージの容量使用率 (%)	StorageUsed {SSD} * 100/StorageCapacity {SSD}

モニタリングとパフォーマンス	方法を教えてください	チャート	関連するメトリクス
ファイルサーバーのパフォーマンス	ファイルシステムがネットワークスループットの制限に近づいているかどうかを判断するにはどうすればよいですか?	ネットワークスループット – 使用率 (%)	NetworkThroughputUtilization
	ファイルシステムがディスクのスループット制限に近づいているかどうかを判断するにはどうすればよいですか?	ディスクスループット - 使用率 (%)	FileServerDiskThroughputUtilization
	ファイルシステムがディスクスループットの許容バーストクレジット数を使い果たしているかどうかを判断するにはどうすればよいですか?	ディスクスループット - バーストバランス (%)	FileServerDiskThroughputBalance
	ファイルシステムがファイルサーバーの SSD IOPS 制限に近づいているかどうかを判断するにはどうすればよいですか?	ディスク IOPS — 使用率 (%)	FileServerDiskIopsUtilization
	ファイルシステムが、ファイルサーバーのディスク SSD IOPS の許容バーストクレジットを使い果たしているかどうかを判断するにはどうすればよいですか?	ディスク IOPS — バーストバランス (%)	FileServerDiskIopsBalance
	ファイルシステムの CPU の平均使用率はどのように決定すればよいですか?	CPU 使用率 (%)	CPUUtilization

モニタリングとパフォーマンス	方法を教えてください	チャート	関連するメトリクス
	ワークロードがファイルシステムの RAM と NVMe のリードキャッシュを効率的に使用しているかどうかを判断するにはどうすればよいですか?	キャッシュヒット率 (%)	`FileServerCacheHitRatio`
ディスクパフォーマンス	ファイルシステムが現在プロビジョニングされている SSD IOPS 容量に近づいているかどうかを判断するにはどうすればよいですか?	ディスク IOPS - 使用率 (SSD) (%)	`DiskIopsUtilization`

> **Note**
>
> ネットワーク使用率、CPU 使用率、SSD IOPS 使用率など、パフォーマンスに関連するディメンションの平均スループットキャパシティの使用率を 50% 未満に維持することをお勧めします。これにより、ワークロードの予期しないスパイクや、バックグラウンドのストレージオペレーション (ストレージの同期、データ階層化、バックアップなど) に十分な予備のスループットキャパシティを確保することができます。

Amazon FSx コンソールでボリュームメトリクスをモニタリングする

Amazon FSx コンソールのボリュームのダッシュボードにある [モニタリング] パネルを使用して、その他のパフォーマンスメトリクスを表示することができます。詳細については、「CloudWatch メトリクスへのアクセス」を参照してください。

モニタリング	方法を教えてください	チャート	関連するメトリクス
	ボリュームの使用可能なストレージ容量はどのように決定すればよいですか?	使用可能なスト	`StorageCapacity`

モニタリング	方法を教えてください	チャート	関連するメトリクス
		レージ容量	
	ボリュームの合計クライアントスループットはどのように決定すればよいですか?	合計クライアントスループット (バイト/秒)	SUM(DataReadBytes + DataWriteBytes)/PERIOD (秒単位)
	ボリュームのトータルクライアント IOPS はどのように決定すればよいですか?	合計クライアント IOPS (オペレーション/秒)	SUM(DataReadOperations + DataWriteOperations + MetadataOperations)/PERIOD (秒単位)
	容量プール階層から送られてくる読み取り/書き込みオペレーションの数はどのように決定すればよいですか?	容量プールの IOPS (オペレーション数/秒)	読み込みオペレーション: CapacityPoolReadOperations 書き込みオペレーション: CapacityPoolWriteOperations

モニタリング	方法を教えてください	チャート	関連するメトリクス
	ボリュームの読み取り、書き込み、メタデータオペレーションの平均レイテンシーはどのように決定すればよいですか?	平均レイテンシー (ミリ秒/オペレーション)	平均読み取りレイテンシー: `DataReadOperationTime * 1000/DataReadOperations` 平均書き込みレイテンシー: `DataWriteOperationTime * 1000/DataWriteOperations` メタデータの平均レイテンシー: `MetadataOperationTime * 1000/MetadataOperations`
	ボリュームで使用できるファイルまたは inode の量はどのように決定すればよいですか?	使用可能なファイル (inode)	`FilesCapacity - FilesUsed`
	ボリュームの使用済みストレージキャパシティと空きストレージ容量の配分はどのように決定すればよいですか?	ストレージディストリビューション	`StorageCapacity - StorageUsed`

CloudWatch メトリクスへのアクセス

Amazon FSx の Amazon CloudWatch メトリクスは、次の方法で確認できます。

- Amazon FSx コンソール
- Amazon CloudWatch コンソール
- の AWS Command Line Interface （ AWS CLI ） CloudWatch
- CloudWatch API

次の手順では、Amazon FSx コンソールでファイルシステムの CloudWatch メトリクスを表示する方法について説明します。

Amazon FSx コンソールを使用してファイルシステムの CloudWatch メトリクスを表示するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーションペインで、[File systems] (ファイルシステム) を選択してから、メトリクスを表示するファイルシステムを選択します。
3. [概要] ページで、2 番目のパネルから [モニタリングとパフォーマンス] を選択して、ファイルシステムのメトリクスのグラフを表示します。

[モニタリングとパフォーマンス] パネルには 4 つのタブがあります。

- 概要 (デフォルトタブ) を選択すると、ファイルシステムアクティビティ のアクティブな警告、CloudWatch アラーム、グラフが表示されます。
- [Storage] (ストレージ) を選択して、ストレージ容量および使用率のメトリクスを表示します。
- [パフォーマンス] には、ファイルサーバーとストレージのパフォーマンスメトリクスが表示されます。
- CloudWatch アラームを選択すると、ファイルシステムに設定されたアラームのグラフが表示されます。

次の手順では、Amazon FSx コンソールでボリュームの CloudWatch メトリクスを表示する方法について説明します。

Amazon FSx コンソールを使用してボリュームの CloudWatch メトリクスを表示するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. ナビゲーションペインで、[ボリューム] をクリックし、メトリクスを表示するボリュームを選択します。
3. [概要] ページで、2 番目のパネルから [モニタリング] (デフォルトタブ) を選択して、ボリュームのメトリクスのグラフを表示します。

次の手順では、Amazon CloudWatch コンソールでファイルシステムの CloudWatch メトリクスを表示する方法について説明します。

Amazon CloudWatch コンソールを使用してメトリクスを表示するには

1. ファイルシステムの [概要] ページで、2 番目のパネルから [モニタリングとパフォーマンス] を選択して、ファイルシステムのメトリクスのグラフを表示します。
2. Amazon コンソールで表示するグラフの右上にあるアクションメニューからメトリクスの表示を選択します。 CloudWatch Amazon CloudWatch コンソールでメトリクスページが開きます。

次の手順では、FSx for ONTAP ファイルシステムメトリクスを Amazon CloudWatch コンソールのダッシュボードに追加する方法について説明します。

Amazon CloudWatch コンソールにメトリクスを追加するには

1. Amazon FSx コンソールの [モニタリングとパフォーマンス] パネルでメトリクスのセット ([概要]、[ストレージ]、[パフォーマンス]) のいずれかを選択します。
2. パネルの右上にある [ダッシュボードに追加] をクリックします。これにより、Amazon CloudWatch コンソールが開きます。
3. リストから既存の CloudWatch ダッシュボードを選択するか、新しいダッシュボードを作成します。詳細については、「Amazon ユーザーガイド」の「Amazon CloudWatch ダッシュボードの使用」を参照してください。 CloudWatch

以下の手順では、 AWS CLIを使用してファイルシステムのメトリクスにアクセスする方法を説明します。

からメトリクスにアクセスするには AWS CLI

- `--namespace "AWS/FSx"` パラメータを指定して CloudWatch list-metrics CLI コマンドを使用します。詳細については、『AWS CLI コマンドリファレンス』を参照してください。

次の手順では、 CloudWatch API を使用してファイルシステムのメトリクスにアクセスする方法について説明します。

CloudWatch API からメトリクスにアクセスするには

- GetMetric統計 API オペレーションを呼び出します。詳細については、「Amazon CloudWatch API リファレンス」を参照してください。

ファイルシステムのメトリクス

Amazon FSx for NetApp ONTAP ファイルシステムメトリクスは、ファイルシステムメトリクス または詳細なファイルシステムメトリクス のいずれかに分類されます。

- [File system metrics] (ファイルシステムのメトリクス) は、単一のディメンション `FileSystemId` を使用する単一のファイルシステムのパフォーマンスとストレージのメトリクスを集約したものです。メトリクスは、ファイルシステムのネットワークパフォーマンスとストレージ容量の使用状況を測定します。
- [Detailed File System Metrics] (詳細なファイルシステムメトリクス) は、ファイルシステムのストレージ容量と各ストレージ階層で使用されているストレージ (SSD ストレージや容量プールストレージなど) を測定します。各メトリクスには、`FileSystemId`、`StorageTier`、および `DataType` ディメンションが含まれます。

Amazon FSx がこれらのメトリクスのデータポイントを に発行するタイミングについては、次の点に注意してください CloudWatch。

- 使用率メトリクス (名前が Utilization で終わる `NetworkThroughputUtilization` などのメトリクス) の場合、アクティブなファイルサーバーまたはアグリゲートごとに各期間で 1 つのデータポイントが出力されます。たとえば Amazon FSx では `FileServerDiskIopsUtilization` の場合、アクティブなファイルサーバーごとに 1 分間隔、`DiskIopsUtilization` の場合アグリゲートごとに 1 分間隔でメトリクスが出力されます。
- その他のすべてのメトリクスの場合、アクティブなファイルサーバー (ファイルサーバーメトリクスの `DataReadBytes` など)、またはアグリゲート (ストレージメトリクスの `DiskReadBytes` など) のすべてにおけるメトリクスの合計値に対応する、各期間で 1 つのデータポイントが出力されます。

トピック

ネットワーク I/O メトリクス

メトリクスはすべて、FileSystemId という 1 つのディメンションを取ります。

メトリクス	説明
NetworkThroughputUtilization	ファイルシステムのネットワークスループット使用率 (%)。 Average 統計は、指定した期間におけるファイルシステムのネットワークスループットの平均使用率です。 Minimum 統計は、指定した期間におけるファイルシステムのネットワークスループットの最小使用率です。 Maximum 統計は、指定した期間におけるファイルシステムのネットワークスループットの最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum
NetworkSentBytes	ファイルシステムから送信されたバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間にファイルシステムから送信されたバイト数の合計です。 統計の送信スループット (バイト/秒) を算出するには、統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum

メトリクス	説明
NetworkReceivedBytes	ファイルシステムが受信したバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間にファイルシステムが受信したバイト数の合計です。 統計の受信スループット (バイト/秒) を算出するには、統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
DataReadBytes	クライアントによる読み取りからファイルシステムへのバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間に読み取りオペレーションと関連付けられているバイト数の合計です。指定した期間の平均スループット (バイト/秒) を算出するには、Sum 統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum

メトリクス	説明
DataWriteBytes	クライアントによるファイルシステムへの書き込みからのバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間に書き込みオペレーションと関連付けられているバイト数の合計です。指定した期間の平均スループット (バイト/秒) を算出するには、Sum 統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum
DataReadOperations	クライアントによる読み取りからファイルシステムへの読み取り操作 (ネットワーク I/O) の数。 Sum 統計は、指定した期間に発生した I/O オペレーションの合計数です。指定した期間の 1 秒あたりの平均読み取りオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum

メトリクス	説明
DataWriteOperations	クライアントによるファイルシステムへの書き込みからの書き込みオペレーション (ネットワーク I/O) の数。 Sum 統計は、指定した期間に発生した I/O オペレーションの合計数です。指定した期間の 1 秒あたりの平均書き込みオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum
MetadataOperations	クライアントによるファイルシステムへのメタデータオペレーション (ネットワーク I/O) の数。 Sum 統計は、指定した期間に発生した I/O オペレーションの合計数です。指定した期間の 1 秒あたりの平均メタデータオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum

メトリクス	説明
DataReadOperationTime	ファイルシステム内のデータにアクセスするクライアントからの読み取りオペレーション (ネットワーク I/O) を実行するためにファイルシステム内で費やされた合計時間。 Sum 統計は、指定した期間に読み取りオペレーションに費やされた合計秒数です。ある期間の平均読み取りレイテンシーを計算するには、Sum 統計を同じ期間の DataReadOperations メトリクスの Sum で割ります。 単位: 秒 有効な統計: Sum
DataWriteOperationTime	ファイルシステム内のデータにアクセスするクライアントからの書き込みオペレーション (ネットワーク I/O) を実行するためにファイルシステム内で費やされた合計時間。 Sum 統計は、指定した期間に書き込みオペレーションに費やされた合計秒数です。ある期間の平均書き込みレイテンシーを計算するには、Sum 統計を同じ期間の DataWriteOperations メトリクスの Sum で割ります。 単位: 秒 有効な統計: Sum

メトリクス	説明
CapacityPoolReadBytes	ファイルシステムの容量プール階層から読み取られた (ネットワーク I/O) バイト数。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間にファイルシステムの容量プール階層から読み取られたバイト数の合計です。1 秒あたりの容量プールのバイト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
CapacityPoolReadOperations	ファイルシステムの容量プール階層における読み取りオペレーション (ネットワーク I/O) の数。この数は、容量プールの読み取りリクエストに変換されます。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間におけるファイルシステムの容量プール階層における読み取りオペレーションの合計数です。1 秒あたりの容量プールのリクエスト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: カウント 有効な統計: Sum

メトリクス	説明
CapacityPoolWriteBytes	ファイルシステムの容量プール階層に書き込まれた (ネットワーク I/O) バイト数。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間にファイルシステムの容量プール階層に書き込まれたバイト数の合計です。1 秒あたりの容量プールのバイト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
CapacityPoolWriteOperations	容量プール階層からファイルシステムへの書き込みオペレーション (ネットワーク I/O) の数。この数は、書き込みリクエストに変換されます。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間におけるファイルシステムの容量プール階層への書き込みオペレーションの合計数です。1 秒あたりの容量プールのリクエスト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: カウント 有効な統計: Sum

ファイルサーバーのメトリクス

メトリクスはすべて、FileSystemId という 1 つのディメンションを取ります。

メトリクス	説明
CPUUtilization	ファイルシステムの CPU リソースの使用率 (%)。 Average 統計は、指定した期間におけるファイルシステムの平均 CPU 使用率です。 Minimum 統計は、指定した期間におけるファイルシステムの最小 CPU 使用率です。 Maximum 統計は、指定した期間におけるファイルシステムの最大 CPU 使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum
FileServerDiskThroughputUtilization	ファイルサーバーとプライマリ階層間のディスクスループットを、スループットキャパシティによって決定されるプロビジョニング制限に対する割合 (%) で表したものです。 Average 統計は、指定した期間におけるファイルサーバーのディスクスループットの平均使用率です。 Minimum 統計は、指定した期間におけるファイルサーバーのディスクスループットの最小使用率です。 Maximum 統計は、指定した期間におけるファイルサーバーのディスクスループットの最大使用率です。 単位: パーセント

メトリクス	説明
	有効な統計: Average、Minimum、Maximum
FileServerDiskThroughputBalance	ファイルサーバーとプライマリ階層間のディスクスループットに使用できるバーストクレジットの割合 (%)。これは、512 MBps 以下のスループットキャパシティでプロビジョニングされたファイルシステムに対して有効です。 Average 統計は、指定した期間に利用可能な平均バーストバランスです。 Minimum 統計は、指定した期間に利用可能な最小バーストバランスです。 Maximum 統計は、指定した期間に利用可能な最大バーストバランスです。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
FileServerDiskIopsBalance	ファイルサーバーとプライマリ階層間のディスク IOPS に使用できるバーストクレジットの割合 (%)。これは、512 MBps 以下のスループットキャパシティでプロビジョニングされたファイルシステムに対して有効です。 Average 統計は、指定した期間に利用可能な平均バーストバランスです。 Minimum 統計は、指定した期間に利用可能な最小バーストバランスです。 Maximum 統計は、指定した期間に利用可能な最大バーストバランスです。 単位: パーセント 有効な統計: Average、Minimum、Maximum
FileServerDiskIopsUtilization	ファイルサーバーの使用可能なディスク IOPS 容量の IOPS 使用率。 Average 統計は、指定した期間におけるファイルシステムのディスク IOPS の平均使用率です。 Minimum 統計は、指定した期間におけるファイルシステムのディスク IOPS の最小使用率です。 Maximum 統計は、指定した期間におけるファイルシステムのディスク IOPS の最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
FileServerCacheHitRatio	ファイルシステムの RAM と NVMe キャッシュ内のデータによって処理されたすべての読み取りリクエストの割合。パーセンテージが高いほど、ファイルシステムのリードキャッシュによって多くの読み取りが処理されることを意味します。 単位: パーセント Average 統計は、指定した期間におけるファイルシステムの平均キャッシュヒット率です。 Minimum 統計は、指定した期間におけるファイルシステムの最小キャッシュヒット率です。 Maximum 統計は、指定した期間におけるファイルシステムの最大キャッシュヒット率です。 有効な統計: Average、Minimum、Maximum

ディスク I/O メトリクス

メトリクスはすべて、FileSystemId という 1 つのディメンションを取ります。

メトリクス	説明
DiskReadBytes	ディスクからファイルシステムのプライマリ階層に読み込まれるバイト数 (ディスク I/O)。 Sum 統計は、指定した期間にファイルシステムから読み取られたバイト数の合計です。 統計のディスク読み取りスループット (バイト/秒) を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト

メトリクス	説明
	有効な統計: Sum
DiskWriteBytes	ディスクからファイルシステムのプライマリ階層に書き込まれたバイト数 (ディスク I/O)。 Sum 統計は、指定した期間にファイルシステムから書き込まれたバイト数の合計です。 統計のディスク書き込みスループット (バイト/秒) を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
DiskIopsUtilization	ファイルサーバーとストレージボリューム間のディスク IOPS を、プライマリ階層のプロビジョニングされたディスク IOPS 制限に対する割合 (%) で表したものです。 Average 統計は、指定した期間におけるファイルシステムのディスク IOPS の平均使用率です。 Minimum 統計は、指定した期間におけるファイルシステムのディスク IOPS の最小使用率です。 Maximum 統計は、指定した期間におけるファイルシステムのディスク IOPS の最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
DiskReadOperations	ファイルシステムのプライマリ階層における読み取りオペレーション (ディスク I/O) の数。 Sum 統計は、指定した期間におけるプライマリ階層の読み取りオペレーションの合計数です。 単位: カウント 有効な統計: Sum
DiskWriteOperations	ファイルシステムのプライマリ階層に対する書き込みオペレーション (ディスク I/O) の数。 Sum 統計は、指定した期間におけるプライマリ階層への書き込みオペレーションの合計数です。 単位: カウント 有効な統計: Sum

ストレージ容量のメトリクス

メトリクスはすべて、FileSystemId という 1 つのディメンションを取ります。

メトリクス	説明
StorageEfficiencySavings	ストレージ効率化機能 (圧縮、重複排除、空き領域の活用) によって節約されたバイト数。 Average 統計は、指定した期間におけるストレージ効率の平均節約率です。1 分間に保存された全データに対するストレージ効率の節約を算出するには、StorageUsed の Sum 統計を使用して、StorageEfficiencySavings を StorageEfficiencySavings と

メトリクス	説明
	StorageUsed ファイルシステムメトリクスの合計で割ります。 Minimum 統計は、指定した期間におけるストレージ効率の最小節約率です。 Maximum 統計は、指定した期間におけるストレージ効率の最大節約率です。 単位: バイト 有効な統計: Average、Minimum、Maximum
StorageUsed	プライマリ (SSD) 層と容量プール層の両方で、ファイルシステムに保存されている物理データの合計量。このメトリクスには、データ圧縮や重複排除などのストレージ効率機能による節約が含まれます。 単位: バイト 有効な統計: Average、Minimum、Maximum

