Windows ユーザーガイド

Amazon FSx for Windows File Server

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon FSx for Windows File Server: Windows ユーザーガイド

Copyright © 2025 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使用してはならず、どんな形でも、お客様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することはできません。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

FSx for Windows ファイルサーバーとは？ ... 1
Amazon FSx リソース ... 1
ファイル共有へのアクセス ... 2
セキュリティとデータ保護 ... 3
可用性と耐久性 ... 3
ファイルシステムを管理する ... 3
料金とパフォーマンスの柔軟性 ... 4
Amazon FSx の料金 ... 4
前提 ... 4
前提条件 ... 5
Amazon FSx for Windows File Server フォーラム ... 5
Amazon FSx を初めて使用しますか? ... 6
FSx for Windows のベストプラクティス ... 7
一般的なベストプラクティス ... 7
モニタリングプランの作成 ... 7
ファイルシステムに十分なリソースがあることの確認 ... 7
セキュリティに関するベストプラクティス ... 7
ネットワークセキュリティ ... 8
アクティブディレクトリ ... 8
Active Directory の設定ミスによる可用性の低下を回避する ... 9
Windows ACL ... 10
ファイルシステムの設定と適切なサイズ ... 10
デプロイタイプの選択 ... 10
スループットキャパシティの選択 ... 10
ストレージ容量とスループット容量の増加 ... 11
アイドル期間中のスループットキャパシティの変更 ... 11
入門 ... 13
のセットアップ AWS アカウント ... 13
... 14
ステップ 1. Active Directory のセットアップ ... 16
ステップ 2: Amazon EC2 コンソールで Windows インスタンスを起動する ... 17
ステップ 3: インスタンスに接続する ... 19
ステップ 4: インスタンスを AWS Directory Service ディレクトリに結合する ... 21
ステップ 5. ファイルシステムを作成 ... 23

ステップ 6。Windows サーバーを実行する EC2 インスタンスへファイル共有をマッピングします ... 29
ステップ 7。ファイル共有にデータを書き込む ... 30
ステップ 8: ファイルシステムをバックアップする ... 31
ステップ 9。リソースをクリーンアップする ... 31
データへのアクセス ... 33
サポートされているクライアント ... 33
内からのデータへのアクセス AWS クラウド ... 34
別の VPC AWS アカウントからのデータへのアクセス AWS リージョン ... 36
オンプレミスからデータにアクセスする ... 36
デフォルトの DNS 名を使用したデータへのアクセス ... 37
DNS 名を使用した Kerberos 認証の使用 ... 38
分散ファイルシステム (DFS) 名前空間のサポート ... 38
DNS エイリアスを使用したデータへのアクセス ... 39
Kerberos 認証と DNS エイリアスを使用した暗号化の使用 ... 39
DNS エイリアスをファイルシステムに関連付ける ... 40
Kerberos のサービスプリンシパル名 (SPN) を設定する ... 41
DNS CNAME レコードを更新または作成する ... 45
グループポリシーオブジェクト (GPO) を使用した Kerberos 認証の強制 ... 47
ファイル共有を使用したデータへのアクセス ... 48
ファイル共有のマッピング ... 48
Amazon EC2 Windows インスタンスでのファイル共有のマッピング ... 49
Amazon EC2 Mac インスタンスへのファイル共有のマウント ... 51
Amazon EC2 Linux インスタンスへのファイル共有のマウント ... 54
Amazon EC2 Linux インスタンスへのファイル共有の自動マウント ... 60
ファイル共有の管理 ... 63
New-FsxsmbShare コマンドが一方向の信頼で失敗する ... 69
可用性と耐久性 ... 70
シングル AZ またはマルチ AZ ファイルシステムのデプロイタイプを選択する ... 70
デプロイタイプがサポートする機能 ... 71
フェイルオーバープロセス ... 71
Windows のクライアントでのフェイルオーバーのエクスペリエンス ... 72
Linux のクライアントでのフェイルオーバーのエクスペリエンス ... 72
ファイルシステムでフェイルオーバーをテストする ... 73
シングル AZ およびマルチ AZ ファイルシステムリソース ... 73
サブネット ... 73

ファイルシステム Elastic Network Interface 74
アクティブディレクトリの使用 76
の使用 AWS Managed Microsoft AD 77
ネットワークの前提条件 78
リソースフォレスト分離モデルの使用 84
アクティブディレクトリの設定をテストする 84
異なる VPC またはアカウント AWS Managed Microsoft AD での の使用 85
アクティブディレクトリドメインコントローラーへの接続の検証 86
セルフマネージド Active Directory を使用する 89
前提条件 91
セルフマネージド Active Directory を使用する場合のベストプラクティス 97
Amazon FSx サービスアカウント 98
Amazon FSx への権限の委任 99
アクティブディレクトリ設定の検証 101
FSx をセルフマネージドアクティブディレクトリに結合させる 105
手動 DNS エントリの IP アドレスの取得 115
セルフマネージド Active Directory の更新 116
Amazon FSx サービスアカウントの変更 118
セルフマネージドアクティブディレクトリの更新のモニタリング 120
パフォーマンス 124
ファイルシステムのパフォーマンス 124
パフォーマンスに関するその他の考慮事項 125
レイテンシー 126
スループットと IOPS 126
シングルクライアントパフォーマンス 126
バーストパフォーマンス 126
スループットキャパシティとパフォーマンス 127
スループットキャパシティの選択 130
ストレージ構成とパフォーマンス 131
HDD バーストパフォーマンス 132
例: ストレージ容量とスループットキャパシティ 132
CloudWatch メトリクスを使用したパフォーマンスの測定 133
パフォーマンスのトラブルシューティング 133
ファイルシステムのスループットと IOPS 制限を決定する 134
ネットワーク I/O とディスク I/O の違いは何ですか? これらが異なる理由を教えてください。 134

ネットワーク I/O が低いのに CPU やメモリの使用率が高いのはなぜですか? 135
バーストとは何ですか? 私のファイルシステムではどのくらいのバーストが使用されてるでしょうか? バーストクレジットがなくなるとどうなりますか? 135
[Monitoring & performance] (モニタリングとパフォーマンス) ページに警告が表示されます。ファイルシステムの設定を変更する必要はありますか? 136
メトリクスが一時的に消えてしまいました。どうすればよいですか? 136
ファイルシステムの管理 138
Amazon FSx ファイルシステムのステータス 139
PowerShell での Amazon FSx CLI の使用 140
Amazon FSx リモート PowerShell セッションの開始 142
1 回限りのファイルシステムセットアップタスク 143
ストレージの消費量の管理 143
シャドウコピーを有効にして、エンドユーザーがファイルやフォルダを以前のバージョンにリカバリできるようにする 144
転送時の暗号化の強制 144
PowerShell での Amazon FSx CLI へのアクセスのトラブルシューティング 145
ファイルシステムのセキュリティグループには、リモート PowerShell 接続を許可するために必要なインバウンドルールがありません 145
AWS マネージド Microsoft Active Directory とオンプレミス Active Directory の間に外部信頼が設定されている 145
リモート PowerShell セッションを開始しようとすると、言語ローカライズエラーが発生します 145
メンテナンスウィンドウ 146
週次メンテナンスウィンドウを変更する 147
DNS エイリアス 147
DNS エイリアスのステータス 150
Kerberos での DNS エイリアスの使用 150
既存の DNS エイリアスの表示 151
DNS エイリアスとファイルシステムの関連付け 151
既存のファイルシステム上の DNS エイリアスを管理する 153
ユーザーセッションと開いているファイル 156
GUI を使用してユーザーとセッションを管理する 156
PowerShell を使用してユーザーセッションを管理し、ファイルを開く 159
ストレージの管理 160
ストレージコストの最適化 161
ストレージ容量の管理 161

ストレージタイプの管理 165
SSD IOPS の管理 166
データ重複除外 167
ストレージクォータの管理 171
ストレージ容量を増やす 173
ストレージの増加のモニタリング 174
ストレージ容量を動的に増やす 178
ストレージタイプの更新 183
ストレージタイプの更新をモニタリング 184
SSD IOPS の更新 185
プロビジョニングされた SSD IOPS 更新のモニタリング 186
データ重複除外の管理 187
データ重複排除のトラブルシューティング 191
DFS 名前空間の使用 193
DFS 名前空間の使用 193
シャードによるパフォーマンスの向上 194
ファイルシステムを 1 つの名前空間にグループ化する 195
スケールアウトパフォーマンスのための DFS 名前空間を使用したデータのシャーディング 196
スループット容量の管理 198
スループットスケーリングの仕組み 199
スループットキャパシティを変更するタイミングを知る 200
スループットキャパシティの変更 201
スループットキャパシティの更新のモニタリング 202
リソースのタグ付け 204
タグの基本 205
リソースのタグ付け 205
タグの制限 206
リソースにタグを付けるために必要なアクセス許可 207
を使用してファイルシステムを更新する AWS CLI 207
データの保護 209
バックアップでデータを保護する。 209
自動の日次バックアップの操作 211
ユーザー主導のバックアップ機能 212
Amazon FSx AWS Backup での の使用 212
バックアップのコピー 213

新しいファイルシステムへのバックアップの復元 215
ユーザーによるバックアップの作成 216
バックアップの削除 217
バックアップのサイズ 218
バックアップのコピー 219
バックアップの復元 220
シャドウコピーによるデータの保護 221
ベストプラクティス 222
シャドウコピーのセットアップ 223
デフォルト設定を使用するようにシャドウコピーを設定する 228
シャドウコピーストレージの最大量の設定 230
シャドウコピーストレージを表示する 232
カスタムシャドウコピースケジュールを作成する 233
シャドウコピースケジュールの表示 235
シャドウコピーの作成 235
既存のシャドウコピーの表示 235
シャドウコピーの削除 236
シャドウコピースケジュールの削除 237
シャドウコピー設定の削除 238
シャドウコピーのトラブルシューティング 238
スケジュールされたレプリケーション 240
FSx for Microsoft SQL Server で FSx for Windows File Server の使用 241
アクティブ SQL Server データファイルに Amazon FSx を使用する 241
継続的に利用可能な共有を作成する 242
SMB のタイムアウト設定を構成する 242
Amazon FSx を SMB ファイル共有監視として使用する 242
Amazon FSx への移行 243
FSx for Windows File Server にファイルを移行する 243
移行のベストプラクティス 244
を使用したファイルの移行 AWS DataSync 244
Robocopy を使用したファイルの移行 248
ファイル共有設定の移行 252
オンプレミス DNS 設定の FSx for Windows File Server への移行 254
FSx for Windows File Server へのカットオーバー 257
Amazon FSx へのカットオーバーの準備 257
Kerberos 認証用の SPN の設定 258

Amazon FSx ファイルシステムの DNS CNAME レコードを更新する 261
ファイルシステムのモニタリング 263
自動モニタリングと手動モニタリング 263
自動ツール 263
手動モニタリングツール 264
Amazon CloudWatch によるモニターリング 265
メトリクスとディメンション 267
CloudWatch メトリクスの使用 272
パフォーマンスの警告と推奨事項 277
ファイルシステムメトリクスへのアクセス 279
CloudWatch アラームの作成 284
CloudTrail ログ 287
CloudTrail 内の Amazon FSx 情報 287
Amazon FSx ログファイルエントリの概要 288
セキュリティ 291
データ保護 292
データ暗号化 293
保管中の暗号化 293
転送中の暗号化 295
Windows ACL 297
関連リンク 298
Amazon VPC を使用したファイルシステムアクセスコントロール 298
Amazon VPC セキュリティグループ 299
Amazon VPC ネットワーク ACL 303
エンドユーザーアクセスのログ記録 303
監査イベントログの宛先 304
監査コントロールの移行 306
イベントログの表示 306
ファイルとフォルダの監査コントロールの設定 314
ファイルアクセス監査の管理 316
Identity and Access Management 321
対象者 321
アイデンティティを使用した認証 322
ポリシーを使用したアクセスの管理 326
Amazon FSx for Windows File Server と IAM の連携の仕組み 328
アイデンティティベースのポリシーの例 335

AWS マネージドポリシー 338
トラブルシューティング 355
Amazon FSx でのタグの使用 357
サービスにリンクされたロールの使用 362
コンプライアンス検証 369
インターフェイス VPC エンドポイント 370
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 370
Amazon FSx API 用のインターフェイス VPC エンドポイントの作成 371
Amazon FSx 用の VPC エンドポイントポリシーの作成 372
他の サービスでの使用 373
Amazon AppStream 2.0 で Amazon FSx を使用する 373
個人用の永続的ストレージを各ユーザーに提供する 374
ユーザー間で共有フォルダを提供する 376
Amazon Kendra で FSx for Windows ファイルサーバーを使用する 377
ファイルシステムのパフォーマンス 378
クォータ 379
増やすことができるクォータ 379
ファイルシステムあたりのリソースクォータ 380
追加の考慮事項 381
Microsoft Windows 固有のクォータ 382
トラブルシューティング 383
ファイルシステムにアクセスできない 383
ファイルシステム Elastic Network Interface が変更または削除されました 384
ファイルシステム Elastic Network Interface に接続された Elastic IP アドレスが削除されました 384
ファイルシステムのセキュリティグループには、必要なインバウンドまたはアウトバウンドルールがありません。 384
コンピューティングインスタンスの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 384
アクティブディレクトリに結合していないコンピューティングインスタンス 384
ファイル共有は存在しません 385
アクティブディレクトリユーザーに必要な許可がありません 385
削除されたフルコントロール許可の NTFS ACL 許可 385
オンプレミスのクライアントを使用してファイルシステムにアクセスできない 386
新しいファイルシステムは DNS に登録されていません 386
DNS エイリアスを使用してファイルシステムにアクセスできない 387

IP アドレスを使用してファイルシステムにアクセスすることができない 388
ファイルシステムの作成が失敗する 389
VPC セキュリティグループの設定ミス 389
ファイルシステム管理者グループ名の重複 389
DNS サーバーまたはドメインコントローラーに到達できない 390
サービスアカウントの認証情報が無効 392
サービスアカウントのアクセス許可が不十分 393
サービスアカウントの容量超過 394
OU にアクセスできない 394
ファイルシステム管理グループが不正 395
ドメインで Amazon FSx の接続が失われた 396
サービスアカウントに正しいアクセス許可がない 396
作成パラメータで使用される Unicode 文字 397
バックアップの復元中にストレージタイプを HDD に切り替えると失敗する 398
ファイルシステムが正しく設定されていない状態です 398
誤って設定されたファイルシステム: Amazon FSx は、ドメインの DNS サーバーまたはドメインコントローラーのいずれにも到達できません。 400
ファイルシステムの設定ミス: サービスアカウントの認証情報が無効です 401
ファイルシステムの設定ミス: 提供されたサービスアカウントには、ファイルシステムをドメインに結合させる許可がありません 401
ファイルシステムの設定ミス: サービスアカウントは、これ以上コンピュータをドメインに結合させることができません 402
ファイルシステムの設定ミス: サービスアカウントが OU にアクセスできません 402
マルチ AZ またはシングル AZ 2 ファイルシステムで DFS-R を設定することができない 403
ストレージまたはスループットキャパシティの更新が失敗する 403
Amazon FSx がファイルシステムの にアクセスできないため、ストレージ容量の増加は失敗します。 AWS KMS key 403
セルフマネージドアクティブディレクトリの設定ミスのため、ストレージまたはスループットキャパシティの更新に失敗する 404
スループットキャパシティが不十分なため、ストレージ容量の増加に失敗する 404
スループットキャパシティを 8 MBps に更新できない 405
ドキュメント履歴 406
..... cdxxii

FSx for Windows ファイルサーバーとは？

Amazon FSx for Windows File Server は、フルマネージドの Microsoft Windows ファイルサーバーで、完全にネイティブの Windows ファイルシステムでバックアップされています。FSx for Windows ファイルサーバーには、エンタープライズアプリケーションを簡単にリフトアンドシフト AWS クラウドに移行するための機能、パフォーマンス、および互換性があります。

Amazon FSx は、Microsoft Windows Server 上に構築されたフルマネージド型ファイルストレージを使用して、幅広いエンタープライズ Windows ワークロードをサポートします。Amazon FSx は、Windows ファイルシステム機能と、ネットワーク経由でファイルストレージにアクセスするための業界標準のサーバーメッセージブロック (SMB) プロトコルをネイティブでサポートしています。Amazon FSx は、Windows のネイティブ互換性 AWS クラウド、エンタープライズのパフォーマンスと機能、一貫したミリ秒未満のレイテンシーにより、 のエンタープライズアプリケーション向けに最適化されています。

Amazon FSx のファイルストレージを使用すると、Windows のデベロッパーや管理者が今日使用しているコード、アプリケーション、およびツールを変更することなく引き続き使用できます。Amazon FSx に最適な Windows アプリケーションとワークロードには、ビジネスアプリケーション、ホームディレクトリ、ウェブ配信、コンテンツ管理、データ分析、ソフトウェアビルド設定、およびメディア処理ワークロードが含まれます。

フルマネージドサービスとして、FSx for Windows ファイルサーバーは、ファイルサーバーとストレージボリュームのセットアップとプロビジョニングの管理オーバーヘッドを排除します。さらに、Amazon FSx は Windows ソフトウェアを最新の状態に保ち、ハードウェア障害を検出して対処し、バックアップを実行します。また、AWS IAM、、Amazon WorkSpacesAWS Directory Service for Microsoft Active Directory、、 AWS Key Management Serviceなどの他の AWS サービスとの豊富な統合も提供しますAWS CloudTrail。

FSx for Windows ファイルサーバーリソース: ファイルシステム、バックアップ、ファイル共有

Amazon FSx の主なリソースは、ファイルシステム と バックアップ です。ファイルシステムとは、ファイルやフォルダを保存してアクセスする場所です。ファイルシステムは、1 つまたは複数の Windows ファイルサーバーとストレージボリュームで設定されています。ファイルシステムを作成するときは、ストレージ容量 (GiB 単位) 、SSD IOPS、スループット容量 (MBps 単位) を指定します。ファイルシステムの作成後、ニーズの変化に応じて、これらのプロパティを変更できます。詳細

についてはストレージ容量の管理、SSD IOPS の管理、およびスループット容量の管理を参照してください。

FSx for Windows ファイルサーバーバックアップは、ファイルシステムの一貫性、高い耐久性、および増分バックアップです。ファイルシステムの整合性を確保するために、Amazon FSx は Microsoft Windows のボリュームシャドウコピーサービス (VSS) を使用します。自動日次バックアップは、ファイルシステムの作成時にデフォルトでオンになっています。また、いつでも追加の手動バックアップを取ることもできます。詳細については、「バックアップでデータを保護する。」を参照してください。

Windows ファイル共有は、ファイルシステム内の特定のフォルダー (およびそのサブフォルダー) で、SMB を使用してコンピューティングインスタンスにアクセスできるようにします。ファイルシステムには、既に「`\share`」というデフォルトの Windows ファイル共有が付属しています。Windows の共有フォルダグラフィカルユーザーインターフェイス (GUI) ツールを使用して、他の Windows ファイル共有を必要な数だけ作成と管理ができます。詳細については、「ファイル共有を使用したデータへのアクセス」を参照してください。

ファイル共有にアクセスするには、ファイルシステムの DNS 名またはファイルシステムに関連付けた DNS エイリアスのいずれかを使用します。詳細については、「DNS エイリアスを管理する」を参照してください。

ファイル共有へのアクセス

Amazon FSx は、SMB プロトコル (バージョン 2.0 から 3.1.1 をサポート) のコンピューティングインスタンスからアクセスできます。共有には、Windows Server 2008 および Windows 7 以降のすべての Windows バージョン、および現在のバージョンの Linux からアクセスできます。Amazon FSx ファイル共有は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、WorkSpaces インスタンス、Amazon AppStream 2.0 インスタンス、VMware Cloud AWS VMsにマッピングできます。

AWS Direct Connect または AWS VPNを使用して、オンプレミスコンピューティングインスタンスからファイル共有にアクセスできます。ファイルシステム AWS リージョン と同じ VPC、 AWS アカウント、および にあるファイル共有にアクセスすることに加えて、別の Amazon VPC、アカウント、または にあるコンピューティングインスタンスから共有にアクセスすることもできます AWS リージョン。VPC ピアリングまたはトランジットゲートウェイを使用して行います。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」を参照してください。

セキュリティとデータ保護

Amazon FSx は、ユーザーのデータが確実に保護されるよう、複数のレベルのセキュリティとコンプライアンスを提供します。() で管理するキーを使用して、保管中のデータ (ファイルシステムとバックアップの両方) を自動的に暗号化します AWS Key Management Service AWS KMS。送信中のデータは、SMB Kerberos セッションキーを使用して自動的に暗号化されます。ISO、PCI-DSS、SOC の認定に準拠していることが評価されており、HIPAA 資格があります。

Amazon FSx は、Windows アクセスコントロールリスト (ACL) を使用して、ファイルおよびフォルダーレベルでのアクセスコントロールを提供します。Amazon Virtual Private Cloud (Amazon VPC) セキュリティグループを使用して、ファイルシステムレベルでアクセスコントロールを提供します。また、 AWS Identity and Access Management (IAM) アクセスポリシーを使用して、API レベルでのアクセスコントロールを提供します。ファイルシステムにアクセスするユーザーは、Microsoft アクティブディレクトリで認証されます。Amazon FSx は と統合 AWS CloudTrail して API コールをモニタリングおよびログ記録するため、Amazon FSx リソースでユーザーが実行したアクションを確認できます。

さらに、日常的にファイル・システムの高い耐久性バックアップを自動的に作成することでデータを保護し、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、「Amazon FSx のセキュリティ」を参照してください。

可用性と耐久性

FSx for Windows ファイルサーバーは、2 つのレベルの可用性と耐久性を備えたファイルシステムを提供します。シングル AZ ファイルは、コンポーネントの障害を自動的に検出および対処することにより、単一のアベイラビリティーゾーン (AZ) 内の高可用性を保証します。さらに、マルチ AZ ファイルシステムは、 AWS リージョン内の別のアベイラビリティーゾーンにスタンバイファイルサーバーをプロビジョニングして維持することで、複数のアベイラビリティーゾーンにわたって高可用性とフェイルオーバーサポートを提供します。シングル AZ とマルチ AZ のファイルシステムのデプロイについては、「可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム」を参照してください。

ファイルシステムを管理する

FSx for Windows ファイルサーバーを管理するには、カスタムリモート管理 PowerShell コマンドを使用するか、場合によっては Windows ネイティブ GUI を使用します。Amazon FSx ファイルシステムの管理の詳細については、「FSx for Windows ファイルシステムの管理」を参照してください。

料金とパフォーマンスの柔軟性

FSx for Windows ファイルサーバーでは、ソリッドステートドライブ (SSD) とハードディスクドライブ (HDD) の両方のストレージタイプを提供することで、料金とパフォーマンスの柔軟性を提供します。HDD ストレージは、ホームディレクトリ、ユーザーと部門の共有、コンテンツ管理システムなど、幅広いワークロード向けに設計されています。SSD ストレージは、データベース、メディア処理ワークロード、データ分析アプリケーションなど、最もパフォーマンスが高く、レイテンシーの影響を受けやすいワークロード向けに設計されています。

FSx for Windows ファイルサーバーを使用すると、ファイルシステムのストレージと SSD IOPS、スループットを個別にプロビジョニングして、コストとパフォーマンスの適切な組み合わせを実現できます。ファイルシステムのストレージ、SSD IOPS、スループットキャパシティを変更し、ワークロードのニーズの変化に対応して必要な分だけ料金を支払えます。

Amazon FSx の料金

Amazon FSx では、ハードウェアまたはソフトウェアの初期費用は発生しません。最低コミットメント、セットアップコスト、追加料金なしで、使用したリソースに対してのみ、お支払いいただきます。サービスに関連する料金については、「Amazon FSx for Windows File Server の料金」を参照してください。

前提

Amazon FSx を使用するには、サポートされているタイプの VMware Cloud on AWS 環境で実行されている Amazon EC2 インスタンス、WorkSpaces インスタンス、AppStream 2.0 インスタンス、または VM を持つ AWS アカウントが必要です。

このガイドでは、以下の仮定を行います。

- Amazon EC2 を使用している場合は、Amazon EC2 に精通していることを前提としています。Amazon EC2 の使用方法の詳細については、Amazon Elastic Compute Cloud のドキュメントを参照してください。
- WorkSpace を使用している場合は、WorkSpace に精通していることを前提としています。WorkSpace の使用方法の詳細については、Amazon WorkSpaces ユーザーガイド を参照してください。
- VMware Cloud on を使用している場合は AWS、VMware Cloud on に精通していることを前提としています。詳細については、AWSの VMware クラウド を参照してください。

- Microsoft アクティブディレクトリの概念に精通していることを前提としています。

前提条件

Amazon FSx ファイルシステムを作成するには、次のものが必要です。

- Amazon FSx ファイルシステムと Amazon EC2 インスタンスを作成するために必要なアクセス許可を持つ AWS アカウント。詳細については、「のセットアップ AWS アカウント」を参照してください。
- Amazon FSx ファイルシステムに関連付ける Amazon VPC サービスに基づき、Microsoft Windows サーバーを仮想プライベートクラウド (VPC) で実行している Amazon EC2 インスタンス。作成方法については、Amazon EC2 ユーザーガイドの「Amazon EC2 Windows インスタンスの使用開始方法」を参照してください。
- Amazon FSx は Microsoft アクティブディレクトリと連携して、ユーザー認証とアクセスコントロールを実行します。作成中に Amazon FSx ファイルシステムを Microsoft アクティブディレクトリに接続します。詳細については、「Microsoft Active Directory の使用」を参照してください。
- このガイドでは、Amazon VPC サービスに基づいて VPC のデフォルトのセキュリティグループのルールを変更していないことを前提としています。存在する場合は、Amazon EC2 インスタンスから Amazon FSx ファイルシステムへのネットワークトラフィックを許可するために必要なルールを追加する必要があります。詳細については、「Amazon FSx のセキュリティ」を参照してください。
- AWS Command Line Interface () をインストールして設定しますAWS CLI。サポートされているバージョンは 1.9.12 以降です。詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS CLIのインストール、更新、およびアンインストール」を参照してください。

> **Note**
>
> `aws --version` コマンドを使用して、 AWS CLI 使用している のバージョンを確認できます。

Amazon FSx for Windows File Server フォーラム

Amazon FSx の使用中に問題が発生した場合は、フォーラムをご利用ください。

Amazon FSx を初めて使用しますか?

