aws

ONTAP のユーザーガイド

FSx for ONTAP



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

FSx for ONTAP: ONTAP のユーザーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスに関連して、ユーザーに混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用してはなりません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Amazon FSx for NetApp ONTAP とは何ですか? ... 1
FSx for ONTAP の特徴 ... 2
セキュリティとデータ保護 ... 3
モニタリングツール ... 3
FSx for ONTAP の料金 ... 4
AWS re:Post での ONTAP 用 FSx ... 4
Amazon FSx を初めてご使用のユーザーですか？ ... 4
使用方法 ... 5
ファイルシステム ... 5
ストレージ仮想マシン ... 5
ボリューム ... 6
ストレージ階層 ... 6
データ階層化 ... 7
ストレージ効率 ... 7
データへのアクセス ... 7
FSx for ONTAP リソースの管理 ... 7
開始方法 ... 9
設定 ... 9
にサインアップする AWS アカウント ... 9
管理アクセスを持つユーザーを作成する ... 10
次のステップ ... 11
FSx for ONTAP ファイルシステムを作成する ... 12
Microsoft Active Directory に参加している SVM を作成する ... 15
ファイルシステムのマウント ... 16
リソースのクリーンアップ ... 17
AWS リージョン ... 19
データへのアクセス ... 23
サポートされているクライアント ... 24
ブロックストレージプロトコルの使用 ... 25
内からのデータへのアクセス AWS クラウド ... 26
同じ VPC からのデータへのアクセス ... 26
別の VPC からデータにアクセスする ... 26
オンプレミスからデータにアクセスする ... 31
オンプレミスから NFS、SMB、ONTAP CLI および API へのアクセス ... 31

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 ... 32
VPC の外部からマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する ... 33
オンプレミスからマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する ... 34
Linux クライアントでのマウント ... 35
/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 ... 37
Windows クライアントでのマウント ... 38
前提条件 ... 39
macOS クライアントでのマウント ... 40
Linux 用 iSCSI のプロビジョニング ... 43
開始する前に ... 43
Linux コストに iSCSI をインストールして設定する ... 45
FSx for ONTAP ファイルシステムで iSCSI を設定する ... 47
Linux クライアントにiSCSI LUN をマウントします ... 49
Windows 用 iSCSI のプロビジョニング ... 55
Windows クライアントで iSCSI を設定する ... 57
FSx for ONTAP ファイルシステムで iSCSI を設定する ... 57
Windows クライアントに iSCSI LUN をマウントします ... 59
iSCSI 設定の検証 ... 63
Linux 用の NVMe/TCP のプロビジョニング ... 64
開始する前に ... 65
Linux ホストに NVMe をインストールして設定する ... 66
FSx for ONTAP ファイルシステムで NVMe を設定する ... 66
Linux クライアントに NVMe デバイスをマウントする ... 69
S3 アクセスポイントを介したデータへのアクセス ... 75
AWS リージョン FSx for ONTAP の Amazon S3 アクセスポイントを使用する ... 76
命名規則、制限、制限 ... 76
アクセスポイントの参照 ... 78
アクセスポイントの互換性 ... 80
アクセスの管理 ... 84
アクセスポイントの作成 ... 87
アクセスポイントの管理 ... 93
アクセスポイントの使用 ... 96
アクセスポイントのトラブルシューティング ... 99
他の AWS サービスからのデータへのアクセス ... 99
Amazon WorkSpaces の使用 ... 100

Amazon ECS を使用する 106
Amazon EVS の使用 109
VMware Cloud を使用する 109
可用性、耐久性、デプロイオプション 110
ファイルシステムのデプロイタイプを選択 110
シングル AZ デプロイデプロイタイプ 110
マルチ AZ デプロイのタイプ 111
ファイルシステム生成の選択 113
FSx for ONTAP のフェイルオーバープロセス 114
ファイルシステムでフェイルオーバーをテストする 115
ネットワークリソース 115
サブネット 115
ファイルシステム Elastic Network Interface 115
パフォーマンス 118
パフォーマンスの測定 118
レイテンシー 118
スループットと IOPS 118
SMB マルチチャネルおよび NFS nconnect のサポート 119
パフォーマンスの詳細 119
デプロイタイプがパフォーマンスに与える影響 121
ストレージ容量のパフォーマンスへの影響 123
スループット容量がパフォーマンスに与える影響 124
例: ストレージ容量とスループットキャパシティ 130
リソースの管理 132
ストレージ容量の管理 132
ストレージ階層 133
ファイルシステムのストレージ容量の選択 134
ファイルシステムのストレージ容量および IOPS 138
ボリュームストレージ容量 164
ファイルシステムの管理 189
ファイルシステムリソース 190
ファイルシステムの作成 192
ファイルシステムの更新 206
HA ペアの管理 210
NVMe キャッシュの管理 218
ネットワークタイプの管理 219

ファイルシステムの詳細のモニタリング 221
ファイルシステムの削除 223
SVM の管理 223
ファイルシステムあたりの SVM の最大数 224
SVM の作成 225
SVM の更新 229
SVM Microsoft Active Directory 設定の管理 231
ファイルアクセスの監査 233
ワークグループのセットアップ 245
SVM の詳細のモニタリング 252
SVM の削除 252
ボリュームの管理 254
ボリュームスタイル 255
ボリュームの種類 257
ボリュームセキュリティスタイル 258
ボリュームの作成 259
ボリュームの更新 264
ボリュームの移動 268
ボリュームのモニタリング 272
ボリュームの削除 274
iSCSI LUN の作成 277
次のステップ 278
メンテナンスウィンドウの更新 279
スループット容量の管理 280
スループット容量を変更するタイミング 281
同時リクエストの処理方法 282
スループットキャパシティの更新 283
スループット容量の変更のモニタリング 284
SMB 共有の管理 286
NetApp アプリケーションでの管理 288
NetApp アカウントへのサインアップ 288
の使用NetApp Console 290
NetApp ONTAP CLI の使用 290
ONTAP REST API の使用 294
リソースのタギング 294
タグの基本 295

リソースのタグ付け ... 296
バックアップへのタグのコピー ... 297
タグの制限 ... 298
許可とタグ ... 298
データの保護 ... 299
ボリュームのバックアップ ... 299
バックアップの仕組み ... 300
ストレージの要件 ... 301
日次自動バックアップ ... 301
ユーザー主導のバックアップ ... 302
バックアップへのタグのコピー ... 303
の使用AWS Backup ... 303
バックアップの復元 ... 304
バックアップのパフォーマンス ... 306
SnapLock ボリュームのバックアップ ... 307
ユーザー起動のバックアップの作成 ... 307
バックアップの復元 ... 308
データのサブセットの復元 ... 311
ボリューム復元の進行状況のモニタリング ... 312
バックアップの削除 ... 315
ボリュームスナップショットの使用 ... 316
スナップショットポリシー ... 317
スナップショットからのファイルの復元 ... 318
共通スナップショットの表示 ... 319
スナップショットの予約スペースの更新 ... 320
自動スナップショットの無効化 ... 321
スナップショットの削除 ... 323
スナップショットの削除 ... 323
スナップショットリザーブ ... 325
Autonomous Ransomware Protection によるデータの保護 ... 325
ARP の仕組み ... 326
ARP が検索する対象 ... 326
ARP による疑わしい攻撃への対応方法 ... 327
ARP の有効化 ... 328
ARP アラートへの対応 ... 329
ARP の EMS アラートの理解 ... 331

SnapLock を使用したデータの保護 332
SnapLock の仕組み 333
SnapLock コンプライアンスについて 338
SnapLock エンタープライズ について 339
SnapLock 保存期間について理解する 340
ファイルを WORM にコミットする 342
FlexCache によるデータの複製 348
FlexCache の仕組み 348
FlexCache書き込みモード 349
FlexCache ボリューム作成の概要 349
「FlexCache」の作成 350
スケジュールされたレプリケーションに SnapMirror を使用する 356
NetApp Consoleを使用したレプリケーションのスケジュール 357
ONTAPCLI を使用した複製のスケジュール 357
請求および使用状況レポート 358
FSx for ONTAP 請求レポート 358
FSx for ONTAP 使用状況レポート 361
ファイルシステムのモニタリング 366
CloudWatch によるモニタリング 367
CloudWatch メトリクスへのアクセス 368
Amazon FSx コンソールでのモニタリングする 370
ファイルシステムのメトリクス 382
第 2 世代のファイルシステムメトリクス 399
ボリュームメトリクス 417
EMS イベントのモニタリング 426
EMS イベントの概要 426
EMS イベントを表示する 427
Syslog サーバーへの EMS イベント転送 434
データインフラストラクチャインサイトによるモニタリング 436
Harvest と Grafana によるモニタリング 437
Harvest と Grafana の開始方法 437
サポートされている Harvest ダッシュボード 437
サポートされていない Harvest ダッシュボード 439
CloudFormation テンプレート 439
Amazon EC2 インスタンスタイプ 440
デプロイ手順 440

Grafana にログインする 444
Harvest と Grafana のトラブルシューティング 444
によるモニタリングAWS CloudTrail 447
CloudTrail 内の Amazon FSx 情報 448
Amazon FSx ログファイルエントリの概要 449
アクティブディレクトリの使用 452
セルフマネージド Active Directory の前提条件 453
セルフマネージド Active Directory の要件 453
ネットワークの設定要件 453
アクティブディレクトリサービスアカウントの要件 455
セルフマネージド Active Directory のベストプラクティス 457
Amazon FSx サービスアカウントにアクセス許可を委任する 457
AD 設定を最新の状態に保つ 459
セキュリティグループで VPC 内のトラフィックを制限する 459
アウトバウンドセキュリティグループのルールの作成 459
を使用した Active Directory 認証情報の保存 AWS Secrets Manager 460
SVM を Active Directory に結合する仕組み 468
Active Directory に必要な情報 469
SVM Active Directory 設定の管理 471
SVM を Active Directory に結合する 471
Active Directory 設定の更新 475
NetApp CLI を使用して Active Directory 設定を更新する 476
Amazon FSx への移行 482
SnapMirror を使用した移行 482
始める前に 484
宛先ボリュームの作成 485
出典と宛先のクラスター間 LIF をレコードします 487
出典と宛先の間でクラスターピアリングを確立する 487
SVM ピアリング関係を作成する 488
SnapMirror 関係を作成する 489
FSx for ONTAP ファイルシステムへのデータの転送 490
Amazon FSx にカットオーバー 491
AWS DataSync を使用したファイル移行 492
前提条件 493
DataSync 移行の基本ステップ 494
セキュリティ 495

データ保護 496
FSx for ONTAP でのデータ暗号化 497
保管中の暗号化 497
Encrypting data in transit 499
ID とアクセス管理 521
オーディエンス 522
アイデンティティを使用した認証 522
ポリシーを使用したアクセスの管理 523
FSx for ONTAP と IAM 525
アイデンティティベースのポリシーの例 530
IAM のトラブルシューティング 533
サービスにリンクされたロールの使用 535
Amazon FSx でのタグの使用 541
AWS 管理ポリシー 547
AmazonFSxServiceRolePolicy 548
AmazonFSxDeleteServiceLinkedRoleAccess 548
AmazonFSxFullAccess 548
AmazonFSxConsoleFullAccess 549
AmazonFSxConsoleReadOnlyAccess 550
AmazonFSxReadOnlyAccess 551
ポリシーの更新 552
Amazon VPC によるファイルシステムアクセスコントロール 565
Amazon VPC セキュリティグループ 565
コンプライアンス検証 568
インターフェイス VPC エンドポイント 568
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 569
Amazon FSx API 用のインターフェイス VPC エンドポイントの作成 569
Amazon FSx 用の VPC エンドポイントポリシーの作成 570
耐障害性 570
バックアップと復元 571
スナップショット 571
アベイラビリティーゾーン 571
インフラストラクチャセキュリティ 572
ウイルス対策ソフトウェアの仕様 573
ONTAP ロールとユーザー 573
ファイルシステム管理者のロールとユーザー 573

SVM 管理者ロールとユーザー 575
Active Directory を使用した ONTAP ユーザーの認証 577
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 578
ONTAP ユーザーの作成 579
SVM ロールの作成 582
ONTAP ユーザーの Active Directory 認証の設定 583
パブリックキー認証を設定する 585
パスワード要件の更新 587
fsxadmin アカウントのパスワードの更新が失敗する 587
クォータ 589
増加可能なクォータ 589
ファイルシステムあたりのリソースクォータ 591
トラブルシューティング 598
設定ミスのあるファイルシステム 598
VPC 共有が無効 598
マルチ AZ ファイルシステムを作成できない 599
SSD 階層の使用率が 90% を超える 599
ファイルシステムにアクセスできません 600
ルートテーブルタグがない 600
ルートが多すぎます 601
サーバーへのルートがありません 601
変更または削除された ENI 601
削除された ENI 602
インバウンドルールがない 602
欠落しているアウトバウンドルール 602
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 602
マルチ AZ ルートテーブルを更新できない 603
iSCSI にアクセスできない 603
非共有 VPC サブネット 603
異なる VPC およびオンプレミスからアクセスできない NFS、SMB、ONTAP CLI、API 604
SVM の設定ミス 604
SVM にオフラインボリュームがあります 604
SVM には SCSI LUN または NVMe/TCP ネームスペースを持つオフラインボリュームがあります 604
AWS Secrets Manager シークレットまたは KMS キーが正しく設定されていない 605

SSD の減少についての問題のトラブルシューティング 605
SSD の減少が一時停止–高使用率 606
SSD の減少を一時停止しています – FlexClone 606
ボリュームのリダイレクトが減少中に失敗しました 607
SSD の減少に時間がかかりすぎる 607
SVM をアクティブディレクトリに加えることができない 608
ホームドメインと同じ SVM NetBIOS 名 609
SVM が別のアクティブディレクトリに接続しています 609
SVM NetBIOS 名は既に使用されています 609
Amazon FSx は、 で Active Directory サービスアカウントの認証情報にアクセスできません AWS Secrets Manager 610
FSx が Active Directory ドメインコントローラーに到達できない 612
ポート設定またはサービスアカウントのアクセス許可が不十分です 612
サービスアカウントの認証情報が無効 613
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 613
アクティブディレクトリ DNS サーバーまたはドメインコントローラーにアクセスできません 614
Active Directory ドメイン名が無効です 616
サービスアカウントが Active Directory の管理者グループにアクセスできません 617
ご指定の OU は無効です 618
SVM またはボリュームを削除できません 618
削除に失敗した場合の識別 619
SVM 削除: ルートテーブルにアクセスできません 619
SVM 削除: ピアリング関係 620
SVM またはボリュームの削除: SnapMirror 621
SVM 削除: Kerberos が有効の LIF 622
SVM の削除: その他の理由 624
ボリューム削除: FlexCache 関係 626
ボリュームの設定ミス 627
ボリュームが 98% を超えています 627
ブロックストレージボリュームがオフラインです 627
オフラインFlexCacheオリジンボリューム 628
SnapMirror 関係のあるオフラインボリューム 628
ブロックストレージボリュームが制限されています 629
制限された FlexCache オリジンボリューム 629

SnapMirrorレーションシップを持つ制限付きボリューム 630
ボリュームのストレージ不足 630
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 630
ボリュームのストレージ容量の増加 631
ボリュームの自動サイズ調整の使用 631
ファイルシステムのプライマリストレージが満杯 631
スナップショットの削除 631
ボリュームの最大ファイル容量の増加 632
失敗したボリュームバックアップ 633
削除されたボリュームの復旧 633
ネットワーク問題のトラブルシューティング 633
パケットトレースをキャプチャしたい 633
ドキュメント履歴 637
..... dclxiii

Amazon FSx for NetApp ONTAP とは何ですか?

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、信頼性が高く、スケーラブルで、パフォーマンスが高く、機能が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、および API オペレーションと、フルマネージド AWS のサービス の俊敏性、スケーラビリティ、およびシンプルさを兼ね備えています。

Amazon FSx for NetApp 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、多機能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しているお客様にとって、FSx for ONTAP は、アプリケーションのコードやデータ管理方法を変更することなく、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 AWS 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、AWS Identity and Access Management (IAM)、Amazon WorkSpaces、AWS Key Management Service (AWS KMS)、AWS CloudTrail などの他の AWS サービスとの豊富な統合も提供します。

トピック

- FSx for ONTAP の特徴
- セキュリティとデータ保護
- モニタリングツール
- FSx for ONTAP の料金
- AWS re:Post での ONTAP 用 FSx
- Amazon FSx を初めてご使用のユーザーですか？

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 GB/秒 (GBps) の throughput per file system(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)、不揮発性メモリエクスプレス (NVMe) 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
- 可用性と耐久性に優れたマルチ AZ およびシングル AZ 導入オプション
- 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
- ファイルシステムにアクセスして管理するための IPv4 専用とデュアルスタック (IPv4 と IPv6 の両方をサポート) の 2 つのネットワークタイプオプションのサポート
- NetAppのSnapMirrorレプリケーション機能のサポート
- NetAppのFlexCacheオンプレミスキャッシュソリューションのサポート

- ネイティブの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 マネジメントコンソール、 AWS Command Line Interface 、(AWS CLI)、および SDKs
  - NetApp ONTAP CLI、REST API、NetApp コンソール

セキュリティとデータ保護

Amazon FSx for NetApp ONTAP のセキュリティ に関連して、責任共有モデルが採用されています。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。

FSx for ONTAP はデータ保護、セキュリティ、およびアクセス制御機能をサポートしています:

- AWS KMS keysを使用したファイル システム データとバックアップのための保存データの暗号化
- 転送中のデータの暗号化:
  - SMB Kerberos
  - IPSEC
  - ニトロベースの暗号化
- 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承認
- ファイルアクセスの監査
- NetAppSnapLockWORM には、Compliance と Enterprise という 2 種類の保持モードがあります

詳細については、「Amazon FSx for NetApp ONTAP におけるデータ保護」および「データの保護」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。

モニタリングツール

モニタリングツールには、CloudWatch、CloudTrail、ONTAPEMS イベント、NetAppデータインフラストラクチャインサイト、NetAppHarvest などがあります。

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、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。

AWS re:Post での ONTAP 用 FSx

Amazon FSxの使用中に問題が発生した場合は、 AWS re:Post を使用して FSx for ONTAP 質問に対する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. AWS を初めて使用する場合は AWS アカウント をセットアップするための「FSx for ONTAP の設定」を参照してください。
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 の使用

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、詳しい説明、重要な実装の詳細、ステップバイステップの設定手順を含むセクションへのリンクを提供します。

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、ONTAP リソースのプライマリ FSx で、オンプレミス NetApp ONTAP クラスターに類似しています。ファイルシステムの SSD スループットキャパシティ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、その構成に応じて 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。第 1 世代 FSx for ONTAP ファイルシステムと第 2 世代マルチ AZ ファイルシステムは、1 つの HA ペアをサポートしています。第 2 世代シングル AZ ファイルシステムは、最大 12 の HA ペアをサポートしています。詳細については、「高可用性 (HA) ペアの管理」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 上にホストされる論理コンテナであり、そのコンテナ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することで、データがどのストレージ階層に格納されているかに関係なく、保存可能な物理データの量を決定します。また、ボリュームタイプは、RW (読み取り書き込み可能) または DP (データ保護) のいずれかに設定します。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できます。

Sx for ONTAP ボリュームとはボリュームに格納されているデータのストレージ容量のみを消費するシンプロビジョニングを指します。シンプロビジョニングボリュームでは、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、空き領域はファイルシステムに解放されます。例えば、10 TiB の空きストレージ容量で構成されたファイルシステムに、3 つの 10 TiB ボリュームを作成できます。ただし、3 つのボリューム内に格納されたデータの合計容量が常に 10 TiB を超えない限りです。ボリュームに物理的に格納されているデータ量は、ストレージ容量の全体的な消費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。ストレージの必要量が増加した場合、ファイルシステムの SSD ストレージ容量を拡張できます。第 2 世代のファイルシステムでは、高性能ストレージ要件が変更されたときに SSD ストレージ容量を減らすこともできます。これにより、ストレージコストを最適化できます。詳細については、「ファイルシステムのストレージ容量および IOPS」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 と容量プールストレージ階層間で自動的にデータを移動させるプロセスです。各ボリュームには、データが非アクティブになったとき (コールド) に容量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は、データがいつ非アクティブ (コールド) になるかを決定します。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性機能 (圧縮、重複排除) をサポートして、データが消費するストレージ容量を削減します。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、「ストレージ効率」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。また、Non-Volatile Memory Express (NVMe) および Internet Small Computer Systems Interface (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、「FSx for ONTAP 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。AWS と NetApp ONTAP 管理ツールの両方を使用して FSx for ONTAP リソースを管理することができます

- AWS 管理ツール
  - AWS マネジメントコンソール
  - AWS Command Line Interface (AWS CLI)
  - Amazon FSx API と SDK

    - AWS CloudFormation
- NetApp 管理ツール:
    - NetApp コンソール
    - 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。

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を説明します。この入門演習では、次のステップが含まれます。

1. にサインアップ AWS アカウント し、アカウントに管理ユーザーを作成します。
2. Amazon FSx コンソールを使用して Amazon FSx for NetApp ONTAP ファイルシステムを作成します。
3. Amazon EC2 Linux インスタンスからファイルシステムをマウントします。
4. 作成した リソースをクリーンアップします。

トピック

- FSx for ONTAP の設定
- Amazon FSx for NetApp ONTAP ファイルシステムを作成する
- 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
- リソースのクリーンアップ

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
- 管理アクセスを持つユーザーを作成する
- 次のステップ

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

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] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

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、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM アイデンティティセンター、 を有効にして管理ユーザーを作成します。

を保護する 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 マネジメントコンソールとして 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 (コンソール) の仮想 MFA デバイスを有効にする」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 アイデンティティセンター ユーザーガイド」の「AWS IAM アイデンティティセンターの有効化」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、AWS IAM アイデンティティセンター 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」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 「 アクセスポータルにサインインする」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 アイデンティティセンター ユーザーガイド」の「アクセス許可セットを作成する」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 アイデンティティセンター ユーザーガイド」の「グループの追加」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 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。サービス推奨の設定で 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、[Quick create] (クイック作成) オプションを使用します。

[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を結合している SVM も含まれます。選択したデプロイタイプと作成時に追加した HA ペアの数に応じて、高可用性 (HA) ペアを追加することもできます。

> **Note**
>
> クイック作成 オプションで作成された FSx for ONTAP ファイルシステムは、`IPv4` の ネットワークタイプ を使用します。`Dual-stack` (IPv4 と IPv6 の両方をサポート) の [ネットワークタイプ] でファイルシステムを作成するには、[標準作成] オプションを使用します。

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と、AWS CLI および API を使用する方法については、「」を参照してください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. [Create file system] (ファイルシステムの種類を選択) ページで、Amazon FSx for NetApp ONTAP、[Next] (次へ) の順に選択します。[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、耐久性、デプロイオプション」を参照してください。

   > **Note**
   >
   > で使用できる最新世代の FSx for ONTAP ファイルシステムがデフォルトで選択 AWS リージョン されています。標準作成オプションを使用して、ファイルシステム (使用可能な場合 AWS リージョン) の生成を指定できます。詳細については、「ファイルシステムの作成」を参照してください。

7. SSD のストレージ容量 については、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 ~ 1,048,576 の範囲の任意の整数を入力します。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。

   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を選択することもできます (デプロイタイプと HA ペアの量に応じて最大 73,728 MBps)。

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. (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

    - [VPC からの未割り当ての IPv4 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 IPv4 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。

- [VPC 外のフローティング IPv4 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。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、また、同じ VPC およびルートテーブルで別のファイルシステムによって使用されていない限り、VPC の IPv4 アドレス範囲の内側でも外側でも可能です。VPC の IP アドレス範囲内の範囲を使用することをお勧めします。

> **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。

11. 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。
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、デフォルトのサービスマネージド AWS KMS キーを使用して保管時に暗号化されます。

Microsoft Active Directory に参加している SVM の作成

ファイルシステムを作成した後、Microsoft Active Directory に参加する追加の SVM を作成することで、Windows および macOS クライアントからの SMB アクセスを有効にできます。FSx for ONTAP は AWS Secrets Manager と統合され、Microsoft Active Directory ドメイン結合サービスアカウントの認証情報を安全に管理します。

Microsoft Active Directory に参加している SVM を作成するには

1. Amazon FSx コンソールの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。
2. [ストレージ仮想マシンを作成] を選択します。
3. [ファイルシステム] で、作成したファイルシステムを選択します。
4. ストレージ仮想マシン名 に、SVM の名前を入力します。
5. Microsoft Active Directory の設定 で、Microsoft Active Directory に参加する を選択します。
6. [ドメイン結合サービスアカウントの認証情報] で、[Secrets Manager で管理] (デフォルト) を選択して、Secrets Manager を使用して安全な認証情報管理を行います。

   > **Note**
   >
   > Secrets Manager を使用すると、プレーンテキスト認証情報を保存する必要がなくなり、認証情報を一元管理できます。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。

7. [シークレット] では、ドメイン参加サービスアカウントの認証情報を含む Secrets Manager から既存のシークレットを選択するか、新しいシークレットを作成 を選択して作成します。
8. 環境に応じて、残りの Microsoft Active Directory 設定フィールドに入力します。

9. [ストレージ仮想マシンを作成] を選択します。

SVM は Secrets Manager に保存された認証情報を使用して作成され、Microsoft Active Directory に参加します。Windows および macOS クライアントアクセスのため、この SVM 上に SMB 共有とボリュームを作成できるようになりました。

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 インスタンスへの接続」を参照してください。
4. Amazon EC2 インスタンスで secure shell (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、[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、Amazon FSx コンソールのボリューム詳細ページの [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生じた場合 (接続のタイムアウトなど) は、「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。

リソースのクリーンアップ

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。
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。

AWS リージョン による可用性

Amazon FSx for NetApp ONTAP ファイルシステムは、以下の AWS リージョン にて利用可能であり、各リージョンごとのデプロイメントタイプのサポート状況が示されます。

AWS リージョン	シングル AZ 1	マルチ AZ 1	シングル AZ 2	マルチ AZ 2		
米国東部 (バージニア北部)	✓	✓	✓	✓		
米国東部 (オハイオ)	✓	✓	✓	✓		
米国西部 (北カリフォルニア)	✓	✓	✓	✓		
米国西部 (オレゴン)	✓	✓	✓	✓		
AWS GovCloud (米国東部)	✓	✓				
AWS GovCloud (米国西部)	✓	✓				
アフリカ (ケープタウン)	✓	✓				
アジアパシフィック (香港)	✓	✓				

AWS リージョン	シングル AZ 1	マルチ AZ 1	シングル AZ 2	マルチ AZ 2		
アジアパシフィック (東京)	✓	✓	✓	✓		
アジアパシフィック (ソウル)	✓	✓	✓	✓		
アジアパシフィック (大阪)	✓	✓				
アジアパシフィック (ムンバイ)	✓	✓	✓	✓		
アジアパシフィック (ハイデラバード)	✓	✓				
アジアパシフィック (シンガポール)	✓	✓	✓	✓		
アジアパシフィック (シドニー)	✓	✓	✓	✓		
アジアパシフィック (ジャカルタ)	✓	✓				

AWS リージョン	シングル AZ 1	マルチ AZ 1	シングル AZ 2	マルチ AZ 2		
アジアパシフィック (メルボルン)	✓	✓				
アジアパシフィック (マレーシア)	✓	✓				
アジアパシフィック (台北)	✓	✓				
アジアパシフィック (タイ)	✓	✓				
カナダ (中部)	✓	✓	✓	✓		
カナダ西部 (カルガリー)	✓	✓				
欧州 (フランクフルト)	✓	✓	✓	✓		
欧州 (チューリッヒ)	✓	✓	✓	✓		
欧州 (ストックホルム)	✓	✓	✓	✓		

AWS リージョン	シングル AZ 1	マルチ AZ 1	シングル AZ 2	マルチ AZ 2		
欧州 (ミラノ)	✓	✓				
欧州 (スペイン)	✓	✓	✓	✓		
欧州 (アイルランド)	✓	✓	✓	✓		
欧州 (ロンドン)	✓	✓				
欧州 (パリ)	✓	✓				
イスラエル (テルアビブ)	✓	✓				
メキシコ (中部)	✓	✓				
中東 (アラブ首長国連邦)	✓	✓				
中東 (バーレーン)	✓	✓				
南米 (サンパウロ)	✓	✓				

FSx for ONTAP 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、以下に記載されるとおり、NetApp ONTAP CLI、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結合している場合、またはワークグループを使用している場合)
- `Iscsi` - 共有ブロックストレージサポートのために、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て接続する場合
- `Nvme` – 共有ブロックストレージのサポートのために TCP/IP 経由で非揮発性メモリエクスプレス (NVMe) を使用して接続する場合。
- `Management`NetApp ONTAP CLI または API、または NetApp コンソールを使用して SVM を管理する場合

> **Note**
>
> iSCSI プロトコルは、高可用性ペア (HA) ペアが 6 つ以下のすべてのファイルシステムで使用できます。NVMe/TCP プロトコルは、HA ペアが 6 つ以下の第 2 世代ファイルシステムで使用できます。

トピック

- サポートされているクライアント
- ブロックストレージプロトコルの使用
- 内からのデータへのアクセス AWS クラウド
- オンプレミスからデータにアクセスする
- VPC の外部からマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する

- オンプレミスからマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する
- ボリュームの Linux クライアントへのマウント
- Microsoft Windows クライアントへのボリュームのマウント
- macOS クライアントでのボリュームのマウント
- Linux 用 iSCSI のプロビジョニング
- Windows 用 iSCSI のプロビジョニング
- Linux 用の NVMe/TCP のプロビジョニング
- Amazon S3 アクセスポイントを介したデータへのアクセス
- 他の AWS サービスからのデータへのアクセス

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、ボリュームの Linux クライアントへのマウント、Microsoft Windows クライアントへのボリュームのマウント、および macOS クライアントでのボリュームのマウント 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 OpenShift Service とは AWS」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。

ブロックストレージプロトコルの使用

Amazon FSx for NetApp ONTAP は、TCP (NVMe/TCP) ブロックストレージプロトコルで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) と非揮発性メモリエクスプレス (NVMe) をサポートしています。ストレージエリアネットワーク (SAN) 環境では、ストレージシステムはストレージターゲットデバイスを持つターゲットです。iSCSI の場合、ストレージターゲットデバイスは論理単位 (LUN) と呼ばれます。NVMe/TCP の場合、ストレージターゲットデバイスは名前空間と呼ばれます。

SVM の iSCSI 論理インターフェイス (LIF) を使用して、NVMe ブロックストレージと iSCSI ブロックストレージの両方に接続します。

ストレージを設定するには、iSCSI 用の LUN を作成し、NVMe 用の名前空間を作成します。その後 LUN と名前空間は、iSCSI または TCP プロトコルを使用してホストによってアクセスされます。

iSCSI および NVMe/TCP ブロックストレージの設定の詳細については、以下を参照してください。

- Linux 用 iSCSI のプロビジョニング

- Windows 用 iSCSI のプロビジョニング
- Linux 用の NVMe/TCP のプロビジョニング

内からのデータへのアクセス AWS クラウド

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。

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に、それが配置されている 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 SVM およびボリュームも同じ VPC に配置されます。ボリュームをマウントするときに、ボリュームをマウントするファイルシステムとクライアントが同じ VPC にあり 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。

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 NetApp ONTAP のマルチ AZ ファイルシステムの NFS、SMB、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。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。

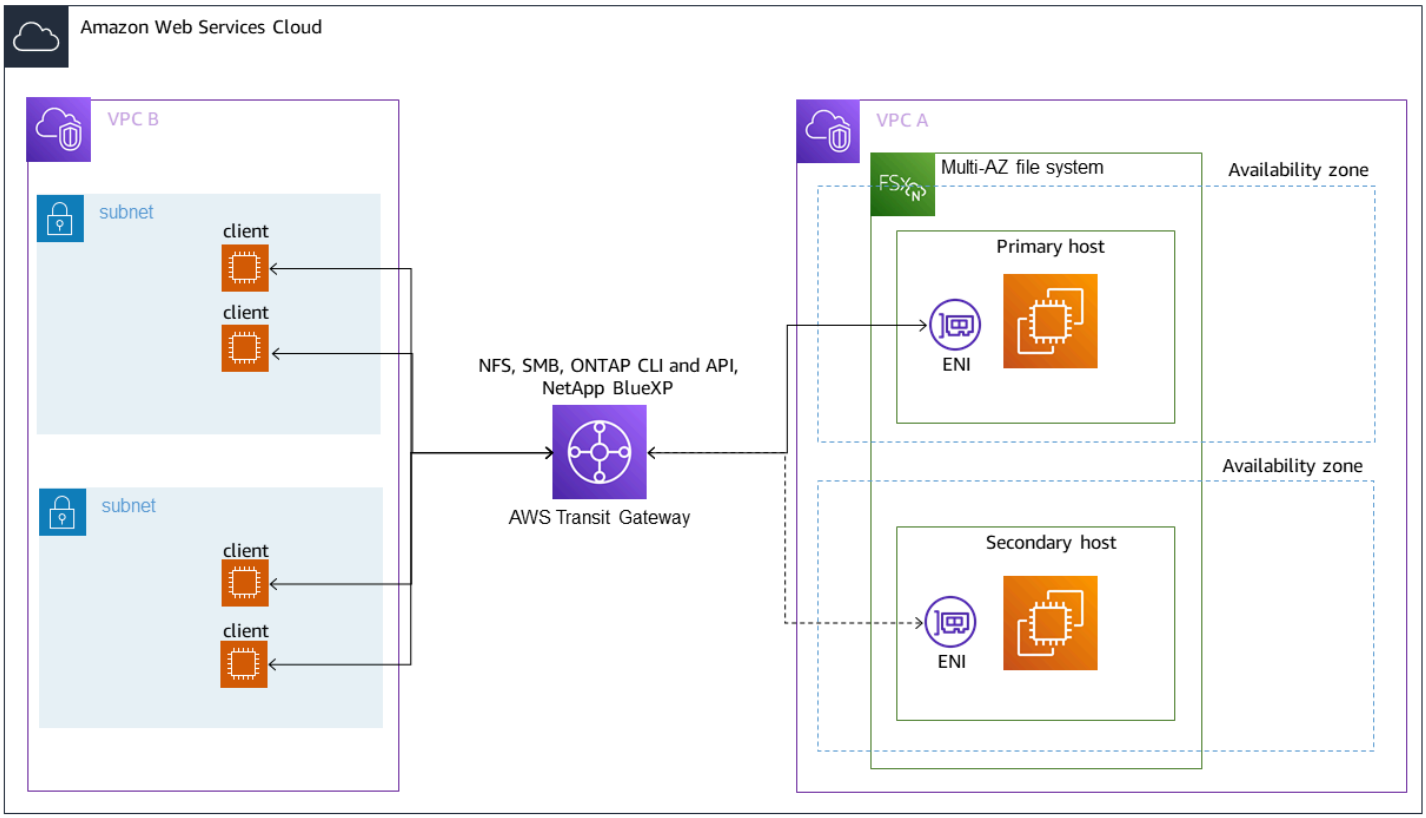
これらのフローティング IP アドレスは、ファイルシステムに関連付けられた VPC ルートテーブルに作成され、作成時に指定したファイルシステムの`EndpointIPv4AddressRange`または`EndpointIPv6AddressRange`内にあります。エンドポイント IP アドレス範囲は、ファイルシステムの作成方法に応じて、次のアドレス範囲を使用します：

- Amazon FSx コンソールまたは Amazon FSx API で作成されたマルチ AZ デュアルスタックファイルシステムは、デフォルトで、VPC の CIDR 範囲のいずれかから Amazon FSx によって選択された使用可能な/118 IP アドレス範囲を使用します。どのサブネットと重複しない限り、同じ VPC/ルートテーブルにデプロイされたファイルシステムのエンドポイント IP アドレスを重複させることができます。
- Amazon FSx コンソールを使用して作成されたマルチ AZ IPv4 のみの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エンドポイント IP アドレス範囲に対して 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 IPv4-onlyファイルシステムは、デフォルトでエンドポイント IP アドレス範囲の`198.19.0.0/16`アドレスブロック内の IP アドレス範囲を使用します。
- どちらのネットワークタイプでも、標準作成オプションを使用するときに、独自の IP アドレス範囲を指定することもできます。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、また、同じ VPC およびルートテーブルで別のファイルシステムによって使用されていない限り、VPC の IP アドレス範囲の内側でも外側でも可能です。このオプションでは、VPC の IP アドレス範囲内の範囲を使用することをお勧めします。

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 Direct Connect、 および は、推移的なピアリングをサポート Site-to-Site 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。

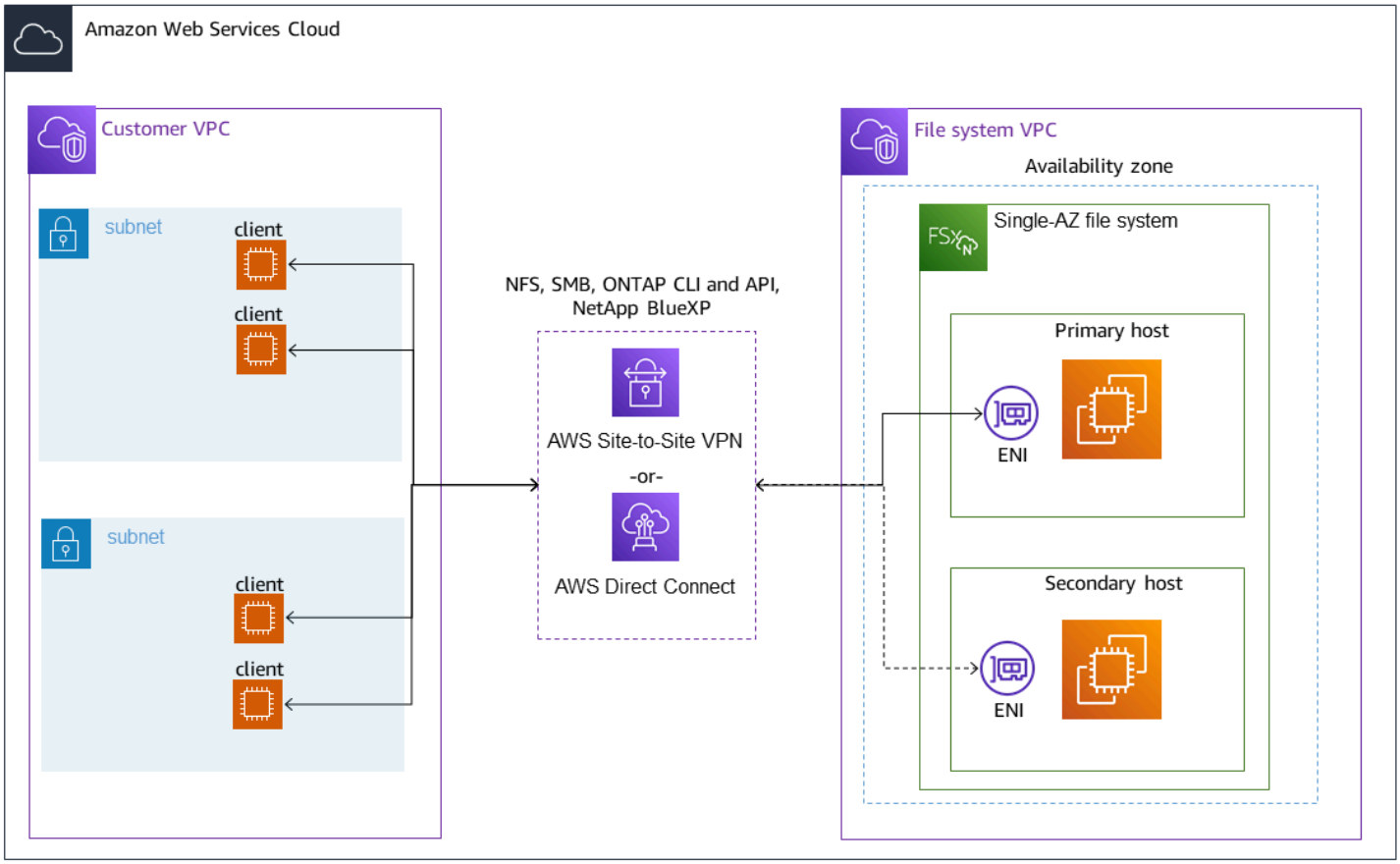
FSx for ONTAP ファイルシステムにアクセスするために Transit Gateway を使用する必要がある場合の詳細については、「Transit Gateway はどのような場合に必要ですか。」を参照してください。

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 CloudFormation することをお勧めします。

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 ピアリングを使用して AWS Direct Connect、または必要と Site-to-Site 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 Direct Connect に Site-to-Site 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 NetApp Console 経由での FSx へのアクセス	次の場合のみ必要です。 • 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、 • NetApp FlexCache またはグローバルファイルキャッシュインスタンスから FSx にアクセスしない
iSCSI 経由でデータにアクセスする	不可
NVMe 経由でのデータへのアクセス	不可
SVM をアクティブディレクトリに結合する	不可
SnapMirror	不可
FlexCache キャッシュ	不可
グローバルファイルキャッシュ	不可

デプロイ用 VPC の外部の NVMe、iSCSI およびクラスター間エンドポイントへのアクセス

VPC ピアリングまたは を使用して、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 NVMe、iSCSI、クラスター間エンドポイント AWS Transit Gateway にアクセスできます。VPC ピアリングを使用して、VPC 間で NVMe、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 ピア接続は 2 つの VPC 間のネットワーク接続であり、プライベート IPv4 または IPv6 アドレスを使用して VPC 間の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

Site-to-Site VPN および 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、および ONTAP CLI および 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。

オンプレミスからのマルチ AZ ファイルシステムへのアクセス

Amazon FSx では、 AWS Transit Gateway を使用するか、リモート NetApp グローバルファイルキャッシュまたは NetApp FlexCache を設定して、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 IP アドレスを使用するため、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 Site-to-Site VPN にアクセスするには、 AWS Direct Connect または AWS Transit Gatewayと組み合わせて を使用する必要があります。これらのインターフェイスに使用される Floating 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するEndpointIPv4AddressRangeまたはEndpointIPv6AddressRangeの範囲内です。エンドポイント IP アドレス範囲は、ファイルシステムの作成方法に応じて、次のアドレス範囲を使用します：

- Amazon FSx コンソールまたは Amazon FSx API で作成されたマルチ AZ デュアルスタックファイルシステムは、デフォルトで、VPC の CIDR 範囲のいずれかから Amazon FSx によって選択された使用可能な/118 IP アドレス範囲を使用します。どのサブネットと重複しない限り、同じ VPC/ルートテーブルにデプロイされたファイルシステムのエンドポイント IP アドレスを重複させることができます。
- Amazon FSx コンソールを使用して作成されたマルチ AZ IPv4 のみの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エンドポイント IP アドレス範囲に対して 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 IPv4-onlyファイルシステムは、デフォルトでエンドポイント IP アドレス範囲の198.19.0.0/16アドレスブロック内の IP アドレス範囲を使用します。

- どちらのネットワークタイプでも、標準作成オプションを使用するときに、独自の IP アドレス範囲を指定することもできます。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、また、同じ VPC およびルートテーブルで別のファイルシステムによって使用されていない限り、VPC の IP アドレス範囲の内側でも外側でも可能です。このオプションでは、VPC の IP アドレス範囲内の範囲を使用することをお勧めします。

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。

詳細については、「オンプレミスからマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する」を参照してください。

オンプレミスからシングル AZ ファイルシステムへのアクセス

オンプレミスネットワークからデータにアクセス AWS Transit Gateway するために を使用する要件は、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、オンプレミスの NetApp デプロイと FSx for ONTAP 間を含む NetApp 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、異なるファイルシステムにまたがるストレージ仮想マシン

(SVM) およびボリュームとの間の SnapMirror、FlexCache、FlexClone 関係と、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 Site-to-Site VPN または Direct Connect を使用して VPC への安全な接続を確立する必要があります。

詳細については、「オンプレミスからマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する」を参照してください。

VPC の外部からマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する

VPC の IP アドレス範囲外EndpointIPv6AddressRangeの EndpointIPv4AddressRangeまたはを持つマルチ AZ ファイルシステムがある場合は、ピアリング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 アドレス範囲内にエンドポイント IP アドレス範囲があるシングル 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、追加のトランジット Gateway 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. Amazon FSx コンソール (https://console.aws.amazon.com/fsx/) 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. ネットワークとセキュリティで、エンドポイントの 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 トランジットゲートウェイのトランジットゲートウェイの使用をご参照ください。
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。

オンプレミスからマルチ AZ ファイルシステムにアクセスするようにルーティングを設定する

オンプレミスからマルチ AZ ファイルシステムにアクセスする AWS Transit Gateway ように を設定するには

VPC の CIDR 範囲外`EndpointIPv6AddressRange`の `EndpointIPv4AddressRange`または を持つマルチ AZ ファイルシステムがある場合は、ピアリング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 アドレス範囲内にエンドポイント IP アドレス範囲があるシングル 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、追加のトランジット Gateway 設定は必要ありません。

1. Amazon FSx コンソール (https://console.aws.amazon.com/fsx/) 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 IPv4 or IPv6 address range (エンドポイント IPv4 または IPv6 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。個別の Transit Gateway アタッチメントサブネットがある場合は、それらのサブネットのルートテーブルを Amazon FSx に関連付けして、Amazon FSx エンドポイントアドレスで更新されるようにする必要もあります。

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。

ボリュームの Linux クライアントへのマウント

Linux クライアントをマウントするボリュームには、`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ご参照ください。
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 インスタンスへの接続」を参照してください。
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
   ```

   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第 2 世代の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**
>
> 第 2 世代の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、「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場合は、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」の次のトピックを参照ください：

- [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. 適切な工ディタで、/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 クライアントへのボリュームのマウント

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 AWS リージョンに配置されている場合、この手順では、AWS Transit Gateway または AWS Direct Connect を使用した専用ネットワーク接続または AWS Virtual Private Network を使用したプライベートで安全なトンネルをセットアップ済みであることも前提としています。詳しくは、「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 を結合しているか、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方法の詳細については、ワークグループでの SMB サーバーのセットアップをご参照ください。
- アタッチするボリュームのセキュリティスタイル設定はNTFSである必要があります。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。

SMB と Active Directory を使用して Windows クライアントにボリュームをマウントするには

1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
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を結合している 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ご参照ください。

   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。
   - `SHARE_NAME` を SMB 共有の名前に置き換えます。`C$` は SVM の名前空間のルートにあるデフォルトの SMB 共有ですが、ストレージをルートボリュームに公開し、セキュリティとサービスの中断を引き起こす可能性があるため、マウントしないでください。`C$` 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。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第 2 世代の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 クライアントでのボリュームのマウント

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または別の VPC にある場合、 AWS アカウント または を使用して AWS Transit Gateway または専用ネットワーク接続をセットアップした場合 AWS リージョン、 AWS Direct Connect または を使用してプライベートで安全なトンネルをセットアップした場合 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 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
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ご参照ください。
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 インスタンスへの接続」を参照してください。
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第 2 世代の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 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
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ご参照ください。
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 インスタンスへの接続」を参照してください。
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
   ```

   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第 2 世代の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
```

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第 2 世代の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
```

Linux 用 iSCSI のプロビジョニング

FSx for ONTAP は iSCSI プロトコルをサポートしています。iSCSI プロトコルを使用してクライアントとファイルシステム間でデータを転送するには、Linux クライアントとファイルシステムの両方で iSCSI をプロビジョニングする必要があります。iSCSI プロトコルは、高可用性 (HA) ペアが 6 つ以下のすべてのファイルシステムで使用できます。

Amazon FSx for NetApp ONTAP で iSCSI を設定するプロセスには、主に 3 つのステップがあります。これらのステップについては、次の手順で説明します。

1. Linux ホストに iSCSI クライアントをインストールして設定する
2. ファイルシステムの SVM で iSCSI を設定します。
   - iSCSI イニシエータグループを作成します。
   - イニシエータグループを LUN にマッピングします。
3. Linux クライアントに iSCSI LUN をマウントします

開始する前に

iSCSI 用にファイルシステムを設定するプロセスを開始する前に、次の項目を完了しておく必要があります。

- 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」を参照してください。
- ファイルシステムに iSCSI LUN を作成します。詳細については、「iSCSI LUN の作成」を参照してください。

- ファイルシステムと同じ VPC にある Amazon Linux 2 Amazon マシンイメージ (AMI) を実行する EC2 インスタンスを作成します。これは、iSCSI を設定し、ファイルデータにアクセスする Linux ホストです。

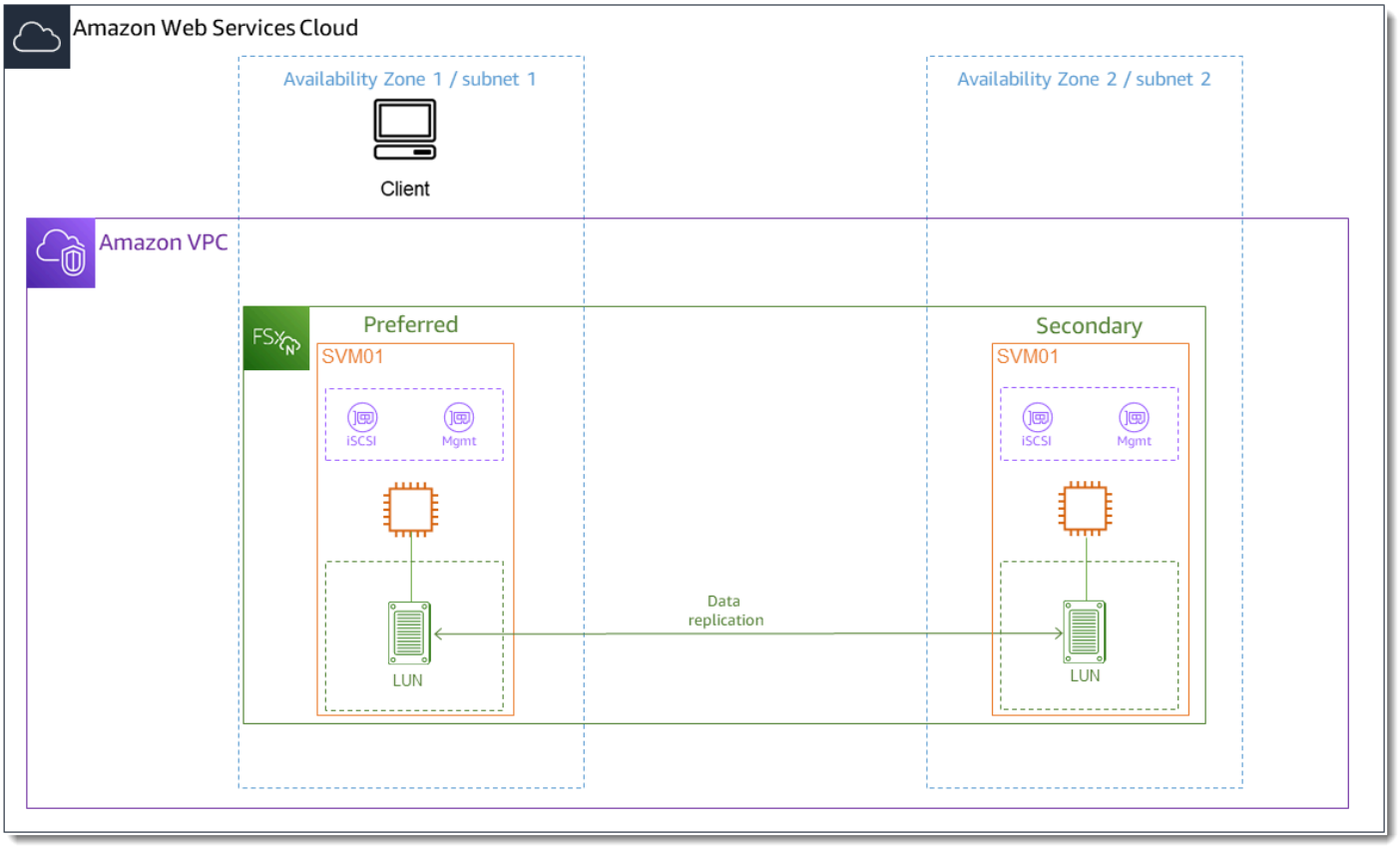
  これらの手順の範囲を超えて、ホストが別のVPCにある場合は、VPC ピアリングまたは AWS Transit Gateway を使用して、他の VPC にボリュームの iSCS Iエンドポイントへのアクセスを許可できます。詳細については、「デプロイ用の VPC の外部からのデータへのアクセス」を参照してください。

- 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 Linux ホストの VPC セキュリティグループを設定します。

- ONTAP CLI へのアクセスに使用する `fsxadmin` 権限を持つ ONTAP ユーザーの認証情報を取得します。詳細については、「ONTAP ロールとユーザー」を参照してください。

- iSCSI 向けに設定し、FSx for ONTAP ファイルシステムにアクセスするために使用する Linux ホストは、同じ VPC と AWS アカウント にあります。

- 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。



EC2 インスタンスが Amazon Linux 2 とは異なる Linux AMI を実行している場合、これらの手順や例で使用されるユーティリティの一部がすでにインストールされている可能性があり、必要なパッケージをインストールするために異なるコマンドを使用する場合があります。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。

トピック

- Linux コストに 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 コストに 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 LUN を作成した FSx for ONTAP ファイルシステムの NetApp 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ーグループ (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。そうでない場合は、そのための詳細のステップバイステップについては、「iSCSI LUN の作成」を参照してください。

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

Linux クライアントに iSCSI LUN をマウントするプロセスには、次の 3 つのステップがあります。

1. ターゲット iSCSI ノードの検出
2. iSCSI LUN のパーティション分割
3. iSCSI LUN をクライアントにマウントする

これらについては、以下の手順で説明します。

ターゲット iSCSI ノードを検出するには

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) iSCSI LUN に対して Amazon EC2 シングルクライアントの最大 5 Gbps (~625 MBps) よりも高いスループットを実現するには、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの Amazon EC2 インスタンスのネットワーク帯域幅で説明されている手順に従って、スループットを向上させるための追加セッションを確立します。

   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ごとに 8 つのセッションを確立し、クライアントが iSCSI LUN に対して最大 40 Gbps (5,000 MBps) の総スループットを実現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わかりやすい名前を割り当てるには

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固有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。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。

> **Note**
>
> Last sector 値は、iSCSI LUN のサイズ (この例では 10GB) によって異なります。

```
~$ 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 コマンドの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特定のユーザーに所有権を付与する場合は、*username* を所有者のユーザー名に置き換えます。

```
~$ 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 用 iSCSI のプロビジョニング

FSx for ONTAP は iSCSI プロトコルをサポートしています。iSCSI プロトコルを使用してクライアントとファイルシステム間でデータを転送するには、Windows クライアントと SVM とボリュームの両方で iSCSI をプロビジョニングする必要があります。iSCSI プロトコルは、高可用性 (HA) ペアが 6 つ以下のすべてのファイルシステムで使用できます。

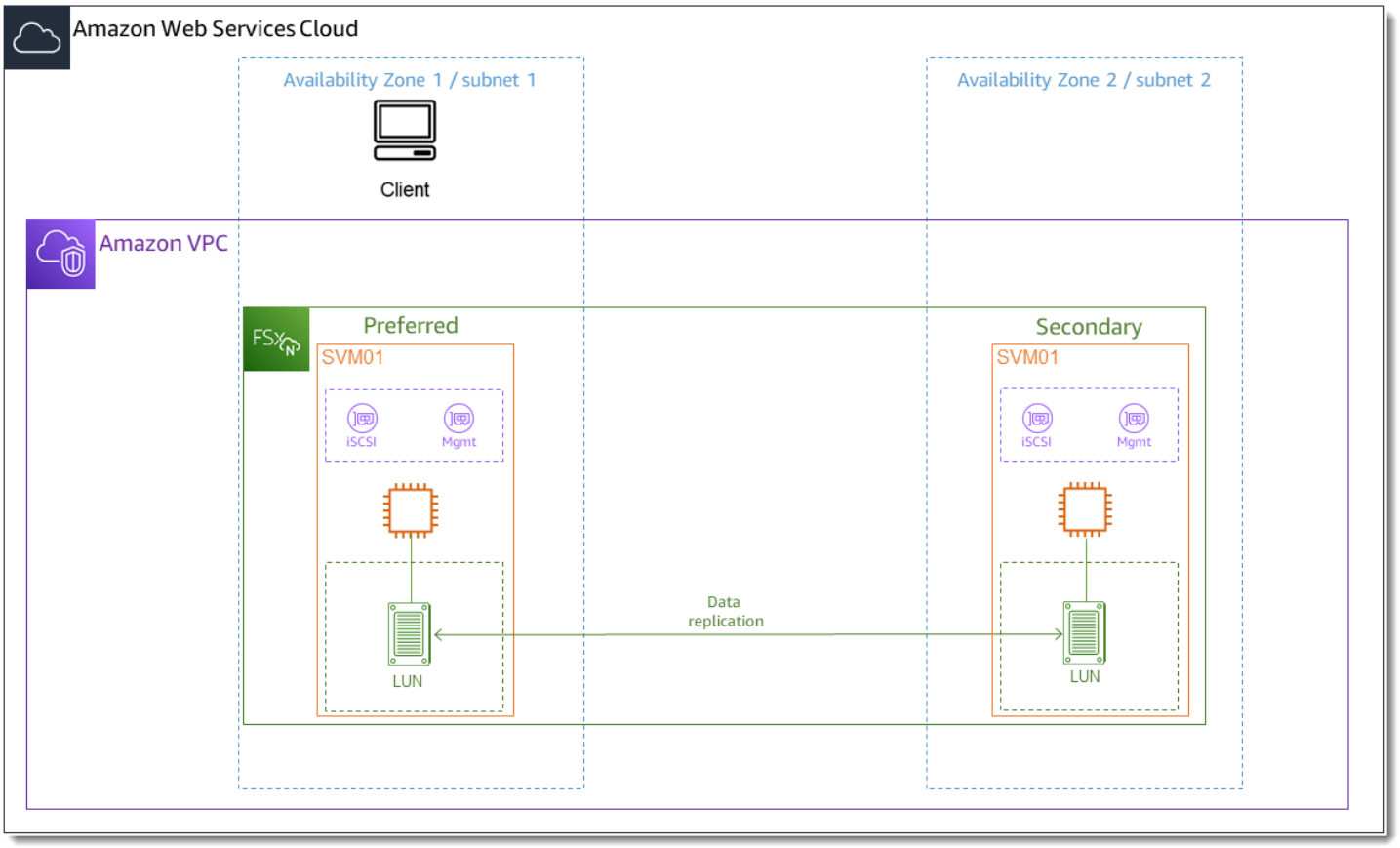
これらの手順で示す例は、クライアントと FSx for ONTAP ファイルシステムで iSCSI プロトコルをプロビジョニングし、以下のセットアップを使用する方法を示しています。