メトリクス	説明
LogicalDataStored	SSD 層とキャパシティプール層の両方を考慮した、ファイルシステムに保存されている論理データの合計量。このメトリクスには、スナップショットと の合計論理サイズが含まれますが FlexClones、圧縮、圧縮、重複排除によって達成されるストレージ効率の節約は含まれません。 ストレージ効率の節約をバイト単位でコンピューティングするには、特定の期間の StorageUsed の Average を取得し、同じ期間の LogicalDataStored の Average から減算します。 合計論理的なデータサイズのパーセンテージとしてストレージ効率の節約をコンピューティングするには、特定の期間の StorageUsed の Average を取得し、同じ期間の LogicalDataStored の Average から減算します。次に、同じ期間の LogicalDataStored の Average で差を割ります。 単位: バイト 有効な統計: Average、Minimum、Maximum

詳細なファイルシステムメトリクス

詳細なファイルシステムメトリクスは、各ストレージ層の詳細なストレージ使用率メトリクスです。詳細なファイルシステムメトリクスはすべて、FileSystemId、StorageTier、および DataType のディメンションを持っています。

- StorageTier ディメンションは、メトリクスが測定するストレージ階層を示し、SSD と StandardCapacityPool の可能な値を示します。

- DataType ディメンションは、メトリクスが測定するデータのタイプを、可能な値 All で示します。

特定のメトリクスとディメンションのキーバリューのペアの一意の組み合わせごとに行があり、その組み合わせが何を測定するかが説明されています。

メトリクス	説明
StorageCapacityUtilization	ファイルシステムのアグリゲートごとのストレージ容量の使用率。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間でのファイルシステムのパフォーマンス階層におけるストレージ容量の平均使用量です。 Minimum 統計は、指定した期間でのファイルシステムのパフォーマンス階層におけるストレージ容量の最小使用量です。 Maximum 統計は、指定した期間でのファイルシステムのパフォーマンス階層におけるストレージ容量の最大使用量です。 単位: パーセント 有効な統計: Average、Minimum、Maximum
StorageCapacity	プライマリ (SSD) 層の合計ストレージ容量。 単位: バイト 有効な統計: Maximum
StorageUsed	ストレージ層に固有の、使用済みの物理ストレージ容量 (バイト単位) 。この値には、データ圧縮や重複排除などのストレージ効率機能による節約が含まれます。StorageTier の有

メトリクス	説明
	効なディメンション値は SSD と StandardCapacityPool で、このメトリクスが測定するストレージ階層に対応します。このメトリクスには、値 All の DataType ディメンションも必要です。 Average、Minimum、および Maximum 統計は、特定の期間における層ごとのストレージ消費量 (バイト単位) です。 プライマリ (SSD) ストレージ階層のストレージ容量使用率を算出するには、StorageTier ディメンションを SSD と等しくして、統計のいずれかを同じ期間の Maximum StorageCapacity で割ります。 プライマリ (SSD) ストレージ層の空きストレージ容量をバイト単位で計算するには、同じ期間の Maximum StorageCapacity から統計のいずれかを除外し、ディメンション StorageTier を SSD に等しくします。 単位: バイト 有効な統計: Average、Minimum、Maximum

スケールアウトファイルシステムのメトリクス

次のメトリクスは、2 つ以上の高可用性 (HA) ペアを持つ ONTAP ファイルシステムの FSx 用に提供されています。これらのメトリクスでは、HA ペアごと、およびアグリゲートごと (ストレージ使用率メトリクス用) にデータポイントが出力されます。

> **Note**
>
> 複数の HA ペアを含むファイルシステムがある場合は、単一の HA ペアのファイルシステムメトリクスおよびボリュームメトリクスを使用することもできます。

トピック

ネットワーク I/O メトリクス

メトリクスはすべて、FileSystemId と FileServer の 2 つのディメンションを取ります。

- FileSystemId – ファイルシステムの AWS リソース ID。
- FileServer — ONTAP 内のファイルサーバー (またはノード) の名前 (FsxId01234567890abcdef-01 など)。奇数番号のファイルサーバーは、ファイルシステムがセカンダリファイルサーバーにフェイルオーバーされていない限りトラフィックを処理する優先ファイルサーバーです。偶数番号のファイルサーバーは、パートナーが使用できない場合にのみトラフィックを処理するセカンダリファイルサーバーです。このため、通常、セカンダリファイルサーバーは優先ファイルサーバーよりも使用率が低くなります。

メトリクス	説明
NetworkThroughputUtilization	ファイルシステムで利用可能なネットワークスループットの割合で表される、ネットワークスループットの使用率です。このメトリクスは、ファイルシステムにおける 1 つの HA ペアのネットワークスループットキャパシティの割合で表される、NetworkSentBytes および NetworkReceivedBytes の最大値に相当します。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。

メトリクス	説明
	Average 統計は、指定した期間での特定のファイルサーバーにおけるネットワークスループットの平均使用率です。 Minimum 統計は、指定した期間での 1 分間の特定のファイルサーバーにおけるネットワークスループットの最小使用率です。 Maximum 統計は、指定した期間での 1 分間の特定のファイルサーバーにおけるネットワークスループットの最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
NetworkSentBytes	ファイルシステムから送信されたバイト数 (ネットワーク IO)。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間に特定のファイルサーバーからネットワーク経由で送信されたバイト数の合計です。 Average 統計は、指定した期間に特定のファイルサーバーからネットワーク経由で送信されたバイト数の平均です。 Minimum 統計は、指定した期間に特定のファイルサーバーからネットワーク経由で送信された最小のバイト数です。 Maximum 統計は、指定した期間に特定のファイルサーバーからネットワーク経由で送信された最大のバイト数です。 統計の送信スループット (バイト/秒) を算出するには、統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum、Average、Minimum、Maximum

メトリクス	説明
NetworkReceivedBytes	ファイルシステムにより受信されたバイト数 (ネットワーク IO)。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間にネットワーク経由で特定のファイルサーバーによって受信されたバイト数の合計です。 Average 統計は、指定した期間に 1 分間でネットワークを通じて、特定のファイルサーバーによって受信されたバイト数の平均です。 Minimum 統計は、指定した期間に 1 分間でネットワークを通じて、特定のファイルサーバーによって受信された最小のバイト数です。 Maximum 統計は、指定した期間に 1 分間でネットワークを通じて、特定のファイルサーバーによって受信された最大のバイト数です。 統計の受信スループット (バイト/秒) を算出するには、統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum、Average、Minimum、Maximum

ファイルサーバーのメトリクス

メトリクスはすべて、FileSystemId と FileServer の 2 つのディメンションを取ります。

メトリクス	説明
CPUUtilization	ファイルシステムの CPU リソースの使用率 (%)。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間におけるファイルシステムの平均 CPU 使用率です。 Minimum 統計は、指定した期間における特定のファイルサーバーの最小 CPU 使用率です。 Maximum 統計は、指定した期間における特定のファイルサーバーの最大 CPU 使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum
FileServerDiskThroughputUtilization	スループットキャパシティによって決定されるプロビジョニング制限に対する割合 (%) で表される、ファイルサーバーとアグリゲート間のディスクスループットです。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。このメトリクスは、ファイルシステムにおける 1 つの HA ペアのファイルサーバーのディスクスループットキャパシティの割合で表される、DiskReadBytes および DiskWriteBytes の合計に相当します。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間における特定のファイルサーバーでのファイルサーバーディスクスループットの平均使用率です。

メトリクス	説明
	Minimum 統計は、指定した期間における特定のファイルサーバーでのファイルサーバーディスクスループットの最小使用率です。 Maximum 統計は、指定した期間における特定のファイルサーバーでのファイルサーバーディスクスループットの最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
FileServerDiskIopsUtilization	ディスク IOPS 制限に対する割合で表される、ファイルサーバーにおける使用可能なディスク IOPS 容量の IOPS 使用率です。これは、プロビジョニングされたディスク IOPS とは対照的に、ディスク IOPS の使用率がファイルサーバーの処理できる最大値を超えているという点で DiskIopsUtilization とは異なります。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間における特定のファイルサーバーでのディスク IOPS の平均使用率です。 Minimum 統計は、指定した期間における特定のファイルサーバーでのディスク IOPS の最小使用率です。 Maximum 統計は、指定した期間における特定のファイルサーバーでのディスク IOPS の最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
FileServerCacheHitRatio	各 HA ペア (HA ペア内のアクティブなファイルサーバーなど) のファイルシステムの RAM または NVMe キャッシュにあるデータによって処理されるすべての読み取りリクエストの割合です。割合が高いほど、読み取りの合計数に対するキャッシュ読み取りの比率が高くなります。バックグラウンドタスク (、階層化 SnapMirror、バックアップなど) を含むすべての I/O が考慮されます。ファイルシステムのファイルサーバーごと、1 分間で 1 つのメトリクスが出力されます。 単位: パーセント Average 統計は、指定した期間におけるファイルシステムのいずれかの HA ペアでの平均キャッシュヒット率です。 Minimum 統計は、指定した期間におけるファイルシステムのいずれかの HA ペアでの最小キャッシュヒット率です。 Maximum 統計は、指定した期間におけるファイルシステムのいずれかの HA ペアでの最大キャッシュヒット率です。 有効な統計: Average、Minimum、Maximum

ディスク I/O メトリクス

メトリクスはすべて、FileSystemId と Aggregate の 2 つのディメンションを取ります。

- FileSystemId – ファイルシステムの AWS リソース ID。
- Aggregate — ファイルシステムのパフォーマンス階層は、アグリゲートと呼ばれる複数のストレージプールで構成されています。HA ペアごとに 1 つのアグリゲートがあります。たとえば、アグリゲート aggr1 は HA ペアのファイルサーバー FsxId01234567890abcdef-01 (アクティブ

なファイルサーバー) およびファイルサーバー FsxId01234567890abcdef-02 (セカンダリファイルサーバー) にマッピングされます。

メトリクス	説明
DiskReadBytes	このアグリゲートから読み取られた任意のディスクのバイト数 (ディスク IO)。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間に 1 分間で特定のアグリゲートから読み込まれたバイト数の合計です。 Average 統計は、指定した期間に 1 分間で特定のアグリゲートから読み込まれたバイト数の平均です。 Minimum 統計は、指定した期間に 1 分間で特定のアグリゲートから読み込まれた最小のバイト数です。 Maximum 統計は、指定した期間に 1 分間で特定のアグリゲートから読み込まれた最大のバイト数です。 統計のディスク読み取りスループット (バイト/秒) を算出するには、統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum、Average、Minimum、Maximum

メトリクス	説明
DiskWriteBytes	このアグリゲートに書き込まれた任意のディスクのバイト数 (ディスク IO)。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間に特定のアグリゲートに書き込まれたバイト数の合計です。 Average 統計は、指定した期間に 1 分間で特定のアグリゲートに書き込まれたバイト数の平均です。 Minimum 統計は、指定した期間に 1 分間で特定のアグリゲートに書き込まれた最小のバイト数です。 Maximum 統計は、指定した期間に 1 分間で特定のアグリゲートに書き込まれた最大のバイト数です。 統計のディスク書き込みスループット (バイト/秒) を算出するには、 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum、Average、Minimum、Maximum

メトリクス	説明
DiskIopsUtilization	アグリゲートのディスク IOPS 制限に対する割合で表される、1 つのアグリゲートのディスク IOPS 使用率です。これは、ファイルシステムの合計 IOPS をファイルシステムにおける HA ペアの数で割った値です。これは、ファイルサーバーでサポートされる最大ディスク IOPS (つまり、HA ペアごとに設定されたスループット容量によって決まる) とは対照的に、プロビジョンド IOPS 制限に対するプロビジョンドディスク IOPS の使用率であるFileServerDiskIopsUtilization 点で とは異なります。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間における特定のアグリゲートでのディスク IOPS の平均使用率です。 Minimum 統計は、指定した期間における特定のアグリゲートでのディスク IOPS の最小使用率です。 Maximum 統計は、指定した期間における特定のアグリゲートでのディスク IOPS の最大使用率です。 単位: パーセント 有効な統計: Average、Minimum、Maximum

メトリクス	説明
DiskReadOperations	このアグリゲートへの読み取りオペレーション (ディスク IO) の数。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間で特定のアグリゲートにより実行された読み取りオペレーションの合計数です。 Average 統計は、指定した期間に 1 分間で特定のアグリゲートにより実行された読み取りオペレーションの平均数です。 Minimum 統計は、指定した期間に 1 分間で特定のアグリゲートにより実行された読み取りオペレーションの最小数です。 Maximum 統計は、指定した期間に 1 分間で特定のアグリゲートにより実行された読み取りオペレーションの最大数です。 その期間におけるディスク IOPS の平均を計算するには、Average 統計を使用してその結果を 60 (秒) で割ります。 単位: カウント 有効な統計: Sum、Average、Minimum、Maximum

メトリクス	説明
DiskWriteOperations	このアグリゲートへの書き込みオペレーション (ディスク IO) の数。バックグラウンドタスク (、階層化、バックアップなど) SnapMirrorを含むすべてのトラフィックがこのメトリクスで考慮されます。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Sum 統計は、指定した期間で特定のアグリゲートにより実行された書き込みオペレーションの合計数です。 Average 統計は、指定した期間に 1 分間で特定のアグリゲートにより実行された書き込みオペレーションの平均数です。 その期間におけるディスク IOPS の平均を計算するには、Average 統計を使用してその結果を 60 (秒) で割ります。 単位: カウント 有効な統計: Sum および Average

詳細なファイルシステムメトリクス

詳細なファイルシステムメトリクスは、各ストレージ層の詳細なストレージ使用率メトリクスです。詳細なファイルシステムメトリクスには、FileSystemId、StorageTier、DataType ディメンション、または、FileSystemId、StorageTier、DataType、Aggregate ディメンションがあります。

- Aggregate ディメンションが指定されていない場合、メトリクスはファイルシステム全体のものです。StorageUsed および StorageCapacity メトリクスには、ファイルシステムの総消費ストレージ (ストレージ階層ごと) および合計ストレージ容量 (SSD 階層の場合) に対応する、1 分間で 1 つのデータポイントが存在します。一方 StorageCapacityUtilization メトリクスでは、アグリゲートごとに 1 分間で 1 つのメトリクスが発行されます。

- Aggregate ディメンションを指定すると、メトリクスはアグリゲートごとのものになります。

ディメンションの説明は次のとおりです。

- FileSystemId – ファイルシステムの AWS リソース ID。
- Aggregate — ファイルシステムのパフォーマンス階層は、アグリゲートと呼ばれる複数のストレージプールで構成されています。HA ペアごとに 1 つのアグリゲートがあります。たとえば、アグリゲート aggr1 は HA ペアのファイルサーバー FsxId01234567890abcdef-01 (アクティブなファイルサーバー) およびファイルサーバー FsxId01234567890abcdef-02 (セカンダリファイルサーバー) にマッピングされます。
- StorageTier — メトリクスが測定するストレージ階層を示し、SSD と StandardCapacityPool の可能な値を示します。
- DataType — メトリクスが測定するデータのタイプを可能な値 All で示します。

特定のメトリクスとディメンションのキーバリューのペアの一意の組み合わせごとに行があり、その組み合わせが何を測定するかが説明されています。

メトリクス	説明
StorageCapacityUtilization	特定のファイルシステムのアグリゲートにおけるストレージ容量の使用率。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間における特定のアグリゲートでのストレージ容量の平均使用量です。 Minimum 統計は、指定した期間における特定のアグリゲートでのストレージ容量の最小使用量です。 Maximum 統計は、指定した期間における特定のアグリゲートでのストレージ容量の最大使用量です。 単位: パーセント

メトリクス	説明
	有効な統計: Average、Minimum、Maximum
StorageCapacity	特定のファイルシステムアグリゲートにおけるストレージ容量。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定した期間における特定のアグリゲートでの平均のストレージ容量です。 Minimum 統計は、指定した期間における特定のアグリゲートでの最小のストレージ容量です。 Maximum 統計は、指定した期間における特定のアグリゲートでの最大のストレージ容量です。 単位: バイト 有効な統計: Average、Minimum、Maximum

メトリクス	説明
StorageUsed	ストレージ層に固有の、使用済みの物理ストレージ容量 (バイト単位) 。この値には、データ圧縮や重複排除などのストレージ効率機能による節約が含まれます。StorageTier の有効なディメンション値は SSD と StandardCapacityPool で、このメトリクスが測定するストレージ階層に対応します。ファイルシステムのアグリゲートごと、1 分間で 1 つのメトリクスが出力されます。 Average 統計は、指定された期間で特定のアグリゲートが特定のストレージ階層で消費した平均の物理ストレージ容量です。 Minimum 統計は、指定された期間で特定のアグリゲートが特定のストレージ階層で消費した最小の物理ストレージ容量です。 Maximum 統計は、指定された期間で特定のアグリゲートが特定のストレージ階層で消費した最大の物理ストレージ容量です。 単位: バイト 有効な統計: Average、Minimum、Maximum

ボリュームメトリクス

Amazon FSx for NetApp ONTAP ファイルシステムには、データを保存する 1 つ以上のボリュームを含めることができます。ボリュームにはそれぞれ、[Volume metrics] (ボリュームメトリクス) または詳細ボリュームメトリクス のいずれかに分類される一連のメトリクスがあります。

- [Volume metrics] (ボリュームメトリクス) は、ボリュームごとのパフォーマンスとストレージのメトリクスであり、FileSystemId と VolumeId の 2 つのディメンションを取ります。FileSystemId は、ボリュームが属するファイルシステムにマッピングされます。

- 詳細なボリュームメトリクスは、StorageTierディメンション (SSDおよび の値が可能StandardCapacityPool) を持つ階層ごと、およびDataTypeディメンション (User、、の値が可能) を持つデータ型ごとにストレージ消費量を測定する per-storage-tier メトリクスSnapshotですOther。メトリクスには、FileSystemId、VolumeId、StorageTier、および DataType のディメンションがあります。

トピック

ネットワーク I/O メトリクス

メトリクスはすべて、FileSystemId と VolumeId の 2 つのディメンションを取ります。

メトリクス	説明
DataReadBytes	クライアントがボリュームから読み取ったバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間に読み取りオペレーションと関連付けられているバイト数の合計です。指定した期間の平均スループット (バイト/秒) を算出するには、Sum 統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum
DataWriteBytes	クライアントがボリュームに書き込んだバイト数 (ネットワーク I/O)。 Sum 統計は、指定した期間に書き込みオペレーションと関連付けられているバイト数の合計です。指定した期間の平均スループット (バイト/

メトリクス	説明
	秒) を算出するには、Sum 統計をその期間の秒数で割ります。 単位: バイト 有効な統計: Sum
DataReadOperations	クライアントによるボリュームでの読み取りオペレーション (ネットワーク I/O) の数。 Sum 統計は、指定した期間の読み取りオペレーションの合計数です。指定した期間の 1 秒あたりの平均読み取りオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum
DataWriteOperations	クライアントによるボリュームでの書き込みオペレーション (ネットワーク I/O) の数。 Sum 統計は、指定した期間の書き込みオペレーションの合計数です。指定した期間の 1 秒あたりの平均書き込みオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum

メトリクス	説明
MetadataOperations	クライアントによるメタデータアクティビティからボリュームへの I/O オペレーション (ネットワーク I/O) の数。 Sum 統計は、指定した期間のメタデータオペレーションの合計数です。指定した期間の 1 秒あたりの平均メタデータオペレーション数を算出するには、Sum 統計をその期間の秒数で割ります。 単位: カウント 有効な統計: Sum
DataReadOperationTime	ボリューム内のデータにアクセスするクライアントからの読み取りオペレーション (ネットワーク I/O) のためにボリューム内で費やされた合計時間。 Sum 統計は、指定した期間に読み取りオペレーションに費やされた合計秒数です。ある期間の平均読み取りレイテンシーを計算するには、Sum 統計を同じ期間の DataReadOperations メトリクスの Sum で割ります。 単位: 秒 有効な統計: Sum