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

1. 初めて 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 Windows File Server の開始方法 を試してください。
2. パフォーマンスの詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。
3. Amazon FSx セキュリティの詳細については、「Amazon FSx のセキュリティ」を参照してください。
4. 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。

FSx for Windows File Server のベストプラクティス

Amazon FSx for Windows File Server を使用する場合は次のベストプラクティスに従うことをお勧めします。

トピック

- 一般的なベストプラクティス
- セキュリティに関するベストプラクティス
- アクティブディレクトリ
- ファイルシステムの設定と適切なサイズ

一般的なベストプラクティス

モニタリングプランの作成

ファイルシステムのメトリックを使用して、ストレージとパフォーマンスの使用状況をモニタリングし、使用パターンを把握し、使用量がファイルシステムのストレージまたはパフォーマンスの制限に近づくときに通知をトリガーできます。Amazon FSx ファイルシステムとアプリケーション環境の他の部分と一緒に監視することで、パフォーマンスに影響する可能性のある問題をすばやくデバッグできます。

ファイルシステムに十分なリソースがあることの確認

リソースが不足していると、I/O リクエストの待ち時間が長くなり、ファイルシステムが完全または部分的に利用できなくなったように見える場合があります。パフォーマンスの監視とパフォーマンスの警告と推奨事項へのアクセスについて詳しくは、「パフォーマンスの警告と推奨事項」を参照してください。

セキュリティに関するベストプラクティス

ファイルシステムのセキュリティとアクセス制御を管理するには、次のベストプラクティスに従うことをお勧めします。Amazon FSx を設定してセキュリティおよびコンプライアンスの目標を満たすための詳細については、「Amazon FSx のセキュリティ」を参照してください。

ネットワークセキュリティ

ファイルシステムに関連付けられている ENI を変更または削除しないでください

Amazon FSx ファイルシステムは、ファイルシステムに関連付ける仮想プライベートクラウド (VPC) 内に存在する Elastic Network Interface (ENI) を通してアクセスされます。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。

セキュリティグループとネットワーク ACL の使用

セキュリティグループとネットワークアクセスコントロールリスト (ACL) を使用して、ファイルシステムへのアクセスを制限できます。VPC セキュリティグループについては、デフォルトのセキュリティグループがコンソールでファイルシステムにすでに追加されています。ファイルシステムを作成するサブネットのセキュリティグループとネットワーク ACL が、ポート上のトラフィックを許可していることを確認してください。

アクティブディレクトリ

Amazon FSx ファイルシステムを作成するときは、Microsoft Active Directory ドメインに結合して、ユーザー認証、共有レベル、ファイルレベル、フォルダレベルのアクセスコントロール認可を提供できます。ユーザーは、既存の Active Directory アカウントを使用してファイル共有に接続し、その中のファイルとフォルダにアクセスできます。さらに、既存のセキュリティ ACL の設定を修正することなく、Amazon FSx に移行できます。Amazon FSx には、AWS マネージド Microsoft Active Directory とセルフマネージド Microsoft Active Directory の 2 つのオプションがあります。

AWS マネージド Microsoft Active Directory を使用している場合は、Active Directory セキュリティグループのデフォルト設定のままにしておくことをお勧めします。これらの設定を変更する場合は、ネットワーク要件を満たすネットワーク構成を維持することを確認します。詳細については、「ネットワークの前提条件」を参照してください。

セルフマネージド Microsoft Active Directory を使用している場合は、ファイルシステムを設定するための追加オプションがあります。セルフマネージド Microsoft Active Directory で Amazon FSx を使用する場合、初期設定には次のベストプラクティスをお勧めします。

- サブネットを単一の Active Directory サイトに割り当てる: Active Directory 環境に多数のドメインコントローラーがある場合は、Active Directory サイトとサービスを使用して、Amazon FSx ファイルシステムで使用されるサブネットを、可用性と信頼性が最も高い単一の Active Directory サイ

トに割り当てます。VPC セキュリティグループ、VPC ネットワーク ACL、DCs の Windows ファイアウォールルール、および Active Directory インフラストラクチャにあるその他のネットワークルーティングコントロールで、必要なポートで Amazon FSx からの通信が許可されていることを確認します。これにより、割り当てられた Active Directory サイトを使用できない場合、Windows は他の DCs に戻すことができます。詳細については、「Amazon VPC を使用した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。

- 別の組織単位 (OU) を使用する: Amazon FSx ファイルシステムには、他の組織単位とは別の OU を使用します。
- 必要最小限の権限を持つサービスアカウントを設定する: Amazon FSx に提供するサービスアカウントを、必要最低限の権限で設定または委任します。詳細については、「セルフマネージド Microsoft Active Directory を使用する」を参照してください。
- Active Directory 設定を継続的に検証する: Amazon FSx ファイルシステムを作成する前に、Amazon FSx Active Directory 検証ツールを Active Directory 設定に対して実行して、設定が Amazon FSx での使用に有効であることを確認し、ツールが公開する可能性のある警告やエラーを検出します。 FSx

Active Directory の設定ミスによる可用性の低下を回避する

セルフマネージド Microsoft Active Directory で Amazon FSx を使用する場合は、ファイルシステムの作成時だけでなく、継続的なオペレーションと可用性のためにも、有効な Active Directory 設定を持つことが重要です。障害回復イベント、定期メンテナンスイベント、およびスループットキャパシティ更新アクション中に、Amazon FSx はファイルサーバーリソースを Active Directory に再結合します。イベント中に Active Directory 設定が有効でない場合、ファイルシステムは設定ミスのステータスに変わり、使用できなくなるリスクがあります。ここでは、可用性を損なわないための方法を紹介します。

- Active Directory 設定を Amazon FSx で更新する: サービスアカウントのパスワードのリセットなどの変更を行う場合は、このサービスアカウントを使用するファイルシステムの設定を必ず更新してください。
- Active Directory の設定ミスをモニタリングする: 必要に応じてファイルシステムの Active Directory 設定をリセットできるように、誤って設定されたステータス通知を自分で設定します。Lambda ベースのソリューションを使用してこれを実現する例については、「Amazon EventBridge と を使用した Amazon FSx ファイルシステムのヘルスのモニタリング AWS Lambda」を参照してください。
- Active Directory 設定を定期的に検証する: Active Directory の設定ミスをプロアクティブに検出する場合は、Active Directory 設定に対して Active Directory 検証ツールを継続的に実行することをお

勧めします。検証ツールの実行中に警告やエラーが表示される場合は、ファイルシステムが誤って設定されるリスクがあることを意味します。

- FSx によって作成されたコンピュータオブジェクトを移動または変更しないでください。Amazon FSx は、指定したサービスアカウントとアクセス許可を使用して、Active Directory にコンピュータオブジェクトを作成および管理します。これらのコンピューターオブジェクトを移動または変更すると、ファイルシステムが誤って設定される可能性があります。

Windows ACL

Amazon FSx では、きめ細かい共有レベル、ファイルレベル、およびフォルダレベルのアクセスコントロールでスタンダードの Windows アクセスコントロールリスト (ACL) を使用します。Amazon FSx ファイルシステムは、ファイルシステムデータにアクセスするユーザーの認証情報を自動的に検証して、これらの Windows ACL を適用します。

- SYSTEM ユーザーの NTFS ACL アクセス許可を変更しない: Amazon FSx では、SYSTEM ユーザーがファイルシステム内のすべてのフォルダーに対するフルコントロールの NTFS ACL アクセス許可を持っている必要があります。SYSTEM ユーザーの NTFS ACL アクセス許可を変更すると、ファイルシステムにアクセスできなくなり、今後のファイルシステムバックアップが使用できなくなる可能性があります。

ファイルシステムの設定と適切なサイズ

デプロイタイプの選択

Amazon FSx には、シングル AZ とマルチ AZ の 2 つのデプロイ オプションがあります。共有 Windows ファイルデータの高可用性を必要とするほとんどのプロダクションワークロードでは、マルチ AZ ファイルシステムの使用をお勧めします。詳細については、「可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム」を参照してください。

スループットキャパシティの選択

ワークロードの予想トラフィックだけでなく、ファイルシステムで有効にする機能をサポートするために必要な追加のパフォーマンスリソースも満たせるように、十分なスループットキャパシティでファイルシステムを構成します。例えば、データ重複排除を実行している場合、選択するスループットキャパシティは、使用しているストレージに基づいて重複排除を実行するのに十分なメモリを提供する必要があります。シャドウコピーを使用している場合は、Windows Server がシャドウコピーを

削除しないように、スループットキャパシティをワークロードによって駆動されると予想される値の 3 倍以上の値に増やしてください。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。

ストレージ容量とスループット容量の増加

空きストレージが不足している場合や、ストレージ要件が現在のストレージ制限よりも大きくなることが予想される場合は、ファイルシステムのストレージキャパシティを増やします。ファイルシステム上で常に 20% 以上の空きストレージ容量を維持することをお勧めします。また、ストレージ容量を増やす前にスループット容量を少なくとも 20% 増やして、ストレージの増加中のパフォーマンスへの影響を相殺することをお勧めします。FreeStorageCapacity CloudWatch メトリクスを使用して、利用可能な空きストレージの量をモニタリングし、その傾向を把握することができます。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。

また、ワークロードが現在のパフォーマンス制限によって制約されている場合は、ファイルシステムのスループットキャパシティも増やす必要があります。FSx コンソールの [Monitoring and performance] (監視とパフォーマンス) ページを使用して、ワークロードの要求がパフォーマンスの制限に近づいたか、またはそれを超えたかを確認して、ファイルシステムがワークロードに対して十分にプロビジョニングされていないかどうかを判断できます。

ストレージのスケーリング時間を最小限に抑え、書き込みパフォーマンスの低下を防ぐには、ストレージキャパシティを増やす前に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、ストレージキャパシティの増加が完了した後にスループットキャパシティを縮小することをお勧めします。ほとんどのワークロードでは、ストレージのスケーリング中にパフォーマンスへの影響が最小限に抑えられます。ただし、HDD ストレージタイプを持つファイルシステムや、多数のエンドユーザー、高レベルの I/O、または多数の小さなファイルを持つデータセットを含むワークロードでは、一時的にパフォーマンスが低下する可能性があります。詳細については、「ストレージ容量の拡張とファイルシステムのパフォーマンス」を参照してください。

アイドル期間中のスループットキャパシティの変更

スループットキャパシティを更新すると、シングル AZ ファイルシステムでは数分間可用性が中断され、マルチ AZ ファイルシステムではフェイルオーバーおよびフェイルバックが発生します。マルチ AZ ファイルシステムでは、フェイルオーバーおよびフェイルバック中にトラフィックが継続している場合、このときに実行したすべてのデータ変更をファイルサーバー間で同期する必要があります。書き込みが多いワークロードや IOPS が多いワークロードでは、データ同期プロセスに数時間かかることがあります。この間、ファイルシステムは引き続き利用可能になりますが、データ同期の期間を短縮するため、ファイルシステムの負荷が最小であるアイドル期間中に保守ウィンドウをスケジュー

リングし、スループットキャパシティの更新を実行することをお勧めします。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。

Amazon FSx for Windows File Server の開始方法

次に、FSx for Windows File Server の使用方法を説明します。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. を使用して AWS Managed Microsoft AD Active Directory を作成します AWS Directory Service。ファイルシステムとコンピューティングインスタンスを Active Directory に統合します。
3. Microsoft Windows Server を実行する Amazon Elastic Compute Cloud コンピューティングインスタンスを作成します。このインスタンスを使用してファイルシステムにアクセスします。
4. Amazon FSx コンソールを使用して、Amazon FSx for Windows File Server ファイルシステムを作成します。
5. ファイルシステムを EC2 インスタンスにマッピングする
6. ファイルシステムにデータを書き込みます。
7. ファイルシステムをバックアップします。
8. 作成した リソースをクリーンアップします。

トピック

- のセットアップ AWS アカウント
- ステップ 1. Active Directory のセットアップ
- ステップ 2: Amazon EC2 コンソールで Windows インスタンスを起動する
- ステップ 3: インスタンスに接続する
- ステップ 4: インスタンスを AWS Directory Service ディレクトリに結合する
- ステップ 5. ファイルシステムを作成
- ステップ 6。Windows サーバーを実行する EC2 インスタンスへファイル共有をマッピングします
- ステップ 7。ファイル共有にデータを書き込む
- ステップ 8: ファイルシステムをバックアップする
- ステップ 9。リソースをクリーンアップする

のセットアップ AWS アカウント

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

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、 のセキュリティを確保し AWS IAM Identity Center、 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 Management Consoleとして にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (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 Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 AWS IAM Identity Center 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 Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

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

ステップ 1. Active Directory のセットアップ

Amazon FSx を使用すると、Windows ベースのワークロード用にフルマネージド型ファイルストレージを操作できます。同様に、 はワークロードのデプロイで使用するフルマネージドディレクトリ AWS Directory Service を提供します。EC2 インスタンスを使用して仮想プライベートクラウド (VPC) AWS で で実行されている既存の社内 Active Directory ドメインがある場合は、ユーザーベースの認証とアクセスコントロールを有効にできます。これを行うには、 AWS Managed Microsoft Active Directory と企業ドメインの間に信頼関係を確立します。Amazon FSx での Windows 認証の場合、一方向のフォレスト信頼のみが必要で、 AWS マネージドフォレストは企業ドメインフォレストを信頼します。

企業ドメインは信頼されたドメインのロールを引き受け、 AWS Directory Service マネージドドメインは信頼するドメインのロールを引き受けます。検証済み認証リクエストは、ドメイン間を一方向にしか移動しません。これにより、企業ドメインのアカウントがマネージドドメインで共有されているリソースに対して認証を行うことができます。この場合、Amazon FSx はマネージドドメインとのみ対話します。マネージドドメインは、認証リクエストを企業ドメインに渡します。

> **Note**
>
> 信頼されたドメインに対して Amazon FSx で外部の信頼タイプを使用することもできます。

アクティブディレクトリのセキュリティグループでは、Amazon FSx ファイルシステムのセキュリティグループからのインバウンドアクセスを有効にする必要があります。

Microsoft Active Directory 用の AWS Directory Services を作成するには

- まだない場合は、 AWS Directory Service を使用して AWS Managed Microsoft Active Directory ディレクトリを作成します。詳細については、 AWS Directory Service 管理ガイドのAWS 「マネージド Microsoft Active Directory の作成」を参照してください。

> **Important**
>
> 管理者ユーザーに割り当てたパスワードを覚えておいてください。この入門演習の後半で必要になります。パスワードを忘れた場合は、新しい AWS Directory Service ディレクトリと管理者ユーザーを使用して、この演習の手順を繰り返す必要があります。

- 既存の Active Directory がある場合は、 AWS Managed Microsoft Active Directory と既存の Active Directory の間に信頼関係を作成します。詳細については、「AWS Directory Service 管理ガイド」の「信頼関係を作成するタイミング」を参照してください。

ステップ 2: Amazon EC2 コンソールで Windows インスタンスを起動する

次の手順で説明 AWS Management Console するように、 を使用して Windows インスタンスを起動できます。これは、初めてのインスタンスをすばやく起動できるように設計されています。そのため、可能なすべてのオプションを扱ってはいません。詳細オプションの詳細については、「インスタンスの起動」を参照してください。

インスタンスを起動するには

1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
2. コンソールダッシュボードから、インスタンスの起動 を選択します。
3. Amazon マシンイメージ (AMI) の選択ページには、インスタンスのテンプレートとして機能する Amazon マシンイメージ (AMI) と呼ばれる基本設定のリストが表示されます。Windows Server 2016 Base 以降の AMI を選択します。これらの AMI は [Free tier eligible] と表示されていることに注意してください。
4. インスタンスタイプの選択ページで、インスタンスのハードウェア設定を選択できます。デフォルトで選択されている `t2.micro` タイプを選択します。このインスタンスタイプは無料利用枠の対象であることに注意してください。
5. 確認して起動を選択して、ウィザードが他の設定を完了できるようにします。
6. インスタンスの起動の確認ページのセキュリティグループの下に、ウィザードが作成、選択したセキュリティグループが表示されます。このセキュリティグループを使用することも、セットアップ時に作成したセキュリティグループを次のステップで選択することもできます。

   a. セキュリティグループの編集 を選択します。

b. セキュリティグループの設定 ページで、既存のセキュリティグループを選択する が選択されていることを確認します。

c. 既存のセキュリティグループのリストからセキュリティグループを選択し、確認して起動を選択します。

7. インスタンスの起動の確認ページで、起動を選択します。

8. キーペアの入力を求められたら、[Choose an existing key pair] (既存のキーペアを選択) を選択し、セットアップ時に作成したキーペアを選択します。

   または、新しいキーペアを作成することもできます。新しいキーペアの作成 を選択し、キーペアの名前を入力して、キーペアのダウンロードを選択します。プライベートキーファイルを保存できるのはこれが唯一のチャンスなので、必ずダウンロードしてください。プライベートキーファイルを安全な場所に保存します。インスタンスを起動する際はキーペアの名前を指定する必要があり、インスタンスに接続する際は毎回対応するプライベートキーを指定する必要があります。

   > **Warning**
   >
   > キーペアオプションなしで続行を選択しないでください。キーペアなしでインスタンスを起動すると、インスタンスに接続できません。

   準備ができたら、確認チェックボックスを選択し、インスタンスの起動を選択します。

9. 確認ページは、インスタンスが起動中であることを通知します。インスタンスの表示を選択して確認ページを閉じ、コンソールに戻ります。

10. インスタンス画面で、起動のステータスを確認できます。インスタンスの起動には短時間かかります。インスタンスを起動すると、その初期状態は `pending` です。インスタンスがスタートすると、その状態は `running` に変わり、公開 DNS 名を受け取ります。(公開 DNS (IPv4) 列が非表示の場合は、ページの右上隅にある 列の表示 / 非表示 (歯車のシェープをしたアイコン) を選択してから、公開 DNS (IPv4) を選択します。)

11. インスタンスが接続できるようになるまで、インスタンスの準備が整うまでに数分かかる場合があります。インスタンスがステータスチェックに合格したことを確認してください。この情報は、ステータスチェック 列で確認できます。

> **Important**
>
> このインスタンスを起動したときに作成されたセキュリティグループの ID をメモします。Amazon FSx ファイルシステムを作成するときに必要になります。

インスタンスが起動したので、インスタンスに接続できます。

ステップ 3: インスタンスに接続する

Windows インスタンスに接続するには、初期管理者パスワードを取得してから、リモートデスクトップを使用してインスタンスに接続するときにこのパスワードを指定する必要があります。

管理者アカウントの名前は、オペレーティングシステムの言語によって異なります。例えば、英語の場合は [Administrator]、フランス語の場合は [Administrateur]、ポルトガル語の場合は [Administrador] です。詳細については、「Microsoft TechNet Wiki」の「Windows での管理者アカウントのローカライズされた名前」を参照してください。

インスタンスをドメインに結合させた場合は、 AWS Directory Serviceで定義したドメイン認証情報を使用してインスタンスに接続できます。リモートデスクトップのログイン画面では、ローカルコンピュータ名と生成されたパスワードを使用しないでください。代わりに、管理者には完全修飾ユーザー名を使用し、このアカウントのパスワードを使用してください。例は **`corp.example.com\Admin`** です。

Windows Server オペレーティングシステム (OS) のライセンスでは、管理目的で 2 つの同時リモート接続が許可されています。Windows Server のライセンスは、Windows インスタンスの料金に含まれています。3 つ以上の同時リモート接続が必要な場合は、リモートデスクトップサービス (RDS) ライセンスを購入する必要があります。3 番目の接続を試みると、エラーが発生します。詳細については、「接続に許可される同時リモート接続の数を設定する」を参照してください。

RDP クライアントを使用して Windows インスタンスに接続するには

1. Amazon EC2 コンソールでインスタンスを選択し、[Connect] (接続) を選択します。
2. [Connect to Your Instance] (インスタンスに接続) ダイアログボックスで、[Get Password] (パスワードの取得) を選択します (インスタンスが起動してからパスワードが使用可能になるまでに数分かかります)。

3. [Browse] (参照) を選択して、インスタンスの起動時に作成したプライベートキーファイルに移動します。ファイルを選択し、[Open] (開く) を選択して、ファイルの内容全体を[Contents] (コンテンツ) フィールドにコピーします。
4. [Decrypt Password] (パスワードを復号化) を選択します。コンソールの [Connect to Your Instance] (インスタンスに接続) ダイアログボックスにインスタンスのデフォルトの管理者パスワードが表示され、前に示した [Get Password] (パスワードの取得) へのリンクが実際のパスワードに置き換えられます。
5. デフォルトの管理者パスワードをレコードするか、クリップボードにコピーします。このパスワードはインスタンスに接続するのに必要です。
6. [Download Remote Desktop File] (リモートデスクトップファイルのダウンロード) を選択します。ブラウザから .rdp ファイルを開くか、保存するかを確認するメッセージが表示されます。どちらのオプションでも構いません。終了したら、[Close] (閉じる) を選択して[Connect to Your Instance] (インスタンスに接続) ダイアログボックスを閉じることができます。
   - .rdp ファイルを開くと、[Remote Desktop Connection] (リモートデスクトップ接続) ダイアログボックスが表示されます。
   - .rdp ファイルを保存した場合は、ダウンロードディレクトリに移動し、.rdp ファイルを開いてダイアログボックスを表示します。
7. リモート接続の発行元が不明であるという警告が表示される場合があります。インスタンスへの接続を続行できます。
8. プロンプトが表示されたら、オペレーティングシステムの管理者アカウントと、以前にレコードまたはコピーしたパスワードを使用して、インスタンスにログインします。リモートデスクトップ接続 にすでに管理者アカウントが設定されている場合は、別のアカウントを使用する オプションを選択し、ユーザー名とパスワードを手動で入力する必要がある場合があります。

   > **Note**
   >
   > コンテンツをコピーして貼り付けると、データが破損する場合があります。ログインしようとしたときに 「Password Failed」というエラーが発生した場合は、パスワードを手動で入力してください。

9. 自己署名証明書の性質上、セキュリティ証明書を認証できなかったという警告が表示される場合があります。以下の手順を使用してリモートコンピュータのアイデンティティを確認するか、証明書を信頼する場合は、[Yes] (はい) または [Continue] (続行) を選択して続行します。

a. Windows PC から リモートデスクトップ接続 を使用している場合は、[View certificate] (証明書の表示) を選択します。Mac で Microsoft リモートデスクトップ を使用している場合は、[Show Certificates] (証明書の表示) を選択します。

b. 詳細 タブを選択し、Windows PC の場合は 拇印 エントリまで、Mac の場合は SHA1 指紋 エントリまで下にスクロールします。これは、リモートコンピュータのセキュリティ証明書の一意の識別子です。

c. Amazon EC2 コンソールで、インスタンスを選択し、[Action] (アクション) を選択してから、[Get System Log] (システムログを取得する) を選択します。

d. システムログ出力で、`RDPCERTIFICATE-THUMBPRINT` というラベルの付いたエントリを探します。この値が証明書の拇印または指紋と一致する場合は、リモートコンピュータのアイデンティティを確認しています。

e. Windows PC から リモートデスクトップ接続 を使用している場合は、証明書 ダイアログボックスに戻り、[OK] を選択します。Mac で Microsoft リモートデスクトップ を使用している場合は、[Verify Certificate] (証明書の確認) に戻り、[Continue] (続行) を選択します。

f. [Windows] リモートデスクトップ接続 ウィンドウで [Yes] を選択して、インスタンスに接続します。

インスタンスに接続したので、インスタンスを AWS Directory Service ディレクトリに結合させることができます。

ステップ 4: インスタンスを AWS Directory Service ディレクトリに結合する

次の手順では、既存の Amazon EC2 Windows インスタンスを AWS Directory Service ディレクトリに手動で結合する方法を示します。

Windows インスタンスを AWS Directory Service ディレクトリに結合するには

1. リモートデスクトッププロトコルクライアントを使用してインスタンスに接続します。
2. インスタンスの TCP / IPv4 プロパティダイアログボックスを開きます。

   a. ネットワーク接続を開きます。

> **Tip**
>
> インスタンスのコマンドプロンプトから次のコマンドを実行すると、ネットワーク接続を直接開くことができます。
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. 有効なネットワーク接続のコンテキスト (右クリック) メニューを開き、[Properties] (プロパティ) を選択します。

c. 接続プロパティのダイアログボックスで、[Internet Protocol Version 4] (インターネットプロトコルバージョン 4) を開きます (ダブルクリックします)。

3. (オプション) 次の DNS サーバーアドレスを使用し、優先 DNS サーバーと代替 DNS サーバーのアドレスを、提供された AWS Directory Service DNS サーバーの IP アドレスに変更して、OK を選択します。

4. インスタンスの[System Properties] (システムのプロパティ) ダイアログボックスを開き、[Computer Name] (コンピュータ名) タブを選択して、[Change] (変更) を選択します。

> **Tip**
>
> インスタンスのコマンドプロンプトから次のコマンドを実行すると、[System Properties] (システムのプロパティ) ダイアログボックスを直接開くことができます。
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. 「メンバー」ボックスに「ドメイン」を選択し、 AWS Directory Service ディレクトリの完全修飾名を入力し、「OK」を選択します。

6. ドメイン管理者の名前とパスワードの入力を求められたら、管理者アカウントのユーザー名とパスワードを入力します。

> **Note**
>
> ドメインの完全修飾名、または NetBios 名のいずれかを入力し、バックスラッシュ (\)、ユーザー名、そしてこの場合は [Admin] (管理者) を後に続けて入力します。例えば、corp.example.com\Admin または corp\Admin です。

7. ドメインへのアクセスを歓迎するメッセージを受け取ったら、インスタンスを再起動して変更を有効にします。
8. RDP 経由でインスタンスに再接続し、 AWS Directory Service ディレクトリの管理者ユーザーのユーザー名とパスワードを使用してインスタンスにサインインします。

インスタンスがドメインに結合したので、Amazon FSx ファイルシステムを作成する準備が整いました。

ステップ 5. ファイルシステムを作成

ファイルシステムの作成方法 (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. ダッシュボードで [Create file system] (ファイルシステムの作成) を選択して、ファイルシステム作成ウィザードをスタートします。
3. [Select file system type] (ファイルシステムのタイプを選択) のページで、[FSx for Windows File Server] (FSx for Windows ファイルサーバー) を選択し、[Next] (次へ) を選択します。[Create file system] (ファイルシステムを作成) ページが表示されます。
4. [作成方法] は、[スタンダードの作成] を選択します。

ファイルシステムの詳細

1. [File system details] (ファイルシステム詳細) セクションで、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 個の Unicode 文字、空白文字、数字、そして特殊文字 (+ - = . _ : /) が使用できます
2. [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) を選択して、利用できないアベイラビリティーゾーンにも対応できるファイルシステムをデプロイします。このオプションは、SSD と HDD ストレージをサポートします。
   - [Single-AZ] (シングル AZ) を選択して、1 つのアベイラビリティーゾーンにデプロイされたファイルシステムをデプロイします。[Single-AZ 2] (シングル AZ 2) は、最新世代の単一アベイラビリティーゾーンファイルシステムで、SSD および HDD ストレージをサポートします。

詳細については、「可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム」を参照してください。

3. ストレージタイプ では、SSD または HDD のいずれかを選択できます。

   FSx for Windows ファイルサーバーは、ソリッドステートドライブ (SSD) とハードディスクドライブ (HDD) のストレージタイプを提供します。SSD ストレージは、データベースやメディア処理ワークロード、データ分析アプリケーションなど、最高のパフォーマンスでレイテンシーに最も敏感なワークロード向けに設計されています。HDD ストレージは、ホームディレクトリ、ユーザーおよび部門のファイル共有、コンテンツ管理システムなど、幅広いワークロードに対応するように設計されています。詳細については、「ストレージタイプについて」を参照してください。

4. [プロビジョンド SSD IOPS] では、[自動] モードまたは [ユーザープロビジョニング] モードのいずれかを選択できます。

   自動モードを選択すると、FSx for Windows ファイルサーバーは SSD IOPS を自動的にスケールして、ストレージ容量の GiB あたり 3 SSD IOPS を維持します。ユーザープロビジョニングモードを選択した場合は、96 ~ 400,000 の範囲の任意の整数を入力します。SSD IOPS を 80,000 以上にスケールできるのは、米国東部 (バージニア北部)、米国西部 (オレゴン)、米国東部 (オハイオ)、欧州 (アイルランド)、アジアパシフィック (東京)、アジアパシフィック (シンガポール) です。詳細については、「SSD IOPS の管理」を参照してください。

5. [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。SSD ストレージを使用している場合は、32 ~ 65,536 の範囲で任意の整数を入力します。HDD ストレージを使用している場合は、2,000 ~ 65,536 の範囲で任意の整数を入力します。ファイルシステムの作成した後、いつでも必要な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。

6. スループット容量 はデフォルト設定のままにします。スループット容量 は、ファイルシステムをホストするファイルサーバーがデータを提供できる持続可能速度です。推奨スループット容量設定は、選択したストレージ容量に基づきます。推奨スループット容量を超える容量が必要な場合は、[Specify throughput capacity] (スループット容量の指定) を選択し、値を選択します。詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。

> **Note**
>
> ファイルアクセス監査を有効にする場合は、32 MBps 以上のスループット容量を選択する必要があります。詳細については、「ファイルアクセス監査によるエンドユーザーアクセスのログ記録」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作成した後、いつでも必要に応じて変更できます。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。

ネットワークとセキュリティ

1. [Network & security] (ネットワークとセキュリティ) セクションで、ファイルシステムに関連付ける Amazon VPC を選択します。この入門演習では、 AWS Directory Service ディレクトリと Amazon EC2 インスタンスに選択したのと同じ Amazon VPC を選択します。
2. [VPC Security Groups] (VPC セキュリティグループ) では、デフォルト Amazon VPC のデフォルトのセキュリティグループが、コンソール内のファイルシステムにすでに追加されています。デフォルトのセキュリティグループを使用していない場合は、選択したセキュリティグループがファイルシステム AWS リージョン と同じ にあることを確認してください。EC2 インスタンスをファイルシステムに接続できるようにするには、選択したセキュリティグループに次のルールを追加する必要があります。

   a. 以下のインバウンドおよびアウトバウンドルールを追加して、次のポートを許可します。

ルール	ポート
UDP	53、88、123、389、464
TCP	53、88、135、389、445、464、636、3268、3269、5985、9389、49152〜65535

   IP アドレスまたはセキュリティグループから、およびファイルシステムにアクセスするクライアント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 IP アドレスまたはセキュリティグループ ID に追加します。

b. アウトバウンドルールを追加して、ファイルシステムに結合されているアクティブディレクトリへのすべてのトラフィックを許可します。これを行うには、次のいずれかを実行します。

- AWS マネージド AD ディレクトリに関連付けられているセキュリティグループ ID への、アウトバウンドトラフィックを許可します。
- セルフマネージドアクティブディレクトリドメインコントローラーに関連付けられた IP アドレスへの、アウトバウンドトラフィックを許可します。

> **Note**
>
> 場合によっては、 AWS Managed Microsoft AD セキュリティグループのルールをデフォルト設定から変更した可能性があります。その場合、このセキュリティグループに Amazon FSx ファイルシステムからのトラフィックを許可するために必要なインバウンドルールがあることを確認してください。必要なインバウンドルールの詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD 前提条件」を参照してください。

詳細については、「Amazon VPC を使用した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。

3. マルチ AZ ファイルシステムには、プライマリファイルサーバーとスタンバイファイルサーバーがあり、それぞれが独自のアベイラビリティーゾーンとサブネットにあります。マルチ AZ ファイルシステムを作成する場合 (ステップ 5 を参照)、プライマリファイルサーバーの [優先サブネット] 値とスタンバイファイルサーバーの [スタンバイサブネット] 値を選択します。

   シングル AZ ファイルシステムを作成する場合は、ファイルシステムの [サブネット] を選択します。

Windows 認証

- Windows 認証 では、次のオプションがあります。

  ファイルシステムを が管理する AWS Microsoft Active Directory ドメインに結合する場合は、Managed Microsoft Active Directory を選択し AWS、リストから AWS Directory Service ディレクトリを選択します。詳細については、「Microsoft Active Directory の使用」を参照してください。

セルフマネージド Microsoft Active Directory のドメインにファイルシステムを結合する場合は、[セルフマネージド Microsoft Active Directory] をクリックし、Active Directory に関する次の詳細を入力します。詳細については、「セルフマネージド Microsoft Active Directory を使用する」を参照してください。

- アクティブディレクトリの完全修飾ドメイン名。

> **Important**
>
> シングル AZ 2 およびすべてのマルチ AZ ファイルシステムの場合は、アクティブディレクトリのドメイン名は 47 文字を超えてはいけません。この制限は、 AWS Directory Service とセルフマネージド Active Directory ドメイン名の両方に適用されます。Amazon FSx では、DNS IP アドレスへの直接接続または内部トラフィックが必要です。インターネットゲートウェイ経由の接続はサポートされていません。代わりに、AWS Virtual Private Network、VPC ピアリング、 AWS Direct Connect、または AWS Transit Gateway 関連付けを使用します。

- DNS サーバーの IP アドレス - ドメインの DNS サーバーの IPv4 アドレス

> **Note**
>
> DNS サーバーで EDNS (DNS の拡張メカニズム) が有効になっている必要があります。EDNS が無効になっている場合、ファイルシステムの作成が失敗する可能性があります。

- サービスアカウントのユーザーネーム - 既存のアクティブディレクトリでのサービスアカウントのユーザー名。ドメインのプレフィックスやサフィックスを含めないでください。
- サービスアカウントのパスワード - サービスアカウントのパスワード。
- (オプション) 組織単位 (OU) - ファイルシステムを結合させる組織単位の識別パス名。
- (オプション) 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するアクティブディレクトリ内のグループの名前。デフォルトのグループは「ドメイン管理者」です。詳細については、「Amazon FSx サービスアカウント」を参照してください。

暗号化、監査、アクセス (DNS エイリアス)

1. 暗号化 では、保管中のファイルシステムのデータを暗号化するために使用される AWS KMS key 暗号化キーを選択します。キーの ARN を指定することで AWS KMS、 によって管理されるデフォルトの aws/fsx (デフォルト) 、既存のキー、またはカスタマーマネージドキーを選択できます。詳細については、「保管中のデータの暗号化」を参照してください。
2. [Auditing - optional] (監査 - オプション) の場合、ファイルアクセス監査はデフォルトで無効になっています。ファイルアクセス監査の有効化と設定の詳細については、「ファイルアクセス監査によるエンドユーザーアクセスのログ記録」を参照してください。
3. [Access - optional] (アクセス - オプション) の場合、ファイルシステムに関連付ける DNS エイリアスを入力します。各エイリアス名は、完全修飾ドメイン名 (FQDN) としてフォーマットする必要があります。詳細については、「DNS エイリアスを管理する」を参照してください。