- 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 VPC 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. 管理者として Windows PowerShell 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、NetApp ONTAP CLI を使用して FSx for ONTAP ファイルシステムで iSCSI を設定する際に使用します。

```
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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. ONTAP CLI lun igroup create を使用して、イニシエーターグループまたは igroup を作成します。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、lun igroup create ONTAP CLI コマンドを使用して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。

3. lun igroup show ONTAP CLI 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。そうでない場合は、そのための詳細のステップバイステップについては、「iSCSI LUN の作成」を参照してください。

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。

- 各 iSCSI 接続に対して 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 iSCSI LUN に対して最大 40 Gbps (5,000 MBps) の総スループットを実現できます。8 つのセッションを使用することで、単一のクライアントが、ONTAP スループット容量のための最高レベルの FSx に対して、完全な 4,000 MBps スループット容量を駆動できることが保証されます。オプションで、RecommendedConnectionCount変数を変更することにより、セッション数を増減することができます (各セッションは最大 625 MBps のスループットを提供します) 。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。

```
Write-Host "Starting iSCSI connection setup..."
     $TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
     $RecommendedConnectionCount = 8

     Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
     }

     New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

     $currentMPIOSettings = Get-MPIOSetting
     if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
         Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
     } else { Write-Host "MPIO path verification state already Enabled" }

     $portalConnectionCounts = @{}
     foreach ($TargetPortalAddress in $TargetPortalAddresses)
 { $portalConnectionCounts[$TargetPortalAddress] = 0 }

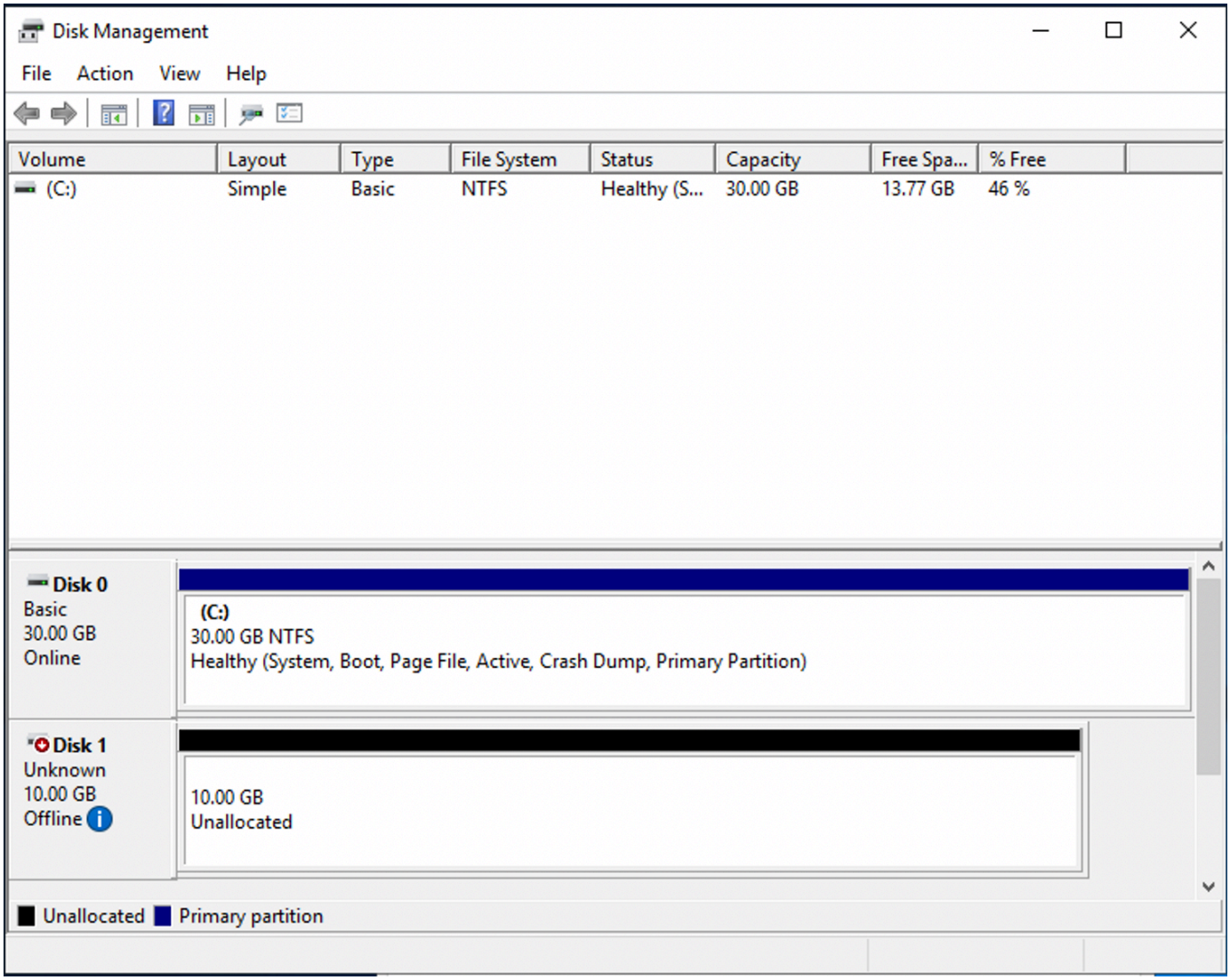
     $sessions = Get-IscsiSession
     if ($sessions) {
         foreach ($session in $sessions) {
             if ($session.IsConnected) {
```

```
                $targetPortal = (Get-IscsiTargetPortal -iSCSISession
 $session).TargetPortalAddress
                if ($portalConnectionCounts.ContainsKey($targetPortal))
 { $portalConnectionCounts[$targetPortal]++ }
            }
        }
    }

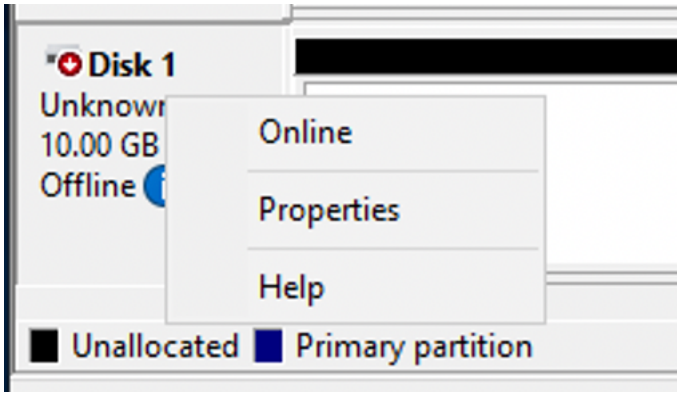
    foreach ($TargetPortalAddress in $TargetPortalAddresses) {
        $existingCount = $portalConnectionCounts[$TargetPortalAddress];
 $remainingConnections = $RecommendedConnectionCount - $existingCount
        Write-Host "Portal $TargetPortalAddress has $existingCount
 existing connections, $remainingConnections remaining (max recommended:
 $RecommendedConnectionCount)"
        if ($remainingConnections -gt 0) {
            Write-Host "Creating $remainingConnections connections for portal
 $TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
 $TargetPortalAddress" }
    }

    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 セットアップが正しく設定されていることを確認するスクリプトが用意されます。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、成功した iSCSI 設定を示しています。

```
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.

MPIO Load Balance Policy is set to Round Robin (RR).
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
```

Linux 用の NVMe/TCP のプロビジョニング

FSx for ONTAP は、TCP (NVMe/TCP) ブロックストレージプロトコルによる非揮発性メモリエクスプレスをサポートしています。NVMe/TCP では、ONTAP CLI を使用して名前空間とサブシステムをプロビジョニングし、LUN のプロビジョニング方法や iSCSI のイニシエータグループ (igroup) へのマッピング方法と同様に、名前空間をサブシステムにマッピングします。NVMe/TCP プロトコルは、高可用性 (HA) ペアが 6 つ以下の第 2 世代ファイルシステムで使用できます。

> **Note**
>
> FSx for ONTAP ファイルシステムは、iSCSI と NVMe/TCP ブロックストレージプロトコルの両方で SVM の iSCSI エンドポイントを使用します。

Amazon FSx for NetApp ONTAP で NVMe/TCP を設定するプロセスには、主に 3 つのステップがあります。これらのステップについては、次の手順で説明します。

1. Linux ホストの NVMe クライアントをインストールおよび設定します。
2. ファイルシステムの SVM で NVMe を設定します。
   - NVMe 名前空間を作成します。
   - NVMe サブシステムを作成します。

- 名前空間をサブシステムにマッピングします。
- クライアント NQN をサブシステムに追加します。

3. Linux クライアントに NVMe デバイスをマウントします。

開始する前に

ファイルシステムを NVMe/TCP に設定するプロセスを開始する前に、次の項目を完了しておく必要があります。

- 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」を参照してください。
- Red Hat Enterprise Linux (RHEL) 9.3 を実行する EC2 インスタンスをファイルシステムと同じ VPC に作成します。これは、NVMe を設定し、NVMe/TCP for Linux を使用してファイルデータにアクセスする NVMe ホストです。

  これらの手順の範囲を超えて、ホストが別の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 VPC にボリュームの iSCS I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。
- 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 Linux ホストの VPC セキュリティグループを設定します。
- ONTAP CLI へのアクセスに使用する `fsxadmin` 権限を持つ ONTAP ユーザーの認証情報を取得します。詳細については、「ONTAP ロールとユーザー」を参照してください。
- NVMe 向けに設定し、FSx for ONTAP ファイルシステムにアクセスするために使用する Linux ホストは、同じ VPC と AWS アカウント にあります。
- 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。

EC2 インスタンスが RHEL 9.3 とは異なる Linux AMI を実行している場合、これらの手順や例で使用されるユーティリティの一部がすでにインストールされている可能性があり、異なるコマンドを使用して必要なパッケージをインストールできます。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。

トピック

- Linux ホストに NVMe 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 NVMe を設定する
- Linux クライアントに NVMe デバイスをマウントする

Linux ホストに NVMe をインストールして設定する

NVMe クライアントをインストールするには

1. 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 を使用して Linux または macOS から Linux インスタンスに接続する」を参照してください。
2. 次のコマンドを使用して nvme-cli をインストールします。

```
~$ sudo yum install -y nvme-cli
```

3. nvme-tcp モジュールをホストにロードします。

```
$ sudo modprobe nvme-tcp
```

4. 次のコマンドを使用して、Linux ホストの NVMe 修飾名 (NQN) を取得します。

```
$ cat /etc/nvme/hostnqn
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

後のステップで使用するレスポンスを記録します。

FSx for ONTAP ファイルシステムで NVMe を設定する

ファイルシステムで NVMe を設定するには

NVMe デバイス (複数可) を作成する予定の FSx for ONTAP ファイルシステムの NetApp ONTAP CLI に接続します。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. NVMe インターフェイスへのアクセスに使用する SVM に新しいボリュームを作成します。

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
     [Job 597] Job succeeded: Successful
```

3. vserver nvme namespace create NetApp ONTAP CLI コマンドを使用して NVMe 名前空間 ns_1 を作成します。名前空間はイニシエータ (クライアント) にマッピングされ、どのイニシエータ (クライアント) が NVMe デバイスにアクセスできるかを制御します。

```
::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
 -ostype linux
Created a namespace of size 100GB (107374182400).
```

4. vserver nvme subsystem create NetApp ONTAP CLI コマンドを使用して NVMe サブシステムを作成します。

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. 作成したサブシステムに名前空間をマッピングします。

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
nvme_vol1/ns_1
```

6. 以前に取得した NQN を使用して、クライアントをサブシステムに追加します。

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
 nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

このサブシステムにマッピングされたデバイスを複数のホストで使用できるようにする場合は、コンマ区切りのリストで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 Docs の「vserver nvme サブシステムホスト追加」を参照してください。

7. vserver nvme namespace show コマンドを使用して、名前空間が存在することを確認します。

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
```

```
            Namespace Path: /vol/nvme_vol1/ns_1
                      Size: 100GB
                 Size Used: 90.59GB
                   OS Type: linux
                   Comment:
                Block Size: 4KB
                     State: online
         Space Reservation: false
Space Reservations Honored: false
              Is Read Only: false
             Creation Time: 5/20/2024 17:03:08
            Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
                  Vdisk ID: 80d42c6f00000000187cca9
      Restore Inaccessible: false
   Inconsistent Filesystem: false
       Inconsistent Blocks: false
                   NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
               Volume Name: nvme_vol1
                Qtree Name:
          Mapped Subsystem: sub_1
            Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
              Namespace ID: 00000001h
              ANA Group ID: 00000001h
              Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
                Vserver ID: 3
              Volume MSID: 2161388655
              Volume DSID: 1029
                Aggregate: aggr1
            Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
 Namespace Container State: online
        Autodelete Enabled: false
          Application UUID: -
               Application: -
  Has Metadata Provisioned: true

1 entries were displayed.
```

8. network interface show -vserver コマンドを使用して、NVMe デバイスを作成した SVM のブロックストレージ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 -data-protocol nvme-tcp
```

```
            Logical                Status     Network            Current
        Current Is
Vserver     Interface              Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------             ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1                up/up      172.31.16.19/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2                up/up      172.31.26.134/20
 FSxId0123456789abcdef8-02  e0e     true
2 entries were displayed.
```

> **Note**
>
> iscsi_1 LIF は iSCSI と NVMe/TCP の両方に使用されます。

この例では、iscsi_1 の IP アドレスは 172.31.16.19、iscsi_2 は 172.31.26.134 です。

Linux クライアントに NVMe デバイスをマウントする

Linux クライアントに NVMe デバイスをマウントするプロセスには、次の 3 つのステップがあります。

1. NVMe ノードの検出
2. NVMe デバイスのパーティション分割
3. クライアントへの NVMe デバイスのマウント

これらについては、以下の手順で説明します。

ターゲット NVMe ノードを検出するには

1. Linux クライアントで、次のコマンドを使用して、ターゲット NVMe ノードを検出します。*iscsi_1_IP* を iscsi_1 の IP アドレスに、*client_IP* をクライアントの IP アドレスに置き換えます。

> **Note**
>
> iscsi_1 および iscsi_2 LIFsは、iSCSI ストレージと NVMe ストレージの両方に使用されます。

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  0
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.26.134
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  1
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.16.19
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
```

2. (オプション) ファイル NVMe デバイスに対して Amazon EC2 シングルクライアントの最大 5 Gbps (~625 MBps) よりも高いスループットを実現するには、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの Amazon EC2 インスタンスのネットワーク帯域幅で説明されている手順に従って、追加のセッションを確立します。
3. コントローラ損失タイムアウトが 1800 秒以上のターゲットイニシエータにログインします。この場合も、*iscsi_1_IP* の iscsi_1の IP アドレスと *client_IP* のクライアントの IP アドレスを使用します。NVMe デバイスは使用可能なディスクとして表示されます。

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. 次のコマンドを使用して、NVMe スタックが複数のセッションを識別してマージし、マルチパスを設定済みであることを確認します。設定が正常に完了すると、コマンドが Y を返します。

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. 次のコマンドを使用して、NVMe-oF 設定 model が NetApp ONTAP Controller に設定され、使用可能なすべてのパスで I/O を分散するために、各 ONTAP 名前空間の負荷分散 iopolicy が round-robin に設定されていることを確認します。

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. 次のコマンドを使用して、名前空間が作成され、ホストで正しく検出されていることを確認します。

```
~$ sudo nvme list
Node                  Generic               SN                   Model
                        Namespace  Usage                      Format           FW
 Rev
--------------------- --------------------- --------------------
 ---------------------------------------- ---------- --------------------------
 ---------------- --------
/dev/nvme0n1          /dev/ng0n1            vol05955547c003f0580 Amazon Elastic
 Block Store               0x1         25.77  GB /  25.77  GB    512   B +  0 B
 1.0
/dev/nvme2n1          /dev/ng2n1            lWB12JWY/XLKAAAAAAAC NetApp ONTAP
 Controller                0x1        107.37  GB / 107.37  GB      4 KiB +  0 B
 FFFFFFFF
```

出力の新しいデバイスは /dev/nvme2n1 です。この命名スキームは、Linux のインストールによって異なる場合があります。

7. 各パスのコントローラの状態がライブで、適切な非対称名前空間アクセス (ANA) マルチパスステータスであることを確認します。

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
 NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
               hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
               iopolicy=round-robin
\
 +- nvme2 tcp
 traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live non-optimized
 +- nvme3 tcp
 traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live optimized
```

この例では、NVMe スタックはファイルシステムの代替 LIF、iscsi_2、172.31.26.134 を自動的に検出しました。

8. NetApp プラグインが各 ONTAP 名前空間デバイスに正しい値を表示していることを確認します。

```
~$ sudo nvme netapp ontapdevices -o column
Device           Vserver                   Namespace Path
           NSID UUID                                   Size
---------------- ------------------------
 ------------------------------------------------- ----
 ------------------------------------ ---------
/dev/nvme2n1     fsx                       /vol/nvme_vol1/ns_1
           1    0441c609-3db1-4b0b-aa83-790d0d448ece   107.37GB
```

デバイスをパーティション分割するには

1. 次のコマンドを使用して、device_name nvme2n1 へのパスが存在することを確認します。

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

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。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。

> **Note**
>
> Last sector 値は、NVMe デバイスのサイズ (この例では 100 GiB) によって異なります。

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

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 2.37.4).
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 (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
 26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
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/nvme2n1 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 コマンドの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/nvme2n1 を使用してファイルシステムを作成します。

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

システムは次の出力でレスポンスします。

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Linux クライアントに NVMe をマウントするには

1. Linux インスタンスの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/nvme2n1 /directory_path/mount_point
```

3. (オプション) マウントディレクトリの特定のユーザーに所有権を付与する場合は、*username* を所有者のユーザー名に置き換えます。

```
~$ 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 NVMe デバイスが正常に作成されてマウントされました。

Amazon S3 アクセスポイントを介したデータへのアクセス

S3 アクセスポイントを使用して、S3 にあるかのように Amazon FSx ファイルシステムに保存されているファイルデータにアクセスすることもできます。これにより、アプリケーションを変更したり、ファイルストレージからデータを移動したりすることなく、S3 と連携するアプリケーションやサービスで使用できます。Amazon S3 アクセスポイントは、S3 バケットまたは FSx for ONTAP および FSx for OpenZFS ボリュームにアタッチする S3 エンドポイントです。Amazon S3 アクセスポイントは、S3 で動作するすべてのアプリケーションまたは AWS サービスのデータアクセスの管理を簡素化します。S3 アクセスポイントを使用すると、データレイク、メディアアーカイブ、ユーザー生成コンテンツなどの共有データセットを持つお客様は、それぞれにカスタマイズされた名前とアクセス許可を持つ個別のアクセスポイントを作成することで、数百のアプリケーション、チーム、または個人のデータアクセスを簡単に制御およびスケーリングできます。

Amazon FSx for NetApp ONTAP ボリュームにアタッチされた S3 アクセスポイントは、Amazon S3 エンドポイントに対する S3 オブジェクトオペレーション (`GetObject`、`PutObject`、 など`ListObjectsV2`) を使用したファイルデータへの読み取りおよび書き込みアクセスをサポートします。 Amazon S3

FSx for ONTAP ファイルシステムにアタッチされた各 S3 アクセスポイントには、 AWS Identity and Access Management (IAM) アクセスポイントポリシーと、アクセスポイントを介して行われたすべてのリクエストを承認するために使用される関連する UNIX または Windows ファイルシステムユーザーがあります。S3 は、リクエストごとに、まずユーザー、アクセスポイント、S3 VPC エンドポイント、サービスコントロールポリシーなど、関連するすべてのポリシーを評価してリクエストを承認します。リクエストが S3 によって承認されると、リクエストはファイルシステムによって承認され、S3 アクセスポイントに関連付けられたファイルシステムユーザーにファイルシステム上のデータへのアクセス許可があるかどうかが評価されます。Virtual Private Cloud (VPC) からのリクエストのみを受け入れるようにアクセスポイントを設定して、プライベートネットワークへの Amazon S3 データアクセスを制限できます。Amazon S3 は、FSx for ONTAP ボリュームにアタッチされているすべてのアクセスポイントに対して、デフォルトでパブリックアクセスのブロックを強制します。この設定を変更または無効にすることはできません。

Amazon FSx コンソール、CLI、API を使用して S3 アクセスポイントを作成し、FSx for ONTAP ボリュームにアタッチします。 FSx アクセスポイントを使用すると、S3 API を使用してファイルデー

タにアクセスできますが、データは引き続き FSx for ONTAP ファイルシステムに存在し、NFS および SMB プロトコルを使用して S3 API とともにデータにアクセスできます。

FSx for ONTAP ファイルシステムの Amazon S3 アクセスポイントは、S3 バケットアクセスと一致する数十ミリ秒の範囲のレイテンシーを提供します。S3 API を介して Amazon FSx ファイルシステムにドライブできる 1 秒あたりのスループットとリクエスト数は、ファイルシステムのプロビジョニングされたスループットによって異なります。ファイルシステムのパフォーマンス機能の詳細については、「」を参照してください。 Amazon FSx for NetApp ONTAP のパフォーマンス

トピック

- AWS リージョン FSx for ONTAP の Amazon S3 アクセスポイントを使用する
- アクセスポイントの命名規則、制約と制限
- ARNs、アクセスポイントエイリアス、またはvirtual-hosted-style URIs を使用したアクセスポイントの参照
- アクセスポイントの互換性
- アクセスポイントアクセスの管理
- アクセスポイントの作成
- Amazon S3 アクセスポイントの管理
- アクセスポイントの使用
- S3 アクセスポイントの問題のトラブルシューティング

AWS リージョン FSx for ONTAP の Amazon S3 アクセスポイントを使用する

FSx for ONTAP の Amazon S3 アクセスポイントは、 AWS リージョンアフリカ (ケープタウン) 、アジアパシフィック (香港、ハイデラバード、ジャカルタ、メルボルン、ムンバイ、大阪、ソウル、シンガポール、シドニー、東京、カナダ (中部) 、カナダ西部 (カルガリー) 、欧州 (フランクフルト、アイルランド、ロンドン、ミラノ、パリ、スペイン、ストックホルム、チューリッヒ) 、イスラエル (テルアビブ) 、中東 (バーレーン、アラブ首長国連邦) 、南米 (サンパウロ) 、米国東部 (バージニア北部、オハイオ) 、米国西部 (オレゴン) でサポートされています。

アクセスポイントの命名規則、制約と制限

S3 アクセスポイントを作成するときは、そのアクセスポイントの名前を選択します。以下のトピックでは、S3 アクセスポイントの命名規則と制限について説明します。

トピック

- アクセスポイントの命名規則
- アクセスポイントの制約と制限

アクセスポイントの命名規則

S3 アクセスポイントを作成するときは、その名前を選択します。アクセスポイント名は、 AWS アカウント または 間で一意である必要はありません AWS リージョン。同じ AWS アカウント で同じ名前のアクセスポイントを作成する AWS リージョン 場合もあれば、同じアクセスポイント名を使用する AWS アカウント 場合もあります。ただし、1 つの 内に 2 つの同じ名前のアクセスポイントがない AWS リージョン AWS アカウント 場合があります。

S3 アクセスポイント名は`-ext-s3alias`、アクセスポイントエイリアス用に予約されているサフィックス で終わることはできません。アクセスポイントの命名規則の完全なリストについては、Amazon Simple Storage Service ユーザーガイドの「Amazon Amazon S3 アクセスポイントの命名規則」を参照してください。

アクセスポイントの制約と制限

FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントには以下の制限がありますが、S3 バケットにアタッチされたアクセスポイントには適用されません。

- S3 アクセスポイントは、アタッチ先の FSx for ONTAP ボリューム AWS リージョン と同じ にのみ作成できます。
- 同じ が FSx for ONTAP ファイルシステムと S3 アクセスポイントを所有している AWS アカウント 必要があります。所有している FSx for ONTAP ボリュームにアタッチされている S3 アクセスポイントのみを作成できます。別の が所有するボリュームにアタッチされた S3 アクセスポイントを作成することはできません AWS アカウント。
- NetApp ONTAP バージョン 9.17.1 以降を実行している FSx for ONTAP ファイルシステムに対してのみ、S3 アクセスポイントを作成してアタッチできます。

アクセスポイントのすべての制限と制限の完全なリストについては、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントの制限と制限」を参照してください。

ARNs、アクセスポイントエイリアス、またはvirtual-hosted-style URIs を使用したアクセスポイントの参照

FSx for ONTAP ボリュームにアタッチされたアクセスポイントを作成したら、 AWS CLI および S3 API、SS3-compatible AWS およびサードパーティーのサービスとアプリケーションを介してデータにアクセスできます。 AWS のサービス またはアプリケーションのアクセスポイントを参照するときは、Amazon リソースネーム (ARN)、アクセスポイントエイリアス、または仮想ホスト形式の URI を使用できます。

トピック

- アクセスポイント ARN
- アクセスポイントエイリアス
- 仮想ホスティング形式の URI

アクセスポイント ARN

アクセスポイントには Amazon リソースネーム (ARN) があります。アクセスポイント ARNs は S3 バケット ARNs に似ていますが、明示的に入力され、アクセスポイントの AWS リージョン とアクセスポイントの所有者の AWS アカウント ID がエンコードされます。ARN の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「Amazon AWS リソースネーム (ARNs」を参照してください。

アクセスポイント ARNs形式は次のとおりです。

```
arn:aws::s3:region:account-id:accesspoint/resource
```

arn:aws:s3:us-west-2:777777777777:accesspoint/*test* は、*us-west-2* リージョンのアカウント 777777777777 が所有する *test* という名前のアクセスポイントを表します。

アクセスポイントを介してアクセスされるオブジェクトとファイルの ARNs は、次の形式を使用します。

```
arn:aws::s3:region:account-id:accesspoint/access-point-name/object/resource
```

arn:aws:s3:us-west-2:111122223333:accesspoint/*test*/object/*lions.jpg* は、*us-west-2* リージョンのアカウント 111122223333 が所有する *test* というアクセスポイントを介してアクセスされるファイル *lions.jpg* を表します。

アクセスポイント ARNs の詳細については、Amazon Simple Storage Service ユーザーガイドARNsを参照してください。

アクセスポイントエイリアス

アクセスポイントを作成すると、Amazon S3 はアクセスポイントエイリアスを自動的に生成し、S3 バケット名を使用してデータにアクセスできる任意の場所で使用できます。

アクセスポイントエイリアスは変更できません。FSx for ONTAP ボリュームにアタッチされたアクセスポイントの場合、アクセスポイントエイリアスは次の部分で構成されます。

```
access point prefix-metadata-ext-s3alias
```

以下は、FSx CLI コマンドへのレスポンスの一部として返される、FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントdescribe-s3-access-point-attachmentsの ARN とアクセスポイントのエイリアスを示しています。この例のアクセスポイントの名前は ですmy-ontap-ap。

```
...
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
...
```

> **Note**
>
> -ext-s3alias サフィックスは、FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントのエイリアス用に予約されており、アクセスポイント名には使用できません。

一部の S3 データプレーンオペレーションでは、Amazon S3 アクセスポイント ARN の代わりにアクセスポイントエイリアスを使用できます。 S3 サポートされているオペレーションのリストについては、「」を参照してくださいアクセスポイントの互換性。

アクセスポイントエイリアスの制限の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントエイリアスの制限」を参照してください。

仮想ホスティング形式の URI

アクセスポイントでは、仮想ホスト形式のアドレス指定のみがサポートされます。仮想ホスト形式の URI では、アクセスポイント名 AWS アカウント、および AWS リージョン は URL のドメイン名の一部です。FSx for ONTAP ボリュームにアタッチされたアクセスポイントの S3 URI S3 アクセスポイントの詳細の下にあるアクセスポイントの詳細ページで、S3 アクセスポイントにリストされているアクセスポイント名を選択します。これにより、Amazon S3 コンソールのアクセスポイントの詳細ページに移動します。S3 URI は Propertiesにあります。

詳細については、「Amazon Simple Storage Service ユーザーガイド」の「仮想ホスト形式の URI」を参照してください。

アクセスポイントの互換性

アクセスポイントを使用して、次の Amazon S3 APIs を使用して FSx for ONTAP ボリュームに保存されているデータにアクセスできます。以下に示すすべてのオペレーションで、アクセスポイント ARN またはアクセスポイントエイリアスのいずれかを許可できます。

次の表は、Amazon S3 オペレーションの一部リストであり、アクセスポイントと互換性があるかどうかを示しています。この表は、データソースとして FSx for ONTAP ボリュームを使用するアクセスポイントでサポートされているオペレーションを示しています。

S3 オペレーション	FSx for ONTAP ボリュームにアタッチされたアクセスポイント
AbortMultipartUpload	サポート対象
CompleteMultipartUpload	サポート
CopyObject (同じリージョンへのコピーのみ)	送信元と送信先が同じアクセスポイント内にある場合、サポートされます
CreateMultipartUpload	サポート対象
DeleteObject	サポート対象
DeleteObjects	サポート対象
DeleteObjectTagging	サポート

S3 オペレーション	FSx for ONTAP ボリュームにアタッチされたアクセスポイント
GetBucketAcl	サポートされません
GetBucketCors	サポート外
GetBucketLocation	サポート
GetBucketNotificationConfiguration	サポートされません
GetBucketPolicy	サポート外
GetObject	サポート
GetObjectAcl	サポート外
GetObjectAttributes	サポート
GetObjectLegalHold	サポートされません
GetObjectRetention	サポート外
GetObjectTagging	サポート対象
HeadBucket	サポート対象
HeadObject	サポート対象
ListMultipartUploads	サポート対象
ListObjects	サポート対象
ListObjectsV2	サポート
ListObjectVersions	サポート外
ListParts	サポート
Presign	サポート外

S3 オペレーション	FSx for ONTAP ボリュームにアタッチされたアクセスポイント
PutObject	サポート
PutObjectAcl	サポートされません
PutObjectLegalHold	サポートされません
PutObjectRetention	サポート外
PutObjectTagging	サポート
RestoreObject	サポート外
UploadPart	サポート
UploadPartCopy (同じリージョンへのコピーのみ)	送信元と送信先が同じアクセスポイント内にある場合、サポートされます

Amazon S3 オペレーションの使用に関する制限は次のとおりです。

- アップロードの最大オブジェクトサイズは 5 GB ですが、それより大きいオブジェクトをダウンロードできます
- FSX_ONTAP はサポートされている唯一のストレージクラスです
- SSE-FSX は、サポートされている唯一のサーバー側の暗号化モードです
- 次の Amazon S3 機能はサポートされていません。アクセスコントロールリスト (ACLs)、リクエスタ支払い、オブジェクトバージョニング、オブジェクトロック、オブジェクトライフサイクル、静的ウェブサイトホスティング (ウェブサイトリダイレクトなど) 、多要素認証 (MFA)、条件付き書き込み

アクセスポイントを使用してファイルデータに対してデータアクセスオペレーションを実行する例については、「」を参照してくださいアクセスポイントの使用。

オブジェクト ETag

エンティティタグは、オブジェクトのハッシュです。ETag は、オブジェクトのコンテンツに加えた変更のみを反映し、メタデータに加えた変更は反映しません。ETag はオブジェクトデータの MD5 ダイジェストではありません。

オブジェクトチェックサム

チェックサム値を使用して、アップロードするデータの整合性を検証できます。データをアップロードしてチェックサムアルゴリズムを指定すると、 AWS SDK は選択したチェックサムアルゴリズムを使用して、データ転送前にチェックサム値を計算します。次に、Amazon S3 はデータのチェックサムを個別に計算し、指定されたチェックサム値と照合して検証します。オブジェクトは、Amazon S3 への転送中にデータの整合性が維持されたことを確認した後にのみ受け入れられます。Amazon S3 汎用バケット内のオブジェクトのチェックサムとは異なり、チェックサム値はオブジェクトメタデータおよびオブジェクト自体として FSx for NetApp ONTAP ボリュームに保存されません。つまり、チェックサム値はレスポンスで返されず、ダウンロード時のオブジェクトの整合性の検証には使用されません。

Amazon FSx を使用したサーバー側の暗号化 (SSE-FSX)

すべての Amazon FSx ファイルシステムはデフォルトで暗号化が設定されており、 を使用して管理されるキーを使用して保管時に暗号化されます AWS Key Management Service。データは、ファイルシステムに書き込まれ、ファイルシステムから読み取られると、ファイルシステムで自動的に暗号化および復号されます。これらのプロセスは Amazon FSx によって透過的に処理されます。

マルチパートアップロード

マルチパートアップロードを使用すると、単一のオブジェクトをパートのセットとしてアップロードすることができます。各パートは、オブジェクトのデータの連続する部分です。これらのオブジェクトパートは、任意の順序で個別にアップロードできます。マルチパートアップロードでは、FSx for ONTAP で S3 アクセスポイントを使用する場合に以下の考慮事項があります。

- 進行中のマルチパートアップロード (不完全なアップロード) に関連付けられたパートは、FSx for ONTAP ボリュームバックアップに含まれません。
- 進行中のマルチパートアップロード (不完全なアップロード) パーツに関連付けられた使用済みストレージは、送信先ボリュームの`StorageUsed`ストレージ容量 CloudWatch メトリクスには反映されませんが、親ファイルシステムの`StorageUsed`ストレージ容量 CloudWatch メトリクスには反映されます。
- マルチパートアップロードオペレーションが完了すると、関連付けられたパートメタデータは オブジェクトに保存されなくなります。つまり、 を使用してオブジェクトパートのメタデータを取

得GetObjectAttributesしたり、読み取り対象のオブジェクトのパート番号でオブジェクトの単一のパートをダウンロードしたりすることはできません。

アクセスポイントアクセスの管理

各 S3 アクセスポイントは、そのアクセスポイントを使用して行われたリクエストに対して S3 が適用する個別のアクセス許可とネットワークコントロールで設定できます。S3 アクセスポイントは、リソース、ユーザー、またはその他の条件別にアクセスポイントの使用を制御するために使用できる AWS Identity and Access Management (IAM) リソースポリシーをサポートします。アプリケーションまたはユーザーがアクセスポイントを介してファイルにアクセスするには、アクセスポイントと基になるボリュームの両方がリクエストを許可する必要があります。詳細については、「IAM アクセスポイントポリシー」を参照してください。

FSx for ONTAP の Amazon S3 アクセスポイントは、IAM AWS アクセス許可とファイルシステムレベルのアクセス許可を組み合わせた二層式認可モデルを使用します。このアプローチにより、データアクセスリクエストが AWS サービスレベルと基盤となるファイルシステムレベルの両方で適切に承認されます。

アプリケーションまたはユーザーがアクセスポイントを介してデータに正常にアクセスするには、S3 アクセスポイントポリシーと基盤となる FSx for ONTAP ボリュームの両方がリクエストを許可する必要があります。

トピック

- ファイルシステムのユーザー ID と認可
- S3 API リクエストの承認
- S3 ブロックパブリックアクセス
- IAM アクセスポイントポリシー

ファイルシステムのユーザー ID と認可

FSx for ONTAP ボリュームの S3 アクセスポイントを作成するときは、そのアクセスポイントを介して行われたすべてのファイルシステムリクエストを承認するために使用するファイルシステム ID を指定します。このファイルシステムアイデンティティは、ファイルシステムのアクセス許可モデルに基づいて、基盤となるファイルとディレクトリへのアクセスレベルを決定します。ファイルシステムのユーザーは、基盤となる Amazon FSx ファイルシステムのユーザーアカウントです。ファイルシステムユーザーに読み取り専用アクセスがある場合、アクセスポイントを使用して行われた読み取り

リクエストのみが承認され、書き込みリクエストはブロックされます。ファイルシステムユーザーに読み取り/書き込みアクセスがある場合、アクセスポイントを使用してアタッチされたボリュームへの読み取りリクエストと書き込みリクエストの両方が許可されます。

ファイルシステム ID は、次の 2 つのタイプのいずれかになります。

- UNIX ID – UNIX セキュリティスタイルでボリュームにアクセスするときは、UNIX ID (ユーザー名) を使用します。
- Windows Identity – NTFS セキュリティスタイルでボリュームにアクセスするときは、Windows ID (ドメインとユーザー名) を使用します。

UNIX または Windows ID を指定すると、アクセスポイントを介して実行されるすべての S3 API オペレーションは、ファイルシステムに対するそのユーザーのアクセス許可を使用して承認されます。

アクセスポイントに関連付けるファイルシステム ID によって、ファイルとディレクトリへのアクセスレベルが決まります。たとえば、アクセスポイントをルート UNIX ID (UID 0) に関連付けると、通常はファイルシステムに対する完全なファイルアクセス許可を持つため、すべてのファイルオペレーションが許可されます。逆に、アクセスポイントを制限されたユーザー ID に関連付けると、ファイルオペレーションは、ファイルシステムのアクセス許可モデルに基づいてそのユーザーがアクセスできるものに制限されます。

UNIX セキュリティスタイルのボリュームには UNIX ファイルシステム ID タイプを使用し、NTFS セキュリティスタイルのボリュームには Windows ID タイプを使用する必要があります。この調整により、認可モデルがボリュームのセキュリティ設定と一致するようになります。

UNIX セキュリティスタイルボリュームの場合、ファイルシステムはモードビットまたは NFSv4 ACLs を使用してアクセスを制御します。NTFS セキュリティスタイルボリュームの場合、ファイルシステムは Windows ACLs を使用してアクセスを制御します。

> **Important**
>
> S3 アクセスポイントを FSx for ONTAP ボリュームにアタッチしても、ボリュームが NFS または SMB 経由で直接アクセスされるときのボリュームの動作は変わりません。ボリュームに対する既存のオペレーションはすべて、以前と同じように動作し続けます。S3 アクセスポイントポリシーに含める制限は、アクセスポイントを使用して行われたリクエストにのみ適用されます。

S3 API リクエストの承認

FSx for NetApp ONTAP ボリュームにアタッチされたアクセスポイントを介して S3 API リクエストを行うと、Amazon S3 は呼び出し元プリンシパルの IAM アクセス許可をアクセスポイントの IAM リソースポリシーに対して評価します。IAM プリンシパル呼び出し元は、アイデンティティベースのポリシーを通じて必要なアクセス許可を付与されている必要があり、アクセスポイントのリソースポリシーもリクエストされたアクションを許可する必要があります。

Amazon S3 は、ユーザーポリシー、アクセスポイントポリシー、VPC エンドポイントポリシー、サービスコントロールポリシーなど、関連するすべてのポリシーを評価して、リクエストを承認するかどうかを判断します。

また、特定の Virtual Private Cloud (VPC) からのリクエストのみを受け入れるように S3 アクセスポイントを設定して、データアクセスを制限することもできます。詳細については、「Virtual Private Cloud に制限されたアクセスポイントの作成」を参照してください。

S3 ブロックパブリックアクセス

FSx for ONTAP ボリュームにアタッチされた Amazon S3 アクセスポイントは、パブリックアクセスブロックを有効にして自動的に設定されます。これは変更できません。

IAM アクセスポイントポリシー

Amazon S3 アクセスポイントは、リソース、ユーザー、またはその他の条件別にアクセスポイントの使用を制御できる AWS Identity and Access Management (IAM) リソースポリシーをサポートします。アプリケーションまたはユーザーがアクセスポイントを介してオブジェクトにアクセスできるようにするには、アクセスポイントと基盤となるデータソースの両方がリクエストを許可する必要があります。

オプションのアクセスポイントポリシーを作成するには、 アクセス`s3:PutAccessPointPolicy`許可が必要です。

S3 アクセスポイントを Amazon FSx ボリュームにアタッチすると、ボリュームに対する既存のすべてのオペレーションは以前と同じように動作し続けます。アクセスポイントポリシーに含めた制限は、そのアクセスポイントを介したリクエストにのみ適用されます。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Amazon FSx コンソールを使用して FSx for ONTAP ボリュームにアタッチされたアクセスポイントを作成するときに、アクセスポイントポリシーを設定できます。 FSx 既存の S3 アクセスポイント

でアクセスポイントポリシーを追加、変更、または削除するには、S3 コンソール、CLI、または API を使用できます。

アクセスポイントの作成

Amazon FSx コンソール、CLI、API、およびサポートされている SDKs を使用して、Amazon FSx ボリュームにアタッチする S3 アクセスポイントを作成および管理できます。

> **Note**
>
> 他のユーザーがアクセスポイントを使用できるように S3 アクセスポイント名を公開する場合があるため、S3 アクセスポイント名に機密情報を含めないでください。アクセスポイント名は、ドメインネームシステム (DNS) と呼ばれるパブリックアクセス可能なデータベースに公開されます。アクセスポイント名の詳細については、「」を参照してくださいアクセスポイントの命名規則。

必要なアクセス許可

Amazon FSx ボリュームにアタッチされた S3 アクセスポイントを作成するには、次のアクセス許可が必要です。

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`

Amazon FSx または S3 コンソールを使用してオプションのアクセスポイントポリシーを作成するには、 アクセス`s3:PutAccessPointPolicy`許可が必要です。詳細については、「IAM アクセスポイントポリシー」を参照してください。

アクセスポイントを作成するには、以下のトピックを参照してください。

トピック

- アクセスポイントの作成
- Virtual Private Cloud に制限されたアクセスポイントの作成

アクセスポイントの作成

ボリュームの S3 アクセスポイントを作成するときは、FSx for ONTAP ボリュームがアカウントに既に存在している必要があります。

FSx for OpenZFS ボリュームにアタッチされた S3 アクセスポイントを作成するには、次のプロパティを指定します。

- アクセスポイント名。アクセスポイントの命名規則の詳細については、「」を参照してくださいアクセスポイントの命名規則。
- アクセスポイントを使用して行われたファイルアクセスリクエストを承認するために使用するファイルシステムのユーザー ID。含める POSIX ユーザー名を UNIX または Windows のいずれかに指定します。詳細については、「ファイルシステムのユーザー ID と認可」を参照してください。
- アクセスポイントのネットワーク設定は、アクセスポイントがインターネットからアクセス可能かどうか、またはアクセスが特定の仮想プライベートクラウド (VPC) に制限されているかどうかを決定します。詳細については、「Virtual Private Cloud に制限されたアクセスポイントの作成」を参照してください。

FSx ボリュームにアタッチされた S3 アクセスポイントを作成するには (FSx 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. ページ上部のナビゲーションバー AWS リージョン で、アクセスポイントを作成する を選択します。アクセスポイントは、関連付けられたボリュームと同じリージョンに作成する必要があります。
3. ナビゲーションペインで [ボリューム] を選択します。
4. ボリュームページで、アクセスポイントをアタッチする FSx for ONTAP ボリュームを選択します。
5. アクションメニューから S3 アクセスポイントの作成 を選択して、S3 アクセスポイントの作成ページを表示します。
6. アクセスポイント名に、アクセスポイントの名前を入力します。アクセスポイント名のガイドラインと制限の詳細については、「」を参照してくださいアクセスポイントの命名規則。

   データソースの詳細には、ステップ 3 で選択したボリュームの情報が入力されます。
7. ファイルシステムのユーザー ID は、このアクセスポイントを使用して行われたファイルアクセスリクエストを認証するために Amazon FSx によって使用されます。指定するファイルシステ

ムユーザーに、FSx for ONTAP ボリュームに対する正しいアクセス許可があることを確認してください。

ファイルシステムのユーザー ID タイプで、UNIX または Windows を選択します。

8. Username には、ユーザーのユーザー名を入力します。
9. ネットワーク設定パネルで、アクセスポイントがインターネットからアクセス可能か、アクセスが特定の仮想プライベートクラウドに制限されるかを選択します。

   ネットワークオリジンで、インターネットを選択してインターネットからアクセスポイントにアクセスできるようにするか、仮想プライベートクラウド (VPC) を選択して、アクセスポイントへのアクセスを制限する VPC ID を入力します。

   アクセスポイントのネットワークオリジンの詳細については、「Virtual Private Cloud に制限されたアクセスポイントの作成」を参照してください。
10. (オプション) アクセスポイントポリシー - オプションで、オプションのアクセスポイントポリシーを指定します。ポリシーの警告、エラー、提案は必ず解決してください。アクセスポイントポリシーの指定の詳細については、Amazon Simple Storage Service ユーザーガイドの「アクセスポイントを使用するための IAM ポリシーの設定」を参照してください。
11. アクセスポイントの作成を選択して、アクセスポイントのアタッチメント設定を確認します。

FSx ボリュームにアタッチされた S3 アクセスポイントを作成するには (CLI)

次のコマンド例では、アカウント の FSx for ONTAP ボリュームにアタッチ*my-ontap-ap*されている という名前*fsvol-0123456789abcdef9*のアクセスポイントを作成します*111122223333*。

```
$ aws fsx create-and-attach-s3-access-point --name my-ontap-ap --type ONTAP --ontap-configuration \
   VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-user}}' \
   --s3-access-point VpcConfiguration='{VpcId=vpc-0123467},Policy=access-point-policy-json
```

リクエストが成功すると、システムは新しい S3 アクセスポイントアタッチメントを返すことで応答します。

```
$ {
  {
     "S3AccessPointAttachment": {
```

```
        "CreationTime": 1728935791.8,
        "Lifecycle": "CREATING",
        "LifecycleTransitionReason": {
            "Message": "string"
        },
        "Name": "my-ontap-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "ec2-user"
                }
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-0123467"
        }
    }
  }
}
```

Virtual Private Cloud に制限されたアクセスポイントの作成

アクセスポイントを作成するときは、インターネットからアクセスポイントにアクセスできるようにするか、そのアクセスポイントを介して行われるすべてのリクエストが特定の Amazon Virtual Private Cloud から発信されるように指定できます。インターネットからアクセス可能なアクセスポイントは、Internet をネットワークオリジンとすると言います。インターネット上のどこからでも使用できます。ただし、アクセスポイント、基盤となるバケットまたは Amazon FSx ボリューム、およびリクエストされたオブジェクトなどの関連リソースに対するその他のアクセス制限が適用されます。指定された Amazon VPC からのみアクセス可能なアクセスポイントのネットワークオリジンは でありVPC、Amazon S3 はその Amazon VPC から発信されていないアクセスポイントに対して行われたリクエストを拒否します。

> **Important**
>
> アクセスポイントのネットワークオリジンは、アクセスポイントの作成時にのみ指定できます。アクセスポイントの作成後は、そのネットワークオリジンを変更できません。

アクセスポイントを Amazon VPC のみのアクセスに制限するには、アクセスポイントを作成するリクエストに VpcConfigurationパラメータを含めます。VpcConfiguration パラメータで、アクセスポイントを使用できるようにする Amazon VPC ID を指定します。アクセスポイントを介してリクエストが行われた場合、リクエストは Amazon VPC から発信する必要があります。そうしないとAmazon S3はリクエストを拒否します。

アクセスポイントのネットワークオリジンは AWS CLI、、 AWS SDKs、または REST APIs を使用して取得できます。アクセスポイントに Amazon VPC 設定が指定されている場合、そのネットワークオリジンは ですVPC。それ以外の場合、アクセスポイントのネットワークオリジンは Internet です。

Example

例: Amazon VPC アクセスに制限されたアクセスポイントを作成する

次の例では、vpc-1a2b3cAmazon VPC からのアクセスのみ123456789012を許可する amzn-s3-demo-bucket アカウントの バケットexample-vpc-apに という名前のアクセスポイントを作成します。次に、新しいアクセスポイントのネットワークオリジンが VPC であることを確認します。

AWS CLI

```
$ aws fsx create-and-attach-s3-access-point --name example-vpc-ap --type ONTAP --
ontap-configuration \

 VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-
user}}' \
   --s3-access-point VpcConfiguration='{VpcId=vpc-id},Policy=access-point-policy-
json
```

```
$ {
  {
     "S3AccessPointAttachment": {
        "Lifecycle": "CREATING",
        "CreationTime": 1728935791.8,
        "Name": "example-vpc-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "my-unix-user"
                }
```

```
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-
vpc-ap",
            "Alias": "access-point-abcdef0123456789ab12jj77xy51zacd4-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-1a2b3c"
            }
        }
    }
}
```

Amazon VPC でアクセスポイントを使用するには、Amazon VPC エンドポイントのアクセスポリシーを変更する必要があります。Amazon VPC エンドポイントを使用すると、トラフィックは Amazon VPC から Amazon S3 に流れることができます。Amazon VPC 内のリソースが Amazon S3 とやり取りする方法を制御するアクセスコントロールポリシーがあります。Amazon VPC から Amazon S3 へのリクエストは、Amazon VPC エンドポイントポリシーがアクセスポイントと基盤となるバケットの両方へのアクセスを許可する場合にのみ、アクセスポイントを介して成功します。

> **Note**
>
> Amazon VPC 内でのみリソースにアクセスできるようにするには、Amazon VPC エンドポイントのプライベートホストゾーンを必ず作成してください。プライベートホストゾーンを使用するには、Amazon VPC ネットワーク属性 と が に設定されるように Amazon VPC 設定を変更しますtrue。 https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support enableDnsHostnames enableDnsSupport

次のポリシーステートメントの例では、 GetObjectおよび という名前のアクセスポイントへの呼び出しを許可するように Amazon VPC エンドポイントを設定しますexample-vpc-ap。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Principal": "*",
```

```
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:us-east-1:123456789012:accesspoint/example-vpc-ap/object/
*"
        ]
    }]
}
```

> **Note**
>
> この例の `Resource` 宣言では、Amazon リソースネーム (ARN) を使用してアクセスポイントを指定します。

Amazon VPC エンドポイントポリシーの詳細については、Amazon S3のゲートウェイエンドポイント」を参照してください。

Amazon S3 アクセスポイントの管理

このセクションでは、 AWS マネジメントコンソール、 AWS Command Line Interface、または API を使用して Amazon S3 アクセスポイントを管理および使用する方法について説明します。

トピック

- S3 アクセスポイントアタッチメントの一覧表示
- アクセスポイントの詳細の表示
- S3 アクセスポイントアタッチメントの削除

S3 アクセスポイントアタッチメントの一覧表示

このセクションでは、 AWS マネジメントコンソール、 AWS Command Line Interface、または REST API を使用して S3 アクセスポイントを一覧表示する方法について説明します。

FSx for ONTAP ボリュームにアタッチされているすべての S3 アクセスポイントを一覧表示するには (Amazon FSx 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. コンソールの左側にあるナビゲーションペインで、ボリュームを選択します。
3. ボリュームページで、アクセスポイントアタッチメントを表示する ONTAP ボリュームを選択します。
4. ボリュームの詳細ページで S3 を選択して、ボリュームにアタッチされているすべての S3 アクセスポイントのリストを表示します。

FSx for ONTAP ボリュームにアタッチされているすべての S3 アクセスポイントを一覧表示するには (AWS CLI)

次のコマンド`describe-s3-access-point-attachments`例は、 を使用して S3 アクセスポイントアタッチメント AWS CLI を一覧表示する方法を示しています。

次のコマンドは、FSx for ONTAP ファイルシステム fs-0abcdef123456789 のボリュームにアタッチされているすべての S3 アクセスポイントを一覧表示します。

```
aws fsx describe-s3-access-point-attachments --filter {[Name: file-system-id, Values:
{[fs-0abcdef123456789]}}
```

次のコマンドは、FSx for ONTAP ボリューム vol-9abcdef123456789] にアタッチされた S3 アクセスポイントを一覧表示します。

```
aws fsx describe-s3-access-point-attachments --filter {[Name: volume-id, Values:
{[vol-9abcdef123456789]}}
```

詳細と例については、「AWS CLI コマンドリファレンス」の「list-access-points」を参照してください。

アクセスポイントの詳細の表示

このセクションでは、 AWS マネジメントコンソール、 AWS Command Line Interface、または REST API を使用して S3 アクセスポイントの詳細を表示する方法について説明します。

FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントの詳細を表示するには (Amazon FSx 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. 詳細を表示するアクセスポイントにアタッチされているボリュームに移動します。
3. ボリュームにアタッチされたアクセスポイントのリストを表示するには、S3 を選択します。

4. 詳細を表示するアクセスポイントを選択します。
5. S3 アクセスポイントアタッチメントの概要で、選択したアクセスポイントの設定の詳細とプロパティを表示します。

   ファイルシステムのユーザー ID 設定と S3 アクセスポイントのアクセス許可ポリシーも、アクセスポイントアタッチメントについて一覧表示されます。
6. Amazon S3 コンソールでアクセスポイントの S3 設定を表示するには、S3 アクセスポイントの下に表示される S3 アクセスポイント名を選択します。 Amazon S3 Amazon S3 コンソールのアクセスポイントの詳細ページに移動します。

S3 アクセスポイントアタッチメントの削除

このセクションでは、 AWS マネジメントコンソール、 AWS Command Line Interface、または REST API を使用して S3 アクセスポイントを削除する方法について説明します。

S3 アクセスポイントアタッチメントを削除するには、`fsx:DetatchAndDeleteS3AccessPoint`および アクセス`s3control:DeleteAccessPoint`許可が必要です。

FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントを削除するには (Amazon FSx 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. 削除する S3 アクセスポイントアタッチメントがアタッチされているボリュームに移動します。
3. S3にアタッチされた S3 アクセスポイントのリストを表示するには、S3 を選択します。
4. 削除する S3 アクセスポイントアタッチメントを選択します。
5. [削除] を選択します。
6. S3 アクセスポイントを削除することを確認し、削除を選択します。

FSx for ONTAP ボリュームにアタッチされた S3 アクセスポイントを削除するには (AWS CLI)

- S3 アクセスポイントアタッチメントを削除するには、次の例に示すように、 detach-and-delete-s3-access-point CLI コマンド (または同等の DetachAndDeleteS3AccessPoint API オペレーション) を使用します。`--name` プロパティを使用して、削除する S3 アクセスポイントアタッチメントの名前を指定します。

```
aws fsx detach-and-delete-s3-access-point \
```

```
    --region us-east-1 \
    --name my-ontap-ap
```

アクセスポイントの使用

次の例は、アクセスポイントを使用して、S3 API を使用して FSx for ONTAP ボリュームに保存されているファイルデータにアクセスする方法を示しています。FSx for ONTAP ボリュームにアタッチされたアクセスポイントでサポートされている Amazon S3 API オペレーションの完全なリストについては、「」を参照してくださいアクセスポイントの互換性。

> **Note**
>
> FSx for ONTAP ボリューム上のファイルは、 StorageClassの で識別されますFSX_ONTAP。

トピック

- S3 アクセスポイントを使用したファイルのダウンロード
- S3 アクセスポイントを使用したファイルのアップロード
- S3 アクセスポイントを使用したファイルの一覧表示
- S3 アクセスポイントを使用したファイルのタグ付け
- S3 アクセスポイントを使用したファイルの削除

S3 アクセスポイントを使用したファイルのダウンロード

次のコマンドget-object例は、 を使用してアクセスポイント経由でファイル AWS CLI をダウンロードする方法を示しています。ダウンロードしたオブジェクトのファイル名である outfile を含める必要があります。

この例では、アクセスポイントmy-image.jpgを介してファイルをリクエストmy-ontap-apし、ダウンロードしたファイルを として保存しますdownload.jpg。

```
$ aws s3api get-object --key my-image.jpg --bucket my-ontap-ap-
hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias download.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "Mon, 14 Oct 2024 17:01:48 GMT",
```

```
    "ContentLength": 141756,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb-1\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "SSE_FSX",
    "Metadata": {},
    "StorageClass": "FSX_ONTAP"
}
```

REST API を使用して、アクセスポイントを介してオブジェクトをダウンロードすることもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

S3 アクセスポイントを使用したファイルのアップロード

次のコマンドput-object例は、 を使用してアクセスポイントを介してファイル AWS CLI をアップロードする方法を示しています。アップロードされたオブジェクトのファイル名である outfile を含める必要があります。

この例では、アクセスポイント*my-new-image.jpg*を介してファイルをアップロード*my-ontap-ap*し、アップロードしたファイルを として保存します*my-new-image.jpg*。

```
$ aws s3api put-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-new-image.jpg --body  my-new-image.jpg
```

REST API を使用して、アクセスポイントを介してオブジェクトをアップロードすることもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObject」を参照してください。

S3 アクセスポイントを使用したファイルの一覧表示

次の の例では、リージョン のアカウント ID *my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b*-ext-s3aliasが所有するアクセスポイントエイリアスを介してファイルを一覧表示*111122223333*します*us-east-2*。

```
$ aws s3api list-objects-v2 --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias
{
    "Contents": [
        {
            "Key": ".hidden-dir-with-data/file.txt",
            "LastModified": "2024-10-29T14:22:05.4359",
```

```
            "ETag": "\"88990077ab44cd55ef66aa77-1\"",
            "Size": 18,
            "StorageClass": "FSX_ONTAP"
        },
        {
            "Key": "documents/report.rtf",
            "LastModified": "2024-11-02T10:18:15.6621",
            "ETag": "\"ab12cd34ef56a89219zg6aa77-1\"",
            "Size": 1048576,
            "StorageClass": "FSX_ONTAP"
        },
    ]
}
```

REST API を使用してファイルを一覧表示することもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「ListObjectsV2」を参照してください。

S3 アクセスポイントを使用したファイルのタグ付け

次のコマンドput-object-tagging例は、 を使用してアクセスポイントを介してタグセット AWS CLI を追加する方法を示しています。各タグはキーバリューのペアです。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「タグを使用してストレージを分類する」を参照してください。

この例では、アクセスポイント my-image.jpgを使用して既存のファイルにタグセットを追加しますmy-ontap-ap。

```
$ aws s3api put-object-tagging --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg --tagging TagSet=[{Key="finance",Value="true"}]
```

REST API を使用して、アクセスポイントを介してオブジェクトにタグセットを追加することもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectTagging」を参照してください。

S3 アクセスポイントを使用したファイルの削除

次のコマンドdelete-object例は、 を使用してアクセスポイントを介してファイル AWS CLI を削除する方法を示しています。

```
$ aws s3api delete-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg
```

REST API を使用して、アクセスポイントを介してオブジェクトを削除することもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteObject」を参照してください。

S3 アクセスポイントの問題のトラブルシューティング

このセクションでは、S3 アクセスポイントから FSx データにアクセスする際に問題が発生した場合の症状、原因、解決策について説明します。

ファイルシステムが S3 リクエストを処理できない

特定のワークロードの S3 リクエストボリュームがトラフィックを処理するファイルシステムの容量を超える場合、S3 リクエストエラー (、`Internal Server Error`503 `Slow Down`、 など) が発生する可能性がありますService Unavailable。Amazon CloudWatch メトリクス (や など) を使用して、ファイルシステムのパフォーマンスをプロアクティブにモニタリングNetwork throughput utilizationおよびアラームできますCPU utilization。パフォーマンスが低下した場合は、ファイルシステムのスループットキャパシティを増やすことでこの問題を解決できます。