メトリクス	説明
DataWriteOperationTime	ボリューム内のデータにアクセスするクライアントからの書き込みオペレーション (ネットワーク I/O) を実行するためにボリューム内で費やされた合計時間。 Sum 統計は、指定した期間に書き込みオペレーションに費やされた合計秒数です。ある期間の平均書き込みレイテンシーを計算するには、Sum 統計を同じ期間の DataWriteOperations メトリクスの Sum で割ります。 単位: 秒 有効な統計: Sum
MetadataOperationTime	ボリューム内のデータにアクセスしているクライアントからのメタデータオペレーション (ネットワーク I/O) を実行するために、ボリューム内で費やされた合計時間。 Sum 統計は、指定した期間に読み取りオペレーションに費やされた合計秒数です。ある期間の平均レイテンシーを計算するには、Sum 統計を同じ期間の MetadataOperations の Sum で割ます。 単位: 秒 有効な統計: Sum

メトリクス	説明
CapacityPoolReadBytes	ボリュームの容量プール階層から読み取られた (ネットワーク I/O) バイト数。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間にボリュームの容量プール階層から読み取られたバイト数の合計です。1 秒あたりの容量プールのバイト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
CapacityPoolReadOperations	ボリュームの容量プール階層における読み取りオペレーション (ネットワーク I/O) の数。この数は、容量プールの読み取りリクエストに変換されます。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間にボリュームの容量プール階層から行われた読み取りオペレーションの数です。1 秒あたりの容量プールのリクエスト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: カウント 有効な統計: Sum

メトリクス	説明
CapacityPoolWriteBytes	ボリュームの容量プール階層に書き込まれたバイト数 (ネットワーク I/O)。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間にボリュームの容量プール階層に書き込まれたバイト数の合計です。1 秒あたりの容量プールのバイト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: バイト 有効な統計: Sum
CapacityPoolWriteOperations	容量プール階層からボリュームへの書き込みオペレーションの数 (ネットワーク I/O)。この数は、書き込みリクエストに変換されます。 データの整合性を確保するため、ONTAP は書き込みオペレーションを実行した直後に容量プールで読み取りオペレーションを実行します。 Sum 統計は、指定した期間におけるボリュームの容量プール階層に対する書き込みオペレーションの合計数です。1 秒あたりの容量プールのリクエスト数を算出するには、Sum 統計を指定した期間の秒数で割ります。 単位: カウント 有効な統計: Sum

ストレージ容量のメトリクス

メトリクスはすべて、FileSystemId と VolumeId の 2 つのディメンションを取ります。

メトリクス	説明
StorageCapacity	ボリュームのサイズ (バイト単位)。 単位: バイト 有効な統計: Maximum
StorageUsed	ボリュームの使用済み論理ストレージキャパシティ。 単位: バイト 有効な統計: Average、Minimum、Maximum
StorageCapacityUtilization	ボリュームのストレージ容量の使用率。 単位: パーセント 有効な統計: Average
FilesUsed	ボリューム上で使用されているファイル (ファイルまたは inode の数)。 単位: カウント 有効な統計: Average、Minimum、Maximum
FilesCapacity	ボリューム上に作成できる inode の総数。 単位: カウント 有効な統計: Maximum

詳細なボリュームメトリクス

詳細なボリュームメトリクスは、ボリュームメトリクスよりも多くのディメンションを取り、データのより詳細な測定を可能にします。すべての詳細なボリュームメトリクスには、FileSystemId、VolumeId、StorageTier、および DataType のディメンションがあります。

- StorageTier ディメンションは、メトリクスが測定するストレージ階層を示し、All、SSD、および StandardCapacityPool の値を持つ可能性があります。
- DataType ディメンションは、メトリクスが測定するデータのタイプを示し、All、User、Snapshot、および Other の可能な値を示します。

次の表は、リスト化されたディメンションに関して StorageUsed メトリクスが測定するものを示しています。

メトリクス	説明
StorageUsed	使用されている論理スペースの量 (バイト単位)。このメトリクスは、このメトリクスと共に使用されたディメンションに応じて、さまざまなタイプのスペースの使用量を測定します。StorageTier を SSD または StandardCapacityPool に設定し、DataType を All に設定すると、このメトリクスは、このボリュームの、SSD 階層と容量プール階層それぞれの論理スペースの使用量を測定します。DataType ディメンションを User、Snapshot、Other のいずれかに設定し、StorageTier を All に設定すると、このメトリクスは各データタイプにおける論理スペース使用量を測定します。Snapshot データ使用量にはスナップショットリザーブが含まれます。これは、デフォルトではボリュームサイズの 5% です。 単位: バイト

メトリクス	説明
	有効な統計: `Average`、`Minimum`、`Maximum`
`StorageCapacityUtilization`	ボリュームの使用済み物理ディスク容量の割合。 単位: パーセント 有効な統計: `Maximum`

パフォーマンスの警告と推奨事項

FSx for ONTAP は、これらの CloudWatch メトリクスの 1 つが、複数の連続するデータポイントの事前定義されたしきい値に近づいたり超えたりすると、メトリクスの警告を表示します。これらの警告により、ファイルシステムのパフォーマンスを最適化するために使用できる実用的な推奨事項が示されます。

警告は、[Monitoring & performance] (モニタリングとパフォーマンス) ダッシュボードのいくつかのエリアからアクセスできます。アクティブまたは最近の Amazon FSx パフォーマンス警告と、ALARM 状態にあるファイルシステムに設定された CloudWatch アラームはすべて、概要セクションのモニタリングとパフォーマンスパネルに表示されます。この警告は、メトリクスグラフが表示されているダッシュボードのセクションにも表示されます。

Amazon FSx メトリクスの CloudWatch アラームを作成できます。詳細については、「Amazon FSx をモニタリングする Amazon CloudWatch アラームの作成」を参照してください。

パフォーマンスの警告を使用してファイルシステムのパフォーマンスを向上させる

Amazon FSx は、ファイルシステムのパフォーマンスを最適化するために使用できる実用的な推奨事項を提供します。これらの推奨事項では、潜在的なパフォーマンスのボトルネックに対処する方法が説明されています。アクティビティが今後も続くと予想される場合、またはそのアクティビティがファイルシステムのパフォーマンスに影響を及ぼしている場合は、推奨されるアクションを実行します。警告をトリガーしたメトリクスに応じて、次の表に示すように、ファイルシステムのスループットキャパシティまたはストレージ容量のいずれかを増やすことで解決できます。

ダッシュボードセクション	このメトリクスに対応する警告が存在する場合	この操作を行います
[Storage (ストレージ)]	プライマリストレージ容量の使用率	ファイルシステムがまだ SSD ストレージの最大容量に達していない場合は、ファイルシステムのプライマリストレージ容量を増やしてください。詳細については、「SSD ストレージ容量とプロビジョンド IOPS の変更」を参照してください。 ファイルシステムに複数の HA ペアがあり、プライマリストレージ容量の使用率がファイルシステムのアグリゲート (プライマリストレージ層を構成するストレージプール) におけるサブセットでのみ高い場合は、プライマリストレージ容量の使用率がファイルシステム全体に均等に分散されるようにワークロードを再調整することもできます。ワークロードの再調整について詳しくは、「FSx for ONTAP ワークロードバランスのモニタリング」を参照してください。
ファイルサーバーのパフォーマンス	ネットワークスループット ディスクスループット ディスク IOPS CPU 使用率	ファイルシステムがまだ最大のスループットキャパシティに達していない場合は、ファイルシステムのスループットキャパシティを増やしてください。スループットキャパシティの更新についての詳細は、「スループット容量を変更する方法」を参照してください。 ファイルシステムに複数の HA ペアがあり、ファイルサーバー内のサブセットの使用率が 1 つのみ高い場合は、ファイルシステムの各 HA ペアにおけるパフォーマンス機能をより均等に活用できるようにワークロードを再調整することもできます。ワークロードの再調整について詳しくは、「FSx for ONTAP ワークロードバランスのモニタリング」を参照してください。

ダッシュボードセクション	このメトリクスに対応する警告が存在する場合	この操作を行います
ディスクパフォーマンス	ディスク IOPS	ファイルシステムが現在のスループットキャパシティにおける最大 SSD IOPS に達していない場合は、SSD IOPS を増やしてください。ファイルシステムのプロビジョンド IOPS の更新について詳しくは、「SSD ストレージ容量とプロビジョンド IOPS の変更」を参照してください。 ファイルシステムに複数の HA ペアがあり、ディスク IOPS の使用率がファイルシステムのアグリゲート (プライマリストレージ層を構成するストレージプール) におけるサブセットでのみ高い場合は、ディスク IOPS がファイルシステム全体に均等に分散されるようにワークロードを再調整することもできます。ワークロードの再調整について詳しくは、「FSx for ONTAP ワークロードバランスのモニタリング」を参照してください。

ファイルシステムのパフォーマンスに関する詳細については、「Amazon FSx for NetApp ONTAP のパフォーマンス」を参照してください。

Amazon FSx をモニタリングする Amazon CloudWatch アラームの作成

CloudWatch アラームの状態が変更されたときに Amazon Simple Notification Service (Amazon SNS) メッセージを送信するアラームを作成できます。1 つのアラームで、指定した期間中、1 つのメトリクスをモニタリングします。必要に応じて、アラームは、特定のしきい値に関連するメトリクスの値に基づいて、複数の期間にわたって 1 つ以上のアクションを実行します。アクションは、Amazon SNS トピックまたは Auto Scaling ポリシーに送信される通知です。

アラームは、持続する状態変化に対してのみアクションを呼び出します。 CloudWatch アラームは、特定の状態にあるという理由でのみアクションを呼び出しません。状態が変更され、指定された期間にわたって維持されている必要があります。Amazon FSx コンソールまたは Amazon CloudWatch コンソールからアラームを作成できます。

次の手順では、Amazon FSx コンソール、 AWS Command Line Interface 、(AWS CLI)、API を使用してアラームを作成する方法について説明します。

Amazon FSx コンソールを使用してアラームを設定するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 左側のナビゲーションペインで、[File system] (ファイルシステム) を選択してから、アラームを作成するファイルシステムを選択します。
3. [概要] ページで、[モニタリングとパフォーマンス] をクリックします。
4. CloudWatch アラームタブを選択します。
5. CloudWatch アラームの作成 を選択します。 CloudWatch コンソールにリダイレクトされます。
6. [Select metric] (メトリクスの選択) を選択します。
7. [Metrics] (メトリクス) セクションで、[FSx] を選択します。
8. メトリクスカテゴリを選択します。
   - [File system metrics] (ファイルシステムのメトリクス)
   - [Detailed File System Metrics] (詳細なファイルシステムメトリクス)
   - [Volume metrics] (ボリュームメトリクス)
   - [Detailed Volume Metrics] (詳細なボリュームメトリクス)
9. アラームを設定するメトリクスを選択してから、[Select metric] (メトリクスの選択) を選択します。
10. [条件] セクションで、アラームに使用する条件を選択し、[次へ] をクリックします。

    > **Note**
    >
    > ファイルシステムのメンテナンス中は、メトリクスが公開されない場合があります。不要で誤解を招くアラーム条件の変更を防ぎ、欠落しているデータポイントに回復できるようにアラームを設定するには、「Amazon CloudWatch ユーザーガイド」の CloudWatch 「アラームが欠落しているデータを処理する方法の設定」を参照してください。

11. アラーム状態がアクションを開始したときに E メールまたは Amazon SNS 通知 CloudWatch を送信する場合は、アラーム状態トリガー のアラーム状態を選択します。

    [以下の SNS トピックに通知を送信] で、オプションを選択します。[Create topic] (トピックの作成) を選択すると、新しいメールサブスクリプションリスト用の名前とメールアドレスを設定で

きます。このリストは保存され、今後のアラーム用のフィールドに表示されます。[Next] (次へ) を選択します。

> **Note**
>
> [Create topic] (トピックの作成) を使用して新しい Amazon SNS トピックを作成する場合、メールアドレスを検証しなければ、そのアドレスで通知を受け取ることができません。E メールは、アラームがアラーム状態になったときにのみ送信されます。アラーム状態になったときに、E メールアドレスの検証がまだ完了していない場合は、そのアドレスで通知を受け取ることはできません。

12. [アラーム名] と [アラームの説明] フィールドに入力し、[次へ] をクリックします。
13. [プレビューと作成] ページで、作成しようとしているアラームを確認し、[アラームを作成] をクリックします。

CloudWatch コンソールを使用してアラームを設定するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. [Create Alarm] (アラームの作成) を選択して、[Create Alarm Wizard] (アラームウィザードの作成) を起動します。
3. 「Amazon FSx コンソールを使用してアラームを設定するには」のステップ 6 から手順に従います。

を使用してアラームを設定するには AWS CLI

- put-metric-alarm CLI コマンドを呼び出します。詳細については、「AWS CLI コマンドリファレンス」を参照してください。

CloudWatch API を使用してアラームを設定するには

- PutMetricアラーム API オペレーションを呼び出します。詳細については、「Amazon CloudWatch API リファレンス」を参照してください。

FSx for ONTAP ワークロードバランスのモニタリング

複数の HA ペアを持つファイルシステムを使用している場合、そのシステムにおけるパフォーマンスとスループットは、各 HA ペアに分散されます。FSx for ONTAP は、ファイルがファイルシステムに書き込まれる際、自動的にファイルのバランスを調整します。ただまれに、ワークロードのデータまたは I/O が HA ペア間で不均衡になり、ワークロードの全体的なパフォーマンスに影響を与えることがあります。ファイルシステムの各 HA ペア (およびそれらと同等のファイルサーバとアグリゲート、つまりプライマリストレージ階層を構成するストレージプール) 間で、負荷のバランスが保たれていることを確認するために、ワークロードをモニタリングできます。

トピック

プライマリストレージ使用率のバランス

ファイルシステムのプライマリストレージ容量は、ストレージプール (アグリゲートと呼ばれます) 内の各 HA ペアに均等に分配されます。各 HA ペアには 1 つのアグリゲートがあります。プライマリストレージ階層の平均使用率は、継続して 80% 以下に維持することをお勧めします。複数の HA ペアを使用するファイルシステムの場合は、アグリゲートごとの平均使用率を 80% 以下に維持することをお勧めします。

80% の使用率を維持することで、新しい受信データ用の空き領域が保証されるので、メンテナンス操作がアグリゲートの一時的な空き領域を要求できるだけの、適切なオーバーヘッドが維持されます。

アグリゲートでの不均衡が確認された場合には、ファイルシステムのプライマリストレージ容量 (それに応じた各アグリゲートのストレージ容量) を増加するか、ONTAP CLI の volume move コマンドを使用してアグリゲート間でボリュームを移動します。

ファイルサーバとディスクのパフォーマンス使用率における不均衡

ファイルシステムの総合的なパフォーマンス能力 (ネットワークスループット、ファイルサーバーからディスクへのスループットおよび IOPS、ディスク IOPS など) は、ファイルシステムの HA ペア

間で均等に配分されます。すべてのパフォーマンス制限について、平均使用率を継続して 50% 未満 (最大ピーク使用率は 80% 未満) に維持することをお勧めします。これは、すべての HA ペアにおけるファイルシステムのファイルサーバーリソースの全体的な使用率と、ファイルサーバーごとの使用率の両方に当てはまります。

ファイルサーバで不均衡なパフォーマンス使用率 (および不均衡なワークロードが置かれたファイルサーバの使用率が継続的に 80% を超えた状態) を確認した場合は、ONTAP CLI と REST API を使用して、パフォーマンスの不均衡の原因を詳細に診断し修正を行います。次の表は、不均衡を示している可能性のある指標と、それを詳細に診断するための手順を示しています。

ファイルシステムの状態	結果...
ファイルサーバーのディスクスループットまたはファイルサーバーのディスク IOPS が不均衡	HA ペアのサブセット (アクセスされているデータが多すぎるボリュームのサブセット) で I/O にホットスポットが発生し、HA ペアのサブセットに対するボトルネックとなっており、ワークロードの全体的なパフォーマンスが制限される可能性があります。使用率の高い各ファイルサーバーについて、最も使用率の高いボリュームをチェックし、アグリゲート内で最もアクティビティの多いボリュームを確認します。この手順の詳細については、「使用率の高いボリュームのリバランシング」を参照してください。
ネットワークスループットに不均衡が生じているものの、ファイルサーバのディスクスループット、ファイルサーバのディスク IOPS、またはディスク IOPS のバランスに不均衡は生じていない	データは HA ペア間で均等に分散されているものの、クライアントの分散が不均衡です。ネットワークスループット使用率が他のサーバーよりも高いファイルサーバーについて、使用率が上位のクライアントを確認し、それらのクライアントからいずれかのボリュームをマウント解除します。その後、別の HA ペアの別のエンドポイントを使用してボリュームを再マウントすることで、クライアントの再調整を行います。この手順の詳細については、「トラフィックの多いクライアントのリバランシング」を参照してください。

ONTAP CLI および REST API リソースへの CloudWatch ディメンションのマッピング

スケールアウトファイルシステムには、 `FileServer`または `Aggregate`ディメンションの Amazon CloudWatch メトリクスがあります。不均衡の症状をより詳細に診断するには、これらのディメン

ション値を ONTAP CLI または REST API の特定のファイルサーバ (またはノード) とアグリゲートにマッピングする必要があります。

- ファイルサーバの場合、各ファイルサーバの名前は ONTAP のファイルサーバ (またはノード) の名前 (例: FsxId01234567890abcdef-01) にマップされます。奇数番号のファイルサーバーは、ファイルシステムがセカンダリファイルサーバーにフェイルオーバーされていない限りトラフィックを処理する優先ファイルサーバーです。偶数番号のファイルサーバーは、パートナーが使用できない場合にのみトラフィックを処理するセカンダリファイルサーバーです。このためセカンダリファイルサーバーの使用率は、通常、優先ファイルサーバーよりも低くなります。
- アグリゲートの場合、各アグリゲートの名前は ONTAP のアグリゲートにマップされます (例: aggr1)。HA ペアごとに 1 つのアグリゲートがあります。つまり、アグリゲートaggr1は HA ペアのファイルサーバー FsxId01234567890abcdef-01 (アクティブなファイルサーバー) と FsxId01234567890abcdef-02 (セカンダリファイルサーバー) で共有され、アグリゲートaggr2はファイルサーバーFsxId01234567890abcdef-03と で共有FsxId01234567890abcdef-04されます。

ONTAP CLI を使用すると、すべてのアグリゲートとファイルサーバ間のマッピングを表示できます。

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. -fields node パラメータを指定して、storage aggregate show コマンドを使用します。

```
::> storage aggregate show -fields node
aggregate                      node
------------------------------ -------------------------
aggr1                          FsxId01234567890abcdef-01
aggr2                          FsxId01234567890abcdef-03
aggr3                          FsxId01234567890abcdef-05
aggr4                          FsxId01234567890abcdef-07
aggr5                          FsxId01234567890abcdef-09
aggr6                          FsxId01234567890abcdef-11
6 entries were displayed.
```

トラフィックの多いクライアントのリバランシング

ファイルサーバー間で I/O の不均衡が (特にネットワークスループット使用率に関して) 発生している場合、I/O クライアントの使用率の高さが原因であと考えられます。トラフィックの多いクライアントを特定するには、ONTAP CLI を使用します。

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. トラフィックが上位にあるクライアントを表示するには、ONTAP CLI の statistics top client show コマンドを使用します。オプションで -node パラメータを指定すると、特定のファイルサーバの上位クライアントのみを表示できます。特定のファイルサーバーの不均衡を診断する場合は、(node_name をファイルサーバーの名前、例えば FsxId01234567890abcdef-01 に置き換えて) -node パラメーターを使用します。