バックアップとメンテナンス

日次自動バックアップとこのセクションの設定の詳細については、「バックアップでデータを保護する。」を参照してください。

1. [日次自動バックアップ] はデフォルトで有効になっています。Amazon FSx がファイルシステムのバックアップを毎日自動的に取得したくない場合は、この設定を無効にすることができます。
2. 自動バックアップが有効になっている場合、バックアップはバックアップウィンドウと呼ばれる期間内に実行されます。デフォルトのウィンドウを使用するか、ワークフローに最適な [自動バックアップウィンドウの開始時間] を選択できます。
3. [自動バックアップ保持期間] では、デフォルト設定の [30] 日を使用するか、Amazon FSx がファイルシステムの日次自動バックアップを保持する 1 ~ 90 日の値を設定できます。この設定は、ユーザーが開始したバックアップ、または AWS Backupによって実行されたバックアップには適用されません。
4. [Tags - optional] (タグ - オプション) では、キーと値を入力して、ファイルシステムにタグを追加します。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。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。

   [Next] (次へ) を選択します。

設定を確認し、作成する

1. 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。参照のために、ファイルシステム作成後は変更できないファイルシステム設定を書き留めます。ファイルシステムを作成する を選択します。
2. Amazon FSx がファイルシステムを作成したら、[ファイルシステム] ダッシュボードのファイルシステム ID を選択し詳細を表示します。[アタッチ] を選択し、ファイルシステムの [DNS 名] を [ネットワークとセキュリティ] タブに書き留めます。共有を EC2 インスタンスにマッピングするには、次の手順でこれが必要です。

ステップ 6。Windows サーバーを実行する EC2 インスタンスへファイル共有をマッピングします

ディレクトリに参加している Microsoft Windows ベースの Amazon EC2 インスタンスに Amazon FSx ファイルシステムをマウントできるようになりました AWS Directory Service 。ファイル共有の名前は、ファイルシステムの名前と同じではありません。

GUI を使用して Amazon EC2 Windows インスタンス上のファイル共有をマッピングするには

1. Windows インスタンスにファイル共有をマウントする前に、EC2 インスタンスを起動し、ファイルシステムが参加 AWS Directory Service for Microsoft Active Directory した に結合する必要があります。このアクションを実行するには、 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. 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 インスタンスに接続する」を参照してください。
3. 接続したら、ファイルエクスプローラーを開きます。
4. ナビゲーションペインから、[Network] (ネットワーク) のコンテキスト (右クリック) メニューを開き、[Map Network Drive] (ネットワークドライブのマッピング) を選択します。
5. ドライブ 用に選択したドライブ文字を選択します。
6. Amazon FSx によって割り当てられたデフォルトの DNS 名、またはユーザーが選択した DNS エイリアスを使用して、ファイルシステムをマッピングできます。この手順では、デフォルトの DNS 名を使用してファイル共有をマッピングする方法について説明します。DNS エイリアスを

使用してファイル共有をマッピングする場合は、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

[Folder] (フォルダ) には、ファイルシステムの DNS 名と共有名を入力します。デフォルトの Amazon FSx 共有は `\share` と言います。Amazon FSx コンソール内の DNS 名は、https://console.aws.amazon.com/fsx/、[Windows File Server] (Windows ファイルサーバー) > [Network & Security] (ネットワークとセキュリティ) セクション、または CreateFileSystem ないし DescribeFileSystems API コマンドのレスポンスで見つけることができます。

- AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
fs-0123456789abcdef0.ad-domain.com
```

- セルフマネージドアクティブディレクトリを結合しているシングル AZ ファイルシステムおよびマルチ AZ ファイルシステムの場合、DNS 名は次のようになります。

```
amznfsxaa11bb22.ad-domain.com
```

例えば、`\\fs-0123456789abcdef0.ad-domain.com\share` と入力します。

7. ファイル共有を [Reconnect at sign-in] (サインイン時に再接続) するかどうかを選択し、[Finish] (完了) を選択します。

ステップ 7。ファイル共有にデータを書き込む

ファイル共有がインスタンスにマッピングされているので、Windows 環境内の他のディレクトリと同様にファイル共有を使用できます。

ファイル共有にデータを書き込むには

1. メモ帳のテキストエディタを開きます。
2. テキストエディタにコンテンツを書き込みます。例えば、*[Hello, world!]* (こんにちは、皆様！)
3. ファイルをファイル共有のドライブレターに保存します。
4. エクスプローラーを使用して、ファイル共有に移動し、先ほど保存したテキストファイルを見つけます。

ステップ 8: ファイルシステムをバックアップする

Amazon FSx ファイルシステムとそのファイル共有が使用できる状態になっているので、ファイルシステムをバックアップできます。デフォルトでは、ファイルシステムの 30 分間のバックアップ時間枠中に、日次バックアップが自動的に作成されます。ただし、ユーザーによるバックアップはいつでも作成できます。バックアップには、関連する追加コストがあります。バックアップ料金の詳細については、「料金設定」を参照してください。

コンソールからファイルシステムのバックアップを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. コンソールダッシュボードから、この演習のために作成したファイルシステムの名前を選択します。
3. ファイルシステムの [Overview] (概要) タブから、[Create backup] (バックアップの作成) を選択します。
4. [Create backup] (バックアップの作成) ダイアログボックスが開いたら、バックアップの名前を入力します。この名前には、最大 256 文字の Unicode 文字が使用でき、空白文字、数字、および以下の特殊文字を含むことができます: + - = . _ : /
5. [Create backup] (バックアップの作成) を選択します。
6. ファイルシステムの復元やバックアップの削除のため、リスト内のすべてのバックアップを表示するには、[Backups] (バックアップ) を選択します。

新しいバックアップを作成すると、作成中のステータスは [CREATING] (作成中) に設定されます。これは数分かかることがあります。バックアップが使用可能になると、ステータスは [AVAILABLE] (使用可能) に変更されます。

ステップ 9。リソースをクリーンアップする

この演習を完了したら、以下の手順に従ってリソースをクリーンアップし、 AWS アカウントを保護する必要があります。

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. Amazon FSx コンソールで、ファイルシステムを削除します。すべての自動バックアップは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を削除する必要があります。以下のステップは、このプロセスの概要を説明します。

   a. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
   b. コンソールダッシュボードから、この演習のために作成したファイルシステムの名前を選択します。
   c. [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。
   d. [Delete file system] (ファイルシステムの削除) ダイアログボックスが開き、最終バックアップを作成するかどうかを決定します。作成する場合は、最終バックアップの名前を入力します。自動的に作成されたすべてのバックアップも削除されます。

      > **Important**
      > 新しいファイルシステムは、バックアップから作成できます。ベストプラクティスとして、最終バックアップを作成することをお勧めします。一定期間が経過した後も、その最終バックアップが必要なかった場合、その他の手動で作成したバックアップとともに削除できます。

   e. [File system ID] (ファイルシステム ID) ボックスに、削除するファイルシステムの ID を入力します。
   f. [Delete file system] (ファイルシステムの削除) を選択します。
   g. ファイルシステムが削除中となり、ダッシュボードのステータスが [DELETING] (削除中)に変わります。ファイルシステムが削除されると、ダッシュボードに表示されなくなります。
   h. これで、手動で作成したファイルシステムのバックアップを削除できるようになりました。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。
   i. ダッシュボードから、削除したファイルシステムと同じ ファイルシステム ID を持っているバックアップを選択し、[Delete backup] (バックアップの削除) を選択します。
   j. [Delete backups] (バックアップの削除) ダイアログボックスが開きます。選択したバックアップの ID のチェックボックスはオンのままにして、[Delete backups] (バックアップの削除) を選択します。

   Amazon FSx ファイルシステムおよび関連する自動バックアップが削除されました。

3. この演習用に作成した AWS Directory Service ディレクトリを削除するには、「 AWS Directory Service 管理ガイド」の「ディレクトリの削除」を参照してください。

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。

トピック

- サポートされているクライアント
- 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
- デフォルトの DNS 名を使用したデータへのアクセス
- 分散ファイルシステム (DFS) 名前空間のサポート
- DNS エイリアスを使用したデータへのアクセス
- ファイル共有を使用したデータへのアクセス
- ファイル共有の作成、更新、削除

サポートされているクライアント

FSx for Windows File Server は、サーバーメッセージブロック (SMB) プロトコルバージョン 2.0 から 3.1.1 をサポートしているため、さまざまなコンピューティングインスタンスとオペレーティングシステムを使用してファイルシステムに接続できます。

Amazon FSx 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。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス。Microsoft Windows、Mac、Amazon Linux、Amazon Linux 2 インスタンスが含まれます。詳細については、「ファイル共有のマッピング」を参照してください。
- Amazon Elastic Container Service (Amazon ECS) コンテナ 詳細については、「Amazon Elastic Container Service (Amazon ECS) デベロッパーガイド」の「FSx for Windows ファイルサーバーボリューム」を参照してください。
- WorkSpaces インスタンス – 詳細については、 AWS ブログ記事「Amazon WorkSpaces で FSx for Windows File Server を使用する Amazon WorkSpaces」を参照してください。
- Amazon AppStream 2.0 インスタンス – 詳細については、 AWS ブログ記事「Amazon AppStream 2.0 で Amazon FSx を使用するAmazon AppStream 2.0」を参照してください。

- VMware Cloud on AWS 環境で実行されている VMs – 詳細については、 AWS ブログ記事VMware Cloud on AWS Environment で FSx for Windows File Server とファイルの保存と共有」を参照してください。

Amazon FSx では、次のオペレーティングシステムがサポートされています。

- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、および Windows Server 2022。
- Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10 (WorkSpace の Windows 7 と Windows 10 のデスクトップエクスペリエンスを含む)、および Windows 11。
- `cifs-utils` ツールを使用した Linux。
- macOS

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 Windows File Server 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。ファイルシステムとは異なる または ファイルシステム AWS リージョン とは異なる VPCs AWS アカウント からファイルシステムにアクセスすることもできます。以降のセクションで説明する FSx for Windows File Server 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 を使用した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。

FSx for Windows File Server ファイルシステムには、ファイルシステムと同じ VPC にある、サポートされているクライアントからアクセスできます。

次の表は、ファイルシステムが作成された時期に応じて、サポートされている各環境で Amazon FSx がクライアントからのアクセスをサポートする環境を示しています。

次の場所に所在するクライアント	2019 年 2 月 22 日以前に作成されたファイルシステムへのアクセス	2020 年 12 月 17 日以前に作成されたファイルシステムへのアクセス	2020 年 12 月 17 日以降に作成されたファイルシステムへのアクセス
ファイルシステムが作成されるサブネット	✓	✓	✓
ファイルシステムが作成された VPC のプライマリ CIDR ブロック	✓	✓	✓
ファイルシステムが作成された VPC のセカンダリ CIDR		RFC1918 プライベート IP アドレス範囲内の IP アドレスを持つクライアント: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP アドレスが次の CIDR ブロック範囲外にあるクライアント: 198.19.0.0/16
その他の CIDR またはピアリングされたネットワーク			

> **Note**
>
> 場合によっては、2020 年 12 月 17 日以前に作成されたファイルシステムに、非プライベート IP アドレス範囲を使用してオンプレミスからアクセスしたいことがあります。これを行うには、ファイルシステムのバックアップから新しいファイルシステムを作成します。詳細については、「バックアップでデータを保護する。」を参照してください。

別の VPC AWS アカウントからのデータへのアクセス AWS リージョン

FSx for Windows File Server ファイルシステムには、別の VPC にあるサポートクライアントから AWS アカウント、または VPC ピアリングまたはトランジットゲートウェイを使用してファイルシステムに関連付けられているもの AWS リージョン からアクセスできます。VPC ピアリング接続またはトランジットゲートウェイを使用して VPC を接続する場合、ある VPC にあるコンピューティングインスタンスは、別の VPC にある Amazon FSx ファイルシステムにアクセスできます。このアクセスは、VPC が異なる AWS アカウントに属していても、VPC が異なる AWS リージョンリージョンに存在していても可能です。

VPC ピアリング接続 とは、2 つの VPC 間のネットワーク接続のことで、プライベート IPv4 アドレスまたは IP バージョン 6 (IPv6) アドレスを使って VPC 間でトラフィックをルーティングする場合に使用できます。VPC ピアリングを使用して、同じ AWS リージョン内または AWS リージョン間で VPCs を接続できます。VPC ピアリングの詳細については、「Amazon VPC ピアリングガイド」の「VPC ピアリングとは?」を参照してください。

トランジットゲートウェイ は、VPC とオンプレミスネットワークを相互接続するために使用できるネットワークのトランジットハブです。VPC トランジットゲートウェイの使用についての詳細は、「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開始方法」を参照してください。

VPC ピアリング接続またはトランジットゲートウェイ接続を設定したら、DNS 名を使用してファイルシステムにアクセスできます。これは、関連付けられた VPC 内のコンピューティングインスタンスからの場合と同じように行います。

オンプレミスからデータにアクセスする

FSx for Windows File Server は、オンプレミスのコンピューティングインスタンスからファイルシステムにアクセス AWS VPN するための AWS Direct Connect または の使用をサポートしています。をサポートする FSx for Windows File Server を使用すると AWS Direct Connect、オンプレミス環境からの専用ネットワーク接続を介してファイルシステムにアクセスできます。をサポートする FSx for Windows File Server を使用すると AWS VPN、安全でプライベートなトンネルを介してオンプレミスデバイスからファイルシステムにアクセスできます。

Amazon FSx ファイルシステムに関連付けられた VPC にオンプレミス環境を接続すると、DNS 名または DNS エイリアスを使用してファイルシステムにアクセスできるようになります。これは、VPC 内のコンピューティングインスタンスからの場合と同様に行います。 AWS Direct Connectの詳細については、「AWS Direct Connect ユーザーガイド」を参照してください。 AWS VPN 接続の設定の詳細については、「Amazon VPC ユーザーガイド」の「VPN 接続」を参照してください。

> **Note**
>
> 場合によっては、2020 年 12 月 17 日以前に作成されたファイルシステムに、非プライベート IP アドレス範囲を使用してオンプレミスからアクセスしたいことがあります。これを行うには、ファイルシステムのバックアップから新しいファイルシステムを作成します。詳細については、「バックアップでデータを保護する。」を参照してください。

FSx for Windows ファイルサーバーでは Amazon FSx ファイルゲートウェイの使用もサポートし、オンプレミスのコンピューティングインスタンスからクラウド内 FSx for Windows ファイルサーバー共有に低レイテンシーでシームレスにアクセスできます。詳細については、「Amazon FSx ファイルゲートウェイユーザーガイド」を参照してください。

> **Note**
>
> 新規のお客様への Amazon FSx File Gateway の提供は終了しました。FSx File Gateway の既存のお客様は、通常どおりサービスを引き続き使用できます。FSx File Gateway に似た機能については、このブログ記事を参照してください。

デフォルトの DNS 名を使用したデータへのアクセス

FSx for Windows ファイルサーバーは、すべてのファイルシステムに対してドメインネームシステム (DNS) 名を提供します。FSx for Windows ファイルサーバーファイルシステムにアクセスするには、この DNS 名を使用して、コンピューティングインスタンス上のドライブ文字を Amazon FSx ファイル共有にマッピングします。詳細については、「ファイル共有を使用したデータへのアクセス」を参照してください。

> **Important**
>
> Amazon FSx は、Microsoft DNS をデフォルトの DNS として使用している場合にのみ、ファイルシステムの DNS レコードを登録します。サードパーティー DNS を使用している場合は、Amazon FSx ファイルシステムの DNS エントリをマニュアルで設定する必要があります。ファイルシステムに使用する正しい IP アドレスの選択については、「手動 DNS エントリに使用する正しいファイルシステムの IP アドレスの取得」を参照してください。

DNS 名を見つけるには:

- Amazon FSx コンソールで [File systems] (ファイルシステム) を選択し、[Details] (詳細) を選択します。[Network & Security] (ネットワークとセキュリティ) で DNS 名を表示します。
- または、CreateFileSystem ないし DescribeFileSystems API コマンドのレスポンスで表示します。

AWS Managed Microsoft Active Directory に参加しているすべてのシングル AZ ファイルシステムの場合、DNS 名は次の形式になります。 `fs-0123456789abcdef0.ad-dns-domain-name`

セルフマネージド Active Directory に接続しているすべてのシングル AZ ファイルシステム、およびマルチ AZ ファイルシステムでは、DNS 名の形式は `amznfsxaa11bb22.ad-domain.com` になります。

DNS 名を使用した Kerberos 認証の使用

Amazon FSx との転送中に、Kerberos ベースの認証と暗号化を使用することをお勧めします。Kerberos は、ファイルシステムにアクセスするクライアントに対して最も安全な認証を提供します。SMB セッションで転送中のデータの Kerberos ベースの認証と暗号化を有効にするには、Amazon FSx によって提供されるファイルシステムの DNS 名を使用してファイルシステムにアクセスします。

AWS Managed Microsoft Active Directory とオンプレミス Active Directory の間に外部信頼を設定している場合、Kerberos 認証で Amazon FSx Remote PowerShell を使用するには、フォレスト検索順序のためにクライアントでローカルグループポリシーを設定する必要があります。詳細については、「Microsoft ドキュメント」の「Kerberos フォレスト検索順序 (KFSO) の設定」を参照してください。

分散ファイルシステム (DFS) 名前空間のサポート

FSx for Windows ファイルサーバーでは、Microsoft DFS 名前空間の使用がサポートされています。DFS 名前空間を使用して、複数のファイルシステム上にあるファイル共有を、ファイルデータセット全体にアクセスするために使用する 1 つの共通のフォルダ構造 (名前空間) に整理します。DFS 名前空間内の名前を使用して Amazon FSx ファイルシステムにアクセスするには、リンクターゲットをファイルシステムの DNS 名に設定します。詳細については、「複数の FSx for Windows File Server のファイルシステムと DFS 名前空間のグループ化」を参照してください。

DNS エイリアスを使用したデータへのアクセス

FSx for Windows ファイルサーバー、ファイル共有にアクセスするために使用できるすべてのファイルシステムの DNS 名を提供します。FSx for Windows File Server ファイルシステムの DNS エイリアスを登録することで、デフォルトの DNS 名以外の DNS 名を使用してファイル共有にアクセスすることもできます。

DNS エイリアスを使用すると、Windows ファイル共有データを FSx for Windows File Server に移動しても、既存の DNS 名を引き続き使用して Amazon FSx のデータにアクセスできます。DNS エイリアスを使うと、意味を持った名前を使用して Amazon FSx ファイルシステムに接続するためのツールやアプリケーションを管理しやすくすることもできます。ファイルシステムには、一度で最大 50 個の DNS エイリアスを関連付けることができます。DNS エイリアスの FSx for Windows File Server ファイルシステムとの関連付けと関連付け解除の詳細については、「DNS エイリアスを管理する」を参照してください。

DNS エイリアスを使用して FSx for Windows File Server ファイルシステムに引き続きアクセスするには、次のステップを実行する必要があります。

1. DNS エイリアスをファイルシステムに関連付ける.
2. ファイルシステムおよびそれに関連付けられた DNS エイリアスの DNS CNAME レコードを更新または作成します。

FSx for Windows File Server ファイルシステムで DNS エイリアスを使用する方法の詳細については、「DNS エイリアスを管理する」を参照してください。

Kerberos 認証と DNS エイリアスを使用した暗号化の使用

Amazon FSx との転送中に、Kerberos ベースの認証と暗号化を使用することをお勧めします。Kerberos は、ファイルシステムにアクセスするクライアントに対して最も安全な認証を提供します。DNS エイリアスを使用して Amazon FSx にアクセスするクライアントに対して Kerberos 認証を有効にするには、Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトの DNS エイリアスに対応するサービスプリンシパル名 (SPN) を追加する必要があります。

DNS エイリアスを使用してファイルシステムにアクセスするときに Kerberos 認証と暗号化を設定するには、「Kerberos のサービスプリンシパル名 (SPN) を設定する」を参照してください。

必要に応じて、アクティブディレクトリで次のグループポリシーオブジェクト (GPO) を設定することで、DNS エイリアスを使用してファイルシステムにアクセスするクライアントに Kerberos 認証と暗号化を使用するように強制できます。

- NTLM の制限: リモートサーバーへの発信 NTLM トラフィック - このポリシー設定を使用して、コンピュータから Windows オペレーティングシステムを実行しているリモートサーバーへの発信 NTLM トラフィックを拒否または監査します。
- NTLM の制限: NTLM 認証用のリモート サーバーの例外を追加する - このポリシー設定を使用すると、ネットワークセキュリティ: NTLM の制限: リモートサーバーへの発信 NTLM トラフィックのポリシーが設定されている場合に、クライアントデバイスが NTLM 認証を使用することが許可されるリモートサーバーの例外リストを作成できます。

DNS エイリアスを使用してファイルシステムにアクセスするときに Kerberos 認証と暗号化を適用するには、「グループポリシーオブジェクト (GPO) を使用した Kerberos 認証の強制」を参照してください。

DNS エイリアスを使用するようにファイルシステムを設定する方法の詳細については、次の手順を参照してください。

- DNS エイリアスをファイルシステムに関連付ける
- Kerberos のサービスプリンシパル名 (SPN) を設定する
- DNS CNAME レコードを更新または作成する
- グループポリシーオブジェクト (GPO) を使用した Kerberos 認証の強制

DNS エイリアスをファイルシステムに関連付ける

DNS エイリアスは、新しいファイルシステムを作成する際と、 Amazon FSx コンソール、CLI、および API を使用してバックアップから新しいファイルシステムを作成する際に、既存の FSx for Windows ファイルサーバーのファイルシステムに関連付けることができます。別のドメイン名でエイリアスを作成する場合は、親ドメインを含むフルネームを入力して、エイリアスを関連付けます。

この手順では、Amazon FSx コンソールを使用して新しいファイルシステムを作成するときに DNS エイリアスを関連付ける方法について説明します。DNS エイリアスと既存のファイルシステムとの関連付けに関する情報、および CLI および API の使用の詳細については、「DNS エイリアスを管理する」を参照してください。

新しいファイルシステムを作成するときに DNS エイリアスを関連付けるには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 「開始方法」セクションの ステップ 5. ファイルシステムを作成 で説明されているように、新しいファイルシステムを作成する手順に従います。

3. [Create file system] (ファイルシステムの作成) ウィザードの [Access - optional] (アクセス - オプション) セクションで、ファイルシステムに関連付ける DNS エイリアスを入力します。

   DNS エイリアスを指定する場合は、次のガイドラインを使用します。

   - `accounting.example.com` などの完全修飾ドメイン名 (FQDN) *`hostname.domain`* としてフォーマットする必要があります。
   - 英数字およびハイフン (-) を使用できます。
   - ハイフンでスタートまたは終了することはできません。
   - 数字で始めることができます。

   DNS エイリアス名の場合、大文字または小文字を指定するか、あるいはエスケープコードで対応する文字を指定するかどうかに関係なく、Amazon FSx は英字を小文字 (a ~ z) として格納します。
4. メンテナンス設定 については、必要に応じて変更を加えてください。
5. タグ - オプション セクションで、必要なタグを追加し、[Next] (次へ) を選択します。
6. ファイルシステムの作成 ページに表示されるファイルシステム設定を確認します。ファイルシステムの作成 を選択して、ファイルシステムを作成します。

Kerberos のサービスプリンシパル名 (SPN) を設定する

Amazon FSx との転送中に、Kerberos ベースの認証と暗号化を使用することをお勧めします。Kerberos は、ファイルシステムにアクセスするクライアントに最も安全な認証を提供します。

DNS エイリアスを使用して Amazon FSx にアクセスするクライアントに対して Kerberos 認証を有効にするには、Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトの DNS エイリアスに対応するサービスプリンシパル名 (SPN) を追加する必要があります。SPN は、一度に 1 つのアクティブディレクトリのコンピュータオブジェクトにのみ関連付けることができます。元のファイルシステムのアクティブディレクトリコンピュータオブジェクトに対して設定された DNS 名の既存の SPN がある場合は、まずそれらを削除する必要があります。

Kerberos 認証に必要な SPN は 2 つあります。

```
HOST/alias
HOST/alias.domain
```

エイリアスが `finance.domain.com` の場合、必要な SPN は次の 2 つです。

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Amazon FSx ファイルシステムのアクティブディレクトリ (AD) コンピュータオブジェクトの新しいホスト SPN を作成する前に、アクティブディレクトリコンピュータオブジェクトの DNS エイリアスに対応する既存のホスト SPN を削除する必要があります。AD に DNS エイリアスの SPN が存在する場合、Amazon FSx ファイルシステムの SPN を設定しようとすると失敗します。

次の手順では、その方法を説明します。

- 元のファイルシステムのアクティブディレクトリコンピュータオブジェクト上の既存の DNS エイリアス SPN を検索します。
- 既存の SPN が見つかった場合、削除します。
- Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクト用の新しい DNS エイリアス SPN を作成します。

必要な PowerShell アクティブディレクトリのモジュールをインストールするには

1. Amazon FSx ファイルシステムが接続しているアクティブディレクトリに接続している Windows インスタンスにログオンします。
2. 管理者として PowerShell を開きます。
3. 次のコマンドを使用して、PowerShell アクティブディレクトリのモジュールをインストールします。

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

元のファイルシステムのアクティブディレクトリコンピュータオブジェクト上で、既存の DNS エイリアス SPN を検索して削除するには

アクティブディレクトリ内のコンピュータオブジェクト上の別のファイルシステムに割り当てた DNS エイリアスに SPN が設定されている場合は、ファイルシステムのコンピュータオブジェクトに SPN を追加する前に、まずこれらの SPN を削除する必要があります。

1. 次のコマンドを使用して、既存の SPN を検索します。*alias_fqdn* を、ステップ 1 でファイルシステムに関連付けた DNS エイリアスに置き換えます。

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 次のスクリプティング例を使用して、前のステップで返された既存の HOST SPN を削除します。

   - *alias_fqdn* を ステップ 1 でファイルシステムに関連付けたフル DNS エイリアスに置き換えます。
   - *file_system_DNS_name* を元のファイルシステムの DNS 名に置き換えます。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. ステップ 1 でファイルシステムに関連付けた各 DNS エイリアスについて、これまでの手順を繰り返します。

Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトに SPN を設定するには

1. 次のコマンドを実行して、Amazon FSx ファイルシステムの新しい SPN を設定します。

   - *file_system_DNS_name* を Amazon FSx がファイルシステムに割り当てた DNS 名に置き換えます。

     Amazon FSx コンソールでファイルシステムの DNS 名を確認するには、ファイルシステムを選択し、自分のファイルシステムを選択し、ファイルシステムの詳細ページのネットワークとセキュリティペインを選択します。

また、DescribeFileSystems API オペレーションのレスポンスで DNS 名を取得することもできます。

- *alias_fqdn* をステップ 1 でファイルシステムに関連付けたフル DNS エイリアスに置き換えます。

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
 @($Alias, $Alias.Split(".")[0])}
```

> **Note**
>
> 元のファイルシステムのコンピュータオブジェクトの AD に、DNS エイリアスの SPN が存在する場合は、Amazon FSx ファイルシステムの SPN の設定は失敗します。既存の SPN の検索および削除については、「元のファイルシステムのアクティブディレクトリコンピュータオブジェクト上で、既存の DNS エイリアス SPN を検索して削除するには」を参照してください。

2. 次のスクリプティング例を使用して、新しい SPN が DNS エイリアス用に設定されていることを確認します。この手順で前述したように、レスポンスに 2 つのホスト SPN (HOST/*alias* と HOST/*alias_fqdn*) が含まれていることを確認します。

   file_system_DNS_name を Amazon FSx がファイルシステムに割り当てた DNS 名に置き換えてください。Amazon FSx コンソールでファイルシステムの DNS 名を検索するには、[Files systems] (ファイルシステム) を選択し、ファイルシステムを選択してから、ファイルシステムの詳細ページで [Network & security] (ネットワークとセキュリティ) ペインを選択します。