自動的に作成されたサービスロールのデフォルトの S3 アクセスポイントアクセス許可でアクセスが拒否されました

一部の S3-integrated AWS サービスは、カスタムサービスロールを作成し、アタッチされたアクセス許可を特定のユースケースにカスタマイズします。S3 アクセスポイントエイリアスを S3 リソースとして指定する場合、アタッチされたアクセス許可には、アクセスポイント ARN 形式 (などarn:aws:s3:::my-fsx-ap-foo7detztxouyjpwtu8krroppxytruse1a-ext-s3alias) ではなくバケット ARN 形式 (など) を使用するアクセスポイントが含まれる場合がありますarn:aws:s3:us-east-1:1234567890:accesspoint/my-fsx-ap。これを解決するには、アクセスポイントの ARN を使用するようにポリシーを変更します。

他の AWS サービスからのデータへのアクセス

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 Amazon Elastic VMware Service を使用します

- 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。

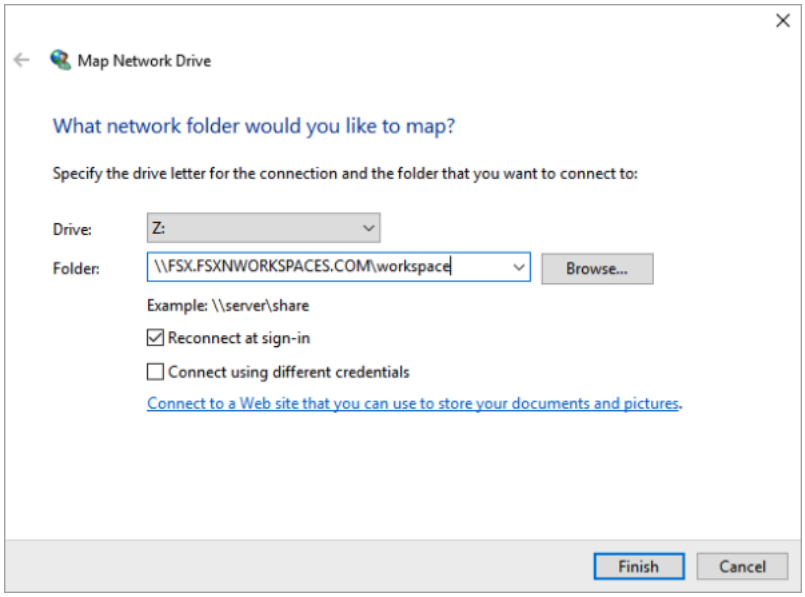
ステップ 1: Amazon FSx を使用してドメインユーザー用のプロファイルフォルダの場所を作成する

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を結合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、「FSx for ONTAP 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

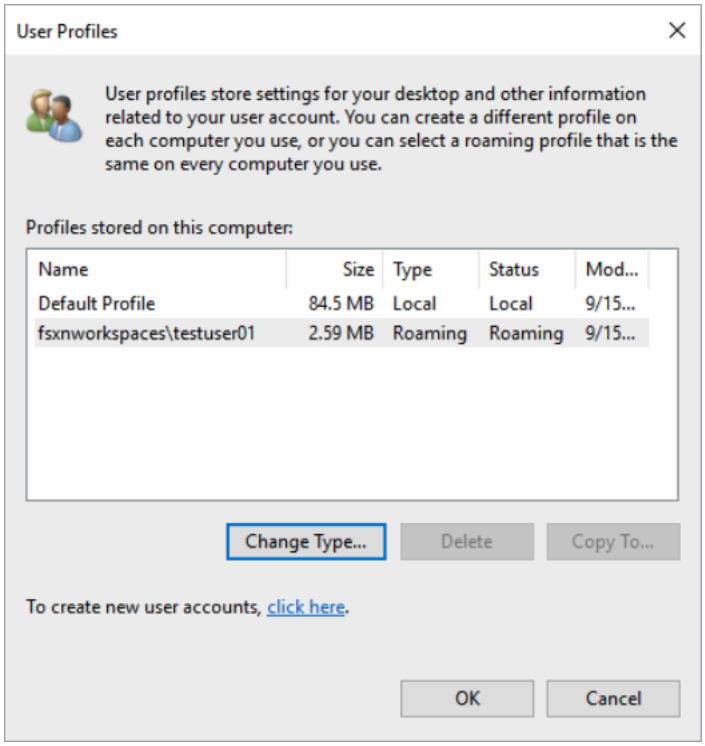
1. テストユーザーの WorkSpace で、Windows > システム > システムの詳細設定 を選択します。
2. System Properties (システムプロパティ) で、Advanced (詳細設定) タブを選択し、User Profiles (ユーザープロファイル) セクションの Settings (設定) ボタンを押します。ログインしているユーザーのプロファイルタイプは `Local` になります。
3. WorkSpace からテストユーザーをログアウトします。
4. Amazon FSx ファイルシステム上にローミングプロファイルを配置するようにテストユーザーを設定します。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
   ```

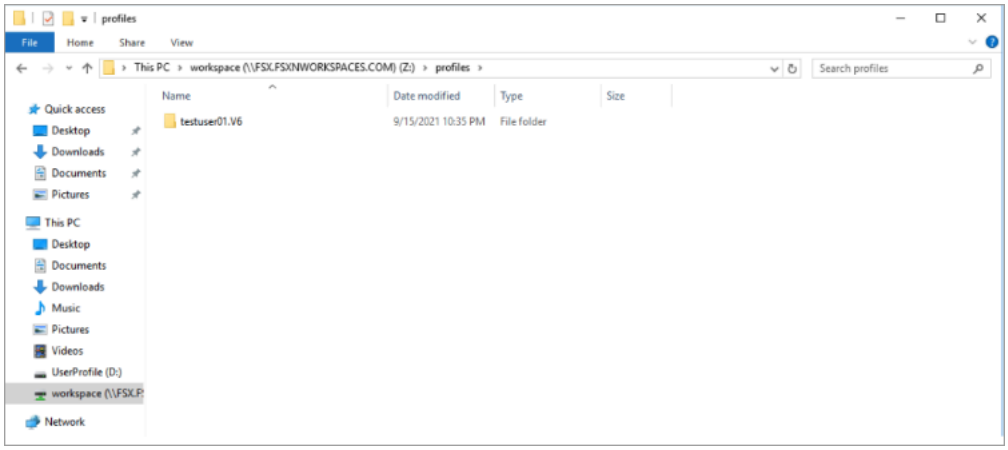
   例:

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

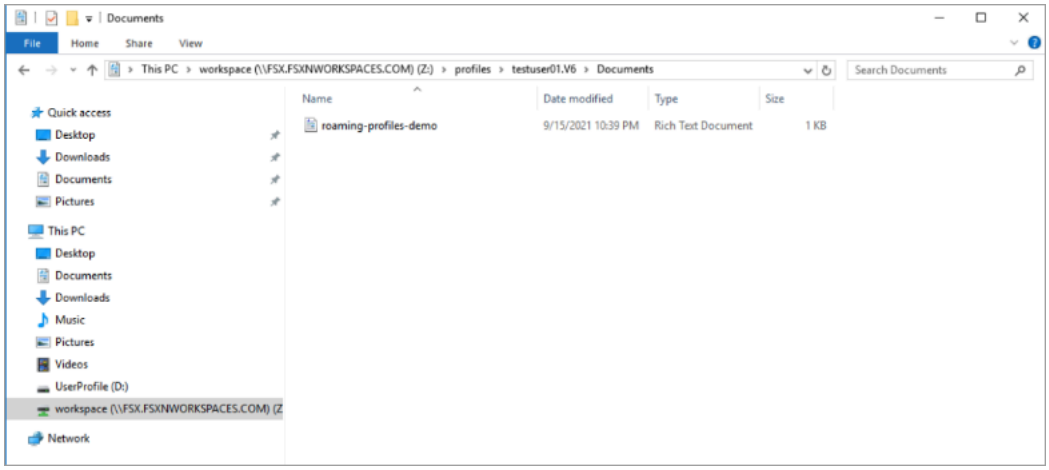
5. テストユーザー WorkSpace にログオンします。
6. System Properties (システムプロパティ) で、Advanced (詳細設定) タブを選択し、User Profiles (ユーザープロファイル) セクションの Settings (設定) ボタンを押します。ログインしているユーザーのプロファイルタイプは `Roaming` になります。



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。

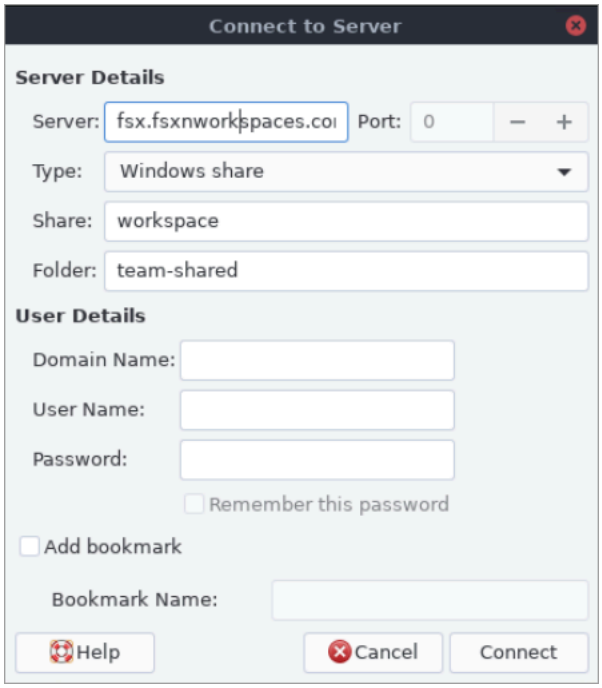
    b. タイプを `Windows share` に設定します。

    c. 共有を `workspace` などの SMB 共有の名前に設定します。

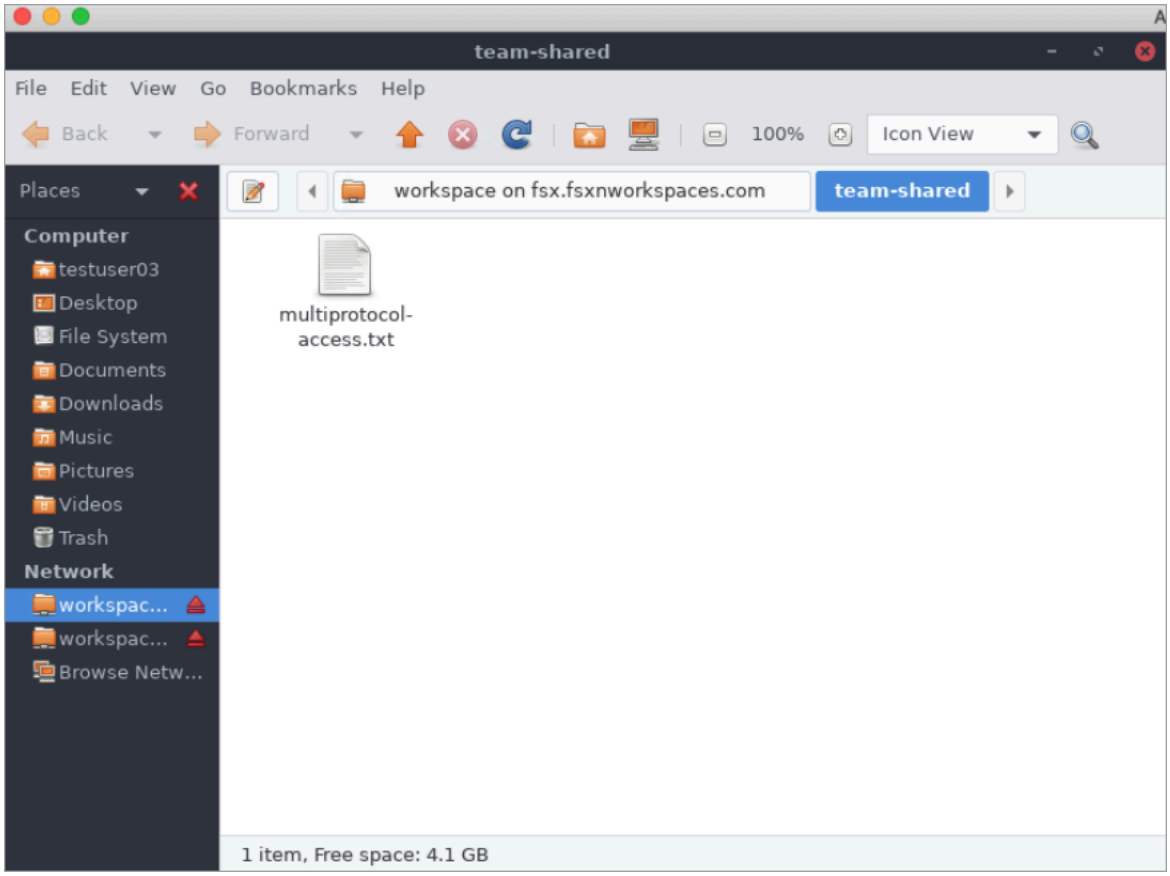
    d. フォルダは `/` のままにするか、`team-shared` という名前のフォルダなどのフォルダに設定することができます。

    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 インスタンス上の 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
   ```

   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。

   ```
   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. ドメインを結合している 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を結合している 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 Amazon Elastic VMware Service を使用します

Amazon Elastic VMware Service (Amazon EVS) ソフトウェア定義データセンター (SDDC) の外部データストアとして FSx for ONTAP を使用できます。詳細については、Amazon FSx for NetApp ONTAP を使用した高性能ワークロードの実行を参照してください。詳細な手順については、Amazon FSx for NetApp ONTAP を NFS データストアとして設定するおよび Amazon FSx for NetApp ONTAP を iSCSI データストアとして設定するをご参照ください。

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、耐久性、デプロイオプション

Amazon FSx for NetApp ONTAP は、シングル AZ およびマルチ AZ 配置タイプを使用します。シングル AZ 1、シングル AZ 2、マルチ AZ 1、マルチ AZ 2 の 4 つのオプションから選択できます。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
- ファイルシステム生成の選択
- FSx for ONTAP のフェイルオーバープロセス
- ネットワークリソース

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 ファイルシステムには、シングル AZ 1 とシングル AZ 2 を選択できます。シングル AZ 1 は 1 つの高可用性 (HA) ペアを持つ第 1 世代のファイルシステムですが、シングル AZ 2 は 1 ~ 12 の HA ペアを持つ第 2 世代のファイルシステムです。詳細については、「ファイルシステム生成の選択」を参照してください。

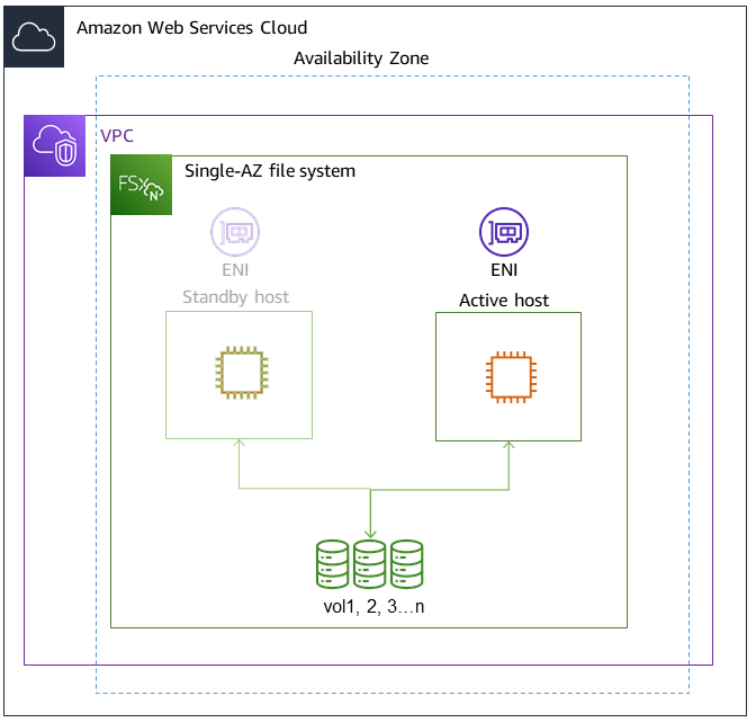
シングル AZ ファイルシステムを作成すると、Amazon FSx は、アクティブ/スタンバイ構成のファイルサーバーのペア (1 ~ 12 個) を自動的にプロビジョニングします。各ペアのアクティブなファイルサーバーとスタンバイファイルサーバーは、AWS リージョン の単一のアベイラビリティーゾーン内の個別の障害ドメインに配置されます。予定されたファイルシステムのメンテナンス中、またはアクティブファイルサーバーの予定外のサービス中断中に、Amazon FSx は、通常数秒以内に、その高可用性 (HA) ペアをスタンバイファイルサーバーに自動的かつ個別にフェイルオーバーします。フェイルオーバー中も、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、または 1 つ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、オンプレミスまたは他の AWS リージョン 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 第 1 世代のファイルシステムのアーキテクチャを示します。

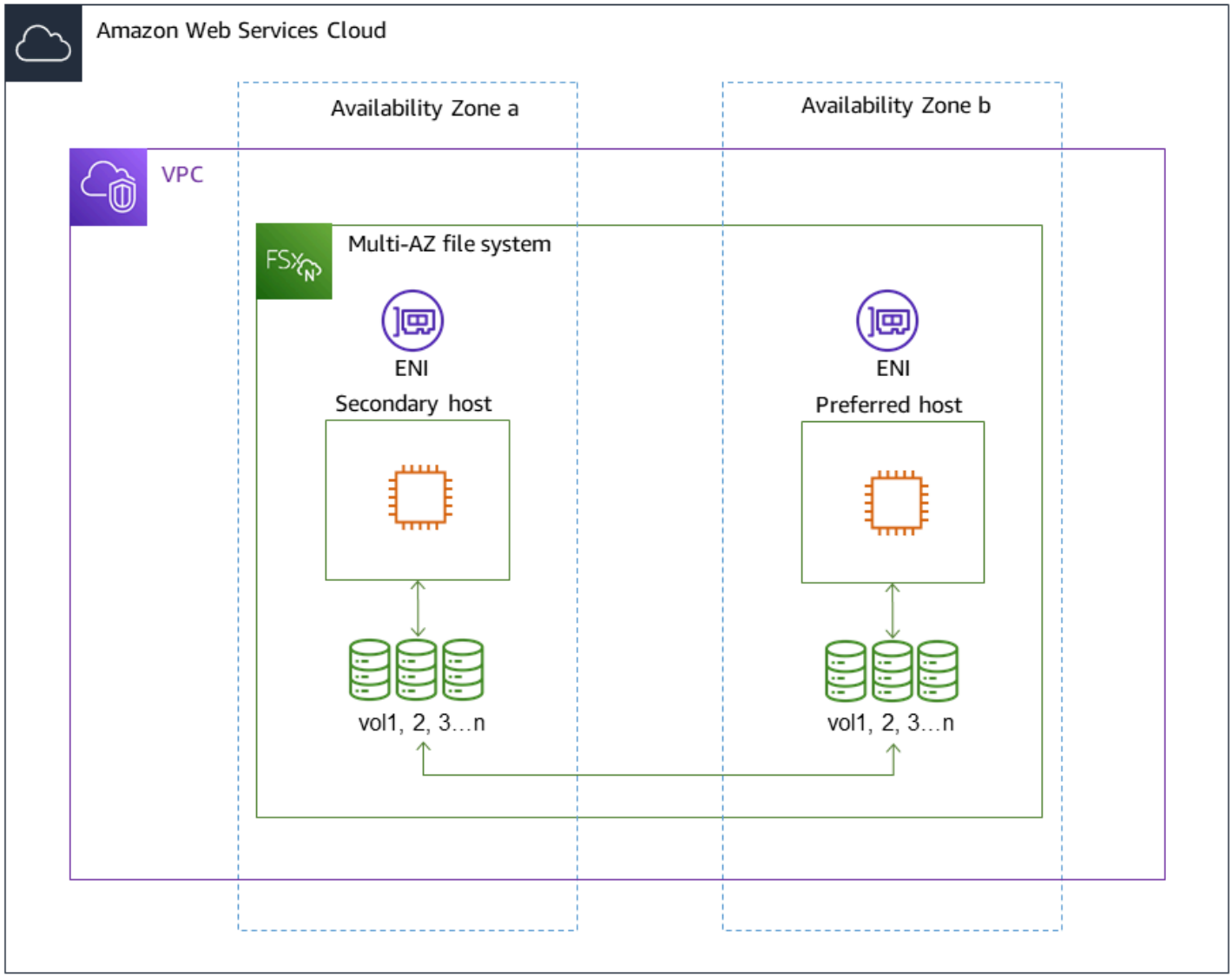


マルチ AZ デプロイのタイプ

マルチ AZ ファイルシステムでは、マルチ AZ 1 とマルチ AZ 2 を選択できます。マルチ AZ 1 は第 1 世代のファイルシステムであり、マルチ AZ 2 は第 2 世代のファイルシステムです。どちらのオプションにも 1 つの HA ペアがあります。詳細については、「ファイルシステム生成の選択」を参照してください。

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 第 1 世代のファイルシステムのアーキテクチャを示します。



ファイルシステム生成の選択

次の表は、ONTAP ファイルシステム用の第 1 世代シングル AZ と第 2 世代マルチ AZ FSx の違いを示しています。

FSx ONTAP ファイルシステム生成用

ディメンション	第 1 世代	第 2 世代 (単一 HA ペア)	第 2 世代 (マルチペア)
デプロイタイプ	SINGLE_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2
HA ペア	1 HA ペア		1 ~ 12 の HA ペア
SSD ストレージ	最小: 1 TiB 最大: 192 TiB	最小: 1 TiB 最大: 512 TiB	最小: 1 TiB (HA ペアあたり) 最大: 1 PiB (合計)
SSD IOPS	最小: SSD の 3 IOPS/GIB 最大: 160,000	最小: SSD の 3 IOPS/GIB 最大: 200,000	最小: SSD の 3 IOPS/GIB 最大: 2,400,000 (HA ペアあたり 200,000)
スループット容量	128 MBps、256 MBps、512 MBps、1,024 MBps、2,048 MBps、4,096 MBps	384 MBps、768 MBps、1,536 MBps、3,072 MBps、6,144 MBps	1,536 MBps (HA ペアあたり)、3,072 MBps (HA ペアあたり)、6,144 MBps (HA ペアあたり)

> **Note**
>
> 作成後にファイルシステムのデプロイタイプを変更することはできません。デプロイタイプを変更する場合 (シングル AZ 1 からシングル AZ 2 に移行する場合など)、データをバックアップし、新しいファイルシステムに復元できます。NetApp SnapMirror、AWS DataSync、またはサードパーティーのデータコピーツールを使用してデータを移行することもできま

す。詳細については、「NetApp SnapMirror を使用した FSx for ONTAP への移行」および「AWS DataSync を使用した FSx for ONTAP への移行」を参照してください。

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**
>
> 複数の HA ペアを持つ第 2 世代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 クラウド」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で、ファイルシステムのフェイルオーバーをテストすることができます。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。

	第 1 世代シングル AZ	第 2 世代シングル AZ	マルチ AZ
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

	第 1 世代シングル AZ	第 2 世代シングル AZ	マルチ AZ
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。

Amazon FSx for NetApp ONTAP のパフォーマンス

以下では、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示し、利用可能なパフォーマンスオプションとスループットオプションを説明して、役に立つパフォーマンスのヒントを以下に示します。

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
- パフォーマンスの詳細
- デプロイタイプがパフォーマンスに与える影響
- ストレージ容量のパフォーマンスへの影響
- スループット容量がパフォーマンスに与える影響
- 例: ストレージ容量とスループットキャパシティ

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) ストレージを使用したサブミリ秒のファイルオペレーションのレイテンシーを提供し、容量プールストレージに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 GBps 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、単一の 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。NFS クライアントのドキュメントを参照して、確認してください。nconnectはクライアントバージョンでサポートされています。nconnect の NetApp ONTAP のサポートの詳細については、「NFSv4.1 の ONTAP サポート」を参照してください。

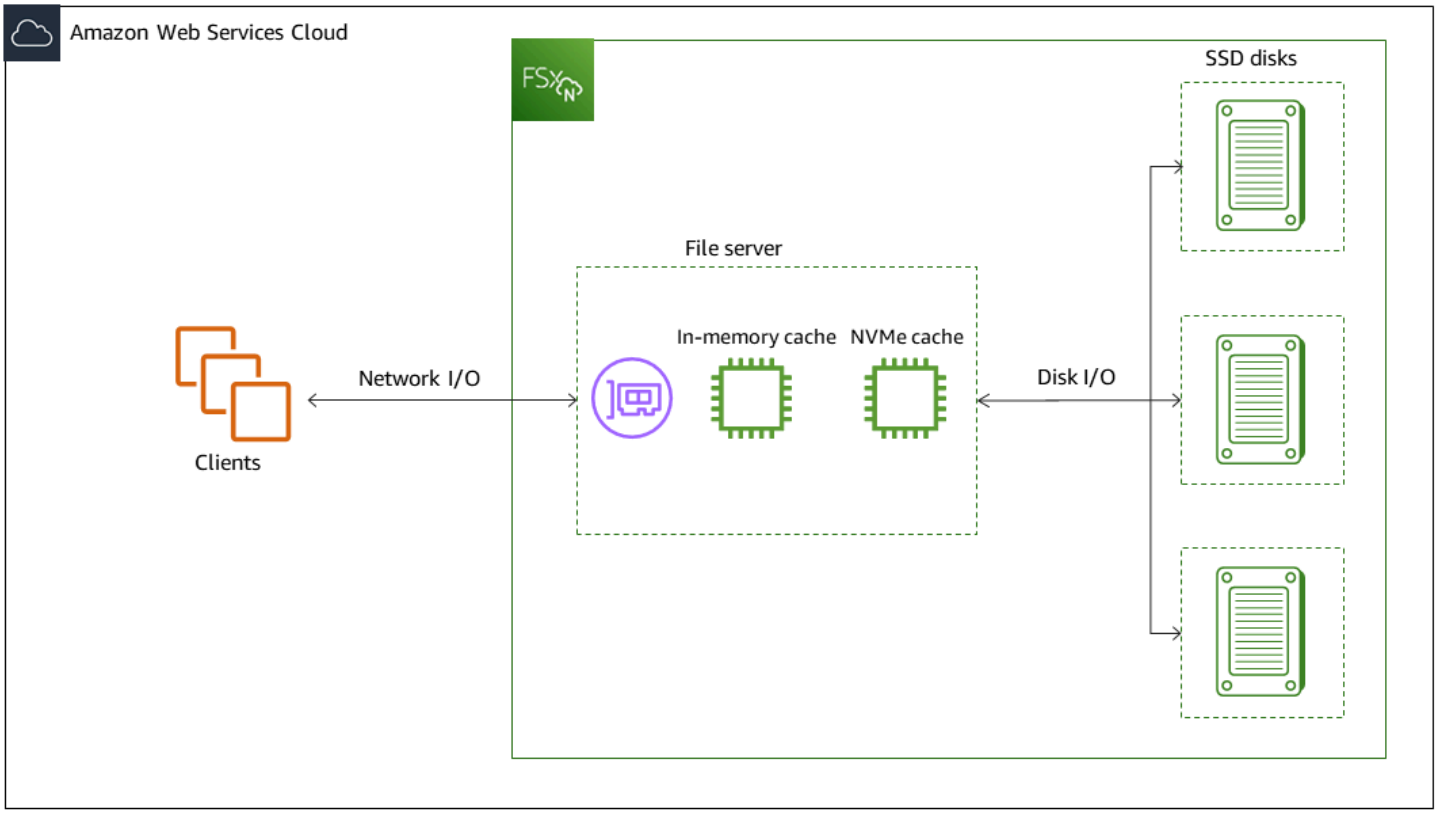
ジャンボフレーム

読み取りまたは書き込みスループットを最大化するには、クライアント EC2 インスタンスを含む Amazon FSx ファイルシステムへのデータパス内のすべてのネットワークインターフェイスでジャンボフレームを有効にすることをお勧めします。FSx for ONTAP ファイルシステムのネットワークインターフェイスのデフォルトの最大送信単位 (MTU) 設定は 9,001 バイトです。

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を詳細に理解するために、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。AWS またはオンプレミスで存在しているかどうかに関わらず、クライアントコンピューティングインスタンスは 1 つまたは複数の Elastic Network Interface (ENI) を使用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背後には、NetApp ONTAP ファイルサーバがあり、ネットワーク経由で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供給しています。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。



アーキテクチャコンポーネント (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) に対応して、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。

> **Note**
>
> iSCSI および NVMe/TCP SAN プロトコルの場合、シーケンシャル読み取りクライアント操作では、ファイルシステムの最大ネットワーク I/O バーストまたはベースラインスループットまで達成できます。

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 を使用して、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。第 1 世代のファイルシステム (シングル AZ とマルチ AZ の両方) と第 2 世代のマルチ AZ ファイルシステムは、1 つの高可用性 (HA) ペアを搭載しています。第 2 世代シングル AZ ファイルシステムは、最大 12 の HA ペアを搭載しています。詳細については、「高可用性 (HA) ペアの管理」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 1 およびマルチ AZ 2 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 ファイルシステム 1
- ペアごとのスループットキャパシティが少なくとも 6 GBps のシングル AZ ファイルシステム 2

> **Note**
>
> 第 2 世代のファイルシステム (シングル AZ 2 およびマルチ AZ 2) では、NVMe キャッシュを使用すると、高スループットまたは大規模な I/O ワークロードの合計スループットがワークロードで低下する可能性があります。スループットバウンドワークロードがある場合は、NVMe キャッシュを無効にすることをお勧めします。詳細については、「NVMe キャッシュの管理」を参照してください。

次の表は、高可用性 (HA) ペアの数や AWS リージョン 可用性などの要因に応じてスケールアップできる、ファイルシステムのスループットキャパシティを示しています。

First-generation file systems

これらのパフォーマンス仕様は、第 1 世代シングル AZ およびマルチ AZ ファイルシステムに適用されます。

第 1 世代の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 を使用できる他のすべての AWS リージョン	
	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]	1,000	2,048	750
マルチ AZ	4,096[1]	1,800	2,048	1,300

> **Note**
>
> [1] 4 GBps のスループット容量をプロビジョニングするには、ファイルシステムを 5,120 GiB 以上の SSD ストレージ容量と 16 万 SSD IOPS で構成する必要があります。

Second-generation file systems

これらのパフォーマンス仕様は、第 2 世代のシングル AZ およびマルチ AZ ファイルシステムに適用されます。一般に、第 2 世代のファイル・システムは、読み取りにはプロビジョニングされた容量全体を、書き込みにはプロビジョニングされたスループット容量の最大 3 分の 1 を提供できます。ただし、この表にリストされている 6,144 MB/秒オプションは例外です。

第 2 世代の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	6,144[1]	1,024[1]
マルチ AZ	6,144	2,048

> **Note**
> HA ペアごとに [1] (最大 12)。詳細については、「高可用性 (HA) ペアの管理」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 1 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

> **Note**
>
> 第 2 世代のファイルシステムで SSD ストレージ容量を減らすと、ほとんどの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。ただし、書き込みが多いワークロードでは、パフォーマンスが一時的に低下する可能性があります。クライアントアクセスが新しいディスクにリダイレクトされるため、短い I/O 一時停止 (最大 60 秒) が発生する場合もあります。
> パフォーマンスへの影響を最小限に抑えるには、SSD の削減操作を開始する前に、進行中のワークロードが一貫して 50% を超える CPU、50% のディスクスループット、または 50% の SSD IOPS を消費しないように注意します。SSD ストレージ容量の削減の詳細については、SSD ストレージ容量を削減するタイミング をご参照ください。

スループット容量がパフォーマンスに与える影響

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。

First-generation Single-AZ file system

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第 1 世代のシングル AZ 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)、米国東部 (オハイオ)、米国西部 (オレゴン)、および欧州 (アイルランド) の AWS リージョン における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)	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。

これらの性能仕様は、FSx for ONTAP が利用可能な他のすべての AWS リージョン における第 1 世代のシングル AZ ファイルシステムに適用されます。

FSx for ONTAP が利用可能な他のすべての AWS リージョン における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
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。

Second-generation Single-AZ file system

これらのパフォーマンス仕様は、第 2 世代のシングル AZ ファイルシステムに適用されます。

第 2 世代のシングル AZ 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
384**	781	6,250	数十万、ベースライン	16	–	384	3,125	12,500	65,000
768**	1,563	6,250		32	–	768	3,125	25,000	65,000
1,536	3,125	6,250		64	–	1,536	3,125	50,000	65,000
3,072	6,250	–		128	–	3,072	–	100,000	–
6,144	12,500	–		256	1,900	6,144	–	200,000	–

> **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。
> ** 第 2 世代のシングル AZ ファイルシステムは、384 および 768 のスループットキャパシティをサポートしますが、1 つの HA ペアでのみサポートされます。HA ペアを追加するには、ファイルシステムを少なくとも 1,536 MBps のスループットキャパシティに設定する必要があります。

First-generation Multi-AZ file system

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第 1 世代のマルチ AZ 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)、米国東部 (オハイオ)、米国西部 (オレゴン)、および欧州 (アイルランド) の AWS リージョン における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)	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。

これらの性能仕様は、FSx for ONTAP が利用可能な他のすべての AWS リージョン における出し 1 世代のマルチ AZ ファイルシステムに適用されます。

FSx for ONTAP が利用可能な他のすべての AWS リージョン における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)	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。

Second-generation Multi-AZ file systems

これらのパフォーマンス仕様は、第 2 世代のマルチ AZ ファイルシステムに適用されます。

第 2 世代マルチ AZ 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
384	781	6,250	数十万、ベースライン	16	237	384	3,125	12,500	65,000
768	1,563	6,250		32	474	768	3,125	25,000	65,000
1,536	3,125	6,250		64	950	1,536	3,125	50,000	65,000
3,072	6,250	–		128	1,900	3,072	–	100,000	–
6,144	12,500	–		256	3,800	6,144	–	200,000	–

> **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第 1 世代の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 マネジメントコンソール、 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 (SVM)、ボリュームの作成、バックアップ、およびタグの作成、一覧表示、更新および削除。
- アクセス、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の管理

トピック

- ストレージ容量の管理
- FSx for ONTAP ファイルシステムの管理
- FSx for ONTAP ストレージ仮想マシンの管理
- FSx for ONTAP ボリュームの管理
- iSCSI LUN の作成
- 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
- スループット容量の管理
- SMB 共有の管理
- NetApp アプリケーションを使用した ONTAP リソースの FSx の管理
- Amazon FSx リソースのタグ付け

ストレージ容量の管理

Amazon FSx for NetApp ONTAP 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を数多く提供しています。

トピック

- FSx for ONTAP ストレージ階層
- 適切な量のファイルシステム SSD ストレージの選択
- ファイルシステムのストレージ容量および IOPS

- ボリュームストレージ容量

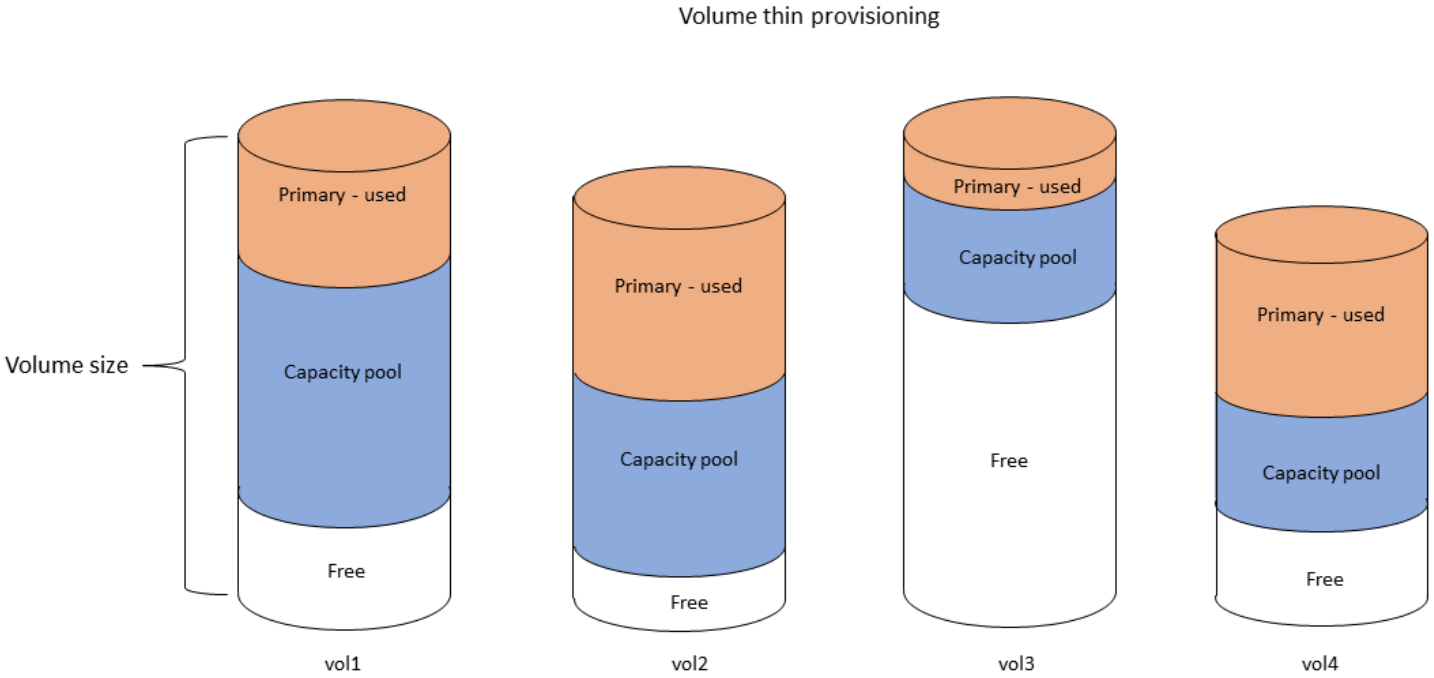
FSx for ONTAP ストレージ階層

ストレージ階層は、Amazon FSx for NetApp ONTAP ファイルシステムの物理的な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。

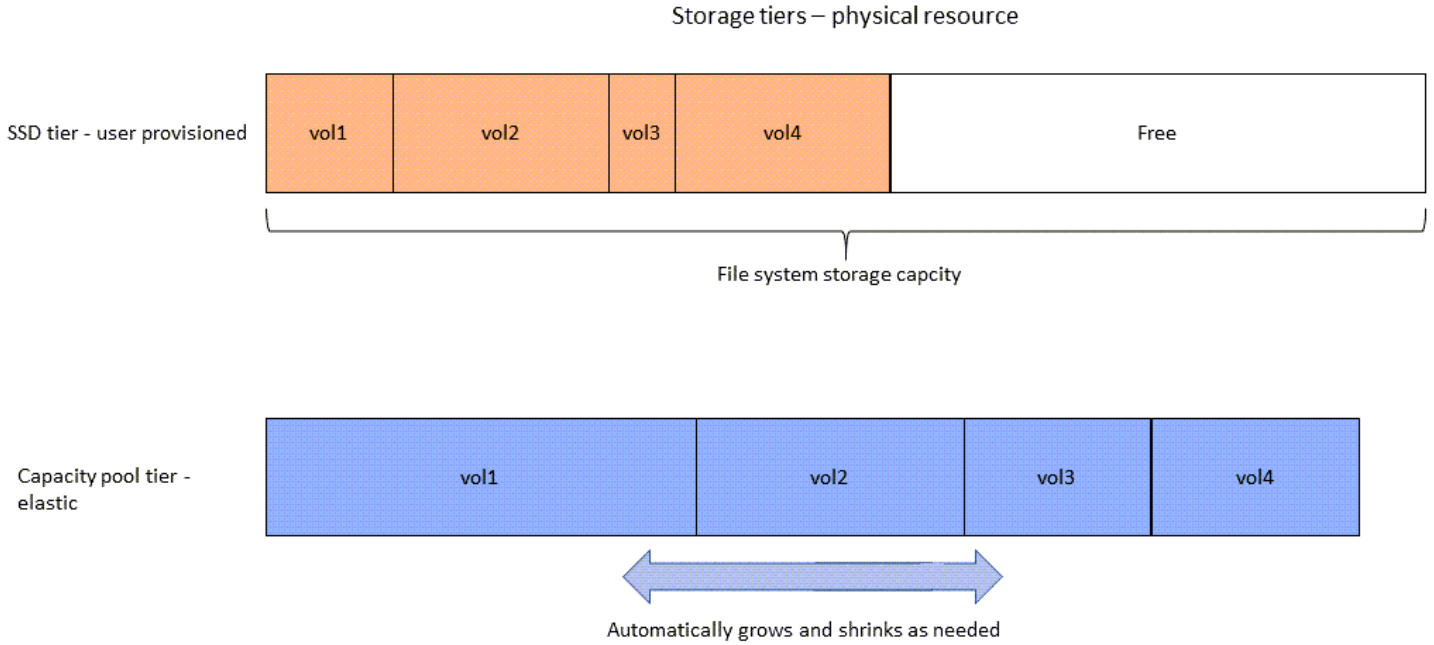
- SSD 階層 — データセットのアクティブな部分専用に設計された、ユーザーがプロビジョニングする高性能ソリッドステートドライブ (SSD) ストレージです。
- 容量プール層 — ペタバイト規模まで自動的に拡張する、伸縮自在なストレージで、アクセス頻度の低いデータに対してコストを最適化します。

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 ストレージの選択

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です。
- 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 ソフトウェアオーバーヘッド

他の NetApp ONTAP ファイルシステムと同様に、最大 16% のファイルシステムの SSD ストレージ容量は ONTAP オーバーヘッド用に予約されているため、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ソフトウェアに割り当てられています。SSD ストレージ容量が 30 テビバイト (TiB) を超える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、[すべて] のデータ階層化ポリシーが設定されたボリュームで SnapMirror を使用する場合に、データがキャパシティプールに直接書き込まれた場合を除いて、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。第 2 世代の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、NetApp の ONTAP に関する推奨事項と整合性があります。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キャパシティ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。

ストレージ効率

NetApp ONTAP は、圧縮、コンパクト化、重複排除などのブロックレベルストレージ効率機能をボリュームレベルで提供します。これらの機能により、パフォーマンスを低下させることなく、一般的なファイル共有のストレージ容量を最大 65% 削減できます。ボリュームごとにストレージ効率を有効にできます。これらの機能により、データが消費するストレージ容量が削減され、SSD、容量プール、およびバックアップストレージで消費されるストレージ領域を減らすことができます。SSD ストレージ内のデータに対して、各ボリュームで圧縮と重複排除を有効にできます。SSD ストレージの圧縮と重複排除によるストレージの節約は、データがキ容量プールストレージに階層化されている場合に維持されます。ファイルシステムのストレージ効率設定に関係なく、バックアップデータに対してストレージ効率は常に有効になります。

次の表は、一般的なストレージ節約の例を示しています。

	圧縮のみ	重複排除のみ	圧縮と重複排除
汎用ファイル共有	50%	30%	65%
仮想サーバーとデスクトップ	55%	70%	70%
データベース	65～70%	0%	65～70%
データエンジニアリング	55%	30%	75%
地理地震データ	40%	3%	40%

ほとんどのワークロードでは、圧縮と重複排除を有効にしても、ファイルシステムのパフォーマンスに悪影響を及ぼしません。ほとんどのワークロードでは、圧縮により全体的なパフォーマンスが向上します。FSx for ONTAP ファイルサーバーは、RAM キャッシュからの高速な読み取りと書き込みを実現するために、ファイルサーバーとストレージディスク間で利用可能なものよりも高いレベルのネットワーク帯域幅をフロントエンドネットワークインターフェイスカード (NIC) に搭載しています。データ圧縮はファイルサーバーとストレージディスク間で送信されるデータ量を減らすため、ほとんどのワークロードでは、データ圧縮を使用するとファイルシステム全体のスループットキャパシティが増加します。データ圧縮に関連するスループットキャパシティの増加は、ファイルシステムのフロントエンド NIC を飽和させると制限されます。

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、容量を節約する他の 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節約量を確認するには、「ストレージ効率節約のモニタリング」を参照してください。

ストレージ効率節約の計算

LogicalDataStored や 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、FlexClones によるストレージの節約量を計算できます。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 TiB) が自動的に容量プール階層に階層化され、残りの 20% (20 TiB) 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および 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。第 2 世代のシングル AZ 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。第 2 世代のシングル AZ 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 SSD ストレージと IOPS の更新
- SSD のストレージ容量を増やすタイミング
- SSD ストレージ容量の増加
- SSD ストレージ容量の増加の考慮事項
- SSD ストレージ容量を削減するタイミング
- SSD ストレージ容量の削減
- SSD ストレージ容量削減に関する考慮事項
- SSD ストレージ容量を減らすための制限事項
- ファイルシステムのストレージ容量使用率アラームの作成
- ストレージ容量とプロビジョンド IOPS の更新
- ストレージ容量の動的な更新
- SSD ストレージ使用率のモニタリング
- ストレージ効率節約のモニタリング
- ストレージ容量と IOPS アップデートのモニタリング

ファイルシステム 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追加のストレージが必要な場合は、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。第 2 世代のファイルシステムでは、ワークロードの変化するストレージニーズに合わせて SSD ストレージ容量を減らすこともできます。ストレージ容量を増減するには、Amazon FSx コンソール、Amazon FSx API、または AWS Command Line Interface (AWS CLI) を使用できます。詳細については、「ストレージ容量とプロビジョンド IOPS の更新」を参照してください。

SSD の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。

ファイルシステム上で利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。このメトリクスで 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 CloudWatch によるモニタリング」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。第 2 世代の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 ストレージの選択 を参照してください。

SSD ストレージ容量の増加

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、ご利用可能になった時点で課金されます。詳細については、「Amazon FSx for NetApp ONTAP の料金」および「AWS FSx for ONTAP の請求と使用状況レポート」を参照してください。

ストレージ容量を増やすと、Amazon FSx はデータの再バランシングのために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数時間かかり、ワークロードのパフォーマンスへの顕著な影響は最小限に抑えられます。

Amazon FSx コンソール、AWS 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。

SSD ストレージ容量の増加の考慮事項

ファイルシステムの SSD ストレージ容量および IOPS を増加させる際に考慮すべき重要なポイントは、以下の通りです:

- (第 1 世代ファイルシステムのみ) 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。
- 増加の間隔 — ファイルシステムの SSD スループットキャパシティ、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増やした後に、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 Pricing] (Amazon FSx for NetApp ONTAP の料金表) を参照してください。

SSD ストレージ容量を削減するタイミング

以下のようなシナリオでは、FSx for ONTAP 第 2 世代ファイルシステムの SSD ストレージ容量を減らすことを希望するかもしれません:

- 高性能ストレージが不要になったプロジェクトベースのワークロードを完了した後
- 一時的な追加容量を使用してデータインジェストを高速化した大規模なデータ移行が完了した後

SSD ストレージ容量の削減

ファイルシステムの SSD ストレージ容量を減らすと、Amazon FSx はファイルシステムの各 HA ペアに、より小さい新しいディスクセット (集約) をアタッチします。その後、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、古いディスクから新しいディスクにデータをボリュームごとに移動させます。各ボリュームのデータが移動されると、Amazon FSx はクライアントアクセスを新しいディスク上のボリュームにリダイレクトします。その後、Amazon FSx はファイルシステムから古いディスクをデタッチします。

SSD 削減オペレーション全体で、SSD 階層の既存のサイズと新しくリクエストされたサイズに対して課金されます。たとえば、SSD ストレージ容量を 10 TiB から 5 TiB に削減する場合、SSD 削減操作中は 15 TiB 分の課金が発生し、操作完了後は 5 TiB 分の課金となります。請求の詳細については、「AWS FSx for ONTAP の請求と使用状況レポート」を参照してください。

SSD ストレージ容量の減少には、ファイルシステムに格納されているデータの量、減少操作中にファイルシステムにドライブされる正味新規書き込みの量、ファイルシステムで使用可能なネットワークおよびディスクリソースの量などの要因に応じて、数時間から数週間かかることがあります。

減少オペレーション中、データは読み取りと書き込みに引き続き使用できます。ほとんどのワークロードのパフォーマンスへの影響は最小限ですが、書き込みが多いワークロードでは一時的なパフォーマンス低下が発生する可能性があります。クライアントアクセスが各ボリュームの新しいディスクにリダイレクトされると、短い I/O 一時停止 (最大 60 秒) が発生することがあります。

パフォーマンスへの影響を最小限に抑えるには、SSD の減少操作を開始する前に、進行中のワークロードが一貫して 50% の CPU、50% のディスクスループット、または 50% の SSD IOPS を超えて消費しないようにすることで、ファイルシステムに十分なヘッドルームを維持する必要があります。これらの使用率メトリクスは、Amazon FSx コンソールのファイルシステムの[モニタリングとパフォーマンス] タブでモニタリングできます。

> **Note**
>
> 減少オペレーション中に SSD ストレージ層が 80% の使用率を超えると、Amazon FSx はオペレーションを一時停止し、使用率が 80% を下回った後に自動的に再開します。新しいディスクの SSD 使用率を減らすには、データを容量プールに階層化するか、クライアント

アクセスが新しいディスクセットに正常にリダイレクトされたボリュームからデータを削除できます。

削減オペレーション中に追加の SSD 容量が必要な場合は、AWS CLI または同等の UpdateFileSystem API オペレーションで `update-file-system` を呼び出し、新しいターゲット値を指定することで、SSD 容量を増やすリクエストを送信できます。Amazon FSx は SSD 増加リクエストの完了を優先し、SSD 減少オペレーションを再開する前に数分以内に新しい SSD 容量を使用できるようにします。

SSD ストレージ容量削減に関する考慮事項

ファイルシステムの SSD ストレージ容量およびプロビジョニング済み IOPS を削減する際に考慮すべき重要なポイントは、以下の通りです:

- 減少オペレーション中のストレージ容量の増加 – 減少オペレーションが進行中でも、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。この柔軟性により、減少オペレーション中にアグリゲートのいずれかがいっぱいになった場合に備えて、パフォーマンスと可用性を確保できます。SSD 容量を元の容量よりも小さいサイズに減らした場合、Amazon FSx は新しくリクエストされた (ターゲット) 集計のサイズのみを調整します。ただし、SSD 容量を元のサイズよりも大きいサイズに増やすと、Amazon FSx は両方のアグリゲートのサイズを新しいターゲット値に合わせて増やします。たとえば、ストレージ容量を 10,000 GiB から 5,000 GiB に減らし、7,000 GiB への引き上げをリクエストすると、ターゲット集計のみが 7,000 GiB に増加し、ファイルシステムの最終 SSD ストレージ容量は 7,000 GiB になります。しかし、12,000 GiB への増加を要求すると、両方のアグリゲートが 12,000 GiB に増加します。元の SSD 容量以上に増設する必要が生じる状況を避けるため、慎重な計画を推奨します。
- SSD の削減を一時停止する – 新しいアグリゲートの使用率が 80% を超えると、Amazon FSx は SSD の削減オペレーションを一時停止し、使用率が 80% を下回ると自動的に削減オペレーションを再開します。
- (第 2 世代のシングル AZ ファイルシステムのみ) 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。
- ストレージ容量の減少中のパッチ適用 – SSD 削減オペレーション中にファイルシステムにパッチが適用された場合、Amazon FSx はボリュームのデータの移動を中止します。その結果、オペレーション中にパッチが発生した場合、SSD 削減オペレーションの進行状況が失われる可能性があります。Amazon FSx は、パッチオペレーションの完了後に `vol move` を自動的に再起動します。

- 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。SSD 容量を減らすと、自動 SSD IOPS は比例的にスケールダウンします。

    > **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。

  - ユーザープロビジョニングモード – 現在のプロビジョンド IOPS 以上の IOPS 値を指定する必要があります。SSD 容量を減らす場合、より小さなアグリゲートでサポートされる最大 SSD IOPS (リクエストされた SSD 容量の GB あたり 50 IOPS) を超えない限り、追加のユーザープロビジョンド SSD IOPS を保持できます。プロビジョンド IOPS が、より小さいアグリゲートでサポートされる最大値より大きい場合は、SSD 容量を減らす前に IOPS を減らします。

SSD ストレージ容量を減らすための制限事項

ファイルシステムの SSD ストレージ容量を減らすときは、以下の制限が適用されます:

- (第 2 世代ファイルシステムのみ) ストレージ容量の削減 – ストレージ容量を減らすことができるのは、第 2 世代ファイルシステムのみです。
- ストレージ容量の最小減少 – 各 SSD ストレージ容量の減少は、ファイルシステムの現在の SSD ストレージ容量の 9% 以上である必要があります。また、この減少により、ファイルシステムの SSD 容量が減少操作後に 80% の使用率を超えないようにする必要があります。たとえば、ファイルシステムに 10,000 GiB のストレージ容量と 5,000 GiB のストレージが使用されている場合、SSD 使用率が 80% 未満になるようにストレージ容量を 6,251 GiB に減らすことができます。SSD ストレージ容量は、HA ペアあたり 1,024 GiB の最小サポートサイズまで減らすことができます。
- SSD 層に 50 TiB を超えるデータを持つボリュームが 1 つ以上含まれるファイル システムの SSD ストレージ容量を減らすには、HA ペアごとに少なくとも 1,536 MB/秒の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。SSD 階層内の任意のボリュームが 100 TiB を超えるデータを含む場合、各 HA ペアあたり少なくとも 3,072 MB/秒 のスループットキャパシティをプロビジョニングする必要があります。SSD 階層内のボリュームに 200 TiB を超えるデータがある場合、各

HA ペアあたり 6,144 MB/秒 のスループットキャパシティをプロビジョニングする必要があります。

- 更新の間隔 — ファイルシステムの SSD スループットキャパシティ、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。
- ファイルシステムのスループットキャパシティを増やすことはできますが、減らすことはできません
- HA ペアをファイルシステムに追加することはできません
- ボリューム内のデータが新しいアグリゲートに移動している間は、ボリュームを以前の状態に戻すことはできません (`volume snapshot restore` を使用)。ただし、現在移動されていない他のボリュームで `volume snapshot restore` を実行できます。
- ボリュームのオフライン化、ボリュームの移動、FlexClone の作成、SnapLock ボリュームの作成、ボリュームのストレージ効率設定の変更は、減少操作中には実行できません。

ファイルシステムの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。以下の手順は、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 アラームを作成方法を示しています。

ファイルシステムのストレージ容量使用率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. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. 左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。アラーム作成ウィザード内で、[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] > [詳細ファイルシステムメトリクス] の順に選択します。
   - [メトリクス名] で、[MAX (StorageCapacityUtilization)] を選択します。

- [次でフィルタリング] で、オプションで ID で特定のファイルシステムを含めるか除外できます。[次でフィルタリング] を空のままにした場合、ファイルシステムがアラームのストレージ容量使用率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。ウィザードに戻り、[メトリクス] セクションで、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. メトリクスが[80 より大きい/と等しい]場合は常に、[条件] で、[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

設定したしきい値に達するとアラームがトリガーされるように、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説明しています。

1. [通知] セクションで、アラームが ALARM 状態のときに通知するための SNS トピックを選択します。新しいトピックを作成することも、既存のトピックを使用することもできます。E メールアドレスにアラーム通知を受け取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] を選択します。

アラームを終了するには

CloudWatch アラームの作成プロセスを完了するには、次の手順に従います。

1. [名前と説明の追加] ページで、アラームに名前を付け、オプションで説明を記入して、[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。

ストレージ容量とプロビジョンド IOPS の更新

Amazon FSx コンソール、AWS CLI、または API を使用して、ファイルシステムの SSD ベースのストレージおよびプロビジョンド SSD IOPS の量を増減することができます。

ファイルシステム (コンソール) の SSD ストレージ容量またはプロビジョンド IOPS を増やす方法

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。
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。第 2 世代の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のプロビジョンド IOPS を更新する方法 (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 を増やすには、update-file-system の AWS CLI コマンドまたは同等の UpdateFileSystem API アクションを使用します。ユーザーの値で、以下のパラメータを設定します。

- `--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` を現在の値より少なくとも 10% 大きい値になるように所望のストレージ容量の値を設定します。
- 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、プロビジョンド SSD ストレージの容量の GiB あたり 3 つの 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、ユーザーがプロビジョンド 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}'
```

describe-file-systems の AWS CLI コマンドを使用して、更新の進捗状況をモニタリングすることができます。出力で `AdministrativeActions` セクションを探します。

詳細については、[Amazon FSx for NetApp ONTAP API Reference] (Amazon FSx for NetApp ONTAP API リファレンス) の [AdministrativeAction] (管理アクション) を参照してください。

ファイルシステムのストレージ容量を減らす方法 (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. 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. [アクション] > [ファイルシステムを更新] > [SSD ストレージ容量/IOPS を更新] 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横にある [SSD storage capacity] (ストレージ容量) の [Update] (更新) を選択します。
4. SSD ストレージ容量を減らすには、[アクションタイプ] で [減少] 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、以下のいずれか 1 つを行います。

- [割合] には、[希望する減少率 (%)] 値を入力します。この値は、現在の値より 9% 以上小さい値である必要があります。
- [絶対値] には、[希望するストレージ容量] の値を GiB 単位で入力します。

7. [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。第 2 世代の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のプロビジョンド IOPS を更新する方法 (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 を減らすには、update-file-system の AWS CLI コマンドまたは同等の UpdateFileSystem API アクションを使用します。ユーザーの値で、以下のパラメータを設定します。

1. SSD 容量を減らすには、以下のコマンドを使用します:

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096
```

ユーザープロビジョンド IOPS モードを使用していて、現在の IOPS レベルを保持する場合は、`DiskIopsConfiguration` パラメータを含めます:

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096 \
--ontap-configuration 'DiskIopsConfiguration={Iops=15000,Mode=USER_PROVISIONED}'
```

2. 減少オペレーションの進行状況をモニタリングするには、describe-file-systems コマンドを使用します:

```
aws fsx describe-file-systems --file-system-id fs-0123456789abcdef0
```

コマンドは、`AdministrativeActions` セクションの縮小オペレーションに関する情報を返します。例:

```
{
    "FileSystem": {
        "StorageCapacity": 4096,
        "StorageType": "SSD",
        "AdministrativeActions": [
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining.
 https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
                "ProgressPercent": 4,
                "RequestTime": 1748981251.591,
                "Status": "IN_PROGRESS",
                "TargetFileSystemValues": {
                    "StorageCapacity": 4096
                }
            }
        ]
    }
}
```

describe-file-systems AWS CLI コマンドを使用して、更新の進捗状況をモニタリングすることができます。出力で AdministrativeActions セクションを探します。

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

ストレージ容量の動的な更新

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、ストレージ容量しきい値、そのしきい値に基づく Amazon CloudWatch アラーム、そしてファイルシステムのストレージ容量を増加させる 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パーセンテージです。