   オプションで -interval パラメーターを追加し、各レポートが出力されるまでの時間を (秒単位で) 測定する間隔を指定できます。この間隔を (たとえば、最大 300 秒にまで) 増加すると、各ボリュームに向かうトラフィック量についての長期的なサンプルが得られます。デフォルト値は 5 (秒)です。

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   出力では、上位のクライアントが IP アドレスとポート別に表示されます。

   ```
                                                    *Total     Total
               Client   Vserver          Node           Ops     (Bps)
   ------------------ --------- ------------------------- ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

3. 一覧表示されたトラフィックの多いクライアントのサブセットは、他のファイルサーバに再配分できます。それを行うためには、クライアントからボリュームをマウント解除し、SVM の NFS/SMB エンドポイントの DNS 名を使用して (これにより、ランダムな HA ペアに対応するランダムなエンドポイントが返されます)、ボリュームを再マウントします。

DNS 名は再利用することが推奨されますが、オプションで、特定のクライアントがマウントする HA ペアを明示的に選択することができます。確実に、別のエンドポイントにクライアントがマウントされるようにするために、トラフィックの多いノードに対応する IP アドレスとは別のエンドポイント IP アドレスを指定します。このためには、次の コマンドを実行します。

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
 address,curr-node
vserver   lif                  address      curr-node
--------- -------------------- ------------ -------------------------
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

この statistics top client show コマンドの出力例を見ると、クライアント 172.17.236.53 は多くのトラフィックを FsxId01234567890abcdef-01 に送っています。network interface show コマンドの出力では、このアドレスが 172.31.15.89 であることがわかります。別のエンドポイントにマウントするには、他のいずれかのアドレスを選択します (この例における他のアドレスは、FsxId01234567890abcdef-03 に対応するアドレス 172.31.8.112 だけです)。

使用率の高いボリュームのリバランシング

ボリュームまたはアグリゲート全体で I/O の不均衡が見られる場合は、ボリュームをリバランスすることで I/O トラフィックをボリューム間で再配分できます。

> **Note**
>
> アグリゲート間でストレージの使用率に不均衡が確認されている場合は、通常、高い使用率に I/O の不均衡が伴わない限りパフォーマンスに対する影響はありません。アグリゲート間でボリュームを移動してストレージ使用率のバランスを取ることもできますが、ボリュームの移動はパフォーマンスに影響がある場合にのみ行うことをお勧めします。移動を検討している各ボリュームで発生する I/O も考慮しないと、パフォーマンスに悪影響を及ぼす可能性があるためです。

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. ONTAP CLI の statistics volume show コマンドを (以下の点を変更し) 使用して、特定のアグリゲートで最もトラフィックの多いボリュームを表示します。

   - *aggregate_name* は、アグリゲートの名前 (例: aggr1) に置き換えます。
   - オプションで -interval パラメーターを追加し、各レポートが出力されるまでの時間を (秒単位で) 測定する間隔を指定できます。この間隔を (たとえば、最大 300 秒にまで) 増加すると、各ボリュームに向かうトラフィック量についての長期的なサンプルが得られます。デフォルト値は 5 (秒)です。

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

選択した間隔によっては、データが表示されるまでに最大 5 分かかることがあります。このコマンドは、アグリゲートに送られているトラフィック量と共に、そのアグリゲート内のすべてのボリュームを表示します。

```
                           *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

ボリュームの統計情報は構成要素ごとに表示されます (例えば、vol1__0015 は FlexGroup vol1 の 15 番目の構成要素です) 。出力例からわかるように、aggr1 の構成要素での使用率は、aggr2 の構成要素よりも高くなっています。アグリゲート間でトラフィックを均衡させる

には、トラフィックがより均等に分散されるように、構成ボリュームをアグリゲート間で移動します。

3. アグリゲート間でボリュームを移動するには、ONTAP CLI の volume move start コマンドを (次の値を置き換えて) 使用します。

   - *svm_name* は、移行対象のボリュームをホストしている SVM の名前に置き換えます。
   - *volume_name*は、ボリューム構成要素の名前 (例: vol1__0001) に置き換えます。
   - *aggregate_name* は、ボリュームの移動先アグリゲートの名前に置き換えます。

   > **Important**
   >
   > ボリュームの移動では、ソースおよびターゲットのファイルサーバにおいて、ネットワークとディスクのリソースが消費されます。その結果、進行中のボリューム移動プロセスが、ワークロードのパフォーマンスに影響を与える可能性があります。さらに、ボリューム移動プロセスにはカットオーバーフェーズも存在し、ボリュームへのトラフィックの I/O を一時的に停止させます。

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

ボリューム移動操作の状態を確認するには、ONTAP CLI の volume move show コマンドを使用します。

```
::> volume move show -vserver svm_name -volume volume_name
                          Vserver Name: svm01
                           Volume Name: vol1__0001
                  Actual Completion Time: -
                         Bytes Remaining: 1.00TB
            Specified Action For Cutover: retry_on_failure
          Specified Cutover Time Window: 30
                  Destination Aggregate: aggr2
                       Destination Node: FsxId01234567890abcdef-03
                        Detailed Status: Transferring data: 12.23GB sent.
                    Percentage Complete: 1%
```

```
                        Move Phase: replicating
            Prior Issues Encountered: -
        Estimated Remaining Duration: 00:40:25
              Replication Throughput: 434.3MB/s
                    Duration of Move: 00:00:27
                    Source Aggregate: aggr2
                         Source Node: FsxId01234567890abcdef-01
                          Move State: healthy
```

このコマンドでは、情報フィールドの 1 つとして、移動が完了するまでの推定時間を表示します。操作が終了した場合は、この同じコマンドで、Move Phase フィールドに完了したことが表示されます。

各 FlexGroup が、アグリゲート全体で均等に分散されていることを確認してください。構成要素の数は、各アグリゲートで推奨される 8 個となることが理想的です。1 つの構成ボリュームを、他の点ではバランスが取れている FlexGroup のために別のアグリゲートに移動した際には、バランスを保つために、別の (使用率の低い) 構成ボリュームをソースのアグリゲートに移動する必要があります。

FSx for ONTAP EMS イベントのモニタリング

FSx for ONTAP ファイルシステムのイベントは、NetApp ONTAP のネイティブの Events Management System (EMS) を使用することでモニタリングできます。これらのイベントは、ONTAP CLI を使用して NetApp表示できます。

トピック

- EMS イベントの概要
- EMS イベントを表示する
- Syslog サーバーへの EMS イベント転送

EMS イベントの概要

EMS イベントとは、事前に定義した条件が FSx for ONTAP ファイルシステム発生したときに警告する、自動生成される通知のことです。これらの通知は、絶えず情報を提供することで、より大きな問題 (ストレージ仮想マシン (SVM) の認証問題やフルボリュームなど) につながる可能性のある問題の、予防または修正を可能にします。

デフォルトでは、イベントはイベント管理システムのログに記録されます。EMS を使用すると、ユーザーパスワードの変更、容量がいっぱいに FlexGroup 近づいている構成要素、論理単位番号 (LUN) が手動でオンラインまたはオフラインになった、ボリュームのサイズ変更などのイベントをモニタリングできます。

ONTAP EMS イベントの詳細については、ONTAP ドキュメントセンターの NetApp 「ONTAP EMS リファレンス」を参照してください。イベントカテゴリを表示するには、ドキュメントの左側にあるナビゲーションペインを使用します。

> **Note**
>
> ONTAP EMS メッセージの中には、FSx for ONTAP ファイルシステムで使用できないものがあります。使用可能な ONTAP EMS メッセージのリストを表示するには、 NetApp ONTAP CLI イベントカタログ show コマンドを使用します。

EMS イベントの説明には、イベント名、重大度、考えられる原因、ログメッセージ、そして、対応の仕方を決める際に役立つ是正措置が記されています。例えば、ボリュームの自動サイズ調整が失敗すると、wafl.vol.autoSize.fail イベントが発生します。このイベントの説明には、是正措置は、自動サイズ調整中にボリュームの最大サイズを増やすことと記されています。

EMS イベントを表示する

NetApp ONTAP CLI イベントログ表示コマンドを使用して、イベントログの内容を表示します。このコマンドは、お使いのファイルシステムに `fsxadmin` ロールがある場合に使用できます。コマンドの構文は以下のとおりです。

```
event log show [event_options]
```

最新のイベントが一番上に表示されます。デフォルトでは、このコマンドにより、重大度のレベルが `EMERGENCY`、`ALERT`、`ERROR` であるイベントが以下の情報と共に表示されます。

- [時刻] — イベントの発生時刻です。
- [ノード] — イベントの発生場所であるノードです。
- [重大度] - イベントの重大性のレベルです。重大度が `NOTICE`、`INFORMATIONAL`、`DEBUG` であるイベントを表示するときは、`-severity` オプションを使用します。
- [イベント] — イベントの名前とメッセージです。

イベントに関する詳細情報を表示するには、以下の表にあるイベントオプションを 1 つまたは複数使用します。

イベントオプション	説明
`-detail`	追加のイベント情報を表示します。
`-detailtime`	詳細なイベント情報を新しい順に表示します。
`-instance`	すべてのフィールドに関する詳細情報を表示します。
`-node` *`nodename`*`|local`	指定したノードのイベントリストを表示します。詳細情報を表示するには、このオプションを `-seqnum` と共に使用します。
`-seqnum` *`sequence_number`*	この番号に一致するシーケンス内のイベントを選択します。詳細情報を表示するには、`-node` と共に使用します。
`-time` *`MM/DD/YYYY HH:MM:SS`*	この特定の時刻に発生したイベントを選択します。MM/DD/YYYY HH: MM: SS [+-HH: MM] という形式を使用します。2 つのタイムステートメント間に `..` 演算子を使用すると、時間範囲を指定できます。 `event log show -time "04/17/2023`

イベントオプション	説明
	05:55:00".."04/17/2023 06:10:00" 比較時刻値は、コマンドを実行した時点の現在時刻が基準となります。次の例は、過去 1 分間に発生したイベントのみを表示する方法を示しています。 `event log show -time >1m` このオプションの月と日のフィールドはゼロパディングされていません。これらのフィールドは 1 桁の数字でもかまいません (例: 4/1/2023 06:45:00)。

イベントオプション	説明
-severity *sev_level*	*sev_level* の値に一致するイベントを選択します。次のいずれかになるはずです。 • EMERGENCY — 中断 • ALERT — 単一障害点 • ERROR — 低下 • NOTICE - 情報 • INFORMATIONAL - 情報 • DEBUG - デバッグ情報 すべてのイベントを表示するには、重大度を以下のように指定します。 `event log show -severity <=DEBUG`

イベントオプション	説明
-ems-severity *ems_sev_level*	*ems_sev_level* の値に一致するイベントを選択します。以下のいずれかになるはずです。 • NODE_FAULT — データの破損が検出されたか、ノードがクライアントサービスを提供できない。 • SVC_FAULT — 一時的なサービスの中断 (通常は短時間のソフトウェア障害) が検出された。 • NODE_ERROR — ハードウェアのエラーが検出された (ただし、直ちに復旧不可能になるレベルではない)。 • SVC_ERROR — ソフトウェアのエラーが検出された (ただし、直ちに復旧不可能になるレベルではない)。 • WARNING — 優先度の高いメッセージ。障害は示されていない。 • NOTICE — 優先度が中程度のメッセージ。障害は示されていない。 • INFO — 優先度の低いメッセージ。障害は示されていない。 • DEBUG — デバッグメッセージ。

イベントオプション	説明
	• VAR — 実行時に選択された、重大度が変化する可能性のあるメッセージ。 すべてのイベントを表示するには、重大度を以下のように指定します。 `event log show -ems-severity <=DEBUG`
-source *text*	*text* 値に一致するイベントを選択します。ソースは通常、ソフトウェアモジュールです。
-message-name *message_name*	*message_name* 値に一致するイベントを選択します。メッセージ名は記述的であるため、メッセージ名で出力をフィルタリングすると、特定のタイプのメッセージが表示されます。
-event *text*	*text* 値に一致するイベントを選択します。event フィールドには、パラメータを含むイベントの全文が含まれます。
-kernel-generation-num *integer*	*integer* 値に一致するイベントを選択します。kernel 生成番号があるのは、kernel から発生したイベントのみです。

イベントオプション	説明
-kernel-sequence-num *integer*	*integer* 値に一致するイベントを選択します。kernel シーケンス番号があるのは、kernel から発生したイベントのみです。
-action *text*	*text* 値に一致するイベントを選択します。action フィールドには、状況を修正するにはどの是正措置を講じる必要があるかが (もしある場合に) 記されています。
-description *text*	*text* 値に一致するイベントを選択します。description フィールドには、イベントが発生した理由とそれが意味することが記されています。
-filter-name *filter_name*	*filter_name* 値に一致するイベントを選択します。既存のフィルターに含まれる、この値に一致するイベントのみが表示されます。
-fields *fieldname* ,...	コマンド出力に、指定された 1 つまたは複数のフィールドも含まれていることを、示しています。-fields ? を使用すれば、指定するフィールドを選択できます。

EMS イベントを表示するには

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. イベントログの内容を表示するときは、`event log show` コマンドを使用します。

```
::> event log show
Time                 Node          Severity      Event
-------------------- ------------- ------------- ------------------------
6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
 received on node node1, port e0a.
6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
 received on node node1, port e0d.
```

`event log show` コマンドによって返される EMS イベントの詳細については、ONTAP ドキュメントセンターの ONTAP EMS リファレンスを参照してください。 NetApp

Syslog サーバーへの EMS イベント転送

Syslog サーバーに通知を転送するように EMS イベントを設定できます。EMS イベント転送は、ファイルシステムのリアルタイムモニタリングに使用され、さまざまな問題の根本原因を特定して分離します。環境にイベント通知用の Syslog サーバーがまだ含まれていない場合は、まずサーバーを作成する必要があります。Syslog サーバー名を解決するには、ファイルシステムで DNS を設定する必要があります。

Syslog サーバーに通知を転送するように EMS イベントを設定するには

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. イベント通知送信先 create コマンドを使用して、次の属性を指定して`syslog`、タイプ のイベント通知送信先を作成します。

- *dest_name* – 作成する通知先の名前 (例: syslog-ems) 。イベント通知の送信先名の長さは 2～64 文字である必要があります。有効な文字は、A～Z、a～z、0～9、「_」、「-」の ASCII 文字です。名前は、A～Z、a～z、または 0～9 で始まる必要があります。
- *syslog_name* – Syslog メッセージが送信される Syslog サーバーのホスト名または IP アドレス。
- *transport_protocol* – イベントの送信に使用されるプロトコル。
  - udp-unencrypted – セキュリティのないユーザーデータグラムプロトコル。これはデフォルトのプロトコルです。
  - tcp-unencrypted — セキュリティのない Transmission Control Protocol。
  - tcp-encrypted — Transport Layer Security (TLS) を使用した Transmission Control Protocol。このオプションを指定すると、FSx for ONTAP は証明書を検証して送信先ホストの ID を検証します。
- *port_number* – Syslog メッセージが送信される Syslog サーバーポート。デフォルト値syslog-portパラメータは、 syslog-transportパラメータの設定によって異なります。syslog-transport が に設定されている場合tcp-encrypted、syslog-portデフォルト値は です6514。syslog-transport が に設定されている場合tcp-unencrypted、のデフォルト値syslog-portは です601。それ以外の場合、デフォルトのポートは に設定されます514。

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. イベント通知作成コマンドを使用して、イベントフィルターで定義された一連のイベントの新しい通知を、前のステップで作成した通知送信先に作成し、次の属性を指定します。

   - *node_name* – イベントフィルターの名前。イベントフィルターに含まれるイベントは、 -destinationsパラメータで指定された宛先に転送されます。
   - *dest_name* – イベント通知の送信先となる既存の通知先の名前。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. event notification destination check コマンドを使用してテストメッセージを生成し、セットアップが機能することを確認します。コマンドで次の属性を指定します。

   - *node_name* – ノードの名前 (例: FsxId07353f551e6b557b4-01) 。

- *dest_name* – イベント通知の送信先となる既存の通知先の名前。

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

クラウドインサイトによるモニタリング

NetApp Cloud Insights は、Amazon FSx for NetApp ONTAP ファイルシステムを他の NetApp ストレージソリューションとともにモニタリングするために使用できる NetApp サービスです。クラウドインサイトを使用すると、設定、容量、およびパフォーマンスメトリクスを経時的にモニタリングして、ワークロードの傾向を理解し、将来のパフォーマンスとストレージ容量のニーズを計画できます。また、既存のワークフローや生産性ツールと統合できるメトリクス条件に基づいてアラートを作成することもできます。

> **Note**
>
> クラウドインサイトはスケールアウトファイルシステムではサポートされていません。

クラウドインサイトでは以下を提供します。

- 幅広いメトリクスとログ - 設定、容量、およびパフォーマンスのメトリクスを収集します。事前定義されたダッシュボード、アラート、およびレポートを使用して、ワークロードがどのようにトレンドになっているのかを理解します。
- ユーザー分析とランサムウェア保護 - Cloud Secure と ONTAP スナップショットを使用すると、ユーザーエラーとランサムウェアのインシデントを監査、検出、停止、および修復できます。
- SnapMirror レポート — SnapMirror 関係を理解し、レプリケーションの問題に関するアラートを設定します。
- 容量計画 - オンプレミスワークロードのリソース要件を理解して、ワークロードをより効率的な FSx for ONTAP 設定に移行するのに役立てます。インサイトを使用して、FSx for ONTAP のデプロイでより多くのパフォーマンスまたは容量が必要になる時期を計画することもできます。

Cloud Insights の詳細については、「Cloud Central の Cloud NetApp Insights」を参照してください。 NetApp

Harvest と Grafana を使用した ONTAP ファイルシステムの FSx のモニタリング

NetApp Harvest は、ONTAP システムからパフォーマンスと容量のメトリクスを収集するためのオープンソースツールで、FSx for ONTAP と互換性があります。Harvest と Grafana をオープンソースのモニタリングソリューションに使用できます。

Harvest と Grafana の開始方法

次のセクションでは、FSx for ONTAP ファイルシステムのパフォーマンスとストレージ容量の使用率を測定するように Harvest と Grafana をセットアップおよび設定する方法について詳しく説明します。

Harvest と Grafana を使用して、Amazon FSx for NetApp ONTAP ファイルシステムをモニタリングできます。 NetApp Harvest は、FSx for ONTAP ファイルシステムからパフォーマンス、容量、ハードウェアメトリクスを収集して ONTAP データセンターをモニタリングします。Grafana は、収集された Harvest 指標を表示できるダッシュボードを提供します。

サポートされている Harvest ダッシュボード

Amazon FSx for NetApp ONTAP は、オンプレミス NetApp ONTAP とは異なるメトリクスのセットを公開します。そのため、FSx for ONTAP での使用`fsx`は現在、 でタグ付けされた次の out-of-the-box Harvest ダッシュボードのみがサポートされています。これらのダッシュボードの一部のパネルには、サポートされていない情報が表示されない可能性があります。

- ONTAP: コンプライアンス
- ONTAP: データ保護スナップショット
- ONTAP: セキュリティ
- ONTAP: SVM
- ONTAP: ボリューム

AWS CloudFormation テンプレート

開始するには、Harvest と Grafana を実行する Amazon EC2 インスタンスを自動的に起動する AWS CloudFormation テンプレートをデプロイします。 AWS CloudFormation テンプレートへの入力として、このデプロイの一部として追加されるファイルシステムの`fsxadmin`ユーザーと Amazon FSx

管理エンドポイントを指定します。デプロイが完了したら、Grafana ダッシュボードにログインしてファイルシステムをモニタリングできます。

このソリューションでは AWS CloudFormation 、 を使用して Harvest および Grafana ソリューションのデプロイを自動化します。テンプレートによって Amazon EC2 Linux インスタンスが作成され、Harvest および Grafana ソフトウェアがインストールされます。このソリューションを使用するには、fsx-ontap-harvest-grafana.template AWS CloudFormation テンプレートをダウンロードします。