   また、DescribeFileSystems API オペレーションのレスポンスで DNS 名を取得することもできます。

```
## Verify SPNs on FSx file system AD computer object
```

```
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. ステップ 1 でファイルシステムに関連付けた各 DNS エイリアスについて、これまでの手順を繰り返します。

DNS CNAME レコードを更新または作成する

ファイルシステムの SPN を適切に設定した後、元のファイルシステムに解決された各 DNS レコードを、Amazon FSx ファイルシステムのデフォルトの DNS 名に解決する DNS レコードに置き換えることによって、Amazon FSx にカットオーバーできます。

このセクションで説明するコマンドを実行するには、`dnsserver` と `activedirectory` の Windows モジュールが必要です。

必要な PowerShell モジュールをインストールするには

1. Amazon FSx ファイルシステムが参加しているのと同じ Active Directory に結合している Windows インスタンスに、DNS 管理権限を持つグループ (AWS の委任されたドメイン名システム管理者、 のドメイン管理者 AWS Managed Microsoft AD、またはセルフマネージド Active Directory で DNS 管理権限を委任した別のグループ) のメンバーであるユーザーとしてログオンします。

   詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。
2. 管理者として PowerShell を開きます。
3. この手順の要領を実行するには、PowerShell DNS サーバーモジュールが必要です。次のコマンドを使用してインストールします。

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Amazon FSx ファイルシステムにカスタム DNS 名を更新または作成するには

1. DNS 管理権限を持つグループ (AWS マネージド Active Directory AWS の委任されたドメイン名システム管理者、ドメイン管理者、またはセルフマネージド Active Directory の DNS 管理権限

を委任した別のグループ) のメンバーであるユーザーとして Amazon EC2 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 インスタンスに接続する」を参照してください。

2. コマンドプロンプトで、以下のスクリプティングを実行します。このスクリプティングは、既存の DNS CNAME レコードを Amazon FSx ファイルシステムに移行します。見つからない場合は、Amazon FSx ファイルシステムのデフォルト DNS 名に解決する DNS エイリアス *alias_fqdn* の新しい DNS CNAME レコードを作成します。

   スクリプティングを実行するには。

   - *alias_fqdn* をファイルシステムに関連付けた DNS エイリアスに置き換えます。
   - *file_system_DNS_name* を Amazon FSx がファイルシステムに割り当てた DNS 名に置き換えてください。

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. ステップ 1 でファイルシステムに関連付けた各 DNS エイリアスについて、前のステップを繰り返します。

これにより、DNS エイリアスを使用して Amazon FSx ファイルシステムの DNS CNAME 値を追加しました。これで、DNS エイリアスを使用してデータにアクセスできます。

> **Note**
>
> DNS CNAME レコードを更新して、以前に別のファイルシステムを指した Amazon FSx ファイルシステムを指す場合、クライアントはしばらくファイルシステムに接続できないことがあります。クライアント DNS キャッシュが更新されると、DNS エイリアスを使用して

接続できます。詳細については、「DNS エイリアスを使用してファイルシステムにアクセスできない」を参照してください。

グループポリシーオブジェクト (GPO) を使用した Kerberos 認証の強制

アクティブディレクトリで次のグループポリシーオブジェクト (GPO) を設定することにより、ファイルシステムにアクセスするときに Kerberos 認証を適用できます。

- NTLM の制限: リモートサーバーへの発信 NTLM トラフィック - このポリシー設定を使用して、コンピュータから Windows オペレーティングシステムを実行しているリモートサーバーへの発信 NTLM トラフィックを拒否または監査します。
- NTLM の制限: NTLM 認証用のリモート サーバーの例外を追加する - このポリシー設定を使用すると、NTLM の 制限: リモートサーバーへの送信 NTLM トラフィックのポリシー設定が設定されている場合に、クライアントデバイスが NTLM 認証を使用することが許可されるリモートサーバーの例外リストを作成できます。

1. Amazon FSx ファイルシステムが管理者として参加しているアクティブディレクトリに結合させられた Windows インスタンスにログオンします。セルフマネージドアクティブディレクトリを設定してる場合は、アクティブディレクトリに次の手順を直接適用します。
2. [Start] (スタート) を選択し、[Administrative Tools] (管理ツール) を選択して[Group Policy Management] (グループポリシーの管理) を選択します。
3. グループポリシーオブジェクト を選択します。
4. グループポリシーオブジェクトが存在していない場合は、作成してください。
5. 既存の [Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers] (ネットワークセキュリティ: NTLM の制限: リモートサーバーへの送信 NTLM トラフィック) ポリシーを見つけます。(既存のポリシーが存在しない場合は、新しいポリシーを作成します。) ローカルセキュリティ設定 タブで、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。
6. [Deny all] (すべてを拒否) を選択します。
7. [Apply] (適用) を選択して、セキュリティ設定を保存します。
8. クライアントの特定のリモートサーバーへの NTLM 接続の例外を設定するには、ネットワークセキュリティ: NTLM の制限: リモートサーバーの例外の追加を特定します。

コンテキスト (右クリック) メニューを開き、ローカルセキュリティ設定 タブの プロパティ を選択します。

9. 例外リストに追加するサーバーの名前を入力します。
10. [Apply] (適用) を選択して、セキュリティ設定を保存します。

ファイル共有を使用したデータへのアクセス

Microsoft Windows ファイル共有は、ファイルシステム上の特定のフォルダまたディレクトリです。これには、存在する可能性のあるサブフォルダが含まれます。クライアントは、サーバーメッセージブロック (SMB) プロトコルを使用してファイルシステム上のファイル共有にアクセスします。FSx for Windows File Server ファイルシステムには、`share` という名前のデフォルトの Windows ファイル共有が付属しています。Windows の共有フォルダグラフィカルユーザーインターフェイス (GUI) ツールを使用して、他のファイル共有を必要な数だけ作成および管理できます。

Microsoft Windows の継続的可用性 (CA) 共有は、クラスター内のサーバーノードに障害が発生した場合でも、共有ファイルへの中断のないアクセスを維持するという主な利点を提供します。CA ファイル共有を使用すると、ファイルシステムのメンテナンスウィンドウ中にデータファイルをこれらのファイル共有に保存しているサーバーアプリケーションの中断を最小限に抑えることができます。

CA 共有など、FSx for Windows File Server ファイルシステムでのファイル共有の作成と管理の詳細については、「」を参照してくださいファイル共有の作成、更新、削除。

ファイル共有のマッピング

ファイル共有にアクセスするには、Windows マップネットワークドライブ機能を使用して、コンピューティングインスタンス上のドライブ文字を Amazon FSx ファイル共有にマッピングします。ファイル共有をコンピューティングインスタンス上のドライブにマッピングするプロセスは、Linux ではファイル共有の マウント と呼ばれています。このプロセスは、コンピューティングインスタンスのタイプとオペレーティングシステムによって異なります。ファイル共有がマップされると、アプリケーションとユーザーはローカルファイルやフォルダであるかのように、ファイル共有上のファイルやフォルダにアクセスできます。

ファイル共有をマッピングおよびマウントしてファイルシステム上のデータにアクセスする方法の詳細については、以下の手順を参照してください。

- Amazon EC2 Windows インスタンスでのファイル共有のマッピング.

- Amazon EC2 Mac インスタンスへのファイル共有のマウント
- Amazon EC2 Linux インスタンスへのファイル共有のマウント

Amazon EC2 Windows インスタンスでのファイル共有のマッピング

Windows ファイルエクスプローラーまたはコマンドプロンプトを使用して、EC2 Windows インスタンスにファイル共有をマッピングして FSx for Windows File Server ファイルシステムにアクセスできます。

Amazon EC2 Windows インスタンスのファイル共有をマップするには (ファイルエクスプローラー)

1. EC2 Windows インスタンスを起動し、Amazon FSx ファイルシステムを結合した 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」から以下の手順のいずれかを選択します。
   - 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接続する
2. 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 インスタンスに接続する」を参照してください。
3. 接続したら、ファイルエクスプローラーを開きます。
4. ナビゲーションペインで、ネットワーク のコンテキスト (右クリック) メニューを開き、マップネットワークドライブ を選択します。
5. ドライブ では、ドライブ文字を選択します。
6. フォルダ では、ファイルシステムの DNS 名またはファイルシステムに関連する DNS エイリアス、および共有名を入力します。

> **Important**
>
> DNS 名の代わりに IP アドレスを使用すると、マルチ AZ ファイルシステムのフェイルオーバープロセス中に使用できなくなる可能性があります。また、マルチ AZ およびシングル AZ ファイルシステムでの Kerberos ベースの認証には、DNS 名または関連する DNS エイリアスが必要です。

ファイルシステムの DNS 名と関連する DNS エイリアスは、Amazon FSx コンソール で Windowsファイルサーバー、ネットワークとセキュリティ を選択して見つけることができま

す。または、CreateFileSystem ないし DescribeFileSystems API オペレーションのレスポンスにもあります。DNS エイリアスの使用については、「DNS エイリアスを管理する」を参照してください。

- AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
fs-0123456789abcdef0.ad-domain.com
```

- セルフマネージドアクティブディレクトリを結合しているシングル AZ ファイルシステムおよびマルチ AZ ファイルシステムの場合、DNS 名は次のようになります。

```
amznfsxaa11bb22.ad-domain.com
```

例えば、シングル AZ ファイルシステムの DNS 名を使用する場合、フォルダ に次のように入力します。

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

マルチ AZ ファイルシステムの DNS 名を使用するには、フォルダ に次のように入力します。

```
\\amznfsxaa11bb22.ad-domain.com\share
```

ファイルシステムに関連付けられた DNS エイリアスを使用するには、フォルダ に次のように入力します。

```
\\fqdn-dns-alias\share
```

7. サインイン時にファイル共有を再接続するかどうかを示す [Reconnect at sign-in] (サインイン時に再接続) オプションを選択してから、完了 を選択します。

Amazon EC2 Windows インスタンス (コマンドプロンプト) でファイル共有をマッピングするには

1. EC2 Windows インスタンスを起動し、Amazon FSx ファイルシステムに結合した 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」から以下の手順のいずれかを選択します。

   - 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. AWS Managed Microsoft AD ディレクトリのユーザーとして 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 インスタンスに接続する」を参照してください。
3. 接続したら、コマンドプロンプトウィンドウを開きます。
4. 選択したドライブ文字、ファイルシステムの DNS 名、および共有名を使用してファイル共有をマウントします。DNS 名は、Amazon FSx コンソール を使って Windows ファイルサーバー、[Network & security] (ネットワークとセキュリティ) を選択することで、検索できます。または、`CreateFileSystem` ないし `DescribeFileSystems` API オペレーションのレスポンスでそれらを見つけることができます。

   - AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - セルフマネージドアクティブディレクトリに結合しているシングル AZ ファイルシステムおよびマルチ AZ ファイルシステムの場合、DNS 名は次のようになります。

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   ファイル共有をマウントするコマンドの例を次に示します。

   ```
   $ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
   ```

   `net use` コマンドの代わりに、サポートされている任意の PowerShell コマンドを使用してファイル共有をマウントすることもできます。

Amazon EC2 Mac インスタンスへのファイル共有のマウント

ファイル共有を、Active Directory に結合している、または結合していない Amazon EC2 Mac インスタンス にマントし、FSx for Windows File Server ファイルシステムにアクセスできます。インスタンスがアクティブディレクトリに接続していない場合は、インスタンスが常駐する Amazon Virtual Private Cloud (Amazon VPC) に設定された DHCP オプションを更新して、アクティブディレクトリ

ドメインの DNS ネームサーバーを含めるようにしてください。次に、インスタンスを再起動します。

Amazon EC2 Mac インスタンス (GUI) にファイル共有をマウントするには

1. EC2 Mac インスタンスを起動します。これを行うには、Amazon EC2 ユーザーガイドから以下の手順を選択してください。
   - コンソールを使用した Mac インスタンスの起動
   - を使用して Mac インスタンスを起動する AWS CLI
2. Virtual Network Computing (VNC) を使用して 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「VNC を使用してインスタンスに接続する」を参照してください。
3. EC2 Mac インスタンスで、次のように Amazon FSx ファイル共有に接続します。
   a. Finder を開き、[Go] (進む) を選択し、[Connect to Server] (サーバーに接続) を選択します。
   b. サーバーに接続 ダイアログボックスで、ファイルシステムの DNS 名またはファイルシステムに関連付けられた DNS エイリアス、および共有名を入力します。次に、[Connect] (接続) を選択します。

      ファイルシステムの DNS 名と関連する DNS エイリアスは、Amazon FSx コンソール で Windowsファイルサーバー、ネットワークとセキュリティ を選択して見つけることができます。または、CreateFileSystem ないし DescribeFileSystems API オペレーションのレスポンスにもあります。DNS エイリアスの使用については、「DNS エイリアスを管理する」を参照してください。

   c. 次の画面で、[Connect] (接続) を選択して続行します。

d. 次の例に示すように、Amazon FSx サービスアカウントの Microsoft アクティブディレクトリ (AD) 認証情報を入力します。次に、[Connect] (接続) を選択します。

e. 接続が成功すると、Finder ウィンドウの 場所 の下に Amazon FSx 共有が表示されます。

Amazon EC2 Mac インスタンス (コマンドライン) にファイル共有をマウントするには

1. EC2 Mac インスタンスを起動します。これを行うには、Amazon EC2 ユーザーガイドから以下の手順を選択してください。

   - コンソールを使用した Mac インスタンスの起動
   - を使用して Mac インスタンスを起動する AWS CLI

2. Virtual Network Computing (VNC) を使用して 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「VNC を使用してインスタンスに接続する」を参照してください。

3. 次のコマンドでファイル共有をマウントします。

```
mount_smbfs //file_system_dns_name/file_share mount_point
```

   DNS 名は、Amazon FSx コンソール で、Windows ファイルサーバー、ネットワークとセキュリティ を選択することで確認できます。または、`CreateFileSystem` ないし `DescribeFileSystems` API オペレーションのレスポンスでそれらを見つけることができます。

   - AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
fs-0123456789abcdef0.ad-domain.com
```

- セルフマネージドアクティブディレクトリに結合しているシングル AZ ファイルシステムおよびマルチ AZ ファイルシステムの場合、DNS 名は次のようになります。

```
amznfsxaa11bb22.ad-domain.com
```

この手順で使用するマウントコマンドは、指定されたポイントで以下を実行します。

- *//file_system_dns_name/file_share* - マウントするファイルシステムの DNS 名と共有を指定します。
- *mount_point* - ファイルシステムをマウントする EC2 インスタンス上のディレクトリ。

Amazon EC2 Linux インスタンスへのファイル共有のマウント

FSx for Windows ファイルサーバー共有は、Active Directory に接続している、または接続していない Amazon EC2 Linux インスタンスにマウントして、FSx for Windows File Server ファイルシステムにアクセスできます。

> **Note**
>
> - 次のコマンドは、SMB プロトコル、キャッシュ、読み取りおよび書き込みバッファサイズなどのパラメータを例として指定します。Linux のパラメータの選択 `cifs` コマンド、および Linux カーネルのバージョンを使用すると、クライアントと Amazon FSx ファイルシステム間のネットワークオペレーションのスループットとレイテンシーに影響を与える可能性があります。詳細については、使用している Linux 環境の「`cifs` ドキュメント」をご覧ください。
> - Linux のクライアントは、DNS ベースの自動フェイルオーバーをサポートしていません。詳細については、「Linux のクライアントでのフェイルオーバーのエクスペリエンス」を参照してください。

Active Directory に接続している Amazon EC2 Linux インスタンスにファイル共有をマウントするには

1. 実行中の EC2 Linux インスタンスを Microsoft アクティブディレクトリに接続していない場合は、「AWS Directory Service 管理者ガイド」の「Linux インスタンスを手動で接続する」を参照して、接続の手順を確認してください。
2. 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。
3. 次のコマンドを実行して、`cifs-utils` パッケージをインストールします。このパッケージは、Linux で Amazon FSx のようなネットワークファイルシステムをマウントするために使用されます。

```
$ sudo yum install cifs-utils
```

4. マウントポイントディレクトリ **/mnt/fsx** を作成します。ここで Amazon FSx ファイルシステムをマウントします。

```
$ sudo mkdir -p /mnt/fsx
```

5. 次のコマンドを使用して、Kerberos で認証します。

```
$ kinit
```

6. 次のコマンドでファイル共有をマウントします。

```
$ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
 vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
file-server-Ip
```

DNS 名は、Amazon FSx コンソール で、Windows ファイルサーバー、ネットワークとセキュリティ を選択することで確認できます。または、`CreateFileSystem` ないし `DescribeFileSystems` の API オペレーションのレスポンスでも検索できます。

- AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
fs-0123456789abcdef0.ad-domain.com
```

- セルフマネージドアクティブディレクトリに結合しているシングル AZ ファイルシステムおよびマルチ AZ ファイルシステムの場合、DNS 名は次のようになります。

```
amznfsxaa11bb22.ad-domain.com
```

CIFSMaxBufSize を、カーネルで許可されている最大値に置き換えます。この値を取得するには、次のコマンドを実行します。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

出力は、最大バッファサイズが 130048 であることを示しています。

7. 次のコマンドを実行して、ファイルシステムがマウントされていることを確認します。このコマンドを実行すると、共通インターネットファイルシステム (CIFS) タイプのファイルシステムだけが返されます。

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

この手順で使用するマウントコマンドは、指定されたポイントで以下を実行します。

- *//file_system_dns_name/file_share* - マウントするファイルシステムの DNS 名と共有を指定します。
- *mount_point* - ファイルシステムをマウントする EC2 インスタンス上のディレクトリ。
- `-t cifs vers=`*SMB_version* - ファイルシステムのタイプを CIFS、SMB プロトコルのバージョンとして指定します。Amazon FSx for Windows File Server では、SMB バージョン 2.0 から 3.1.1 がサポートされています。
- `sec=krb5` - 認証に Kerberos バージョン 5 を使用するように指定します。
- `cache=`*cache_mode* - キャッシュモードを設定します。この CIFS キャッシュのオプションはパフォーマンスに影響を与える可能性があるため、カーネルとワークロードに最適な設定をテストする (さらに、Linux のドキュメントを確認する) 必要があります。`loose` では、プロトコルのセマンティクスが緩いため、データの不整合が発生する可能性があるため、オプション `strict` および `none` をお勧めします。

- `cruid=ad_user` - 認証情報キャッシュの所有者の uid を AD ディレクトリ管理者に設定します。
- `/mnt/fsx` - EC2 インスタンスの Amazon FSx ファイル共有のマウントポイントを指定します。
- `rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize` - 読み取りおよび書き込みバッファのサイズを、CIFS プロトコルで許容される最大値として指定します。`CIFSMaxBufSize` を、カーネルで許可されている最大値に置き換えます。次のコマンドを実行して `CIFSMaxBufSize` を決定します。

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  出力は、最大バッファサイズが 130048 であることを示しています。
- `ip=preferred-file-server-Ip` - 宛先 IP アドレスを、ファイルシステムの優先ファイルサーバーのものに設定します。

  ファイルシステムの優先ファイルサーバー IP アドレスを取得するには、次のようにします。
  - ファイルシステムの詳細 ページのネットワークとセキュリティタブで Amazon FSx コンソールを使用します。
  - `describe-file-systems` CLI コマンドまたは同等の DescribeFileSystems API コマンドのレスポンスで。

Active Directory に結合していない Amazon EC2 Linux インスタンスにファイル共有をマウントするには

次の手順では、アクティブディレクトリ (AD) に接続していない Amazon EC2 Linux インスタンスに Amazon FSx ファイル共有をマウントします。AD に接続していない EC2 Linux インスタンスの場合、FSx for Windows ファイルサーバーのファイル共有のみが、プライベート IP アドレスを使用してマウントできます。ファイルシステムのプライベート IP アドレスは、Amazon FSx コンソールのネットワークとセキュリティタブにある優先ファイルサーバー IP アドレス で取得できます。

この例では、NTLM 認証を使用します。これを行うには、FSx for Windows ファイルサーバーのファイルシステムが接続している Microsoft アクティブディレクトリドメインのメンバーであるユーザーとして、ファイルシステムをマウントします。ユーザーアカウントの認証情報は、EC2 インスタンス `creds.txt` で作成するテキストファイルで提供されます。このファイルには、ユーザーのユーザー名、パスワード、およびドメインが含まれています。

```
$ cat creds.txt
```

```
username=user1
password=Password123
domain=EXAMPLE.COM
```

Amazon Linux EC2 インスタンスの起動と設定を行うには

1. Amazon EC2 コンソールを使用して、Amazon Linux EC2 インスタンスを起動します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。
2. Amazon Linux EC2 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。
3. 次のコマンドを実行して、`cifs-utils` パッケージをインストールします。このパッケージは、Linux で Amazon FSx のようなネットワークファイルシステムをマウントするために使用されます。

   ```
   $ sudo yum install cifs-utils
   ```

4. Amazon FSx ファイルシステムをマウントする予定のマウントポイント **/mnt/fsxx** を作成します。

   ```
   $ sudo mkdir -p /mnt/fsx
   ```

5. 前述のフォーマットで、`/home/ec2-user` ディレクトリに `creds.txt` の認証情報ファイルを作成します。
6. 次のコマンドを実行して、ユーザー (所有者) だけがファイルの読み取りと書き込みをできるように `creds.txt` ファイル許可を設定します。

   ```
   $ chmod 700 creds.txt
   ```

ファイルシステムをマウントするには

1. アクティブディレクトリに接続していないファイル共有は、そのプライベート IP アドレスを使用してマウントします。ファイルシステムのプライベート IP アドレスは、Amazon FSx コンソールのネットワークとセキュリティタブにある優先ファイルサーバー IP アドレスで取得できます。
2. 次のコマンドでファイルシステムをマウントします。

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

CIFSMaxBufSize を、カーネルで許可されている最大値に置き換えます。この値を取得するには、次のコマンドを実行します。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

出力は、最大バッファサイズが 130048 であることを示しています。

3. 次のコマンドを実行して、ファイルシステムがマウントされていることを確認します。このコマンドは、CIFS ファイルシステムのみを返します。

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

この手順で使用するマウントコマンドは、指定されたポイントで以下を実行します。

- *//file-system-IP-address/file_share* – マウントするファイルシステムの IP アドレスと共有を指定します。
- `-t cifs vers=`*SMB_version* - ファイルシステムのタイプを CIFS、SMB プロトコルのバージョンとして指定します。Amazon FSx for Windows File Server では、SMB バージョン 2.0 から 3.1.1 がサポートされています。
- `sec=ntlmsspi` - 認証に NT LAN Manager セキュリティサポートプロバイダーインターフェイス (NTLMSSPI) を使用するように指定します。
- `cache=`*cache_mode* - キャッシュモードを設定します。この CIFS キャッシュのオプションはパフォーマンスに影響を与える可能性があるため、カーネルとワークロードに最適な設定をテストする (さらに、Linux のドキュメントを確認する) 必要があります。`loose` では、プロトコルのセマンティクスが緩いため、データの不整合が発生する可能性があるため、オプション `strict` および none をお勧めします。
- `cred=/home/ec2-user/creds.txt` - ユーザー認証情報を取得する場所を指定します。
- */mnt/fsx* - EC2 インスタンスの Amazon FSx ファイル共有のマウントポイントを指定します。

- `rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize` - 読み取りおよび書き込みバッファのサイズを、CIFS プロトコルで許容される最大値として指定します。*CIFSMaxBufSize* を、カーネルで許可されている最大値に置き換えます。次のコマンドを実行して CIFSMaxBufSize を決定します。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Amazon EC2 Linux インスタンスへのファイル共有の自動マウント

FSx for Windows ファイルサーバー共有は、マウント先の Amazon EC2 Linux インスタンスが再起動されるたびに自動的にマウントし、FSx for Windows File Server ファイルシステムにアクセスできます。これを行うには、EC2 インスタンスの `/etc/fstab` ファイルにエントリを追加します。`/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時に実行されるコマンド mount -a は、`/etc/fstab` ファイルにリストされているファイルシステムをマウントします。

Active Directory に登録していない Amazon EC2 Linux インスタンスの場合、プライベート IP アドレスを使用して FSx for Windows ファイルサーバーのファイル共有のみをマウントできます。ファイルシステムのプライベート IP アドレスは、Amazon FSx コンソールのネットワークとセキュリティタブにある優先ファイルサーバー IP アドレス で取得できます。

次の手順では、Microsoft NTLM 認証を使用します。ファイルシステムは、FSx for Windows ファイルサーバーシステムが接続している Microsoft アクティブディレクトリドメインのメンバーであるユーザーとしてマウントします。次のコマンドを使用して、`creds.txt` ファイルからユーザーアカウントの認証情報を取得できます。

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

アクティブディレクトリに結合していない Amazon Linux EC2 インスタンスにファイル共有を自動的にマウントするには

Amazon Linux EC2 インスタンスの起動と設定を行うには

1. Amazon EC2 コンソールを使用して、Amazon Linux EC2 インスタンスを起動します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動」を参照してください。
2. 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。
3. 次のコマンドを実行して、`cifs-utils` パッケージをインストールします。このパッケージは、Linux で Amazon FSx のようなネットワークファイルシステムをマウントするために使用されます。

```
$ sudo yum install cifs-utils
```

4. `/mnt/fsx` ディレクトリを作成します。ここで Amazon FSx ファイルシステムをマウントします。

```
$ sudo mkdir /mnt/fsx
```

5. `/home/ec2-user` ディレクトリに `creds.txt` の認証情報ファイルを作成します。
6. 次のコマンドを実行して、ユーザー (所有者) だけがファイルを読み取れるように、ファイル許可を設定します。

```
$ sudo chmod 700 creds.txt
```

ファイルシステムを自動的にマウントするには

1. アクティブディレクトリに接続していないファイル共有は、そのプライベート IP アドレスを使用して自動的にマウントします。ファイルシステムのプライベート IP アドレスは、Amazon FSx コンソールのネットワークとセキュリティタブにある優先ファイルサーバー IP アドレス で取得できます。
2. プライベート IP アドレスを使用してファイル共有を自動的にマウントするには、`/etc/fstab` ファイルを開きます。

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none 0 0
```

CIFSMaxBufSize を、カーネルで許可されている最大値に置き換えます。この値を取得するには、次のコマンドを実行します。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

出力は、最大バッファサイズが 130048 であることを示しています。

3. 「all」および「verbose」オプションと組み合わせて「fake」オプションを指定した `mount` コマンドを使用して、`fstab` エントリをテストします。

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. ファイル共有をマウントするには、Amazon EC2 インスタンスを再起動します。
5. インスタンスが再び利用可能になったら、次のコマンドを実行して、ファイルシステムがマウントされていることを確認します。

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

この手順で `/etc/fstab` ファイルに追加された行は、指定されたポイントで以下を実行します。

- *//file-system-IP-address/file_share* - マウントする Amazon FSx ファイルシステムの IP アドレスと共有を指定します。
- `/mnt/fsx` - EC2 インスタンスの Amazon FSx ファイルシステムのマウントポイントを指定します。
- `cifs vers=`*SMB_version* - ファイルシステムのタイプを CIFS、SMB プロトコルのバージョンとして指定します。Amazon FSx for Windows File Server では、SMB バージョン 2.0 から 3.1.1 がサポートされています。

- `sec=ntlmsspi` - NTLMチャレンジレスポンス認証を容易にするために NT LAN Manager セキュリティサポートプロバイダーインターフェイスを使用することを指定します。
- `cache=`*`cache_mode`* - キャッシュモードを設定します。この CIFS キャッシュのオプションはパフォーマンスに影響を与える可能性があるため、カーネルとワークロードに最適な設定をテストする (さらに、Linux のドキュメントを確認する) 必要があります。`loose` では、プロトコルのセマンティクスが緩いため、データの不整合が発生する可能性があるため、オプション `strict` および `none` をお勧めします。
- `cred=/home/ec2-user/creds.txt` - ユーザー認証情報を取得する場所を指定します。
- `_netdev` - ファイルシステムがネットワークアクセスを必要とするデバイスに存在することをオペレーティングシステムに通知します。このオプションを使用すると、クライアントでネットワークサービスが有効になるまで、インスタンスがファイルシステムをマウントできなくなります。
- `0` - 0 以外の値の場合、ファイルシステムを dump でバックアップする必要があることを示しています。Amazon FSx の場合、この値は `0` である必要があります。
- `0` - `fsck` が起動時にファイルシステムをチェックする順序を指定します。Amazon FSx ファイルシステムの場合、この値は `0` であり、起動時に `fsck` を実行しないことを示します。

ファイル共有の作成、更新、削除

このトピックでは次のタスクを実行して、ファイル共有を管理する方法を説明します。

- 新しいファイル共有を作成する
- 既存のファイル共有を変更する
- 既存のファイル共有を削除する

PowerShell でのリモート管理に Windows ネイティブの共有フォルダ GUI と Amazon FSx CLI を使用して、 FSx for Windows File Server ファイルシステム上のファイル共有を管理できます。共有フォルダ GUI ([fsmgmt.msc]) を使用する際、異なるファイルシステムにある共有のコンテキストメニューを最初に開くときに遅延が発生することがあります。このような遅延を回避するには、PowerShell を使用して複数のファイルシステムにあるファイル共有を管理します。

Microsoft Windows では、ファイルとディレクトリの命名規則と制限が適用されます。データを正常に作成してアクセスできるようにするには、Windows のガイドラインに従ってファイルとディレクトリに名前を付ける必要があります。詳細については、「命名規則」を参照してください。

> **Warning**
>
> Amazon FSx には、すべてのフォルダで SMB ファイル共有を作成する NTFS ACL のアクセス許可のある フルコントロール の SYSTEM ユーザーが必要です。ファイル共有にアクセスできなくなる可能性があるため、フォルダに対するこのユーザーの NTFS ACL アクセス許可を変更しないでください。

共有フォルダ GUI を使用したファイル共有の管理

Amazon FSx ファイルシステム上のファイル共有を管理するには、共有フォルダ GUI を使用できます。共有フォルダ GUI は、Windows サーバー上のすべての共有フォルダを一元管理するための場所を提供します。次の手順では、ファイル共有を管理する方法について説明します。

FSx for Windows File Server ファイルシステムに共有フォルダを接続するには

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。AWS Managed Microsoft Active Directory では、このグループは委任 AWS FSx 管理者と呼ばれます。セルフマネージド Microsoft アクティブディレクトリで、このグループはドメイン管理者、または作成時に指定した管理者グループのカスタム名と呼ばれます。詳細については、「Windows インスタンス用 Amazon Elastic Compute Cloud のユーザーガイド」の「Windows インスタンスに接続」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) を選択します。
5. [Another computer] (別のコンピュータ) で、Amazon FSx ファイルシステムのドメインネームシステム (DNS) 名 (例えば、**`amznfsxabcd0123.corp.example.com`**) を入力します。

   Amazon FSx コンソールでファイルシステムの DNS 名を確認するには、[File systems] (ファイルシステム) を選択してファイルシステムを選択し、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) セクションをクリックします。DNS 名は、DescribeFileSystems 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。

共有フォルダが Amazon FSx ファイルシステムに接続され、ファイルシステム上の Windows ファイル共有を管理できるようになりました。デフォルトの共有は `\share` と呼ばれます。次のアクションでこれを行うことができます。

- 新しいファイル共有の作成 - 共有フォルダツールの左側のペインで、[Shares] (共有) を選択して、Amazon FSx ファイルシステムのアクティブ共有を表示します。[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。これを行うには、次のようにします。

  - 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に [Browse] (参照) をクリックし、[Make new folder] (新しいフォルダを作成) をクリックしてローカルフォルダを作成します。
  - コマンドラインの使用

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- 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] ツールで、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**
>
> シングル AZ 2 およびマルチ AZ ファイルシステムでは、共有フォルダ GUI ツールを使用したファイル共有の削除またはファイル共有の変更 (アクセス許可、ユーザー制限、およびその他のプロパティの更新を含む) は、Amazon FSx ファイルシステムの DNS 名を使用して fsmgmt.msc に接続する場合のみ可能です。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する場合、共有フォルダー GUI ツールはこれらのアクションをサポートしません。

> **Note**
>
> fsmgmt.msc Shared Folders GUI ツールを使用して複数の FSx for Windows File Server ファイルシステムにある共有にアクセスする場合、別のファイルシステムにある共有のファイル共有コンテキストメニューを最初に開くときに遅延が発生することがあります。このような遅延を回避するために、以下の説明に従って PowerShell を使用してファイル共有を管理できます。

PowerShell でのファイル共有の管理

PowerShell のカスタム FSx for Windows File Server リモート管理コマンドを使用して、ファイル共有を管理できます。これらのコマンドは、次のようなファイル共有タスクの管理を自動化するのに役立ちます。

- 既存のファイルサーバーから Amazon FSx へのファイル共有の移行
- ディザスタリカバリ AWS リージョン のために 間でファイル共有を同期する
- チームファイル共有のプロビジョニングなど、進行中のワークフローにおけるファイル共有のプログラムによる管理

PowerShell でのリモート管理に Amazon FSx CLI を使用する方法については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

以下の表は、FSx for Windows File Server ファイルシステム上のファイル共有の管理に使用できる Amazon FSx CLI でのリモート管理 PowerShell コマンドの一覧です。

共有管理コマンド	説明
New-FSxSmbShare	新しいファイル共有を作成します。
Remove-FSxSmbShare	ファイル共有を削除します。
Get-FSxSmbShare	既存のファイル共有を取得します。

共有管理コマンド	説明
Set-FSxSmbShare	共有のプロパティを設定します。
Get-FSxSmbShareAccess	共有のアクセスコントロールリスト (ACL) を取得します。
Grant-FSxSmbShareAccess	共有のセキュリティ記述子に、トラスティの許可アクセスコントロールエントリ (ACE) を追加します。
Revoke-FSxSmbShareAccess	共有のセキュリティ記述子から、トラスティの許可 ACE をすべて削除します。
Block-FSxSmbShareAccess	共有のセキュリティ記述子に、トラスティの拒否 ACE を追加します。
Unblock-FSxSmbShareAccess	共有のセキュリティ記述子から、トラスティの拒否 ACE をすべて削除します。

各コマンドのオンラインヘルプには、すべてのコマンドオプションのリファレンスが記載されています。このヘルプにアクセスするには、`-?` (例えば、 `New-FSxSmbShare -?`) でコマンドを実行します。

New-FsxsmbShare に認証情報を渡す

New-FsxSmbShare に認証情報を渡して、毎回認証情報を再入力しなくても、数百または数千の共有をループで実行できます。

次のいずれかのオプションを使用して、 FSx for Windows File Server でファイル共有を作成するために必要な認証情報オブジェクトを準備します。

- 認証情報オブジェクトをインタラクティブに生成するには、次のコマンドを使用します。