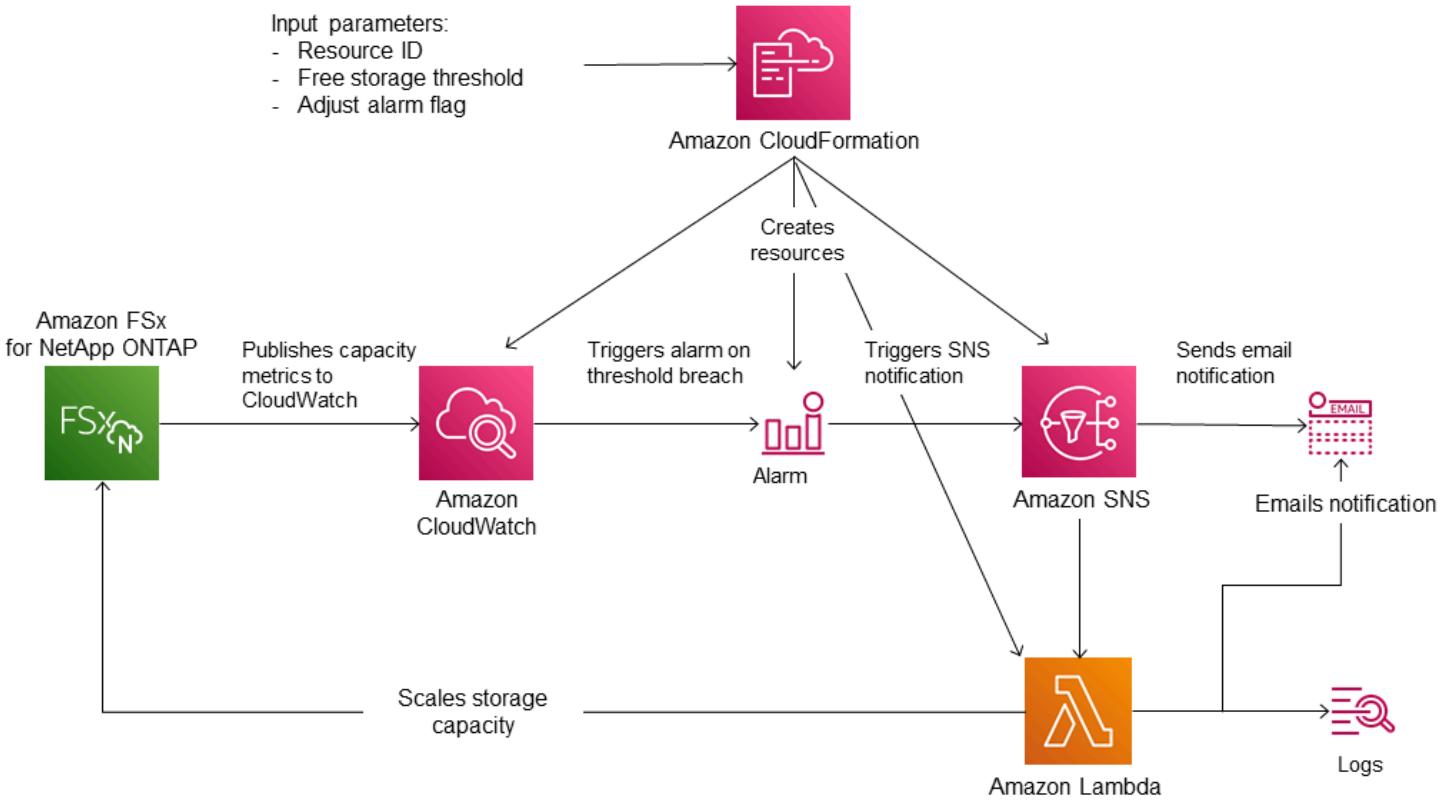
- ストレージ容量の増加率 (%)。
- スケーリング通知の受信に使用する E メールアドレス。

トピック

- アーキテクチャの概要
- CloudFormation テンプレート
- CloudFormation による自動デプロイ

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. 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 AWS Identity and Access Management (IAM) ロールをデプロイします。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しているストレージ容量が指定されたしきい値を超えると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. 元の CloudWatch アラームの状態と Lambda 関数オペレーションの結果は、Amazon SNS キューに送信されます。

CloudWatch アラームへのレスポンスとして実行される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の確認 電子メールに記載されているリンクに従って Amazon SNS トピックのサブスクリプションを確認する必要があります。

CloudFormation テンプレート

このソリューションは CloudFormation を使用し、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 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**
>
> CloudWatch アラームが ALARM 状態になるたびに、ストレージのスケーリングが一度試行されます。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。

MaxFSxSizeinGiB

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。

CloudFormation による自動デプロイ

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拡張するための CloudFormation スタックを設定し、デプロイします。デプロイには、数分かかります。CloudFormation スタックの作成に関する詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation コンソールでスタックを作成する」を参照してください。

> **Note**
>
> このソリューションを実行すると、関連する AWS のサービスに料金が発生します。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。

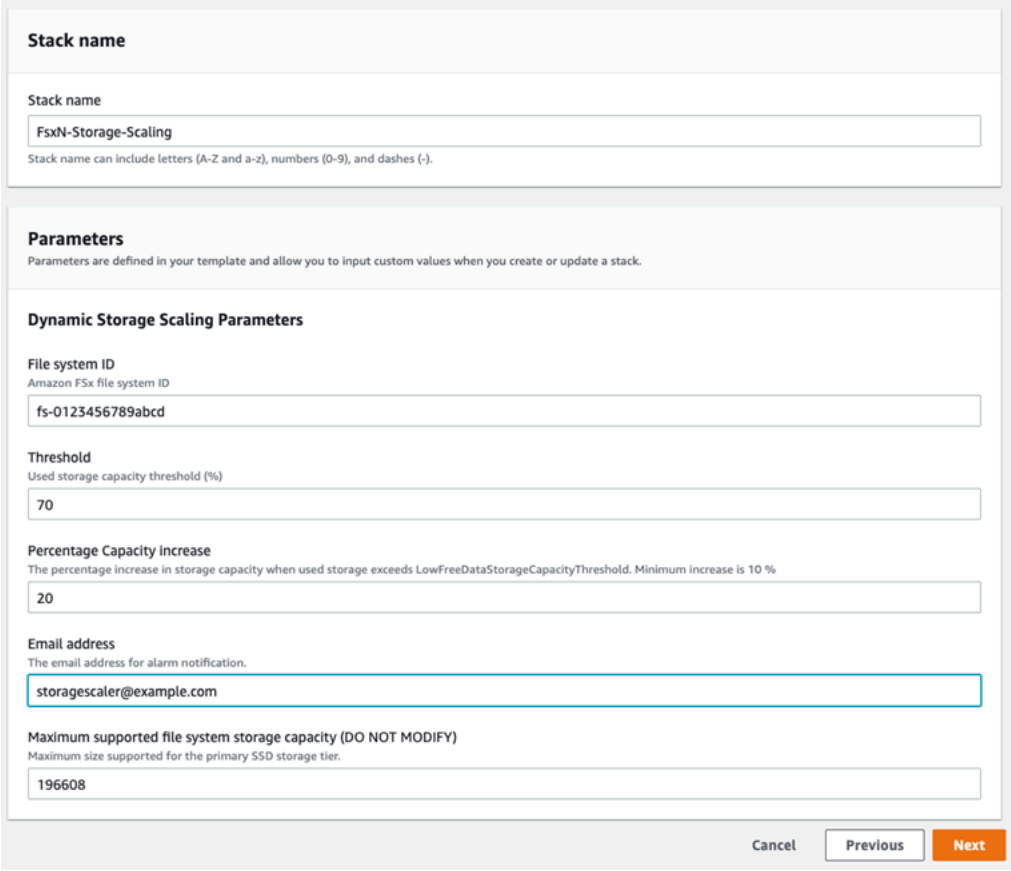
開始するには、AWS アカウント の Amazon Virtual Private Cloud (Amazon VPC) で実行されている Amazon FSx ファイルシステムの ID が必要になります。Amazon FSx リソースの作成の詳細については、「Amazon FSx for NetApp ONTAP の開始方法」を参照してください。

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. CloudFormation テンプレート FSxOntapDynamicStorageScaling 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. CloudFormation コンソールから、[Create stack > With new resources] (スタックの作成 > 新しいリソースの使用) 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、このテンプレートをデプロイした後に受信する 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。

CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。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。

SSD ストレージ使用率のモニタリング

さまざまな AWS や NetApp ツールを使用して、ファイルシステムの SSD ストレージ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状況をモニタリングし、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 SSD ストレージと IOPS の更新」を参照してください。

Amazon FSx コンソールでは、ファイルシステムの利用可能な SSD ストレージと、全体のストレージがどのように配分されているかを確認できます。[利用可能なプライマリストレージ容量] 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、ファイルシステムの SSD ストレージ容量使用率を AWS マネジメントコンソール 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] をクリックして、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。[使用可能なプライマリストレージ容量] と [アグリゲートあたりのトレージ容量使用率] が表示されます。

ストレージ効率節約のモニタリング

有効にすると、Amazon FSx コンソール、Amazon CloudWatch コンソール、および ONTAP CLI でどれだけストレージ容量を節約しているか確認できます。

ストレージ効率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の効率の節約には、FlexClone とスナップショットによる節約が含まれます。

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 番目のパネルにある [モニタリングとパフォーマンス] タブの [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。

ストレージ効率節約を表示するには (ONTAP CLI)

ONTAP を使用して `storage aggregate show-efficiency` コマンドを実行すると、スナップショットや FlexClones の影響を排除した、圧縮、コンパクト化、重複排除だけによるストレージ効率が向上が確認できます。詳細については、NetApp ONTAP ドキュメントセンターの「ストレージアグリゲートの効率化を表示」を参照してください。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 コマンドには、すべてのアグリゲートのストレージ効率に関する情報が表示されます。ストレージ効率は 4 つの異なるレベルで表示されます。

   - Total
   - 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

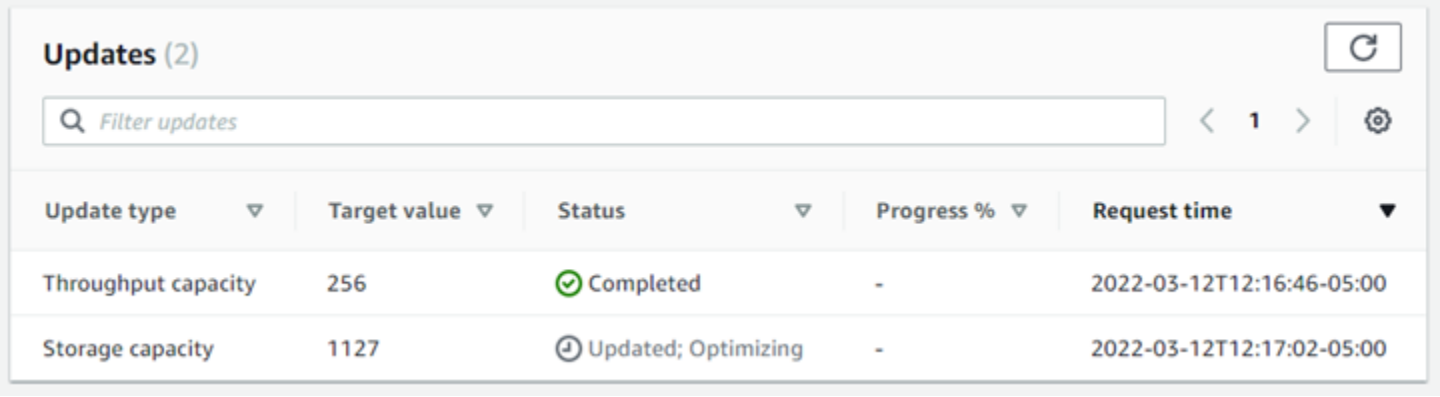
Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

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、API を使用してストレージ容量の拡大の進捗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 更新をモニタリングするには (CLI)

describe-file-systems AWS CLI command and the DescribeFileSystems API オペレーションを使用して、ファイルシステムストレージ容量の増減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。ファイルシステムの SSD ストレージ容量を減らすと、AdministrativeActions アクションは1つだけ生成されます。それはFILE_SYSTEM_UPDATE アクションです。

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"
    }
]
```

SSD 容量を減らす場合、FILE_SYSTEM_UPDATE アクションには、現在移動中のボリュームと残りのボリューム数に関する情報を提供する Message プロパティが含まれます。例:

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining. https://
docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
        "Status": "IN_PROGRESS",
        "TargetFileSystemValues": {
```

```
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

ターゲット集計の使用率が 80% を超えたために SSD 削減オペレーションが一時停止された場合、ステータスは適切なメッセージで PAUSED に変わります:

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Your file system has insufficient free space in its SSD tier.
 Please free up space or increase your file system's storage capacity.",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
        "Status": "PAUSED",
        "TargetFileSystemValues": {
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

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"
        }
    }
]
```

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 マネジメントコンソール、 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
- ストレージ効率の管理
- 自動サイズ調整の有効化
- クラウド書き込みモードの有効化
- ストレージ容量の更新
- 階層化ポリシーの更新
- 最低冷却日数の更新
- ボリュームのクラウド検索ポリシーの更新

- ボリューム上のファイルの最大数の更新
- ボリュームストレージ容量のモニタリング
- ボリュームのファイル容量のモニタリング

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、しきい値設定に基づいて、容量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。

> **Note**
>
> FSx for ONTAP は、SnapLock タイプに関係なく、すべての SnapLock ボリュームの容量プールへのデータの階層化をサポートしています。詳細については、「SnapLock の仕組み」を参照してください。

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をどのように使用するかは、ファイルシステムのボリュームごとに階層化ポリシーを選択することによって決定します。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のポリシーです。
- [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。既にデータが含まれているボリュームに All ポリシーが適用されている場合、既存のデータは SSD から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。他のポリシーの使用後にボリュームをこのポリシーに設定すると、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 (スナップショットを含む) は、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。このデータ移行は、SSD の使用率が 90% 未満で、クラウド取得ポリシーが`promote`または`on-read`に設定されている場合にのみ行われます。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。

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、階層化ポリシーの更新 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] 階層化では、データは容量プール階層に移動する前に、少なくとも 2 日間 (ボリュームの冷却期間に基づく) SSD スト

レージ階層に格納されます。ONTAP は、SSD ストレージ階層に格納されているデータに対してプロセス後の重複排除を定期的に実行し、ボリュームのデータ変更率に基づいて頻度を自動的に調整します。変更率が高いほど、プロセス後の重複排除ジョブがトリガーされます。

デフォルトでは、ファイルシステムの進行中のワークロードに対するパフォーマンスへの影響により、後処理圧縮は ONTAP では無効になっています。後処理圧縮を有効にする前に、ワークロードのパフォーマンスへの影響を評価する必要があります。後処理圧縮を有効にするには、ONTAP CLI で診断特権レベルを予測し、次のコマンドを実行します。

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP は、SSD ストレージに少なくとも 14 日間保持されるデータの後処理圧縮を実行します。より短い期間後にデータにアクセスする可能性が低いワークロードの場合、後処理圧縮を早く実行するように後処理圧縮の設定を変更できます。例えば、5 日間アクセスされていないデータに後処理圧縮の節約を適用するには、次の ONTAP CLI コマンドを実行します。

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

コマンドの詳細については、「ボリューム効率非アクティブデータ圧縮の変更」を参照してください。

SSD にデータを保持することで、SSD ストレージのデータ転送レートが高くなるため、作成したボリュームバックアップの転送速度を最大化できます。

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、最低冷却日数の更新 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更新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 ストレージ容量の使用率によって、ONTAP がすべてのボリュームの階層化動作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。第 2 世代の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 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

snapshot (スナップショット) は、ある時点での 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、「スナップショットによるデータの保護」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、権限、サイズなどのファイルメタデータを保存したり、データブロックへのポインタとして機能したりするために使用され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、「ボリュームのファイル容量のモニタリング」を参照してください。

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。

ボリュームが格納できるファイルの最大数の変更については、「ボリューム上のファイルの最大数の更新」を参照してください。

ストレージ効率の管理

FSx for ONTAP ボリュームでストレージ効率を有効にすることで、ストレージ使用率を最適化し、ストレージコストを削減し、ファイルシステム全体のパフォーマンスを向上させることができます。

> **Note**
>
> Amazon FSx コンソール、API、または を使用してストレージ効率を有効に AWS CLI し、最適なストレージ効率設定がボリュームに適用されるようにすることをお勧めします。

ONTAPは、ファイルを 4 キビバイト (KiB) のデータブロックに編成します。ストレージの効率は、個々のファイルのレベルではなく、データブロックレベルで行われます。ストレージ効率を有効にすると、ONTAP はデータ削減手法を組み合わせて、重複するデータを排除し、データのサイズを圧縮し、最適なディスク使用量のためにデータのレイアウトを再編成します。

ストレージ効率は 2 つの方法で適用されます。これらは、データをインライン (ディスクに書き込む前、メモリ内) に適用され、ストレージの節約を即座に実現します。また、定期的な効率ジョブを通じて SSD ストレージ層のバックグラウンド (データがディスクに書き込まれた後) のデータに適用され、時間の経過とともにストレージ使用率を最適化します。バックグラウンドストレージの効率は、容量プールに階層化されたデータでは実行されません。ただし、データが SSD に格納されている間にストレージの節約があった場合、これらの節約は、データが容量プールに階層化されると保持されます。

> **Note**
>
> ONTAP は、データ保護 (DP) ボリュームでのストレージ効率の有効化をサポートしていません。ただし、ソースの読み取り/書き込み可能 (RW) ボリュームで達成されたストレージの節約は、データが宛先 DP ボリュームにレプリケートされるときに保持されます。

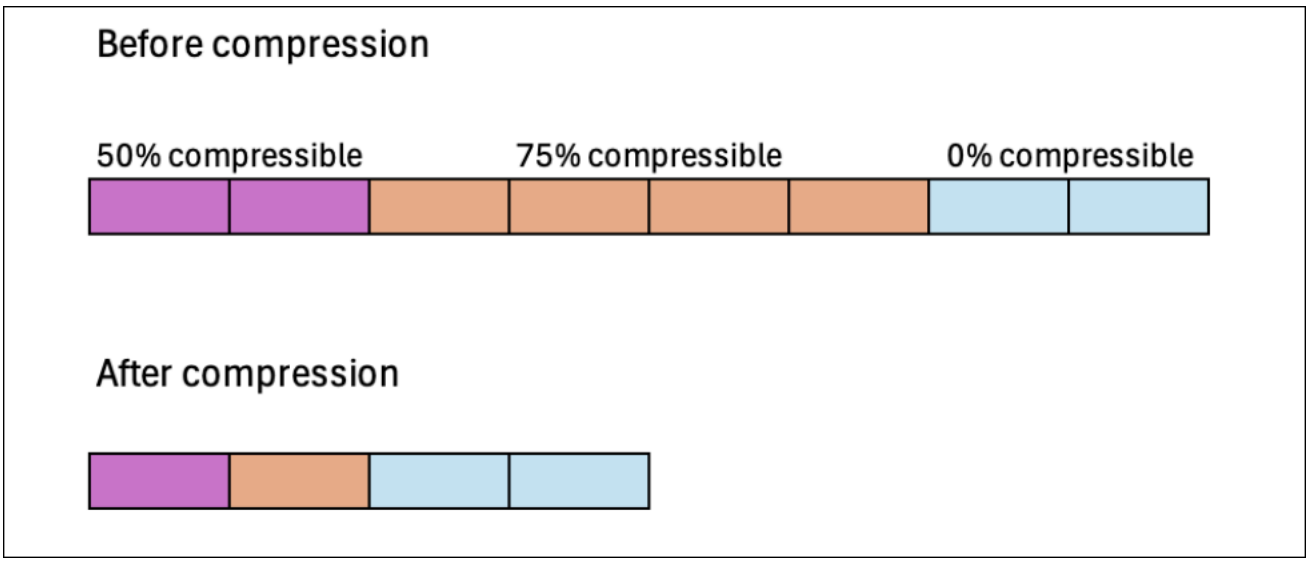
データブロックの圧縮

圧縮グループは、1 つのブロックとして管理および圧縮されるデータの論理グループです。ONTAP はデータブロックを自動的に圧縮グループにパックするため、ディスクで消費されるスペースが削減されます。パフォーマンスとストレージの使用率を最適化するために、ONTAP は、アクセスパターンに基づいてデータに適用される圧縮の程度を調整して、データを管理するためのバランスの取れたアプローチを提供します。

デフォルトでは、データをボリュームに書き込むときに最適なパフォーマンスを確保するために、データは 8 KB の圧縮グループを使用してインラインで圧縮されます。必要に応じて、ボリュームで非アクティブなデータ圧縮を有効にして SSD 内のデータをさらに圧縮することで、データにより大きな圧縮を適用できます。非アクティブなデータ圧縮では、コールドデータに 32 KB の圧縮グループを使用して、ストレージのさらなる節約を実現します。詳細については、NetApp ONTAP Documentation Center の `volume efficiency inactive-data-compression modify` コマンドを参照してください

> **Note**
>
> 非アクティブなデータ圧縮は、追加の CPU とディスク IOPS を消費し、リソース集約型のタスクになる可能性があります。この機能を有効にする前に、ワークロードに対して非アクティブなデータ圧縮を実行することによるパフォーマンスへの影響を評価することをお勧めします。

次の図は、データブロックを圧縮することで実現できるストレージの節約を示しています。



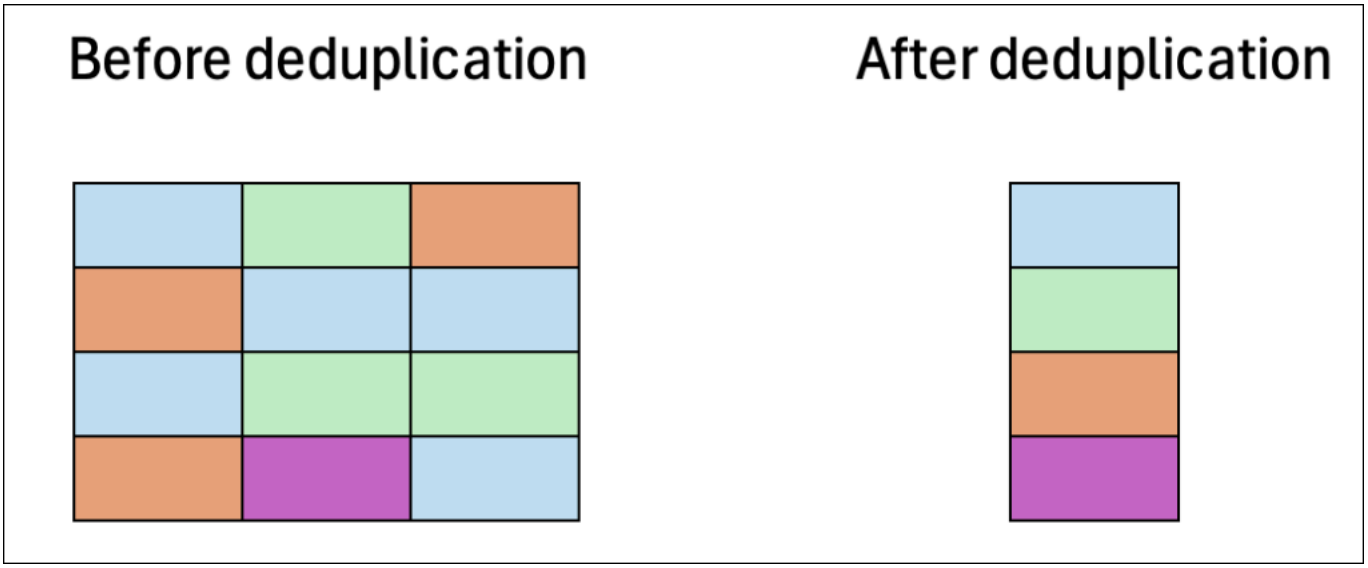
データブロックの重複排除

ONTAP は、重複するデータブロックを検出して排除し、データの冗長性を軽減します。重複ブロックは、共有一意のブロックへの参照に置き換えられます。

デフォルトでは、データがディスクに書き込まれる前にストレージフットプリントを減らすために、データはインラインで重複排除されます。ONTAP は、指定された間隔でバックグラウンド重複排除スキャナーも実行し、ディスクに書き込まれた後に重複データを識別して排除します。これらのスケジュールされたスキャン中、ONTAP は変更ログを処理し、最後のスキャン以降にまだ重複排除されていない新規または変更されたデータブロックを特定します。重複が見つかった場合、ONTAP はメタデータを更新して重複ブロックの 1 つのコピーを指し、冗長ブロックを再利用する準備ができた空き領域としてマークします。

> **Note**
>
> ONTAP は、一度に 4 KB の受信書き込みに重複排除を適用するため、4 KB 未満の書き込みでワークロードを実行すると重複排除の節約額が減る場合があります。
> FSx for ONTAP は、クロスボリューム重複排除をサポートしていません。

次の図は、重複排除で実現できるストレージの節約を示しています。



データブロックのコンパクト化

ONTAP は、それぞれ 4 KB 未満の部分的に埋められたデータブロックを、より効率的に使用される 4 KB ブロックに統合します。

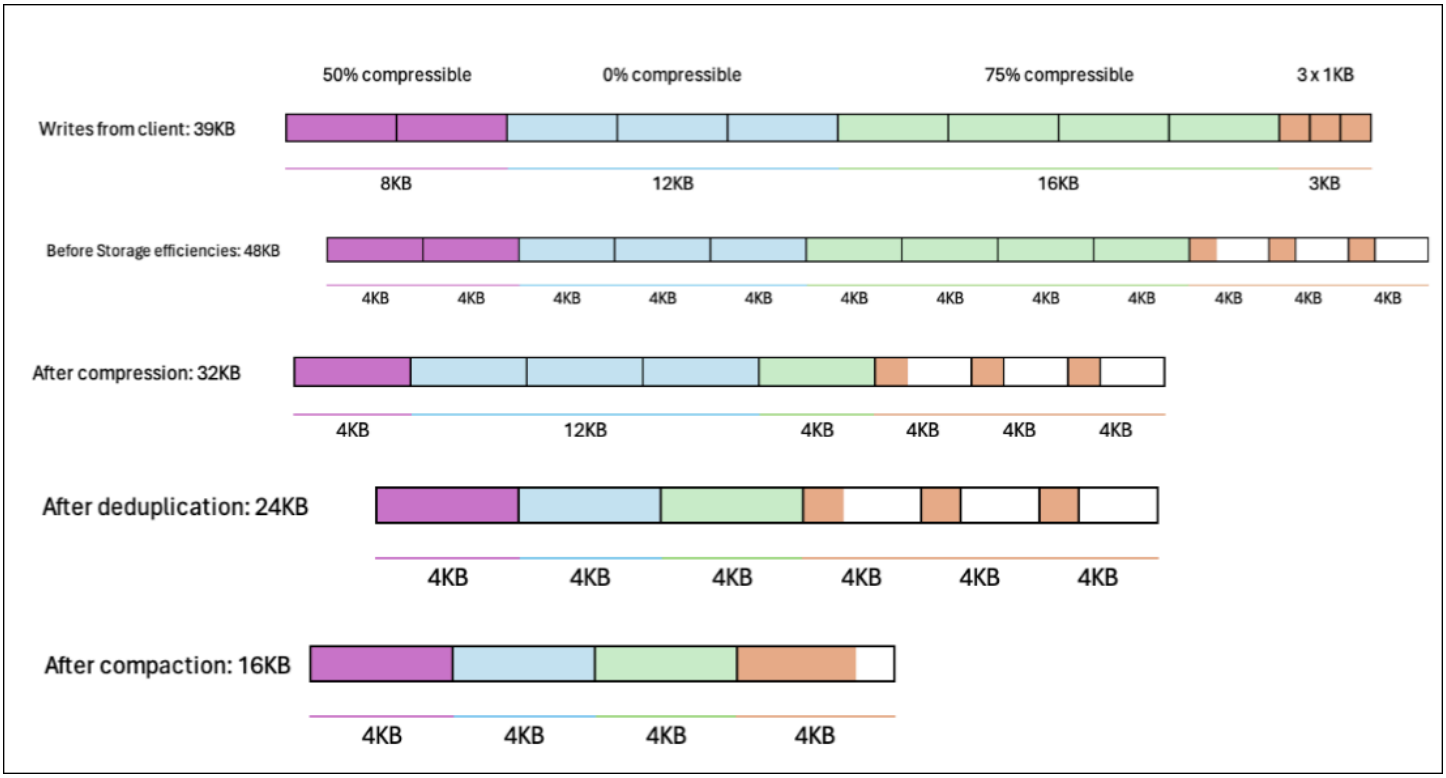
デフォルトでは、データはインラインにコンパクト化され、ディスクに書き込まれるデータのレイアウトを最適化して、ストレージのオーバーヘッドを最小限に抑え、断片化を減らし、読み取りパフォーマンスを向上させます。

次の図は、コンパクト化で実現できるストレージの節約を示しています。



例: ストレージ効率

次の図は、ストレージ効率がデータにどのように適用されるかを示しています。



自動サイズ調整の有効化

ボリュームの自動サイズ調整を有効にして、ボリュームが使用済みスペースのしきい値に達した場合に指定したサイズに自動的に引き上げられるようにします。これは、`volume autosize` ONTAP 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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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
```

3. 以下のコマンドを実行して、現在の自動サイズ設定を確認します。*svm_name* and *vol_name* を実際の情報に置き換えます。

```
::> volume autosize -vserver svm_name -volume vol_name
```

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」の「volume modify」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、「階層化ポリシーの更新」を参照してください。

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場合など、移行などの場合に便利です。

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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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、クラウド書き込みモードを設定するボリュームの名前に置き換えてください。
   - *vol_cw_mode* を `true` に置き換えて、ボリュームでクラウド書き込みモードを有効にするか、`false` に置き換えて無効にします。

   ```
   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.
   ```

ストレージ容量の更新

ボリュームストレージ容量を管理するには、、 API AWS マネジメントコンソール、 AWS CLI ONTAP CLI を使用してボリュームサイズを手動で増減します。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。

ONTAP CLI を使用して、volume modify コマンドで、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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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することもできます。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。
   - *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。
   - *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
   ```

階層化ポリシーの更新

ボリュームの階層化ポリシーは、、 API AWS マネジメントコンソール、 AWS CLI 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 マネジメントコンソールを使用して、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 の 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 Amazon FSx API アクションと同等です)。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」の「volume modify」を参照してください。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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
```

最低冷却日数の更新

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」(ボリューム更新) の CLI コマンドを使用してボリューム設定を変更します (「UpdateVolume」(ボリューム更新) は Amazon FSx API アクションと同等です)。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」の「volume modify」を参照してください。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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更新

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」の「volume modify」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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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.
   ```

ボリューム上のファイルの最大数の更新

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すことができます。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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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

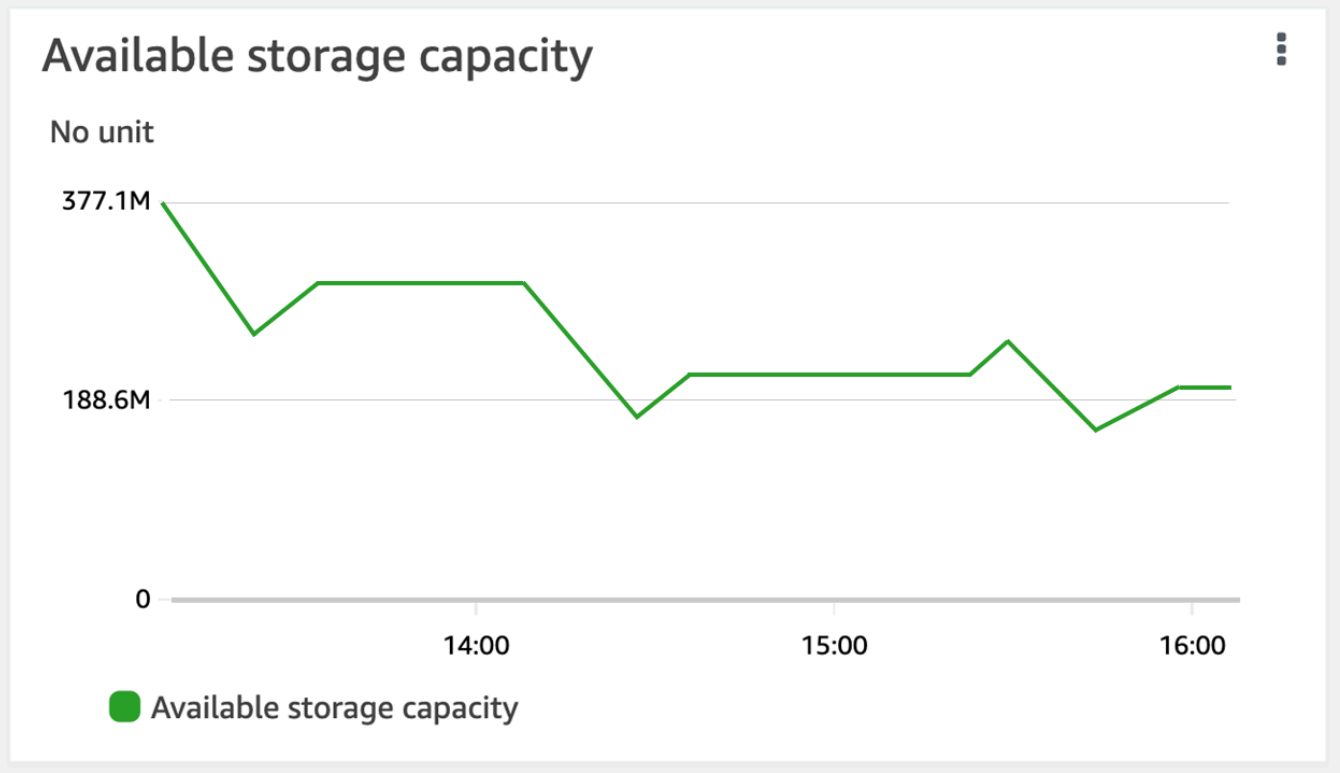
ボリュームの使用可能なストレージとそのストレージディストリビューション、 AWS マネジメントコンソール AWS CLIおよび NetApp ONTAP CLI を表示できます。

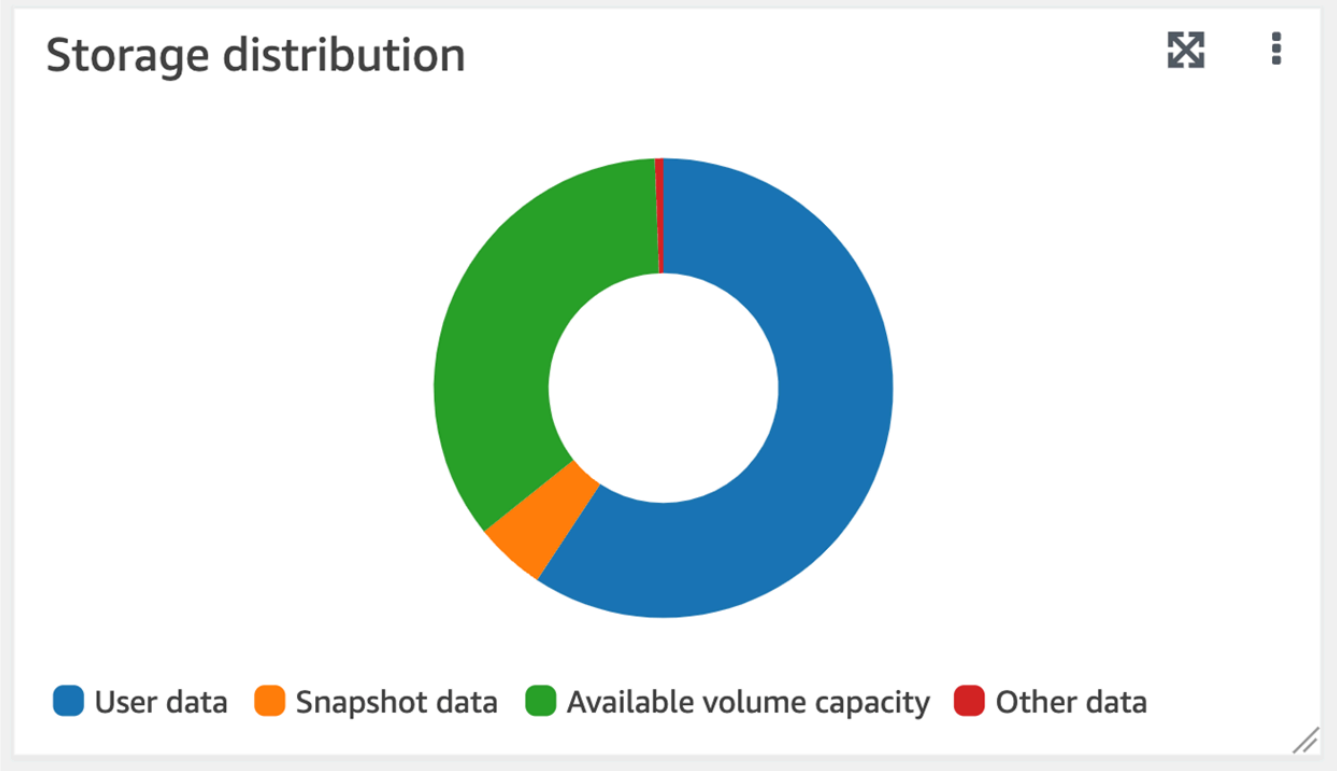
ボリュームのストレージ容量をモニタリングするには (コンソール)

[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 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モニタリングすることができます。詳細については、NetApp ONTAP ドキュメントセンターの「`volume show-space`」を参照してください。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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。

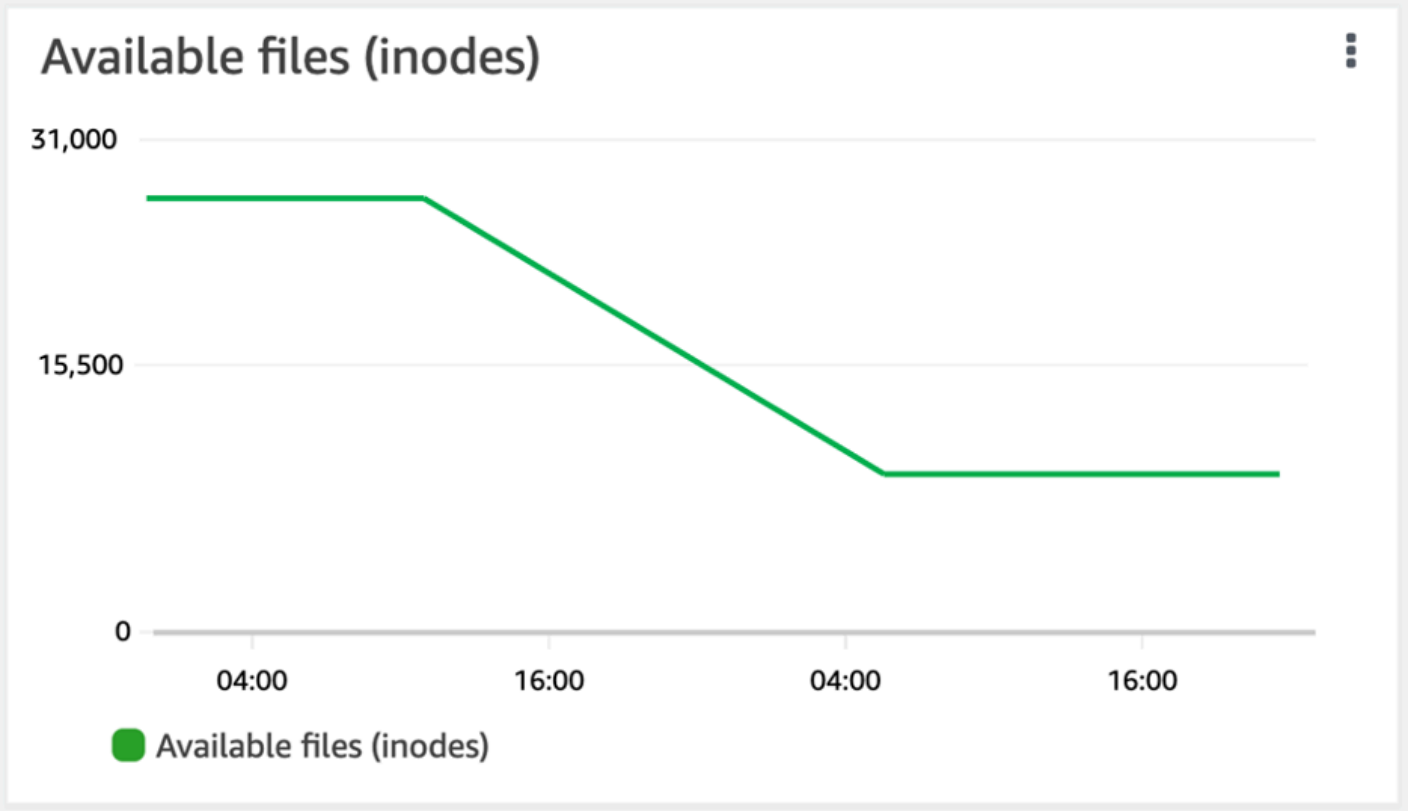
使用可能な領域を増やすには、次の手順に示すように、ボリュームのサイズを大きくするか、使用していないスナップショットを削除します。

FlexVol ボリュームタイプ (デフォルトの FSx for ONTAP のボリュームタイプ) の場合、ボリュームの自動サイズ調整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。

ボリュームのファイル容量のモニタリング

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。



FSx for ONTAP ファイルシステムの管理

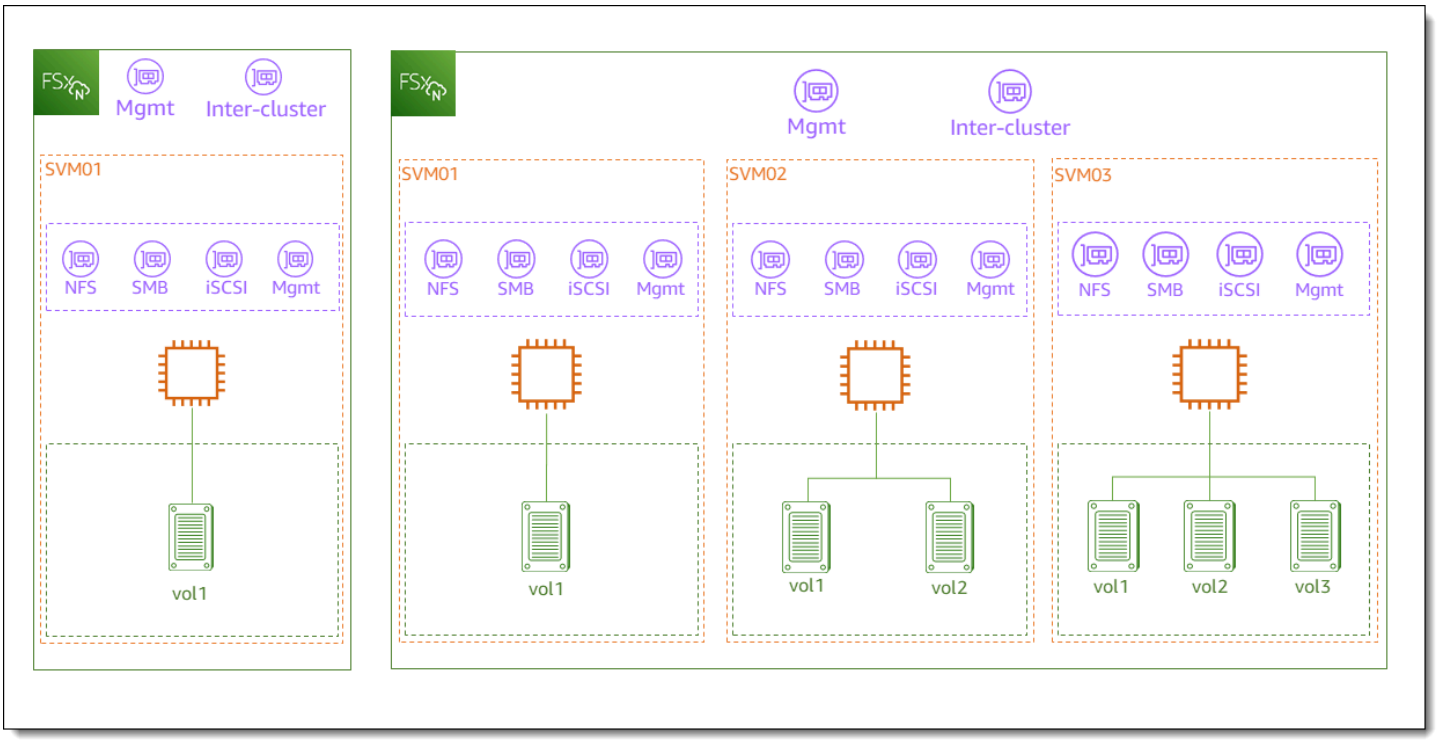
ファイルシステムは オンプレミス ONTAP クラスターに類似した Amazon FSx のプライマリリソースです。ファイルシステムの SSD ストレージ容量とスループットキャパシティを指定し、ファイルシステムが作成される仮想プライベートクラウド (VPC) を選択します。各ファイルシステムには管理エンドポイントがあり、ONTAP CLI または REST API を使用してリソースとデータを管理できます。

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、以下のプライマリリソースで設定されます。

- 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。第 1 世代ファイルシステムとマルチ AZ 第 2 世代ファイルシステムには 1 つの HA ペアがあり、第 2 世代シングル AZ ファイルシステムには最大 12 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 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。

次の画像は、第 1 世代の FSx for ONTAP ファイルシステム (1 つの HA ペアを伴う) のアーキテクチャと、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 SVM にはそれぞれ管理用の複数のエンドポイントがあり、SVM にはデータアクセスエンドポイントもあります。



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)。Single-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。第 1 世代シングル AZ ファイルシステムは、1 つの HA ペアをサポートしています。第 2 世代シングル AZ ファイルシステムは、最大 12 の HA ペアをサポートしています。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。第 1 世代と第 2 世代のマルチ AZ ファイルシステムはどちらも 1 つの HA ペアをサポートしています。

  > **Note**
  >
  > 作成後にファイルシステムのデプロイタイプを変更することはできません。デプロイタイプを変更する場合 (シングル AZ 1 からシングル AZ 2 に移行する場合など)、データをバックアップし、新しいファイルシステムに復元できます。NetApp SnapMirror、 AWS DataSync、またはサードパーティーのデータコピーツールを使用してデータを移行することもできます。詳細については、「NetApp SnapMirror を使用した FSx for ONTAP への移行」および「AWS DataSync を使用した FSx for ONTAP への移行」を参照してください。

- ストレージ容量 – これは SSD ストレージの量で、第 1 世代ファイルシステムでは最大 192 テビバイト (TiB)、第 2 世代マルチ AZ ファイルシステムでは 512 TiB、第 2 世代シングル AZ ファイルシステムでは 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。ONTAP CLI および REST API を使用してファイルシステムを管理するためのユーザーを使用することができます。

ネットアップの ONTAP CLI または REST API を使用して ONTAP ファイルシステムの FSx を管理できます。また、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) との間の SnapMirror または SnapVault 関係を設定することもできます。各 Amazon FSx for NetApp 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、Secure Shell (SSH) 経由で ONTAP CLI にアクセスするか、ファイルシステムで ONTAP REST API を使用します。
- クラスター間 - NetApp SnapMirror または NetApp FlexCache を使用してレプリケーションをセットアップする場合は、このエンドポイントを使用します。

詳細については、「NetApp アプリケーションを使用した ONTAP リソースの FSx の管理」および「NetApp SnapMirrorを使用したデータの複製」を参照してください。

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、 AWS CLIまたは Amazon FSx API を使用して 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 AWS アカウント が共有している VPC で作成できます。結合する VPC でマルチ AZ ファイルシステムを作成する際には、いくつかの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、「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. [ファイルシステムのタイプを選択] ページの [ファイルシステムのオプション] で、[Amazon FSx for NetApp ONTAP]、[次へ] の順に選択します。
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。
- [デプロイタイプ] では、[マルチ AZ 2]、[シングル AZ 2]、[マルチ AZ 1]、または [シングル AZ 1] 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。マルチ AZ 1 は、ONTAP ファイルシステム用の第 1 世代 FSx です。マルチ AZ 2 は第 2 世代のファイルシステムです。これらはどちらも 1 つの高可用性 (HA) ペアをサポートしています。
  - [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。シングル AZ 1 は、1 つの HA ペアをサポートする第 1 世代 FSx for ONTAP ファイルシステムです。シングル AZ 2 は、最大 12 の HA ペアをサポートする第 2 世代ファイルシステムです。詳細については、「高可用性 (HA) ペアの管理」を参照してください。

    デプロイタイプの詳細については、「可用性、耐久性、デプロイオプション」を参照してください。

    > **Note**
    >
    > 作成後にファイルシステムのデプロイタイプを変更することはできません。デプロイタイプを変更する場合 (シングル AZ 1 からシングル AZ 2 に移行する場合など)、データをバックアップし、新しいファイルシステムに復元できます。NetApp SnapMirror、 AWS DataSync、またはサードパーティーのデータコピーツールを使用してデータを移行することもできます。詳細については、「NetApp SnapMirror を使用した FSx for ONTAP への移行」および「AWS DataSync を使用した FSx for ONTAP への移行」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) ペアの管理」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。
- (マルチ AZ のみ) [優先サブネット] に関して、使用可能なサブネットのリストから任意の値を選択します。また、スタンバイファイルサーバの [スタンバイサブネット] 値を選択します。
- (マルチ AZ のみ) [サブネット] に関して、使用可能なサブネットのリストから任意の値を選択します。
- (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 CloudFormation することをお勧めします。

- ネットワークタイプでは、IPv4 (IPv4 サポートのみ) またはデュアルスタック (IPv4 と IPv6 の両方のサポート) を選択します。既存のファイルシステムのネットワークタイプはいつでも変更できます。詳細については、「ネットワークタイプの変更」を参照してください。

  > **Note**
  >
  > デュアルスタックモードを使用する FSx for ONTAP ファイルシステムを作成する場合は、まず Amazon が提供する IPv6 CIDR ブロックを VPC とサブネットに割り当てる必要があります。詳細については、Amazon Virtual Private Cloud ユーザーガイドの「VPC に IPv6 サポートを追加する」をご参照ください。

- (マルチ AZ のみ) [エンドポイント IPv4 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、IPv4 アドレスの範囲を指定します。

  エンドポイント IPv4 アドレスの範囲には、以下の 3 つのオプションがあります:

  - [VPC からの未割り当ての IPv4 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 IPv4 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。

  - [VPC 外のフローティング IPv4 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。
  - [IPv4 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 IPv4 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

- (マルチ AZ およびデュアルスタックのみ) [エンドポイント IPv6 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、IPv6 アドレスの範囲を指定します。エンドポイント IPv6 アドレスの範囲には、以下の 2 つのオプションがあります:
  - [VPC からの未割り当ての IPv6 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 IPv6 アドレス範囲として使用するため、VPC の IPv6 CIDR 範囲の 1 つから利用可能な 1024 個の IPv6 アドレスのブロックを選択します。
  - [IPv6 アドレス範囲を入力] — 任意の IPv6 CIDR 範囲を指定できます。選択する IPv6 アドレス範囲は、サブネットと重複しない限り VPC の IPv6 アドレス範囲の内側でも外側でも可能です。

7. [暗号化] セクションの [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、「ONTAP CLI 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、「ONTAP CLI を使用した SVM 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。
   - ボリュームのセキュリティスタイルについて、Unix (Linux) と NTFS から選択してください。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。

- 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結合しない 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結合する) 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 または IPv6 アドレス。
  - [サービスアカウントの認証情報] – サービスアカウントの認証情報を指定する方法を選択します:
    - オプション 1: AWS Secrets Manager シークレット ARN - Active Directory 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を含むシークレット。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。
    - オプション 2: プレーンテキスト認証情報
      - サービスアカウントのユーザー名 - 既存の Microsoft Active Directory 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) - 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、委任 FSx 管理者、 AWS 委任管理者、OU AWS への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 に結合している場合は、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。
    - (HA ペアが 1 つだけのファイルシステム) ボリュームスタイルには、FlexVolまたはFlexGroupのいずれかを選択します。FlexVolボリュームは、最大 300 テビバイト (TiB) の汎用ボリュームです。FlexGroupボリュームは、高パフォーマンスのワークロードを対象としており、最大 20 PiB のサイズにすることができます。
    - [ボリュームサイズ] では、FlexVol ボリュームの場合は 20 ~ 314,572,800 メビバイト (MiB)、FlexGroup ボリュームの場合は 1 つの HA ペアあたり 800 ギビバイト (GiB) ~ 2,400 TiB の範囲の整数を入力します。例えば、12 の HA ペアを持つファイルシステムの場合、最小ボリュームサイズは 9,600 GiB、最大サイズは 20,480 TiB です。
    - ボリュームの種類では、読み取り/書き込み (RW) を選択して読み取り可能および書き込み可能なボリュームを作成するか、データ保護 (DP) を選択して読み取り専用のボリュームを作成し、NetApp SnapMirrorまたはSnapVaultリレーションシップの宛先として使用できます。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、「ストレージ効率」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. [デフォルトボリューム SnapLock 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 コンプライアンスについて」および「SnapLock エンタープライズ について」を参照してください。SnapLock の詳細については、「SnapLock でのデータの保護」を参照してください。

13. 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。

14. 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。

15. 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。

16. 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 ファイルシステムの作成 CLI コマンド (または同等のコマンド CreateFileSystem API オペレーション) を使用します。

> **Note**
>
> 作成後にファイルシステムのデプロイタイプを変更することはできません。デプロイタイプを変更する場合 (シングル AZ 1 からシングル AZ 2 に移行する場合など)、データをバックアップし、新しいファイルシステムに復元できます。NetApp SnapMirror、 AWS DataSync、またはサードパーティーのデータコピーツールを使用してデータを移行することもできます。詳細については、「NetApp SnapMirror を使用した FSx for ONTAP への移行」および「AWS DataSync を使用した FSx for ONTAP への移行」を参照してください。

```
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 (SVM) 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、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、VPCs とサブネットを他の と安全に共有 AWS Resource Access Manager するために を使用する必要があります AWS アカウント。詳細については、「 AWS Resource Access Manager ユーザーガイド」の AWS 「リソースの共有」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 マネジメントコンソール 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、以下に示すように、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、Amazon FSx コンソールと CLI を使用して更新する手順を説明します。Amazon FSx コンソール、および API を使用して AWS CLI、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。詳細については、「日次自動バックアップ」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。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、「ONTAP CLI 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、NetApp こんそ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 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)

以下の手順では、 AWS マネジメントコンソールを使用して既存の FSx for ONTAP ファイルシステムを更新する方法を説明します。

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] パネルで、[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。パスワード設定の変更方法などの詳細については、「fsxadmin アカウントのパスワードの更新が失敗する」を参照してください。

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. [アクション] で、[ファイルシステムを更新 > ルートテーブルを更新] を選択します。または、[ネットワークとセキュリティ] パネルで、ファイルシステムの [ルートテーブル] の横にある [管理] を選択します。
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] を選択してください。

ファイルシステムを更新するには (CLI)

次の手順は、 AWS CLI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。

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 (または同等のコマンド UpdateFileSystem 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
```

高可用性 (HA) ペアの管理

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 つ以上の高可用性 (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 第 1 世代の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 第 2 世代のマルチ AZ ファイルシステムも 1 つの HA ペアを搭載し、最大 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。FSx for ONTAP 第 2 世代のシングル AZ ファイルシステムには、最大 12 の HA ペアが搭載されており、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) を実現します。

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 6 GBps のスループットキャパシティと 200,000 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 ペアを第 2 世代の シングル AZ ファイルシステムに追加できます。詳細については、「高可用性 (HA) ペアの追加」を参照してください。それ以外の場合は、 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。

高可用性 (HA) ペアの追加

FSx for ONTAP ファイルシステムは、1 つ以上の HA ペアのファイルサーバーで構成されます。第 1 世代ファイルシステムと第 2 世代マルチ AZ ファイルシステムは 1 つの HA ペアをサポートしますが、第 2 世代シングル AZ ファイルシステムは最大 12 の HA ペアをサポートしています。第 2 世代のシングル AZ ファイルシステムを作成した後、HA ペアをさらに追加することもできます (最大 12)。HA ペアの追加は破壊的なものではなく、通常、完了までに数分しかかかりません。

HA ペアをファイルシステムに追加するときは、次の点を考慮してください。

- HA ペアをファイルシステムに追加すると、独自のストレージ (またはアグリゲート) を持つ新しいファイルサーバーが導入されます。新しい HA ペアのスループットキャパシティとストレージ容量は、ファイルシステムの既存の HA ペアと同じです。例えば、ファイルシステムに合計 12 GBps のスループットキャパシティと 2 テビバイト (TiB) の SSD ストレージを持つ 2 つの HA ペアがあるとします。新しい HA ペアを 1 つ追加すると、ファイルシステムには 18 GBps のスループットキャパシティと 3 TiB の SSD ストレージがあります。
- 新しい HA ペアのパフォーマンスを向上させるには、既存のボリュームの一部を新しい HA ペアに移動し、クライアントを再マウントして接続する必要があります。詳細については、「HA ペア間でワークロードのバランスを取る」を参照してください。
- HA ペアを追加するとき、または HA ペアを追加する更新が進行中のときは、ファイルシステムのスループットキャパシティ、SSD ストレージキャパシティ、またはプロビジョニングされた SSD IOPS を変更することはできません。
- HA ペアを追加した後にその HA を削除することはできません。一時的にパフォーマンスを向上させる必要がある場合は、ファイルシステムのスループットキャパシティをスケーリングすることをお勧めします (ファイルシステムがスループットキャパシティの上限に達していないことが前提)。これにより、ファイルシステムの既存の HA ペアのスループットキャパシティが増加します。
- iSCSI プロトコルは、高可用性ペア (HA ペア) が 6 つ以下のファイルシステムで使用できます。NVMe /TCP プロトコルは、HA ペアが 6 つ以下の第 2 世代ファイルシステムで使用できます。詳細については、「FSx for ONTAP データへのアクセス」を参照してください。
- ファイルシステムに新しい HA ペアを追加すると、新しいファイルシステムノードの NVMe キャッシュがデフォルトで有効になります。スループットの高いワークロードでは、無効にすることをお勧めします。詳細については、「NVMe キャッシュの管理」を参照してください。

HA ペアを追加するには

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. [概要] パネルの [HA ペアの数] で、[更新] を選択します。
4. [HA ペア] ドロップダウンから、ファイルシステムに追加する HA ペアの数を選択します。
5. [Update] (更新) ボタンを選択します。

HA ペアを追加したら、既存のデータのバランスを再調整して、I/O がファイルシステムの HA ペア全体に均等に分散されるようにすることが重要です。詳細については、「HA ペア間でワークロードのバランスを取る」を参照してください。