> **Note**
>
> このソリューションを実装すると、関連する AWS サービスの料金が発生します。詳細については、それらのサービスの料金詳細ページを参照してください。

Amazon EC2 インスタンスタイプ

テンプレートを設定するときは、Amazon EC2 インスタンスタイプを指定します。 NetAppのインスタンスサイズに関する推奨事項は、モニタリングするファイルシステムの数と収集を選択したメトリクスの数によって異なります。デフォルト設定では、モニタリングする 10 個のファイルシステムごとに、 NetApp が以下を推奨します。

- CPU: 2 コア
- メモリ:1 GB
- ディスク: 500 MB (主にログファイルで使用されます)

次は設定例および選択する `t3` インスタンスタイプを示します。

ファイルシステム	CPU	ディスク	インスタンスタイプ
10 未満	2 コア	500 MB	`t3.micro`
10～40	4 コア	1000 MB	`t3.xlarge`
40 以上	8 コア	2000 MB	`t3.2xlarge`

Amazon EC2 インスタンスタイプの詳細については、「Amazon EC2 ユーザーガイド」の「汎用インスタンスAmazon EC2」を参照してください。

インスタンスポートルール

Amazon EC2 インスタンスを設定するときは、Amazon EC2 Harvest および Grafana インスタンスが属するセキュリティグループのインバウンドトラフィック用にポート 3000 と 9090 が開いていることを確認します。起動されたインスタンスは HTTPS 経由でエンドポイントに接続するため、エンドポイントを解決する必要があります。これには、DNS のポート 53 TCP/UDP が必要です。さらに、エンドポイントに到達するには、HTTPS とインターネットアクセスにポート 443 TCP が必要です。

デプロイ手順

次の手順では、Harvest / Grafana ソリューションを設定してデプロイします。デプロイには約 5 分かかります。開始する前に、 AWS アカウントの Amazon Virtual Private Cloud (Amazon VPC) で実行されている FSx for ONTAP ファイルシステムと、以下に示すテンプレートのパラメータ情報が必要です。ファイルシステムの作成の詳細については、「FSx for ONTAP ファイルシステムの作成」を参照してください。

Harvest / Grafana ソリューションスタックを起動するには

1. fsx-ontap-harvest-grafana.template AWS CloudFormation テンプレートをダウンロードします。 AWS CloudFormation スタックの作成の詳細については、「 ユーザーガイド」の「 AWS CloudFormation コンソールでのスタックの作成AWS CloudFormation 」を参照してください。

   > **Note**
   >
   > デフォルトでは、このテンプレートは米国東部 (バージニア北部) AWS リージョンで起動します。このソリューションは、Amazon FSx AWS リージョン が利用可能な で起動する必要があります。詳細については、「AWS 全般のリファレンス」の「Amazon FSx エンドポイントとクォータ」を参照してください。

2. [Parameters] (パラメータ) については、テンプレートのパラメータを確認し、ファイルシステムのニーズに合わせて変更します。このソリューションは以下のデフォルト値を使用します。

パラメータ	デフォルト	[Description] (説明)
InstanceType	`t3.micro`	Amazon EC2 インスタンスタイプ 以下が `t3` インスタンスタイプです。 • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` このパラメータで許可される Amazon EC2 インスタンスタイプの値の完全なリストについては、「.template fsx-ontap-harvest-grafana」を参照してください。
KeyPair	デフォルト値なし	Amazon EC2 インスタンスへのアクセスに使用されるキーペア。
SecurityGroup	デフォルト値なし	Harvest / Grafana インスタンスのセキュリティグループ ID。ポート 53 と 443 に加えて、インバウンドポート 3000 と 9090 が、Grafana ダッシュボードへのアクセスに使用するクライアントから開かれていることを確認します。

パラメータ	デフォルト	[Description] (説明)
サブネットタイプ	デフォルト値なし	`public` または `private` のいずれかのサブネット タイプを指定します。インターネットに接続する必要があるリソースには `public` サブネットを、インターネットに接続しないリソースにはプライベートサブネットを使用してください。詳細については、「Amazon VPC ユーザーガイド」の「サブネットタイプ」を参照してください。
サブネット	デフォルト値なし	Amazon FSx for NetApp ONTAP ファイルシステムの優先サブネットと同じサブネットを指定します。Fsx for ONTAP ファイルシステム詳細ページの [Network & security] (ネットワークとセキュリティ) タブの Amazon FSx コンソールで [Preferred subnet] (優先サブネット) の IDを検索できます。
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	特定の AWS リージョン内の Amazon Linux 2 AMI の最新バージョン。

パラメータ	デフォルト	[Description] (説明)
F SxEndポイント	デフォルト値なし	ファイルシステムの管理エンドポイントの IP アドレス。FSx for ONTAP ファイルシステムの詳細ページの [Administration] (管理) タブの Amazon FSx コンソールのファイルシステムで管理エンドポイント [IP address] (IP アドレス) を検索できます。
SecretName	デフォルト値なし	AWS Secrets Manager ファイルシステムの `fsxadmin`ユーザーのパスワードを含むシークレット名。これは、ファイルシステムを作成したときに指定したパスワードです。

3. [Next] (次へ) を選択します。
4. [Options] (オプション) には、[Next] (次へ) を選択します。
5. [Review] (確認) で、設定を確認して確定します。テンプレートが IAM リソースを作成することを確認するチェックボックスを選択する必要があります。
6. [Create] (作成) を選択してスタックをデプロイします。

スタックのステータスは、 ステータス列の AWS CloudFormation コンソールで表示できます。約 5 分で CREATE_COMPLETE (作成完了) のステータスが表示されます。

Grafana にログインする

デプロイが完了したら、ブラウザを使用して、Amazon EC2 インスタンスの IP およびポート 3000 で Grafana ダッシュボードにログインします。

```
http://EC2_instance_IP:3000
```

プロンプトが表示されたら、Grafana デフォルトのユーザー名 (admin) とパスワード (pass) を使用します。ログインしたらすぐにパスワードを変更することをお勧めします。

詳細については、「」の NetApp 「収穫」ページを参照してください GitHub。

Harvest と Grafana のトラブルシューティング

Harvest と Grafana ダッシュボードに記載されているデータが失われている場合、または FSx for ONTAP で Harvest と Grafana をセットアップできない場合は、次のトピックで潜在的な解決策を確認してください。

トピック

- SVM とボリュームのダッシュボードが空白
- CloudFormation タイムアウト後にロールバックされた スタック

SVM とボリュームのダッシュボードが空白

AWS CloudFormation スタックが正常にデプロイされ、Grafana に連絡できるが、SVM とボリュームのダッシュボードが空白の場合は、次の手順を使用して環境のトラブルシューティングを行います。Harvest と Grafana がデプロイされている Amazon EC2 インスタンスへの SSH アクセスが必要です。

1. Harvest クライアントと Grafana クライアントが実行されている Amazon EC2 インスタンスに SSH 接続します。

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. 次のコマンドを使用して harvest.yml ファイルを開き、
   - FSx for ONTAP インスタンスのエントリが として作成されたことを確認しますCluster-2。
   - ユーザー名とパスワードのエントリがfsxadmin認証情報と一致することを確認します。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. パスワードフィールドが空白の場合は、エディタで ファイルを開き、次のようにfsxadminパスワードで更新します。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. 今後のデプロイでは、fsxadminユーザー認証情報が Secrets Manager に次の形式で保存され、をパスワードfsxadmin_passwordに置き換えます。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation タイムアウト後にロールバックされた スタック

CloudFormation スタックを正常にデプロイできず、エラーでロールバックする場合は、次の手順を使用して問題を解決します。 CloudFormation スタックによってデプロイされた EC2 インスタンスへの SSH アクセスが必要です。

1. CloudFormation スタックを再デプロイし、自動ロールバックが無効になっていることを確認します。
2. Harvest クライアントと Grafana クライアントが実行されている Amazon EC2 インスタンスに SSH 接続します。

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. 次のコマンドを使用して、Docker コンテナが正常に起動されたことを確認します。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

レスポンスには、次のように 5 つのコンテナが表示されます。

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                     NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                             harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                            harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                    0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
```

```
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                    0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. Docker コンテナが実行されていない場合は、次のように /var/log/cloud-init-output.log ファイルで障害がないか確認します。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ****************************************************

TASK [Gathering Facts] ***************************************************
ok: [localhost]

TASK [Verify images] *****************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP ***************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. 障害が発生した場合は、次のコマンドを実行して Harvest コンテナと Grafana コンテナをデプロイします。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
```

```
    [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
    [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml
    [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml --tags api
```

6. を実行して Harvest sudo docker psと Grafana URL に接続することで、コンテナが正常に起動したことを確認します。

AWS CloudTrail での FSx for ONTAP API コールのロギング

Amazon FSx は、AWS CloudTrail と統合されています。これは、Amazon FSx のユーザー、ロール、または AWS のサービスで実行されたアクションをレコードするためのサービスです。CloudTrail は、Amazon FSx for NetApp ONTAP に対するすべての Amazon FSx API コールをイベントとしてキャプチャします。キャプチャされたコールには、Amazon FSx コンソールからのコールと、Amazon FSx API オペレーションへのコードコールが含まれます。

追跡を作成する場合は、Amazon FSx のイベントなど、Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報に基づいて、Amazon FSx に対して行われたリクエストを判断できます。リクエストの実行元 IP アドレス、実行者、実行日時、および追加の詳細を判断することもできます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail 内の Amazon FSx 情報

CloudTrail は、アカウントを作成すると AWS アカウントで有効になります。Amazon FSx で API アクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) で AWS のその他のサービスのイベントと共に CloudTrail イベントにレコードされます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Amazon FSx のイベントなど、AWS アカウントのイベントを継続的にレコードするには、追跡を作成します。[Trail] (追跡) により、CloudTrail はログファイルを Simple Storage Service (Amazon S3) バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡では、AWS パーティション内のすべての AWS リージョンからのイベントを記録し、指定した Simple Storage Service (Amazon S3)バケットにログファ

イルを配信します。さらに、CloudTrail· ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS サービスを設定できます。次のトピックの詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

- AWS アカウント の追跡の作成
- AWS サービスと CloudTrail ログの統合
- CloudTrail の Amazon SNS 通知の設定
- 複数のリージョンからのCloudTrailログファイルの受信 と 複数のアカウントからのCloudTrailログファイルの受信

すべての Amazon FSx API コール は CloudTrail によってログに記録されます。例えば、`CreateFileSystem` と `TagResource` オペレーションへのコールは、CloudTrail ログファイルにエントリを生成します。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか.
- リクエストがロールまたはフェデレーティッドユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「AWS CloudTrail ユーザーガイド」の [CloudTrail userIdentity element] (CloudTrail userIdentity 要素) を参照してください。

Amazon FSx ログファイルエントリの概要

[Trail] (追跡) は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一か複数のログエントリがあります。イベント は、任意の出典からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail· ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、ファイルシステムのタグがコンソールから作成されたときの `TagResource` オペレーションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

次の例は、ファイルシステムのタグがコンソールから削除されたときの UntagResource アクションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

クォータ

Amazon FSx for NetApp ONTAP を使用する際のクォータについては、以下を参照してください。

トピック

増やすことができるクォータ

以下は、 AWS アカウントごとに引き上げ AWS リージョンることができる各 の Amazon FSx for NetApp ONTAP のクォータです。

リソース	デフォルト	[Description] (説明)
ONTAP ファイルシステム	100	このアカウントで作成できる Amazon FSx for NetApp ONTAP ファイルシステムの最大数。
ONTAP SSD ストレージ容量	524,288	このアカウントで保持できるすべての Amazon FSx for NetApp ONTAP ファイルシステムの SSD ストレージ容量 (GiB 単位) の最大量。
ONTAP スループットキャパシティ	10,240	このアカウントで保持できるすべての Amazon FSx for NetApp ONTAP ファイルシステムのスループットキャパシティの最大量 (MBps 単位) 。
ONTAP SSD IOPS	1,000,000	このアカウントで保持できるすべての Amazon FSx for NetApp ONTAP ファイルシステムの SSD IOPS の最大量。

リソース	デフォルト	[Description] (説明)
ONTAP ファイルシステムあたりのバックアップ	10,000	このアカウントで保持できるすべての Amazon FSx for NetApp ONTAP ファイルシステムのユーザー主導ボリュームバックアップの最大数。

クォータの引き上げをリクエストするには

1. AWS Support ページを開き、必要に応じてサインインし、[Create case] (ケースの作成) を選択します。
2. [Create case] (ケースの作成) で、[Account and billing support] (アカウントおよび請求サポート) を選択します。
3. [Case details] (ケースの詳細) パネルで、次のエントリを作成します。
   - [Type] (タイプ) に、[Account] (アカウント) を選択します。
   - [Category] (カテゴリ) で、[Other Account Issues] (その他のアカウントの問題) を選択します。
   - [Subject] (件名) に **`Amazon FSx for NetApp ONTAP service limit increase request`** と入力します。
   - 入力するリクエストの詳細 [Description] (説明) には、以下が含まれます。
     - 引き上げたい FSx クォータ、そして判明している場合は引き上する値。
     - クォータ引き上げを希望する理由。
     - 増加をリクエストしている各ファイルシステムのファイルシステム ID とリージョン。
4. 希望の 連絡先オプション を入力し、[Submit] (提出) を選択します。

ファイルシステムあたりのリソースクォータ

次の表に、 の各ファイルシステムの Amazon FSx for NetApp ONTAP リソースのクォータを示します AWS リージョン。

リソース	ファイルシステムあたりの制限
SSD の最小ストレージ容量	高可用性 (HA) ペアあたり 1,024 GiB
SSD の最大ストレージ容量	• スケールアウト: HA ペアあたり 512 TiB、最大 1 PiB • スケールアップ: 192 TiB
最大 SSD IOPS	スケールアウト: • HA ペアあたり 200,000 (最大 12 ペア) スケールアップ: • 米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、および欧州 (アイルランド) では、160,000 • FSx for ONTAP AWS リージョン が利用可能な他のすべての で 80,000
最小スループット容量	• スケールアウト: HA ペアあたり 3,072 MBps • スケールアップ: 128 MBps
最大スループット容量	スケールアウト: • 73,728 MBps [1] スケールアップ: • 米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リー

リソース	ファイルシステムあたりの制限
	ジョン、および欧州 (アイルランド) で 4,096 MBps [2] • FSx for ONTAP AWS リージョン が利用可能な他のすべての で 2,048 MBps
ボリュームの最大数	• スケールアウト: 1,000 • スケールアップ: 500
スナップショットの最大数	ボリュームあたり 1,023 個[3]
バックアップの最大数	ボリュームあたり 4,091
SVM の最大数	スケールアウト: • 5 スケールアップ: • 6 (128 MBps のスループット容量) • 6 (256 MBps のスループット容量) • 14 (512 MBps のスループット容量) • 14 (1,024 MBps のスループット容量) • 24 (2,048 MBps のスループット容量) • 24 (4,096 MBps のスループット容量)
タグの最大数	50
自動バックアップの最大保持期間	90 日間
ユーザーによるバックアップの最大保持期間	保持期限なし

リソース	ファイルシステムあたりの制限
ファイルシステムごとにサポートされるルートの最大数	50[5]

Note

[1] 12 個の HA ペア (HA ペアあたり 6,144 MBps) を持つスケールアウトファイルシステムの場合。詳細については、「高可用性 (HA) ペア」を参照してください。

[2] 4 GBps のスループット容量をプロビジョニングするには、FSx for ONTAP スケールアップファイルシステムには、サポートされている で最大 SSD IOPS (160,000) と最低 5,120 GiB の SSD ストレージ容量の設定が必要です AWS リージョン。4,096 MBps のスループットキャパシティ AWS リージョン をサポートする の詳細については、「」を参照してくださいスループット容量がパフォーマンスに与える影響。

[3] ボリュームごとに最大 1,023 個のスナップショットを任意の時点で保存できます。この制限に達したら、ボリュームの新しいスナップショットを作成する前に、既存のスナップショットを削除する必要があります。

[4] ボリュームごとに最大 4,091 個のバックアップを任意の時点で保存できます。この制限に達したら、ボリュームの新しいバックアップを作成する前に、既存のバックアップを削除する必要があります。

[5] ファイルシステムごとに任意の時点で最大 50 のルートを設定できます。この制限に達したら、新しいルートを設定する前に既存のルートを削除する必要があります。ファイルシステムが持つルートの数は、そのファイルシステムが持つ SVMs の数とそれに関連付けられたルートテーブルの数によって決まります。(1 + ファイルシステム内の SVMs の数) * (ファイルシステムに関連付けられたルートテーブル) の計算式を使用して、ファイルシステムへの既存のルート数を決定できます。

Amazon FSx for NetApp ONTAP のトラブルシューティング

以下のシナリオを使用して、FSx for ONTAP で発生する問題をトラブルシューティングします。

トピック

マルチ AZ ファイルシステムが **MISCONFIGURED** 状態にある

次のように、ファイルシステムが MISCONFIGURED 状態になる原因はいくつか考えられますが、それぞれ独自の解決方法があります。

トピック

VPC 所有者アカウントがマルチ AZ VPC 共有を無効にしました

共有 VPC サブネット AWS アカウント の参加者が作成したマルチ AZ ファイルシステムは、次のいずれかの理由で MISCONFIGURED状態になります。

- VPC サブネットを共有した所有者アカウントが、FSx for ONTAP ファイルシステムのマルチ AZ VPC 共有サポートを無効にしています。
- 所有者アカウントが VPC サブネットの共有を解除しました。

所有者アカウントが VPC サブネットの共有を解除した場合、そのファイルシステムのコンソールに次のメッセージが表示されます。