```
$credential = Get-Credential
```

- AWS Secrets Manager リソースを使用して認証情報オブジェクトを生成するには、次のコマンドを使用します。

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
```

```
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

継続的に利用可能な (CA) 共有を作成するには

PowerShell のリモート管理用の Amazon FSx CLI を使用して、継続的に利用可能な (CA) 共有を作成できます。FSx for Windows File Server マルチ AZ ファイルシステム上に作成された CA 共有は、高い耐久性と、高い可用性を備えています。Amazon FSx シングル AZ ファイルシステムは、シングルノードクラスター上に構築されています。その結果、シングル AZ ファイルシステムで作成された CA 共有は耐久性が高くなりますが、可用性は高くありません。`-ContinuouslyAvailable` オプションを `$True` に設定した `New-FSxSmbShare` コマンドを使用すると、継続的に利用可能な共有であることを指定できます。次に、CA 共有を作成するコマンドの例を示します。

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

`Set-FSxSmbShare` コマンドを使用して、既存のファイル共有上の `-ContinuouslyAvailable` オプションを変更できます。

既存のファイル共有が継続的に利用できるかどうかを判断する

次のコマンドを使用して、既存のファイル共有の Continuously Available プロパティの値を表示します。

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

CA が有効になっている場合、出力には次の行が含まれます。

```
[...]
ContinuouslyAvailable : True
[...]
```

CA が有効になっていない場合、出力には次の行が含まれます。

```
[...]
ContinuouslyAvailable : False
[...]
```

既存のファイル共有で Continuously Available を有効にするには、次のコマンドを使用します。

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

New-FsxsmbShare コマンドが一方向の信頼で失敗する

Amazon FSx は、一方向の信頼があり、ユーザーが存在するドメインが Amazon FSx ファイルシステムに関連付けられたドメインを信頼するように設定されていない場合、`New-FSxSmbShare` PowerShell コマンドの実行をサポートしません。

この状況は、次のいずれかの解決策を使用して解決できます。

- `New-FSxSmbShare` コマンドを実行するユーザーは、FSx ファイルシステムと同じドメインにいる必要があります。
- fsmgmt.msc GUI を使用して、ファイルシステム上に共有を作成できます。詳細については、「共有フォルダ GUI を使用したファイル共有の管理」を参照してください。

可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム

Amazon FSx for Windows File Server は、2 種類のファイルシステムのデプロイを提供します。シングル AZ およびマルチ AZ です。以下のセクションでは、ワークロードに適したデプロイタイプを選択するのに役立つ情報を提供します。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。

シングル AZ ファイルシステムは、単一の Windows ファイルサーバーインスタンスと、単一のアベイラビリティーゾーン (AZ) 内の一連のストレージボリュームで構成されます。シングル AZ ファイルシステムでは、ほとんどの場合、単一のコンポーネントの障害からそのデータを保護できるように自動的に複製されます。Amazon FSx はハードウェア障害を継続的に監視し、障害が発生したインフラストラクチャコンポーネントを交換することで、障害イベントから自動的に回復します。シングル AZ ファイルシステムの場合、通常、障害復旧イベント中、およびファイルシステム用に設定した計画されたメンテナンスウィンドウ中に、約 30 分のダウンタイムが発生します。シングル AZ ファイルシステムでは、複数のコンポーネントに障害が発生したり、単一ファイルサーバーに障害が発生してファイルシステムが一貫性のない状態になったりして、まれにファイルシステムの障害を回復できない場合があります。その場合は、最新のバックアップからファイルシステムを回復できます。

マルチ AZ ファイルシステムは、Windows Server フェイルオーバー クラスタリング (WSFC) テクノロジーと 2 つの AZ のそれぞれにあるストレージボリュームセットを活用して、2 つの AZ (優先 AZ とスタンバイ AZ) に分散した Windows ファイルサーバーの高可用性クラスターで構成されます。データは、個々の AZ 内と 2 つの AZ 間で同期的に複製されます。シングル AZ 配置と比較して、マルチ AZ 配置では AZ 間でデータをさらに複製することで耐久性が向上し、スタンバイ AZ に自動的にフェイルオーバーされるため、計画的なシステムメンテナンスや計画外のサービス中断時の可用性が向上します。これにより、引き続きデータにアクセスできるようになり、インスタンスの障害や AZ の中断からデータを保護することに役立ちます。

シングル AZ またはマルチ AZ ファイルシステムのデプロイタイプを選択する

高い可用性と耐久性モデルを備えたマルチ AZ ファイルシステムは、ほとんどのプロダクションワークロードで使用することをお勧めします。シングル AZ 配置は、テストおよび開発ワークロード、アプリケーションレイヤーにレプリケーションが組み込まれ、追加のストレージレベルの冗長性を必要としない特定の本番ワークロード、および可用性と目標復旧時点 (RPO) のニーズが緩い本番ワー

クロード向けのコスト効率の高いソリューションとして設計されています。可用性と RPO のニーズが緩やかなワークロードでは、計画的なファイルシステムのメンテナンスや計画外のサービス中断が発生した場合、最大 20 分間の一時的な可用性の喪失を許容できます。また、まれに、最新のバックアップ以降のデータ更新の損失が発生することもあります。

ファイルシステムの可用性モデルを見直し、ファイルシステムのメンテナンス、スループットキャパシティの変更、計画外のサービス中断などのイベントが発生したときに選択したデプロイタイプのファイルシステムで予想される回復動作に対してワークロードに回復力があることを確認することもお勧めします。

デプロイタイプがサポートする機能

以下の表は、FSx for Windows ファイルサーバーのファイルシステムデプロイタイプがサポートする機能の概要を示したものです。

デプロイタイプ	SSD ストレージ	HDD ストレージ	DFS 名前空間	DFS レプリケーション	カスタム DNS 名	CA の共有
シングル AZ 1	✓		✓	✓	✓	
シングル AZ 2	✓	✓	✓		✓	✓*
マルチ AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * シングル AZ 2 ファイルシステムに継続的に使用可能 (CA) な共有を作成することは可能ですが、SQL Server HA のデプロイにはマルチ AZ ファイルシステムの CA 共有を使用する必要があります。

フェイルオーバープロセス

マルチ AZ 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、優先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。

- アベイラビリティーゾーンの機能停止が発生した場合。
- 優先ファイルサーバーが使用できなくなった場合。
- 優先ファイルサーバーが計画的なメンテナンスを実行する場合。

あるファイルサーバーから別のファイルサーバ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自動的に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処理し始めます。優先サブネットのリソースが使用可能になると、Amazon FSx は優先サブネット内の優先ファイルサーバーに自動的にフェイルバックします。アクティブファイルサーバ上の障害を検出してからスタンバイファイルサーバがアクティブ状態に推進するまで、フェイルオーバーは通常 30 秒以内に完了します。元のマルチ AZ 設定へのフェールバックも 30 秒以内に完了し、優先サブネット内のファイルサーバーが完全に復旧した後にのみ実行されます。

ファイルシステムがフェイルオーバーおよびフェイルバックする短い期間に、I/O が一時停止され、Amazon CloudWatch メトリクスが一時的に利用できなくなる場合があります。マルチ AZ ファイルシステムの場合、フェイルオーバーとフェイルバック中に発生するファイルの読み取りおよび書き込みアクティビティは、プライマリファイルサーバーとセカンダリファイルサーバー間で同期する必要があります。このプロセスは、HDD ストレージを持つファイルシステム、および書き込み負荷が高く IOPS が多いワークロードでは、最大数時間かかることがあります。ファイルシステムの負荷が軽いうちに、フェイルオーバーがアプリケーションに与える影響をテストすることをお勧めします。

Windows のクライアントでのフェイルオーバーのエクスペリエンス

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、新しいアクティブなファイルサーバーは、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の処理を自動的に開始します。優先サブネットのリソースが使用可能になると、Amazon FSx は優先サブネット内の優先ファイルサーバーに自動的にフェイルバックします。ファイルシステムの DNS 名が変わらないため、フェイルオーバーは Windows アプリケーションに対して透過的に行われ、マニュアル操作することなくファイルシステムオペレーションを再開することができます。アクティブファイルサーバ上の障害を検出してからスタンバイファイルサーバがアクティブ状態に推進するまで、フェイルオーバーは通常 30 秒以内に完了します。元のマルチ AZ 設定へのフェールバックも 30 秒以内に完了し、優先サブネット内のファイルサーバーが完全に復旧した後にのみ実行されます。

Linux のクライアントでのフェイルオーバーのエクスペリエンス

Linux のクライアントは、DNS ベースの自動フェイルオーバーをサポートしていません。そのため、フェイルオーバー時にスタンバイファイルサーバーに自動的に接続されることはありません。マ

ルチ AZ ファイルシステムが優先サブネット内のファイルサーバーにフェイルバックした後、ファイルシステムオペレーションを自動的に再開します。

ファイルシステムでフェイルオーバーをテストする

マルチ AZ ファイルシステムのスループット容量を変更することで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容量を変更すると、Amazon FSx はファイルシステムのファイルサーバーを切り替えます。マルチ AZ 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 は優先サーバーファイルのサーバーを最初に置き換えます。その後、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、スループット容量更新リクエストの進行状況をモニタリングできます。更新が正常に完了すると、ファイルシステムがセカンダリサーバーにフェイルオーバーされ、プライマリサーバーにフェイルバックします。ファイルシステムのスループット容量の変更、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。

シングル AZ およびマルチ AZ ファイルシステムリソース

以下のセクションで説明するように、シングル AZ ファイルシステムとマルチ AZ ファイルシステムは、サブネットと Elastic Network Interface を異なる方法で消費します。

サブネット

Virtual Private Cloud (VPC) を作成すると、 内のすべてのアベイラビリティーゾーン (AZs) にまたがります AWS リージョン。アベイラビリティーゾーンは、他のアベイラビリティーゾーンの障害から隔離されるように設計された別個の場所です。VPC を作成した後、各アベイラビリティーゾーンに 1 つまたは複数のサブネットを追加することができます。各アベイラビリティーゾーンにはデフォルト VPC のサブネットがあります。サブネットは、VPC の IP アドレスの範囲です。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

FSx for Windows File Server シングル AZ ファイルシステムには、作成時に指定するサブネットが 1 つ必要です。選択したサブネットは、ファイルシステムを作成するアベイラビリティーゾーンを定義します。

マルチ AZ ファイルシステムには、優先ファイルサーバー用とスタンバイファイルサーバー用の 2 つのサブネットが必要です。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する必要があります。

AWS アプリケーション内の場合は、レイテンシーを最小限に抑えるために、任意のファイルサーバーと同じアベイラビリティーゾーンでクライアントを起動することをお勧めします。

ファイルシステム Elastic Network Interface

Elastic Network Interface は、仮想ネットワークカードを表す VPC 内の論理ネットワークコンポーネントです。Amazon FSx ファイルシステムを作成すると、Amazon FSx はファイルシステムに関連付ける VPC に 1 つ以上の Elastic Network Interface をプロビジョニングします。Elastic Network Interface を使用すると、クライアントはファイルシステムと通信してマウントできます。Elastic Network Interface は、アカウントの VPC の一部であるにもかかわらず、Amazon FSx のサービス範囲内にあると見なされます。マルチ AZ ファイルシステムには、ファイルサーバーごとに 1 つずつ、合計 2 つの Elastic Network Interface があります。シングル AZ ファイルシステムには 1 つの elastic network interface があります。

> **Warning**
>
> ファイルシステムに関連付けられた 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、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。

次の表は、FSx for Windows File Server シングル AZ およびマルチ AZ ファイルシステムのリソース使用率をまとめたものです。

ファイルシステムのデプロイタイプ	サブネット数	Elastic Network Interface 数	IP アドレス番号
シングル AZ 2	1	1	2
シングル AZ 1	1	1	1
マルチ AZ	2	2	4

ファイルシステムが作成されると、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。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 アドレスがファイルシステムの Elastic Network Interface に添付されると、Amazon FSx は自動的にデタッチします。

Microsoft Active Directory の使用

FSx for Windows FIle Server ファイルシステムを作成するときは、そのファイルシステムを Active Directory ドメインに結合して、ユーザー認証とファイルレベルおよびフォルダレベルのアクセスコントロールを提供します。Amazon FSx は、Microsoft Active Directory と連携して、既存の Microsoft Windows 環境と統合します。Amazon FSx では、FSx for Windows File Server を Active Directory での Amazon FSx の使用 AWS Directory Service for Microsoft Active Directory および セルフマネージド Microsoft Active Directory を使用する で使用するために 2 つのオプションが用意されています。

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、管理者およびユーザーがその情報を簡単に検索および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。

その後、ユーザーは Active Directory 内の既存のユーザー ID を使用して自分自身を認証し、FSx for Windows File Server ファイルシステムにアクセスできます。ユーザーは、既存の ID を使用して、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もできます。さらに、既存のファイル、フォルダに加え、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。

> **Note**
>
> Amazon FSx は、Microsoft Azure アクティブディレクトリ に結合できる Microsoft Azure アクティブディレクトリドメインサービス をサポートしています。

ファイルシステムに対して結合したアクティブディレクトリ設定を作成した後、次のプロパティのみを更新できます。

- サービスユーザーの認証情報
- DNS サーバーの IP アドレス

ファイルシステムをさくせした後で、結合した Microsoft AD の以下のプロパティは変更できません。

- DomainName
- OrganizationalUnitDistinguishedName

- FileSystemAdministratorsGroup

ただし、バックアップから新しいファイルシステムを作成し、その新しいファイルシステムの Microsoft Active Directory 統合設定でこれらのプロパティを変更できます。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。

> **Note**
>
> Amazon FSx は Active Directory Connector および Simple Active Directory をサポートしていません。

ファイルシステムへの接続を中断する Active Directory 設定に変更があった場合、FSx for Windows File Server は [設定ミス] になることがあります。ファイルシステムを[使用可能] 状態に戻すには、Amazon FSx コンソールの [回復を試みる] ボタンを選択するか、Amazon FSx API またはコンソールで `StartMisconfiguredStateRecovery` コマンドを使用します。詳細については、「ファイルシステムが正しく設定されていない状態です」を参照してください。

トピック

- での Amazon FSx の使用 AWS Directory Service for Microsoft Active Directory
- セルフマネージド Microsoft Active Directory を使用する

での Amazon FSx の使用 AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory（AWS Managed Microsoft AD) は、クラウド内でフルマネージド型の高可用性の実際の Active Directory ディレクトリを提供します。これらの Active Directory ディレクトリは、ワークロードのデプロイで使用できます。

組織が AWS Managed Microsoft AD を使用して ID とデバイスの管理を行っている場合は、Amazon FSx ファイルシステムを と統合することをお勧めします AWS Managed Microsoft AD。これにより、Amazon FSx with AWS Managed Microsoft AD. を使用したターンキーソリューションが 2 つのサービスのデプロイ、運用、高可用性、信頼性、セキュリティ、シームレスな統合 AWS を処理し、独自のワークロードを効果的に運用することに集中できます。

AWS Managed Microsoft AD セットアップで Amazon FSx を使用するには、Amazon FSx コンソールを使用できます。コンソールで新しい FSx for Windows ファイルサーバーファイルシステムを作

成する場合は、[Windows 認証)] セクションの AWS [マネージド Microsoft Active Directory] を選択します。使用する特定のディレクトリも選択します。詳細については、「ステップ 5. ファイルシステムを作成」を参照してください。

組織は、セルフマネージドアクティブディレクトリドメイン (オンプレミスまたはクラウド) で ID とデバイスを管理している場合があります。その場合は、Amazon FSx ファイルシステムを既存のセルフマネージド型 Active Directory ドメインに直接結合できます。詳細については、「セルフマネージド Microsoft Active Directory を使用する」を参照してください。

さらに、リソースフォレスト分離モデルの恩恵を受けるようにシステムを設定することもできます。このモデルでは、Amazon FSx ファイルシステムを含むリソースを、ユーザーがいる場所から別の Active Directory フォレストに分離します。

> **Important**
>
> シングル AZ 2 およびすべてのマルチ AZ ファイルシステムの場合、Active Directory 完全修飾ドメイン名 (FQDN) は 47 文字を超えることはできません。

ネットワークの前提条件

AWS Microsoft Managed Active Directory ドメインに参加している FSx for Windows File Server ファイルシステムを作成する前に、次のネットワーク設定を作成して設定していることを確認してください。

- VPC セキュリティグループ の場合、デフォルトの Amazon VPC のデフォルトのセキュリティグループは、コンソールのファイルシステムにすでに追加されています。FSx 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と VPC ネットワーク ACL が、次の図表に示す方向のポートでのトラフィックを許可していることを確認してください。

以下の表に、各ポートのロールを示します。

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)

プロトコル	ポート	ロール
TCP / UDP	88	Kerbe認証
TCP / UDP	464	パスワードを変更/設定する
TCP / UDP	389	Lightw ht Direct Acces Protoc (LDAP
UDP	123	Netwo Time Protoc (NTP)

プロトコル	ポート	ロール
TCP	135	Distributed Comp Environt / End Point Mappe (DCE EPMA
TCP	445	Direct Servic SMB ファイル共有
TCP	636	TLS/SSL (LDAP を介した Lightwht Direct Acces Protoc (LDAP

プロトコル	ポート	ロール
TCP	3268	Micros グローバルカタログ
TCP	3269	SSL 経由の Micros グローバルカタログ
TCP	5985	WinRI 2.0 (Micro t Windo リモート管理)

プロトコル	ポート	ロール
TCP	9389	Micros AD DS ウェブサービス、PowerS
TCP	49152 - 65535	RPC 用のエフェメラルポート

> **Important**
>
> シングル AZ 2 および、すべてのマルチ AZ ファイルシステムのデプロイでは、TCP ポート 9389 でアウトバウンドトラフィックを許可する必要があります。

> **Note**
>
> VPC ネットワーク ACL を使用している場合は、FSx ファイルシステムからのダイナミックポート (49152-65535) でのアウトバウンドトラフィックも許可する必要があります。

- Amazon FSx ファイルシステムを別の VPC またはアカウントの AWS Managed Microsoft Active Directory に接続する場合は、その VPC とファイルシステムを作成する Amazon VPC 間の接続を確認します。詳細については、「別の VPC またはアカウントの AWS Managed Microsoft AD で Amazon FSx を使用する」を参照してください。

> **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、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。

Amazon FSx ネットワーク検証ツール を使用して、アクティブディレクトリドメインコントローラーへの接続を検証します。

リソースフォレスト分離モデルの使用

ファイルシステムを AWS Managed Microsoft AD 設定に結合します。次に、作成した AWS Managed Microsoft AD ドメインと既存のセルフマネージド Active Directory ドメインの間に一方向のフォレスト信頼関係を確立します。Amazon FSx での Windows 認証の場合、一方向のフォレストの信頼のみが必要です。 AWS マネージドフォレストは企業ドメインのフォレストを信頼します。

企業ドメインは信頼されたドメインのロールを、 AWS Directory Service マネージドドメインは信頼するドメインのロールを引き受けます。検証済み認証リクエストは、ドメイン間を一方向にしか移動しません。これにより、企業ドメインのアカウントがマネージドドメインで共有されているリソースに対して認証を行うことができます。この場合、Amazon FSx は AWS マネージドドメインとのみ対話します。Kerberos 認証シナリオでは、企業クライアントから発信された認証リクエストは企業ドメインによって検証され、それが を参照し AWS Managed Microsoft AD、最終的にクライアントはサービスチケットを FSx for Windows File Server ファイルシステムに提示します。信頼の詳細については、 AWS セキュリティブログの「 との信頼について知りたいこと AWS Managed Microsoft AD」の投稿を参照してください。

アクティブディレクトリの設定をテストする

Amazon FSx ファイルシステムを作成する前に、Amazon FSx ネットワーク検証ツールを使用してアクティブディレクトリドメインコントローラーへの接続を検証することをお勧めします。詳細については、「アクティブディレクトリドメインコントローラーへの接続の検証」を参照してください。

FSx for Windows File Server AWS Directory Service for Microsoft Active Directory で を使用するときは、以下の関連リソースが役立ちます。

- AWS Directory Service 管理ガイドAWS Directory Serviceの内容
- AWS Directory Service 管理ガイドのAWS 「マネージド Active Directory の作成」
- AWS Directory Service 管理ガイド で 信頼関係を作成するタイミング

別の VPC またはアカウントの AWS Managed Microsoft AD で Amazon FSx を使用する

VPC ピアリングを使用して、FSx for Windows File Server ファイルシステムを同じアカウント内の別の VPC にある AWS Managed Microsoft AD ディレクトリに結合できます。また、 AWS Managed Microsoft AD ディレクトリ共有を使用して、ファイルシステムを別の AWS アカウントのディレクトリに結合することもできます。

> **Note**
>
> は、ファイルシステム AWS リージョン と同じ AWS Managed Microsoft AD 内でのみ選択できます。クロスリージョン VPC ピアリング設定を使用する場合は、セルフマネージド型の Microsoft Active Directory を使用する必要があります。詳細については、「セルフマネージド Microsoft Active Directory を使用する」を参照してください。

ファイルシステムを別の VPC AWS Managed Microsoft AD にある に結合するワークフローには、次のステップが含まれます。

1. ネットワーク環境を設定します。
2. ディレクトリを共有します。
3. ファイルシステムを共有ディレクトリに結合します。

詳細については、「AWS Directory Service 管理ガイド」の「ディレクトリの共有」を参照してください。

ネットワーク環境を設定するには、 AWS Transit Gateway または Amazon VPC を使用して VPC ピアリング接続を作成します。さらに、ネットワークトラフィックが 2 つの VPC 間で許可されていることを確認してください。

トランジットゲートウェイ は、VPC とオンプレミスネットワークを相互接続するために使用できるネットワークの中継ハブです。VPC Transit Gateway の使用の詳細については、「Amazon VPC Transit Gateway ガイド」の「Transit Gateway の開始方法」を参照してください。

VPC ピアリング接続 は、2 つの VPC 間のネットワーク接続です。この接続では、インターネットプロトコルバージョン 4 (IPv4) またはインターネットプロトコルバージョン 6 (IPv6) のプライベートアドレスを使用して、2 つの VPC 間でトラフィックを送信できます。VPC ピアリングを使用して、同じ 内 AWS リージョン または 間で VPCs を接続できます AWS リージョン。VPC ピアリングについての詳細については、「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。

ファイルシステムを、ファイルシステムとは異なるアカウントの AWS Managed Microsoft AD ディレクトリに結合する場合、別の前提条件があります。また、Microsoft Active Directory を他のアカウントと共有します。これを行うには、 AWS Managed Microsoft Active Directory のディレクトリ共有機能を使用できます。詳細については、「AWS Directory Service 管理ガイド」の「ディレクトリの共有」を参照してください。

アクティブディレクトリドメインコントローラーへの接続の検証

アクティブディレクトリに結合している FSx for Windows ファイルサーバーファイルシステムを作成する前に、Amazon FSx アクティブディレクトリ検証ツールを使用して、アクティブディレクトリドメインへの接続を検証します。このテストは、FSx for Windows File Server を AWS Managed Microsoft Active Directory で使用するか、セルフマネージド Active Directory 設定で使用するかにかかわらず使用できます。ドメインコントローラーのネットワーク接続テスト (Test-FsxadControllerConnection) は、ドメイン内のすべてのドメインコントローラーに対して一連のネットワーク接続チェックを実行しません。代わりに、このテストを使用して、特定のドメインコントローラーのセットに対してネットワーク接続検証を実行します。

アクティブディレクトリドメインコントローラーへの接続を検証するには

1. FSx for Windows ファイルサーバーファイルシステムに使用するのと同じサブネットと、同じ Amazon VPC セキュリティグループで Amazon EC2 Windows インスタンスを起動します。マルチ AZ 配置タイプの場合は、優先アクティブファイルサーバーのサブネットを使用します。
2. EC2 Windows インスタンスをアクティブディレクトリに結合します。詳細については、「AWS Directory Service 管理ガイド」の「Windows インスタンスを手動で結合する」を参照してください。
3. EC2 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 インスタンスに接続する」を参照してください。

4. EC2 インスタンスで Windows PowerShell ウィンドウを開きます (管理者として実行 を使用)。

   Windows PowerShell で必要なアクティブディレクトリモジュールがインストールされているかどうかをテストするには、次のテストコマンドを使用します。

```
PS C:\> Import-Module ActiveDirectory
```

   上記でエラーが返された場合は、次のコマンドを使用してインストールします。

```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

5. 次のコマンドを使用して、ネットワーク検証ツールをダウンロードします。

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

6. 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 "AmazonFSxADValidation.zip"
```

7. AmazonFSxadValidation モジュールを現在のセッションに追加します。

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. アクティブディレクトリドメインコントローラーの IP アドレスの値を設定し、次のコマンドを使用して接続テストを実行します。

```
$ADControllerIp = '10.0.75.243'
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. 次の例は、テスト出力を取得し、接続テストが成功した結果を示しています。

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
```

```
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

次の例は、テストを実行して、失敗した結果を取得する方法を示しています。

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                            Value
----                            -----
TcpDetails                      {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         False
FailedTcpPorts                  {9389}
```

```
PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

```
Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx
```

> **Note**
>
> 上記の手順の代わりに、`AWSSupport-ValidateFSxWindowsADConfig`ランブックを使用してセルフマネージド Active Directory 設定を検証できます。詳細についてはAWS Systems Manager 「 自動 ランブックリファレンス」の`AWSSupport-ValidateFSxWindowsADConfig`を参照してください。

セルフマネージド Microsoft Active Directory を使用する

組織がオンプレミスまたはクラウドのセルフマネージド Active Directory を使用して ID とデバイスを管理している場合は、FSx for Windows File Server ファイルシステムを作成時に Active Directory ドメインに結合できます。

ファイルシステムをセルフマネージド Active Directory に結合すると、FSx for Windows File Server ファイルシステムは同じ Active Directory フォレスト (ドメイン、ユーザー、コンピュータを含む Active Directory 設定内の最上位の論理的なコンテナ) と、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 ドメイン内に存在します。

> **Note**
>
> Amazon FSx ファイルシステムを含むリソースを、ユーザーが常駐するフォレストとは別の Active Directory フォレストに分離できます。これを行うには、ファイルシステムを AWS Managed Microsoft Active Directory に結合し、作成した AWS Managed Microsoft Active Directory と既存のセルフマネージド Active Directory との間に一方向のフォレスト信頼関係を確立します。

- Amazon FSx がファイルシステムを Active Directory ドメインを結合させるために使用する 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
- (オプション) ファイルシステムに結合させたいドメイン内の組織単位 (OU)
- (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許可を付与するドメイングループ。たとえば、このドメイングループは、Windows ファイル共有の管理、ファイルシステムのルートフォルダ上の Access Control Lists (ACLs) の管理、ファイルとフォルダの所有権を取得できます。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ループに委任します。

> **Note**
>
> 指定するドメイングループ名は、Active Directory で一意である必要があります。FSx for Windows File Server は、以下の状況ではドメイングループを作成しません。
>
> - 指定した名前のグループが既に存在する場合
> - 名前を指定せず、「ドメイン管理者」という名前のグループが Active Directory に既に存在する場合。

詳細については、「セルフマネージド Microsoft アクティブディレクトリドメインへの Amazon FSx ファイルシステムの結合」を参照してください。

トピック

- 前提条件
- セルフマネージド Active Directory を使用する場合のベストプラクティス
- Amazon FSx サービスアカウント
- Amazon FSx サービスアカウントまたはグループへのアクセス許可の委任
- アクティブディレクトリ設定の検証
- セルフマネージド Microsoft アクティブディレクトリドメインへの Amazon FSx ファイルシステムの結合
- 手動 DNS エントリに使用する正しいファイルシステムの IP アドレスの取得
- セルフマネージド Active Directory 設定の更新
- Amazon FSx サービスアカウントの変更
- セルフマネージドアクティブディレクトリの更新のモニタリング

前提条件

FSx for Windows File Server ファイルシステムをセルフマネージド Microsoft Active Directory ドメインに結合する前に、以下の前提条件を確認して、Amazon FSx ファイルシステムをセルフマネージド Active Directory に正常に結合できるようにします。

オンプレミス構成

これらは、Amazon FSx ファイルシステムを結合するオンプレミスまたはクラウドベースのセルフマネージド Microsoft Active Directory の前提条件です。

- Active Directory ドメインコントローラー:
  - Windows Server 2008 R2 以降では、ドメイン機能レベルが必要です。
  - 書き込み可能である必要があります。
  - 到達可能なドメインコントローラーの少なくとも 1 つは、フォレストのグローバルカタログである必要があります。
- DNS サーバーは、次のように名前を解決できる必要があります。
  - ファイルシステムを結合するドメインで
  - フォレストのルートドメイン内
- DNS サーバーと Active Directory ドメインコントローラーの IP アドレスは、Amazon FSx ファイルシステムが作成された時期によって異なる以下の要件を満たしている必要があります。