HA ペア間でワークロードのバランスを取る

複数の高可用性 (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スループットとストレージは、各 HA ペアに分散されます。FSx for ONTAP は、ファイルシステムに書き込まれるときにファイルのバランスを自動的に調整しますが、HA ペアを追加すると、ワークロードデータと I/O のバランスは取れなくなります。さらに、まれに、ワークロードデータまたは I/O がファイルシステムの既存の HA ペア間で不均衡になる場合があり、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可能性があります。ワークロードが不均衡である場合、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、バランスの再調整ができます。

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
- CloudWatch ディメンションを ONTAP CLI および REST API リソースにマッピングする
- クライアントのバランスの再調整
- ボリュームのバランスの再調整

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、アグリゲート間でボリュームを移動します。詳細については、「アグリゲート間のボリュームの移動」を参照してください。

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、「ボリュームのバランスの再調整」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	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

ファイルシステムの状態	結果...
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	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、「クライアントのバランスの再調整」を参照してください。

CloudWatch ディメンションを ONTAP CLI および REST API リソースにマッピングする

第 2 世代のファイルシステムには、`FileServer` または `Aggregate` のディメンションを持つ Amazon CloudWatch メトリクスが備わっています。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`)。各 HA ペアにはアグリゲートが 1 つ存在します。つまり、HA ペア内でアグリゲート `aggr1` は ファイルサーバ `FsxId01234567890abcdef-01` (アクティブなファイルサーバ) と `FsxId01234567890abcdef-02` (セカンダリファイルサーバ) によって共有され、アグリゲート `aggr2` はファイルサーバ `FsxId01234567890abcdef-03` および `FsxId01234567890abcdef-04` その他によって共有されることを意味します。

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」の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.
```

クライアントのバランスの再調整

HA ペアを追加した後、またはファイルサーバー間で I/O の不均衡 (特にネットワークスループット使用率による) が発生した場合は、クライアントのバランスを再調整できます。HA ペアを追加した後にクライアントのバランスを再調整する場合は、クライアントの再マウント にスキップできます。それ以外の場合は、ワークロード I/O のバランスを再調整するために、まず移動する、トラフィックの多いクライアントを特定する必要があります。

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。

トラフィックの多いクライアントを特定する

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」の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
```

クライアントの再マウント

- クライアントのバランスを他の HA ペアに再調整できます。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ファイルサーバーに対応する 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)。

ボリュームのバランスの再調整

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」の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. 新しい HA ペアを追加した場合は、既存のボリュームを新しいアグリゲートに移動する必要があります。詳細については、「アグリゲート間のボリュームの移動」を参照してください。

NVMe キャッシュの管理

NVMe キャッシュは、第 2 世代ファイルシステムでデフォルトで有効になっています。第 2 世代のファイルシステムにスループットの高いワークロードがある場合は、NVMe キャッシュを無効にしてパフォーマンスを向上させることができます。次の手順では、ファイルシステムの NVMe キャッシュを有効、無効に、検証する方法について説明します。

NVMe キャッシュを管理するには

1. ONTAP ファイルシステムに SSH します。詳細については、「the section called “NetApp ONTAP CLI の使用”」を参照してください。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. system node external-cache modify ONTAP CLI コマンドを使用します。**true** を選択して NVMe キャッシュを有効にするか、**false** を選択して無効にします。

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. system node external-cache show ONTAP CLI コマンドを使用して、NVMe キャッシュが有効か無効かを確認します。

```
::> system node external-cache show -node * -fields is-enabled
```

NVMe キャッシュは、ノードごとに有効または無効になります。新しい高可用性 (HA) ペアをファイルシステムに追加すると、新しいノードごとに新しいファイルシステムのノードと同じデフォルトの動作になります。したがって、既存のノードが無効になっている場合でも、ファイルシステム上の新しいノードに対して NVMe キャッシュが有効になります。詳細については、「高可用性 (HA) ペアの追加」を参照してください。

ネットワークタイプの管理

FSx for ONTAP ファイルシステムを作成するときは、ネットワークタイプを指定する必要があります。ネットワークタイプは、以下のいずれかのオプションである必要があります:

- `IPv4` を使用すると、ファイルシステムはインターネットプロトコルバージョン 4 (IPv4) のみを使用して通信できます。
- `Dual-stack` を使用すると、ファイルシステムはインターネットプロトコルバージョン 6 (IPv6) と IPv4 の両方を使用して通信できます。

既存の FSx for ONTAP ファイルシステムのネットワークタイプは、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 SDK を使用していつでも変更できます。例えば、サブネットが IPv4 と IPv6 の両方のアドレス指定をサポートしている場合、既存のファイルシステムを IPv4 専用 モードからデュアルスタックモードに更新できます。また、デュアルスタックファイルシステムを IPv4 専用 に更新することもできます。

デュアルスタックモードの使用

IPv6 クライアントから Amazon FSx ファイルシステムにネイティブにアクセスして管理する必要がある場合は、デュアルスタックモードを使用する必要があります。デュアルスタックアドレッシングを使用するように Amazon FSx ファイルシステムを設定することで、同じ Amazon VPC、別のAWS

アカウントの VPC、またはオンプレミスネットワーク内の IPv6 クライアントおよび IPv4 クライアントからファイルデータにアクセスできます。たとえば、Amazon FSx ファイルシステムがデュアルスタックを使用するように設定されている場合、既存の IPv4 クライアントと新しい IPv6 クライアントがファイルシステムに保存されているファイルデータにアクセスできるようになります。

デフォルトでは、Amazon FSx と Amazon VPC は IPv4 アドレス設定プロトコルを使用します。そのため、IPv6 を使用する前提条件として、Amazon FSx ファイルシステムで IPv6 を使用する前に、まず Amazon が提供する IPv6 クラスレスドメイン間範囲 (CIDR) ブロックを VPC とサブネットに割り当てる必要があります。VPC で IPv6 を有効にする方法については、Amazon Virtual Private Cloud ユーザーガイド」の「VPC の IPv6 サポートを追加する」を参照してください。

デュアルスタックモードに設定された ONTAP ファイルシステムの FSx を作成する場合、既存の IPv4 のアドレス範囲に加えて、ファイルシステムにアクセスするエンドポイントが作成される IPv6 の アドレス範囲を指定できます。デフォルトでは、Amazon FSx はファイルシステムのエンドポイント IPv6 アドレスの範囲として使用する VPC の IPv6 CIDR 範囲の 1 つから 1024 個の IP アドレスのブロックを選択します。

ネットワークタイプの変更

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ネットワークタイプを変更できます。

ファイルシステムのネットワークタイプを変更するには (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. [ファイルシステム] に移動してネットワークタイプを変更する ONTAP ファイルシステムを選択します。
3. [アクション] で、[ネットワークタイプの更新] を選択します。または、[ネットワークとセキュリティ] パネルで、ファイルシステムの [ネットワークタイプ] の横にある [管理] を選択します。

   [ストレージタイプの更新] ウィンドウが表示されます。
4. [希望するネットワークタイプ] で、[IPv4] または [デュアルスタック] を選択します。

   - `IPv4` を選択した場合、必要な設定はこれだけです。
   - `Dual-stack` を選択した場合は、ファイルシステムエンドポイントが使用する IPv6 アドレス範囲を指定します:
     - [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 IPv6 アドレス範囲として使用するため、VPC の IPv6 CIDR 範囲から利用可能な/118 個の IP アドレスを選択します。

- [IPv6 アドレス範囲を入力] — 任意の IPv6 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。

5. [更新] を選択します。

ファイルシステムのネットワークタイプを変更する方法 (CLI)

- FSx for ONTAP ファイルシステムの設定を更新するには、以下の例に示すように update-file-system CLI コマンド (または同等のコマンド UpdateFileSystem API オペレーション) を使用します。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --network-type DUAL
```

ファイルシステムの詳細のモニタリング

Amazon FSx コンソール、、API、およびサポートされている AWS SDKs を使用して AWS CLI、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 – 以下のファイルシステム管理情報を表示します:
    - デフォルト Amazon VPC
    - マルチ AZ ファイルシステムに関連付けられた Amazon VPC ルートテーブル
    - ファイルシステムのネットワークタイプ (IPv4 専用またはデュアルスタック)
    - エンドポイント IPv4 または IPv6 アドレス範囲
    - AWS Key Management Service (AWS KMS) キー ID
  - 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 CloudWatch によるモニタリング」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 コンソールの 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。

ファイルシステムのステータス	説明
[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。 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。

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 - リソースのクリーンアップ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。

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 マネジメントコンソール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いつでも追加の SVMs を作成できます。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 に結合させることで、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、およびにネットワークタイプにも依存します。

高可用性 (HA) ペア	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 (IPv4 専用モード)	ファイルシステムあたりの SVM の最大数 (デュアルスタックモード)
	128	6	6
	256	6	6
	384	6	6
	512	14	11
	768	14	11
1 HA ペア	1,024	14	11
	1,536	14	11
	2,048	24	11
	3,072	24	11
	4,096	24	11
	6,144	24	11
2 ~ 12 の HA ペア	いずれか	11	11

トピック

- ストレージ仮想マシン (SVM) の作成
- ストレージ仮想マシン (SVM) の更新
- SVM Microsoft Active Directory 設定の管理
- ファイルアクセスの監査
- ワークグループでの SMB サーバーのセットアップ
- ストレージ仮想マシン (SVM) 設定の詳細のモニタリング
- ストレージ仮想マシン (SVM) の削除

ストレージ仮想マシン (SVM) の作成

FSx for ONTAP SVM は AWS マネジメントコンソール、、 AWS CLI、および API を使用して作成できます。

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、ネットワークタイプ、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 または NTFS) 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、「ONTAP CLI を使用した SVM 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。
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、「ONTAP CLI を使用した SVM 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 サーバの IP アドレス:ドメインの DNS サーバの IPv4 または IPv6 アドレス。
     - [サービスアカウントの認証情報] – サービスアカウントの認証情報を指定する方法を選択します:
       - オプション 1: AWS Secrets Manager シークレット ARN - Active Directory 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を含むシークレット。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。
       - オプション 2: プレーンテキスト認証情報

- サービスアカウントのユーザー名 - 既存の Microsoft Active Directory 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) - 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、委任 FSx 管理者、 AWS 委任管理者、OU AWS への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 に結合している場合は、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 (または同等のコマンド 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 (SVM) 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 Microsoft Active Directory 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–

- 現在の AWS アカウント 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、Storage 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、次の例で示すように、「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"
      }
    }
  }
}
```

SVM Microsoft Active Directory 設定の管理

SVM を Microsoft アクティブディレクトリに参加させたり、既に Microsoft アクティブディレクトリに参加している SVM の Microsoft アクティブディレクトリ構成を変更したりできます。FSx for ONTAP は と統合 AWS Secrets Manager して、ドメイン参加サービスアカウントの認証情報を安全に管理します。

SVM Microsoft Active Directory 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. 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–

   - 現在の AWS アカウント 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、Storage 仮想マシンを展開ONTAPして選択します。
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] > [Microsoft Active Directory 設定を更新] を選択します。[Microsoft アクティブディレクトリ設定を更新]ウィンドウが表示されます。
5. [ドメイン結合サービスアカウントの認証情報] では、[Secrets Manager で管理] (推奨) を選択して、Secrets Manager を使用して認証情報を安全に管理します。

   > **Note**
   >
   > Secrets Manager を使用すると、プレーンテキスト認証情報を保存する必要がなくなり、認証情報を一元管理できます。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。

6. シークレット では、更新されたドメイン結合サービスアカウントの認証情報を含む Secrets Manager から既存のシークレットを選択するか、[新しいシークレットを作成] を選択して作成します。
7. 環境の必要に応じて、他の Microsoft Active Directory 設定フィールドを更新します。
8. [変更を保存] を選択して変更を保存します。

SVM Microsoft Active Directory 設定を更新するには (CLI)

- FSx for ONTAP SVM の Microsoft Active Directory 設定を更新するには、次の例に示すように、update-storage-virtual-machine CLI コマンドを `--active-directory-configuration` パラメータとともに使用します。

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--active-directory-configuration DomainJoinServiceAccountSecret=secret-arn
```

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を設定するためのタスクの概要

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、またはその両方の口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	ファイルアクセス

イベント ID (EVT / EVTX)	イベント	説明	カテゴリ
		(ファイルまたはディレクトリ) を開く	
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 security file-directory ntfs sacl add コマンドファミリーを使用して設定できます。

例えば、以下のコマンドは、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 に作成します。

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

次に、以下のコマンドは p1 セキュリティポリシーを vs0 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。

ワークグループでの SMB サーバーのセットアップ

Microsoft ActiveDirectory ドメインインフラストラクチャが使用できないときに SVM を Microsoft Active Directory に結合する代わりに、ワークグループでサーバーメッセージブロック (SMB) サーバーを設定できます。ワークグループは、SMB プロトコルを使用するピアツーピアネットワークであり、ローカルアカウントとグループのみがあります。

ワークグループのメンバーとして SMB サーバーを設定するプロセスは、以下で構成されます:

- ストレージ仮想マシン (SVM) での SMB サーバーの作成。
- ローカルユーザーおよびグループの作成。
- ローカルユーザーまたはグループをワークグループのメンバーとして追加する。

ワークグループモードの SMB サーバーは、以下の SMB 機能をサポートしていないことに留意してください:

- SMB3 Witness プロトコル
- SMB3 CA 共有
- SMB 経由の SQL
- フォルダのリダイレクト

- ローミングプロファイル
- グループポリシーオブジェクト (GPO)
- ボリュームスナップショットサービス (VSS)

また、ワークグループモードの SMB サーバーは NTLM 認証のみをサポートし、Kerberos 認証はサポートしていません。

以下の手順では、ワークグループ内の SVM に SMB サーバーをセットアップし、ローカルアカウントを作成し、これらのアカウントをワークグループメンバーシップに追加するプロセスについて説明します。これらの手順を実装するには、ファイルシステムまたは SVM 管理インターフェイスから NetApp ONTAP CLI を使用します。詳細については、「NetApp ONTAP CLI の使用」を参照してください。

トピック

- ワークグループでの SMB サーバーの作成
- SMB サーバーでのローカルユーザーアカウントの作成
- SMB サーバーでのローカルグループの作成
- ローカルグループへのローカルユーザーの追加

ワークグループでの SMB サーバーの作成

vserver cifs create ONTAP CLI コマンドを使用して SVM に SMB サーバーを作成し、それが属するワークグループを指定できます。

開始する前に

データの提供に使用する SVM とボリューム (およびインターフェイス) は、SMB プロトコルを許可するように設定されている必要があります。

LIF は、SVM で設定された DNS サーバーに接続できる必要があります。ファイルシステムでは CIFS ライセンスが必要になる場合がありますが、SMB サーバーを認証にのみ使用する場合、CIFS ライセンスは必要ありません。

ワークグループに SMB サーバーを作成するには

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. ワークグループに SMB サーバーを作成します:

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

以下のコマンドは、ワークグループ smb_server01 に SMB サーバー workgroup01 を作成します:

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -
workgroup workgroup01
```

SVM の管理ポートに接続されている場合は、-vserver を指定する必要はありません。

3. vserver cifs show コマンドを使用して SMB サーバーの設定を確認します。

以下の例では、コマンド出力は、smb_server01 という名前の SMB サーバーがワークグループ workgroup01 の SVM svm1 に作成されたことを示しています:

```
FSxIdabcde123456::> vserver cifs show -vserver svm1

                                          Vserver: svm1
                        CIFS Server NetBIOS Name: SMB_SERVER01
                NetBIOS Domain/Workgroup Name: workgroup01
                 Fully Qualified Domain Name: -
                         Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                 Workgroup Name: workgroup01
                            Authentication Style: workgroup
            CIFS Server Administrative Status: up
                              CIFS Server Description:
                              List of NetBIOS Aliases: -
```

SMB サーバーでのローカルユーザーアカウントの作成

SMB 接続を介して SVM に含まれるデータへのアクセスを許可するために使用できるローカルユーザーアカウントを作成できます。SMB セッションを作成するときに、認証にローカルユーザーアカウントを使用することもできます。ローカルユーザーの機能は、SVM の作成時にデフォルトで有効になっています。ローカルユーザーアカウントを作成するときは、ユーザー名を指定し、アカウントを関連付ける SVM を指定する必要があります。

SMB サーバーでローカルユーザーアカウントを作成するには

1. vserver cifs users-and-groups local-user create ONTAP CLI コマンドを使用してローカルユーザーを作成します:

   ```
   vserver cifs users-and-groups local-user create -vserver svm_name -user-
   name user_name optional_parameters
   ```

   以下のオプションパラメータが役立つ場合があります:

   - `-full-name` – ユーザーのフルネーム。
   - `-description` – ローカルユーザーの説明。
   - `-is-account-disabled {true|false}` – ユーザーアカウントが有効か無効かを指定します。このパラメータが指定されない場合、デフォルトではユーザーアカウントは有効です。

   このコマンドは、ローカルユーザーのパスワードの入力を求めます。
2. ローカルユーザーのパスワードを入力し、パスワードを確認します。
3. ユーザーが正常に作成されたことを確認します:

   ```
   vserver cifs users-and-groups local-user show -vserver svm_name
   ```

以下の例では、SVM `svm1` に関連付けられたフルネーム `Sue Chang` のローカルユーザー `SMB_SERVER01\sue` を作成します:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1
 -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- ------------------------- ---------- -------------
svm1     SMB_SERVER01\Administrator            Built-in administrator account
svm1     SMB_SERVER01\sue           Sue Chang
```

SMB サーバーでのローカルグループの作成

SMB 接続を介して SVM に関連付けられたデータへのアクセスを許可するために使用できるローカルグループを作成できます。グループのメンバーが所有するユーザー権限または機能を定義する権限を割り当てることもできます。

ローカルグループの機能は、SVM の作成時にデフォルトで有効になっています。ローカルグループを作成するときは、グループの名前を指定し、グループを関連付ける SVM を指定する必要があります。グループ名は、ローカルドメイン名の有無にかかわらず指定でき、オプションでローカルグループの説明を指定できます。ローカルグループを別のローカルグループに追加することはできません。

SMB サーバーにローカルグループを作成するには

1. vserver cifs users-and-groups local-group create ONTAP CLI コマンドを使用してローカルグループを作成します。

   ```
   vserver cifs users-and-groups local-group create -vserver svm_name -group-
   name group_name [-description local_group_description
   ```

   ローカルグループに説明を付けることは有効です。
2. グループが正常に作成されたことを確認します:

   ```
   vserver cifs users-and-groups local-group show -vserver svm_name
   ```

以下の例では、SVM svm1 に関連付けられたローカルグループ SMB_SERVER01\engineering を作成します:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1
```

```
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
svm1             BUILTIN\Administrators        Built-in Administrators group
svm1             BUILTIN\Backup Operators      Backup Operators group
svm1             BUILTIN\Guests                Built-in Guests group
svm1             BUILTIN\Power Users           Restricted administrative privileges
svm1             BUILTIN\Users                 All users
svm1             SMB_SERVER01\engineering
```

ローカルグループへのローカルユーザーの追加

ローカルグループメンバーシップを管理するには、ローカルユーザーまたはドメインユーザーを追加または削除するか、ドメイングループを追加または削除します。これは、グループに配置されたアクセスコントロールに基づいてデータへのアクセスを制御する場合、またはユーザーにそのグループに関連付けられた権限を付与する場合に有効です。ローカルユーザー、ドメインユーザー、またはドメイングループに、グループ内のメンバーシップに基づくアクセス権限や権限が不要になった場合は、グループからメンバーを削除できます。

ローカルグループにメンバーを追加するときは、以下の点に注意してください:

- 特別な Everyone グループにユーザーを追加することはできません。
- ローカルグループを別のローカルグループに追加することはできません。
- ドメインユーザーまたはグループをローカルグループに追加するには、ONTAP が名前を SID に解決できる必要があります。

ローカルグループからメンバーを削除するときは、以下の点に留意してください:

- 特別な Everyone グループからメンバーを削除することはできません。
- ローカルグループからメンバーを削除するには、ONTAP が名前を SID に解決できる必要があります。

この手順で使用されるコマンドを実行するには、`fsxadmin` ロールが必要です。詳細については、「ONTAP ロールとユーザー」を参照してください。

ローカルグループメンバーシップを管理するには

- vserver cifs users-and-groups local-group add-members および vserver cifs users-and-groups local-group remove-members ONTAP CLI コマンドを使用して、メンバーをグループに追加または削除します。

- ワークグループにメンバーを追加するには:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-
name group_name -member-names name[,...]
```

ローカルユーザー、ドメインユーザー、またはドメイングループのカンマ区切りリストを指定して、指定したローカルグループに追加できます。

- ワークグループのメンバーを表示するには:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-
name group_name
```

- ワークグループからメンバーを削除するには:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -
group-name group_name -member-names name[,...]
```

ローカルユーザー、ドメインユーザー、またはドメイングループのカンマ区切りリストを指定して、指定されたローカルグループから削除できます。

以下の例では、SVM svm1 のローカルグループ SMB_SERVER01\engineering にローカルユーザー SMB_SERVER01\sue を追加します:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1
 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

以下の例では、ローカルユーザー SMB_SERVER01\sueと SMB_SERVER01\james を SVM svm1 のローカルグループ SMB_SERVER01\engineering から削除します:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names
 SMB_SERVER01\sue,SMB_SERVER01\james
```

以下の例では、ローカルグループ SMB_SERVER01\engineering のメンバーを一覧表示します:

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -
vserver svm_name -group-name group_name
```

```
            Vserver: svm1
        Domain Name: SMB_SERVER01
         Group Name: SMB_SERVER01\engineering
        Member Name: SMB_SERVER01\anita
                     SMB_SERVER01\james
                     SMB_SERVER01\liang
```

ストレージ仮想マシン (SVM) 設定の詳細のモニタリング

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は AWS CLI、Amazon FSx コンソール、、および Amazon FSx API を使用して確認できます。

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 - delete-storage-virtual-machine CLI コマンドまたは DescribeStorageVirtualMachines API 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。

ストレージ仮想マシン (SVM) の削除

FSx for ONTAP SVM は AWS CLI、Amazon FSx コンソール、、および API を使用してのみ削除できます。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**
>
> SVM は、NetApp ONTAP CLI または API を使用して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 (または同等のコマンド 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
```

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 マネジメントコンソール、AWS CLI、Amazon FSx API、または NetApp Console 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 ボリューム、すべての HA ペアで最大 1,000 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、FlexGroup ごとに 8 の構成ボリュームがあります。

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 FlexGroup のどちらかです。
- 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。
- ストレージ効率化 - ストレージ効率化機能 (データのコンパクト化、圧縮、重複排除など) により、汎用的なファイル共有ワークロードで通常 65% のストレージが節約されます。

- ボリューム セキュリティスタイル (Unix または NTFS) - ユーザーを認証する際に、ボリュームのデータアクセスに使用するパーミッションの種類を決定します。
- データ階層化 – 階層化ポリシーは、費用対効果の高い容量プール層に格納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、容量プールストレージに移動す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。3 つの事前定義されたポリシーから選択するか、ONTAP CLI または REST API を使用して作成したカスタムポリシーを使用できます。
- タグをバックアップにコピー – Amazon FSx は、このオプションを使用してボリュームからすべてのタグをバックアップに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
- アグリゲート間のボリュームの移動
- ボリュームのモニタリング
- ボリュームの削除

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、AWS CLI、および Amazon FSx API を使用して FlexVol ボリュームまたは FlexGroup ボリュームのいずれかを作成できます。

- 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、1 つの HA ペアを持つ第 1 世代のファイルシステムおよび第 2 世代の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 ボリュームは複数の HA ペアを持つ第 2 世代の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。

FlexVol スタイルのボリュームを ONTAP CLI で FlexGroup スタイルに変換できます。変換すると、単一の構成要素から成る FlexGroup が作成されます。ただし、データが確実に FlexGroup's 構成要素全体に均等に分散されるように、AWS DataSync を使用して FlexVol ボリュームと新しい FlexGroup ボリュームとの間でデータを移動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、データは 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な場合で、すべての構成要素が既に最大サイズ (構成要素あたり 300 TiB) になっている場合にのみ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。以前のスナップショットは、新しい構成要素がまだ存在していなかったため、FlexGroup ボリュームの完全な現時点のイメージにはなっていません。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 では、Amazon FSx コンソール、AWS CLI、および Amazon FSx API を使用して 2 種類のボリュームを作成できます。

- 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 ボリュームを作成するときは、Unix と NTFS の 2 つのセキュリティスタイルから選択できます。各セキュリティスタイルは、データに対する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、どのクライアントタイプがデータにアクセスできるか、またはアクセスできないか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の決定に使用する 2 つの要素は、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、API でボリュームを作成すると、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。AWS CLI または API を使用して、ボリュームのセキュリティスタイルを変更できます。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。

ボリュームの作成

NetAppONTAP コマンドラインインターフェイス (CLI) と REST API の他に、Amazon FSx コンソール、AWS CLI、および Amazon FSx API を使用することでも FSx for ONTAP FlexVol ボリュームまたは 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. [ファイルシステムのタイプ] には、[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。
   - ボリュームの種類では、読み取り/書き込み (RW) を選択して読み取り可能および書き込み可能なボリュームを作成するか、データ保護 (DP) を選択して読み取り専用のボリュームを作成し、NetApp SnapMirrorまたはSnapVaultリレーションシップの宛先として使用できます。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。
- [ストレージ効率] で、このボリュームで、[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、「ストレージ効率」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について、Unix (Linux) と NTFS から選択してください。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 コンプライアンスについて」および「SnapLock エンタープライズ について」を参照してください。SnapLock の詳細については、「SnapLock でのデータの保護」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、複数の HA ペアを持つファイルシステム用の FlexGroup ボリュームのみです。複数の HA ペアを持つファイルシステム用の 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. [ファイルシステムのタイプ] には、[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 [FlexGroup] 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、HA ペアごとに 800 ギビバイト (GiB) ~ 2,400 ペビバイト (PiB) の範囲で任意の整数を入力します。例えば、高可用性 (HA) ペアが 12 のファイルシステムの場合、最小ボリュームサイズは 9,600 GiB、最大サイズは 20,480 TiB になります。
   - [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、「ストレージ効率」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について、Unix (Linux) と NTFS から選択してください。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 コンプライアンスについて」および「SnapLock エンタープライズ について」を参

照してください。SnapLock の詳細については、「SnapLock でのデータの保護」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、create-volume CLI コマンド (または同等のコマンド CreateVolume API オペレーション) が使用できます。

```
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、「新しいボリュームへのバックアップの復元」を参照してください。

ボリュームの更新

NetAppONTAP コマンドラインインターフェイス (CLI) と REST API の他に、Amazon FSx コンソール、AWS CLI、および Amazon FSx API を使用して、FSx for 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、[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) をボリュームで有効にするか、[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 で、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 (または同等のコマンド 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
```

FlexGroup ボリュームの拡大

ONTAP CLI の `volume expand` コマンドを使用して、FlexGroup ボリュームに追加の構成ボリュームを追加できます。これは、FlexGroup ボリュームのバランスが保たれるため、高可用性 (HA) ペアをファイルシステムに追加した後のベストプラクティスです。

FlexGroup ボリュームを拡張する前に、次の点を考慮してください。

- すべての FlexGroup's 構成ボリュームのストレージ容量は同じです。追加の構成要素で FlexGroup ボリュームを拡張すると、各構成要素は既存の構成要素と同じサイズになります。したがって、構成要素を追加する前に、各集計に十分なスペースがあることを確認してください。
- AWS では、FlexGroup ボリュームごとに集計ごとに 8 つの構成ボリュームを維持することをお勧めします。アグリゲートあたり 8 の構成ボリュームは、FlexGroup ボリュームの並列性を最大化し、ワークロードに最適なパフォーマンスを提供します。一般的に、HA ペアを追加する場合にのみ、追加の構成要素を使用して FlexGroup ボリュームを拡張することをお勧めします。これは、アグリゲートごとに 8 の構成要素を維持するために構成要素を追加する必要がある唯一のシナリオです。

- FlexGroup ボリュームが SnapMirror 関係にある場合、ソースボリュームと送信先 FlexGroup ボリュームの両方に同じ数の構成要素が必要です。それ以外の場合、SnapMirror 転送は失敗します。SnapMirror は構成レベルで動作し、個々の構成要素間でデータを転送します。したがって、追加の構成要素ボリュームで FlexGroup ボリュームを拡張する場合は、そのボリュームと SnapMirror 関係があるボリュームを手動で拡張する必要があります。
- 追加の構成要素を使用して FlexGroup ボリュームを拡張すると、既存のスナップショットコピーはすべて「部分」コピーになります。部分的なコピーは復元できませんが、参照したり、個々のファイルを復元したりできます。さらに、これにより Amazon FSx バックアップ、AWS バックアップ、または SnapMirror リレーションシップの増分が失われます。
- 一度追加すると、構成ボリュームを削除することはできません。

FlexGroup ボリューム構成要素の追加

ONTAP CLI を使用して、FlexGroup ボリュームに構成ボリュームを追加できます。

FlexGroup ボリューム構成を追加するには

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、「ONTAP CLI 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. ボリューム拡張 ONTAP CLI コマンドを使用して、追加の構成要素を使用して FlexGroup ボリュームを拡張します。以下の値を置き換えます:

   - FlexGroup ボリュームをホストするストレージ仮想マシン (SVM) の名前の `svm_name` (例: `svm1`)。
   - 展開する FlexGroup ボリュームの名前の `vol_name` (例: `vol1`)。
   - FlexGroup 構成ボリュームを追加するアグリゲートのカンマ区切りリストを持つ `aggregates`。例えば、1 つのアグリゲートの `aggr1` や複数のアグリゲートの `aggr1,aggr2` です。

- 指定された constituent_per_aggregate のそれぞれに追加する追加の構成要素の数を有する aggregates。FlexGroup ボリュームが存在するアグリゲート全体で構成要素の数のバランスがとれるように、十分な構成要素のみを追加する必要があります。

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-
list-multiplier constituents_per_aggregate
```

> **Important**
>
> FlexGroup 構成要素を追加した後は削除できないため、前のコマンドを実行する前に入力を確認してください。

アグリゲート間のボリュームの移動

高可用性 (HA) ペアをファイルシステムに追加する場合は、ボリュームを新しいアグリゲートに移動して、既存のデータのバランスを調整する必要があります。アグリゲート間でボリュームを移動するには、ONTAP CLI で volume move コマンドを使用します。

volume move コマンドを使用する前に、次の点を考慮してください。

- volume move コマンドを使用すると、ファイルシステム上のネットワークリソースとディスクリソースを消費するため、パフォーマンスに影響を与える可能性があります。したがって、アクティビティが少ない時間帯に、ボリュームをアグリゲート間で移動することをお勧めします。または、ボリュームの移動中に、ファイルシステムのネットワークスループット使用率とディスクスループット使用率を 50% 以下に減らすこともできます。
- ファイルシステムのパフォーマンスへの影響を減らすために、一度に 2 つの HA ペアとアグリゲートの間で 1 つのボリュームを移動することをお勧めします。例えば、ファイルシステムに 4 つの HA ペアがある場合は、一度に 2 つのボリュームを移動することをお勧めします (ボリュームの移動が同じ HA ペアとの間で異なる場合を想定)。ONTAP では、各 HA ペアで一度に最大 8 つのボリュームを移動できますが、同時にボリュームを移動すると、クライアント I/O と進行中のボリューム移動の両方のパフォーマンスが低下します。
- 影響を受けるボリュームの SSD 階層に保存されているデータは、物理的に別のファイルサーバー上の異なるディスクセットに移動します。このオペレーションはバックグラウンドで行われ、時間がかかります。転送にかかる時間は、ファイルシステムのスループットキャパシティとファイルシ

ステムのアクティビティ量によって異なります。ただし、ボリューム移動はスロットリングできます。詳細については、「スロットリングボリュームの移動」を参照してください。

- HA ペアが同じ容量プールストレージを共有しているため、キャパシティプールに格納されているデータは物理的に移動されません。代わりに、ONTAP はキャパシティプールの各ブロックを完全に記述するメタデータを移動します (論理的な移動)。ファイルメタデータは常に SSD 階層に格納されることに注意してください。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。

ボリュームの移動フェーズ

ボリューム移動オペレーションには、レプリケーションフェーズとカットオーバーフェーズの 2 つのフェーズがあります。レプリケーションフェーズ中、既存のデータはボリュームの新しいアグリゲートにレプリケートされます。カットオーバーフェーズ中、ONTAP はボリュームの新しいアグリゲートへの最終的な高速転送を試みます。これには、転送フェーズ中に書き込まれたデータの転送や、ボリュームの新しい集計への新しいトラフィックのリダイレクトが含まれます。デフォルトでは、カットオーバーウィンドウは 30 秒で、ボリュームに対するすべての I/O が停止します。ONTAP がカットオーバーウィンドウ中にこれらのステップをすべて実行できない場合、失敗します。デフォルトでは、ONTAP は 3 回連続してカットオーバーを試みます。3 回連続してすべての試行が失敗した場合、ONTAP は成功するまで 1 時間に 1 回再試行します。カットオーバーフェーズが始まる前に I/O トラフィックをボリュームに減らすか一時停止することで、ファイルシステムの負荷を軽減してカットオーバーフェーズを確実に成功させることができます。

ボリューム移動の開始

ボリューム移動を開始するには

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、「ONTAP CLI 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. ボリューム移動開始 ONTAP CLI コマンドを実行します。以下の値を置き換えます:

   - 移動対象のボリュームをホストしている SVM の名前を持つ `vserver_name`。

- ボリューム構成要素の名前を持つ volume_name (例: vol1__0001)。
- ボリュームの移動先アグリゲートの名前を持つ aggregate_name。
- ボリューム移動の合計スループットをスロットリングする -enforce-network-throttling。これはオプションです。

```
::> volume move start -vserver svm_name -volume volume_name --destination-
aggregate 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.
```

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。したがって、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、ボリュームへの I/O トラフィックは、ボリューム移動のカットオーバーフェーズ中に一時的に一時停止されます。

ボリューム移動のモニタリング

ボリューム移動をモニタリングするには

- 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: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

コマンド出力には、移動を完了するまでの推定時間が表示されます。完了すると、completed のステータスが Move phase に表示されます。

バランスの取れた FlexGroup ボリュームの維持

ワークロードが最適に機能するには、FlexGroup ボリュームがすべてのアグリゲートにまたがり、アグリゲートあたりの構成要素ボリューム数が均等である必要があります。アグリゲートごとに 8 つの構成要素を持つことをお勧めします。FlexGroup ボリュームのバランスを再調整する場合は、次のシナリオを考慮してください。

- 既存のアグリゲート間で FlexGroup 構成要素を移動する: FlexGroup's 構成要素ボリュームを別のバランスの取れた FlexGroup のアグリゲートに移動する場合は、元のアグリゲートにあまり利用されない別の構成要素を移動させる必要があります。これにより、FlexGroup のアグリゲートあたりの構成要素数が均等になります。

  HA ペアを追加した後に FlexGroup 構成要素を新しいアグリゲートに移動する: HA ペアを追加した後に FlexGroup's 構成要素ボリュームを新しいアグリゲートに移動する場合は、構成要素を失ったアグリゲートに追加の構成要素を含む FlexGroup を拡張する必要があります。これにより、FlexGroup のアグリゲートあたりの構成要素数が均等になります。詳細については、「the section called “FlexGroup ボリュームの拡大”」を参照してください。

スロットリングボリュームの移動

ファイルシステムのボリューム移動の帯域幅を制限する場合は、オペレーションの最初に -enforce-network-throttling オプションを追加できます。

> **Note**
>
> このオプションを使用すると、ファイルシステムの受信 SnapMirror レプリケーションデータ転送に影響します。ファイルシステムのレプリケーションオプションの設定方法は、設定後に表示できないため、常に把握してください。

ボリューム移動をスロットリングするには

1. スロットリングはグローバルレプリケーションスロットルを使用します。グローバルレプリケーションスロットルを設定するには、ONTAP CLI で次のコマンドを使用します。

```
::> options -option-name replication.throttle.enable on
```

2. レプリケーションで使用できる最大合計帯域幅を指定し、次のオプションを置き換えます。

   - 任意のレプリケーション (SnapMirror およびボリューム移動を含む) に使用する最大希望スループット (キロバイト/秒)を持つ `kbs_throttle`。

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

ボリュームのモニタリング

Amazon FSx コンソール、AWS CLI、Amazon FSx API、SDK を使用して、現在ファイルシステム上にあるボリュームを確認できます。

ファイルシステム上のボリュームをモニタリングするには

- [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。

```
$ aws fsx describe-volumes
{
```

```
    "Volumes": [
        {
            "CreationTime": "2024-03-04T20:17:44+00:00",
            "FileSystemId": "fs-abcdef0123a0bb087",
            "Lifecycle": "CREATED",
            "Name": "SVM8_ext_root",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/",
                "SecurityStyle": "NTFS",
                "SizeInMegabytes": 1024,
                "StorageEfficiencyEnabled": false,
                "StorageVirtualMachineId": "svm-01234567890abcdef",
                "StorageVirtualMachineRoot": true,
                "TieringPolicy": {
                    "Name": "NONE"
                },
                "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
                "OntapVolumeType": "RW",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
                "VolumeStyle": "FLEXVOL",
                "AggregateConfiguration": {
                    "Aggregates": [
                        "aggr1"
                    ]
                },
                "SizeInBytes": 1073741824
            },
            "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
            "VolumeId": "fsvol-abcdef0123456789a",
            "VolumeType": "ONTAP"
        }
    ]
}
```


オフラインボリュームの表示

ソース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 show` ONTAP CLI コマンドを使用して、ボリュームの現在のステータスを決定できます。

```
volume show -vserver svm-name
```

ファイルシステムの ONTAP CLI へのアクセスについては、「NetApp ONTAP CLI の使用」を参照してください。

```
FsxIdabc12345::> volume show -vserver vs1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs1       vol1         aggr1        online     RW          2GB      1.9GB    5%
vs1       vol1_dr      aggr0_dp     online     DP        200GB    160.0GB   20%
vs1       vol2         aggr0        online     RW        150GB    110.3GB   26%
vs1       vol2_dr      aggr0_dp     online     DP        150GB    110.3GB   26%
vs1       vol3         aggr1        online     RW        150GB    120.0GB   20%
vs1       vol3_dr      aggr1_dp     online     DP        150GB    120.0GB   20%
vs1       vol4         aggr1        online     RW        200GB    159.8GB   20%
7 entries were displayed.
```

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

ボリュームの削除

FSx for ONTAP ボリュームは、NetApp ONTAP コマンドラインインターフェイス (CLI) と REST API の他に Amazon FSx コンソール、AWS CLI、Amazon FSx API を使用して削除できます。

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。

> **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。

最終ボリュームバックアップの作成

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。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。

ボリュームバックアップの詳細については、「ボリュームバックアップによるデータの保護」を参照してください。

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. (SnapLock Enterprise ボリュームのみ) [SnapLock Enterprise Retention をバイパス] で、[はい] を選択します。
7. 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。
8. 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。
9. [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 (または同等のコマンド [Delete volume] (ボリュームの削除) API オペレーション) を使用します。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

SnapLock ボリュームの削除

このセクションでは、SnapLock ボリュームを削除する方法について説明します。

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たままアカウントを 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。

必要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。ONTAP CLI を使用して SnapLock Enterprise ボリュームを削除するには、`fsxadmin` ロールが必要です。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。

Amazon FSx コンソール、CLI 、または Amazon FSx API を使用して有効な保持ポリシーを持つ WORM データを含む、SnapLock Enterprise ボリュームを削除するには、`fsx:BypassSnapLockEnterpriseRetention` IAM アクセス許可を持っている必要があります。

> **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。

iSCSI LUN の作成

このプロセスでは、NetApp ONTAP CLI lun create コマンドを使用して、Amazon FSx for NetApp ONTAP ファイルシステムに iSCSI LUN 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の「lun create」を参照してください。

> **Note**
>
> iSCSI プロトコルは、6 つ以上の HA ペアを持つ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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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」の「lun create」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 用 iSCSI のプロビジョニングまたはWindows 用 iSCSI のプロビジョニングを参照してください。

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。パッチ適用が発生すると、ファイルシステムの各ファイルサーバーに一度に 1 つずつパッチが適用され、各ファイルサーバーにパッチを適用するのに通常最大 1 時間かかります。HA ペア内でファイルサーバーにパッチを適用する前に、ファイルシステムは自動的にファイルサーバーの HA パートナーにフェイルオーバーします。これにより、その HA ペアに向けられた I/O のために I/O が短時間 (60 秒未満) 一時停止する可能性があります。その後、ファイルシステムはフェイルバックされ、別の短い (60 秒未満) I/O 一時停止が発生する可能性があります。ファイルシステムの作成時にメンテナンスウィンドウ開始時間を選択します。ウィンドウを選択しない場合、ウィンドウは自動的に割り当てられます。

> **Important**
>
> ファイルシステムに正常にパッチを適用できるように、FSx for ONTAP はパッチ適用プロセス中にオフラインボリュームをオンラインにします。Amazon FSx がオンラインに戻すボリュームには、クライアントはアクセスできません。

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は、少なくとも 14 日ごとに 1 回実行されていれば、必要に応じて何度でも移動できます。パッチがリリースされ、14 日以内にメンテナンスが実行されない場合、FSx for ONTAP は、セキュリティと信頼性を確保するためにファイルシステムのメンテナンスを続行します。

> **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 管理コンソール、AWS CLI、AWS API、またはいずれかの AWS SDK 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。

update-file-system CLI コマンドを使用して週次のメンテナンスウィンドウを変更するには、「ファイルシステムを更新するには (CLI)」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。ファイルシステムのスループット容量はいつでも変更できます。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、第 1 世代の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の更新”」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
- 同時リクエストの処理方法
- スループットキャパシティの更新
- スループット容量の変更のモニタリング

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 “Amazon FSx コンソールでのモニタリングする”」を参照してください。

同時リクエストの処理方法

第 1 世代のファイルシステムについて、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。

第 2 世代のファイルシステムのスループットキャパシティの更新をリクエストする場合は、次の点を考慮してください。

- 第 2 世代のファイルシステムのスループットキャパシティを更新するまで、少なくとも 6 時間待つ必要があります。
- スループットキャパシティのクールダウン期間は、SSD/IOPS スケーリングと共有されます。
- スループットキャパシティスケーリングと SSD/IOPS スケーリングは、それらいずれかの進行中はシミュレート的に実行することもキューに入れることもできません。
- スループットキャパシティスケーリングまたは SSD/IOPS スケーリングが進行中は、高可用性 (HA) ペアを組み合わせて追加することはできません。ただし、HA ペアを追加しても、SSD/IOPS スケーリングとスループットキャパシティスケーリングによるクールダウンは共有されません。詳細については、「高可用性 (HA) ペアの追加」を参照してください。

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。

スループットキャパシティの更新

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。

> **Note**
>
> 第 2 世代のファイルシステムのスループットキャパシティを更新するまで、少なくとも 6 時間待つ必要があります。

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。
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。

- `--file-system-id`更新するファイルシステムの ID への 。
- `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キャパシティは 128 MBps、ターゲットスループットキャパシティは 256 MBps 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。

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、「NetApp Console での NetApp Systems Manager の使用」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。DNS 名は、DescribeStorageVirtualMachines API オペレーションのレスポンスで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。

NetApp アプリケーションを使用した ONTAP リソースの FSx の管理

AWS マネジメントコンソール、AWS CLI、AWS API および SDK に加えて、NetApp 管理ツールおよび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

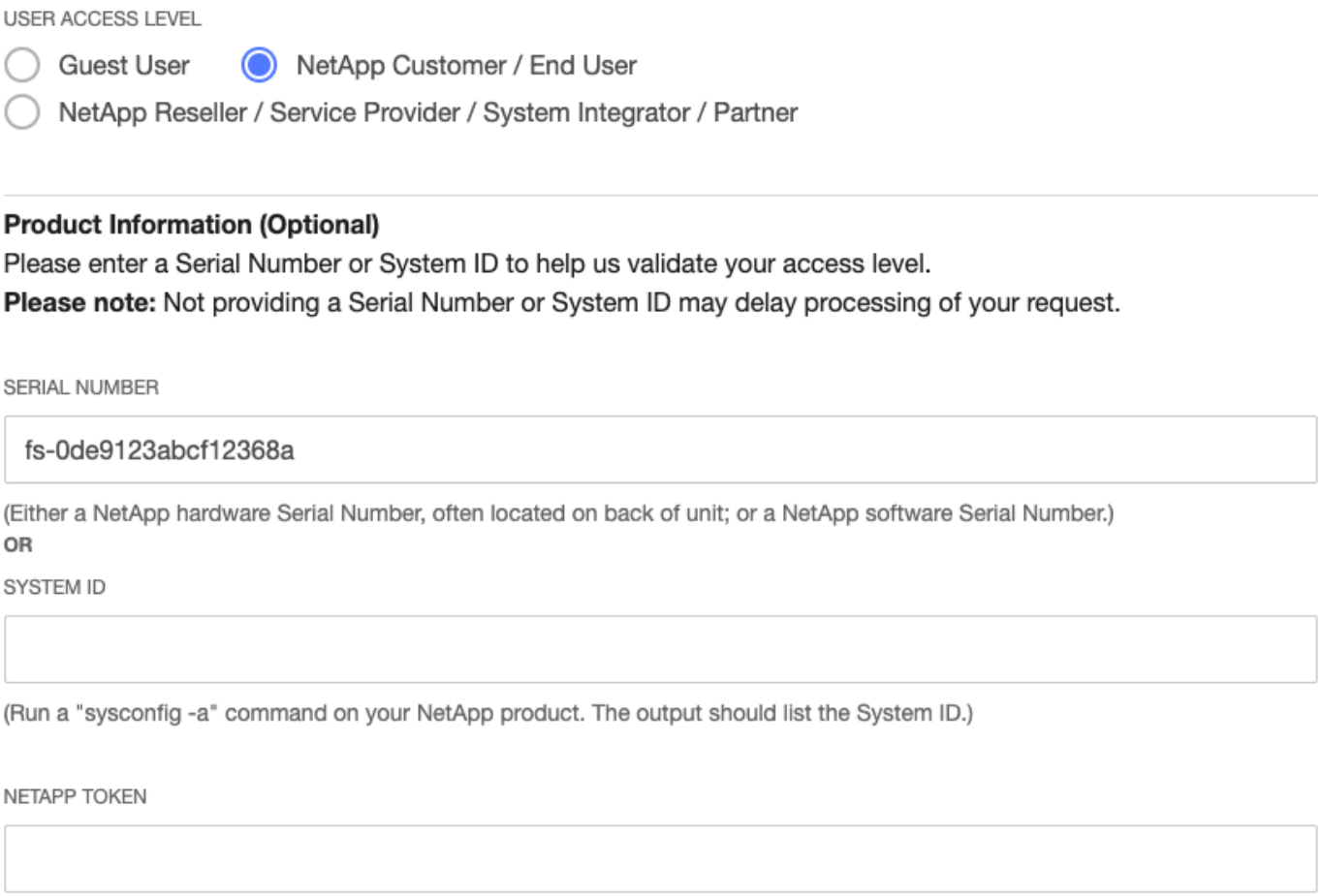
- NetApp アカウントへのサインアップ
- の使用NetApp Console
- NetApp ONTAP CLI の使用
- ONTAP REST API の使用

> **Important**
>
> Amazon FSx は定期的に ONTAP と同期して、一貫性を確保します。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、変更が AWS マネジメントコンソール、AWS CLI、API、および SDK に反映されるまでに最大で数分かかる場合があります。

NetApp アカウントへのサインアップ

NetApp Console、SnapCenter、ONTAP Antivirus Connector などの一部の 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、以下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、新規の NetApp ユーザーアカウントを登録します。
2. フォームに必要事項を入力します。[NetApp のお客様/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、NSS アカウントを 1 営業日以内にお客様レベルアクセスにレベルアップできます。NetApp を初めて利用するお客様は、NSS アカウントがお客様レベルのアクセスレベルにレベルアップされるほか、標準的なビジネスプラクティスに従ってオンボーディングされます。ファイルシステム ID を指定すると、このプロセスを迅速に行えます。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。

の使用NetApp Console

NetApp コンソール (旧 NetApp BlueXP) は、オンプレミスとクラウド環境の、ストレージとデータサービスの管理を簡素化する一体型のコントロールプレーンです。NetApp コンソールは、AWS およびオンプレミスでの ONTAP のデプロイを管理、モニタリング、およびオートメーションするための集中型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 Console documentation」および「Amazon FSx for NetApp ONTAP managemen」ドキュメントを参照ください。

> **Note**
>
> NetApp Console は、複数の高可用性 (HA) ペアを持つ第 2 世代ファイルシステムではサポートされていません。

NetApp Console での NetApp Systems Manager の使用

Amazon FSx for NetApp ONTAP ファイルシステムは、NetApp Console から直接 System Manager を使用して管理できます。NetApp Console では、使い慣れたものと同じ 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で管理できます。また、NetApp コンソールの他の機能にもアクセスできます。詳細については、NetApp ONTAP ドキュメントの「Integrate ONTAP System Manager with NetApp Console」のトピックを参照ください。

> **Note**
>
> NetApp System Manager は、複数の HA ペアを持つ第 2 世代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

NetApp ONTAP CLI を使用して、Amazon FSx for 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 (NetApp ONTAP クラスターに類似) レベルと SVM レベルで管理できます。

ONTAP CLI を使用したファイルシステムの管理

ONTAP CLI コマンドは、NetApp ONTAP クラスターで実行する場合と同様に、FSx for ONTAP ファイルシステムで実行できます。ファイルシステム上のONTAP CLI にアクセスするには、ファイルシステムの管理エンドポイントへの secure shell (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します。カスタム作成フローまたは AWS CLI を使用してファイルシステムを作成するときに、`fsxadmin` パスワードを設定するオプションがあります。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する必要があります。ファイルシステムの `fsxadmin`、パスワードの設定の詳細については、「ファイルシステムの更新」を参照してください。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、Amazon FSx コンソールの FSx for ONTAP ファイルシステムの詳細ページの [管理] タブにあります。

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、まず FSx for ONTAP ファイルシステムと同じ VPC 内の EC2 インスタンスにログインします。EC2 インスタンスにログインしたら、以下の例のように、`fsxadmin` ユーザーとパスワードを使用してファイルシステムの管理エンドポイントの IP アドレスまたは DNS 名に SSH します。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

SSH コマンドとサンプル値:

```
ec2user $ 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:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

サンプル DNS 名を使用した SSH コマンド

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin_password

This is your first recorded login.
FsxId0abcdef123456789::>
```

fsxadmin で使用できる ONTAP CLI コマンドの範囲

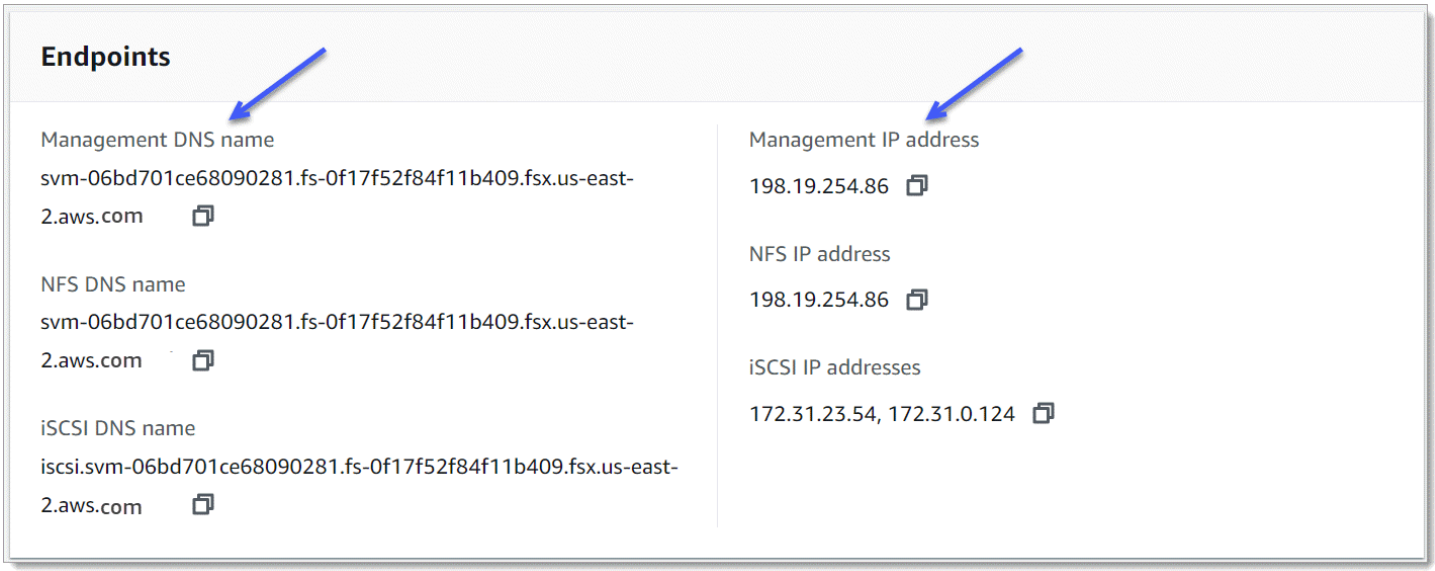
fsxadmin の管理ビューはファイルシステムレベルにあり、ファイルシステム内のすべての SVM とボリュームが含まれます。fsxadmin ロールは、ONTAP クラスター管理者のロールを実行します。Amazon FSx for NetApp ONTAP ファイルシステムはフルマネージドであるため、fsxadmin ロールは使用可能な ONTAP CLI コマンドのサブセットを実行できます。

fsxadmin が実行できるコマンドの一覧を表示するには、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
.
.
.
378 entries were displayed.
```

ONTAP CLI を使用した SVM の管理

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 Secure Shell (SSH) 接続を確立することで、SVM の ONTAP CLI 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、以下の図に示すように、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 コンソールで確認できます。



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 ユーザー名とパスワードのいずれかを使用できます。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 (SVM) 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 コマンドの詳細については、「ONTAP コマンド: マニュアル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 ONTAP REST API を使用して 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 認証局 (CA) を信頼する - 各リージョンの CA の証明書バンドルは、次の URL にあります。
  - パブリック AWS リージョン の場合は、https://fsx-aws-certificates.s3.amazonaws.com/bundle-*aws-region*.pem です
  - AWS GovCloud リージョンの場合は、https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-*aws-region*.pem です
  - AWS 中国リージョンの場合は、https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-*aws-region*.pem です

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 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:
  - TagResourceAPI 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、「ボリュームバックアップによるデータの保護」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。

データの保護

ファイルシステムのデータを自動的にレプリケートして高い耐久性を確保するだけでなく、Amazon FSx には、データをさらに保護するためのオプションもあります:

- Amazon FSx のネイティブボリュームバックアップは、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、複数のAWS のサービスにわたって一元管理された自動バックアップおよび保存戦略を実装します。
- 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、不要なファイルの変更を容易に元に戻すことを可能にします。
- SnapLock を使用してワンライト・マルチリード(WORM) ストレージボリュームを作成し、一度コミットされたファイルの変更や削除を、指定した保存期間にわたって防止します。
- FlexCache ボリュームは、データの大部分が変更されない読み取り負荷の高いワークロードに対して、高ストレージ効率、高コスト効率、高パフォーマンスのデータ・レプリケーションを提供します。
- SnapMirror を使用して、データ保護とディザスタリカバリのための 2 番目のファイルシステムへのスケジュールされた自動ファイルシステムレプリケーションを作成します。

トピック

- ボリュームバックアップによるデータの保護
- スナップショットによるデータの保護
- Autonomous Ransomware Protection によるデータの保護
- SnapLock でのデータの保護
- FlexCache によるデータの複製
- NetApp SnapMirrorを使用したデータの複製

ボリュームバックアップによるデータの保護

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行うことにより、データを保護できます。ボリュームの定期的なバックアップを作成することは、データの保持とコンプライアンスのニーズをサポートするのに役立つベストプラクティスです。ボリュームバックアップは、バックアップが格納されているのと同じ AWS リー

ジョン にアクセスできる既存の FSx for ONTAP ファイルシステムに復元できます。Amazon FSx バックアップを使用すると、ボリュームのバックアップを簡単に作成、表示、復元、削除できます。

Amazon FSx は、読み取り/書き込み (RW) の `OntapVolumeType` で ONTAP ボリュームのバックアップをサポートします。

> **Note**
>
> Amazon FSx では、データ保護 (DP) ボリューム、ロードシェアリングミラー (LSM) ボリューム、またはFlexCacheとSnapMirrorの宛先ボリュームのバックアップをサポートしていません。

トピック

- バックアップの仕組み
- ストレージの要件
- 日次自動バックアップ
- ユーザー主導のバックアップ
- バックアップへのタグのコピー
- Amazon FSx で AWS Backup を使用する
- 新しいボリュームへのバックアップの復元
- バックアップと復元のパフォーマンス
- SnapLock ボリュームのバックアップ
- ユーザー起動のバックアップの作成
- 新しいボリュームへのバックアップの復元
- データのサブセットの復元
- バックアップを復元する際の進捗状況のモニタリング
- バックアップの削除

バックアップの仕組み

すべての Amazon FSx バックアップ (日次自動バックアップとユーザー主導バックアップ) は増分的です。つまり、前回のバックアップが完了した以降のデータの変更のみを格納します。これにより、バックアップの作成に必要な時間と、各バックアップで使用されるストレージの量の両方が最小限に

抑えられます。増分バックアップは、重複データを格納しないことでストレージコストを最適化します。FSx for ONTAP バックアップはボリュームごとに行われ、各バックアップには 1 つの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、高い耐久性を実現するために、複数のアベイラビリティーゾーンに冗長的に格納されます。

Amazon FSx バックアップは、スナップショット (ある時点の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。バックアップが行われるたびに、Amazon FSx はまずボリュームのスナップショットを取得します。バックアップスナップショットはボリュームに格納され、ボリュームのストレージ領域を消費します。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のコストを最適化するために、ONTAP はボリュームのストレージ効率の節約をバックアップに維持します。

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。各 Amazon FSx 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ために必要なすべての情報が含まれており、ボリュームのポイントインタイムスナップショットを効果的に復元します。

AWS アカウント ごとに格納できるバックアップの数と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、「増加可能なクォータ」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。

ストレージの要件

ボリュームとファイルシステムには、バックアップスナップショットを格納するために十分な SSD ストレージ容量が必要です。スナップショットのために追加で消費される容量によってボリュームの SSD ストレージ使用率が 98% を超える場合は、バックアップスナップショットを作成することはできません。この場合、バックアップは失敗します。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して、バックアップが中断されないようにすることができます。

日次自動バックアップ

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に対して日次自動バックアップがデフォルトで有効になります。既存のファイルシステムの日次自動バックアップは、いつでも有効また