```
The vpc ID vpc-012345abcde does not exist
```

問題を解決するには、VPC サブネットを共有した所有者アカウントに連絡する必要があります。詳細については、「共有サブネット内での FSx for ONTAP ファイルシステムの作成」を参照してください。

マルチ AZ ファイルシステム上に新しい SVM を作成することはできません

共有 VPC AWS アカウント の参加者が作成したマルチ AZ ファイルシステムでは、次のいずれかの理由で新しい SVM を作成できません。

- VPC サブネットを共有した所有者アカウントが、FSx for ONTAP ファイルシステムのマルチ AZ VPC 共有サポートを無効にしています。
- 所有者アカウントが VPC サブネットの共有を解除しました。

問題を解決するには、VPC サブネットを共有した所有者アカウントに連絡する必要があります。詳細については、「共有サブネット内での FSx for ONTAP ファイルシステムの作成」を参照してください。

ファイルシステムにアクセスできない

次のように、ファイルシステムにアクセスできない原因はいくつか考えられますが、それぞれ独自の解決方法があります。

トピック

- ファイルシステムの Elastic network interface が変更または削除されました
- ファイルシステムの Elastic Network Interface に接続された Elastic IP アドレスが削除されました
- ファイルシステムの VPC セキュリティグループに、必要なインバウンドルールがありません
- コンピューティングインスタンスの VPC セキュリティグループに、必要なアウトバウンドルールがありません
- コンピューティングインスタンスのサブネットが、ファイルシステムに関連付けられたルートテーブルを使用しない
- Amazon FSx は、 を使用して作成されたマルチ AZ ファイルシステムのルートテーブルを更新できません AWS CloudFormation
- 別の VPC のクライアントから iSCSI 経由でファイルシステムにアクセスできない

- 所有アカウントが VPC サブネットの共有を解除しました
- 別の VPC またはオンプレミスのクライアントから NFS、SMB、ONTAP CLI、ONTAP REST API 経由でファイルシステムにアクセスできない

ファイルシステムの Elastic network interface が変更または削除されました

ファイルシステムの Elastic Network Interface を変更または削除しないでください。このネットワークインターフェイスを変更または削除すると、仮想プライベートクラウド (VPC) とファイルシステム間の接続が完全に失われる可能性があります。新しいファイルシステムを作成し、Amazon FSx ネットワークインターフェイスは変更あるいは削除しないでください。詳細については、「Amazon VPC によるファイルシステムアクセスコントロール」を参照してください。

ファイルシステムの Elastic Network Interface に接続された Elastic IP アドレスが削除されました

Amazon FSx は、公開インターネットからのファイルシステムへのアクセスをサポートしていません。Amazon FSx は、インターネットから到達可能なパブリック IP アドレスである Elastic IP アドレスを自動的にデタッチし、ファイルシステムの Elastic Network Interface にアタッチします。詳細については、「サポートされているクライアント」を参照してください。

ファイルシステムの VPC セキュリティグループに、必要なインバウンドルールがありません

Amazon VPC セキュリティグループ で指定されているインバウンドルールを確認し、ファイルシステムに関連付けられているセキュリティグループに対応するインバウンドルールがあることを確認します。

コンピューティングインスタンスの VPC セキュリティグループに、必要なアウトバウンドルールがありません

Amazon VPC セキュリティグループ で指定されたアウトバウンドルールを確認し、コンピューティングインスタンスに関連付けられているセキュリティグループに、対応するアウトバウンドルールがあることを確認します。

コンピューティングインスタンスのサブネットが、ファイルシステムに関連付けられたルートテーブルを使用しない

FSx for ONTAP は、VPC ルートテーブル内のファイルシステムにアクセスするためのエンドポイントを作成します。クライアントが存在するサブネットに関連付けられているすべての VPC ルートテーブルを使用するようにファイルシステムを設定する必要があります。デフォルトでは、Amazon FSx は VPC のメインルートテーブルを使用します。オプションで、ファイルシステムを作成するときに Amazon FSx で使用する 1 つ以上のルートテーブルを指定できます。

ファイルシステムのクラスタ間エンドポイントに ping を実行できるが、ファイルシステムの管理エンドポイントに ping を実行できない場合 (詳細については ファイルシステムリソース を参照)、クライアントはファイルシステムのルートテーブルの 1 つに関連付けられているサブネットにない可能性があります。ファイルシステムにアクセスするには、ファイルシステムのルートテーブルの 1 つをクライアントのサブネットに関連付けます。ファイルシステムの Amazon VPC のルートテーブルの更新に関する詳細については、ファイルシステムの更新 を参照してください。

Amazon FSx は、 を使用して作成されたマルチ AZ ファイルシステムのルートテーブルを更新できません AWS CloudFormation

Amazon FSx は、タグベースの認証を使用してマルチ AZ ファイルシステムの VPC ルートテーブルを管理します。これらのルートテーブルには `Key: AmazonFSx; Value: ManagedByAmazonFSx` のタグが付けられています。を使用して FSx for ONTAP マルチ AZ ファイルシステムを作成または更新する場合は、 `Key: AmazonFSx; Value: ManagedByAmazonFSx` タグを手動で追加 AWS CloudFormation することをお勧めします。

マルチ AZ ファイルシステムにアクセスできない場合は、ファイルシステムに関連付けられている VPC ルートテーブルに `Key: AmazonFSx; Value: ManagedByAmazonFSx` のタグが付いているかどうかを確認してください。タグが付いていないと、Amazon FSx はそのルートテーブルを更新することができません。その結果、フェイルオーバーイベントが発生したときに、管理ポートとデータポートのフローティング IP アドレスをアクティブファイルサーバーにルーティングできなくなります。ファイルシステムの Amazon VPC のルートテーブルの更新に関する詳細については、ファイルシステムの更新 を参照してください。

別の VPC のクライアントから iSCSI 経由でファイルシステムにアクセスできない

別の VPC のクライアントから [Internet Small Computer Systems Interface] (インターネットスモールコンピュータシステムインターフェイス) iSCSI 経由でファイルシステムにアクセスす

るには、ファイルシステムに関連付けられている VPC とクライアントが存在する VPC の間で、Amazon VPC ピアリングまたは AWS Transit Gateway を設定することができます。詳細については、Amazon Virtual Private Cloud ガイドの「VPC ピアリング接続の作成と受け入れ」を参照してください。

所有アカウントが VPC サブネットの共有を解除しました

共有されている VPC サブネット内にファイルシステムを作成した場合、所有アカウントが VPC サブネットの共有を解除している可能性があります。

所有者アカウントが VPC サブネットの共有を解除した場合、そのファイルシステムのコンソールに次のメッセージが表示されます。

```
The vpc ID vpc-012345abcde does not exist
```

所有アカウントに連絡して、サブネットを再共有してもらう必要があります。

別の VPC またはオンプレミスのクライアントから NFS、SMB、ONTAP CLI、ONTAP REST API 経由でファイルシステムにアクセスできない

別の VPC またはオンプレミスのクライアントからネットワークファイルシステム (NFS)、サーバーメッセージブロック (SMB)、または NetApp ONTAP CLI と REST API 経由でファイルシステムにアクセスするには、ファイルシステムに関連付けられている VPC とクライアントが存在するネットワーク AWS Transit Gateway との間で を使用してルーティングを設定する必要があります。詳細については、「データへのアクセス」を参照してください。

ストレージ仮想マシン (SVM) をアクティブディレクトリに接続させることができません

SVM をアクティブディレクトリ (AD) に接続できない場合は、まず SVM を Microsoft アクティブディレクトリに接続する を確認します。SVM をアクティブディレクトリに接続できない原因としてよくある問題については、それぞれの状況で生成されるエラーメッセージと共に以下で説明しています。

トピック

- SVM の NetBIOS 名が、ホームドメインの NetBIOS 名と同じである。
- SVM が既に別のアクティブディレクトリに接続している

- SVM の NetBIOS 名が既に使用されているため、Amazon FSx がアクティブディレクトリのドメインコントローラーに接続できない
- Amazon FSx が、アクティブディレクトリドメインコントローラーと通信できない
- ポート要件またはサービスアカウントのアクセス許可が十分でないため、Amazon FSx がアクティブディレクトリに接続できない
- サービスアカウントの認証情報が無効なため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できません
- サービスアカウントの認証情報が不十分なため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できない
- Amazon FSx が、Active Directory DNS サーバーまたはドメインコントローラーと通信できない
- アクティブディレクトリのドメイン名が無効なため、Amazon FSx がはアクティブディレクトリと通信できない。
- サービスアカウントが、SVM アクティブディレクトリ設定で指定されている管理者グループにアクセスできない
- 指定された組織単位が存在しないか、アクセスできないため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できません

SVM の NetBIOS 名が、ホームドメインの NetBIOS 名と同じである。

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx は、アクティブディレクトリとの接続を確立できません。これは、指定したサーバー名がホームドメインの NetBIOS 名であることが原因です。この問題を解決するには、ホームドメインの NetBIOS 名とは異なる SVM の NetBIOS 名を選択してください。その後、SVM を再度アクティブディレクトリに接続してみてください。

この問題を解決するには、AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順に従って、SVM をアクティブディレクトリに再度接続してください。SVM には、必ずアクティブディレクトリのホームドメインの NetBIOS 名とは異なる NetBIOS 名を使用してください。

SVM が既に別のアクティブディレクトリに接続している

SVM をアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx は、アクティブディレクトリとの接続を確立できません。これは、SVM が既にドメインに接続しているために発生しています。この SVM を別のドメインに接続するには、ONTAP CLI または REST API を使用して、この SVM のアクティブディレクトリへの接続を解除することができます。その後、SVM を別のアクティブディレクトリに再度接続してみてください。

この問題を解決するには、以下の手順を実行します。

1. NetApp ONTAP CLI を使用して、現在のアクティブディレクトリから SVM の接続を解除します。詳細については、「NetApp ONTAP CLI を使用して SVM からアクティブディレクトリの接続を解除する」を参照してください。
2. AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順に従って、SVM を新しい AD に再度接続します。

SVM の NetBIOS 名が既に使用されているため、Amazon FSx がアクティブディレクトリのドメインコントローラーに接続できない

セルフマネージド AD に接続している SVM の作成に失敗し、次のエラーメッセージが表示されます。

Amazon FSx は、アクティブディレクトリとの接続を確立できません。これは、指定した NetBIOS (コンピュータ) 名がすでにアクティブディレクトリで使用されていることが原因です。この問題を解決するには、アクティブディレクトリで使用されていない SVM の NetBIOS 名を選択し、NetBIOS (コンピュータ) を指定してから、SVM をアクティブディレクトリに再度接続してみてください。

この問題を解決するには、AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順に従って、SVM をアクティブディレクトリに再度接続してください。SVM には、必ずアクティブディレクトリでまだ使用されていない、一意の NetBIOS 名を使用してください。

Amazon FSx が、アクティブディレクトリドメインコントローラーと通信できない

SVM をセルフマネージド AD に接続させると、次のエラーメッセージが表示されて失敗します。

Amazon FSx が、アクティブディレクトリと通信できません。この問題を解決するには、Amazon FSx とドメインコントローラーの間のネットワークトラフィックが許可されていることを確認してください。その後、SVM を再度アクティブディレクトリに接続してみてください。

この問題を解決するには、次の操作を行います。

1. ネットワークの設定要件 に記載されている要件を確認し、Amazon FSx と AD 間のネットワーク通信を有効にするために必要な変更を加えます。
2. Amazon FSx が AD と通信できるようになったら、AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順に従い、SVM を AD に再度接続してみてください。

ポート要件またはサービスアカウントのアクセス許可が十分でないため、Amazon FSx がアクティブディレクトリに接続できない

SVM をセルフマネージド AD に接続させると、次のエラーメッセージが表示されて失敗します。

Amazon FSx は、アクティブディレクトリとの接続を確立できません。これは、アクティブディレクトリのポート要件が満たされていないか、指定されたサービスアカウントに、指定された組織単位を持つドメインにストレージ仮想マシンを接続させる許可がないことが原因です。この問題を解決するには、Amazon FSx ユーザーガイドの推奨に従って、ポートとサービスアカウントのアクセス許可の問題を解決してから、ストレージ仮想マシンのアクティブディレクトリ設定を更新してください。

この問題を解決するには、次の操作を行います。

1. ネットワークの設定要件 に記載されている要件を確認し、ネットワーク要件を満たすために必要となる変更を加え、必要なポートで通信が有効になっていることを確認します。
2. アクティブディレクトリサービスアカウントの要件 に記載されているサービスアカウントの要件を確認します。サービスアカウントに、指定された組織単位を使用して SVM を AD ドメインに接続させるにあたり必要となるアクセス権限が委任されていることを確認してください。
3. ポートのアクセス許可またはサービスアカウントを変更したら、AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順に従って、SVM を AD に再度接続してみてください。

サービスアカウントの認証情報が無効なため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できません

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

提供されたサービスアカウントの認証情報が無効であるため、Amazon FSx はアクティブディレクトリドメインコントローラーとの接続を確立できません。この問題を解決するには、ストレージ仮想マシンのアクティブディレクトリ設定を有効なサービスアカウントで更新します。

この問題を解決するには、、 AWS Management ConsoleAWS CLI、および API を使用した既存の SVM アクティブディレクトリ設定の更新 で説明されている手順を使用して SVM のサービスアカウント認証情報を更新します。サービスアカウントのユーザー名を入力するときは、ユーザー名のみを含め (ServiceAcct など)、ドメインプレフィックス (corp.com\ServiceAcct など) またはドメインサフィックス (ServiceAcct@corp.com など) を含めないでください。サービスアカウントのユーザー名 (CN=ServiceAcct,OU=example,DC=corp,DC=com など) を入力するときは、識別名 (DN) を使用しないでください。

サービスアカウントの認証情報が不十分なため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できない

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx は、アクティブディレクトリドメインコントローラーとの接続を確立できません。これは、アクティブディレクトリのポート要件が満たされていないか、指定されたサービスアカウントに、指定された組織単位を持つドメインにストレージ仮想マシンを接続させる許可がないことが原因です。

この問題を解決するには、指定したサービスアカウントに必要なアクセス許可が付与されていることを確認します。サービスアカウントは、ファイルシステムに接続しているドメインの OU 内でコンピュータオブジェクトを作成および削除できる必要があります。サービスアカウントには、少なくとも次の操作を実行するためのアクセス許可が必要です。

- パスワードのリセット
- アカウントのデータの読み取りと書き込みを制限する
- DNS ホスト名への書き込み許可
- サービスプリンシパル名への書き込みを許可
- コンピュータオブジェクトを作成および削除する権限
- アカウントの検証を読み書きするための検証済みの機能

正しいアクセス許可を持つサービスアカウントの作成の詳細については、「アクティブディレクトリサービスアカウントの要件」および「Amazon FSx サービスアカウントにアクセス許可を委任する」を参照してください。

Amazon FSx が、Active Directory DNS サーバーまたはドメインコントローラーと通信できない

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx が、アクティブディレクトリと通信できません。これは、Amazon FSx が提供された DNS サーバーまたはドメインコントローラーに接続できないことが原因です。この問題を解決するには、ストレージ仮想マシンのアクティブディレクトリ設定を、有効な DNS サーバーと、ストレージ仮想マシンからドメインコントローラーへのトラフィックの流れを許可するネットワーク構成で更新します。

この問題を解決するには、次の手順を使用します。

1. 地理的な制限やファイアウォールなどが原因で、アクティブディレクトリ内の一部のドメインコントローラーのみにしかアクセスできない場合は、優先ドメインコントローラを追加できます。このオプションを使用すると、Amazon FSx は優先ドメインコントローラーへの接続を試みます。`vserver cifs domain preferred-dc add` NetApp ONTAP CLI コマンドを使用して、次のように優先ドメインコントローラーを追加します。

   a. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*`management_endpoint_ip`* をファイルシステムの管理ポートの IP アドレスに置き換えます。

      ```
      [~]$ ssh fsxadmin@management_endpoint_ip
      ```

      詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

   b. 次のコマンドを入力します。

      - `-vserver vserver_name` はストレージ仮想マシン (SVM) 名を指定します。
      - `-domain domain_name` は、指定したドメインコントローラーが属するドメインの完全修飾アクティブディレクトリ名 (FQDN) を指定します。
      - `-preferred-dc IP_address,…` は、優先ドメインコントローラーの 1 つ以上の IP アドレスを、コンマ区切りのリストとして優先順に指定します。

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

次のコマンドは、SVM vs1 上の SMB サーバーが cifs.lab.example.com ドメインへの外部からのアクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラー 172.17.102.25 と 172.17.102.24 を追加します。

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. ドメインコントローラーが DNS で解決できることを確認してください。vserver services access-check dns forward-lookup NetApp ONTAP CLI コマンドを使用して、指定した DNS サーバーまたは vserver の DNS 設定でのルックアップに基づいてホスト名の IP アドレスを返します。

   a. NetApp ONTAP CLI にアクセスするには、次のコマンドを実行して、Amazon FSx for NetApp ONTAP ファイルシステムの管理ポートで SSH セッションを確立します。*management_endpoint_ip* をファイルシステムの管理ポートの IP アドレスに置き換えます。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   詳細については、「CLI ONTAP を使用したファイルシステムの管理」を参照してください。

   b. 次のコマンドを使用して ONTAP CLI アドバンスドモードを開始します。

   ```
   FsxId123456789::> set adv
   ```

   c. 次のコマンドを入力します。

   - -vserver vserver_name はストレージ仮想マシン (SVM) 名を指定します。
   - -hostname host_name は、DNS サーバーで検索するホスト名を指定します。
   - -node node_name は、コマンドが実行されるノードの名前を指定します。
   - -lookup-type は、DNS サーバーで検索する IP アドレスのタイプを指定します。デフォルトは all です。

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. SVM を AD に接続させる際に必要な情報を確認してください。
4. SVM を AD に接続させる際のネットワーク要件を確認してください。
5. ネットワークの設定要件 で説明されている手順に従って、AD DNS サーバーの正しい IP アドレスを使用して SVM の AD 設定を更新します。

アクティブディレクトリのドメイン名が無効なため、Amazon FSx がはアクティブディレクトリと通信できない。

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx が、提供された FQDN が無効であることを検出しました。この問題を解決するには、ストレージ仮想マシンのアクティブディレクトリ設定を、設定要件に準拠した FQDN で更新してください。

この問題を解決するには、次の手順を使用します。

1. SVM をアクティブディレクトリに接続するときに必要な情報 で説明されているオンプレミスのアクティブディレクトリドメイン名に関する要件を確認します。接続する AD が要件を満たしていることを確認してください。
2. AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順を使用して、SVM を AD に再度接続してください。AD ドメインの FQDN には必ず正しい形式を使用してください。

サービスアカウントが、SVM アクティブディレクトリ設定で指定されている管理者グループにアクセスできない

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx がアクティブディレクトリ設定を適用できません。これは、指定した管理者グループが存在しないか、指定されたサービスアカウントにアクセスできないことが原因です。この問題を解決するには、ネットワーク設定で SVM からアクティブディレクトリのドメインコントローラーと DNS サーバーへのトラフィックが許可されていることを確認してください。次に、SVM のアクティブディレクトリ設定を更新し、アクティブディレクトリの DNS サーバーを提供して、提供されたサービスアカウントにアクセスできるドメイン内の管理者グループを指定します。

この問題を解決するには、次の操作を行います。

1. SVM で管理アクションを実行するため、ドメイングループの提供に関する情報を確認してください。AD ドメイン管理者グループの正確な名前を使用していることを確認します。
2. AWS Management Console、、 AWS CLI および API を使用して SVM をアクティブディレクトリに接続する で説明されている手順を使用して、SVM を AD に再度接続してください。

指定された組織単位が存在しないか、アクセスできないため、Amazon FSx がアクティブディレクトリドメインコントローラーに接続できません

SVM をセルフマネージドアクティブディレクトリに接続すると、次のエラーメッセージが表示されて失敗します。

Amazon FSx は、アクティブディレクトリとの接続を確立できません。これは、指定した組織単位が存在しないか、指定されたサービスアカウントにアクセスできないためです。この問題を解決するには、ストレージ仮想マシンのアクティブディレクトリ設定を更新し、サービスアカウントに接続できる組織単位を指定します。

この問題を解決するには、次の操作を行います。

1. SVM を AD に接続させるための前提条件を確認してください。
2. SVM を AD に接続させる際に必要な情報を確認してください。
3. 正しい組織単位でこの手順を実行して、SVM を AD に再度接続してみてください。

ストレージ仮想マシンまたはボリュームは削除できません

各 FSx for ONTAP ファイルシステムには、1 つ以上のストレージ仮想マシン (SVM) を含めることができ、各 SVM には 1 つ以上のボリュームを含めることができます。リソースを削除するときは、まず、その子がすべて削除されていることを確認する必要があります。例えば、SVM を削除する前に、まず SVM 内の非ルートボリュームをすべて削除する必要があります。

> **Important**
>
> ストレージ仮想マシンは、Amazon FSx コンソール、API、および CLI を使用してのみ削除できます。ボリュームで Amazon FSx バックアップが有効になっている場合にのみ、Amazon FSx コンソール、API、CLI を使用してボリュームを削除できます。

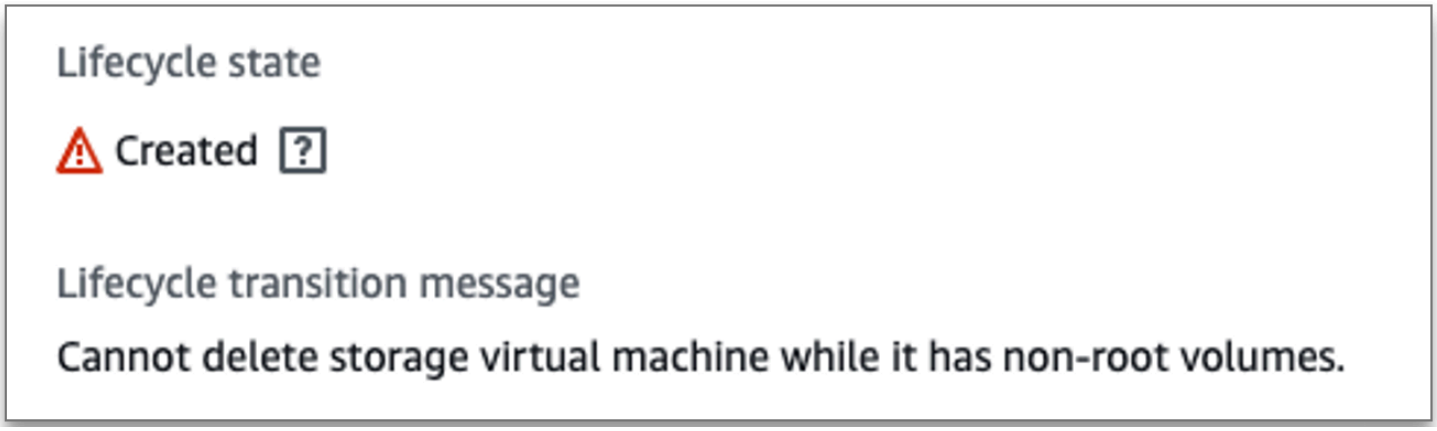
データと設定を保護するために、Amazon FSx は特定の状況で SVM とボリュームの削除を防止します。SVM またはボリュームを削除しようとして、削除リクエストが成功しなかった場合、Amazon FSx はリソースが削除されなかった理由に関する情報を AWS コンソール、 AWS Command Line Interface （ AWS CLI ）、および API に提供します。削除の障害の原因に対処した後、削除リクエストを再試行できます。

トピック

削除に失敗した場合の識別

Amazon FSx SVM またはボリュームを削除すると、通常、Amazon FSx コンソール、CLI、および API からリソースが消えるまでの最大数分間、リソースの `Lifecycle` 状態が `DELETING` に移行するのを確認できます。

リソースを削除しようと試みたところ、`Lifecycle` の状態が `DELETING` から `CREATED` に戻る場合、この動作はリソースが正常に削除されなかったことを示しています。この場合、Amazon FSx は、`CREATED` ライフサイクル状態の横のコンソールでアラートアイコンによって報告されます。アラートアイコンを選択すると、次の例に示すように、削除に失敗した理由が表示されます。



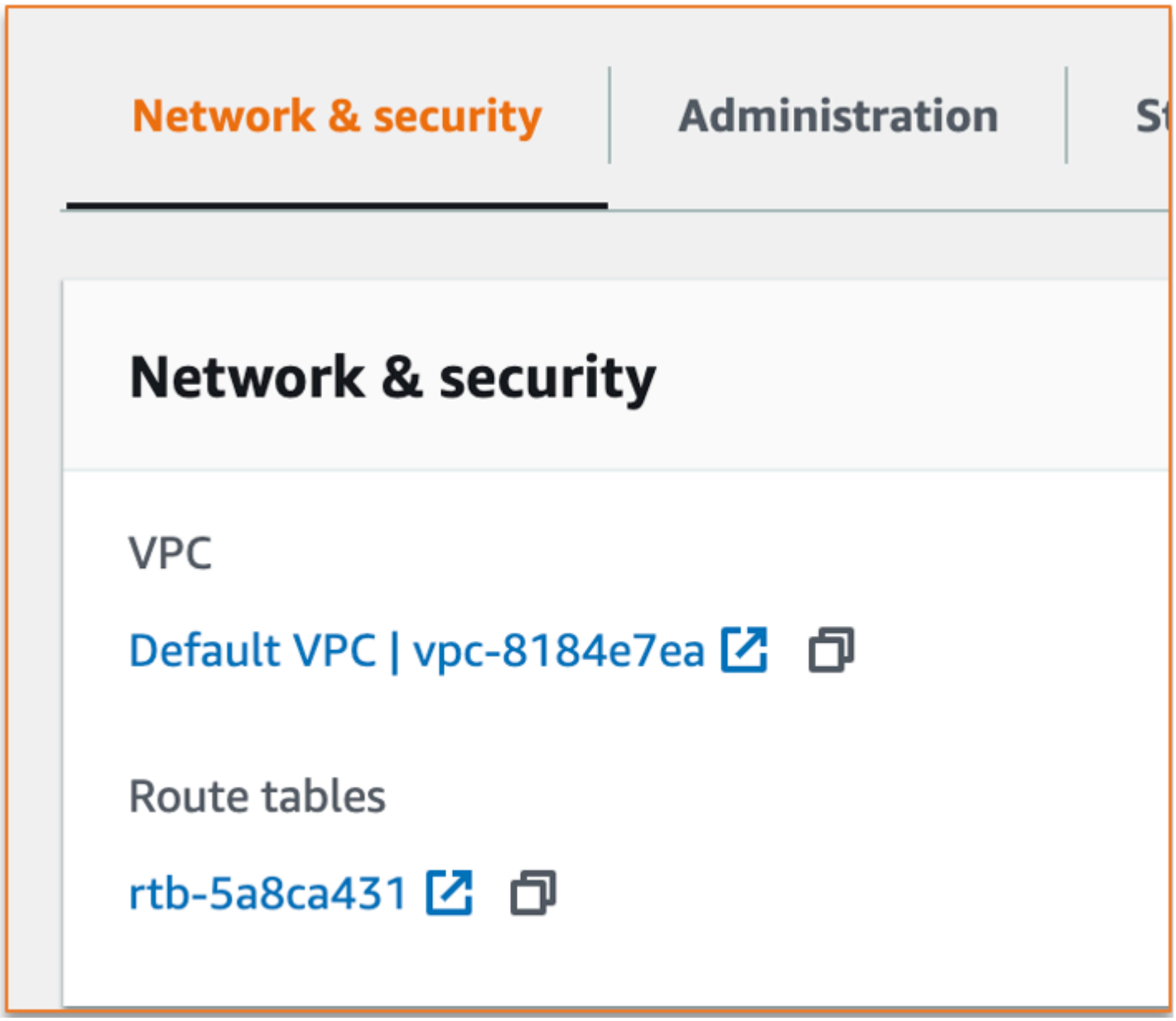
Amazon FSx が SVM とボリュームの削除を妨げる最も一般的な理由については、以下のセクションで説明します。また、これらの問題を解決する方法について step-by-step も説明します。

SVM 削除: ルートテーブルにアクセスできません

各 FSx for ONTAP ファイルシステムは、1 つ以上のルートテーブルエントリを作成して、アベイラビリティーゾーン間で自動フェイルオーバーとフェイルバックを提供します。デフォルトでは、これらのルートテーブルエントリは VPC のデフォルトルートテーブルに作成されます。オプションで、FSx for ONTAP インターフェイスを作成できる、デフォルト以外のルートテーブルを 1 つまたは複数指定できます。Amazon FSx は、ファイルシステムに関連付けられている各ルートテーブルに「AmazonFSx」タグを付けます。このタグを削除すると、Amazon FSx がリソースを削除できなくなる可能性があります。この状況が発生した場合、次の LifecycleTransitionReason が表示されます。

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Amazon FSx コンソールのファイルシステムのルートテーブルは、ネットワークとセキュリティ タブのファイルシステムの概要ページに移動して見つけることができます。



ルートテーブルリンクをクリックすると、ルートテーブルに移動します。次に、ファイルシステムに関連付けられている各ルートテーブルに、次のキーバリューペアでタグ付けされていることを確認します。

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

このタグが存在しない場合は、タグを再作成し、SVM を再度削除してください。

SVM 削除: ピアリング関係

ピアリング関係に含まれる SVM またはボリュームを削除する場合は、SVM またはボリュームを削除する前に、まずピアリング関係を削除する必要があります。この要件により、ピアリングされた SVM が異常になるのを防ぎます。ピアリング関係が原因で SVM を削除できない場合は、次の `LifecycleTransitionReason` が表示されます。

Amazon FSx は SVM ピアリングまたはトランジションピアリング関係の一部であるため、ストレージ仮想マシンを削除できません。関係を削除して再試行してください。

SVM ピアリング関係は ONTAP CLI を使用して削除できます。ONTAP CLI にアクセスするには、CLI ONTAP を使用したファイルシステムの管理 のステップを実行します。ONTAP CLI を使用して、次のステップを実行します。

1. 次のコマンドを使用して、SVM ピアリング関係を確認します。*`svm_name`* を SVM の名前に置き換えます。

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   このコマンドが成功した場合は、以下のような出力が表示されます。

   ```
               Peer        Peer                            Peering        Remote
   Vserver     Vserver     State        Peer Cluster       Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                           snapmirror     fsxDest
   svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                           snapmirror     fsxDest
   ```