2020 年 12 月 17 日以前に作成されたファイルシステムの場合	2020 年 12 月 17 日以降に作成されたファイルシステムの場合
IP アドレスは、RFC 1918 プライベート IP アドレス範囲内でなければなりません。 • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP アドレスは、以下を除く任意の範囲で指定できます。 • ファイルシステムが属する AWS リージョン 内の 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 所有 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。 • CIDR ブロック範囲内の IP アドレス: 198.19.0.0/16

2020 年 12 月 17 日以前に作成された FSx for Windows ファイルサーバーのファイルシステムに、非プライベート IP アドレス範囲を使用してアクセスする必要がある場合は、ファイルシステムのバックアップを復元して、新しいファイルシステムを作成できます。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。

- セルフマネージド Active Directory のドメイン名は、次の要件を満たしている必要があります。
  - シングルラベルドメイン (SLD) 形式ではないドメイン名。Amazon FSx は SLD ドメインをサポートしていません。
  - シングル AZ 2 およびすべてのマルチ AZ ファイルシステムの場合は、ドメイン名は 47 文字を超えることはできません。
- 定義した Active Directory サイトは、次の前提条件を満たす必要があります。
  - ファイルシステムに関連付けられている VPC 内のサブネットは、Active Directory サイトで定義する必要があります。
  - VPC サブネットと Active Directory サイトサブネットの間に競合はありません。

  Amazon FSx では、Active Directory 環境で定義したドメインコントローラーまたは Active Directory サイトへの接続が必要です。Amazon FSx は、ポート 389 でブロックされた TCP および UDP を持つドメインコントローラーを無視します。Active Directory の残りのドメインコントローラーについては、Amazon FSx 接続要件を満たしていることを確認します。さらに、サービスアカウントへの変更がこれらのすべてのドメインコントローラーに反映されていることを確認します。

> **Important**
>
> ファイルシステムの作成後に 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。これを行うと、ファイルシステムが正しく設定されなくなります。

Amazon FSx Active Directory 検証ツールを使用し、Active Directory 設定 (複数のドメインコントローラーの接続テストを含む) を検証できます。接続が必要なドメインコントローラーの数を制限するために、オンプレミスのドメインコントローラーと AWS Managed Microsoft ADの間に信頼関係を構築することもできます。詳細については、「リソースフォレスト分離モデルの使用」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している場合にのみ、ファイルシステムの DNS レコードを登録します。サードパーティーの DNS を使用している場合は、作成後にファイルシステムの DNS レコードエントリを手動で設定する必要があります。

ネットワークの設定

このセクションでは、セルフマネージド Active Directory にファイルシステムを結合するためのネットワーク設定要件について説明します。Amazon FSx Active Directory 検証ツール を使用して、ファイルシステムをセルフマネージド Active Directory に結合させる前に、これらのネットワーク設定をテストすることを強くお勧めします。

- ファイアウォールルールで Active Directory ドメインコントローラーと Amazon FSx 間の ICMP トラフィックが許可されていることを確認します。
- ファイルシステムを作成する Amazon VPC とセルフマネージド Active Directory 間で接続を設定する必要があります。AWS Direct Connect、AWS Virtual Private Network、VPC ピアリング、または AWS Transit Gateway を使用してこの接続性を設定できます。
- デフォルトの Amazon VPC のデフォルト VPC セキュリティグループが、Amazon FSx コンソールのファイルシステムに追加する必要があります。ファイルシステムを作成するサブネットのセキュリティグループと VPC ネットワーク ACL が、以下の図表に示すポート上のトラフィックを許可していることを確認します。

次の表は、プロトコル、ポート、およびそのロールを示しています。

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	464	パスワードを変更/設定する
TCP / UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	分散コンピューティング環境/エンドポイントマッパー (DCE/EPMAP)
TCP	445	Directory Services SMB ファイル共有

プロトコル	ポート	ロール
TCP	636	TLS/SSL (LDAPS) を介した Lightweight Directory Access Protocol (LDAPS)
TCP	3268	Microsoft グローバルカタログ
TCP	3269	SSL 経由の Microsoft グローバルカタログ
TCP	5985	WinRM 2.0 (Microsoft Windows リモート管理)
TCP	9389	Microsoft Active Directory DS Web サービス、PowerShell **Important** シングル AZ 2 およびマルチ AZ ファイルシステムのデプロイでは、TCP ポート 9389 でアウトバウンドトラフィックを許可する必要があります。
TCP	49152 - 65535	RPC 用のエフェメラルポート

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。

> **Note**
> VPC ネットワーク ACL を使用している場合は、ファイルシステムからのダイナミックポート (49152〜65535) でのアウトバウンドトラフィックも許可する必要があります。

> **Important**
>
> Amazon VPC セキュリティグループでは、ネットワークトラフィックが開始される方向でのみポートを開く必要がありますが、ほとんどの Windows ファイアウォールとおよび VPC ネットワーク ACL では両方向にポートを開く必要があります。

サービスアカウントのアクセス許可

サービスアカウントは、コンピュータオブジェクトをセルフマネージド Active Directory ドメインに結合させるアクセス許可を委任されたセルフマネージド Microsoft Active Directory にある必要があります。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。

以下は、ファイルシステムを結合させる OU における Amazon FSx サービスアカウントに委任されている必要がある最低限のアクセス許可です。

- Active Directory ユーザーとコンピュータ MMC で [コントロールの委任] を使用する場合
  - 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)
- Active Directory ユーザーとコンピュータ MMC で高度な機能を使用する場合
  - [許可を変更]
  - コンピュータのオブジェクトの作成
  - コンピュータオブジェクトの削除

詳細については、「Microsoft Windows Server のドキュメント」トピック「エラー: コントロールを付与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結合しようとすると、アクセスが拒否される」を参照してください。

必要な許可の設定の詳細については、「Amazon FSx サービスアカウントまたはグループへのアクセス許可の委任」を参照してください。

セルフマネージド Active Directory を使用する場合のベストプラクティス

Amazon FSx for Windows File Server ファイルシステムをセルフマネージド Microsoft Active Directory に結合させる場合は、これらのベストプラクティスに従うことをお勧めします。これらのベストプラクティスは、ファイルシステムの継続的で中断のない可用性を維持するのに役立ちます。

Amazon FSx に別のサービスアカウントを使用する

別のサービスアカウントを使用して、Amazon FSx に必要な権限を委任し、セルフマネージド Active Directory に結合しているファイルシステムを完全に管理します。この目的でドメイン管理者を使用することはお勧めしません。

Active Directory グループの使用

Active Directory グループを使用して、Amazon FSx サービスアカウントに関連付けられた Active Directory のアクセス許可と設定を管理します。

組織単位の分離 (OU)。

Amazon FSx コンピュータオブジェクトの検索と管理を容易にするために、FSx for Windows File Server ファイルシステムに使用する組織単位 (OU) を他のドメインコントローラーの懸念から分離することをお勧めします。

Active Directory 設定を最新の状態に保つ

ファイルシステムの Active Directory 設定は、変更時に常に最新の状態に保つことが必要不可欠です。例えば、セルフマネージド型 Active Directory 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場合、パスワードがリセットされたらすぐに、ファイルシステムのサービスアカウントのパスワードを更新してください。詳細については、「セルフマネージド Active Directory 設定の更新」を参照してください。

Amazon FSx サービスアカウントの変更

新しいサービスアカウントでファイルシステムを更新する場合、Active Directory に結合するために必要なアクセス許可と権限があり、ファイルシステムに関連付けられた既存のコンピュータオブジェクトに対するフルコントロールアクセス許可を持っている必要があります。詳細については、「Amazon FSx サービスアカウントの変更」を参照してください。

サブネットを単一の Microsoft Active Directory サイトに割り当てる

Active Directory 環境に多数のドメインコントローラーがある場合は、Active Directory サイトとサービスを使用して、Amazon FSx ファイルシステムで使用されるサブネットを、可用性と信頼性が最も高い単一の Active Directory サイトに割り当てます。VPC セキュリティグループ、VPC

ネットワーク ACL、DCs の Windows ファイアウォールルール、および Active Directory インフラストラクチャにあるその他のネットワークルーティングコントロールが、必要なポートで Amazon FSx からの通信を許可していることを確認します。これにより、割り当てられた Active Directory サイトを使用できない場合、Windows は他のドメインコントローラーに戻すことができます。詳細については、「Amazon VPC を使用した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。

セキュリティグループルールを使用してトラフィックを制限する

セキュリティグループルールを使用して、仮想プライベートクラウド (VPC) に最小特権のプリンシパルを実装します。VPC セキュリティグループルールを使用して、ファイルで許可されるインバウンドおよびアウトバウンドのネットワークトラフィックのタイプを制限できます。例えば、セルフマネージド Active Directory ドメインコントローラーへのアウトバウンドトラフィック、または使用しているサブネットまたはセキュリティグループ内のアウトバウンドトラフィックのみを許可することをお勧めします。詳細については、「Amazon VPC を使用した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。

Amazon FSx で作成されたコンピュータオブジェクトを移動させないでください。

> **Important**
>
> ファイルシステムの作成後に 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。これを行うと、ファイルシステムが正しく設定されなくなります。

Active Directoryの設定を検証する

Active Directory に結合している FSx for Windows File Server ファイルシステムを結合しようとする前に、Amazon FSx Active Directory 検証ツールを使用して、Active Directory 設定を検証します。

Amazon FSx サービスアカウント

セルフマネージド Active Directory に結合している Amazon FSx ファイルシステムには、その有効期間を通じて有効なサービスアカウントが必要です。Amazon FSx はサービスアカウントを使用してファイルシステムを完全に管理し、Active Directory ドメインへのコンピュータオブジェクトの結合解除と再結合を必要とする管理タスクを実行します。これらのタスクには、障害が発生したファイルサーバーの置き換えや Microsoft Windows Server ソフトウェアのパッチ適用が含まれます。Amazon

FSx がこれらのタスクを実行するには、Amazon FSx サービスアカウントに、少なくとも委任された サービスアカウントのアクセス許可 で説明されている一連のアクセス許可が必要です。

ドメイン管理者グループのメンバーには、これらのタスクを実行するのに十分な権限がありますが、必要な権限を Amazon FSx に委任するには、別のサービスアカウントを使用することを強くお勧めします。

[Active Directory ユーザーおよびコンピュータ] MMC スナップインの [コントロールの委任]または [高度な機能]を使用して権限を委任する方法については、「Amazon FSx サービスアカウントまたはグループへのアクセス許可の委任」を参照してください。

ファイルシステムを新しいサービスアカウントで更新する場合は、その新しいサービスアカウントに、Active Directory に結合するのに必要なアクセス許可と権限があり、ファイルシステムに関連付けられている既存のコンピュータオブジェクトに対する [フルコントロール] 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。詳細については、「Amazon FSx サービスアカウントの変更」を参照してください。

Amazon FSx サービスアカウントまたはグループへのアクセス許可の委任

Amazon FSx サービスアカウントまたは管理者グループは、FSx for Windows File Server ファイルシステムをセルフマネージド Active Directory ドメインに結合するために必要な権限を持っている必要があります。これらのアクセス許可を委任するには、次の手順で説明するように、Active Directory User and Computers MMC スナップインで [コントロールの委任] または [高度な機能] のいずれかを使用できます。

[コントロールの委任] を使用してアクセス許可を割り当てるには

[コントロールの委任] を使用してサービスアカウントまたはグループにアクセス許可を割り当てるには

1. Active Directory ドメインのドメイン管理者としてシステムにログインします。
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. [追加] を選択して Amazon FSx サービスアカウントまたはグループの名前を追加し、[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. [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)
11. [Next] (次へ) を選択し、[Finish] (完了) を選択します。
12. 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。

[高度な機能] を使用して次のようにアクセス許可を割り当てるには

1. Active Directory ドメインのドメイン管理者としてシステムにログインします。
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. メニューバーから [表示] を選択し、[高度な機能] が有効になっていることを確認します (機能が有効になっている場合、横にチェックマークが表示されます)。
4. タスクペインで、ドメインノードを展開します。
5. 変更する OU のコンテキストメニューを見つけて (右クリックで) 開き、[プロパティ] をクリックします。
6. [OU のプロパティ] ペインで [セキュリティ] タブをクリックします。
7. [セキュリティ] タブで [アドバンスト] をクリックします。次に、[追加] をクリックします。
8. [許可エントリ] ページで [プリンシパルを選択] をクリックし、Amazon FSx サービスアカウントまたはグループの名前を入力します。適用先： で、このオブジェクトとすべての子孫コンピュータを選択します。次の許可が選択されていることを確認します。
    - [許可を変更]
    - [コンピュータオブジェクトの作成]
    - [コンピュータオブジェクトの削除]

9. [適用] を選択してから [OK] を選択します。
10. 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。

アクティブディレクトリ設定の検証

アクティブディレクトリに結合している FSx for Windows ファイルサーバーファイルシステムを作成する前に、Amazon FSx アクティブディレクトリ検証ツールを使用して、アクティブディレクトリ設定を検証します。アクティブディレクトリ設定を正常に検証するには、アウトバウンドのインターネット接続が必要であることに注意してください。

アクティブディレクトリの設定を検証するには

1. FSx for Windows ファイルサーバーファイルシステムに使用するのと同じサブネットと、同じ Amazon VPC セキュリティグループで Amazon EC2 Windows インスタンスを起動します。EC2 インスタンスが `AmazonEC2ReadOnlyAccess` IAM アクセス許可を必要としていることを確認します。IAM ポリシーシミュレーターを使用して、EC2 インスタンスロールのアクセス許可を検証できます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーシミュレーターを使用した IAM ポリシーのテスト」を参照してください。
2. EC2 Windows インスタンスをアクティブディレクトリに結合します。詳細については、「AWS Directory Service 管理ガイド」の「Windows インスタンスを手動で結合する」を参照してください。
3. EC2 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 インスタンスに接続する」を参照してください。
4. EC2 インスタンスで Windows PowerShell ウィンドウを開きます (管理者として実行 を使用)。

   Windows PowerShell で必要なアクティブディレクトリモジュールがインストールされているかどうかをテストするには、次のテストコマンドを使用します。

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   上記でエラーが返された場合は、次のコマンドを使用してインストールします。

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```

5. 次のコマンドを使用して、ネットワーク検証ツールをダウンロードします。

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

6. 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 "AmazonFSxADValidation.zip"
```

7. `AmazonFSxADValidation` モジュールを現在のセッションに追加します。

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. 以下のコマンドを代入して、必要なパラメータを設定します。

   - アクティブディレクトリドメイン名 (*DOMAINNAME.COM*)
   - 次のいずれかのオプションを使用して、サービスアカウントのパスワードの `$Credential` オブジェクトを準備します。
     - 認証情報オブジェクトをインタラクティブに生成するには、次のコマンドを使用します。

       ```
       $Credential = Get-Credential
       ```

     - AWS Secrets Manager リソースを使用して認証情報オブジェクトを生成するには、次のコマンドを使用します。

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - DNS サーバーの IP アドレス (*IP_ADDRESS_1*、*IP_ADDRESS_2*)
   - Amazon FSx ファイルシステムを作成する予定のサブネットのサブネット ID (例えば、*SUBNET_1*、*SUBNET_2*、`subnet-04431191671ac0d19`)。

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
```

```
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (オプション) 検証ツールを実行する前に `README.md` ファイルに含まれる以下の指示に従って、組織単位、委任された管理者グループ、DomainControllersMaxCount を設定し、サービスアカウントの許可を有効にします。

> **Note**
>
> オペレーティングシステムが英語でない場合は、`Domain Admins` グループの名前は異なります。例えば、フランス語の OS バージョンではグループの名前は `Administrateurs du domaine` です。値を指定していない場合、デフォルトの `Domain Admins` グループ名が使用され、ファイルシステムの作成は失敗します。

10. このコマンドを使用して検証ツールを実行します。

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. 以下に、正常なテスト結果の例を示します。

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

以下に、エラーのあるテスト結果の例を示します。

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
```

```
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

検証ツールの実行時に警告またはエラーが表示された場合は、検証ツールパッケージ (TROUBLESHOOTING.md) および Amazon FSx のトラブルシューティング に含まれるトラブルシューティングガイドを参照してください。

セルフマネージド Microsoft アクティブディレクトリドメインへの Amazon FSx ファイルシステムの結合

新しい FSx for Windows ファイルサーバーファイルシステムを作成するときに、セルフマネージド Microsoft アクティブディレクトリドメインに結合するように Microsoft アクティブディレクトリ統合を設定できます。これを行うには、Microsoft アクティブディレクトリに次の情報を指定します。

- オンプレミスの Microsoft Active Directory のディレクトリの完全修飾ドメイン名 (FQDN)。

> **Note**
>
> Amazon FSx は現在、シングルラベルドメイン (SLD) ドメインをサポートしていません。

- ドメインの DNS サーバーの IP アドレス。
- オンプレミスの Microsoft アクティブディレクトリのドメイン内のサービスアカウントの認証情報。Amazon FSx は、これらの認証情報を使用して、セルフマネージド Active Directory に結合します。

オプションで、以下を指定することもできます。

- Amazon FSx ファイルシステムに結合させたいドメイン内の特定の組織単位 (OU)。
- メンバーに Amazon FSx ファイルシステムの管理者許可が付与されているドメイングループの名前。指定するドメイングループ名は、Active Directory で一意である必要があります。

この情報を指定した後、Amazon FSx は、指定したサービスアカウントを使用して、新しいファイルシステムをセルフマネージド Active Directory ドメインに結合します。

> **Important**
>
> Amazon FSx は、結合しているアクティブディレクトリドメインがデフォルトの DNS として Microsoft DNS を使用している場合のみ、ファイルシステムの DNS レコードを登録します。サードパーティー DNS を使用している場合は、ファイルシステムを作成した後、Amazon FSx ファイルシステムの DNS エントリを手動で設定する必要があります。ファイルシステムに使用する正しい IP アドレスの選択の詳細については、「手動 DNS エントリに使用する正しいファイルシステムの IP アドレスの取得」を参照してください。

開始する前に

セルフマネージド Microsoft Active Directory を使用する で 前提条件 の詳細を完了していることを確認してください。

セルフマネージド Active Directory に結合した FSx for Windows ファイルサーバーファイルシステムを作成するには (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. ダッシュボードで [Create file system] (ファイルシステムの作成) を選択して、ファイルシステム作成ウィザードを起動します。
3. FSx for Windows ファイルサーバー を選択してから、[Next] (次へ) を選択します。[Create file system] (ファイルシステムの作成) ページが表示されます。
4. ファイルシステムの名前を入力します。最大 256 文字の Unicode 文字、空白文字、数字、および特殊文字 (+ - = . _ : /) を使用できます。
5. 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 (GiB 単位) を入力します。SSD ストレージを使用している場合は、32 ~ 65,536 の範囲で任意の整数を入力します。HDD ストレージを使用している場合は、2,000 ~ 65,536 の範囲で任意の整数を入力します。ファイルシステムの作成した後、いつでも必要な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。
6. スループット容量 はデフォルト設定のままにします。スループット容量 は、ファイルシステムをホストするファイルサーバーがデータを提供できる持続可能速度です。推奨スループット容量設定は、選択したストレージ容量に基づきます。推奨スループット容量を超える容量が必要な場合は、[Specify throughput capacity] (スループット容量の指定) を選択し、値を選択します。詳細については、「FSx for Windows File Server のパフォーマンス」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作成した後、いつでも必要に応じて変更できます。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。

7. ファイルシステムに関連付ける VPC を選択します。この入門演習では、 AWS Directory Service ディレクトリおよび Amazon EC2 インスタンスと同じ VPC を選択します。
8. アベイラビリティーゾーン と サブネット の値を選択します。
9. VPCセキュリティグループ については、デフォルトの Amazon VPC のデフォルトセキュリティグループが、コンソールのファイルシステムに、すでに追加されています。FSx 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と VPC ネットワーク ACL が、次の図表に示す方向のポートでのトラフィックを許可していることを確認してください。

以下の表に、各ポートのロールを示します。

プロトコル	ポート	ロール
TCP / UDP	53	ドメイン

プロトコル	ポート	ロール
		ネームシステム (DNS)
TCP / UDP	88	Kerbe 認証
TCP / UDP	464	パスワードを変更 / 設定する
TCP / UDP	389	Lightw ht Direct Acces Protoc (LDAP
UDP	123	Netwo Time Protoc (NTP)

プロトコル	ポート	ロール
TCP	135	Distributed Comp Environt / End Point Mappe (DCE EPMA
TCP	445	Direct Servic SMB ファイル共有
TCP	636	TLS/SSL (LDAP を介した Lightwht Direct Acces Protoc (LDAP

プロトコル	ポート	ロール
TCP	3268	Micros グローバルカタログ
TCP	3269	SSL 経由の Micros グローバルカタログ
TCP	5985	WinRI 2.0 (Micro t Windo リモート管理)

プロトコル	ポート	ロール
TCP	9389	Micros Active Direct DS Web サービス、P rShell
TCP	49152 - 65535	RPC 用のエフェメラルポート

> **Important**
>
> シングル AZ 2 および、すべてのマルチ AZ ファイルシステムのデプロイでは、TCP ポート 9389 でアウトバウンドトラフィックを許可する必要があります。

> **Note**
>
> VPC ネットワーク ACL を使用している場合は、FSx ファイルシステムからのダイナミックポート (49152-65535) でのアウトバウンドトラフィックも許可する必要があります。

- セルフマネージド Microsoft アクティブディレクトリドメインの DNS サーバーおよびドメインコントローラーに関連付けられた、IP アドレスへのすべてのトラフィックを許可するアウトバウンドルール。詳細については、「アクティブディレクトリ通信用のファイアウォールの設定に関する Microsoft のドキュメント」を参照してください。
- これらのトラフィックルールが、アクティブディレクトリドメインコントローラー、DNS サーバー、FSx クライアント、および 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ことを確認してください。

> **Note**
>
> アクティブディレクトリのサイトが定義されている場合、Amazon FSx ファイルシステムに関連付けられた VPC 内のサブネットがアクティブディレクトリのサイトで定義されていること、および VPC 内のサブネットとその他のサイトのサブネットの間に競合が存在しないことを確認する必要があります。これらの設定は、アクティブディレクトリのサイトとサービス MMC スナップインを使用して、表示および変更することができます。

> **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。

10. [Windows authentication] (Windows 認証) で、[Self-managed Microsoft Active Directory] (セルフマネージド Microsoft アクティブディレクトリ) を選択します。
11. セルフマネージド Microsoft アクティブディレクトリのディレクトリの [完全修飾ドメイン名] の値を入力します。

> **Note**
> ドメイン名は、シングルラベルドメイン (SLD) 形式であってはなりません。現在 Amazon FSx では SLD ドメインをサポートしていません。

> **Important**
> シングル AZ 2 およびすべてのマルチ AZ ファイルシステムの場合は、アクティブディレクトリドメイン名は 47 文字を超えることはできません。

12. セルフマネージド Microsoft アクティブディレクトリのディレクトリの [組織単位] の値を入力します。

> **Note**
> 指定したサービスアカウントに、ここで指定する OU、または指定しない場合はデフォルトの OU に委任された、アクセス許可があることを確認します。

13. セルフマネージド Microsoft アクティブディレクトリのディレクトリの [DNS サーバー IP アドレス] に 1 つ以上、2 つ以下の値を入力します。
14. `ServiceAcct` など、セルフマネージド Active Directory ドメインのアカウントの [サービスアカウントのユーザーネーム] の文字列値を入力します。Amazon FSx は、このユーザー名を使用して Microsoft アクティブディレクトリドメインに結合します。

> **Important**
> [Service account username] (サービスアカウントのユーザーネーム) を入力するときは、ドメインプレフィクス (`corp.com\ServiceAcct`) またはドメインサフィックス (`ServiceAcct@corp.com`) は含めないでください。
> [Service account username] (サービスアカウントのユーザーネーム) (`CN=ServiceAcct,OU=example,DC=corp,DC=com`) を入力するときは、識別名 (DN) を使用しないでください。

15. セルフマネージド Active Directory ドメインのアカウントの [サービスアカウントのパスワード] の値を入力します。Amazon FSx は、このパスワードを使用して Microsoft アクティブディレクトリドメインに結合します。

16. パスワードを再入力して [Confirm password] (パスワードを確認) で確認します。
17. [委任されたファイルシステム管理者グループ] で、`Domain Admins` グループ、またはカスタムの委任されたファイルシステム管理者グループ (自身で作成した場合)を指定してください。指定したグループには、ファイルシステムで管理タスクを実行するための委任許可が与えられます。値を入力しない場合、Amazon FSx はビルトイン `Domain Admins` グループを使用します。Amazon FSx は、組み込みコンテナにある `Delegated file system administrators group` (指定した `Domain Admins` グループまたはカスタムグループのいずれか) を保持することをサポートしてないことに注意してください。

> **Important**
>
> [委任されたファイルシステム管理者グループ] を提供しない場合、デフォルトでは、Amazon FSx はアクティブディレクトリドメインで組み込み `Domain Admins` グループを使用しようとします。このビルトイングループの名前が変更された場合、またはドメイン管理に別のグループを使用している場合は、そのグループの名前をここに指定する必要があります。

> **Important**
>
> グループ名のパラメータを指定するときは、ドメインプレフィックス (corp.com \ FSxAdmins) またはドメインサフィックス (FSxAdmins@corp.com) を含めないでください。
> グループには識別名 (DN) を使用しないでください。識別名の例には、CN=FSxAdmins、OU=example、DC=corp、DC=com が挙げられます。

セルフマネージド Active Directory に結合した FSx for Windows ファイルサーバーファイルシステムを作成するには (AWS CLI)

次の例では、`us-east-2` アベイラビリティーゾーンにおける `SelfManagedActiveDirectoryConfiguration` で FSx for Windows ファイルサーバーファイルシステムを作ります。

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
```

```
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> ファイルシステムの作成後に 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。これを行うと、ファイルシステムが正しく設定されなくなります。

手動 DNS エントリに使用する正しいファイルシステムの IP アドレスの取得

Amazon FSx は、Microsoft DNS をデフォルトの DNS サービスとして使用している場合にのみ、ファイルシステムの DNS レコードを登録します。サードパーティーの DNS を使用している場合は、Amazon FSx ファイルシステムの DNS エントリを手動で設定する必要があります。このセクションでは、ファイルシステムを DNS に手動で追加する必要がある場合に使用する、正しいファイルシステムの IP アドレスを取得する方法について説明します。ファイルシステムが作成されると、ファイルシステムが削除されるまでその IP アドレスを変更できないことに注意してください。

DNS A エントリに使用するファイルシステムの IP アドレスを取得する方法

1. https://console.aws.amazon.com/fsx/ で、IP アドレスを取得したいファイルシステムを選択すると、ファイルシステムの詳細ページが表示されます。
2. [Network & security] (ネットワークとセキュリティ) タブで、次のいずれかを実行します。
   - シングル AZ 1 ファイルシステムの場合:
     - [Subnet] (サブネット) パネルで、[Network Interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
     - [Primary private IPv4 IP] (プライマリプライベート IPv4 IP) 列には、シングル AZ 1 ファイルシステムが使用する IP アドレスが表示されます。

- シングル AZ 2 またはマルチ AZ ファイルシステムの場合:
  - [Preferred subnet] (優先サブネット) パネルで、[Network interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
  - 使用する優先サブネットの IP アドレスは、[Secondary private IPv4 IP] (セカンダリプライベート IPv4 IP) 列に表示されます。
  - Amazon FSx の [Standby subnet] (スタンバイサブネット) パネルで、[Network Interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
  - 使用するスタンバイサブネットの IP アドレスは、[Secondary private IPv4 IP] (セカンダリプライベート IPv4 IP) 列に表示されます。

> **Note**
>
> シングル AZ 2 またはマルチ AZ ファイルシステムの Windows Remote PowerShell エンドポイントに DNS エントリを設定する必要がある場合は、[優先サブネット] の Elastic Network Interface に [プライマリプライベート IPv4 アドレス] を使用する必要があります。詳細については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

セルフマネージド Active Directory 設定の更新

Amazon FSx ファイルシステムの継続的で中断のない可用性を確保するには、次の Active Directory プロパティのいずれかが変更されたときに、ファイルシステムの Active Directory 設定を更新する必要があります。

- DNS サーバーの IP アドレス
- セルフマネージド Active Directory のサービスアカウント認証情報

Amazon FSx ファイルシステムのセルフマネージド Active Directory 設定を更新すると、更新が適用されている間にファイルシステムの状態が [利用可能] から [更新中] に変わります。更新が適用された後、状態が [Available] (利用可能) に戻っているか検証します。更新が完了するまでには、数分かかる場合があることに注意してください。詳細については、「セルフマネージドアクティブディレクトリの更新のモニタリング」を参照してください。

更新されたセルフマネージド Active Directory 設定に問題がある場合は、ファイルシステムの状態は [設定ミス] に切り替わります。この状態では、コンソール、API、および CLI のファイルシステムの説明の横にエラーメッセージと推奨される修正アクションが表示されます。推奨される修正アクションを実行した後、最終的にファイルシステムの状態が [Available] (使用可能) に変更したかを確認します。

> **Important**
>
> ファイルシステムを新しいサービスアカウントで更新する場合は、その新しいサービスアカウントにファイルシステムに関連付けられている既存のコンピュータオブジェクトに対するフルコントロール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。

セルフマネージド Active Directory 設定に関連する可能性のある問題のトラブルシューティングについては、「ファイルシステムが正しく設定されていない状態です」を参照してください。

AWS Management Console、Amazon FSx API、または を使用して、ファイルシステムのセルフマネージド Active Directory 設定のサービスアカウントのユーザー名とパスワードと DNS サーバーの IP アドレス AWS CLI を更新できます。セルフマネージド Active Directory 設定の更新の進行状況は AWS Management Console、、CLI、および API を使用していつでも追跡できます。詳細については、「セルフマネージドアクティブディレクトリの更新のモニタリング」を参照してください。

セルフマネージドアクティブディレクトリの設定を更新するには (コンソール)

1. Amazon FSx コンソール (https://console.aws.amazon.com/fsx/) を開きます。
2. [ファイルシステム] に移動し、セルフマネージド Active Directory 設定を更新する Windows 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) タブで、DNS サーバーの IP アドレス については [Update] (更新) を選択します。またはサービスアカウントのユーザーネームについては、更新するアクティブディレクトリプロパティによって異なります。
4. 表示されるダイアログに、新しい DNS サーバーの IP アドレスまたは新しいサービスアカウントの認証情報を入力します。
5. [Update] (更新) を選択して、アクティブディレクトリ設定の更新を開始します。

   更新の進行状況は、 または を使用してモニタリングできます AWS CLI。 AWS Management Console

セルフマネージドアクティブディレクトリ設定 (CLI) を更新するには

- FSx for Windows File Server ファイルシステムのセルフマネージド Active Directory 設定を更新するには、 AWS CLI コマンド update-file-system を使用します。以下のパラメータを設定します。
  - 更新するファイルシステムの ID への `--file-system-id`。
  - `UserName` セルフマネージド Active Directory サービスアカウントの新しいユーザーネーム。
  - `Password` セルフマネージド Active Directory アカウントの新しいパスワード。
  - `DnsIps` セルフマネージド Active Directory DNS サーバーの IP アドレス。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
     DnsIps=[192.0.2.0,192.0.2.24]}'
```