は無効にできます。すべてのボリュームの日次自動バックアップは、ファイルシステムの日次バックアップウィンドウ中に行われ、ファイルシステムの作成時に自動的に設定されます。日次バックアップウィンドウはいつでも変更できます。最適なバックアップパフォーマンスを得るには、クライアントとアプリケーションがボリューム上のデータにアクセスしているときに、通常の営業時間外の日次バックアップウィンドウを選択することをお勧めします。

コンソールを使用して、日次自動バックアップの保持期間を、ファイルシステムの作成時またはいつでも 1～90 日の値に設定できます。デフォルトの日次自動バックアップの保持期間は 30 日です。Amazon FSx は、保持期間が終了すると日次自動バックアップを削除します。AWS CLI と API を使用して、保持期間を 0～90 日の値に設定することができます。これを 0 に設定すると、日次自動バックアップはオフになります。

日次自動バックアップ、日次バックアップウィンドウ、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設定です。Amazon FSx コンソール、AWS CLI、または API を使用して、これらの設定を変更できます。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 (日次自動バックアップまたはユーザー主導バックアップ) を作成することはできません。詳細については、「オフラインボリュームの表示」を参照してください。

> **Note**
>
> 日次自動バックアップの最大保持期間は 90 日ですが、ユーザーが作成したユーザー主導のバックアップ (AWS Backup を使用して作成したバックアップを含む) は、ユーザーまたは AWS Backup が削除しない限り、永続的に保持されます。

Amazon FSx コンソール、CLI、および API を使用して、日次自動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、削除しない限り永続的に保持されます。

ユーザー主導のバックアップ

Amazon FSx では、AWS マネジメントコンソール、AWS CLI、および API を使用して、いつでもファイルシステムのボリュームのバックアップを手動で作成できます。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。ユーザー主導のバックアップは、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。

ユーザー主導のバックアップを作成する方法については、「ユーザー起動のバックアップの作成」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 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。ただし、コンソールの使用時にバックアップに名前を付けるなど、ユーザー主導のバックアップの作成時にタグを追加すると、CopyTagsToBackups が有効になっている場合でも、Amazon FSx はボリュームからタグをコピーしません。

Amazon FSx で AWS Backup を使用する

AWS Backup は、Amazon FSx for NetApp ONTAP ボリュームをシンプルかつコスト対効果の高い方法でバックアップします。AWS Backup は、バックアップの作成、復元、削除を簡素化し、レポートと監査を改善するために設計された、統合されたバックアップサービスです。AWS Backup を使用すると、法律、規制、業務に関するコンプライアンスのための、集中型バックアップ戦略を容易に開発できます。さらに、次を実行するための一元的な場所を用意するだけで、AWS ストレージボリューム、データベースとファイルシステムを容易に保護することができます:

- バックアップする AWS リソースの設定と監査。
- バックアップスケジュールのオートメーション。
- 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 は、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したバックアップは、同じレベルのファイルシステムの一貫性とパフォーマンスを備えており、ボリュームに対して取得した他の Amazon FSx のユーザー主導のバックアップと比較すると増分的です。また、Amazon FSx コンソールで取得されるバックアップと同じ復元オプションを備えています。AWS Backup を使用してこれらのバックアップを管理すると、1 時間ごとの頻度で予定されるバックアップを作成する機能などの追加の機能を利用できます。防御レイヤーを追加し、バックアップを バックアップ保管庫に格納することで、不注意や悪意による削除からバックアップを保護できます。

AWS Backup によって作成されたバックアップはユーザー主導のバックアップと見なされ、Amazon FSx のユーザー主導のバックアップのクォータにカウントされます。詳細については、「増加可能なクォータ」を参照してください。AWS Backup で作成したバックアップは、 Amazon FSx コンソール、CLI、および API を使用して確認および復元できます。ただし、AWS Backup で作成したバックアップは、Amazon FSx コンソール、CLI、または API で削除できません。詳細については、AWS Backup デベロッパーガイドの AWS Backup の使用開始 を参照してください。

AWS Backup は、オフラインのボリュームをバックアップできません。

タグを使用して、バックアップ計画で保護する FSx for ONTAP リソースを選択できます。これらのタグは、ファイルシステムレベル全体ではなく、ボリュームレベルで適用する必要があります。詳細は開発者ガイドの「バックアッププランへのリソースの割り当て」AWS Backupをご参照ください。

新しいボリュームへのバックアップの復元

ボリュームバックアップは、バックアップが保存されているのと同じ AWS リージョン にあるファイルシステム上の新しいボリュームに復元できます。バックアップとは別の AWS リージョン にあるファイルシステムにバックアップを復元することはできません。

FSx for ONTAP 第 2 世代のファイルシステムのバックアップを復元する場合、クライアントは復元中にボリュームからデータをマウントして読み取ることができます。クライアントは、Amazon FSx がすべてのメタデータを新しいボリュームにロードし、ボリュームが CREATED のライフサイクルステータスを報告すると、復元するボリュームをマウントしてファイルデータを読み取ることができます。ボリュームのライフサイクルステータスは、Amazon FSx コンソールの [ボリュームの詳細] ページと describe-volumes CLI コマンドのレスポンスで確認できます。

バックアップから復元されている間にボリュームからデータを読み取るときに、データがボリュームにまだダウンロードされていない場合、最初のアクセスには最大数十 ミリ秒の読み込みレイテンシーが発生します。これらの読み取りは SSD 階層にキャッシュされ、後続の読み取りにはミリ秒未満の読み取りレイテンシーが予想されます。

Amazon FSx がボリュームを読み取り専用アクセスに利用できるようにするためにかかる時間は、バックアップに格納されているファイルメタデータの量に比例します。ファイルメタデータは通常、データセットの平均ファイルサイズに応じてバックアップデータの 1～7% を消費します (小さなファイルデータセットは、大きなファイルデータセットよりも多くのメタデータを消費します)。

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します。

> **Note**
>
> Amazon FSx は、ボリュームがバックアップから復元されている間、または第 1 世代のファイルシステムの SnapLock ボリュームに対して、データへの読み取りアクセスをサポートしていません。これらのバックアップを復元すると、復元プロセスが完了した後、ボリュームはデータのマウントとアクセスが可能になり、すべてのメタデータとデータが新しいボリュームにロードされます。

バックアップを復元すると、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。復元中は、復元されるボリュームの階層化ポリシーに従って、データが容量プールストレージに階層化されます。データは最初に SSD 階層に書き込まれるため、ファイルシステムが SSD ストレージ容量を使い果たすと、Amazon FSx は復元プロセスを一時停止します。復元は、プロセスを継続するために十分な SSD 領域が利用可能になるとすぐに自動的に再開されます。復元されたボリュームの階層化ポリシーが `All` の場合、定期的なバックグラウンドプロセスはデータを容量プールに階層化します。復元された階層化ポリシーが `Snapshot Only` または `Auto` である場合、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。

第 2 世代のファイルシステムの新しいボリュームにバックアップを復元するときにワークロードに一貫したミリ秒未満の読み込みレイテンシーが必要な場合は、復元を開始するときにボリュームの階層化ポリシーを `None` に設定し、すべてのデータがボリュームに完全にダウンロードされるまで待ってからアクセスすることをお勧めします。すべてのデータは、アクセスを試みる前に SSD ストレージにロードされるため、データへの一貫した低レイテンシーアクセスが可能になります。

バックアップを新しいボリュームに復元する手順については、「新しいボリュームへのバックアップの復元」を参照してください。

第 2 世代のファイルシステムでは、復元操作全体が完了するまで待つことなく、バックアップからデータのサブセットのみを復元することもできます。バックアップのデータのサブセットのみを復元すると、データの偶発的な削除、変更、破損が発生した場合に、より迅速に操作を再開できます。詳細については、「データのサブセットの復元」を参照してください。

AWS マネジメントコンソール、AWS CLI、および API の第 2 世代のファイルシステムでバックアップを復元するときに、進行状況をモニタリングできます。詳細については、「バックアップを復元する際の進捗状況のモニタリング」を参照してください。

Note

- ボリュームスナップショットの作成とスナップショットベースの操作の実行はできません。スナップショットベースの操作には、クローン作成、SnapMirror レプリケーション、バックアップからの復元中のボリュームのバックアップ作成などが含まれます。
- 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。

バックアップと復元のパフォーマンス

バックアップおよび復元操作の速度には、さまざまな要因が影響する可能性があります。バックアップ操作と復元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 操作よりも優先度が低くなります。クライアント IO 操作には、NFS、CIFS、iSCSI データおよびメタデータの読み取りと書き込みが含まれます。すべてのバックグラウンド操作では、ファイルシステムのスループットキャパシティの未使用部分のみが利用されます。バックアップのサイズとファイルシステムの未使用スループットキャパシティの量によっては、完了までに数分から数時間かかる場合があります。

バックアップおよび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層やデータセットプロファイルなどがあります。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。小さなファイルが大部分を占めるデータセットは、大きなファイルが大部分を占める同様のサイズのデータセットに比べて、バックアップと復元のパフォーマンスが下がります。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。

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ることで、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。

詳細については、「SnapLock の仕組み」を参照してください。

ユーザー起動のバックアップの作成

次の手順では、ボリュームのユーザー主導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、ボリュームのバックアップを作成することはできません。詳細については、「オフラインボリュームの表示」を参照してください。

ユーザー主導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、ボリュームをバックアップする ONTAP 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. 開いた [Create backup] (バックアップの作成) ダイアログボックスで、バックアップの名前を入力します。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、[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が表示されます。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。

新しいボリュームへのバックアップの復元

次の手順では、AWS マネジメントコンソール と AWS CLI を使用して FSx for ONTAP バックアップを新しいボリュームに復元する方法について説明します。ボリュームを第 2 世代のファイルシステムに復元する場合、AWS マネジメントコンソール、AWS CLI、および API を使用して進行状況をモニタリングできます。

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 (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. 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。
6. 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。
7. [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。
8. [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。
9. ボリュームの種類では、読み取り/書き込み (RW) を選択して読み取り可能および書き込み可能なボリュームを作成するか、データ保護 (DP) を選択して読み取り専用のボリュームを作成し、NetApp SnapMirrorまたはSnapVaultリレーションシップの宛先として使用できます。詳細については、「ボリュームの種類」を参照してください。

10. [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。
11. [ストレージ効率] で、[有効] を選択し、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、「ストレージ効率」を参照してください。
12. [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。
13. [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 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。
14. [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。
15. [詳細設定] セクションの [SnapLock 設定] では、デフォルトの [無効] 設定のままにするか、[有効] を選択して SnapLock ボリュームを設定できます。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 コンプライアンスについて」および「SnapLock エンタープライズ について」を参照してください。SnapLock の詳細については、「SnapLock でのデータの保護」を参照してください。
16. [確認] を選択してボリュームを作成します。
17. バックアップを第 2 世代のファイルシステムに復元する場合は、[ボリューム] ページの [更新] タブでバックアップ復元の進行状況をモニタリングできます。詳細については、「バックアップを復元する際の進捗状況のモニタリング」を参照してください。

新しいボリュームへバックアップを復元するには (CLI)

Create-volume-from-backup CLI コマンドまたは同等の CreateVolumeFromBackup API コマンドを使用すると、ボリュームバックアップを新しいボリュームに復元できます。

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

  バックアップを第 2 世代のファイルシステムに復元するための復元リクエストが成功した場合のシステムレスポンスは、次のように表示されます。レスポンスには、リクエストのステータスと進行状況情報を提供する "AdministrativeActions" オブジェクトが含まれます。

  ```
  {
        "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",
    --->    "AdministrativeActions": [
                {
                    "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
                    "RequestTime": 1685729972.069,
                    "Status": "PENDING"
                }
            ]                   <----
        }
    }
  ```
  ```

第 1 世代のファイルシステムにバックアップを復元するリクエストが成功した場合のシステムレスポンスは次のようになります。

```
{
      "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",
      }
  }
```

ボリュームを第 2 世代のファイルシステムに復元する場合、AWS マネジメントコンソール、AWS CLI、および API を使用して進行状況をモニタリングできます。

データのサブセットの復元

データのサブセットは、バックアップデータセット全体が完全に復元されるまで待つことなく、第 2 世代のファイルシステムの新しいボリュームに復元している間にバックアップから復元できます。

次の手順では、バックアップを復元するときにデータのサブセットを復元する必要があり、復元全体が完了するまで待つことができない場合に実行する手順を示します。

バックアップの復元中にデータのサブセットを復元するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [バックアップ] ページで、復元するデータのバージョンを含むバックアップを見つけます。
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] で、ニーズに合わせてボリュームを設定します。
6. [確認] を選択してボリュームを作成します。
7. バックアップの復元の進行状況をモニタリングします。
8. CREATED のライフサイクルステータスが報告されると、復元されるボリュームをマウントします。
9. コピーする必要があるボリューム上のデータのサブセットを見つけます。
10. アプリケーションが使用する既存のボリュームにデータをコピーします。
11. バックアップから必要なデータがターゲットロケーションにコピーされたら、復元されるボリュームがファイルシステムリソースの使用率の最適化を完了する前に削除できます。

バックアップを復元する際の進捗状況のモニタリング

AWS マネジメントコンソール、AWS CLI、および API の第 2 世代のファイルシステムでボリュームのバックアップを復元する際の進行状況をモニタリングできます。すべての Amazon FSx 管理アクションと同様に、操作が完了してから 30 日間、コンソール、CLI、および API でバックアップ復元ステータスを使用できます。

バックアップの復元を行う際の進行状況をモニタリングするには (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. 左側のナビゲーションメニューで [ボリューム] を選択します。
2. バックアップの復元先となるボリュームを選択します。
3. [更新] タブを選択します。
4. [バックアップ復元] と [更新タイプ] は、次の情報を示します。

- [保留中] は、ファイルメタデータをボリュームにダウンロード中であることを示します。ボリュームの [ライフサイクルステータス] は [作成中] です。
- [IN_PROGRESS] は、ボリュームが使用可能であり、クライアントがデータへの読み取り専用アクセスでボリュームをマウントできることを示します。[進行 %] は、ボリュームにダウンロードされたデータの割合を示します。
- [完了済み] は、すべてのデータがボリュームにダウンロードされ、バックアップ復元が完了したことを示します。クライアントは読み取り/書き込みアクセスできるようになりました。RW ボリュームの場合、ボリュームのタイプはこの時点で DP から RW に変わります。

バックアップを復元する際の進行状況をモニタリングするには (CLI)

- 第 2 世代の FSx for ONTAP ファイルシステムの新しいボリュームにバックアップを復元する場合、describe-volumes CLI コマンドを使用して復元の進行状況をモニタリングできます。

  バックアップを第 2 世代のファイルシステムに復元する場合、レスポンスには AdministrativeActions オブジェクトが含まれ、データのダウンロードプロセスに関するステータス情報が提供されます。-

```
$ aws fsx describe-volumes
{
    “Volumes”: [
        {
            “CreationTime”: 1691686114.674,
            “FileSystemId”: fs-029ff92192bd4d375,
            “LifeCycle”: “CREATING”,
            “Name”: vol1,
            “OntapConfiguration”: {
                   “FlexCacheEndpointType”: “NONE”,
                   “JunctionPath”: “/vol1”,
                   “SizeInMegabytes”: 100000,
                   “StorageEfficiencyEnabled”: true,
                   “StorageVirtualMachineId”: “svm-0ed1d714019426ca9”,
                   “StorageVirtualMachineRoot”: false,
                   “TieringPolicy”: {
                    “Name”: “ALL”
                   },
                   “OntapVolumeType”: “DP”,
                   “SnapshotPolicy”: “default”,
                   “CopyTagsToBackups”: false,
```

```
                    },
                    “ResourceARN”: “arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa”,
                    “VolumeId”: “fsvol-094c015af930790fa”,
                    “VolumeType”: “ONTAP”,
                    “AdministrativeActions”: [
                           {
                            “AdministrativeActionType”: “DOWNLOAD_DATA_FROM_BACKUP”,
                            “RequestTime”: 1685729972.069,
                            “Status”: “PENDING”
                           }
                    ]
    }
```

Amazon FSx が復元されたボリュームにすべてのファイルメタデータをロードすると、これらのフィールドには次の値があります。

- "LifeCycle": "CREATED" – ボリュームをマウントする準備ができていることを示します。
- "OntapVolumeType": "DP" – ファイルデータのダウンロード中にボリュームが読み取り専用であることを示します。
- "ProgressPercent – ボリュームにロードされるファイルデータの割合を示します。
- "Status": "IN_PROGRESS" – ファイルデータをボリュームにダウンロード中です。

復元プロセスのこの段階では、復元するバックアップ内のすべてのデータへの読み取り専用アクセスでボリュームをマウントできます。

Amazon FSx が新しいボリュームへのすべてのファイルデータのダウンロードを完了すると、これが RW ボリュームの場合、クライアントは完全な読み取り/書き込みアクセス権を持ちます。インジケータには次の値があります。

- "LifeCycle": "CREATED" – 変更なし
- "OntapVolumeType": "RW" – クライアントに完全な読み取り/書き込みアクセスがあることを示します。
- "Status": "COMPLETED" – 復元が完了したことを示します。

復元プロセスが失敗した場合、FAILED の値は AdminstrativeAction > Status になります。FailureDetails オブジェクトにエラーメッセージが表示されます。詳細については、Amazon FSx リファレンスの「AdministrativeActionFailureDetails」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、Amazon FSx API、または AWS Command Line Interface (AWS CLI) を使用して、ボリュームの日次自動バックアップとユーザー主導のバックアップの両方を削除できます。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。ソースボリュームがオフラインの場合、バックアップを削除することはできません。

ボリュームは、すべての FSx for ONTAP ファイルシステムのバックアップから復元中に削除できます。復元中にボリュームを削除すると、進行中の復元オペレーションが効果的にキャンセルされます。

> **Note**
>
> Amazon FSx は、ONTAP ボリュームの他のすべての AVAILABLE バックアップが削除されない場合のボリュームの最新のバックアップの削除をサポートしていません。

AWS Backup を使用して作成されたバックアップを削除するには、AWS Backup デベロッパーガイドの「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 バックアップの削除] ダイアログボックスで、表示されたバックアップの ID が削除したいバックアップのもの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. [Delete backups] (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)

- ONTAP ボリュームのバックアップを削除するには、次の例に示すように、delete-backup CLI コマンドまたは同等の DeleteBackup コマンド API アクションを使用します。

```
$ 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、リクエストが成功したことを示す DELETED の値を持つライフサイクルステータスが含まれます。

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

スナップショットによるデータの保護

snapshot (スナップショット) は、ある時点での 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し、変更の取り消し、削除したコンテンツの復元、ファイルバージョンの比較ができます。

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含まれません。スナップショットは、default 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。ボリュームごとに最大 1,023 のスナップショットをいつでも保存することができます。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

- スナップショットからのファイルの復元
- 共通スナップショットの表示
- ボリュームのスナップショットリザーブの更新
- 自動スナップショットの無効化
- スナップショットの削除
- スナップショットの削除
- スナップショットリザーブ

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。`timezone -timezone` *`time_zone`* ONTAP CLI コマンドを使用して、FSx for ONTAP ファイルシステムのタイムゾーンを設定できます。ONTAPCLI へのアクセスの詳細はNetApp ONTAP CLI の使用をご参照ください。

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ご参照ください。Amazon FSx コンソール、、または Amazon FSx API でボリュームを作成 AWS CLI または更新するときに、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。

スナップショットからのファイルの復元

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、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。

Linux および macOS クライアントを使用する場合、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 クライアントを使用する場合、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。

共通スナップショットの表示

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ます。この手順では、ボリュームの共通スナップショットを識別する方法について説明します。

ボリュームの共通スナップショットを表示するには

- ボリュームの共通スナップショットであるスナップショットを確認するには、volume snapshot show ONTAP CLI コマンドを使用します。

```
volume snapshot show -volume volume-name
```

出力では、次の例に示すように、共通スナップショットの名前の形式は backup-*id* です。*id* は 17 桁の英数字文字列です。

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                                 ---Blocks---
Vserver Volume    Snapshot                    Size     Total% Used%
-------- -------- --------------------------- -------- ------ -----
dest-svm test_vol
                  snap1                        144KB    0%     3%
                  snap2                        832KB    0%    16%
         --->     backup-abcdef0123456789a    4.87MB    0%    53% <---
                  weekly.2024-05-26_0015      5.02MB    0%    54%
                  weekly.2024-06-02_0015      2.22MB    0%    34%
                  daily.2024-06-04_0010        284KB    0%     6%
                  daily.2024-06-05_0010       4.29MB    0%    50%
                  hourly.2024-06-05_0705       168KB    0%     4%
8 entries were displayed.
```

> **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。ボリュームの共通スナップショットを削除すると、次のバックアップは増分バックアップではなく、ボリュームの完全なバックアップになります。

ボリュームのスナップショットリザーブの更新

次の手順で説明しているように、NetApp ONTAP CLI または API を使用してボリュームのスナップショットリザーブの量を変更できます。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 CII コマンドを使用して、スナップショットコピーリザーブに使用されるディスク容量の割合を変更します。以下のプレースホルダをユーザー自身の値に置き換えます。

   - *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。
   - *percent* — スナップショットコピー用に予約するディスク領域の割合。

   ```
   ::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-
   space percent
   ```

   次の例では、vol1 のスナップショットリザーブをボリュームのストレージ容量の 25% に変更します。

   ```
   ::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
   ```

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に関するデフォルトのスナップショットポリシーで有効にされます。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 AWS マネジメントコンソール、 AWS CLI API、および ONTAP CLI noneを使用して無効にできます。

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. [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、 SnapshotPolicyを 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. none ポリシーを表示するには、volume snapshot policy show ONTAP CLI コマンドを使用します。

```
::> 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 none に設定し、自動スナップショットを無効にします。以下のプレースホルダをユーザー自身の値に置き換えます。

   - *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、ワークロードでデータが急速に書き込まれる場合、古いデータからのスナップショットは、ボリュームのストレージ容量のかなりの部分を占める可能性があります。

例えば、volume show-space ONTAP CLI コマンド出力は 140 KB の User Data を表示します。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。スナップショットは増分であるため、削除時にスナップショットのサイズと等しいストレージの量を再利用することはありません。スナップショットを削除することで再利用できるストレージの量を確認するには、volume snapshot compute-reclaimable-vserver ONTAP CLIコマンドを使用し、*svm_name*、*vol_name*、および *snapshot_name* を置き換えるデータを指定します。

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

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て、スナップショットを削除できます。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削除

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。詳細については、「共通スナップショットの表示」を参照してください。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

スナップショット自動削除ポリシーの作成

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 の 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の自動削除変更」コマンドを参照してください。

スナップショットリザーブ

スナップショットコピーリザーブは、スナップショットコピーを格納するためのボリュームのストレージ容量の特定のパーセントを設定し、デフォルト値は 5% です。スナップショットコピーリザーブには、ボリュームバックアップなど、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スペースを超える場合は、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リザーブの 100% 以上を消費すると、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流出と呼ばれます。スナップショットがアクティブなファイルシステム領域を引き続き占有している場合、ファイルシステムは満杯になるリスクがあります。スナップショットの流出によって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内のスナップショットに十分なディスク領域が利用可能な場合、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領域が解放されます。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内の領域のみを使用します。

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) を超えるディスク領域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領域を確保するために、スナップショットに十分なディスク領域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空き領域は作成されません。これは、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です。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リザーブ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リザーブの更新」を参照してください。

Autonomous Ransomware Protection によるデータの保護

Autonomous Ransomware Protection (ARP) は、Windows または Linux クライアントが侵害された場合に、ランサムウェアやマルウェア攻撃からデータをモニタリングして保護する NetApp ONTAP AI 主導の機能です。機械学習技術により、ARP は FSx for ONTAP ファイルシステムについて学習

し、異常なアクティビティを事前に検出します。ARP は、Amazon FSx for NetApp ONTAP が利用可能なすべての AWS リージョン で、すべての新規および既存の FSx for ONTAP ファイルシステムで使用できます。

ARP の仕組み

ONTAP CLI または REST API を使用して、ARP をボリュームごとに有効にすることも、SVM 内のすべての新しいボリュームでデフォルトで有効にすることもできます。ARP の有効化の詳細については「Autonomous Ransomware Protection の有効化」をご覧ください。

ARP の AI は包括的なデータセットでトレーニングされるため、ARP を FlexVol ボリュームで実行するための学習期間は不要であるため、すぐにアクティブモードで開始されます。ARP AI は、自動更新機能も備えており、最新の脅威に対して常に保護と耐障害性を維持します。アクティブモードでは、ARP はボリュームの受信データとアクティビティをモニタリングして、潜在的なランサムウェアやマルウェア攻撃を特定します。詳細については、「ARP が検索する対象」を参照してください。ARP が異常なアクティビティを検出した場合、潜在的な攻撃時点にできるだけ近い状態でデータを復元できるよう、自動的にONTAP スナップショットが作成されます。スナップショットには `Anti_ransomware_backup` というプレフィックスが付いているため、簡単に識別できます。攻撃の確率が中程度であると判断された場合、ONTAP はイベント管理システム (EMS) メッセージを生成して確認できるようにします。詳細については、「ARP による疑わしい攻撃への対応方法」および「Autonomous Ransomware Protection の EMS アラートの理解」を参照してください。

ARP のパフォーマンスオーバーヘッドは、ほとんどのワークロードで最小限です。ボリュームに読み込み負荷の高いワークロードがある場合、NetApp はファイルシステムあたり 150 個以下のボリュームを保護することを推奨しています。この数を超えると、そのワークロードの IOPS が最大 4% 低下する可能性があります。ボリュームに書き込み負荷の高いワークロードがある場合、NetApp はファイルシステムあたり 60 個以下のボリュームを保護することを推奨しています。そうでない場合は、そのワークロードの IOPS が最大 10% 低下する可能性があります。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。

FSx for ONTAP ファイルシステムで ARP を有効にする場合、追加料金はかかりません。

ARP が検索する対象

ARP は、Windows または Linux クライアントが侵害されている兆候を探します。特に、ARP はボリュームの以下のタイプのアクティビティを探します:

- エントロピーの変化とは、ファイル内のデータのランダム性の差異を意味します。

- ファイル拡張子タイプの変更とは、新しい拡張子が通常使用される拡張子タイプと一致しないことを意味します。デフォルトは、ボリュームで以前に確認されていないファイル拡張子を持つ 20 ファイルです。
- ファイル IOPS の変更。これは、暗号化されたデータを伴う異常なボリュームアクティビティの急増を意味します。

必要に応じて、ボリュームのランサムウェア検出パラメータを変更できます。たとえば、あなたのボリュームが多くのタイプのファイル拡張子をホストしている場合です。詳細については、NetApp ドキュメントセンターの「ONTAP Autonomous Ransomware Protection の攻撃検知パラメータの管理」を参照してください。

> **Note**
>
> ARP は、認証情報を持つ不正な管理者が FSx for ONTAP ファイルシステムにアクセスするのを防ぐものではありません。AWS では、AWS Backup、ONTAP スナップショット、SnapLock などのレイヤードセキュリティアプローチを推奨しています。

ARP による疑わしい攻撃への対応方法

ARP が攻撃を検出すると、復旧ポイントとして使用できるスナップショットが生成されます。スナップショットはロックされているため、通常の手段では削除できません。攻撃の影響度に応じて、影響を受けたボリューム、攻撃の確率、および攻撃のタイムラインを示す EMS アラートも生成されます。新しいスナップショットの作成またはボリュームの新しいファイル拡張子の監視に関するアラートを受信したい場合は、これらのアラートを送信するように ARP 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「Configure ARP alerts」を参照してください。

レポートを生成して、疑わしい攻撃に関する詳細情報を表示できます。レポートを確認すると、ONTAP アラートが誤検知によるものか、疑わしい攻撃によるものかを判断できます。アラートに疑わしい攻撃としてラベルを付ける場合は、攻撃の範囲を決定し、ARP が作成したスナップショットからデータを復元する必要があります。攻撃に誤検出のラベルを付けると、ARP が作成したスナップショットは自動的に削除されます。詳細については、「Autonomous Ransomware Protection アラートへの対応」を参照してください。

ファイルシステムの EMS メッセージとボリュームのステータスを ONTAP CLI および REST API でモニタリングすることをお勧めします。ARP の EMS メッセージの詳細については、「Autonomous Ransomware Protection の EMS アラートの理解」を参照してください。

トピック

- Autonomous Ransomware Protection の有効化
- Autonomous Ransomware Protection アラートへの対応
- Autonomous Ransomware Protection の EMS アラートの理解

Autonomous Ransomware Protection の有効化

以下の手順では、ONTAP CLI を使用して Autonomous Ransomware Protection (ARP) アクティブモードを有効にする方法と、ARP が有効になっていることを確認する方法について説明します。ARP の詳細については、「ARP の仕組み」を参照してください。

アクティブモードで ARP を有効にする

ONTAP CLI を使用して既存のボリュームでアクティブモードで ARP を有効にするには

- 以下のコマンドを実行してください。*vol_name* and *svm_name* を実際の情報に置き換えます。

  ```
  security anti-ransomware volume enable -volume vol_name -vserver svm_name
  ```

  このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume enable」を参照してください。

SVM レベルでの ARP のデフォルトでの有効化

ONTAP CLI を使用して既存の SVM で ARP をデフォルトで有効にするには

- 以下のコマンドを実行してください。*svm_name* を自分の情報に置き換えます。

  ```
  vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
  ```

  このコマンドの詳細については、NetApp ドキュメントセンターの「vserver modify」を参照してください。

ARP のステータスの確認

ONTAPCLI を使用して ARP のステータスを有効化します

- 以下のコマンドを実行してください。

  ```
  security anti-ransomware volume show
  ```

  このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume show」を参照してください。

負荷の高いワークロードイベントを予測する場合は、ARP を一時的に停止 (再開) できます。詳細については、NetApp ドキュメントセンターの ONTAP Autonomous Ransomware Protection を一時停止してワークロードイベントを分析から除外するを参照してください。

Autonomous Ransomware Protection アラートへの対応

以下の手順では、ONTAP CLI を使用して Autonomous Ransomware Protection (ARP) アラートを表示し、攻撃レポートを生成し、レポートに対してアクションを実行する方法について説明します。ARP が攻撃を検出して応答する方法の詳細については、「ARP が検索する対象」および「ARP による疑わしい攻撃への対応方法」を参照してください。

ARP ラートの表示

ONTAP CLI を使用してボリュームの ARP アラートを表示するには

- 以下のコマンドを実行してください。*svm_name* and *vol_name* を実際の情報に置き換えます。

  ```
  security anti-ransomware volume show -vserver svm_name -volume vol_name
  ```

  コマンドが実行されると、以下の例のような出力が表示されます:

  ```
  Vserver Name: fsx
  Volume Name: vol1
  State: enabled
  Attack Probability: moderate
  Attack Timeline: 9/14/2021 01:03:23
  Number of Attacks: 1
  ```

このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume show」を参照してください。

ARP レポートの生成

ONTAP CLI を使用して ARP レポートを生成するには

- 以下のコマンドを実行してください。*vol_name* と */file_location/* を実際の情報に置き換えます。レポートを生成したら、クライアントシステムで表示できます。

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-
path /file_location/
```

このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume attack generate-report」を参照してください。

ARP レポートに対するアクションの実行

ARP レポートの誤検知攻撃に対してONTAP CLI で対応する方法

- 以下のコマンドを実行してください。*svm_name*、*vol_name*、および *[extension identifiers]* を独自の情報に置き換えます。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume attack clear-suspect」を参照してください。

> **Note**
>
> アラートを誤検出としてマークすると、ランサムウェアプロファイルが更新されます。その後、その特定のシナリオに関するアラートは再度送信されません。

ARP レポートの潜在的な攻撃に対してONTAP CLI で対応します

- 以下のコマンドを実行してください。*svm_name*、*vol_name*、および *[extension identifiers]* を独自の情報に置き換えます。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

このコマンドの詳細については、NetApp ドキュメントセンターの「security anti-ransomware volume attack clear-suspect」を参照してください。

Autonomous Ransomware Protection の EMS アラートの理解

NetApp ONTAP's イベント管理システム (EMS) を使用して、ARP に関連する潜在的な攻撃を含むイベントをモニタリングできます。ARP と攻撃の検出方法の詳細については、ARP の仕組みおよびARP が検索する対象を参照してください。

以下の表に、ARP に関連するすべてのアラートを示します。EMS の詳細については、「FSx for ONTAP EMS イベントのモニタリング」を参照してください。

EMS メッセージ名	EMS メッセージ説明
arw.analytics.ext.report	このメッセージは、ランサムウェア対策分析がボリュームに関する 疑わしいファイル拡張子レポートを生成または更新したときに発生します。
arw.analytics.high.entropy	このメッセージは、エントロピーの高いデータログメッセージの数 (ランサムウェアの検出と分析に関連する) がボリュームの事前定義されたしきい値を超えた場合に発生します。
arw.analytics.probability	このメッセージは、ボリュームでランサムウェア対策攻撃の確率が low から high に変更された場合に発生します。

EMS メッセージ名	EMS メッセージ説明
arw.analytics.report	このメッセージは、ボリュームのランサムウェア対策分析レポートが生成または更新されたときに発生します。
arw.analytics.suspects	このメッセージは、ランサムウェア対策分析によって生成された容疑者のリストが、さらなる調査が必要な時点まで増加した場合に発生します。
arw.new.file.extn.seen	このメッセージは、ランサムウェア対策が有効なボリュームで新しいファイル拡張子が観察された場合に発生します。その機能は、観測された拡張についてユーザーにすみやかに通知することを目的としており、これによりタイムリーな調査が可能になります。
arw.snapshot.created	このメッセージは、ランサムウェア対策が有効なボリュームに新しい ARP スナップショットが作成されたときに発生します。さらに、スナップショットが作成された理由に関する情報も提供します。
arw.volume.state	このメッセージは、ボリュームのランサムウェア対策の状態が変更されたときに発生します。
arw.vserver.state	このメッセージは、SVM のランサムウェア対策の状態が変更されたときに発生します。

SnapLock でのデータの保護

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、SnapLock を使用した保持機能を有する Compliance モードと Enterprise モードをサポートしています。詳細については、「SnapLock コンプライアンスについて」および「SnapLock エンタープライズ について」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 の仕組み
- SnapLock コンプライアンスについて
- SnapLock エンタープライズ について
- SnapLock 保存期間について理解する
- ファイルを WORM 状態にコミットする

SnapLock の仕組み

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、両方のモード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 コンプライアンスについて	SnapLock エンタープライズについて
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	あり
イベントベースの保持 (EBR)[1]	はい	あり
リーガルホールド[1]	はい	なし
特権付き削除の使用	なし	あり
ボリューム付加モード	あり	あり
SnapLock 監査ログボリューム	あり	あり

Note

[1] EBR および法的保持操作は、ONTAPCLI および REST API でサポートされています。

> **Note**
>
> FSx for ONTAP は、SnapLock タイプに関係なく、すべての SnapLock ボリュームの容量プールへのデータの階層化をサポートしています。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。

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てください。*`SVM_name`* と *`SnapLockAdmin`* を、自分の情報に置き換えます。

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

詳細については、「ONTAP ロールとユーザー」を参照してください。

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ログ記録されます。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/ にログ記録されます。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。

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。Amazon FSx コンソールの [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。

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 および SSD の容量削減オペレーション

SnapLock ボリュームを作成する前に、SSD の減少に関する以下の点を考慮してください:

- Amazon FSx は、SnapLockボリュームを含むファイルシステムの SSD 容量削減リクエストを拒否します。

- SSD 容量削減オペレーション中にSnapLockボリュームを作成することはできません。

これらの制限が存在するのは、ONTAPによってSnapLock監査ログボリュームに 6 か月の最小保有期間が適用されるためです。これにより、SSD 減少操作の一環としてSnapLockボリュームが移動された場合、その期間中にファイルシステムが削除されることはありません。

SnapLock ボリュームのあるファイルシステムで SSD 容量を減らす必要がある場合は、SSD 容量が小さい新しいファイルシステムにデータを移行する必要があります。制限事項や考慮事項など、SSD 容量減少操作の詳細については、ファイルシステム SSD ストレージと IOPS の更新をご参照ください。

SnapLock コンプライアンスについて

このセクションでは、SnapLockEnterprise リテンションモードの使用ケースと考慮事項について説明します。

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 SnapLock Compliance は、Cohasset Associates により、これらの指令および規制について評価されました。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ご参照ください。
- 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。

SnapLockEnterprise リテンションモードについて考慮すべき重要な項目を次に示します。

- 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 Compliance モードであるなど)。

- 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 エンタープライズ について

このセクションでは、SnapLockEnterprise リテンションモードの使用ケースと考慮事項について説明します。

次の使用ケースでは、SnapLockEnterprise リテンション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。

SnapLockEnterprise リテンションモードについて考慮すべき重要な項目を次に示します。

- 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。

特権付き削除の使用

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。Amazon FSx コンソールの [特権削除] で、[有効] を選択します。

> **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 コンソールの [特権削除] で、[完全に無効] を選択します。

SnapLockエンタープライズモードのバイパス

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 保存期間について理解する

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
[秒]	0 ~ 65,535	
分	0 ~ 65,535	
時間	0 ~ 24	
日間	0 ~ 365	
月	0〜12	
年間	1〜100	
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。

タイプ	値	メモ
未指定 [1]	-	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。

> **Note**
>
> [1] 保存期間を指定せずにファイルを WORM に移行すると、SnapLockボリュームに構成されている最小保存期間がファイルに与えられます。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。Amazon FSx コンソールの [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。

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
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。Amazon FSx コンソールの [自動コミット] で、[有効] を選択します。次に、[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。

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。Amazon FSx コンソールの [ボリューム追加モード] で、[有効] を選択します。

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 ボリュームでは 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。

ONTAPCLI で EBR ポリシーを作成するには

ONTAPCLI で EBR ポリシーを作成するには

- 以下のコマンドを実行してください。*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"
```

ONTAPCLI で EBR ポリシーを適用するには

ONTAPCLI で EBR ポリシーを適用するには

- 以下のコマンドを実行してください。*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 /
```

ONTAPCLI で EBR ポリシーを変更するには

ONTAPCLI で EBR ポリシーを変更するには

- 以下のコマンドを実行してください。*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"
```

ONTAPCLI で EBR ポリシーを削除するには

ONTAPCLI で EBR ポリシーを削除するには

- 以下のコマンドを実行してください。*p1* を自分の情報に置き換えます。

```
vs1::> snaplock event-retention policy delete -name p1
```

NetAppドキュメントセンターの関連コマンド:

- 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。

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のファイルに対する法的証拠保全を開始する

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のファイルの法的証拠保全を開始するには

- 以下のコマンドを実行してください。*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
```

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のすべてのファイルに対して法的証拠保全を開始するには

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のすべてのファイルに対して法的証拠保全を開始するには

- 以下のコマンドを実行してください。*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 /
```

SnapLockCLI を使用してONTAPコンプライアンス· ボリューム内のファイルの法的保持を終了するには

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のファイルの法的証拠保全を終了するには

- 以下のコマンドを実行してください。*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
```

> **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。

SnapLockCLI を使用してONTAPコンプライアンスボリューム内のすべてのファイルに対する法的保持を終了するには

SnapLock CLI を使用してONTAPコンプライアンスボリューム内のすべてのファイルの法的証拠保全を終了するには

- 以下のコマンドを実行してください。*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ドキュメントセンターの関連コマンド:

- snaplock legal-hold abort
- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

FlexCache によるデータの複製

FlexCache は、データセットをクライアントに近づけ、アクセスパフォーマンスを向上させ、コストを削減するNetApp ONTAP'sリモートキャッシュ機能です。ファイル配布を簡素化し、WAN コストを削減します。FlexCache ボリュームを作成すると、最初にオリジンファイルシステムからメタデータのみをコピーします。このアプローチは、フルデータコピーよりも高速でスペース効率が高く、ストレージ容量のごく一部しか消費しません。

FlexCache の仕組み

FlexCache ボリュームは、元のボリュームに格納されているデータへのアクセスを提供する、スパースに格納されたキャッシュです。キャッシュは、オプションでリモートの別のファイルシステムに配置することができます。元のボリュームからすべてのデータをコピーする代わりに、FlexCache は必要なデータのみをコピーします。FlexCacheボリュームは、元のデータを変更するとキャッシュを更新する必要があるため、データ変更の頻度が低い読み取り集中型のワークフローに最適です。

次の設定により FSx for ONTAP でFlexCacheを使用できます:

元ボリューム	FlexCache volume
オンプレミスNetApp ONTAP	FSx for ONTAP

元ボリューム	FlexCache volume
FSx for ONTAP	オンプレミスNetApp ONTAP
FSx for ONTAP	FSx for ONTAP

FlexCache書き込みモード

FlexCache ボリュームは、書き込みオペレーションの 2 つのオペレーションモードをサポートします。書き込みアラウンドモードと書き込みバックモードです。

デフォルトモードであるライトアラウンドモードでは、書き込みはキャッシュから元のボリュームに転送されます。データが元のボリュームのストレージにコミットされ、元のボリュームがキャッシュへの書き戻しを確認するまで、書き込み操作はクライアントに認識されません。各書き込みはキャッシュとオリジン間のネットワークを経由する必要があるため、このモードは書き込みバックモードよりもレイテンシーが高くなります。

ONTAP9.15.1 で導入されたライトバックモードでは、書き込みはキャッシュ位置のストレージにコミットされ、すぐにクライアントに確認応答されます。その後、データはオリジンボリュームに非同期的に書き込まれます。このモードでは、書き込みをローカルに近い速度で実行できるため、分散ワークロードのパフォーマンスが大幅に向上します。

低レイテンシーのキャッシュ書き込みを必要とする書き込み負荷の高いワークロードには、書き込みバックモードを使用します。レイテンシーの影響を受けない読み取り負荷の高いワークロード、またはオリジンファイルシステムに 10 個を超えるFlexCacheオリジンボリュームがある場合、書き込みアラウンドモードを使用します。

FlexCache ボリューム作成の概要

FlexCache ボリュームの作成ステップは以下のとおりです:

1. 出典および宛先論理的なインターフェース (LIF) を収集します
2. オリジンファイルシステムとキャッシュファイルシステム間のクラスターピアリングを確立する
3. ストレージ仮想マシン (SVM) ピアリング関係を作成する
4. FlexCache ボリュームを作成し、書き込みモードを選択する
5. クライアントにFlexCacheボリュームをマウントする

詳細な手順については、「「FlexCache」の作成」を参照してください。

「FlexCache」の作成

以下の手順により、Amazon FSx for NetApp ONTAP ファイルシステムに FlexCache ボリュームを作成します。このボリュームは、オンプレミス NetApp ONTAP クラスターにあるオリジンボリュームによってバックアップされます。

ONTAP CLI の使用

ONTAP CLI を使用して、FSx for ONTAP ファイルシステムで FlexCache 設定を作成および管理します。

これらの手順で使用されるコマンドでは、クラスター、SVM、およびボリュームに対して以下のエイリアスを使用しています:

- `Cache_ID` – キャッシュクラスターの ID (FSxIdabcdef1234567890a 形式)
- `Origin_ID` – オリジンクラスターの ID
- `CacheSVM` – キャッシュ SVM 名
- `OriginSVM` – オリジン SVM 名
- `OriginVol` – ボリューム名
- `CacheVol` – FlexCache ボリューム名

このセクションの手順では、以下の NetApp ONTAP CLI コマンドを使用します。

- `network interfaces show`
- `cluster peer` コマンド
- `volume flexcache create`

前提条件

以下のセクションの手順を使用する前に、以下の前提条件を満たしていることを確認してください:

- 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、AWS Transit Gateway、Direct Connect、または Site-to-Site 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 クラウド」と「Amazon VPC ピアリングガイド」の「VPC ピア機能とは」を参照してください。

- この FSx for ONTAP ファイルシステムの VPC セキュリティグループは、クラスター間エンドポイント (LIF) 用に、 ICMP および TCP ポート 11104 と 11105 でのインバウンドおよびアウトバウンドルールを許可しています。
- SVM を持つ宛先 FSx for ONTAP ファイルシステムは作成しましたが、FlexCache として使用するボリュームはまだ作成していません。詳細については、「ファイルシステムの作成」を参照してください。

出典と宛先のクラスター間 LIF をレコードします

1. 送信先クラスターである FSx for ONTAP ファイルシステムの場合:

   a. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。

   b. ファイルシステム を選択し、続いてファイルシステムの詳細ページを開く送信先クラスターである FSx for ONTAP ファイルシステムを選択します。

   c. [管理] で、[クラスター間エンドポイント - IP アドレス] を見つけ、値を記録します。

   > **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 つのクラスター間エンドポイント IP アドレスがあります。

2. オンプレミスのソースクラスターの場合は、以下の ONTAP CLI コマンドを使用してクラスター間の LIF IP アドレスを取得します:

```
Origin::> network interface show -role intercluster
Logical                          Network
Vserver     Interface  Status    Address/Mask
----------- ---------- -------   ------------
OriginSVM
            inter_1     up/up    10.0.0.36/24
            inter_2     up/up    10.0.1.69/24
```

3. `inter_1` および `inter_2` IP アドレスを保存します。これらは、`OriginSVM` エイリアスでは `origin_inter_1` および `origin_inter_2` として、`CacheSVM` エイリアスでは `cache_inter_1` と `cache_inter_2` として参照されます。

オリジンとキャッシュ間のクラスターピアリングを確立する

cluster peer create ONTAP CLI コマンドを使用して、Cache と Source クラスターでクラスターピア関係を確立します。この 出典と宛先のクラスター間 LIF をレコードします 手順で以前に保存したクラスター間 IP アドレスを指定します。プロンプトが表示されたら、Origin 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 *cluster-peer-passphrase* を作成するように求められます。

1. Cache クラスター (FSx for ONTAP ファイルシステム) でクラスターピアリングを設定します。

   a. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. 以下のコマンドを使用して、作成するパスワードを記録します。スケールアウトファイルシステムの場合は、各 HA ペアの inter_1 および inter_2 IP アドレスを指定します。

   ```
   FSx-Cache::> cluster peer create -address-family ipv4 -peer-
   addrs origin_inter_1,origin_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   Notice: Now use the same passphrase in the "cluster peer create" command in the
    other cluster.
   ```

2. 以下のコマンドを使用して、source (オンプレミス) クラスターでクラスターピアリングを設定します。認証するには、前のステップ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、HA ペアのクラスター間 IP アドレスをそれぞれ指定する必要があります。

   ```
   Origin::> cluster peer create -address-family ipv4 -peer-
   addrs cache_inter_1,cache_inter_2

   Enter the passphrase: cluster-peer-passphrase
   ```

```
Confirm the passphrase: cluster-peer-passphrase
```

3. source クラスターで以下のコマンドを使用して、クラスターピアリングが正常に設定され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。

```
Origin::> cluster peer show

Peer Cluster Name     Availability    Authentication
-------------------   -------------   --------------
Cache_ID              Available       ok
```

出力に Available が表示されない場合は、source および cache クラスターで前のステップを繰り返します。

ストレージ仮想マシン (SVM) ピアリングを設定する

クラスターピアリングを確立したら、次のステップとして、vserver peer コマンドを使用してキャッシュクラスター (キャッシュ) に SVM ピアリング関係を作成します。以下の手順で使用される追加のエイリアスは以下のとおりです:

- *CacheLocalName* - origin SVM で SVM ピアリングを設定するときに cache SVM を識別するために使用される名前。
- *OriginLocalName* - cache SVM で SVM ピアリングを設定するときに origin SVM を識別するために使用される名前。

1. cache SVM で、以下のコマンドを使用して SVM ピアリング関係を作成します。

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-
cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. ソースクラスターで、以下のコマンドを使用して SVM ピアリング関係を承認します。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

3. 送信元クラスターでピアリング関係を承認します。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

4. 以下のコマンドを使用して、SVM ピアリングスが成功していることを確認します。Peer State レスポンスの peered のように設定する必要があります。

```
Origin::> vserver peer show

Vserver      Peer Vserver    Peer State    Peering Cluster    Remote Applications

------------ --------------- ------------- ------------------
 ------------------------
OriginSVM    CacheSVM        peered        FSx-Cache          flexcache
```

FlexCache ボリュームを作成する

SVM ピアリング関係を作成したら、次のステップとしてキャッシュ SVM に FlexCache ボリュームを作成します。FlexCache ボリュームは FlexGroup である必要があります。また、FlexCache ボリュームのオペレーションモードを選択します。詳細については、「FlexCache書き込みモード」を参照してください。

1. キャッシュクラスターで、以下の ONTAP CLI コマンドを使用して FlexCache ボリュームを作成します。この例では、*CacheVol* という名前の 2 TB FlexCache ボリュームを作成します。

   - 書き込みアラウンド FlexCache ボリュームを作成するには、以下のコマンドを使用します。

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1
   ```

   - 書き込みバック FlexCache ボリュームを作成するには、以下のコマンドを使用します。

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1 -is-writeback-enabled true
   ```

> **Note**
>
> volume flexcache config modify -is-writeback-enabled {true|false} コマンドを使用して、書き込みモードを変更できます。このコマンドを使用する前に、set -privilege advanced コマンドを使用して ONTAP CLI アドバンストモードになっていることを確認してください。

2. FlexCache ボリュームとオリジンボリュームの FlexCache 関係を確認します。

   - FlexCache 書き込みアラウンドボリュームの場合、出力は以下の例のようになります。

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
-------   ----------  -------  --------------  -------------  --------------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
```

   - FlexCache 書き込みバックボリュームの場合、出力は以下の例のようになります。

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
 Writeback
-------   ----------  -------  --------------  -------------  --------------
 ---------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
 true
```

FlexCache ボリュームをマウントする

FlexCache ボリュームが AVAILABLE になると、NFSv3、NFSv4、および SMB クライアントはそれをマウントできます。FlexCache がマウントされると、クライアントはオンプレミスのオリジンボリュームのデータセット全体にアクセスできます。

- マウントポイントを作成して FlexCache をマウントするには、クライアントで以下のコマンドを実行します:

```
$ sudo mkdir -p /fsx/CacheVol
```

```
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

NetApp SnapMirrorを使用したデータの複製

NetApp SnapMirrorを使用して、FSx for ONTAP ファイルシステムの第 2 ファイルシステムへの、または第 2 ファイルシステムから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、ONTAP内の 2 つの Amazon FSx ファイルシステム間でレプリケートする場合でも、オンプレミスからAWSにレプリケートする場合でも、AWSシステム全体で高いデータ可用性と高速なデータレプリケーションを実現できます。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。

NetAppストレージシステムにデータをレプリケートし、セカンダリデータを継続的に更新すると、データは最新の状態に保たれ、必要なときにいつでも使用できます。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複製する方法の詳細については、NetApp ConsoleドキュメントNetApp SnapMirrorの Learn about NetApp Replication (複製サービスについて学ぶ)をご参照ください。

NetApp SnapMirrorのデータ保護 (DP) 宛先ボリュームは、NetApp ONTAPCLI および REST API に加えて、Amazon FSx コンソール、AWS CLI、Amazon FSx API を使用して作成できます。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。

NetApp ConsoleまたはONTAPCLI を使用して、ファイルシステムの複製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。Synchronous SnapMirrorを含むStrictSyncはサポートされていません。

NetApp Consoleを使用したレプリケーションのスケジュール

NetApp Consoleを使用して、FSx for ONTAP ファイルシステムで SnapMirror による複製を設定できます。詳細については、NetApp Console のドキュメントの NetApp Replication でデータレプリケーションを設定するをご参照ください。

ONTAPCLI を使用した複製のスケジュール

ONTAP CLI を使用して、スケジュールされたボリュームの複製を設定できます。詳細については、NetApp ONTAP ドキュメントセンターで「Managing SnapMirror volume replication」を参照してください。

AWS FSx for ONTAP の請求と使用状況レポート

AWS は、FSx for ONTAP の 2 つの使用状況レポートを提供します:

- AWS 請求レポートは、FSx for ONTAP も含めて、使用している AWS のサービス のアクティビティすべての概要を示します。
- AWS 使用状況レポートは、特定のサービスのアクティビティの概要を、時間、日、または月単位で集約して示します。FSx for ONTAP の使用状況をグラフで表示する利用状況チャートも含まれています。

> **Note**
>
> 他の AWS のサービス と同様に、FSx for ONTAP は実際に使用した分のみの料金請求となります。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 の AWS 請求レポートを表示する

AWS Billing and Cost Management コンソールの [請求書] ページで、AWS の使用状況と料金の概要をサービス別に表示できます。

AWS 請求レポートを表示するには

1. AWS マネジメントコンソール にサインインし、AWS Billing and Cost Management コンソール (https://console.aws.amazon.com/costmanagement/) を開きます。
2. ナビゲーションペインで [請求] を選択します。
3. [請求期間] (例: 2024 年 8 月) を選択します。
4. Amazon FSx の料金を表示したい場合は、サービス別料金 タブで、サービステキストによるフィルターフィールドに「FSx」と入力し、FSx を展開してAWS リージョンで料金を表示します。

   FSx for ONTAP ファイルシステムの料金は、レポートの Amazon FSx CreateFileSystem:ONTAP エントリの下に表示されます。
5. 詳細な請求レポートを CSV 形式でダウンロードするには、[請求] ページ上部の [すべてを CSV にダウンロード] を選択します。

AWS 請求書の詳細については、「AWS Billing ユーザーガイド」の「Viewing your bill」を参照してください。

請求レポートには、FSx for ONTAP ファイルシステムに適用される以下の使用タイプが含まれています。

First generation FSx for ONTAP file systems

Charge Type (料金タイプ)	単位	説明	
ONTAP シングル AZ SSD ストレージ	GB-月	第 1 世代シングル-AZ ONTAP ファイルシステムにプロビジョニングされた SSD ストレージの量	
ONTAP マルチ AZ SSD ストレージ	GB-月	第 1 世代マルチ-AZ FSx for ONTAP ファイルシステムにプロビジョニングされた SSD ストレージの量	
シングル AZ スループットキャパシティ	MBps-月	第 1 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ	
ONTAP マルチ AZ スループットキャパシティ	MBps-月	第 1 世代マルチ AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ	
プロビジョンド ONTAP シングル-AZ SSD IOPS	IOPS/月	第 1 世代シングル-AZ FSx for ONTAP ファイルシステムにおけるプロビジョニング済み SSD IOPS の量	
プロビジョン済み ONTAP マルチ-AZ SSD IOPS	IOPS/月	第 1 世代マルチ-AZ FSx for ONTAP ファイルシステム上のプロビジョニングされた SSD IOPS の量	

Second generation FSx for ONTAP file systems

Charge Type (料金タイプ)	単位	説明	
ONTAP シングル AZ 2 ストレージ	GB-月	第 2 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされた SSD ストレージ量	
ONTAP マルチ AZ 2 ストレージ	GB-月	第 2 世代マルチ-AZ FSx for ONTAP ファイルシステムにプロビジョニングされた SSD ストレージの量	
ONTAP シングル AZ 2 スループットキャパシティ	MBps-月	第 2 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ	
ONTAP マルチ AZ 2 スループットキャパシティ	MBps-月	第 2 世代マルチ-AZ FSx for ONTAP ファイルシステムにプロビジョニングされたスループットキャパシティ	
プロビジョンド ONTAP シングル AZ 2 SSD IOPS	IOPS/月	第 2 世代 シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされた SSD IOPS の量	
プロビジョンド ONTAP マルチ AZ 2 SSD IOPS	IOPS/月	第 2 世代マルチ-AZ FSx for ONTAP ファイルシステムでプロビジョニングされた SSD IOPS の量	

All FSx for ONTAP filesystems

Charge Type (料金タイプ)	単位	説明	
ONTAP 標準容量プールストレージ	GB-月	FSx for ONTAP ファイルシステムで使用されるキャパシティプールストレージの容量。	
ONTAP バックアップストレージ	GB-月	バックアップに使用されるストレージ容量の量	
SnapLock の使用状況	GB-月	SnapLock ボリュームで使用されるストレージ容量の量	
ONTAP 標準容量プールストレージへの読み取りリクエスト	オペレーション	FSx for ONTAP ファイルシステム上の標準容量プールストレージに対して行われた読み取りリクエストの数	
ONTAP 標準容量プールストレージへのリクエストを書き込む	オペレーション	FSx for ONTAP ファイルシステムの標準容量プールストレージに対して行われた書き込みリクエストの数	

FSx for ONTAP のAWSの使用レポートを表示する

AWS は、請求レポートよりも詳細な FSx 使用状況レポートを提供します。使用状況レポートには、使用状況データが時間、日、または月単位で集計され、リージョンと使用タイプ別に操作が一覧で示されます。

AWS 使用状況レポートを表示するには

1. AWS マネジメントコンソール にサインインし、AWS Billing and Cost Management コンソール (https://console.aws.amazon.com/costmanagement/) を開きます。
2. ナビゲーションペインで、[Cost Explorer] を選択します。
3. [レポートパラメータ] セクションで、レポートの [日付範囲] と粒度を選択します。

4. > ディメンションでグループ化] を サービス に設定したままにします。
5. [フィルター > サービス] で、[FSx] を選択します。
6. 使用タイプを選択します。FSx for ONTAP の使用タイプのリストについては、以下の表を参照してください。
7. レポートに追加のフィルターを選択します。
8. レポートの詳細をファイルにダウンロードするには、CSV 形式でダウンロード を選択します。

以下の表に、レポートをフィルタリングして ONTAP ファイルシステムの使用状況データを表示するために使用できる FSx for ONTAP の使用タイプを示します。Cost Explorer の使用の詳細については、「AWS Cost Management ユーザーガイド」の「Analyzing your costs and usage with AWS Cost Explorer」を参照してください。

First generation FSx for ONTAP file systems

使用タイプ	単位	説明
region-Storage.SAZ_2N:SSD	GB-月	第 1 世代シングル AZ FSx for ONTAP ファイルシステムにプロビジョニングされた SSD ストレージの容量。
region-Storage.MAZ:SSD	GB-月	第 1 世代マルチ-AZ FSx for ONTAP ファイルシステムにプロビジョニングされた SSD ストレージの量。
region-ThroughputCapacity.SAZ_2N	MiBps-Mo	第 1 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ。
region-ThroughputCapacity.MAZ	MiBps-Mo	第 1 世代マルチ-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ。
region-ProvisionedSSDIOPS.SAZ_2N	IOPS-Mo	第 1 世代シングル-AZ FSx for ONTAP ファイルシステムで SSD

使用タイプ	単位	説明
		ストレージの GiB あたり 3 IOPS を超えてプロビジョニング済みの SSD IOPS の量。
region-ProvisionedSSDIOPS.MAZ	IOPS-Mo	第 1 世代マルチ-AZ FSx for ONTAP ファイルシステムで SSD ストレージの GiB あたり 3 IOPS を超えてプロビジョニングされた SSD IOPS の量。