```
2 entries were displayed.
```

2. 次のコマンドを使用して、SVM ピアリング関係を確認します。*svm_name* および *remote_svm_name* を実際の値に置き換えます。

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

このコマンドが成功した場合は、次の出力が表示されます。

```
Info: 'vserver peer delete' command is successful.
```

SVM またはボリュームの削除： SnapMirror

ピアリング関係を持つ SVM を、最初にピアリング関係を削除しないと削除できないのと同様に (「」を参照SVM 削除: ピアリング関係)、 SnapMirror 関係を持つ SnapMirror SVM を、最初に関係を削除しないと削除することはできません。関係を削除するには SnapMirror、ONTAP CLI を使用して、 SnapMirror 関係の宛先であるファイルシステムで次の手順を実行します。ONTAP CLI にアクセスするには、CLI ONTAP を使用したファイルシステムの管理 のステップを実行します。

> **Note**
>
> Amazon FSx バックアップは、 SnapMirror を使用して point-in-timeファイルシステムのボリュームの増分バックアップを作成します。ONTAP CLI では、バックアップのこの SnapMirror 関係を削除することはできません。ただし、この関係は、 AWS CLI、API、またはコンソールを使用してボリュームを削除すると自動的に削除されます。

1. 次のコマンドを使用して、宛先ファイルシステム上の SnapMirror 関係を一覧表示します。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

このコマンドが成功した場合は、以下のような出力が表示されます。

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
```

```
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                        Idle           -         true    -
```

2. 宛先ファイルシステムで次のコマンドを実行して、 SnapMirror 関係を削除します。

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

SVM 削除: Kerberos が有効の LIF

Kerberos が有効な論理的なインターフェイス (LIF) を持つ SVM を削除する場合は、SVM を削除する前に、まずその LIF で Kerberos を無効にする必要があります。

LIF の Kerberos は ONTAP CLI を使用して無効にすることができます。ONTAP CLI にアクセスするには、CLI ONTAP を使用したファイルシステムの管理 のステップを実行します。

1. 次のコマンドを使用して ONTAP CLI で診断モードを入力します。

```
FsxId123456789abcdef::> set diag
```

続行するかどうかを確認するメッセージが表示されたら、**y** を入力します。

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

2. Kerberos が有効になっているインターフェイスを確認します。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

このコマンドが成功した場合は、以下のような出力が表示されます。

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    enabled
```

```
5 entries were displayed.
```

3. 次のコマンドを使用して Kerberos LIF を無効にします。*svm_name* を SVM の名前に置き換えます。この SVM をアクティブディレクトリに接続させるために使用したアクティブディレクトリのユーザーネームとパスワードを入力する必要があります。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

このコマンドがした場合は、次の出力が表示されます。この SVM をアクティブディレクトリに接続させるために使用したアクティブディレクトリのユーザーネームとパスワードを入力します。続行するかどうかを確認するメッセージが表示されたら、**y** を入力します。

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. 次のコマンドを使用して、SVM で Kerberos が無効であることを確認します。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

このコマンドが成功した場合は、以下のような出力が表示されます。

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. インターフェイスが と表示されている場合はdisabled、 AWS CLI、API、またはコンソールから SVM を再度削除してみてください。

前述のコマンドを使用して LIF を削除できなかった場合は、次のコマンドを使用して Kerberos LIF を強制削除できます。*svm_name* を SVM の名前に置き換えます。

> **Important**
>
> 次のコマンドは、アクティブディレクトリ上の SVM のコンピュータオブジェクトを保持できます。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1 -force true
```

このコマンドが成功した場合は、以下のような出力が表示されます。続行するかどうかを確認するメッセージが表示されたら、**y** を入力します。

```
(vserver nfs kerberos interface disable)

Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
 "svm_name" will be deleted.
The corresponding account on the KDC will not be deleted. Do you want to continue?
 {y|n}: y
```

SVM の削除: その他の理由

FSx for ONTAP SVM は、アクティブディレクトリに接続するときにアクティブディレクトリ (AD) にコンピュータオブジェクトを作成します。場合によっては、ONTAP CLI を使用して、Active Directory から SVM を手動で接続を解除することも可能です。ONTAP CLI にアクセスするには、「CLI ONTAP を使用したファイルシステムの管理」のステップに従い、`fsxadmin` 認証情報でファイルシステムレベルの ONTAP CLI にログインします。ONTAP CLI を使用して、次のステップを実行して Active Directory から SVM の接続を解除します。

> **Important**
>
> この手順では、SVM のコンピュータオブジェクトがアクティブディレクトリ上に取り残される可能性があります。

1. 次のコマンドを使用して ONTAP CLI でアドバンストモードを開始します。

```
FsxId123456789abcdef::> set adv
```

このコマンドを実行すると、この出力が表示されます。**y** を入力して続行します。

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. 次のコマンドを使用して、アクティブディレクトリの DNS を削除します。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> DNS レコードがすでに削除されている場合、または DNS サーバーに到達できない場合、このコマンドは失敗します。その場合は、次のステップに進みます。

3. 次のコマンドを使用して DNS を無効にします。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

このコマンドが成功した場合は、次の出力が表示されます。

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. アクティブディレクトリからデバイスの接続を解除します。*svm_name* を SVM の名前に置き換えます。

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

このコマンドを実行すると、次の出力が表示されます。*CORP.EXAMPLE.COM* がドメインの名前に置き換えられています。プロンプトが表示されたら、ユーザー名とパスワードを入力します。サーバーを削除するかどうか尋ねられたら、**y** を入力します。

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

ボリュームの削除： FlexCache 関係

最初にキャッシュ FlexCache 関係を削除しない限り、関係のオリジンボリュームであるボリュームを削除することはできません。ONTAP CLI を使用して、関係がある FlexCacheボリュームを確認できます。ONTAP CLI にアクセスするには、CLI ONTAP を使用したファイルシステムの管理 のステップを実行します。

1. 次のコマンドを使用して、 FlexCache 関係を確認します。

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. 次のコマンドを使用して、キャッシュ関係を削除します。*dest_svm_name* および *dest_vol_name* を実際の値に置き換えます。

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. キャッシュ関係を削除したら、 AWS CLI、API、またはコンソールを使用して SVM を再度削除してみてください。

ボリューム容量が不十分なため、日次自動バックアップが失敗する

ボリュームの自動日次バックアップは、次のメッセージで失敗します。

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

ボリュームに十分な空きストレージ容量がないため、日次自動バックアップが失敗しています。この状態を軽減するには、ボリュームのストレージ容量を解放する必要があります。これは、状況に応じて、次の 1 つ以上のオプションを使用して実行できます。

- ボリュームのストレージ容量を増やす
- ボリュームのスナップショット予約を増やす
- スナップショットの自動削除を無効にする
- ONTAP CLI を使用してバックアップスナップショットを削除しない

ボリューム容量が不足しています

ボリュームの容量が不足している場合は、ここに示す手順を使用して状況を診断し、解決できます。

トピック

- ボリュームストレージ容量がどのように使用されているかを判別します
- ボリュームのストレージ容量の増加
- ボリュームの自動サイズ調整の使用
- ファイルシステムのプライマリストレージが満杯
- スナップショットの削除
- ボリュームの最大ファイル容量の増加

ボリュームストレージ容量がどのように使用されているかを判別します

`volume show-space` NetApp ONTAP CLI コマンドを使用して、ボリュームのストレージ容量がどのように消費されているかを確認できます。この情報は、ボリュームストレージ容量を回収または節約する方法を決定するのに役立ちます。詳細については、「ボリュームのストレージ容量をモニタリングするには (コンソール) 」を参照してください。

ボリュームのストレージ容量の増加

Amazon FSx コンソール、および Amazon FSx API を使用して AWS CLI、ボリュームのストレージ容量を増やすことができます。増加した容量でのボリュームの更新の詳細については、「ボリュームの更新」を参照してください。

または、`volume modify` NetApp ONTAP CLI コマンドを使用してボリュームのストレージ容量を増やすこともできます。詳細については、「ボリュームのストレージ容量を変更するには (コンソール)」を参照してください。

ボリュームの自動サイズ調整の使用

ボリュームの自動サイズを使用すると、ボリュームが指定された量だけ自動的に増加するか、使用されたスペースのしきい値に達したときに指定されたサイズまで増加することができます。これは、ONTAP `volume autosize` NetApp CLI コマンドを使用して、FSx for ONTAP のデフォルトの FlexVol ボリュームタイプであるボリュームタイプに対して実行できます。詳細については、「ボリュームの自動サイズ調整の有効化」を参照してください。

ファイルシステムのプライマリストレージが満杯

FSx for ONTAP ファイルシステムのプライマリストレージが満杯の場合、ボリュームに十分なストレージ容量があることが示されていても、ファイルシステムのボリュームにデータを追加することはできません。利用可能なプライマリストレージ容量は、Amazon FSx コンソールのファイルシステムの詳細ページにある [モニタリングとパフォーマンス] タブで確認できます。詳細については、「SSD ストレージ使用率のモニタリング」を参照してください。

ファイルシステムのプライマリストレージ層のサイズを大きくすると、この問題を解決できます。詳細については、「ファイルシステムの SSD ストレージと IOPS の更新」を参照してください。

スナップショットの削除

スナップショットは、デフォルトのスナップショットポリシーを使用して、ボリューム上でデフォルトで有効になります。スナップショットはボリュームのルート内の `.snapshot` ディレクトリに保存されます。スナップショットに関連するボリュームストレージ容量は、次のような方法で管理することができます：

- 「Manually delete snapshots」(スナップショットの手動削除) — スナップショットを手動で削除してストレージ容量を再利用します。

- 「Create a snapshot autodelete policy」(スナップショット自動削除ポリシーの作成) — デフォルトのスナップショットポリシーよりも積極的にスナップショットを削除するポリシーを作成します。
- 「Turn off automatic snapshots」(自動スナップショットをオフにする) — 自動スナップショットをオフにしてストレージ容量を節約します。

スナップショットの削除とストレージ容量を節約するためのスナップショットポリシーの管理の詳細については、スナップショットの削除 を参照してください。

ボリュームの最大ファイル容量の増加

FSx for ONTAP ボリュームは、使用可能な inode またはファイルポインタの数を使い切ると、ファイル容量が足りなくなることがあります。デフォルトでは、ボリューム上で使用可能な inode の数は 32 KiB のボリュームサイズごとに 1 つです。詳細については、「ボリュームファイル容量」を参照してください。

ボリューム内の inode の数は、ボリュームのストレージ容量に比例して、最大 648 GiB のしきい値まで増加します。デフォルトでは、648 GiB 以上のストレージ容量を持つボリュームは、すべて同じ数 (21,251,126) の inode を持ちます。ボリュームの最大ファイル容量を表示するには、ボリュームのファイル容量を表示する を参照してください。

648 GiB を超えるボリュームを作成し、21,251,126 よりも inode を増やしたい場合は、ボリューム上のファイルの最大数を手動で増やす必要があります。ボリュームのストレージ容量が不足している場合は、最大ファイル容量を確認することができます。ファイル容量が満杯になりつつある場合は、手動で増やすことができます。詳細については、「ボリューム上のファイルの最大数を増やすには (ONTAP CLI)」を参照してください。