更新アクションが成功すると、サービスは HTTP 200 レスポンスを返します。レスポンス内の `AdminstrativeActions` オブジェクトは、リクエストとそのステータスを記述します。

Amazon FSx サービスアカウントの変更

ファイルシステムを新しいサービスアカウントで更新する場合は、その新しいサービスアカウントに Active Directory を結合させるのに必要なアクセス許可と権限、およびファイルシステムに関連付けられている既存のコンピュータオブジェクトに対する [フルコントロール] 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。さらに、新しいサービスアカウントが、[グループポリシー] 設定の [ドメインコントローラー: ドメイン結合中にコンピュータアカウントの再利用を許可する] が有効な信頼されたアカウントの一部であることを確認します。

Active Directory グループを使用して、サービスアカウントに関連付けられた Active Directory のアクセス許可と設定を管理することを強くお勧めします。

Amazon FSx のサービスアカウントを変更する場合、サービスアカウントに次の設定があることを確認してください。

- 新しいサービスアカウント (またはメンバーである Active Directory グループ) が、ファイルシステムに関連付けられている既存のコンピュータオブジェクトに対するフルコントロールアクセス許可を持っている。

- 新規および以前のサービスアカウント (またはそれらが属する Active Directory グループ) は、Active Directory のすべてのドメインコントローラーで、[ドメインコントローラー: ドメイン結合中にコンピュータアカウントを再利用を許可する] グループポリシー設定が有効になっている信頼されたアカウント (または信頼された Active Directory グループ) の一部です。

サービスアカウントがこれらの要件を満たしていない場合、次の条件が発生する可能性があります。

- シングル AZ ファイルシステムの場合、ファイルシステムは MISCONFIGURED_UNAVAILABLE になる可能性があります。
- マルチ AZ ファイルシステムでは、ファイルシステムが MISCONFIGURED になり、RemotePowerShell エンドポイント名が変更される可能性があります。

ドメインコントローラーのグループポリシーの設定

次の Microsoft の推奨手順では、ドメインコントローラーグループポリシーを使用して許可リストポリシーを設定する方法について説明します。

ドメインコントローラーの許可リストポリシーを設定するには

1. 2023 年 9 月 12 日以降の Microsoft Windows 更新プログラムを、セルフマネージド Microsoft Active Directory のすべてのメンバーコンピュータとドメインコントローラーにインストールします。
2. セルフマネージド Active Directory 内のすべてのドメインコントローラーに適用される新規または既存のグループポリシーで、以下の設定を行います。
   a. [コンピュータ設定] > [ポリシー] > [Windows 設定] > [セキュリティ設定] > [ローカルポリシー] > [セキュリティオプション] の順にに移動します。
   b. [ドメインコントローラー: ドメイン結合中にコンピュータアカウントの再利用を許可する] をダブルクリックします。
   c. [このポリシー設定と<セキュリティの編集...>を定義] を選択します。
   d. オブジェクトピッカーを使用して、信頼できるコンピュータアカウント作成者と所有者のユーザーまたはグループを [許可] アクセス許可に追加します。(ベストプラクティスとして、アクセス許可にグループを使用することを強くお勧めします)。ドメイン結合を実行するユーザーアカウントを追加しないでください。

> **Warning**
>
> メンバーシップを信頼されたユーザーとサービスアカウントに限定します。認証されたユーザー、全員、またはその他の大きなグループをこのポリシーに追加しないでください。代わりに、特定の信頼されたユーザーとサービスアカウントをグループに追加し、それらのグループをポリシーに追加します。

3. グループポリシーの更新間隔を待つか、すべてのドメインコントローラーで gpupdate /force を実行します。
4. HKLM\System\CCS\Control\SAM – “ComputerAccountReuseAllowList” レジストリキーに目的の SDDL が入力されていることを確認します。レジストリを手動で編集しないでください。
5. 2023 年 9 月 12 日以降の更新がインストールされているコンピュータへの結合を試みます。ポリシーに記載されているアカウントの 1 つがコンピュータアカウントを所有していることを確認します。また、レジストリで NetJoinLegacyAccountReuse キーが有効になっていない (1 に設定) ことを確認してください。ドメイン結合が失敗した場合、**`c:\windows\debug\netsetup.log`** を確認します。

セルフマネージドアクティブディレクトリの更新のモニタリング

次の手順で説明するように AWS Management Console、、 API、または を使用して AWS CLI、セルフマネージド Active Directory 設定更新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セルフマネージド Active Directory 設定を更新すると、更新が適用されている間にファイルシステムの状態が [利用可能] から [更新中] に変わります。更新が完了すると、状態は [利用可能] に戻ります。Active Directory 設定の更新が完了するまでに最大数分かかる場合があります。

コンソールで更新をモニタリングする

ファイルシステムの詳細 ウィンドウの [Updates] (更新) タブでは、更新の種類ごとに最新の更新プログラムを 10 個表示できます。

セルフマネージドアクティブディレクトリの更新の場合、次の情報を表示できます。

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:

- DNS サーバーの IP アドレス
- サービスアカウントの認証情報

ターゲット値

ファイルシステムのプロパティを更新する目標値。サービスアカウントの認証情報 の更新の場合、ユーザー名のみが表示され、サービスアカウントのパスワードはこのフィールドに含まれません。

[Status] (ステータス)

更新の現在のステータス。セルフマネージドアクティブディレクトリの更新の場合、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) - ファイルシステムの更新が正常に完了しました。
- [Failed] (失敗) - ファイルシステムの更新に失敗しました。障害の詳細を見るには、疑問符 (?) を選択します。

[Progress %] (進行状況 %)

ファイルシステムの更新の進行状況を、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。

AWS CLI および API を使用した更新のモニタリング

describedescribe-file-systems AWS CLI コマンドと DescribeFileSystems API アクションを使用して、進行中のファイルシステム更新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。

以下の例では、2 つのセルフマネージド Active Directory ファイルシステムの更新を表す describe-file-systems CLI コマンドのレスポンスの抜粋を示しています。

```
{
    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 1000,
    "AdministrativeActions": [
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1581694766.757,
            "Status": "PENDING",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                        "UserName": "serviceUser",
                    }
                }
            }
        },
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1619032957.759,
            "Status": "FAILED",
            "TargetFileSystemValues": {
```

```
                        "WindowsConfiguration": {
                            "SelfManagedActiveDirectoryConfiguration": {
                            "DnsIps": [
                                    "10.0.138.161"
                                ]
                            }
                        }
                    },
                    "FailureDetails": {
                        "Message": "Failure details message."
                    }
                }
            ],
    .
    .
    .
```

FSx for Windows File Server のパフォーマンス

FSx for Windows File Server は、さまざまなパフォーマンスニーズを満たすファイルシステム設定オプションを提供します。以下では、Amazon FSx 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設定オプションと役に立つパフォーマンスのヒントを説明します。

トピック

- ファイルシステムのパフォーマンス
- パフォーマンスに関するその他の考慮事項
- 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
- 適切なレベルのスループットキャパシティの選択
- ストレージ構成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
- CloudWatch メトリクスを使用したパフォーマンスの測定
- ファイルシステムのパフォーマンスの問題のトラブルシューティング

ファイルシステムのパフォーマンス

各 FSx for Windows File Server ファイルシステムは、クライアントが通信する Windows ファイルサーバーと、ファイルサーバーに接続されたストレージボリューム (ディスク) のセットで構成されます。各ファイルサーバは、高速のインメモリキャッシュを使用して、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。

次の図は、FSx for Windows File Server ファイルシステムからデータにアクセスする方法を示しています。

クライアントがインメモリキャッシュに保存されているデータにアクセスすると、そのデータはネットワーク I/O として要求元のクライアントに直接提供されます。ファイルサーバーは、データをディスクから読み取ったりディスクに書き込んだりする必要はありません。このデータアクセスのパフォーマンスは、ネットワーク I/O の上限とインメモリキャッシュのサイズによって決まります。

クライアントがキャッシュにないデータにアクセスすると、ファイルサーバーはそのデータをディスク I/O としてディスクから読み取ったり、ディスクに書き込んだりします。その後、データはネットワーク I/O としてファイルサーバーからクライアントに提供されます。このデータアクセスのパフォーマンスは、ネットワーク I/O の上限とディスク I/O の上限によって決まります。

ネットワーク I/O のパフォーマンスとファイルサーバーのインメモリキャッシュは、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ります。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ストレージ構成の組み合わせによって決まります。ファイルシステムが達成できる最大ディスク I/O パフォーマンス (ディスクスループットとディスク IOPS レベルから構成される) は、以下のいずれか低い値になります。

- 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 I/O パフォーマンスレベル。
- ストレージ構成 (ファイルシステム用に選択したストレージ容量、ストレージタイプ、SSD IOPS レベル) によって提供されるディスク I/O パフォーマンスレベル。

パフォーマンスに関するその他の考慮事項

ファイルシステムのパフォーマンスは、通常、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

FSx for Windows File Server では、高速のインメモリキャッシュを使用して、アクティブにアクセスするデータに対して一貫したサブミリ秒のレイテンシーを実現します。インメモリキャッシュにないデータ、つまり、基盤となるストレージボリュームで I / O を実行する必要があるファイル操作の場合、Amazon FSx はソリッドステートドライブ (SSD) ストレージでサブミリ秒のファイル操作のレイテンシーを提供し、ハードディスクドライブ (HDD) ストレージでは 1 桁ミリ秒のレイテンシーを提供します。

スループットと IOPS

Amazon FSx ファイルシステムは、Amazon FSx が利用可能なすべての AWS リージョン で最大 2 GBps と 80,000 IOPS を提供し、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、アジアパシフィック (東京) 、アジアパシフィック (シンガポール) で 12 GBps のスループットと 400,000 IOPS を提供します。ファイルシステムでワークロードが駆動できるスループットと IOPS の特定量は、ファイルシステムのスループットキャパシティ、ストレージ容量、およびストレージタイプ、そしてアクティブなワーキングセットのサイズなどワークロードの性質によって異なります。

シングルクライアントパフォーマンス

Amazon FSx を使用すると、ファイルシステムにアクセスする単一のクライアントからファイルシステムのフルスループットと IOPS レベルまで到達できます。Amazon FSx は [SMB Multichannel] (SMB マルチチャネル) をサポートしています。この機能により、ファイルシステムにアクセスする 1 つのクライアントに対して、最大複数の GBps スループットと数十万 IOPS を提供できます。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。Windows でサポートされている SMB 接続の数には理論上の制限がありますが、この制限は数百万で、実際には無制限の数の SMB 接続を持つことができます。

バーストパフォーマンス

ファイルベースのワークロードは通常、スパイキーであり、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、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

スラインを下回るとクレジットが計上され、I/O オペレーションの実行時にこれらのクレジットを使用できます。

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

スループットキャパシティは、次のカテゴリにおいてファイルシステムのパフォーマンスを決定します。

- ネットワーク I/O – ファイルサーバーがファイルデータにアクセスしているクライアントに対してファイルデータを提供できる速度。
- ファイルサーバーの CPU とメモリ – ファイルデータの提供や、データ重複排除やシャドウコピーなどのバックグラウンドアクティビティの実行に使用できるリソース。
- ディスク I/O – ファイルサーバーがファイルサーバーとストレージボリューム間の I/O をサポートできる速度。

次の表は、プロビジョニングされた各スループットキャパシティ設定で制御できるネットワーク I/O (スループットと IOPS) とディスク I/O (スループットと IOPS) の最大レベル、およびデータ重複排除やシャドウコピーなどのバックグラウンドアクティビティのキャッシュとサポートに使用できるメモリ量の詳細を示しています。Amazon FSx API または CLI を使用する場合、スループットキャパシティのレベルを毎秒 32 メガバイト未満に選択できますが、このレベルは、実稼働ワークロードではなく、テストおよび開発ワークロードを対象としています。

> **Note**
>
> 4,608 MBps 以上のスループットキャパシティレベルは、以下の米国東部 (バージニア北部)、米国西部 (オレゴン)、米国東部 (オハイオ)、欧州 (アイルランド)、アジアパシフィック (東京)、アジアパシフィック (シンガポール)のリージョンでのみサポートされることに注意してください。

ネットワーク I/O とメモリ

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 (MBps)		ネットワーク IOPS	メモリ (GB)
	ベースライン	バースト (1 日数分間)		
32	32	600	数千	4
64	64	600	数万	8
128	150	1,250		8
256	300	1,250	数十万	16
512	600	1,250		32
1,024	1,500	–		72
2,048	3,125	–		144
4,608	9,375	–	数百万	192
6,144	12,500	–		256
9,216	18,750	–		384
12,288	21,250	–		512

ディスク I/O

FSx スループットキャパシティ (MBps)	ディスクスループット (MBps)		ディスク IOPS	
	ベースライン	バースト (1 日 30 分)	ベースライン	バースト (1 日 30 分)

FSx スループットキャパシティ (MBps)	ディスクスループット (MBps)		ディスク IOPS	
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	10K	20K
512	512	–	20K	–
1,024	1,024	–	40K	–
2,048	2,048	–	80K	–
4,608	4,608	–	150K	–
6,144	6,144	–	200K	–
9,216	9,216[1]	–	300K[1]	–
12,288	12,288[1]	–	400K[1]	–

Note

[1]スループットキャパシティが 9,216 または 12,288 MBps のマルチ AZ ファイルシステムを使用している場合、書き込みトラフィックのみのパフォーマンスは 9,000 MBps、262,500 IOPS に制限されます。それ以外の場合は、すべてのマルチ AZ ファイルシステムの読み取りトラフィック、すべてのシングル AZ ファイルシステムの読み取りトラフィックと書き込みトラフィック、その他すべてのスループットキャパシティレベルについて、使用しているファイルシステムが表に示されているパフォーマンスの制限をサポートすることになります。

適切なレベルのスループットキャパシティの選択

Amazon Web Services 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場合、Amazon FSx は、設定したストレージ容量に基づいて、ファイルシステムの推奨されるスループットキャパシティレベルを自動的に選択します。推奨されるスループットキャパシティはほとんどのワークロードで十分ですが、レコメンデーションを上書きし、ワークロードのニーズに合わせて特定のスループットキャパシティを設定するオプションがあります。たとえば、ワークロードがファイルシステムへの 1 GBps のトラフィックを駆動する必要がある場合は、少なくとも 1,024 MBps のスループットキャパシティを選択する必要があります。次の表は、プロビジョニングされたストレージ容量に基づいて、ファイルシステムの最小推奨スループット容量レベルを示しています。

SSD ストレージ容量 (GiB)	HDD ストレージ容量 (GiB)	最小推奨スループットキャパシティ (MBps)
最大 640	最大 3,200	32
641 ~ 1,280	3201 ~ 6,400	64
1281 ~ 2,560	6,401 ~ 12,800	128
2,561 ~ 5,120	12,801 ~ 25,600	256
5,121 ~ 10,240	25,601 ~ 51,200	512
10,241 ~ 20,480	>51,200	1,024
>20,480	NA	2,048

設定するスループットのレベルを決定する際には、ファイルシステムで有効にする予定の機能についても考慮する必要があります。例えば、シャドウコピーを有効にする場合、ファイルサーバーが I/O パフォーマンス容量を使用してシャドウコピーを実行できるよう、予想されるワークロードの 3 倍のレベルまでスループットキャパシティを増やす必要があるかもしれません。データ重複排除を有効にする場合は、ファイルシステムのスループットキャパシティに関連付けるメモリ量を決定し、このメモリ容量がデータのサイズに対して十分であることを確認する必要があります。

スループットキャパシティは、作成後いつでも増減できます。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。

Amazon FSx コンソールの [モニタリングとパフォーマンス > パフォーマンス] タブを表示することにより、ファイルサーバーのパフォーマンスリソースのワークロード使用状況をモニタリングし、選択するスループットキャパシティに対する推奨事項を取得することができます。本番稼働前の環境でテストして、選択した設定がワークロードのパフォーマンス要件を満たしていることを確認することをお勧めします。マルチ AZ ファイルシステムの場合、ファイルシステムのメンテナンス、スループットキャパシティの変更、計画外のサービス中断の際に発生するフェイルオーバープロセスがワークロードに与える影響をテストし、これらのイベント中にパフォーマンスへの影響を防ぐため、十分なスループットキャパシティをプロビジョニングしていることを確認することもお勧めします。詳細については、「ファイルシステムメトリクスへのアクセス」を参照してください。

ストレージ構成がパフォーマンスに与える影響

ファイルシステムのストレージ容量、ストレージタイプ、SSD IOPS レベルはすべて、ファイルシステムのディスク I/O パフォーマンスに影響します。これらのリソースは、ワークロードに必要なパフォーマンスレベルを提供するように構成できます。

ストレージ容量を増やし、SSD IOPS をいつでもスケールできます。詳細については、ストレージ容量の管理およびSSD IOPS の管理を参照してください。また、ファイルシステムを HDD ストレージタイプから SSD ストレージタイプにアップグレードできます。詳細については、「ファイルシステムのストレージタイプの管理」を参照してください。

ファイルシステムは、デフォルトで次のレベルのディスクスループットと IOPS を提供します。

ストレージタイプ	ディスクスループット (ストレージ 1 TiB あたり MBps)	ディスク IOPS (ストレージの TiB あたり)
SSD	750	3,000[1]
HDD	12 ベースライン、80 バースト (ファイルシステムあたり最大 1 GBps)	12 ベースライン; 80 バースト

> **Note**
>
> [1]SSD ストレージタイプのファイルシステムでは、ストレージ 1 GiB あたり最大 500 IOPS、ファイルシステムあたり最大 400,000 IOPS を追加プロビジョニングできます。

HDD バーストパフォーマンス

HDD ストレージボリュームの場合、Amazon FSx はバーストバケットモデルを使用してパフォーマンスを提供します。ボリュームのベースラインスループット (ボリュームのスループットクレジットが蓄積されるレート) は、ボリュームサイズによって決まります。ボリュームのバーストスループット (クレジットがある場合に可能な消費レート) もボリュームサイズによって決まります。ボリュームが大きいほど、ベースラインとバーストスループットの値も大きくなります。また、ボリュームのクレジットが多いほど、バーストレベルでドライブ I/O に使用できる時間が長くなります。

HDD ストレージボリュームの対応可能なスループットは、以下の計算式で示されます。

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

1-TiB の HDD ボリュームの場合、バーストスループットは 80 MiBps に制限され、バケットは 12 MiBps のクレジットでいっぱいになり、最大 1 TiB 分のクレジットを保持できます。

HDD ストレージボリュームでは、ワークロードに応じてパフォーマンスに大きなばらつきが生じる可能性があります。IOPS またはスループットが急激に急増すると、ディスクのパフォーマンスが低下する可能性があります。`DiskThroughputBalance` メトリクスは、ディスクスループットとディスク IOPS 使用率の両方のバーストクレジットバランスに関する情報を提供します。例えば、ワークロードがベースラインの HDD IOPS 制限 (ストレージの 1 TiB あたり 12 IOPS) を超える場合、ディスク IOPS 使用率 (HDD) は 100% を超え、バーストクレジットバランスが枯渇します。これは `DiskThroughputBalance` メトリクスで確認できます。ワークロードが高レベルの I/O を継続的に推進するには、次のいずれかを実行する必要があります。

- バーストクレジット残高が補充されるように、ワークロードの I/O 需要を減らします。
- ファイルシステムのストレージ容量を増やして、より高いベースラインレベルのディスク IOPS を提供します。
- ファイルシステムをアップグレードして SSD ストレージを使用します。これにより、ワークロードの要件により適したベースラインレベルのディスク IOPS が提供されます。

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 HDD ストレージ容量と 32 MBps のスループットキャパシティで設定された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 - 32 MBps のベースラインと 600 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 — 24 MBps のベースラインと 160 MBps のバースト。ディスクスループットは、次より低くなります。
  - ファイルシステムのスループットキャパシティに基づく、ファイルサーバーがサポートする 32 MBps ベースラインおよび 260 MBps バーストのディスクスループットレベル。
  - ストレージタイプと容量に基づく、ストレージボリュームがサポートする 24 MBps ベースライン (12 MBps/TB * 2 TiB) および 160 MBps バースト (80 MBps/TB * 2 TiB) のディスクスループットレベル。

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にキャッシュされ、アクティブにアクセスされたデータで実行されるファイルオペレーションでは、最大 32 MBps のベースラインと 600 MBps のバーストスループットを駆動できます。また、例えば、キャッシュミスなどにより、ディスクまでずっと移動する必要があるファイルオペレーションでは最大 24 MBps のベースラインと 160 MBps のバーストスループットを駆動できます。

CloudWatch メトリクスを使用したパフォーマンスの測定

Amazon CloudWatch を使用して、ファイルシステムのスループットと IOPS を測定してモニタリングできます。詳細については、「Amazon CloudWatch によるモニターリング」を参照してください。

ファイルシステムのパフォーマンスの問題のトラブルシューティング

FSx for Windows File Server ファイルシステムのパフォーマンスは、ファイルシステムへのトラフィック、ファイルシステムのプロビジョニング方法、有効な機能 (データ重複排除やシャドウコピー) によって消費されているリソースなど、いくつかの要因によって決まります。ファイルシステムのパフォーマンスについての詳細は、「FSx for Windows File Server のパフォーマンス」を参照してください。

トピック

- ファイルシステムのスループットと IOPS 制限はどのように決定すればよいですか?
- ネットワーク I/O とディスク I/O の違いは何ですか? ネットワーク I/O がディスク I/O と異なる理由を教えてください。

- ネットワーク I/O が低いのに CPU またはメモリの使用率が高いのはなぜですか?
- バーストとは何ですか? 私のファイルシステムではどのくらいのバーストが使用されてるでしょうか? バーストクレジットがなくなるとどうなりますか?
- [Monitoring & performance] (モニタリングとパフォーマンス) ページに警告が表示されます。ファイルシステムの設定を変更する必要はありますか?
- メトリクスが一時的に消えてしまいました。どうすればよいですか?

ファイルシステムのスループットと IOPS 制限はどのように決定すればよいですか?

ファイルシステムのスループットと IOPS 制限を確認するには、プロビジョニングのスループットキャパシティに基づくパフォーマンスレベルを示す表を参照してください。

ネットワーク I/O とディスク I/O の違いは何ですか? ネットワーク I/O がディスク I/O と異なる理由を教えてください。

Amazon FSx ファイルシステムには、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データを提供する 1 つ以上のファイルサーバーが含まれます。これがネットワーク I/O です。ファイルサーバーには高速のインメモリキャッシュがあり、これにより最も頻繁にアクセスされるデータのパフォーマンスが向上します。また、ファイルサーバーは、ファイルシステムのデータをホストするストレージボリュームにトラフィックを誘導します。これがディスク I/O です。次の図は、Amazon FSx ファイルシステムのネットワーク I/O およびディスク I/O を示しています。

詳しくは、「Amazon CloudWatch によるモニターリング」を参照してください。

ネットワーク I/O が低いのに CPU またはメモリの使用率が高いのはなぜですか?

ファイルサーバーの CPU とメモリの使用率は、ネットワークトラフィックの他、ファイルシステムで有効にした機能によっても異なります。これらの機能をどのように設定およびスケジュールするかは、CPU とメモリの使用率に影響します。

進行中のデータ重複排除のジョブはメモリを消費する可能性があります。重複排除のジョブの設定を変更して、メモリ要件を削減できます。例えば、特定のファイルタイプまたはフォルダーで実行するように最適化を制限したり、最適化のための最小ファイルサイズと経過時間を設定したりできます。また、ファイルシステムのロードが最小限であるアイドル期間中に重複排除ジョブが実行されるように設定することをお勧めします。詳しくは、「データ重複排除によるストレージコストの削減」を参照してください。

アクセスベースの列挙を有効にしている場合、エンドユーザーがファイル共有を表示またはリストしたとき、またはストレージスケーリングのジョブでの最適化フェーズ中に CPU 使用率が高くなることがあります。詳細については、「Microsoft Storage ドキュメント」の「Enable access-based enumeration on a namespace」(名前空間でアクセスベースの列挙を有効にする) を参照してください。

バーストとは何ですか? 私のファイルシステムではどのくらいのバーストが使用されてるでしょうか? バーストクレジットがなくなるとどうなりますか?

通常、ファイルベースのワークロードはスパイキーです。このワークロードは、バースト間のアイドル時間で I/O が高い期間が短く、集中しているのが特徴です。これらのタイプの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維持できるベースライン速度に加えて、Amazon FSx ではネットワーク 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が提供されています。

Amazon FSx は、I/O クレジットメカニズムを使用して、平均使用率に基づきスループットと 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 の使用率がベースラインの制限を下回るとクレジットを蓄積し、必要な時にこれらのクレジットを使用して、ベースラインの制限を越えてバーストできます (バースト制限まで)。ファイルシステムのバースト制限およびバースト期間の詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。

[Monitoring & performance] (モニタリングとパフォーマンス) ページに警告が表示されます。ファイルシステムの設定を変更する必要はありますか?

[Monitoring & performance] (モニタリングとパフォーマンス) ページには、最近のワークロードの要求が、ファイルシステムの設定方法で決まるリソースの制限に近づいたか、超えた場合に警告が表示されます。必ずしも設定を変更する必要があるわけではありませんが、推奨されるアクションを実行しないと、ファイルシステムがワークロードに対して十分にプロビジョニングされない可能性があります。

警告の原因となったワークロードが典型的なものではなく、それが続くとは考えにくい場合は、何の対策も行わず以後の使用率を注意深く監視すれば問題ない場合があります。ただし、警告の原因となったワークロードが典型的なもので、継続またはさらに悪化する場合は、推奨されるアクションに従い (スループットキャパシティを増やして) ファイルサーバーのパフォーマンスを向上させるか、(ストレージ容量を増やすか、HDD から SSD ストレージに切り替えることで) ストレージボリュームのパフォーマンスを向上させることをお勧めします。

> **Note**
>
> 特定のファイルシステムイベントは、ディスク I/O パフォーマンスリソースを消費し、パフォーマンスの警告をトリガーする可能性があります。例:
>
> - ストレージ容量のスケーリングの最適化フェーズでは、ストレージ容量の拡張とファイルシステムのパフォーマンス で説明されているように、ディスクスループットが向上する可能性があります。
> - マルチ AZ ファイルシステムでは、スループットキャパシティのスケーリング、ハードウェアの交換、アベイラビリティーゾーンの中断などのイベントにより、自動的にフェイルオーバーとフェイルバックのイベントが発生します。この期間内に発生したデータ変更は、プライマリファイルサーバーとセカンダリファイルサーバー間で同期させる必要があるため、Windows Server はディスク I/O リソースを消費するデータ同期ジョブを実行します。詳しくは、「スループット容量の管理」を参照してください。

メトリクスが一時的に消えてしまいました。どうすればよいですか?