Second generation FSx for ONTAP file systems

使用タイプ	単位	説明
region-Storage.SAZ_2N2:SSD	GB-月	第 2 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされた SSD ストレージ量。
region-Storage.MAZ2:SSD	GB-月	第 2 世代マルチ-AZ FSx for ONTAP ファイルシステムでプロビジョニングされた SSD ストレージ量。
region-ThroughputCapacity.SAZ_2N2	MiBps-Mo	第 2 世代シングル-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ。
region-ThroughputCapacity.MAZ2	MiBps-Mo	第 2 世代のマルチ-AZ FSx for ONTAP ファイルシステムでプロビジョニングされたスループットキャパシティ。
region-ProvisionedSSDIOPS.SAZ_2N2	IOPS-Mo	第 2 世代シングル-AZ FSx for ONTAP ファイルシステムで、SSD ストレージの GiB あたり 3 IOPS

使用タイプ	単位	説明
		を超えてプロビジョニングされた SSD IOPS の容量。
region-ProvisionedSSDIOPS.MAZ2	IOPS-Mo	第 2 世代マルチ AZ FSx for ONTAP ファイルシステムで、SSD ストレージの GiB あたり 3 IOPS を超えてプロビジョニングされた SSD IOPS の容量。

All FSx for ONTAP file systems

使用タイプ	単位	説明
region-Storage.SAZ_2N:CPoolStd	GB-Mo	第 1 世代または第 2 世代の Single-AZ FSx for ONTAP ファイルシステムで使用される標準容量プールストレージの容量。
region-Storage.MAZ:CPoolStd	GB-Mo	第 1 世代または第 2 世代のマルチ AZ FSx for ONTAP ファイルシステムで使用される標準容量プールストレージの容量。
region-BackupUsage	GB-月	バックアップに使用されるストレージ容量の量。
region-SnaplockUsage	GB-月	SnapLock ボリュームで使用されるストレージ容量の量。
region-Requests.SAZ_2N:CPoolStdRd	オペレーション	シングル AZ FSx for ONTAP ファイルシステム上の標準容量プールストレージに対して行われた読み取りリクエストの数。
	オペレーション	シングル AZ FSx for ONTAP ファイルシステムの標準容量プールスト

使用タイプ	単位	説明
region-Requests.SAZ_2N:CPoolStdWr		レージに対して行われた書き込みリクエストの数。
region-Requests.MAZ:CPoolStdRd	オペレーション	マルチ AZ FSx for ONTAP ファイルシステムの標準容量プールストレージに対して行われた読み取りリクエストの数。
region-Requests.MAZ:CPoolStdWr	オペレーション	マルチ AZ FSx for ONTAP ファイルシステムの標準容量プールストレージに対して行われた書き込みリクエストの数。

Amazon FSx for NetApp ONTAP のモニタリング

次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 CloudWatch 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 CloudWatch は、FSx for ONTAP から raw データを自動的に収集して処理し、読み取り可能なメトリクスにします。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 NetApp Cloud Insights サービスを使用して、OnTAP ファイルシステムの FSx の設定、容量、およびパフォーマンスの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、およびハードウェアメトリクスを収集することにより、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 メトリクス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 CloudWatch によるモニタリング
- FSx for ONTAP EMS イベントのモニタリング
- データインフラストラクチャインサイトによるモニタリング
- 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
- AWS CloudTrail による FSx for ONTAP API コールのモニタリング

Amazon CloudWatch によるモニタリング

Amazon CloudWatch 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 CloudWatch は、Amazon FSx for NetApp ONTAP から raw データを収集して処理し、読み取り可能なほぼリアルタイムのメトリクスに変換します。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 メトリクススデータは、デフォルトで 1 分間隔で CloudWatch に自動的に送信されます。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch とは」を参照してください。

> **Note**
>
> デフォルトでは、FSx for ONTAP は、メトリクスデータを 1 分間隔で CloudWatch に送信しますが、次のようなメトリクスは 5 分間隔で送信されます。
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

FSx for ONTAP の CloudWatch メトリクスは、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る 4 つのカテゴリに分類されます。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]: ファイルシステムレベルのパフォーマンスとストレージ容量のメトリクス。
- [ファイルサーバーメトリクス]: ファイルサーバーレベルのメトリクス。
- [詳細なファイルシステム集計メトリクス]: アグリゲートあたりの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]: ストレージ階層 (SSD、容量プール) ごとのファイルシステムレベルの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、CloudWatch の`AWS/FSx` 名前空間に公開されます。

トピック

- CloudWatch メトリクスへのアクセス
- Amazon FSx コンソールでのモニタリングする
- ファイルシステムのメトリクス
- 第 2 世代のファイルシステムメトリクス
- ボリュームメトリクス

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
- CloudWatch の AWS Command Line Interface (AWS CLI)
- CloudWatch API

以下の手順では、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方法を説明します。

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) には、アクティブな警告、CloudWatch アラーム、[ファイルシステムのアクティビティ] の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] には、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。

以下の手順では、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を説明します。

Amazon FSx コンソールを使用して 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。

以下の手順では、Amazon CloudWatch 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方法を説明します。

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 CloudWatch 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、[メトリクスで表示] を選択します。Amazon CloudWatch コンソールの [メトリクス] ページを新しいタブで開きます。

以下の手順では、ONTAP for FSx ファイルシステムのメトリクスを Amazon CloudWatch コンソールのダッシュボードに追加する方法を説明します。

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 CloudWatch 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。

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"` パラメータで 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。

以下の手順では、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を説明します。

CloudWatch API からメトリクスにアクセスするには

- GetMetricStatistics 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。

Amazon FSx コンソールでのモニタリングする

Amazon FSx によって報告される 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
- 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ための Amazon CloudWatch アラームの作成

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}
	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

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
			メタデータの平均レイテンシー: MetadataOperationTime * 1000/MetadataOperations
	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
Storage	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}

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}
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

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`
	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?	使用可能なストレージ容量	StorageCapacity
	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`

パフォーマンスの警告と推奨事項

FSx for ONTAP では、CloudWatch メトリクスのいずれかが連続した複数のデータポイントで事前に設定されたしきい値に近づいたり超過したりすると、そのメトリクスに対して警告が表示されます。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。Amazon FSx のパフォーマンスに関するアクティブな警告や最新の警

告すべて、およびファイルシステム用に設定された ALARM 状態 にある CloudWatch アラームすべてが、[Summary] (概要) セクションの [Monitoring & performance] (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 のどのメトリクスに対しても、CloudWatch アラームを作成できます。詳しくは、「Amazon FSx をモニタリングするための 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	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、「ストレージ容量とプロビジョンド IOPS の更新」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、「HA ペア間でワークロードのバランスを取る」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
		現在 SSD 削減オペレーションを実行し、新しいディスクセットで使用率が 80% を超える場合は、容量プールにデータを階層化するか、新しいディスクにリダイレクトされたボリュームからデータを削除するか、削減オペレーション中に SSD 容量を増やすリクエストを送信できます。Amazon FSx は、減少オペレーションを再開する前に、増加リクエストに優先順位を付けます。詳細については、「ファイルシステムのストレージ容量を減らす方法 (コンソール)」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、「スループットキャパシティの更新」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、「HA ペア間でワークロードのバランスを取る」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、「ストレージ容量とプロビジョンド IOPS の更新」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、「HA ペア間でワークロードのバランスを取る」を参照してください。

> **Note**
>
> SSD 削減オペレーション中、書き込みが多いワークロードでは、オペレーションがディスクとネットワークリソースを消費するため、一時的にパフォーマンスが低下する可能性があります。パフォーマンスへの影響を最小限に抑えるには、SSD の減少操作を開始する前に、進行中のワークロードが一貫して 50% の CPU、50% のディスクスループット、または 50% の SSD IOPS を消費しないようにして、適切なヘッドルームを維持します。
> クライアントアクセスが新しいディスクセットにリダイレクトされると、ボリュームごとに最大 60 秒の短い I/O 一時停止が発生することがあります。これらの一時停止は、オペレーションのカットオーバーフェーズ中に予想され、正常です。

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ための Amazon CloudWatch アラームの作成

アラームの状態が変わったときに Amazon Simple Notification Service (Amazon SNS) メッセージを送信する CloudWatch のアラームを作成することができます。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、持続してい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だけでアクションを呼び出すことはありません。状態が変更され、指定された期間維持される必要があります。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] タブをクリックします。
5. [Create CloudWatch alarm] (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。不必要で誤解を招くような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対する回復力を持つ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 アラームによる欠落データの扱い方を設定する」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、CloudWatch が E メールまたは Amazon SNS 通知を送信するようにする場合は、[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] (アラームの作成ウィザード) をスタートします。
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

- PutMetricAlarm 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、[File system metrics] (ファイルシステムのメトリクス) または 詳細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 CloudWatch 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。

- 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
- ファイルサーバーのメトリクス
- ディスク I/O メトリクス
- 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

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 (%)。このメトリクスは、トラフィックフローが高いインバウンドまたはアウトバウンドの方向を反映していることに注意してください。各方向の個々のメトリクスを確認するには、NetworkReceivedBytes および NetworkSentBytes メトリクスを参照してください。 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

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 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
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

メトリクス	説明
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
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

メトリクス	説明
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
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

メトリクス	説明
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
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

メトリクス	説明
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
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

メトリクス	説明
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
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

メトリクス	説明
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。

メトリクス	説明
	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 有効な統計: Average、Minimum、Maximum

メトリクス	説明
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 未満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
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 未満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
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
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 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。

メトリクス	説明
	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
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 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
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

メトリクス	説明
	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 FlexClones の論理サイズの合計が含まれますが、圧縮、空き領域の活用、重複排除を通じ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

メトリクス	説明
	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

第 2 世代のファイルシステムメトリクス

FSx for ONTAP 第 2 世代のファイルシステムには、次のメトリクスが用意されています。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
- ファイルサーバーのメトリクス
- ディスク I/O メトリクス
- 詳細なファイルシステムメトリクス

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。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 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。

メトリクス	説明
	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)。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 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)。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 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。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 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 (SnapMirror、階層化、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)。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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。

メトリクス	説明
	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)。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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、ファイルサーバーがサポートする最大のディスク IOPS (HA ペアごとに設定したスループットキャパシティによって決まる) 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ニングされたディスク IOPS の使用率であるという点で FileServerDiskIopsUtilization とは異なります。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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

メトリクス	説明
	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。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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。このメトリクスでは、バックグラウンドタスク (SnapMirror、階層化、バックアップなど) を含むすべてのトラフィックが考慮されます。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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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。

メトリクス	説明
	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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 単位: パーセント 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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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。 SSD 容量削減オペレーションの間、このメトリクスは元の集計 (aggr1_old) と新規のより小さい集計 (aggr1) の両方で報告されます。 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。CloudWatch ボリュームにはそれぞれ、[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。
- [Detailed Volume Metrics] (詳細なボリュームメトリクス) は、ストレージ層ごとのメトリクスであり、StorageTier ディメンション (SSD および StandardCapacityPool の可能な値を使用) を使用した層ごと、および DataType ディメンション (User、Snapshot、および Other の可能な値を使用) を使用したデータタイプごとのストレージ消費量を測定します。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
- 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

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)。

メトリクス	説明
	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
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
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

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、NetApp ONTAP CLI を使用して閲覧できます。

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 を使用すれば、ユーザーパスワードが変更された、FlexGroup 内の構成要素が最大容量に達しつつある、論理ユニット番号 (LUN) が手動でオンラインまたはオフラインにされた、ボリュームが自動的にサイズ変更された、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、NetApp ONTAP ドキュメントセンターの「ONTAP EMS Reference」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 イベントカタログ表示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

イベントログの内容を表示するときは、NetApp ONTAP CLI イベントログ表示 コマンドを使用します。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。

イベントオプション	説明
`-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。

イベントオプション	説明
`-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 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」の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、NetApp ONTAP ドキュメントセンターの「ONTAP EMS Reference」を参照してください。

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判断および分離します。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。DNS は、Syslog サーバー名を解決するようにファイルシステムで設定する必要があります。

> **Note**
>
> Syslog の送信先は、ファイルシステムで使用されるプライマリサブネットにある必要があります。

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」の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の作成コマンドを使用して、次の属性を指定して、タイプ syslog 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 で開始および終了する必要があります。
- *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 User Datagram Protocol。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 tcp-encrypted に設定されている場合、syslog-port の User Datagram Protocol デフォルト値は 6514 です。syslog-transport が tcp-unencrypted に設定されている場合、syslog-port はデフォルト値 601 を持ちます。それ以外の場合、デフォルトポートは 514 に設定されています。

```
::> 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、前のステップで作成した通知先への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送信先に転送されます。
- *dest_name* – イベント通知が送信される既存の通知先の名前。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. TCP を *transport_protocol* として選択した場合は、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* – イベント通知が送信される既存の通知先の名前。

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

データインフラストラクチャインサイトによるモニタリング

NetApp Data Infrastructure Insights (以前の Cloud Insights) は、他の NetApp ストレージソリューションと共に Amazon FSx for NetApp ONTAP ファイルシステムを監視するために使用できる NetApp サービスです。Data Infrastructure Insights を使用することにより、構成、容量、パフォーマンスのメトリックを経時的に監視して、ワークロードの傾向を把握し、将来のパフォーマンスとストレージ容量のニーズに備えて計画することができます。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**
>
> Data Infrastructure Insights は、複数の HA ペアを持つ第 2 世代ファイルシステムではサポートされていません。

Data Infrastructure Insights 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 の関係を理解し、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。

詳細については、NetApp ONTAP 製品ドキュメントの Data Infrastructure Insights のドキュメントをご参照ください。

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キャパシティ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あり、FSx for ONTAP と互換性があります。オープンソースのモニタリングソリューションには、Grafana で Harvest を使用できます。

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ために Harvest と Grafana をセットアップおよび設定する方法について説明します。

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 メトリクス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、オンプレミスの NetApp ONTAP が公開するのとは異なるメトリクスのセットを公開します。そのため、現在、`fsx` での使用がサポートされているのは、 のタグが付いたすぐに使用できる次の Harvest ダッシュボードのみです。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。

- 収集: メタデータ
- ONTAP: アグリゲート
- ONTAP: cDOT
- ONTAP: クラスター
- ONTAP: コンプライアンス
- ONTAP: データセンター
- ONTAP: データ保護
- ONTAP: LUN
- ONTAP: ネットワーク
- ONTAP: ノード
- ONTAP: Qtree
- ONTAP: セキュリティ
- ONTAP: SnapMirror
- ONTAP: SnapMirror の送信先
- ONTAP: SnapMirror ソース
- ONTAP: SVM
- ONTAP: ボリューム
- ONTAP: SVM 別のボリューム
- ONTAP: ボリュームの深堀り

以下の Harvest ダッシュボードは FSx for ONTAP でサポートされていますが、Harvest ではデフォルトで有効になっていません。

- ONTAP: FlexCache
- ONTAP: FlexGroup
- ONTAP: NFS クライアント
- ONTAP: NFSv4 Storepool Monitors
- ONTAP: NFS のトラブルシューティング
- ONTAP: NVMe 名前空間
- ONTAP: SMB

- ONTAP: ワークロード

サポートされていない Harvest ダッシュボード

以下の Harvest ダッシュボードは、FSx for ONTAP ではサポートされていません。

- ONTAP: ディスク
- ONTAP: 外部サービスオペレーション
- ONTAP: ファイルシステム分析 (FSA)
- ONTAP: ヘッドルーム
- ONTAP: ヘルス
- ONTAP: MAV リクエスト
- ONTAP: MetroCluster
- ONTAP: 電力
- ONTAP: シェルフ
- ONTAP: S3 オブジェクトストア

CloudFormation テンプレート

スタートするには、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 CloudFormation テンプレートをデプロイできます。CloudFormation テンプレートへの入力として、`fsxadmin` ユーザーと、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 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は CloudFormation を使用して Harvest と 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 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、関連付けられた AWS のサービス料金が発生します。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提供します。NetApp のインスタンスサイズに関するレコメンデーションは、モニタリングするファイルシステムの数と収集する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 個ごとファイルシステムにつき次のことを推奨しています。

- 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」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 用のポート 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。スタートする前に、FSx for ONTAP ファイルシステムを AWS アカウント、および以

下に示すテンプレートのパラメータ情報内の Amazon Virtual Private Cloud (Amazon VPC) で実行する必要があります。ファイルシステムの作成の詳細については、「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.CloudFormation テンプレートをダウンロードします。CloudFormation スタックの作成の詳細については、『AWS CloudFormation ユーザーガイド』 の「AWS CloudFormation コンソールでのスタックの作成」 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 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. [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	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値の完全なリスト

パラメータ	デフォルト	説明
		については、「fsx-ontap-harvest-grafana.template」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。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ポート 53 および 443 に加え、受信ポート 3000 と 9090 が開いていることを確認します。
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。

パラメータ	デフォルト	説明
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。
FSxEndPoint	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。

CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。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、GitHub の「NetApp Harvest」ページを参照してください。

Harvest と Grafana のトラブルシューティング

Harvest と Grafana ダッシュボードで言及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、次のトピックで使用可能な解決策を確認してください。

トピック

- SVM とボリュームダッシュボードが空白
- タイムアウト後にロールバックされた CloudFormation スタック

SVM とボリュームダッシュボードが空白

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 および Grafana クライアントが実行している Amazon EC2 インスタンスに SSH します。

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. harvest.yml ファイルを開くには、次のコマンドを使用します。

   - FSx for ONTAP インスタンスのエントリが Cluster-2 として作成されたことを確認します。
   - ユーザー名とパスワードのエントリが fsxadmin 認証情報と一致してい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. fsxadmin ユーザー認証情報が、今後のデプロイのために次の形式で Secrets Manager に格納され、*fsxadmin_password* がパスワードに置き換えられていることを確認します。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

タイムアウト後にロールバックされた CloudFormation スタック

CloudFormation スタックを正常にデプロイできず、エラーが発生して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 および Grafana クライアントが実行している Amazon EC2 インスタンスに SSH します。

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. 次のコマンドを使用して、Docker コンテナが正常に開始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. sudo docker ps を実行して Harvest と Grafana URL を接続することで、コンテナが正常に開始されたことを確認します。

AWS CloudTrail による FSx for ONTAP API コールのモニタリング

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、コンソールで証跡を作成すると、すべての AWS リージョンに証跡が適用されます。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ログに記録し、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。詳細については、『AWS CloudTrail ユーザーガイド:』の以下のトピックを参照してください：

- の追跡の作成AWS アカウント
- 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ション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 のログファイルは、単一か複数のログエントリを含みます。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"
}
```

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。

オプションとして、FSx for ONTAP ストレージ仮想マシン (SVM) を Active Directory ドメインに接続させ、ユーザー認証やファイ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することができます。その後、サーバーメッセージブロック (SMB) クライアントで、 Active Directory 内に既存するユーザー ID を使用して自らを認証し、SVM ボリュームにアクセスすることができます。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。

Microsoft Active Directory ドメインインフラストラクチャが利用できない場合、SVM を Microsoft Active Directory に参加させる代替手段として、SVM 上でワークグループ内の Server Message Block (SMB) サーバーを構成します。詳細については、「ワークグループでの SMB サーバーのセットアップ」を参照してください。

Amazon FSx for NetApp ONTAP を Active Directory に結合すると、ファイルシステムの SVM を Active Directory に個別に結合することができます。つまり、Active Directory に接続した複数の SVM を持つファイルシステムと、AD に接続されていない他の SVM を持つファイルシステムを持つことができます。

SVM を Active Directory に接続した後、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
- 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およびパスワード

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
- 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
- SVM を Microsoft Active Directory に接続する仕組み
- SVM Active Directory 設定の管理

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
- ネットワークの設定要件
- アクティブディレクトリサービスアカウントの要件

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、次の設定が含まれる必要があります。

- Active Directory ドメインコントローラードメイン機能レベルは Windows Server 2000 以降です。
- Active Directory が、シングルラベルドメイン (SLD) 形式ではないドメイン名を使用している。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 ファイルシステムと関連付けされた VPC 内のサブネットが同じ Active Directory サイトで定義され、かつ VPC サブネットと Active Directory サイトのサブネットの間に競合がないことを確認してください。

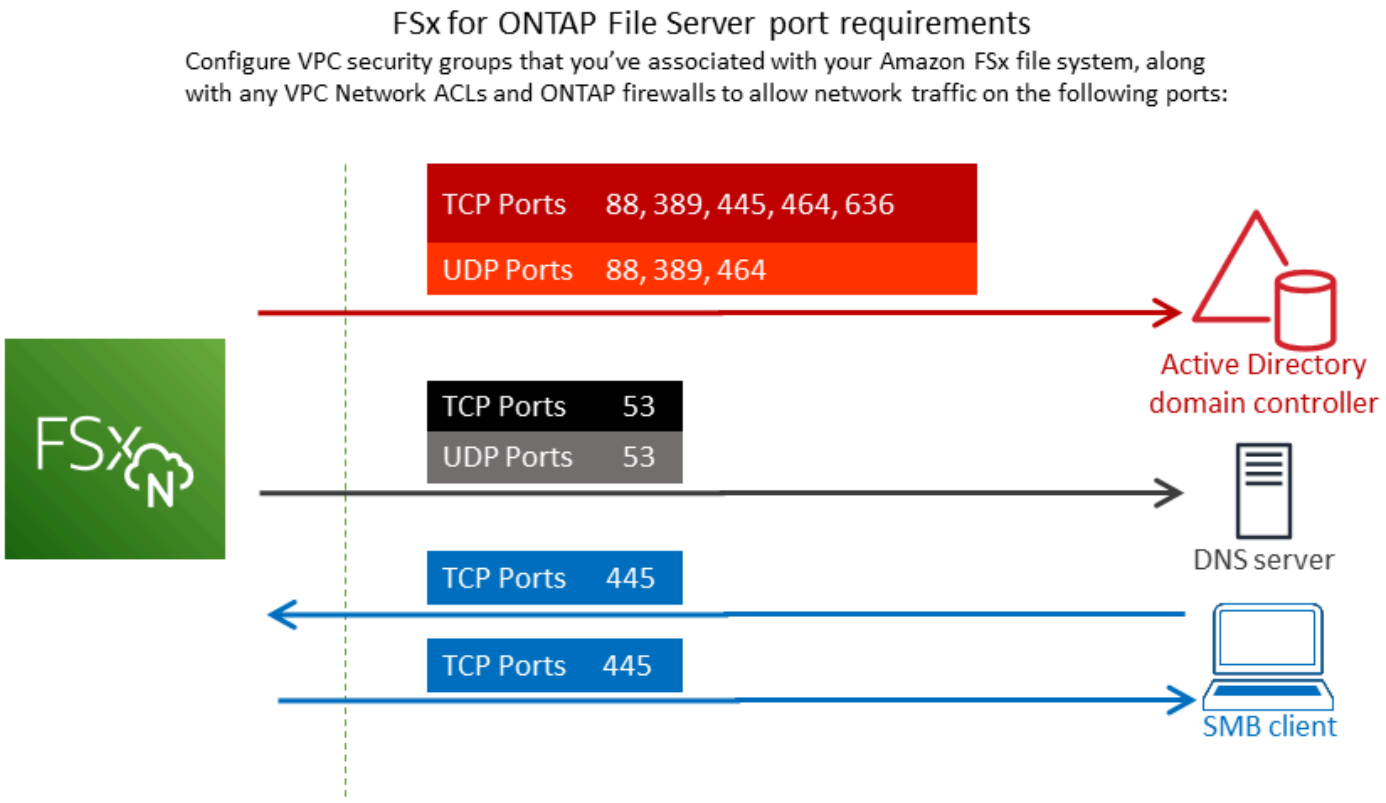
> **Note**
>
> を使用している場合 Directory Service、FSx for ONTAP は SVMs の Simple Active Directory への結合をサポートしていません。

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、「Direct Connect」、「Site-to-Site 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、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 管理者のそれぞれに適用されるファイアウォールにも反映されている必要があります。

> **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結合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。

Active Directory サービスアカウントの認証情報を に保存し AWS Secrets Manager (推奨) 、Active Directory に参加するためのシークレット ARN を Amazon FSx に提供したり、プレーンテキストの認証情報を提供したりできます。

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接続解除や再接続を実行するために必要とな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や SVM の交換、あるいは 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を含む Active Directory の情報を Amazon FSx で定期的に更新してください。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、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**
>
> SVM が作成された後に Amazon FSx が OU に作成したコンピュータオブジェクトを移動したり、SVM が結合されている間に Active Directory 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。

トピック

- 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 でアクティブディレクトリ設定を最新の状態に保つ
- 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
- 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
- を使用した Active Directory 認証情報の保存 AWS Secrets Manager

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 を使用します AWS CLI。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 マネジメントコンソール、 AWS CLI、および API を使用した既存の SVM Active Directory 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。

を使用した Active Directory 認証情報の保存 AWS Secrets Manager

を使用して AWS Secrets Manager 、Microsoft Active Directory ドメイン結合サービスアカウントの認証情報を安全に保存および管理できます。この方法により、機密性の高い資格情報をアプリケーションコードまたは構成ファイルにプレーンテキストで格納する必要がなくなり、セキュリティ体制が強化されます。

シークレットへのアクセスを管理するように IAM ポリシーを設定し、パスワードの自動ローテーションポリシーを設定することもできます。

Active Directory 認証情報を に保存する AWS Secrets Manager (コンソール)

ステップ 1: KMS キーを作成する

Secrets Manager で Active Directory 認証情報を暗号化および復号するための KMS キーを作成します。

キーを作成するには

> **Note**
>
> 暗号化キーの場合は、新しいキーを作成します。 AWS デフォルトの KMS キーは使用しないでください。Active Directory に結合する SVM を含むリージョンと同じリージョン AWS KMS key に を必ず作成してください。

1. https://console.aws.amazon.com/kms で AWS KMS コンソールを開きます。
2. [Create key] (キーの作成) を選択します。
3. [キーの種類] として、[対称] を選択します。
4. [キーの使用方法] として、[暗号化と復号化] を選択します。
5. 詳細オプションについては、以下の操作を実行します:
   a. [キーマテリアルのオリジン] として、[KMS] を選択します。
   b. [リージョナリティ] として、[単一リージョンキー] を選択し、[次へ] を選択します。

6. [次へ] を選択します。
7. [エイリアス] に、KMS キーの名前を指定します。
8. (オプション) [説明] に、KMS キーの説明を入力します。
9. (オプション) タグで、KMS キーのタグを指定し、次へを選択します。
10. (オプション) キー管理者には、このキーを管理する権限を持つ IAM ユーザーとロールを指定します。
11. [キーの削除] で、[キー管理者にこのキーの削除を許可する] のボックスをオンのままにして、[次へ] を選択します。
12. (オプション) [キーユーザー] には、暗号化オペレーションでこのキーを使用する権限を持つ IAM ユーザーとロールを指定します。[次へ] を選択します。
13. [キーポリシー] で、[編集] を選択し、ポリシー [ステートメント] に以下を含めて、Amazon FSx が KMS キーを使用できるようにし、[次へ] を選択します。*us-west-2* をファイルシステムがデプロイ AWS リージョン されている に、*123456789012* を AWS アカウント ID に置き換えてください。

```
{
    "Sid": "Allow FSx to use the KMS key",
    "Version": "2012-10-17",
    "Effect": "Allow",
    "Principal": {
        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:123456789012:key:*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:*",
            "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": [
                "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                "arn:aws:fsx:us-west-2:123456789012:storage-virtual-machine/fs-*/
svm-*"
```

```
            ]
        }
    }
}
```

14. [Finish] を選択してください。

> **Note**
>
> 特定のシークレットとファイルシステムをターゲットにするように `Resource` および `aws:SourceArn` フィールドを変更することで、より詳細なアクセスコントロールを設定できます。

ステップ 2: AWS Secrets Manager シークレットを作成する

シークレットを作成する

1. Secrets Manager のコンソール (https://console.aws.amazon.com/secretsmanager/) を開きます。
2. [Store a new secret] (新しいシークレットを保存する) を選択します。
3. [Secret type] (シークレットタイプ) で、[Other type of secret] (他の種類のシークレット) を選択します。
4. キーと値おペアの場合は、次の手順を実行して 2 つのキーを追加します:
   a. 最初のキーには、`CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` と入力します。
   b. 最初のキーの値には、AD ユーザーのユーザー名 (ドメインプレフィックスなし) のみを入力します。
   c. 2 番目のキーとして、`CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` と入力します。
   d. 2 番目のキーの値には、ドメインの AD ユーザー用に作成したパスワードを入力します。
5. [暗号化キー] の入力では、前のステップで作成した KMS キーの ARN を入力し、[次へ] をクリックします。
6. [シークレット名] として、後でシークレットを見つけやすい、わかりやすい名前を入力します。
7. (オプション) [説明] として、シークレット名の説明を入力します。
8. リソース権限については、編集を選択します。

アクセス許可ポリシーに以下のポリシーを追加して、Amazon FSx にシークレットの使用を許可し、[次へ] を選択します。*us-west-2* をファイルシステムがデプロイ AWS リージョン されている に、*123456789012* を AWS アカウント ID に置き換えてください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "fsx.amazonaws.com"
            },
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                        "arn:aws:fsx:us-west-2:123456789012:storage-virtual-
machine/fs-*/svm-*"
                    ]
                }
            }
        }
    ]
}
```

9. (オプション) 認証情報を自動的にローテーションするように Secrets Manager を設定できます。[次へ] を選択します。
10. [Finish] を選択してください。

Active Directory 認証情報を AWS Secrets Manager (CLI) に保存する

ステップ 1: KMS キーを作成する

Secrets Manager で Active Directory 認証情報を暗号化および復号するための KMS キーを作成します。

KMS キーを作成するには、 AWS CLI コマンド create-key を使用します。

このコマンドで、--policy パラメータを設定して、KMS キーのアクセス許可を定義するキーポリシーを指定します。ポリシーには以下の内容を含める必要があります:

- Amazon FSx のサービスプリンシパル。これは、fsx.amazonaws.com です。
- 必要な KMS アクション: kms:Decrypt および kms:DescribeKey。
- AWS リージョン および アカウントのリソース ARN パターン。
- キーの使用を制限する条件キー:
  - kms:ViaService リクエストが Secrets Manager を介して送信されるようにします。
  - アカウントに制限する aws:SourceAccount。
  - 特定の Amazon FSx ファイルシステムに制限する aws:SourceArn。

以下の例では、Amazon FSx がキーを復号化およびキー説明オペレーションに使用できるようにするポリシーを使用して、対称暗号化 KMS キーを作成します。コマンドは AWS アカウント ID とリージョンを自動的に取得し、これらの値を使用してキーポリシーを設定して、Amazon FSx、Secrets Manager、KMS キー間の適切なアクセスコントロールを確保します。 AWS CLI 環境が Active Directory に参加する SVM と同じリージョンにあることを確認します。

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
```

```
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": [
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
        }
      }
    }
  ]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"
```

> **Note**
>
> 特定のシークレットとファイルシステムをターゲットにするように Resource および aws:SourceArn フィールドを変更することで、より詳細なアクセスコントロールを設定できます。

ステップ 2: AWS Secrets Manager シークレットを作成する

Amazon FSx が Active Directory にアクセスするためのシークレットを作成するには、 AWS CLI コマンド create-secret を使用して、次のパラメータを設定します。

- `--name`: シークレットの識別子。
- `--description`: シークレットの目的の説明。
- `--kms-key-id`: 保管中のシークレットを暗号化するためにステップ 1 で作成した KMS キーの ARN。
- `--secret-string`: AD 認証情報を次の形式で含む JSON 文字列:
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: ドメインプレフィックスを含まない AD サービスアカウントのユーザー名 (`svc-fsx`など) 。`CORP\svc-fsx`などのドメインプレフィックスを指定しないでください。
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: AD サービスアカウントのパスワード
- `--region`: SVM が作成される AWS リージョン 。`AWS_REGION` が設定されていない場合、既定では構成済みのリージョンが使用されます。

シークレットを作成したら、put-resource-policy コマンドを使用してリソースポリシーをアタッチし、以下のパラメータを設定します:

- `--secret-id`: ポリシーをアタッチするシークレットの名前または ARN。次の例では、**`FSxSecret`** を `--secret-id` として使用します。
- `--region`: シークレット AWS リージョン と同じです。
- `--resource-policy`: シークレットへのアクセス許可を Amazon FSx に付与する JSON ポリシードキュメント。ポリシーには以下の内容を含める必要があります:
  - Amazon FSx のサービスプリンシパル。これは、**`fsx.amazonaws.com`** です。
  - 必要な Secrets Manager アクション: `secretsmanager:GetSecretValue` および `secretsmanager:DescribeSecret`。
  - AWS リージョン および アカウントのリソース ARN パターン。
  - アクセスを制限する以下の条件キー:
    - アカウントに制限する `aws:SourceAccount`。
    - 特定の Amazon FSx ファイルシステムに制限する `aws:SourceArn`。

次の例では、必要な形式でシークレットを作成し、Amazon FSx にシークレットの使用を許可するリソースポリシーをアタッチします。この例では、 AWS アカウント ID とリージョンを自動的に取得し、Amazon FSx とシークレット間の適切なアクセスコントロールを確保するために、これらの値を使用してリソースポリシーを設定します。

KMS_KEY_ARN を ステップ 1 で作成したキーの ARN に置き換え、CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME と CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD を Active Directory サービス アカウントの認証情報に置き換えてください。さらに、Active Directory に参加する SVM と同じリージョンに AWS CLI 環境が設定されていることを確認します。

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
```

```
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {
            \"aws:SourceArn\": [
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
          }
        }
      }
    ]
  }"

echo "Resource policy attached successfully"
```

> **Note**
>
> 特定のシークレットとファイルシステムをターゲットにするように Resource および aws:SourceArn フィールドを変更することで、より詳細なアクセスコントロールを設定できます。

SVM を Microsoft Active Directory に接続する仕組み

組織は、オンプレミスかクラウドかを問わず、Active Directory を使用して ID とデバイスを管理する場合があります。FSx for ONTAP を使用すると、次の方法で SVM を既存の Active Directory ドメインに直接接続させることができます。

- 作成時に新しい SVM を Active Directory に結合する
  - 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 SVM をセルフマネージド Active Directory に接続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 (SVM) の作成」を参照してください。
- SVM を既存の Active Directory に結合する
  - AWS マネジメントコンソール、 AWS CLI、および API を使用して SVM を Active Directory に結合し、最初の結合試行が失敗した場合に SVM を Active Directory に再度結合しようとします。既に Active Directory に接続している SVM の一部の Active Directory 構成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 Active Directory 設定の管理」を参照してください。
  - SVM Active Directory 設定の接続、再試行、接続解除には NetApp ONTAP CLI または REST API を使用します。詳細については、「NetApp CLI を使用して SVM Active Directory 設定を更新する」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、委任 FSx AWS 管理者、 AWS 委任管理者、または OU への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。

FSx for ONTAP SVM をセルフマネージド Active Directory に直接接続させる場合、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 設定の最上位論理コンテナ) に存在し、ユーザーおよび既存のリソース (既存のファイルサーバーを含む) と同じ Active Directory ドメイン内にあります。

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

SVM を Active Directory に接続させるときには、選択する API オペレーションに関わらず、Active Directory 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 Active Directory コンピュータオブジェクトの NetBIOS 名。これは Active Directory の SVM の名前であり、Active Directory 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 をドメインに結合するために使用する Active Directory サービスアカウントの認証情報。これらは、次のいずれかの方法で指定できます:
  - オプション 1: AWS Secrets Manager シークレット ARN - Active Directory 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を含むシークレット。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。
  - オプション 2: プレーンテキスト認証情報
    - サービスアカウントのユーザー名 - 既存の Microsoft Active Directory 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。
- (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 Active Directory に結合する場合は、 が関連するディレクトリオブジェクト用に 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、 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 `example.com` の場合、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 ドメインのドメイン管理者グループに委任します。

SVM Active Directory 設定の管理

このセクションでは AWS マネジメントコンソール、 AWS CLI、、FSx API、ONTAP CLI 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 Active Directory に結合する
- 既存の SVM Active Directory 設定を変更する
- Active Directory からの SVM の削除

Active Directory から SVM を削除するには、NetApp ONTAP CLI を使用する必要があります。

トピック

- AWS マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合する
- AWS マネジメントコンソール、 AWS CLI、および API を使用した既存の SVM Active Directory 設定の更新
- NetApp CLI を使用して SVM Active Directory 設定を更新する

AWS マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合する

次の手順を使用して既存の SVM を Active Directory に接続します。この手順では、SVM はまだ Active Directory に接続していません。

SVM を Active Directory (AWS マネジメントコンソール) に接続させるには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。

2. Active Directory に接続させる SVM を選択してください。

   - 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。

   Active Directory に接続させたい SVM をリストから選択します。

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 Active Directory について、次の情報を入力します。

   - SVM 用に作成する Active Directory コンピュータオブジェクトの NetBIOS 名。これは Active Directory の SVM の名前であり、Active Directory 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 サーバの IP アドレス:ドメインの DNS サーバの IPv4 または IPv6 アドレス。
   - [サービスアカウントの認証情報] – サービスアカウントの認証情報を指定する方法を選択します:
     - オプション 1: AWS Secrets Manager シークレット ARN - Active Directory 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を含むシークレット。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。
     - オプション 2: プレーンテキスト認証情報
       - サービスアカウントのユーザー名 - 既存の Microsoft Active Directory 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。

- [Secrets Manager での管理] (デフォルト) – サービスアカウントの認証情報を含む Secrets Manager シークレットの ARN を指定します。シークレットには、キーと値のペア `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` と `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` が含まれている必要があります。
- (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、委任 FSx 管理者、 AWS 委任管理者、または OU AWS への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。

  セルフマネージド Active Directory を結合している場合は、Active Directory 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。

5. 指定した設定を使用して SVM を Active Directory に接続させるには、[Active Directory に接続] を選択します。

SVM を Active Directory に結合するには (AWS CLI)

- FSx for ONTAP SVM を Active Directory に接続させるには、次の例で示すように、「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 マネジメントコンソール、 AWS CLI、および API を使用した既存の SVM Active Directory 設定の更新

次の手順を使用して、既に Active Directory に接続されている SVM の Active Directory 設定を更新します。

SVM Active Directory 設定を更新するには (AWS マネジメントコンソール)

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、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. このウィンドウでは、次の Active Directory 設定プロパティを更新できます。

   - DNS サーバの IP アドレス:ドメインの DNS サーバの IPv4 または IPv6 アドレス。
   - [サービスアカウントの認証情報] – サービスアカウントの認証情報を指定する方法を選択します:
     - オプション 1: AWS Secrets Manager シークレット ARN - Active Directory 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を含むシークレット。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。

- オプション 2: プレーンテキスト認証情報
  - サービスアカウントのユーザー名 - 既存の Microsoft Active Directory 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。

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 Active Directory に接続されている SVM の Active Directory 設定を更新します。

SVM Active Directory 設定を更新するには (AWS CLI)

- AWS CLI または API を使用して SVM の Active Directory 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 を使用して SVM Active Directory 設定を更新する

NetApp ONTAP CLI を使用して、SVM を Active Directory に接続または接続解除したり、既存の SVM Active Directory 設定を変更することができます。

ONTAP CLI を使用して SVM を Active Directory に接続する

次の手順で説明されているように、ONTAP CLI を使用して既存の SVM を Active Directory に接続させることができます。これは、SVM が既に Active Directory に結合している場合でも実行できます。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 に結合させるには、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 を結合させる 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検証するには、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. この結合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。たとえば、 AWS マネージド Active Directory でデフォルトの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 設定を変更することができます。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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、次を置き換え、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 に結合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検証できます。

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 サーバを元に戻します。

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

NetApp ONTAP CLI を使用して、SVM から Active Directory への結合を解除する

NetApp ONTAP CLI を使用して、以下のステップに従って Active Directory から SVM の結合を解除することもできます。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 からデバイスの結合を解除した 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、元々 SVM を Active Directory に結合させるために使用した認証情報を入力します。

   ```
   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 用の DNS サーバーを削除します。

   ```
   ::vserver services name-service dns delete -vserver svm_name
   ```

dns を ns-switch として削除する必要があることを示す次のような警告が表示され、このデバイスを Active Directory に再接続させ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 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 層をモニタリングし、階層化プロセスがキャパシティプールストレージにデータを移行できる速度よりも早く SSD がいっぱいにならないようにしてください。

トピック

- NetApp SnapMirror を使用した FSx for ONTAP への移行
- AWS DataSync を使用した FSx for ONTAP への移行

NetApp SnapMirror を使用した FSx for ONTAP への移行

NetApp ONTAP ファイルシステムは、ネットアップの SnapMirror を使用して Amazon FSx for NetApp ONTAP に移行できます。

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、指定された出典ボリュームからデスティネーションボリュームにデータをレプリケーションします。オンプレミス NetApp ONTAP ファイルシステムを FSx for ONTAP に移行するには、SnapMirror を使用することをお勧めします。NetApp SnapMirror のブロックレベルレプリケーションは、次のようなファイルシステムでも迅速かつ効率的です。

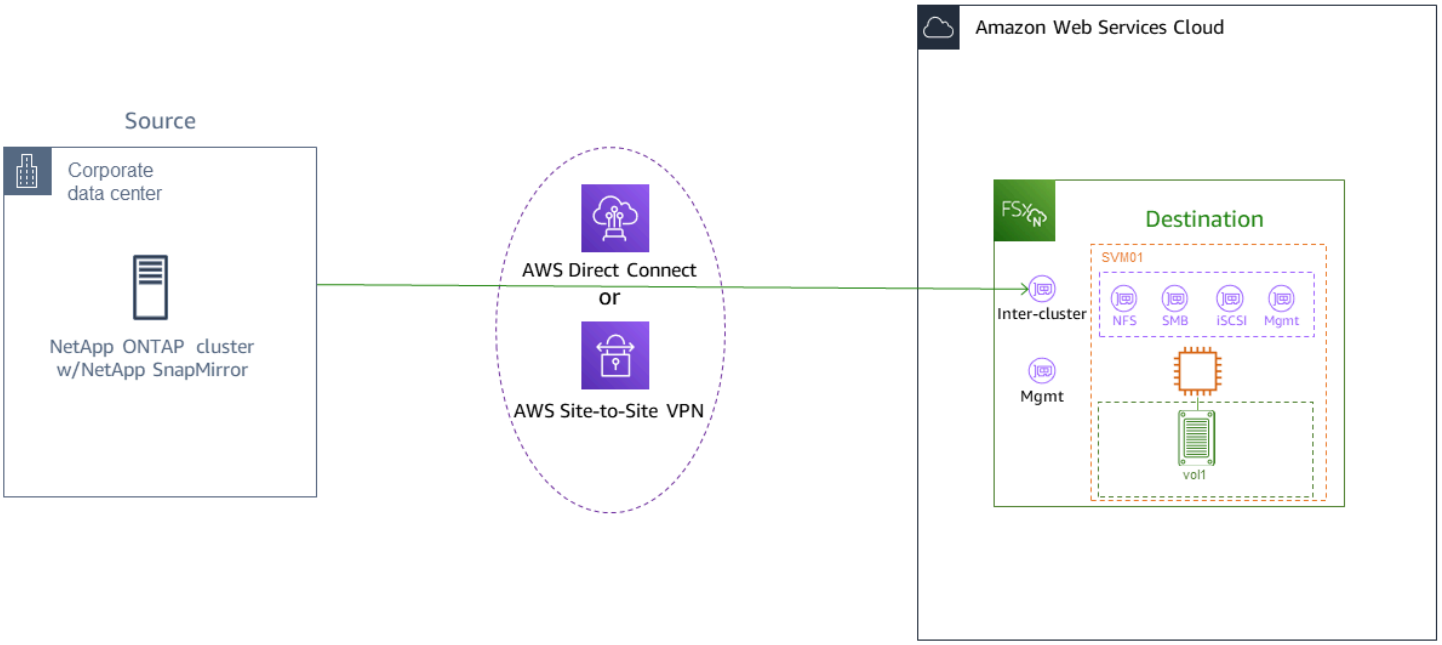
- 複雑なディレクトリ構造

- 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 に移行すると、重複除外および圧縮されたデータはそれらの状態にとどまるため、転送時間が短縮され、移行に必要な帯域幅が削減されます。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 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含まれます。

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 Site-to-Site 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 クラウド 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、移行元ボリュームと移行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 関係に対応した ONTAP バージョン」を参照してください。ここに示された手順では、移行元にオンプレミス NetApp ONTAP ファイルシステムを使用します。

- オンプレミス (移行元) 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、「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* - 宛先 (FSx) クラスターの ID (FSxIdabcdef1234567890a 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 ファイルシステムで SnapMirror 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) 宛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。

> **Note**
>
> ONTAP は、宛先ボリュームの階層化ポリシーが All の場合、送信元で達成された後処理圧縮による節約を送信先 DP ボリュームに保持しません。後処理圧縮の節約を維持するには、送信先ボリューム階層化ポリシーを Auto に設定し、送信先ファイルシステムで inactive-data-compression を有効にして、送信先で後処理圧縮の節約を再適用する必要があります。

次の手順では、NetApp ONTAP CLI を使用して FSx for ONTAP ファイルシステム上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。-type DP を使用して、SnapMirror リレーションシップの宛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、それぞれ一意の IP アドレスを持つクラスタ間論理的なインターフェイス (LIF) を使用して、送信元クラスターと宛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. 出典 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**
>
> 第 2 世代のシングル AZ 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。第 2 世代のシングル AZ 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。第 2 世代のシングル AZ 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

出典 SVM と宛先 SVM をピアリングしたので、次のステップは、宛先クラスターで SnapMirror 関係を作成して初期化することです。

> **Note**
>
> SnapMirror 関係を作成して初期化すると、関係が切断されるまで、宛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、宛先クラスターに 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、データを宛先ファイルシステムに転送できます。

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、SnapMirror は出典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 の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 の関係を解除します。
- 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. SnapMirror のステータスを表示するには、次のコマンドを実行します。

   ```
   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、これ以降の 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 の関係を解除し、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 関係を解除します。

```
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、SnapMirror 関係が壊れたら、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、「FSx for ONTAP 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、NetApp SnapMirror を使用することをお勧めします。AWS DataSync は、自己管理型ストレージシステムと、インターネットまたは Direct Connect 経由の AWS ストレージサービスの間でのデータの移動とレプリケートを簡素化、自動化、加速化するデータ転送サービスです。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および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、異なる AWS リージョン または AWS アカウント内のファイルシステムにデータを移動したりすることもできます。また、他のタスクのために DataSync を FSx for ONTAP ファイルシステムとともに使用できます。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。

DataSync では、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」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 層をモニタリングし、階層化プロセスがキャパシティプールストレージにデータを移行できる速度よりも早く SSD がいっぱいにならないようにしてください。SSD 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に DataSync 転送をスロットリング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、DataSync 要件を満たすサーバーとネットワークが必要です。詳細については、「AWS DataSync ユーザーガイド」の「DataSync の要件」を参照してください。

DataSync を使用してファイルを移行するためのベーシックなステップ

DataSync を使用して、送信元から送信先へファイルを転送するには、次のベーシックステップを行います。

- 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 とお客様の間の責任共有です。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。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。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 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 におけるデータ保護
- Amazon FSx for NetApp ONTAP 向けのアイデンティティとアクセス管理
- AWS Amazon FSx for NetApp ONTAP 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 のレジリエンス
- Amazon FSx for NetApp ONTAP のインフラストラクチャセキュリティ
- FSx for ONTAP で NetApp ONTAP Vscan を使用する

- ONTAP ロールとユーザー

Amazon FSx for NetApp ONTAP におけるデータ保護

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。ユーザーは、このインフラストラクチャでホストされ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に関する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「AWS 責任共有モデルおよび GDPR」のブログ記事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 アイデンティティセンターまたは 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 は必須ですが、TLS 1.3 を推奨します。
- 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。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中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 などの高度な管理された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 140-3 検証済み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) 140-3」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を、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含め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 タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

FSx for ONTAP でのデータ暗号化

Amazon FSx for NetApp ONTAP では、保管中のデータの暗号化と転送中のデータの暗号化がサポートされています。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 に結合しているか、Lightweight Directory Access Protocol (LDAP) を使用するドメインに結合している Storage Virtual Machine (SVM) 内のデータにアクセスする場合、NFS および SMB プロトコル経由で転送中の 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「Encrypting data in transit」を参照してください。

保管中のデータの暗号化

すべての Amazon FSx for NetApp ONTAP ファイルシステムおよびバックアップは、 AWS Key Management Service (AWS KMS) を使用して管理されるキーにより保存中に暗号化されます。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。すべてのバックアップは作成時に自動的に暗号化され、バックアップが新しいボリュームに復元されると自動的に復号されます。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、連邦情報処理標準 (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 と統合されています。Amazon FSx は KMS キーを使用してファイルシステムおよびあらゆるボリュームバックアップを暗号化します。ファイルシステムおよびボリュームバックアップ (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 キーの許可を有効化、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 でサポートされている保管時の暗号化ファイルシステムとバックアップに関連するすべての AWS KMS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) クライアント側の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。この許可は、kms:GenerateDataKey* のデフォルトの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その条件を指定する許可をキーに付与します。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。権限の詳細については、「AWS Key Management Service 開発者ガイド」の「権限の使用」を参照してください。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: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) アカウント内のキーエイリアスをすべて一覧表示します。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との間で、転送中のファイルデータを暗号化する際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 保護された施設を離れる前に、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、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの AWS リージョン「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との間で転送中のデータを暗号化するための、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
- AWS Nitro System を使用した転送中のデータの暗号化
- Kerberos ベースの暗号化を使用した転送中のデータの暗号化
- IPsec 暗号化を使用した転送中のデータの暗号化
- 転送中のデータの SMB 暗号化の有効化
- PSK 認証を使用した IPsec の設定
- 証明書の認証を使用した IPsec の設定

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。

- Active Directory を使用しているかどうか。

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が決まり AWS リージョン ます。詳細については、「AWS Nitro System を使用した転送中のデータの暗号化」を参照してください。

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。

クライアントの場所

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。

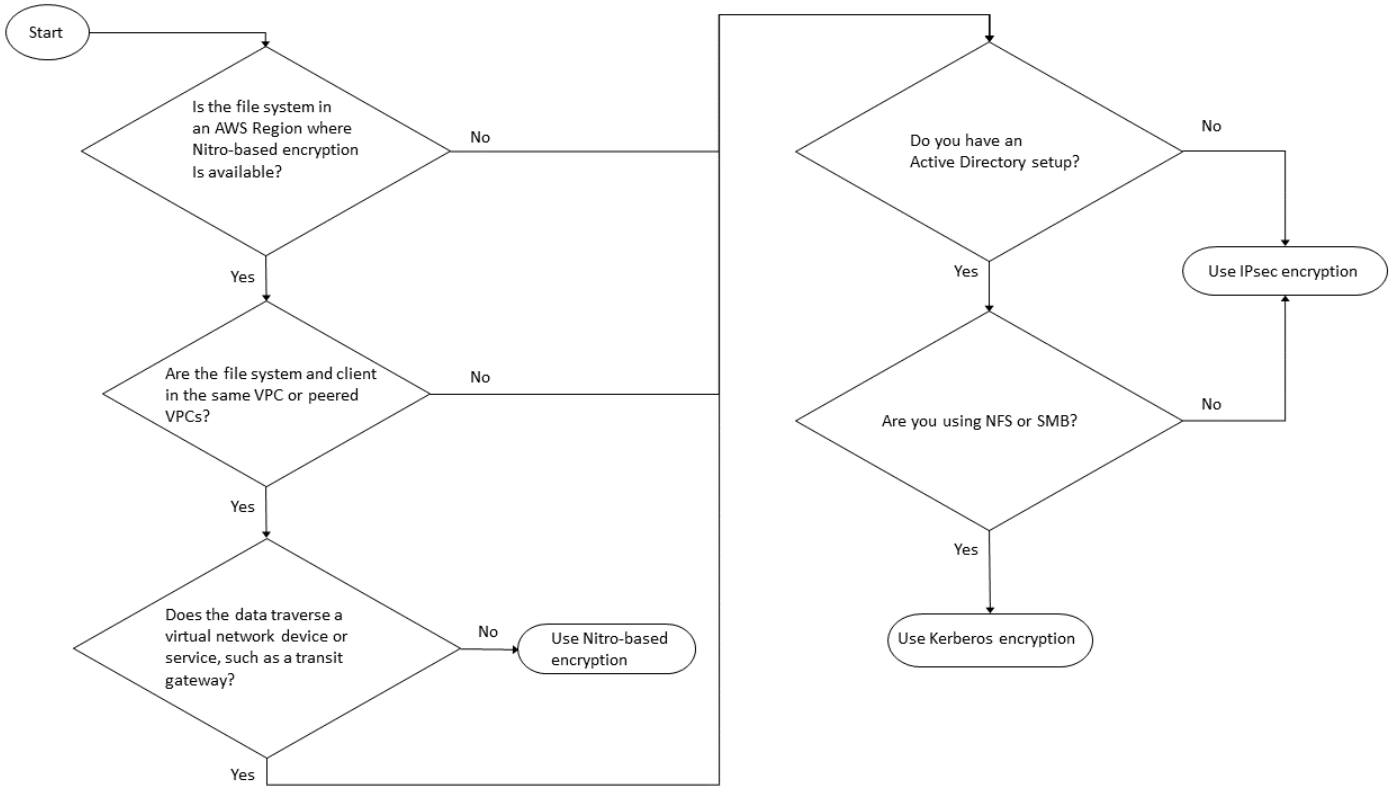
データプロトコル

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。

Active Directory

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 を使用した転送中のデータの暗号化

Nitro ベースの暗号化では、ファイルシステムにアクセスするクライアントが、FSx for ONTAP で使用できる でサポートされている Amazon EC2 Linux または Windows インスタンスタイプ AWS リージョン で実行されている場合、転送中のデータは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。

次の表は、Nitro ベースの暗号化 AWS リージョン が利用可能な の詳細を示しています。

二トロベースの暗号化のサポート

[Generation] (生成)	デプロイタイプ	AWS リージョン
第 1 世代ファイルシステム [1]	シングル AZ 1 マルチ AZ 1	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)
第 2 世代ファイルシステム	シングル AZ 2 マルチ AZ 2	米国東部 (バージニア北部)、米国東部 (オハイオ)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)、欧州 (フランクフルト)、欧州 (アイルランド)、アジアパシフィック (シドニー)

[1] 2022 年 11 月 28 日以降に作成された第 1 世代ファイルシステムは、リストされている AWS リージョンで Nitro ベースの転送中の暗号化をサポートしています。

FSx for ONTAP AWS リージョン が利用可能な 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 プロトコルと SMB プロトコル経由で Kerberos ベースの暗号化を使用して、Active Directory に追加された SVM の子ボリュームの、転送中のデータを暗号化することができます。

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 の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、ONTAP CLI を使用した SVM 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、「転送中のデータの SMB 暗号化の有効化」を参照してください。

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、サポートされているすべての IP トラフィック (NFS、iSCSI、SMB プロトコル) で、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エンドツーエンドで暗号化します。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 を使う場合、使用する IPsec クライアントは、PSK を持つインターネットキー交換のバージョン 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 暗号化を設定する高レベルの手順は、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。

コンソールを使用して IPsec を設定する方法の詳細については、「証明書の認証を使用した IPsec の設定」を参照してください。

転送中のデータの SMB 暗号化の有効化

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. SVM への着信 SMB トラフィックに SMB 暗号化をリクエストするには、vserver cifs security modify NetApp ONTAP CLI コマンドを使用します。

```
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 設定を表示するには、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. ONTAP CLI を使用した SVM の管理 の説明に従って、SVM の管理エンドポイントに secure shell (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

次のトピックでは、FSx for ONTAP ファイルシステムと、Libreswan IPsec を実行しているクライアントで、証明書の認証を使用して IPsec 暗号化を設定する方法について説明します。このソリューションでは AWS Private Certificate Authority 、 AWS Certificate Manager と 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 ファイルシステムと接続されたクライアントの両方で、証明書の認証を使用して IPsec 暗号化を設定する高レベルの手順は、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、エクスポートします。
3. 証明書をインストールし、クライアントインスタンスに IPsec を設定します。
4. 証明書をインストールし、お使いの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、組織内で使用するために、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、「 AWS Private Certificate Authority ユーザーガイド」の「プライベート CA 管理」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、「 AWS Private Certificate Authority ユーザーガイド」の「CA を作成する手順」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、「 AWS Private Certificate Authority 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。

2. issue-certificate AWS CLI コマンドを使用して、プライベート CA にルート証明書を発行して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。

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

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。You
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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 向けのアイデンティティとアクセス管理

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、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- 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 が IAM とどのように連携するか
- 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 アイデンティティとアクセスのための Amazon FSx のトラブルシューティング
- Amazon FSx のサービスリンクロールの使用
- Amazon FSx でのタグの使用

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Amazon FSx for NetApp ONTAP アイデンティティとアクセスのための Amazon FSx のトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Amazon FSx for NetApp ONTAP が IAM とどのように連携するか」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「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)

アイデンティティを使用した認証

認証は、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」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、まず、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 AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID ソースの認証情報 AWS のサービス を使用して Directory Service にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用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「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」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を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス 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、ID AWS またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられたときにアクセス許可を定義します。は、プリンシパル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。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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーと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「管理ポリシーとインラインポリシーのいずれかを選択する」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。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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。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。

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。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の上限を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。

- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。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アクセス許可を理解するのがさらに難しくなります。が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 が IAM とどのように連携するか

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 の機能	Amazon FSx のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし

IAM の機能	Amazon FSx のサポート
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
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については、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のポリシーのサポート: あり

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 許可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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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。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: なし

Amazon FSx のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS 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対してどのような条件下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

ポリシーリソースのサポート: あり

管理者は JSON AWS 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対してどのような条件下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。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。リソースレベ

ルのアクセス許可をサポートしないアクションの場合は、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すために、ワイルドカード (*) を使用します。

```
"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: あり

管理者は JSON AWS 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対してどのような条件下でアクションを実行できるかということです。

`Condition` 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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して、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。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: なし

Amazon FSx での属性ベースのアクセスコントロール (ABAC)

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

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ありです。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 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順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「属性ベースの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: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。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 AWS 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「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」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) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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: なし

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: あり

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。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。

これらのサンプルの 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 ポリシーを作成する (コンソール)」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、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon FS」を参照してください。

トピック

- ポリシーに関する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

ポリシーに関する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では、 AWS アカウントに費用が発生する場合があります。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の付与を開始するには、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することで、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 ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。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、最小特権アクセス許可とも呼ばれています。IAM を使用して許可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 でのポリシーとアクセス許可 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。たとえば、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、サービスアクションが などの特定の を通じて使用されている場合に 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 CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー 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 アクセスアナライザー 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 でポリシーを検証する 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、MFA をオンにしてセキュリティを強化します。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 を使用した安全な API アクセス 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、最小限の許可セットが必要です。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 for NetApp ONTAP 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 アイデンティティとアクセスのための Amazon FSx 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:PassRole を実行する権限がありません
- 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

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、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。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