ネットワーク問題のトラブルシューティング

ネットワークに問題がある場合は、こちらに示す手順を使用することで問題を診断できます。

パケットトレースをキャプチャしたい

パケットトレースとは、レイヤーから宛先までのパケットのパスを検証するプロセスのことです。パケットトレースプロセスは、次の NetApp ONTAP CLI コマンドを使用して制御します。

- network tcpdump start — パケットトレースを開始します

- network tcpdump show — 現在実行しているパケットトレースを表示します
- network tcpdump stop — 実行しているパケットトレースを停止します

これらのコマンドは、ファイルシステム上で fsxadmin のロールを持つユーザーが使用できます。

ファイルシステムからパケットトレースをキャプチャするには

1. ファイルシステムの NetApp ONTAP CLI に SSH 接続するには、「Amazon FSx for NetApp ONTAP ユーザーガイド」のNetApp ONTAP CLI の使用「」セクションに記載されているステップに従います。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 次のコマンドを使用して、ONTAP CLI に診断特権レベルを入力します。

   ```
   ::> set diag
   ```

   続行するかどうかを確認するメッセージが表示されたら、y を入力します。

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

3. パケットトレースを保存するファイルシステムの場所を特定します。ボリュームはオンラインでなければなりません。また、有効なジャンクションパスを使って名前空間にマウントされている必要があります。この基準を満たしているボリュームを、次のコマンドを使用してチェックします。

   ```
   ::*> volume show -junction-path !- -fields junction-path
   vserver volume    junction-path
   ------- --------- -------------
   fsx     test_vol1 /test_vol1
   fsx     test_vol2 /test_vol2
   fsx     test_vol2 /test_vol3
   ```

4. 最低限必要な引数でトレースを開始します。以下に置き換えます:

   - *node_name* をノードの名前 (例:) に置き換えますFsxId01234567890abcdef-01。
   - *svm_name* をストレージ仮想マシンの名前 (例:) に置き換えますfsx。
   - *Jump_path_name* をボリュームの名前 (例:) に置き換えますtest-vol1。

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> パケットトレースをキャプチャできるのは、e0e インターフェイスと Default IP スペースでのみです。FSx for ONTAP では、すべてのネットワークトラフィックが e0e インターフェイスを使用します。

パケットトレースを使用するときは、次の点に注意します。

- パケットトレースを開始するときは、トレースファイルを保存する場所へのパスを / clus/*svm_name* / の形式で含める必要があります。*junction-path-name*
- オプションで、パケットトレースのファイル名を指定します。filter_name が指定されていない場合は、*node-name* *_port-name* *_yyyymmdd_hhmmss* .trc という形式で自動的に生成されます。
- ローリングトレースが指定されている場合、ローテーションシーケンス内の位置を示す番号がファイル名の末尾に付きます。
- ONTAP CLIは、次のオプションの -pass-through 引数も受け入れます。

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
```

```
<filter-expression>
```

- フィルタ式の詳細については、「pcap-filter(7) man page」を参照してください。

5. 実行中のトレースを表示します。

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. トレースを停止します。

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. 管理者権限レベルに戻します。

```
::*> set -priv admin
::>
```

8. パケットトレースにアクセスします。

   パケットトレースは、debug network tcpdump start コマンドを使用して指定したボリュームに保存され、NFS エクスポートまたはそのボリュームに対応する SMB 共有を介してアクセスすることができます。

パケットトレースのキャプチャの詳細については、「 NetApp ナレッジベース」の「ONTAP 9.10+ でデバッグネットワーク tcpdump を使用する方法」を参照してください。

Amazon FSx for NetApp ONTAP のドキュメント履歴

- API バージョン: 2018 年 3 月 1 日
- ドキュメントの最終更新日: 2024 年 4 月 30 日

次の表は、「Amazon FSx NetApp ONTAP ユーザーガイド」の重要な変更点を示しています。ドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
ファイルシステム管理ユーザーの fsxadmin-readonly ロールのサポートが追加されました	このfsxadmin-readonly ロールは、ONTAPファイルシステム管理ユーザーが使用でき、 などのファイルシステムモニタリングアプリケーションに使用できますNetApp Harvest。詳細については、「ファイルシステム管理者のロールとユーザー」を参照してください。	2024 年 4 月 30 日
Windows ドメイン管理ユーザーの SSH パブリックキー認証のサポートが追加されました	Active Directory ドメインファイルシステムおよび SVM ユーザーで SSH パブリックキー認証を使用できるようになりました。詳細については、「https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html」を参照してください。	2024 年 4 月 30 日
スケールアウトファイルシステムで 12 個の HA ペアのサポートが追加されました	Amazon FSx for NetApp ONTAP に、スケールアウトファイルシステムにおける 12 の HA ペアのサポートが追加されました。12 個の	2024 年 3 月 4 日

	HA ペアを持つファイルシステムは、12 個の高可用性 (HA) ペアで最大 72 GBps のスループットキャパシティと 2,400,000 SSD IOPS を提供できます。詳細については、「高可用性 (HA) ペア」および「Amazon FSx for NetApp ONTAP パフォーマンス」を参照してください。	
クラウド書き込みモードのサポートが追加されました	Amazon FSx for NetApp ONTAP に、 ボリュームのクラウド書き込みモードのサポートが追加されました。詳細については、「ボリュームでのクラウド書き込みモードの有効化」を参照してください。	2024 年 2 月 6 日
による FlexGroup ボリュームのバックアップのサポートが追加されました AWS Backup	AWS Backup を使用して、FSx for ONTAP ファイルシステムの FlexGroup ボリュームをバックアップおよび復元できるようになりました。詳細については、「Amazon FSx AWS Backup での の使用」を参照してください。	2024 年 1 月 11 日

Amazon FSx が AmazonFSxFullAccess、AmazonF SxConsoleFullAccess、AmazonF SxReadOnlyAccess、AmazonF 、および AmazonF SxConsoleReadOnlyAccess管理ポリシーを更新しました AmazonFSx ServiceRolePolicy AWS	Amazon FSx は、AmazonFSxFullAccessAmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess ポリシーを更新して、`ec2:GetSecurityGroupsForVpc` アクセス許可を追加しました。 AmazonFSx ServiceRolePolicy 詳細については、「Amazon FSx の AWS マネージドポリシーの更新」を参照してください。	2024 年 1 月 9 日
Amazon FSx が AmazonFSxFullAccess と AmazonFSxConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx はAmazonFSxFullAccess および AmazonFSxConsoleFullAccess ポリシーを更新して、 `ManageCrossAccountDataReplication` アクションを追加しました。詳細については、「Amazon FSx の AWS マネージドポリシーの更新」を参照してください。	2023 年 12 月 20 日
スケールアウトメトリクスのサポートが追加されました	FSx for ONTAP は、複数の HA ペアを持つファイルシステムの Amazon CloudWatch メトリクスを提供するようになりました。詳細については、「スケールアウトファイルシステムメトリクス」を参照してください。	2023 年 11 月 26 日

スケールアウトファイルシステムのサポートが追加されました	Amazon FSx for NetApp ONTAP は、6 つの高可用性 (HA) ペアで最大 36 GBps のスループットキャパシティと 1,200,000 SSD IOPS を提供できるスケールアウトファイルシステムのサポートを追加しました。詳細については、「高可用性 (HA) ペア」および「Amazon FSx for NetApp ONTAP パフォーマンス」を参照してください。	2023 年 11 月 26 日
FlexGroup ボリュームのサポートが追加されました	Amazon FSx for NetApp ONTAP に FlexGroup ボリュームのサポートが追加されました。詳細については、「ボリュームスタイル」を参照してください。	2023 年 11 月 26 日
共有 VPC にマルチ AZ ファイルシステムのサポートが追加されました	参加者アカウントは、共有している VPC にマルチ AZ ファイルシステムを作成できるようになりました。所有者アカウントは、Amazon FSx コンソール、CLI、および API でこの機能を管理できます。詳細については、「共有サブネット」での「FSx for ONTAP ファイルシステムの作成」を参照してください。	2023 年 11 月 26 日

Amazon FSx が AmazonFSx FullAccess と AmazonFSx ConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx はAmazonFSxFullAccess および AmazonFSxConsoleFullAccess ポリシーを更新して、 `fsx:CopySnapshotAndUpdateVolume` アクセス許可を追加しました。詳細については、「Amazon FSx の AWS マネージドポリシーの更新」を参照してください。	2023 年 11 月 26 日
Amazon FSx が AmazonFSx FullAccess と AmazonFSx ConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx はAmazonFSxFullAccess ポリシーと AmazonFSxConsoleFullAccess ポリシーを更新して、 `fsx:DescribeSharedVPCConfiguration` および アクセス`fsx:UpdateSharedVPCConfiguration` 許可を追加しました。詳細については、「Amazon FSx の AWS マネージドポリシーの更新」を参照してください。	2023 年 11 月 14 日
ONTAP のロールとユーザーを追加作成するためのサポートを追加	Amazon FSx for NetApp ONTAP では、ONTAP CLI および REST API を使用する際に、ユーザー機能と権限を定義する追加の ONTAP ロールとユーザーの作成がサポートされるようになりました。詳細については、「Amazon FSx for NetApp ONTAP のロールとユーザー」を参照してください。	2023 年 9 月 6 日

追加の CloudWatch メトリクスと拡張モニタリングダッシュボードのサポートが追加されました	FSx for ONTAP では、パフォーマンスメトリクスの追加とモニタリングダッシュボードの強化によって、ファイルシステムのアクティビティを容易に把握できるようになりました。詳細については、「 によるモニタリング CloudWatch」を参照してください。	2023 年 8 月 17 日
Amazon FSx が AmazonFSx ServiceRolePolicy AWS 管理ポリシーを更新しました	Amazon FSx は AmazonFSxServiceRolePolicyの アクセス`cloudwatch:PutMetricData` 許可を更新しました。詳細については、「Amazon FSx の AWS マネージドポリシーの更新」を参照してください。	2023 年 7 月 24 日
NetApp System Manager を直接使用するためのサポートが追加されました	FSx for ONTAP ファイルシステムを、NetApp BlueXP から直接 System Manager を使って管理することができます。詳細については、BlueXP での NetApp System Manager の使用」を参照してください。	2023 年 7 月 13 日

EMS イベントのモニタリングのサポートを追加	FSx for ONTAP ファイルシステムのイベントは、NetApp ONTAP のネイティブの Events Management System (EMS) を使用することでモニタリングできます。 NetApp ONTAP CLI を使用して EMS イベントを表示できます。詳細については、「Monitoring FSx for ONTAP EMS events」を参照してください。	2023 年 7 月 13 日
SnapLock のサポートを追加	FSx for ONTAP が SnapLock ボリュームのサポートを開始しました。SnapLock は、ファイルを Write Once, Read Many (WORM) に移行することでファイルを保護する機能です。指定された保存期間中はファイルが変更されたり削除されたりすることを防ぐことができます。FSx for ONTAP は、でコンプライアンスおよびエンタープライズ保持モードをサポートします SnapLock。詳細については、「 の使用 SnapLock」を参照してください。	2023 年 7 月 13 日

転送中のデータの IPsec による暗号化のサポートを追加	FSx for ONTAPは、ファイルシステムと接続されたクライアントとの間で転送中のデータの、IPsec 暗号化を使用した暗号化をサポートしました。詳細については、「PSK 認証を使用した IPsec の設定」および「証明書認証を使用した IPsec の設定」を参照してください。	2023 年 7 月 13 日
最大ボリュームサイズが増量	FSx for ONTAP は、ボリュームの最大サイズを 100 TB から 300 TB に更新しました。詳細については、「ボリュームの自動サイズ調整を有効にする」を参照してください。	2023 年 7 月 13 日
Amazon FSx が AmazonFSx FullAccess AWS 管理ポリシーを更新しました	Amazon FSx は AmazonFSx FullAccess ポリシーを更新して、 `fsx:*` アクセス許可を削除し、特定の`fsx`アクションを追加しました。詳細については、AmazonFSxFullAccess ポリシー」を参照してください。	2023 年 7 月 13 日
Amazon FSx が AmazonFSx ConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx は AmazonFSx ConsoleFullAccess ポリシーを更新して、 `fsx:*` アクセス許可を削除し、特定の`fsx`アクションを追加しました。詳細については、AmazonFSx ConsoleFullAccess ポリシー」を参照してください。	2023 年 7 月 13 日

既存のストレージ仮想マシンをアクティブディレクトリに接続させるためのサポートが追加されました	既存のストレージ仮想マシンを Active Directory に参加させるには AWS Management Console、、 AWS CLI 、および API を使用します。詳細については、「SVM をアクティブディレクトリに接続する」を参照してください。	2023 年 6 月 13 日
シングル AZ ファイルシステムに NVMe リードキャッシュのサポートが追加されました	NVMe リードキャッシュが、米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、および欧州 (アイルランド) で、2022 年 11 月 28 日以降に作成されたスループットキャパシティ 2 GBps 以上のシングル AZ ファイルシステムでサポートされるようになりました。詳細については、「Impact of deployment type on performance」(デプロイタイプがパフォーマンスに与える影響) を参照してください。	2022 年 11 月 28 日
VPC 内の IP アドレス範囲を使用してマルチ AZ ファイルシステムを作成できるようになりました	VPC の IP アドレス範囲内にあるエンドポイントを指定することで、ONTAP ファイルシステム用のマルチ AZ FSx を作成できるようになりました。詳細については、「Creating FSx for ONTAP file systems」(ONTAP ファイルシステムの FSx を作成する) を参照してください。	2022 年 11 月 28 日

マルチ AZ ファイルシステムの VPC ルートテーブルの更新をサポートできるようになりました	新しい VPC ルートテーブルを既存のマルチ AZ FSx for ONTAP ファイルシステムに関連付け (追加) したり、既存の VPC ルートテーブルを既存のマルチ AZ FSx for ONTAP ファイルシステムから関連付け解除 (削除) したりできるようになりました。詳細については、「Updating a file system」(ファイルシステムの更新) を参照してください。	2022 年 11 月 28 日
AWS Nitro System で転送中のデータの暗号化のサポートが追加されました	米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、および欧州 (アイルランド) の Amazon EC2 インスタンスからアクセスする場合、転送中のデータは自動的に暗号化されます。詳細については、AWS 「Nitro System による転送中のデータの暗号化」を参照してください。	2022 年 11 月 28 日

DP ボリューム作成をサポートできるようになりました	Amazon FSx コンソール、または Amazon FSx API を使用して AWS CLI DP (データ保護) ボリュームを作成できるようになりました。単一ボリュームのデータを移行または保護する場合は、DP ボリュームを NetApp SnapMirror または SnapVault 関係の送信先として使用できます。詳細については、「Volume types」(ボリュームタイプ) を参照してください。	2022 年 11 月 28 日
ボリュームタグをバックアップにコピーできるようになりました	AWS CLI または Amazon FSx API で、CopyTagsToBackups を有効にすることでボリュームからバックアップにタグを自動的にコピーできるようになりました。詳細については、「Copying tags to backups」(タグをバックアップにコピーする) を参照してください。	2022 年 11 月 28 日

スナップショットポリシーの選択がサポートされるようになりました	Amazon FSx コンソール、または Amazon FSx API を使用してボリュームを作成または更新するときに AWS CLI、3 つの組み込みスナップショットポリシーから選択できるようになりました。ONTAP CLI または REST API で作成したカスタムスナップショットポリシーを選択することもできます。詳細については、「Snapshot policies」(スナップショットポリシー) を参照してください。	2022 年 11 月 28 日
追加のファイルシステムのスループットキャパシティ オプションがサポートされるようになりました	FSx for ONTAP が、米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、および欧州 (アイルランド) で、2022 年 11 月 28 日以降に作成したファイルシステムのスループットキャパシティ 4,096 MBps をサポートしました。詳細については、「スループットキャパシティがパフォーマンスに与える影響」を参照してください。	2022 年 11 月 28 日

追加の SSD IOPS がサポートされるようになりました	FSx for ONTAP が、米国東部 (オハイオ) リージョン、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、および欧州 (アイルランド) で、2022 年 11 月 28 日以降に作成したファイルシステムに対して 160,000 SSD IOPS をサポートしました。詳細については、「スループットキャパシティがパフォーマンスに与える影響」を参照してください。	2022 年 11 月 28 日
VMware Cloud on の外部データストアとして FSx for ONTAP を使用するためのサポートが追加されました AWS	FSx for ONTAP は、VMware Cloud on AWS Software-Defined Data Center (SDDCs) の外部データストアとして使用できます。この追加サポートにより、VMware Cloud on AWS ワークロードのコンピューティングリソースとは別にストレージを柔軟にスケールアップまたはスケールダウンできます。詳細については、「Using VMware Cloud with FSx for ONTAP」(FSx for ONTAP で VMware Cloud を使用する) を参照してください。	2022 年 8 月 30 日

ファイルシステムのストレージ容量を自動的に引き上げる	AWSが開発したカスタマイズ可能な AWS CloudFormation テンプレートを使用して、使用済み SSD ストレージ容量が指定したしきい値を超えたときにファイルシステムのストレージ容量を自動的に増やします。詳細については、「ストレージ容量の動的な引き上げ」を参照してください。	2022 年 6 月 3 日
Amazon FSx が と統合されました AWS Backup	AWS Backup を使用して、ネイティブ Amazon FSx バックアップの使用に加えて、FSx ファイルシステムのバックアップと復元が可能になりました。詳細については、「Amazon FSx AWS Backup での の使用」を参照してください。	2022 年 5 月 18 日
単一のアベイラビリティーゾーン ONTAP ファイルシステムのデプロイにサポートが追加されました	FSx for ONTAP シングル AZ ファイルシステムを作成できます。このファイルシステムは、単一のアベイラビリティーゾーン (AZ) 内で高い可用性と耐久性とを提供できるように設計されています。詳細については、「ファイルシステムのデプロイを選択する」を参照してください。	2022 年 4 月 13 日

AWS PrivateLink インターフェイス VPC エンドポイントのサポートが追加されました	インターフェイス VPC エンドポイントを使用し、インターネット経由でトラフィックを送信せずに、VPC から Amazon FSx API にアクセスできます。詳細については、「Amazon FSx and interface VPC endpoints」を参照してください。	2022 年 4 月 5 日
既存の ONTAP ファイルシステムのスループットキャパシティを変更するためのサポートが追加されました	既存の ONTAP ファイルシステムで使用可能なスループットキャパシティを変更できるようになりました。詳細については、「スループットキャパシティの管理」を参照してください。	2022 年 3 月 30 日
SSD ストレージ容量とプロビジョンド IOPS スケーリングのサポートが追加されました	ストレージと IOPS の要件が変化するにつれて、SSD ストレージ容量と既存の FSx for ONTAP ファイルシステムのプロビジョンド IOPS を増やすことができるようになりました。詳細については、「ストレージ容量の管理、プロビジョンド IOPS」を参照してください。	2022 年 1 月 25 日

Amazon CloudWatch メトリクスのサポートが追加されました	Amazon を使用してファイルシステムをモニタリングできます。Amazon は CloudWatch、FSx for ONTAP から raw データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工します。詳細については、「Amazon によるモニタリング CloudWatch」を参照してください。	2022 年 1 月 19 日
追加ファイルシステムのスループットオプションのサポートが追加されました	FSx for ONTAP は、ファイルシステムのスループットに対して 128 MB / 秒 および 256 MB / 秒のオプションをサポートするようになりました。詳細については、「スループットキャパシティがパフォーマンスに与える影響」を参照してください。	2021 年 11 月 30 日
Amazon FSx for NetApp ONTAP が一般公開されました	FSx for ONTAP は、 NetApp の ONTAP ファイルシステム上に構築された、信頼性が高く、スケーラブルで、パフォーマンスが高く、機能豊富なファイルストレージを提供するフルマネージドサービスです。ファイル NetApp システムの使い慣れた機能、パフォーマンス、機能、APIs に、フルマネージド AWS サービスの俊敏性、スケーラビリティ、シンプルさを提供します。	2021 年 9 月 2 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。