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アクセス許可が必要です。

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アクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
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 が IAM とどのように連携するか」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) へのアクセスの許可 を参照してください。
- 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使用方法の違いについては、IAM ユーザーガイド の IAM でのクロスアカウントのリソースへのアクセス を参照してください。

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、サービスがユーザーに代わって他の AWS 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 サービス」を参照し、サービスリンクロール 列で [Yes] 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、[AWSServiceRoleForAmazonFSx] 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。これは、VPC 内のファイルシステム用のエラスティックネットワークインターフェイスの作成や、CloudWatch 内のファイルシステムとボリュームのメトリクスの公開など、アカウント内で特定のアクションを実行します。

このポリシーの更新については、「AmazonFSxServiceRolePolicy」を参照してください

アクセス許可の詳細

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。AWSServiceRoleForAmazonFSx には以下のアクセス許可があります。

> **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。リストされた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 Directory Service ディレクトリ内のアプリケーションを表示、認可、および認可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。
  - `AmazonFSx.FileSystemId` タグを持つカスタマーネットワークインターフェイスに IPv6 アドレスを割り当てます。
  - `AmazonFSx.FileSystemId` タグを持つカスタマーネットワークインターフェイスから IPv6 アドレスの割り当てを解除します。
  - 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。
  - AWS認可されたユーザーが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 名前空間の CloudWatch 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。

JSON

```
{
    "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"
                }
            }
        }
    ]
}
```

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 マネジメントコンソール、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 サービスリンクロールを編集できません。サービスリンクロールの作成後は、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 を使用してロールの説明を編集することはできます。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、AWSServiceRoleForAmazonFSx サービスにリンクされたロールを削除します。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。

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「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 AWS リソースへのアクセスを制御する方法については、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します。

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。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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、それは Department=Finance でタグ付けされる必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
```

```
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

AWS Amazon FSx for NetApp ONTAP 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、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るように、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。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可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 マネージド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) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージド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 エンティティには `AmazonFSxDeleteServiceLinkedRoleAccess` をアタッチできません。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: AmazonFSxFullAccess

IAM エンティティに AmazonFSxFullAccess をアタッチできます。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 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した条件下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。
- firehose - プリンシパルに Amazon Data Firehose へのレコード書き込みを許可します。これは、ユーザーが Firehose に監査アクセスログを送信して、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。
- 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 CloudWatch Logs に監査アクセスログを送信して、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AmazonFSxFullAccess」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 アイデンティティ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 マネジメントコンソール。

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 Alarms および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 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、ルートテーブルにタグを作成し、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 Amazon FSx ファイルシステムに関連付けられた VPC を一覧表示できるようにします。
  - 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高度なセキュリティグループ検証を提供します。
  - Amazon FSx ファイルシステムに関連付けられた Elastic Network Interfaces をプリンシパルに表示できるようにします。
- 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)。
- secretsmanager – プリンシパルがドメイン結合サービスアカウントの認証情報を選択 AWS Secrets Manager するためのシークレットを に一覧表示できるようにします。
- 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: AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess ポリシーは IAM アイデンティティ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に読み取り専用アクセス許可を付与します AWS マネジメントコンソール。

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 Alarms および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 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
  - Amazon FSx マネジメントコンソールで、プリンシパルが Amazon FSx ファイルシステムに関連付けられている、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。
  - 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高度なセキュリティグループ検証を提供します。
  - Amazon FSx ファイルシステムに関連付けられた Elastic Network Interfaces をプリンシパルに表示できるようにします。
- 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。
- secretsmanager – プリンシパルがドメイン結合サービスアカウントの認証情報を選択 AWS Secrets Manager するためのシークレットを に一覧表示できるようにします。
- 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AmazonFSxConsoleReadOnlyAccess」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 アイデンティティにアタッチできます。

- 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

このサービスがこれらの変更の追跡を開始してからの Amazon FSx の AWS マネージドポリシーの更新に関する詳細を表示します。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
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可が追加されました。`secretsmanager:ListSecrets` これにより、プリンシパルはドメイン結合サービスアカウントの認証情報を選択 AWS Secrets Manager するために でシークレットを一覧表示できます。	2025 年 11 月 5 日
AmazonFSxConsoleReadOnlyAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可が追加されました。`secretsmanager:ListSecrets` これにより、プリンシパルはドメイン結合サービスアカウントの認証情報を選択 AWS Secrets Manager するために でシークレットを一覧表示できます。	2025 年 11 月 3 日
AmazonFSxServiceRolePolicy - 既存のポリシーへの更新	Amazon FSx は、プリンシパルが `AmazonFSx.FileSystemId` タグを持つカスタマーネットワークインターフェイスに IPv6 アドレスを割り当てることを許可する新しいアクセス許可 `ec2:Assig`	2025 年 7 月 22 日

変更	説明	日付
	nIpv6Addresses を追加しました。	
AmazonFSxServiceRolePolicy - 既存のポリシーへの更新	Amazon FSx は、プリンシパルが AmazonFSx.FileSystemId タグを持つカスタマーネットワークインターフェイスから IPv6 アドレスの割り当てを解除できるようにする新しいアクセス許可 ec2:UnassignIpv6Addresses を追加しました。	2025 年 7 月 22 日
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 fsx:CreateAndAttachS3AccessPoint が追加されました。これにより、プリンシパルは S3 アクセスポイントを作成し、FSx ボリュームにアタッチできます。	2025 年 6 月 25 日
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx は、プリンシパルfsx:DescribeS3AccessPointAttachments がの 内のすべての S3 アクセスポイントを一覧表示できるようにする新しいアクセス許可を追加 AWS アカウント しました AWS リージョン。	2025 年 6 月 25 日

変更	説明	日付
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 `fsx:DetachAndDeleteS3AccessPoint` が追加されました。これにより、プリンシパルは S3 アクセスポイントを削除できます。	2025 年 6 月 25 日
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 `fsx:CreateAndAttachS3AccessPoint` が追加されました。これにより、プリンシパルは S3 アクセスポイントを作成し、FSx ボリュームにアタッチできます。	2025 年 6 月 25 日
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx は、プリンシパル`fsx:DescribeS3AccessPointAttachments` がの 内のすべての S3 アクセスポイントを一覧表示できるようにする新しいアクセス許可を追加 AWS アカウント しました AWS リージョン。	2025 年 6 月 25 日
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 `fsx:DetachAndDeleteS3AccessPoint` が追加されました。これにより、プリンシパルは S3 アクセスポイントを削除できます。	2025 年 6 月 25 日

変更	説明	日付
AmazonFSxConsoleReadOnlyAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 `ec2:DescribeNetworkInterfaces` が追加されました。これにより、プリンシパルはファイルシステムに関連付けられた Elastic Network Interface を表示できます。	2025 年 2 月 25 日
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 `ec2:DescribeNetworkInterfaces` が追加されました。これにより、プリンシパルはファイルシステムに関連付けられた Elastic Network Interface を表示できます。	2025 年 2 月 7 日
AmazonFSxServiceRolePolicy - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可、`ec2:GetSecurityGroupsForVpc` が追加されました。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
AmazonFSxReadOnlyAccess – 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可、`ec2:GetSecurityGroupsForVpc` が追加されました。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 - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可、`ec2:GetSecurityGroupsForVpc` が追加されました。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
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可、`ec2:GetSecurityGroupsForVpc` が追加されました。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 - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可、`ec2:GetSecurityGroupsForVpc` が追加されました。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
AmazonFSxFullAccess - 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
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx は、ユーザーが FSx for OpenZFS ファイルシステムの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、新しいアクセス許可を追加しました。	2023 年 11 月 26 日

変更	説明	日付
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx は、ユーザーが FSx for OpenZFS ファイルシステムの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、新しいアクセス許可を追加しました。	2023 年 11 月 26 日
AmazonFSxFullAccess - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	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
AmazonFSxFullAccess - 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 CloudWatch メトリクスを AWS/FSx 名前空間に公開するように既存の cloudwatch:PutMetricData アクセス許可を変更しました。	2023 年 7 月 24 日
AmazonFSxFullAccess - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	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 - トラッキングポリシーをスタートしました	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 - トラッキングポリシーをスタートしました	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 - 既存のポリシーへの更新	Amazon FSx は、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、新しいアクセス許可を追加しました。	2021 年 9 月 2 日
AmazonFSxFullAccess - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	Amazon FSx は、Amazon FSx が Amazon FSx for NetApp ONTAP マルチ AZ 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

変更	説明	日付
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	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 - 既存のポリシーへの更新	Amazon FSx は、Amazon FSx が CloudWatch Logs ロググストリームを記述および書き込むことを許可にする新しいパーミッションを追加しました。 これは、ユーザーが CloudWatch 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 - 既存のポリシーへの更新	Amazon FSx は、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
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx では、プリンシパルが CloudWatch Logs ロググループ、ログストリーミング、およびログストリームへのイベントの書き込みを記述および作成できる新しいアクセス許可が追加されました。 これは、プリンシパルが CloudWatch 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
AmazonFSxFullAccess - 既存のポリシーへの更新	Amazon FSx は、プリンシパルが Amazon Data Firehose にレコードを記述および書き込むことを許可する新しい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 - 既存のポリシーへの更新	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、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ために必要です。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	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、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際に、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 - 既存のポリシーへの更新	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、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 - 既存のポリシーへの更新	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、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 は、 AWS 管理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 SVM にアクセスするには、アクセスタイプによって、そのエンドポイントの 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 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。

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、FlexCache など)。
   - ONTAP REST API、CLI、または ZAPI にアクセスするために使用するすべてのクライアント (例えば、Harvest / Grafana インスタンス、NetApp Connector、または NetApp コンソール)。

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) および NetApp SnapMirror クラスター間通信
TCP	11104	NetApp SnapMirror のクラスター間通信の管理
TCP	11105	クラスター間 LIF を使用した SnapMirror 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、AWS のサービス「コンプライアンスプログラムによる対象範囲内」の「コンプライアンス」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、「Downloading Reports in AWS Artifact」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。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS「 セキュリティドキュメント」を参照してください。

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、または Direct Connect 接続なしで 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 は、IPv4 およびデュアルスタック (IPv4 および IPv6) の IP アドレスタイプで設定された VPC エンドポイントをサポートします。詳細については、Amazon VPC ユーザーガイド の インターフェイス VPC エンドポイントの作成 をご参照ください。

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 VPC 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 内で CreateFileSystem API を呼び出すことで、FSx for ONTAP ファイルシステムを作成することができます。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 は 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 VPC コンソールまたは AWS Command Line Interface () を使用して、Amazon FSx API の VPC エンドポイントを作成できますAWS CLI。詳細については、Amazon VPC ユーザーガイド の インターフェイス VPC エンドポイントの作成 をご参照ください。

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 サポートを表示および更新する」を参照してください。

AWS リージョン 中国を除き、エンドポイントのプライベート 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 エンドポイントを使用して Amazon FSx に API リクエストを行うことができます`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「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」をご参照ください。

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。
- 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 のレジリエンス

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。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続

された、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ー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、フォールトトレランス、および拡張性が優れています。

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機能がいくつか用意されています。

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期間中に、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、「ボリュームバックアップによるデータの保護」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、「スナップショットによるデータの保護」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、 AWS アベイラビリティーゾーン全体で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、耐久性、デプロイオプション」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 は、単一の AWS アベイラビリティーゾーンで高い可用性と耐久性を備え、個別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でも、そのアベイラビリティーゾーン内で継続的に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、耐久性、デプロイオプション」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環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された 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 が必須で、TLS 1.3 をお勧めします。
- 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。

FSx for ONTAP で NetApp ONTAP Vscan を使用する

NetApp ONTAP's の Vscan 機能を使用すると、サポートされているサードパーティ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。

- Deep Instinct – Vscan パートナーソリューションと Deep Instinct ドキュメント [1]
- SentinelOne — Vscan パートナーソリューションと SentinelOne Singularity クラウドデータセキュリティ
- Symantec – Vscan パートナーソリューションと Symantec Protection Engine
- Trellix (旧 McAfee) — Vscan パートナーソリューションと Trellix 製品ドキュメント
- Trend Micro – Vscan パートナーソリューション

> **Note**
>
> [1] Deep Instinct のポータルにログインしてドキュメントを表示する必要があります。

ONTAP 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、ONTAP CLI および REST API を使用する際にユーザーの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。ONTAP REST API と CLI を使用する際に、FSx for 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、組織のニーズに合った追加の 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について説明します。

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 `fsxadmin` で、`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済みのロールは 2 つあり、次のように表示されます。

- **`fsxadmin`** — このロールを持つ管理者には、ONTAP システムに対する無制限の権限があります。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、利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を持ちますが、変更を加えることができないため、NetApp Harvest 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 ONTAP CLI および 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` 独自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`
	readonly	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 には、vsadmin というデフォルトユーザーがいます。このユーザーには vsadmin ロールがデフォルトで割り当てられています。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、組織のニーズを満たす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 管理者とその機能の事前定義されたロールは次のとおりです。

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 • SnapLock オペレーション (特権削除を除く) 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

ロール名	機能
	• 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-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 関係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

ロール名	機能
`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 • SnapLock オペレーション (特権削除を含む) 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
`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 の作成方法の詳細については、「SVM ロールの作成」を参照してください。

Active Directory を使用した ONTAP ユーザーの認証

Windows Active Directory ドメインユーザーの FSx for ONTAP ファイルシステムと SVM へ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 を結合しているか、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 Active Directory に結合するだけの場合は、SVM が Active Directory に結合されたことを確認してください。詳細については、「SVM を Microsoft Active Directory に接続する仕組み」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。

  ONTAP CLI または REST API にアクセスする Windows ドメインユーザーは、パスワード認証または 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 認証の設定に使用する手順については、「ONTAP ユーザーの Active Directory 認証の設定」を参照してください。

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ています。`fsxadmin` ロールを持つファイルシステムユーザーは、`security login create` ONTAP CLI コマンドを使用して新しい SVM 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)、および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、「ONTAP ユーザーの作成」を参照してください。

トピック

- ONTAP ユーザーの作成
- 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 アカウントのパスワードの更新が失敗する

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 とファイルシステムユーザーを作成できます。

1. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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。

   この例では、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 — ログインに使用するユーザー名または Active Directory グループ名を指定します。Active Directory グループ名は、domain 認証、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。
     - ドメイン - Active Directory 認証に使用する
     - パスワード – パスワード認証に使用する
     - パブリックキー — パブリックキー認証に使用する
   - -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) コマンドに以下のパラメータを 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**。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。
  - パスワード – パスワード認証に使用する
  - パブリックキー — パブリックキー認証に使用する
  - nsswitch — NIS 認証または LDAP 認証に使用する
  - なし – 指定しなかった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、SSH とログイン用のパスワードを使用して、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 new_fsxadmin 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 fsx SVM に新しい SVM ユーザー new_vsadmin を作成し、SSH を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. 次のコマンドは、NetApp Harvest アプリケーションがパフォーマンスと容量のメトリクスを収集するために使用する新しい読み取り専用ファイルシステムユーザー harvest2-user 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 SVM 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::>
```

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ているデフォルトの SVM 管理者がいます。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 に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 -vserver vs1.example.com -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。

   - -vserver SVM の名前
   - -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"。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。ロールには、「aggr0」アグリゲート内のみで、「volume」コマンドへのすべてのアクセスがあります。

```
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 ユーザーの Active Directory 認証の使用を設定します。

この手順で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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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. 図のように 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する 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、ファイルシステムへアクセスする Active Directory の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た認証方法。以下に示しているのは、可能な値です。
  - ドメイン - Active Directory 認証用
  - パスワード – パスワード認証用
  - パブリックキー — 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、filesystem1 ファイルシステムの Active Directory ドメインユーザーアカウント CORP\Admin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 認証情報を使用して 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、-versver を含めないでください。

パラメータ	説明
-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。
-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

security login role config modify ONTAP CLI コマンドを使用して、ファイルシステムまたは SVM 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 ロールを持つシステム管理者アカウントをファイルする場合にのみ使用できます。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システムが警告します。

次の例では、fsx SVM に vsadmin-readonly ロールを持つユーザーの最短パスワード要件を 12 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 アカウントの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きに、ファイルシステムで設定したパスワード要件を満たしていない場合はエラーが表示されることがあります。パスワード要件を確認するには、security login role config show ONTAP CLI または REST API コマンドを使用します。

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. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 パラメータでは、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
```

クォータ

Amazon FSx for NetApp ONTAP で作業を行う際のクォータについて以下に説明します。

トピック

- 増加可能なクォータ
- ファイルシステムあたりのリソースクォータ

増加可能なクォータ

以下は、引き上げ AWS アカウント AWS リージョンることができる ごとの Amazon FSx for NetApp ONTAP のクォータです。

[リソース]	デフォルト	説明
ONTAP ファイルシステム	100	このアカウントに作成できる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 ストレージ容量の最大容量 (GiB 単位) です。
ONTAP スループットキャパシティ	10,240	このアカウントで使用できるすべての 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容量 (MBps 単位) です。
ONTAP SSD IOPS	1,000,000	このアカウントで使用できるすべての Amazon FSx for NetApp ONTAP ファイルシス

[リソース]	デフォルト	説明
		テムの SSD IOPS の最大量です。
ONTAP バックアップ	10,000	AWS アカウントで保持できるすべての Amazon FSx for NetApp ONTAP ファイルシステムについて、ユーザー主導ボリュームバックアップの最大数です。
Amazon S3 アクセスポイント	10,000	でリージョンごとに作成できる、サポートされているすべてのデータソースタイプ (FSx for NetApp ONTAP など) の Amazon S3 アクセスポイントの最大数 AWS アカウント。これは、単一の FSx for NetApp ONTAP ファイルシステムまたはボリュームにアタッチできる S3 アクセスポイントの最大数でもあります。このクォータは Amazon S3 サービスクォータであり、Service Quotas を使用して調整できます。

クォータの引き上げをリクエストするには

1. AWS サポート 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

次の表は、 AWS リージョン内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ています。

[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
減少オペレーションを開始するための最小 SSD ストレージ容量	HA ペアあたり 1,126 GiB
SSD の最小減少率	現在の容量より 9% 小さい
SSD の最大ストレージ容量	• 第 2 世代シングル AZ ファイルシステム: HA ペアあたり 512 TiB、最大 1 PiB • 第 2 世代マルチ AZ ファイルシステム: 512 TiB • 第 1 世代ファイルシステム: 192 TiB
SSD の推奨最大使用率	80% で最適なパフォーマンスと階層化機能を実現
削減オペレーションの最大 SSD 使用率	減少操作の前後で 80%

[リソース]	ファイルシステムあたりの制限
最大 SSD IOPS	第 2 世代ファイルシステム: • シングル AZ の場合、HA ペアあたり 200,000 (最大 12 ペア) • マルチ AZ の場合、合計 200,000 第 1 世代ファイルシステム: • 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 が利用可能な他のすべての AWS リージョン で 80,000
最小スループットキャパシティ	• 第 2 世代ファイルシステム (1 HA ペア): 384 MBps • 第 2 世代ファイルシステム (2 つ以上の HA ペア): HA ペアあたり 1,536 MBps • 第 1 世代ファイルシステム: 128 MBps

[リソース]	ファイルシステムあたりの制限
最大スループットキャパシティ	第 2 世代ファイルシステム: • シングル AZ の場合、73,728 MBps[1] • マルチ AZ の場合、6,144 MBps 第 1 世代ファイルシステム: • 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、4,096 MBps[2] • FSx for ONTAP が利用可能な他のすべての AWS リージョン で 2,048 MBps
ボリュームの最大数	• 第 2 世代ファイルシステム (1 HA ペア): 500 • 第 2 世代ファイルシステム (2 つ以上の HA ペア): 1,000 • 第 1 世代ファイルシステム: 500 ファイルシステムで S3 アクセスポイントを使用する場合: • 第 2 世代ファイルシステム (1 HA ペア): 491 • 第 2 世代ファイルシステム (2 つ以上の HA ペア): 2 つの HA ペアで 975 (12 の HA ペアで 903) • 第 1 世代ファイルシステム: 491
スナップショットの最大数	ボリュームあたり 1,023[3]

[リソース]	ファイルシステムあたりの制限
バックアップの最大数	ボリュームあたり 4,091[4]

[リソース]	ファイルシステムあたりの制限
SVM の最大数	1 つの HA ペアと IPv4 専用ネットワークタイプを持つ第 2 世代ファイルシステム: • 6 (384 MBps のスループットキャパシティ) • 6 (768 MBps のスループットキャパシティ) • 14 (1,536 MBps のスループットキャパシティ) • 14 (3,072 MBps のスループットキャパシティ) • 24 (6,144 MBps のスループットキャパシティ) 1 つの HA ペアとデュアルスタックネットワークタイプを持つ第 2 世代ファイルシステム: • 6 (384 MBps のスループットキャパシティ) • 6 (768 MBps のスループットキャパシティ) • 11 (スループット容量 1,536 MBps) • 11 (スループット容量 3,072 MBps) • 11 (スループット容量 6,144 MBps) 2 ~ 12 個の HA ペアを持ち、IPv4 専用またはデュアルスタックのネットワークタイプを持つ第 2 世代ファイルシステム: • 11

[リソース]	ファイルシステムあたりの制限
	IPv4 専用ネットワークタイプの第 1 世代ファイルシステム: • 6 (128 MBps のスループットキャパシティ) • 6 (256 MBps のスループットキャパシティ) • 14 (512 MBps のスループットキャパシティ) • 14 (1,024 MBps のスループットキャパシティ) • 24 (2,048 MBps のスループットキャパシティ) • 24 (4,096 MBps のスループットキャパシティ) デュアルスタックネットワークタイプの第 1 世代ファイルシステム: • 6 (128 MBps のスループットキャパシティ) • 6 (256 MBps のスループットキャパシティ) • 11 (512 MBps のスループットキャパシティ) • 11 (1,024 MBps のスループットキャパシティ) • 11 (2,048 MBps のスループットキャパシティ) • 11 (4,096 MBps のスループットキャパシティ)
タグの最大数	50

[リソース]	ファイルシステムあたりの制限
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
ファイルシステムあたりのサポートされるルートの最大数	50[5]
ファイルサーバーあたりのクライアント接続の最大数 [6]	100,000

Note

[1] 12 の HA ペア (HA ペアあたり 6,144 MBps) を持つ第 2 世代の Single-AZ ファイルシステムの場合。詳細については、「高可用性 (HA) ペアの管理」を参照してください。
[2] 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、FSx for ONTAP 第 1 世代のファイルシステムは、サポートされている AWS リージョンで最大 SSD IOPS (160,000) と最小 5,120 GiB の SSD スループットキャパシティを構成している必要があります。が 4,096 MBps のスループットキャパシティ AWS リージョン をサポートしている 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 のスナップショットをいつでも格納することができます。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 のバックアップをいつでも格納することができます。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] 1 つのファイルシステムごとに最大 50 のルートをいつでも設定することができます。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、持っている SVM 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。
[6] クライアント接続は、特定のファイルサーバーへの単一の TCP 接続として定義されます。ファイルシステムには、HA ペアごとに 1 つのアクティブなファイルサーバーがあります。クライアントは、ファイルサーバーへの複数の TCP 接続を持つことができます。例えば、クライアントがマルチパスを使用している場合です。

Amazon FSx for NetApp ONTAP のトラブルシューティング

次のセクションを使用して、FSx for ONTAP ファイルシステムのトラブルシューティングを行います。

トピック

- ファイルシステムがMISCONFIGURED状態にあります
- ファイルシステムにアクセスできません
- ストレージ仮想マシン (SVM) がMISCONFIGURED状態です
- SSD 削減オペレーションの問題のトラブルシューティング
- 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
- 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
- ボリュームがMISCONFIGURED状態になっています
- ボリュームのストレージ容量が不足している
- ボリューム容量不足によりバックアップが失敗する
- 削除された FSx for ONTAP ボリュームの復旧
- ネットワーク問題のトラブルシューティング

ファイルシステムが**MISCONFIGURED**状態にあります

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
- 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
- ファイルシステムの SSD ストレージ階層が 90% を超えています

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。
- オーナーアカウントが VPC サブネットの共有を停止しました。

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
```

この問題を解決するには、VPC サブネットを共有している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 を作成することはできません。

- 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。
- オーナーアカウントが VPC サブネットの共有を停止しました。

この問題を解決するには、VPC サブネットを共有している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。

ファイルシステムの SSD ストレージ階層が 90% を超えています

シングル AZ またはマルチ AZ ファイルシステムの SSD ストレージ階層の現在の使用率が 90% を超えています。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。ファイルシステムの次のメンテナンスウィンドウの前に SSD ストレージ階層の領域を解放しない場合、FSx for ONTAP はパッチ適用オペレーション中にファイルシステムのスループットを一時的にスロットルダウンします。これは、バックグラウンドメンテナンスプロセスが妥当な期間内に完了できるようにするために行われます。これを回避するには、SSD ストレージ階層の使用率を 90% 未満に減らしてください。SSD 使用率は、次のようないくつかの方法で削減できます:

- ファイルシステムの SSD ストレージ容量を増やす。

- 不要なデータを削除することによって。
- 不要なボリュームスナップショットを削除することによって。

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。

ファイルシステムにアクセスできません

このセクションでは、ファイルシステムにアクセスできないことに関連する問題と解決策について説明します。

トピック

- マルチ AZ ファイルシステムにルートテーブルタグがありません
- ファイルシステムに 50 以上のルートがあります
- ファイルシステムに 1 つ以上のファイルサーバーへのルートがありません
- 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 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停止しました
- 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

マルチ AZ ファイルシステムにルートテーブルタグがありません

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。ファイルシステムに関連付けられた 1 つ以上のルートテーブルに、現在これらのルートテーブルタグがありません。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。次のメンテナンスウィンドウの前にこれらの

タグを手動で追加しない場合、タグがないルートテーブルに関連付けられたサブネット内のクライアントは、パッチ適用オペレーション中に一時的にファイルシステムにアクセスできなくなります。これを回避するには、欠落しているルートテーブルタグを手動で追加してください。

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。

ファイルシステムに 50 以上のルートがあります

現在、ファイルシステムには 50 を超えるルートが関連付けられています。ファイルシステムの次のスケジュールされたメンテナンスウィンドウの前にこれらのルートの一部を削除しない場合、フェイルオーバープロセスに通常よりも時間がかかることがあります。これを回避するには、ルートの数を 50 未満に減らしてください。以下は、ファイルシステムに関連付けられたルートの数を減らすために実行できるステップです:

- 余分なルートの削除
- ファイルシステムに関連付けられている SVMs の数を減らす
- ファイルシステムに関連付けられたルートテーブルの数を減らす

詳細については、「ファイルシステムの更新」および「ストレージ仮想マシン (SVM) の削除」を参照してください。

ファイルシステムに 1 つ以上のファイルサーバーへのルートがありません

ファイルシステムには現在、1 つ以上のファイルサーバーへのルートがなく、既存のルートテーブルに新しいルートテーブルエントリを追加するのに十分なスペースがありません。ファイルシステムの次のスケジュールされたメンテナンスウィンドウの前に欠落しているルートを追加しない場合、接続されているクライアントはパッチ適用オペレーション中に切断されます。これを回避するには、欠落しているルートを追加してください。

詳細については、「ファイルシステムの更新」および「クォータ」を参照してください。

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 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 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停止しました

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た 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、「FSx for ONTAP 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) が**MISCONFIGURED**状態です

ストレージ仮想マシンがMISCONFIGURED状態になる原因は次のようにいくつかが考えられ、それぞれ解決策があります。

SVM にオフラインボリュームがあります

ファイルシステムには、オフライン状態のボリュームが含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。次回のファイルシステムのメンテナンスウィンドウまでにこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用作業の間、一時的にこのボリュームをオンラインにします。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように `volume online` ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、`-vserver`パラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

SVM には SCSI LUN または NVMe/TCP ネームスペースを持つオフラインボリュームがあります

ファイルシステムには、制限された状態にあるボリュームが含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。次回のファイルシステムのメンテナンスウィンドウまでにこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用作業の間、一時的にこのボリュームをオンラインにします。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

AWS Secrets Manager シークレットまたは KMS キーが正しく設定されていない

Amazon FSx は、Microsoft アクティブディレクトリのドメインコントローラー、またはコントローラーとの接続を確立できません。これは、 AWS Secrets Manager シークレット または AWS KMS key が正しく設定されていないためです。詳細については、「を使用した Active Directory 認証情報の保存 AWS Secrets Manager」を参照してください。

設定ミスを解決するには、次の手順を実行します:

- シークレット ARN が正しく、適切な形式に従っていることを確認します: arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars。
- シークレットに、空でない値を持つ両方の必須フィールドが含まれていることを確認します:
  - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME –AD サービスアカウントのユーザ名。
  - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD –AD サービスアカウントのパスワード。
- シークレットとキーに、シークレット値を取得するためのアクセス許可を Amazon FSx サービスプリンシパルfsx.amazonaws.comに付与するリソースベースのポリシーがあることを確認します。

SSD 削減オペレーションの問題のトラブルシューティング

このセクションでは、SSD 容量削減オペレーションに関連する一般的な問題と解決策について説明します。

トピック

- SSD の使用率が高いため、SSD の減少操作が一時停止しています
- FlexClone リレーションシップにより あなたの SSD 減少オペレーションが一時停止されています

- SSD の減少中にボリューム (複数可) のクライアントアクセスのリダイレクトが失敗しました
- SSD の減少操作に予想以上の時間がかかっています

SSD の使用率が高いため、SSD の減少操作が一時停止しています

SSD ストレージ階層の使用率が削減操作中に 80% を超える場合、Amazon FSx は自動的に操作を一時停止します。次のような管理アクションメッセージが表示されることがあります:

```
Your file system has insufficient free space in aggr_1. Please free up space or
 increase your file system's storage capacity.
```

使用率が 80% を下回ると、オペレーションが再開されます。この問題を解決するには、次の操作を行います:

- 新しいディスクに移動済みのボリュームから不要なデータを削除します。
- ボリューム階層化ポリシーを変更して、より多くのデータを容量プールに階層化します。
- 新しいターゲット値を指定して `update-file-system` を呼び出し、SSD 容量を増やす要求を送信します。

ファイルシステムの SSD ストレージ容量を更新して、ファイルシステムの SSD 容量が削減オペレーション後に 80% の使用率を超えないようにする必要があります。詳細については、ファイルシステム SSD ストレージと IOPS の更新を参照してください。

`STORAGE_OPTIMIZATION` 管理アクションの `Message`フィールドを確認することで、新しいディスクに移動されたボリュームを特定できます。

アグリゲートが`aggr1`または`aggr1_old`の場合は、`describe-volumes`を呼び出すこともできます。

FlexClone リレーションシップにより あなたの SSD 減少オペレーションが一時停止されています

SSD 削減操作を開始した後に FlexClone ボリュームが作成された場合、Amazon FSx はクローンが削除されるまで操作を一時停止します。これは、ONTAPがボリュームの移動中にクローン関係を分割し、その結果、新しいディスク上のストレージが重複するためです。この問題を解決するには、減少オペレーションの開始後に作成されたFlexCloneボリュームを特定して削除できます。

すべてのFlexCloneボリュームを削除すると、減少オペレーションが自動的に再開されます。

SSD の減少中にボリューム (複数可) のクライアントアクセスのリダイレクトが失敗しました

SSD 削減操作中、Amazon FSx は各ボリュームについて、クライアントアクセスを古いディスクから新しいディスクへリダイレクトする必要があります。このプロセスが失敗すると、次のような管理アクションメッセージが表示されることがあります:

```
Redirecting client access for volume(s) fsvol-123 has failed due to insufficient SSD
 IOPS, throughput capacity, or because the volume is full.
```

この問題を解決するには、次の操作を行います:

- Amazon CloudWatch でファイルシステムのリソース使用率メトリクスをチェックして、ワークロードが次のリソースの 50% 以上を消費していないことを確認します:
  - `NetworkThroughputUtilization`
  - `FileServerDiskThroughputUtilization`
  - `FileServerDiskIopsUtilization`
  - `CPUUtilization`
  - `DiskIopsUtilization`
- ボリュームがいっぱいの場合は、ボリュームのストレージ容量を増やします。
- 削減オペレーション中にファイルシステムのワークロードを減らします。

これらの問題に対処した後、Amazon FSx は 1 時間に 1 回クライアントアクセスのリダイレクトを自動的に再試行します。

SSD の減少操作に予想以上の時間がかかっています

SSD 削減操作の完了に要する時間は、ファイルシステムに保存されているデータ量、実行中のワークロードの活動状況、利用可能なシステムリソースなど、複数の要因によって異なります。オペレーションに予想以上に時間がかかる場合は、以下を実行できます:

- ファイルシステムに十分なリソースがある (CPU、ディスクスループット、SSD IOPS 使用率が 50% 未満) ことを確認します。
- オペレーション中に書き込み負荷の高いワークロードを減らして、リソースの競合を最小限に抑えます。

STORAGE_OPTIMIZATION 管理アクションで ProgressPercentプロパティを確認することで、オペレーションの進行状況を追跡できます。

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 Active Directory に接続する仕組み 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 は、 で Active Directory サービスアカウントの認証情報にアクセスできません AWS Secrets Manager
- 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 マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合するで説明されている手順に従って、SVM のアクティブディレクトリへの追加を再試行します。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、SVM の現在のアクティブディレクトリへ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 Active Directory への結合を解除する」を参照してください。
2. AWS マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合するで説明されている手順に従って、新しいアクティブディレクトリへの SVM の追加を再試行します。

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

セルフマネージドアクティブディレクトリに接続している SVM の作成に失敗し、次のエラーメッセージが表示される。

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 マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合する 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 は、 で Active Directory サービスアカウントの認証情報にアクセスできません AWS Secrets Manager

以下のセクションでは、一般的な問題とその解決方法について説明します。

SVM をセルフマネージド Active Directory に結合すると、次のエラーメッセージが表示されて失敗します。

```
You can't provide both username/password and a domain join service account
secret to connect to your Active Directory. Provide only one set of
credentials.
```

この問題を解決するには

1. Secrets Manager シークレットに保存されている認証情報を提供するか、プレーンテキストで提供するかを選択します。
2. Active Directory に参加するときは、これらのパラメータのいずれかのみを指定し、両方を指定しないでください。

SVM をセルフマネージド Active Directory に結合すると、次のエラーメッセージが表示されて失敗します。

```
The domain join service account secret ARN format you entered isn't
valid. Use the format: arn:partition:secretsmanager:region:account-
id:secret:secret-name-6chars
```

この問題を解決するには

1. 確認を使用した Active Directory 認証情報の保存 AWS Secrets Manager。

2. 入力する ARN 形式が正しいことを確認します。正しいフォーマットの例はarn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5fです。

SVM をセルフマネージド Active Directory に結合すると、次のエラーメッセージが表示されて失敗します。

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

この問題を解決するには

1. 確認を使用した Active Directory 認証情報の保存 AWS Secrets Manager。
2. 指定した Secrets Manager シークレットに、Amazon FSx がシークレットを使用できるようにする正しいポリシーがあることを確認します。

SVM をセルフマネージド Active Directory に結合すると、次のエラーメッセージが表示されて失敗します。

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

この問題を解決するには

- SecretsManager シークレットの所有者または管理者は、このシークレットを使用するためのアクセス権をアカウントに付与する必要があります。詳細については、アイデンティティベースのポリシー を参照してください。

SVM をセルフマネージド Active Directory に結合すると、次のエラーメッセージが表示されて失敗します。

```
The domain join service account secret format or content isn't valid. Make sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.
```

この問題を解決するには

1. 確認を使用した Active Directory 認証情報の保存 AWS Secrets Manager。
2. 指定する Secrets Manager シークレットに両方の必須フィールドがあることを確認します。

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 マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合する 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、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。指定された組織単位を使用して SVM をアクティブディレクトリドメインに参加させるために必要な委任されたアクセス許可がサービスアカウントにあることをご確認ください。
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 マネジメントコンソール AWS CLI および API を使用して SVMs を Active Directory に結合する 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 マネジメントコンソール、 AWS CLI、および API を使用した既存の SVM Active Directory 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参加させるためのアクセス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、次の手順で優先ドメインコントローラーを追加します。

a. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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-lookupNetApp ONTAP CLI コマンドを使用して、指定した DNS サーバまたは仮想サーバの DNS 構成での検索に基づいてホスト名の IP アドレスを返します。

a. ONTAPCLI 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 ファイルシステムまたは SVM 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、「ONTAP CLI 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 Active Directory ドメイン名の要件を確認します。参加しようとしている Active Directory がその要件を満たしていることを確認します。
2. AWS マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合するで説明されている手順に従って、SVM の Active Directory への参加を再試行してください。Active Directory 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。Active Directory 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 マネジメントコンソールAWS CLI および API を使用して SVMs を Active Directory に結合する 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 Active Directory 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たときに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 で提供します。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
- SVM 削除: ルートテーブルにアクセスできません
- SVM 削除: ピアリング関係
- SVM またはボリュームの削除: SnapMirror
- SVM 削除: Kerberos が有効の LIF
- SVM の削除: その他の理由
- ボリューム削除: FlexCache 関係

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、削除が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を以下のセクションに示し、これらの問題を解決する手順をステップバイステップで説明します。

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 ####.
```

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、ONTAP CLI 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

ピアリング関係のある SVM を削除するには、まずはピアリング関係を削除しなければならないのと同じように (SVM 削除: ピアリング関係 を参照)、SnapMirror 関係のある SVM も、まずは SnapMirror 関係を削除しないと削除できません。SnapMirror 関係を削除するには、ONTAP CLI を使用して SnapMirror 関係の対象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、ONTAP CLI 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、ファイルシステムのボリュームのポイントインタイム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、ターゲットファイルシステムの 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. ターゲット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、ONTAP CLI 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、CLI、API、またはコンソールを使用して SVM AWS 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、「ONTAP CLI 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
```

ボリューム削除: FlexCache 関係

FlexCache 関係の元のボリュームであるボリュームは、最初にキャッシュ関係を削除しない限り、削除できません。FlexCache の関係にあるボリュームを判別するには、ONTAP CLI を使用できます。ONTAP CLI にアクセスするには、ONTAP CLI 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。

ボリュームがMISCONFIGURED状態になっています

ONTAP ボリュームが MISCONFIGURED状態になる潜在的な原因はいくつかあります。以下のトピックで説明します。

ボリュームの使用率が 98% を超えています

現在、ファイルシステムのボリュームが 98% を超えています。ボリュームの使用率が常に 95% を超えないようにすることをお勧めします。ファイルシステムの次のメンテナンスウィンドウまでにボリュームの領域を解放しない場合、Amazon FSx はボリュームの便宜的ロックを無効にし、既存の「oplock」を解除します。Amazon FSx は、パッチ適用プロセスの完了後にボリュームでオプロックを再度有効にします。これを回避するには、ボリュームのストレージ容量使用率を 98% 未満に減らしてください。これを実現する方法には、次のようなものがあります:

- ボリュームのサイズを増やす。
- 不要なデータの削除。
- 不要なスナップショットの削除。

詳細については「ストレージ容量の更新」および「スナップショットの削除」を参照してください。

オフラインボリュームに iSCSI LUN または NVMe/TCP ネームスペースがあります

ファイルシステムは現在オフライン状態のボリュームをホストしており、そのボリュームには iSCSI LUN、NVMe/TCP ネームスペース、またはその両方が含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。次回のファイルシステムのメンテナンスウィンドウまでにこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用作業の間、一時的にこのボリュームをオンラインにします。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように `volume online` ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、`-vserver`パラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

オフラインボリュームはFlexCacheオリジンです

ファイルシステムには、オフライン状態の FlexCache オリジンボリュームが含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。次回のファイルシステムのメンテナンスウィンドウまでにこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用作業の間、一時的にこのボリュームをオンラインにします。この間、キャッシュボリュームのデータを使用してデータが FlexCache オリジンボリュームに書き戻される可能性があります。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

オフラインボリュームは、SnapMirror リレーションシップの一部です

ファイルシステムは現在オフライン状態のボリュームをホストしており、そのボリュームはSnapMirrorソースまたはデスティネーションです。ボリュームは継続的にオンラインにしておくことをお勧めします。ファイルシステムの次のメンテナンスウィンドウの前にこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用オペレーションの期間中、このボリュームを一時的にオンラインにし、SnapMirror関係を一時停止します。この間に、SnapMirrorソースボリュームのデータを使用してSnapMirror宛先ボリュームにデータが書き込まれる可能性があります。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

制限付きボリュームに iSCSI LUN または NVMe/TCP ネームスペースが含まれています

ファイルシステムは現在、制限された状態のボリュームをホストしており、そのボリュームには iSCSI LUN、NVMe/TCP 名前空間、またはその両方が含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。ファイルシステムの次のメンテナンスウィンドウの前にこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用オペレーションの期間中、このボリュームを一時的にオンラインにします。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

制限付きボリュームは FlexCache オリジンです

ファイルシステムには、制限された状態の FlexCache オリジンボリュームが含まれています。ボリュームは継続的にオンラインにしておくことをお勧めします。ファイルシステムの次のメンテナンスウィンドウの前にこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用オペレーションの期間中、このボリュームを一時的にオンラインにします。この間、キャッシュボリュームのデータを使用してデータが FlexCache オリジンボリュームに書き戻される可能性があります。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように volume online ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、-vserverパラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

あなたの制限されたボリュームは、SnapMirror リレーションシップの一部です

ファイルシステムは現在、制限された状態のボリュームをホストしており、そのボリュームはSnapMirrorソースまたはデスティネーションです。ボリュームは継続的にオンラインにしておくことをお勧めします。ファイルシステムの次のメンテナンスウィンドウの前にこのボリュームをオンラインにしない場合、Amazon FSx はパッチ適用オペレーションの期間中、このボリュームを一時的にオンラインにし、SnapMirror関係を一時停止します。この間に、SnapMirrorソースボリュームのデータを使用してSnapMirror宛先ボリュームにデータが書き込まれる可能性があります。これを回避するには、ボリュームをオンラインにするか削除してください。

オフラインボリュームをオンラインに戻すには、次の例に示すように `volume online` ONTAP CLI コマンドを使用します。SVM (V サーバー) が 1 つしか存在しない場合は、`-vserver`パラメーターを指定する必要はありません。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

ボリュームのストレージ容量が不足している

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することができます。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ができます。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、`volume autosize` NetApp ONTAP CLI コマンドを使用して、FSx for ONTAP のデフォルトのボリュームタイプである FlexVol 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、「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 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。

スナップショットを削除しても、削除しているスナップショットのサイズと等しいストレージ容量は再取得されません。スナップショットを削除することで再利用できるストレージの量を確認するには、volume snapshot compute-reclaimable-vserver ONTAP CLIコマンドを使用し、*svm_name*、*vol_name*、および *snapshot_name* を置き換えるデータを指定します。

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

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のモニタリング 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。

ボリューム容量不足により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する

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

ボリュームに空きストレージ容量が不足しているため、日次自動バックアップが失敗しています。この条件を軽減するには、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、次のオプションのうち 1 つ以上を使用して実現できます。

- 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

削除された FSx for ONTAP ボリュームの復旧

FSx for ONTAP ボリュームが削除されると、ONTAP's復旧キューに配置されます。ONTAP CLI を使用してこのキューから直接ボリュームを復旧できますが、復旧したボリュームは AWS コンソールや Amazon FSx API に表示されず、以前にボリュームに適用された AWS タグは完全に失われます。 AWS 統合とタグベースのセキュリティポリシーを維持しながら FSx for ONTAP のボリュームを適切に回復するには、バックアップを新しいボリュームに復元するか、SnapMirrorを使用してボリュームのデータを新しいボリュームにレプリケートします。ONTAP'sリカバリキューの詳細については、 NetApp'sドキュメント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。パケットトレースのプロセスをコントロールするときは、次の NetApp ONTAP CLI コマンドを使用します。

- 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 User Guide のNetApp ONTAP CLI の使用セクションに記載されている手順に従います。

```
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. 必要最小限の引数を使用してトレースを開始します。以下に置き換えます:

   - *node_name* をノードの名前に置き換えます (例: FsxId01234567890abcdef-01)。
   - *svm_name* をストレージ仮想マシンの名前に置き換えます (例: fsx)。
   - *junction_path_name* をボリュームの名前に置き換えます (例: 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*/*junction-path-name* の形式で含める必要があります:
- 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、*node-name _port-name_yyyymmdd_hhmmss*.trc の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、How to use debug network dump in ONTAP 9.10+in theNetApp Knowledge Base 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
- 最新のドキュメント更新: 2025 年 10 月 16 日

以下の表に、Amazon FSx NetApp ONTAP ユーザーガイドの重要な変更点を示します。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
Amazon FSx for NetApp ONTAP の Amazon S3 アクセスポイントのサポートが追加されました FSx NetApp	Amazon FSx for NetApp ONTAP の Amazon S3 アクセスポイントは、Amazon S3 API を使用して FSx for ONTAP ファイルシステムに保存されているデータにアクセスする新しい方法を提供します。 FSx NetApp Amazon S3 アクセスポイントを使用すると、既存のファイルシステム設定を変更することなく、Amazon S3-enabledアプリケーションのデータアクセスを簡素化できます。詳細については、「Amazon FSx for NetApp ONTAP での Amazon S3 アクセスポイント NetAppの使用」を参照してください。	2025 年 12 月 2 日
AWS Secrets Manager 統合のサポートが追加されました	Amazon FSx は、Active Directory 認証情報の管理を強化 AWS Secrets Manager するために と統合されるようになりました。詳細については、AWS Secrets Managerを	2025 年 11 月 5 日

	使用した Active Directory 認証情報の保存を参照してください。	
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx に新しいアクセス許可 が追加されました。これにより`secretsmanager:ListSecrets` 、プリンシパルはドメイン結合サービスアカウントの認証情報を選択 AWS Secrets Manager するために でシークレットを一覧表示できます。詳細については、「AWS managed policy: AmazonFSxFullAccess」を参照してください。	2025 年 11 月 5 日
NetApp BlueXP の名前を NetApp Console に変更	NetApp BlueXP は現在、NetApp Console と呼ばれています。詳細については、「Using NetApp Console」を参照してください。	2025 年 10 月 16 日

インターネットプロトコルバージョン 6 (IPv6) のサポートが追加されました	FSx for ONTAP ファイルシステムは、現在 2 つのネットワークタイプオプションをサポートしています。IPv4 のみ、ならびにデュアルスタック(IPv4 と IPv6 の両方)。ファイルシステムを作成するときは、これらのオプションのいずれかを指定する必要があります。既存の FSx for ONTAP ファイルシステムのネットワークタイプはいつでも変更できます。詳細については、「ネットワークの種類の管理」を参照してください。	2025 年 9 月 30 日
追加の AWS リージョン サポートが追加されました	第 2 世代 (マルチ AZ 2 およびシングル AZ 2) FSx for ONTAP ファイルシステムが、アジアパシフィック (ソウル)、カナダ (中部)、欧州 (スペイン)、欧州 (チューリッヒ) で利用可能になりました。アベイラビリティーゾーンの詳細については、「AWS リージョンによる使用可否」を参照してください。	2025 年 9 月 30 日
追加の AWS リージョン サポートが追加されました	FSx for ONTAP ファイルシステムがアジアパシフィック (台北) リージョンで利用可能になりました。アベイラビリティーゾーンの詳細については、「AWS リージョンによる使用可否」を参照してください。	2025 年 8 月 18 日

SSD ストレージ容量の削減のサポートが追加されました	FSx for ONTAP では、第 2 世代ファイルシステム上のファイルシステムのソリッドステートドライブ (SSD) ストレージ容量を削減できるようになりました。これにより、さまざまな高パフォーマンスストレージへのニーズがあるワークロードのストレージコストを最適化できます。詳細については、SSD ストレージ容量を削減するタイミングを参照してください。	2025 年 8 月 14 日
Amazon FSx が AmazonFSxServiceRolePolicy AWS 管理ポリシーを更新しました	Amazon FSx は、AmazonFSxServiceRolePolicy の `ec2:AssignIpv6Addresses` および `ec2:UnassignIpv6Addresses` アクセス許可を追加しました。詳細については、「Amazon FSx AWS 管理ポリシーの更新」を参照してください。	2025 年 7 月 22 日
Amazon FSx が AmazonFSxFullAccess AWS 管理ポリシーを更新しました	AmazonFSxFullAccess 管理ポリシーが更新され、`fsx:CreateAndAttachS3AccessPoint` 、`fsx:DescribeS3AccessPointAttachments` 、および `fsx:DetachAndDeleteS3AccessPoint` アクセス許可が追加されました。	2025 年 6 月 25 日

Amazon FSx が AmazonFSx ConsoleFullAccess AWS 管理ポリシーを更新しました	AmazonFSxConsoleFullAccess 管理ポリシーが更新され、`fsx:CreateAndAttachS3AccessPoint` 、`fsx:DescribeS3AccessPointAttachments` 、および`fsx:DetachAndDeleteS3AccessPoint` アクセス許可が追加されました。	2025 年 6 月 25 日
FSx for ONTAP は Amazon Elastic VMware Service をサポートしています	FSx for ONTAP を Amazon EVS の外部データストアとして使用できるようになりました。詳細については、「Using Amazon Elastic VMware Service with FSx for ONTAP」を参照してください。	2025 年 6 月 9 日
追加の AWS リージョン サポートが追加されました	第 2 世代 (マルチ AZ 2 およびシングル AZ 2) FSx for ONTAP ファイルシステムが、アジアパシフィック (東京) およびアジアパシフィック (ムンバイ) で利用可能になりました。アベイラビリティーゾーンの詳細については、「AWS リージョンによる使用可否」を参照してください。	2025 年 6 月 2 日
FlexCache ライトバックモードのサポートが追加されました	FSx for ONTAP ボリュームが FlexCache ライトバックモードをサポートするようになりました。詳細については、「Replicating your data with FlexCache」を参照してください。	2025 年 5 月 28 日

追加の AWS リージョン サポートが追加されました	FSx for ONTAP ファイルシステムが、アジアパシフィック (タイ) およびメキシコ (中部) で利用可能になりました。アベイラビリティーゾーンの詳細については、「AWS リージョンによる使用可否」を参照してください。	2025 年 5 月 8 日
Autonomous Ransomware Protection (ARP) がサポートされるようになりました	ランサムウェアやマルウェア攻撃を監視して保護する NetApp の AI 駆動機能である ARP が、FSx for ONTAP でサポートされるようになりました。詳細については、Autonomous Ransomware Protection によるデータ保護を参照してください	2025 年 4 月 7 日
「FSx for ONTAP ユーザーガイド」の新しいトピックでは、ワークグループで SMB サーバーを設定する方法について説明します	ワークグループ内の SMB サーバーのセットアップでは、SVM を Microsoft Active Directory に結合する代わりに、SVM 上のワークグループに SMB サーバーを設定する方法について説明します。	2025 年 3 月 4 日
Amazon FSx が AmazonFSxConsoleReadOnlyAccess AWS 管理ポリシーを更新しました	Amazon FSx は、AmazonFSxConsoleReadOnlyAccess ポリシーに `ec2:DescribeNetworkInterfaces` 権限を追加するように更新しました。詳細は「AmazonFSxConsoleReadOnlyAccess」のポリシーをご参照ください。	2025 年 2 月 25 日

追加の Harvest ダッシュボードがサポートされるようになりました	デフォルトで有効になっていないダッシュボードを含め、追加の Harvest ダッシュボードが FSx for ONTAP でサポートされるようになりました。FSx for ONTAP がサポートしていないダッシュボードのリストも追加されました。詳細については、「Monitoring FSx for ONTAP file systems using Harvest and Grafana」を参照してください。	2025 年 2 月 18 日
FSx for ONTAP ユーザーガイドに新しい FSx for ONTAP 請求および使用状況レポートトピックが追加されました	AWS FSx for ONTAP の請求と使用状況レポートトピックでは、 AWS Billing and Cost Management コンソールで FSx for ONTAP ファイルシステムの使用状況レポートにアクセスする方法について説明します。また、両方のレポートで FSx for ONTAP に固有のすべての使用タイプを提供します。	2025 年 2 月 13 日
Amazon FSx のデュアルスタック VPC インターフェイスエンドポイントのサポートが追加されました	Amazon FSx のデュアルスタック VPC インターフェイスエンドポイントを、IPv4 および IPv6 IP アドレスと DNS 名の両方で作成できるようになりました。詳細については、「Amazon FSx and interface VPC endpoints」を参照してください。	2025 年 2 月 7 日

デュアルスタック API エンドポイント (IPv4 と IPv6) のサポートを追加	ファイルシステムを作成および管理するための Amazon FSx サービス API には、新しいデュアルスタックエンドポイントがあります。詳細については、「Amazon FSx API Reference」の「API endpoints」を参照してください。	2025 年 2 月 7 日
Amazon FSx が AmazonFSx ConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx が AmazonFSx ConsoleFullAccess ポリシーを更新し、`ec2:DescribeNetworkInterfaces` アクセス権限を追加しました。詳細は「AmazonFSx ConsoleFullAccess」のポリシーをご参照ください。	2025 年 2 月 7 日
FlexCache 新しいトピックを使用したデータのレプリケーションが公開されました	FlexCache を使用してオンプレミスの ONTAP ファイルシステムのデータを FSx for ONTAP ファイルシステムにレプリケートする方法を説明する新しいトピックが公開されました。詳細については、FlexCache によるデータのレプリケーションを参照してください。	2024 年 12 月 19 日

第 2 世代ファイルシステムのサポートが追加されました	第 2 世代のシングル AZ およびマルチ AZ ファイルシステムを作成できるようになりました。単一の高可用性 (HA) ペアで、最大 6 GBps のスループットキャパシティと 200,000 SSD IOPS を実現しました。詳細については、「高可用性 (AZ) ペア」を参照してください。	2024 年 7 月 9 日
バックアップから復元されている間にボリュームからデータを読み取るためのサポートが追加されました	第 2 世代のファイルシステムでバックアップから復元されている間、ファイルデータへの読み取り専用アクセスを持つボリュームをマウントできるようになりました。詳細については、「新しいボリュームへのバックアップの復元」を参照してください。	2024 年 7 月 9 日
第 2 世代ファイルシステムのスループットキャパシティの調整のサポートが追加されました	作成後に、第 2 世代ファイルシステムのスループットキャパシティを調整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。	2024 年 7 月 9 日

第 2 世代シングル AZ ファイルシステムに HA ペアを追加するためのサポートが追加されました	作成後に、HA ペアを第 2 世代シングル AZ ファイルシステムに追加できるようになりました。第 2 世代シングル AZ ファイルシステムでは、合計 12 の HA ペアを使用できます。詳細については、「高可用性 (HA) ペアの追加」を参照してください。	2024 年 7 月 9 日
TCP (NVMe /TCP) プロトコルでの非揮発性メモリエクスプレスのサポートが追加されました	Amazon FSx for NetApp ONTAP ファイルシステムのデータ転送に NVMe/TCP プロトコルを使用できるようになりました。詳細については、「ブロックストレージプロトコルの使用」を参照してください。	2024 年 7 月 9 日
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	`fsxadmin-readonly` ロールが ONTAP ファイルシステム管理ユーザーで使用できるようになり、NetApp Harvest 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るようになりました。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、「ONTAP ユーザー の Active Directory 認証の設定」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の 12 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 の HA ペアを持つファイルシステムは、12 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」と「Amazon FSx for NetApp ONTAP のパフォーマンス」を参照してください。	2024 年 3 月 4 日
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、「ボリュームでクラウド書き込みモードを有効にする」を参照してください。	2024 年 2 月 6 日

で FlexGroup ボリュームをバックアップするため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 ファイルシステムで 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 は、AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess、および AmazonFSxServiceRolePolicy AWS 管理ポリシーを更新しました。	Amazon FSx に、AmazonFSxFullAccess、AmazonFSxConsoleFullAccess、AmazonFSxReadOnlyAccess、AmazonFSxConsoleReadOnlyAccess、および AmazonFSxServiceRolePolicy ポリシーを更新して、`ec2:GetSecurityGroupsForVpc` アクセス許可が追加されました。詳細については、「Amazon FSx AWS 管理ポリシーの更新」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 で、AmazonFSxFullAccess ポリシーと AmazonFSxConsoleFullAccess ポリシーが更新され、`ManageCrossAccountDataReplication` アクションが追加されました。詳細については、「Amazon FSx AWS 管理ポリシーの更新」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 では、複数の HA ペアを持つファイルシステムの Amazon CloudWatch メトリクスが提供され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 では、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 を実現できる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。詳細については、「高可用性 (HA) ペア」と「Amazon FSx for NetApp ONTAP のパフォーマンス」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 で、AmazonFSxFullAccess ポリシーと AmazonFSxConsoleFullAccess ポリシーが更新され、`fsx:CopySnapshotAndUpdateVolume` アクセス許可が追加されました。詳細については、「Amazon FSx AWS 管理ポリシーの更新」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 で、AmazonFSxFullAccess ポリシーと AmazonFSxConsoleFullAccess ポリシーが更新され、`fsx:DescribeSharedVPCConfiguration` アクセス許可と `fsx:UpdateSharedVPCConfiguration` アクセス許可が追加されました。詳細については、「Amazon FSx updates to AWS managed policies」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、追加の ONTAP ロールとユーザーを作成して、ONTAP CLI と REST API を使用する際のユーザー権限と特権を定義できるようになりました。詳細については、「Roles and users in Amazon FSx for NetApp ONTAP」を参照してください。	2023 年 9 月 6 日
CloudWatch 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のサポートを追加	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、「Amazon CloudWatch によるモニタリング」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 `cloudwatch:PutMetricData` アクセス許可を更新しました。詳細については、「Amazon FSx updates to AWS managed policies」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を追加	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、「Using NetApp System Manager with BlueXP」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。EMS イベントを、NetApp ONTAP CLI を使用して閲覧できます。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、SnapLock を使用した Compliance 保存モードと Enterprise 保存モードをサポートしています。詳細については、「Working with 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 が AmazonFSx FullAccess ポリシーを更新し、`fsx:*` アクセス権限を削除し、特定の `fsx` アクションを追加しました。詳細については、「AmazonFSx FullAccess」の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 が AmazonFSx ConsoleFullAccess ポリシーを更新し、`fsx:*` アクセス権限を削除し、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」の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	および AWS CLI API を使用して AWS マネジメントコンソール、既存のストレージ仮想マシンを Active Directory に結合できます。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を追加	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 で転送中のデータを暗号化する」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 関係の対象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を追加 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独立してストレージをスケールアップまたはスケールダウンする柔軟性が提供されます。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開発済みのカスタマイズ可能な 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を実行できるようになりました。詳細については、「Amazon FSx AWS Backup で を使用する」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 CloudWatch 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 CloudWatch は、FSx for ONTAP から raw データを収集して処理し、読み取り可能なほぼリアルタイムのメトリクスに変換します。詳細については、「Amazon CloudWatch によるモニタリング」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 MBps および 256 MBps 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 が一般公開されるようになりました	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、機能が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。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、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。