シングル AZ ファイルシステムは、ファイルシステムのメンテナンス中、インフラストラクチャコンポーネントの交換時、およびアベイラビリティーゾーンが利用できないときには利用できません。この間、メトリクスは利用できません。

マルチ AZ 配置では、Amazon FSx は異なるアベイラビリティーゾーンにスタンバイファイルサーバーを自動的にプロビジョニングして、維持します。ファイルシステムのメンテナンスまたは計画外のサービスの中断がある場合、Amazon FSx は自動的にセカンダリファイルサーバーにフェイルオーバーし、手動による介入なしでデータへのアクセスを継続できるようにします。ファイルシステムがフェイルオーバーおよびフェイルバックする短い期間、メトリクスが一時的に利用できなくなる場合があります。

FSx for Windows ファイルシステムの管理

Amazon FSx は、ワークロードやユーザー要件の変化、組織の規制やコンプライアンスのニーズを満たすために、Amazon FSx for Windows File Server ファイルシステムを簡単に管理および拡張するのに役立つ幅広い管理機能を提供します。以下は、、 AWS CLI API AWS Management Console、PowerShell でのリモート管理用の Amazon FSx CLI、およびネイティブ Microsoft Windows Server グラフィカルインターフェイスを使用して管理できるファイルシステム設定の一部のリストです。

- ストレージキャパシティ
- ストレージタイプ
- SSD IOPS
- スループット容量
- DNS エイリアス
- データ重複除外
- シャドウコピー
- ストレージクォータ
- ファイルアクセスの監査
- ファイル共有

以下のセクションでは、利用可能なファイルシステム管理機能と設定について説明します。状況に最適なオプションと、該当する場合はベストプラクティスを判断するのに役立つガイダンスが含まれています。

トピック

- Amazon FSx ファイルシステムのステータス
- PowerShell での Amazon FSx CLI の使用
- Amazon FSx リモート PowerShell セッションの開始
- PowerShell でのリモート管理に Amazon FSx CLI を使用する 1 回限りのファイルシステムセットアップタスク
- PowerShell での Amazon FSx CLI へのアクセスのトラブルシューティング
- ファイルシステムのメンテナンスウィンドウ

- 週次メンテナンスウィンドウを変更する
- DNS エイリアスを管理する
- ユーザーセッションと開いているファイル
- FSx for Windows File Server でのストレージの管理
- DFS 名前空間の使用
- スループット容量の管理
- Amazon FSx リソースのタグ付け
- を使用してファイルシステムを更新する AWS CLI

Amazon FSx ファイルシステムのステータス

Amazon FSx ファイルシステムのステータスを表示するには、Amazon FSx コンソール、 AWS CLI コマンド describe-file-systems、または API オペレーション DescribeFileSystems を使用します。

ファイルシステムのステータス	説明
AVAILABLE (利用可能)	ファイルシステムは正常な状態にあり、到達可能であり、使用可能です。
CREATING (作成)	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。
UPDATING (更新)	ファイルシステムは、お客様によって開始される更新を受けています。
[MISCONFIGURED] (設定ミスです)	アクティブディレクトリ環境での変更により、ファイルシステムが障害状態になっています。ファイルシステムは現在使用できないか、アベイラビリティーを失うリスクがあり、バックアップが成功しない可能性があります。アベイラビリティーの復元の詳細については、「ファイルシステムが正しく設定されていない状態です」を参照してください。

ファイルシステムのステータス	説明
MISCONFIGURED_UNAVAILABLE	アクティブディレクトリ環境での変更により、ファイルシステムは現在使用できません。アベイラビリティーの復元の詳細については、「ファイルシステムが正しく設定されていない状態です」を参照してください。
FAILED	• ファイルシステムの新規作成時に、Amazon FSx は新しいファイルシステムを作成できませんでした。 • ファイルシステムは使用できません。 • 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。 • Amazon FSx はバックアップを作成できません。

PowerShell での Amazon FSx CLI の使用

この章では、PowerShell でのリモート管理のために Amazon FSx CLI にアクセスして、FSx for Windows ファイルシステムのファイルシステム管理タスクを実行する方法について説明します。Microsoft Windows ネイティブグラフィカルユーザーインターフェイス (GUI) を使用して、いくつかの管理タスクを実行することもできます。

PowerShell でのリモート管理の Amazon FSx CLI を使用すると、ファイルシステム管理者グループのユーザーのファイルシステム管理が可能になります。FSx for Windows File Server 上でリモート PowerShell セッションを開始するには、まず次の前提条件を満たす必要があります。

- FSx for Windows File Server ファイルシステムとのネットワーク接続を持つ Windows コンピューティングインスタンスに接続できる。
- ファイルシステム管理者グループのメンバーとして Windows コンピューティングインスタンスにログインする。を使用している場合 AWS Managed Microsoft AD、これはAWS 委任 FSx 管理者グループです。セルフマネージド Microsoft Active Directory を使用している場合、ユーザーは、ドメイン管理者グループ、またはファイルシステムの作成時に管理用に指定したカスタムグループのメンバーである必要があります。詳細については、「セルフマネージド Active Directory を使用する場合のベストプラクティス」を参照してください。

- ファイルシステムのセキュリティグループの VPC インバウンドルールがポート 5985 でのトラフィックを許可していることを確認します。

PowerShell でのリモート管理の Amazon FSx CLI では、次のセキュリティ機能が使用されます。

- ユーザー認証情報は Kerberos 認証を使用して認証されます。
- 接続されたクライアントとファイルシステム間の管理セッション通信は、Kerberos を使用して暗号化されます。

Amazon FSx ファイルシステム上でリモート管理 CLI コマンドを実行するには、2 つのオプションがあります。

- 長時間実行されるリモート PowerShell セッションを確立し、セッション内でコマンドを実行できます。
- `Invoke-Command` を使用して、長時間実行されるリモート PowerShell セッションを確立せずに、単一のコマンドまたは単一のコマンドブロックを実行することができます。

リモート管理コマンドにパラメータとして可変を設定して渡す場合は、`Invoke-Command` を使用する必要があります。

> **Note**
>
> マルチ AZ ファイルシステムの場合、リモート管理に Amazon FSx CLI を使用できるのは、ファイルシステムが優先ファイルサーバーを使用している場合のみです。詳細については、「可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム」を参照してください。

リモート PowerShell にアクセスするには、ファイルシステムの Windows Remote PowerShell エンドポイントを使用する必要があります。リモート管理エンドポイントの形式は `amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*です (例: `amznfsxctlyaa1k.corp.example.com`)。エンドポイント名は、ネットワークとセキュリティタブ AWS Management Console のファイルシステムの詳細ページで を使用して確認できます。`describe-file-systems` コマンドを使用して AWS CLI 、レスポンスで返された `RemoteAdministrationEndpoint`プロパティを表示します。

`Get-Command` コマンドレットを使用して、PowerShell で使用可能なコマンドレット、関数、エイリアスに関する情報を取得できます。詳細については、「Microsoft ドキュメント」の「Get-Command」を参照してください。

次に説明する `Invoke-Command` コマンドレットを使用し、以下の構文を使用し、ファイルシステムの PowerShell コマンドでリモート管理 CLI 用の Amazon FSx CLI を実行することもできます。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

FSx for Windows File Server ファイルシステムで存続期間の長いリモート PowerShell セッションを開始する方法については、「Amazon FSx リモート PowerShell セッションの開始」を参照してください。

Amazon FSx リモート PowerShell セッションの開始

このトピックでは、FSx for Windows File Server ファイルサーバーで存続期間の長いリモート PowerShell セッションを開始する手順について説明します。

ファイルシステム上でリモート PowerShell セッションを開始するには

1. ファイルシステムの作成時に選択した委任された FSx 管理者グループのメンバーであるユーザーとして、ファイルシステムとのネットワーク接続があるコンピューティングインスタンスに接続します。
2. コンピューティングインスタンスで Windows PowerShell ウィンドウを開きます。
3. PowerShell では、次のコマンドを使用して、Amazon FSx ファイルシステム上で存続期間の長いリモートセッションを開きます。*`Remote-PowerShell-Endpoint`* を、管理したいファイルシステムの Windows Remote PowerShell エンドポイントに置き換えます。セッション設定の名前に `FsxRemoteAdmin` を使用します。

   ```
   PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
    -ConfigurationName FsxRemoteAdmin
   [fs-0123456789abcdef0]: PS>
   ```

   インスタンスが Amazon FSx Active Directory ドメインに含まれていない場合は、ポップアップにユーザー認証情報を入力するように求められます。FSx 管理者グループのメンバーである

ユーザーの認証情報を入力します。インスタンスがドメインに含まれている場合、認証情報の入力は要求されません。

> **Important**
>
> セルフマネージドの Active Directory 設定を使用していて、適切な Active Directory グループポリシー設定なしでサービスアカウントを変更すると、Windows Remote PowerShell エンドポイントが変わることがあります。詳細については、「Amazon FSx サービスアカウントの変更 の詳細」を参照してください。

PowerShell でのリモート管理に Amazon FSx CLI を使用する 1 回限りのファイルシステムセットアップタスク

PowerShell コマンドのリモート管理に次の Amazon FSx CLI を使用して、ファイルシステムに以下のベストプラクティスをすばやく実装します。

ストレージの消費量の管理

次のコマンドを使用して、ファイルシステムのストレージの消費量を管理します。

- デフォルトのスケジュールでデータ重複除外を有効にするには、次のコマンドを実行します。

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
  ```

  必要に応じて、次のコマンドを使用して、最低ファイル年齢を必要とすることなく、ファイルの作成後すぐにファイルに対してデータ重複除外を実行できます。

  ```
  Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
   FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
  ```

  詳細については、「データ重複排除によるストレージコストの削減」を参照してください。

- 次のコマンドを使用して、ユーザーストレージクォータの制限を「追跡」モードで有効にします。これはレポートのみを目的としており、強制ではありません。

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

詳細については、「ストレージクォータの管理」を参照してください。

シャドウコピーを有効にして、エンドユーザーがファイルやフォルダを以前のバージョンにリカバリできるようにする

次のように、デフォルトのスケジュール (平日の午前 7 時と正午 12 時) でシャドウコピーを有効にします。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

詳細については、「デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する」を参照してください。

転送時の暗号化の強制

次のコマンドは、ファイルシステムに接続しているクライアントに対して暗号化を強制します。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

開いているすべてのセッションを閉じて、現在接続しているクライアントを暗号化を使用して再接続するように強制できます。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

詳細については、転送時の暗号化の管理およびユーザーセッションと開いているファイルを参照してください。

PowerShell での Amazon FSx CLI へのアクセスのトラブルシューティング

次のように、Remote PowerShell を使用してファイルシステムに接続できない原因はいくつか考えられますが、それぞれ独自の解決方法があります。

最初に、Windows Remote PowerShell エンドポイントに正常に接続できることを確認するために、基本的な接続テストを実行することもできます。例えば、`test-netconnection endpoint -port 5985` コマンドを実行できます。

ファイルシステムのセキュリティグループには、リモート PowerShell 接続を許可するために必要なインバウンドルールがありません

ファイルシステムのセキュリティグループには、Remote PowerShell セッションを確立するために、ポート 5985 でのトラフィックを許可するインバウンドルールが必要です。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。

AWS マネージド Microsoft Active Directory とオンプレミス Active Directory の間に外部信頼が設定されている

Kerberos 認証で Amazon FSx Remote PowerShell を使用するには、フォレストの検索順序についてクライアントでローカルグループポリシーを設定する必要があります。詳細については、Microsoft のドキュメント「Kerberos フォレスト検索順序 (KFSO) の設定」を参照してください。

リモート PowerShell セッションを開始しようとすると、言語ローカライズエラーが発生します

次の `-SessionOption` をコマンドに追加する必要があります: `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

以下は、ファイルシステムでリモート PowerShell セッションを開始するときに `-SessionOption` を使用する 2 つの例です。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

ファイルシステムのメンテナンスウィンドウ

Amazon FSx for Windows File Server は、管理している Microsoft Windows サーバーソフトウェアの定期的なソフトウェアパッチを実行します。メンテナンスウィンドウは、このメンテナンスプロセスが開始される曜日と時刻を指定します。ファイルシステムの作成時に、メンテナンスウィンドウの開始期間を指定できます。指定しない場合、30 分のデフォルトのメンテナンス開始ウィンドウが割り当てられます。メンテナンスウィンドウの期間は、メンテナンスの範囲や、マルチ AZ ファイルシステムのプライマリサーバーとセカンダリサーバーの間でメンテナンス中に発生するファイルの読み取りおよび書き込みアクティビティを同期するプロセスなど、複数の要因によって異なります。詳細については、「フェイルオーバープロセス」を参照してください。

FSx for Windows File Server では、ワークロードと運用要件に合わせてメンテナンスウィンドウの開始時間を調整できます。メンテナンスウィンドウの開始時刻は、少なくとも 14 日に 1 回スケジュールされていれば、必要な頻度で移動できます。14 日以内にメンテナンスウィンドウが設定されていない状態でパッチがリリースされた場合、FSx for Windows File Server 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。ファイルシステムのメンテナンスウィンドウの開始時刻を調整する方法の詳細については、「」を参照してください週次メンテナンスウィンドウを変更する。

パッチの適用中は、シングル AZ ファイルシステムが使用できなくなります (通常 20 分間未満)。マルチ AZ ファイルシステムは引き続き利用可能で、優先ファイルサーバーとスタンバイファイルサーバー間で自動的にフェイルオーバーおよびフェイルバックします。詳細については、「フェイルオーバープロセス」を参照してください。マルチ AZ ファイルシステムのパッチ適用にはファイルサーバー間のフェイルオーバーとフェイルバックが含まれるため、この間に発生するファイルの読み取りおよび書き込みアクティビティは、優先ファイルサーバーとスタンバイファイルサーバー間で同期する必要があります。パッチ適用の時間を短縮するために、ファイルシステムの負荷が最小であるアイドル期間中にメンテナンスウィンドウをスケジュールすることをお勧めします。

> **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、Amazon FSx for Windows File Server は、メンテナンスが開始される前に、ファイルシステムをホストしている基盤と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。

週次メンテナンスウィンドウを変更する

FSx for Windows File Server では、ファイルシステムのメンテナンスウィンドウがいつワークロードと運用要件に合わせて開始されるかを調整できます。 AWS Management Console、 AWS CLI、および Amazon FSx API を使用して、毎週のメンテナンスウィンドウの開始時期を変更できます。詳細については、次の手順を参照してください。

週次メンテナンスウィンドウの開始時刻を変更するには (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開始時刻は、[Administration Settings] (管理設定) 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メンテナンスウィンドウの開始時刻を変更するには、「」を参照してくださいを使用してファイルシステムを更新する AWS CLI。

DNS エイリアスを管理する

Amazon FSx が提供するデフォルトのドメインネームシステム (DNS) 名に加えて、選択した DNS エイリアスをファイルシステムに関連付けることもできます。DNS エイリアスを使用すると、ファイ

ルシステムのストレージをオンプレミスから Amazon FSx に移行するときに、ツールやアプリケーションを更新することなく、既存の DNS 名を使用して Amazon FSx に保存されたデータにアクセスできます。

DNS エイリアスは、新規および既存の FSx for Windows File Server ファイルシステムに関連付けることができます。また、 AWS Management Console および を使用して、バックアップを新しいファイルシステムに復元するときにも関連付けることができます AWS CLI。ファイルシステムには、一度で最大 50 個の DNS エイリアスを関連付けることができます。

> **Note**
>
> DNS エイリアスのサポートは、2020 年 11 月 9 日の午後 12:00 ET 以降に作成された FSx for Windows ファイルサーバーのファイルシステム上で利用できます。2020 年 11 月 9 日の午後 12:00 ET より前に作成されたファイルシステムで DNS エイリアスを使用するには、次の手順を実行します。
>
> 1. 既存のファイルシステムのバックアップを作成します。詳細については、「ユーザー主導のバックアップ機能」を参照してください。
> 2. 新しいファイルシステムにバックアップを復元します。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。
>
> 新しいファイルシステムが使用可能になったら、このセクションに記載されている情報を使い、DNS エイリアスを使用してアクセスできるようになります。

> **Note**
>
> ここで示す情報は、ユーザーがアクティブディレクトリ内のみで作業しており、外部 DNS プロバイダーを使用していないことを前提としています。サードパーティー DNS プロバイダーでは、予想外の動作が発生することがあります。
> Amazon FSx は、結合しているアクティブディレクトリドメインがデフォルトの DNS として Microsoft DNS を使用している場合のみ、ファイルシステムの DNS レコードを登録します。サードパーティー DNS を使用している場合は、ファイルシステムを作成した後、Amazon FSx ファイルシステムの DNS エントリを手動で設定する必要があります。ファイルシステムに使用する正しい IP アドレスの選択の詳細については、「手動 DNS エントリに使用する正しいファイルシステムの IP アドレスの取得」を参照してください。

DNS エイリアスは、新しいファイルシステムを作成する際、およびバックアップから新しいファイルシステムを作成する際に、既存の FSx for Windows File Server ファイルシステムに関連付けることができます。ファイルシステムには、最大 50 個の DNS エイリアスを一度に関連付けることができます。

DNS エイリアスをファイルシステムに関連付けるだけでなく、クライアントが DNS エイリアスを使用してファイルシステムに接続するには、次の操作も実行する必要があります。

- Kerberos 認証と暗号化用のサービスプリンシパル名 (SPN) を設定します。
- Amazon FSx ファイルシステムのデフォルト DNS 名に解決される、DNS エイリアスの DNS CNAME レコードを設定します。

詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

FSx for Windows File Server ファイルシステムの DNS エイリアス名は、次の要件を満たす必要があります。

- 完全修飾ドメイン名 (FQDN) としてフォーマットする必要があります。
- 英数字およびハイフン (-) が使用できます。
- ハイフンでスタートまたは終了することはできません。
- 数字で始めることができます。

DNS エイリアス名の場合、大文字または小文字を指定するか、あるいはエスケープコードで対応する文字を指定するかに関係なく、Amazon FSx は英字を小文字 (a ~ z) として保存します。

ファイルシステムにすでに関連付けられているエイリアスを関連付けしようとした場合、そのエイリアスは無効になります。ファイルシステムが関連付けされていないファイルシステムから、エイリアスの関連付けを解除しようとすると、Amazon FSx は不正リクエストエラーでレスポンスします。

> **Note**
>
> Amazon FSx がファイルシステム上でエイリアスを追加または削除すると、接続されたクライアントは一時的に切断され、自動的にファイルシステムに再接続されます。切断時に非連続使用可能 (CA 以外) 共有をマッピングしているクライアントによって開かれていたファイルは、クライアントによって再度開かれる必要があります。

トピック

- DNS エイリアスのステータス
- Kerberos 認証での DNS エイリアスの使用
- ファイルシステムおよびバックアップの DNS エイリアスの表示
- DNS エイリアスとファイルシステムの関連付け
- 既存のファイルシステム上の DNS エイリアスを管理する

DNS エイリアスのステータス

DNS エイリアスには、次のいずれかのステータス値が設定されます。

- 利用可能 - DNS エイリアスは Amazon FSx ファイルシステムに関連付けられています。
- 作成中 - Amazon FSx は DNS エイリアスを作成し、ファイルシステムに関連付けています。
- 削除 - Amazon FSx はファイルシステムから DNS エイリアスの関連付けを解除し、削除しています。
- 作成に失敗しました - Amazon FSx は DNS エイリアスをファイルシステムに関連付けることができませんでした。
- 削除に失敗しました - Amazon FSx はファイルシステムから DNS エイリアスの関連付けを解除できませんでした。

Kerberos 認証での DNS エイリアスの使用

Amazon FSx との転送中に、Kerberos ベースの認証と暗号化を使用することをお勧めします。Kerberos は、ファイルシステムにアクセスするクライアントに対して最も安全な認証を提供します。DNS エイリアスを使用して Amazon FSx ファイルシステムにアクセスするクライアントの Kerberos 認証を有効にするには、ファイルシステムの Active Directory コンピュータオブジェクトの DNS エイリアスに対応するサービスプリンシパル名 (SPN) を設定する必要があります。

アクティブディレクトリ内のコンピュータオブジェクト上の別のファイルシステムに割り当てた DNS エイリアスに SPN が設定されている場合は、ファイルシステムのコンピュータオブジェクトに SPN を追加する前に、まずこれらの SPN を削除する必要があります。詳細については、「Kerberos のサービスプリンシパル名 (SPN) を設定する」を参照してください。

ファイルシステムおよびバックアップの DNS エイリアスの表示

次の手順で説明するように AWS Management Console、、、および API を使用して AWS CLI、FSx for Windows File Server ファイルシステムとバックアップに現在関連付けられている DNS エイリアスを表示できます。

ファイルシステムに関連付けられている DNS エイリアスを表示するには

- コンソールの使用 - ファイルシステムを選択し、ファイルシステム 詳細ページを表示します。[Network & security (ネットワークとセキュリティ) タブを選択して DNS エイリアス を表示します。
- CLI または API の使用 - `describe-file-system-aliases` CLI コマンドまたは DescribeFileSystemAliases API オペレーションを使用します。

バックアップに関連付けられた DNS エイリアスを表示するには

- コンソールの使用 - ナビゲーションペインで、[Backups] (バックアップ) を選択し、表示するバックアップを選択します。[Summary] (概要) ペインで、DNS エイリアス フィールドを表示します。
- CLI または API の使用 - `describe-backups` CLI コマンドまたは DescribeBackups API オペレーションを使用します。

DNS エイリアスとファイルシステムの関連付け

新しい FSx for Windows File Server ファイルシステムを最初から作成するとき、または、、および API を使用して新しいファイルシステムにバックアップを復元するときに AWS Management Console AWS CLI、DNS エイリアスを関連付けることができます。手順は以下のとおりです。

新しいファイルシステムを作成するときに DNS エイリアスを関連付けるには (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. 「使用開始」セクションの ステップ 5. ファイルシステムを作成 で説明されている新しいファイルシステムを作成する手順に従います。
3. [Create file system] (ファイルシステムの作成) ウィザードの [Access - optional] (アクセス - オプション) セクションで、ファイルシステムに関連付ける DNS エイリアスを入力します。

4. ファイルシステムが [Available] (使用可能) の場合、サービスプリンシパル名 (SPN) を設定して、エイリアスの DNS CNAME レコードを更新、または作成することで、DNS エイリアスを使用してファイルシステムにアクセスできます。詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

新しい Amazon FSx ファイルシステムの作成時に DNS エイリアスを関連付けるには (CLI)

1. 新しいファイルシステムを作成する際は、CreateFileSystem API オペレーションで エイリアス プロパティを使用して、DNS エイリアスを新しいファイルシステムに関連付けます。

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. ファイルシステムが [Available] (使用可能) の場合、サービスプリンシパル名 (SPN) を設定して、エイリアスの DNS CNAME レコードを更新、または作成することで、DNS エイリアスを使用してファイルシステムにアクセスできます。詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

バックアップの復元時に DNS エイリアスを追加または削除するには (CLI)

1. 既存のファイルシステムのバックアップから新しいファイルシステムを作成する場合は、次のように エイリアス プロパティと CreateFileSystemFromBackup API オペレーションを使用します。

- デフォルトでは、バックアップに関連付けられているエイリアスは、新しいファイルシステムに関連付けられます。
- バックアップからエイリアスを保持せずにファイルシステムを作成するには、空のセットで `Aliases` プロパティを使用します。

  追加の DNS エイリアスを関連付けるには、`Aliases` プロパティを選択して、バックアップに関連付けられた元のエイリアスと、関連付ける新しいエイリアスの両方を含めます。

次の CLI コマンドは、Amazon FSx がバックアップから作成しているファイルシステムに 2 つのエイリアスを関連付けます。

```
aws fsx create-file-system-from-backup \
  --backup-id backup-0123456789abcdef0
  --storage-capacity 2000 \
  --storage-type HDD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[transactions.corp.example.com,accts-
rcv.corp.example.com]
```

2. ファイルシステムが [Available] (使用可能) の場合、サービスプリンシパル名 (SPN) を設定して、エイリアスの DNS CNAME レコードを更新、または作成することで、DNS エイリアスを使用してファイルシステムにアクセスできます。詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

既存のファイルシステム上の DNS エイリアスを管理する

既存の FSx for Windows File Server ファイルシステムのエイリアスは、次の手順で説明するように AWS CLI、 AWS Management Console と を使用して追加および削除できます。

ファイルシステム DNS エイリアスを管理するには (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、DNS エイリアスを管理する Windows 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] タブで、[DNS エイリアス] の [管理] を選択して、[DNS エイリアスの管理] ウィンドウを表示します。

- DNS エイリアスを関連付けるには - [Associate new aliases] (新しいエイリアスを関連付ける) ボックスに、関連付ける DNS エイリアスを入力します。[Associate] (関連付け) を選択します。
- DNS エイリアスの関連付けを解除するには - [Current aliases] (現在のエイリアス) リストで、関連付けを解除するエイリアスを選択します。[Disassociate] (関連付け解除) を選択します。

[Current aliases] (現在のエイリアス) リストで管理しているエイリアスのステータスをモニタリングできます。リストを更新してステータスを更新します。エイリアスがファイルシステムに関連付け、または関連付け解除されるまでには、最大 2.5 分かかります。

4. エイリアスが [Available] (使用可能) の場合、サービスプリンシパル名 (SPN) を設定し、エイリアスの DNS CNAME レコードを更新または作成することで、DNS エイリアスを使用してファイルシステムにアクセスできます。詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

既存のファイルシステムに DNS エイリアスを関連付けるには (CLI)

1. `associate-file-system-aliases` CLI コマンド、または AssociateFileSystemAliases API オペレーションを使用して、既存のファイルシステムに DNS エイリアスを関連付けます。

   次の CLI リクエストは、指定されたファイルシステムに 2 つのエイリアスを関連付けます。

```
aws fsx associate-file-system-aliases \
  --file-system-id fs-0123456789abcdef0 \
  --aliases financials.corp.example.com transfers.corp.example.com
```

   レスポンスには、Amazon FSx がファイルシステムに関連付けているエイリアスのステータスが表示されます。

```
{
    "Aliases": [
        {
            "Name": "financials.corp.example.com",
            "Lifecycle": CREATING
        },
        {
            "Name": "transfers.corp.example.com",
            "Lifecycle": CREATING
```

```
        }
    ]
}
```

2. `describe-file-system-aliases` CLI コマンド (DescribeFileSystemAliases は同等の API オペレーション) を使用して、関連付けているエイリアスのステータスをモニタリングします。
3. `Lifecycle` の値が [AVAILABLE] (利用可能) の場合 (最大 2.5 分かかるプロセス)、サービスプリンシパル名 (SPN) を設定し、エイリアスの DNS CNAME レコードを更新または作成することで、DNS エイリアスを使用してファイルシステムにアクセスできます。詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

ファイルシステムから DNS エイリアスの関連付けを解除するには (CLI)

- `disassociate-file-system-aliases` CLI コマンドまたは AssociateFileSystemAliases API オペレーションを使用して、既存のファイルシステムから DNS エイリアスの関連付けを解除します。

  次のコマンドは、ファイルシステムから 1 つのエイリアスの関連付けを解除します。

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  レスポンスには、Amazon FSx がファイルシステムとの関連付けを解除しているエイリアスのステータスが表示されます。

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  エイリアスのステータスをモニタリングするには、`describe-file-system-aliases` CLI コマンド (DescribeFileSystemAliases は同等の API オペレーション) を使用します。エイリアスが削除されるまでには、最大 2.5 分かかります。

ユーザーセッションと開いているファイル

共有フォルダツールを使用して、 FSx for Windows File Server ファイルシステムで、接続されているユーザーセッションと開いているファイルをモニタリングできます。共有フォルダツールを使用すると、ファイルシステムに接続されているユーザーと、どのファイルが誰によって開かれているかをモニタリングするための一元的な場所が提供されます。このツールを使用して、以下のことを行うことができます。

- ロックされたファイルへのアクセスを復元します。
- ユーザーセッションを切断すると、そのユーザーが開いたすべてのファイルが閉じられます。

PowerShell でのリモート管理に Windows ネイティブの共有フォルダ GUI ツールと Amazon FSx CLI を使用して、ユーザーセッションを管理し、 FSx for Windows File Server ファイルシステム上のファイルを開くことができます。

GUI を使用してユーザーとセッションを管理する

次の手順では、Microsoft Windows 共有フォルダツールを使用して、Amazon FSx ファイルシステムでユーザーセッションを管理してファイルを開く方法の詳細を説明します。

共有フォルダツールを起動するには

1. Amazon EC2 インスタンスを起動し、Amazon FSx ファイルシステムが接続している 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。AWS Managed Microsoft Active Directory では、このグループは委任 AWS FSx 管理者と呼ばれます。セルフマネージド Microsoft アクティブディレクトリで、このグループはドメイン管理者、または作成時に指定した管理者グループのカスタム名と呼ばれます。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」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` を使って 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、Amazon FSx ファイルシステムの DNS 名 (例えば、`fs-01234567890123456 7.ad-domain.com`) を入力します。
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。

ユーザーセッションを管理するには (GUI)

共有フォルダツールで、[Sessions] (セッション) を選択し、 FSx for Windows File Server ファイルシステムに接続されているすべてのユーザーセッションを表示します。ユーザーまたはアプリケーションが Amazon FSx ファイルシステム上のファイル共有にアクセスしている場合、このスナップインはユーザーのセッションを表示します。セッションのコンテキスト (右クリック) メニューを開き、[Close Session] (セッションを閉じる) を選択すると、セッションを切断できます。

開いているセッションをすべて切断するには、[Sessions] (セッション) のコンテキスト (右クリック) メニューを開き、[Disconnect All Sessions] (すべてのセッションを切断する) を選択してアクションを確認します。

開いているファイルを管理するには (GUI)

共有フォルダツールで、[Open Files] (開いているファイル) を選択して、現在開いているシステム上のすべてのファイルを表示します。ビューには、どのユーザーがファイルやフォルダを開いているかも表示されます。この情報は、他のユーザーが特定のファイルを開くことができない理由を追跡するのに役立ちます。リスト内のファイルのエントリのコンテキスト (右クリック) メニューを開き、[Close Open File] (開いているファイルを閉じる) を選択すると、ユーザーが開いているすべてのファイルを閉じることができます。

ファイルシステム上で開いているすべてのファイルを切断するには、[Open Files] (開いているファイル) のコンテキスト (右クリック) メニューで 開いているファイルをすべて切断する を選択し、アクションを確認します。

PowerShell を使用してユーザーセッションを管理し、ファイルを開く

PowerShell でのリモート管理用の Amazon FSx CLI を使用して、アクティブなユーザーセッションを管理し、ファイルシステム上のファイルを開くことができます。この CLI を使用する方法については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

ユーザーセッションおよび開いているファイルの管理に使用できるコマンドは次のとおりです。

コマンド	説明
Get-FSxSmbSession	ファイルシステムと関連するクライアント間で現在確立されているサーバーメッセージブロック (SMB) セッションに関する情報を取得します。
Close-FSxSmbSession	SMB セッションを終了します。
Get-FSxSmbOpenFile	ファイルシステムに接続されているクライアントに対して開いているファイルに関する情報を取得します。
Close-FSxSmbOpenFile	SMB サーバーのクライアントの 1 つに対して開いているファイルを閉じます。

各コマンドのオンラインヘルプには、すべてのコマンドオプションのリファレンスが記載されています。このヘルプにアクセスするには、-? (例えば、Get-FSxSmbSession -?) でコマンドを実行します。

FSx for Windows File Server でのストレージの管理

ファイルシステムのストレージ設定には、プロビジョニングされたストレージ容量、ストレージタイプ、ストレージタイプがソリッドステートドライブ (SSD) の場合は SSD IOPS の量が含まれます。ファイルシステムの作成中および作成後に、これらのリソースをスループットキャパシティとともに設定して、ワークロードに望ましいパフォーマンスを達成できます。 AWS Management Console、、および PowerShell でのリモート管理用の Amazon FSx CLI を使用してファイルシステムのストレージとストレージ関連のパフォーマンスを管理する方法については AWS CLI、以下のトピックを参照してください。

トピック

- ストレージコストの最適化
- ストレージ容量の管理
- ファイルシステムのストレージタイプの管理
- SSD IOPS の管理
- データ重複排除によるストレージコストの削減
- ストレージクォータの管理
- ファイルシステムのストレージ容量の増加
- ストレージ容量の拡張をモニタリングする
- FSx for Windows ファイルサーバーファイルシステムのストレージ容量の動的な拡張
- FSx for Windows ファイルシステムのストレージタイプの更新
- ストレージタイプの更新をモニタリング
- ファイルシステムの SSD IOPS の更新
- プロビジョニングされた SSD IOPS 更新のモニタリング
- データ重複除外の管理
- データ重複排除のトラブルシューティング

ストレージコストの最適化

FSx for Windows で使用できるストレージ設定オプションを使用して、ストレージコストを最適化できます。

ストレージタイプオプション - FSx for Windows ファイルサーバーは、ハードディスクドライブ (HDD) およびソリッドステートドライブ (SSD) の 2 種類のストレージを用意しており、お客様のワークロードのニーズに合わせてコストおよびパフォーマンスを最適化することができます。HDD ストレージは、ホームディレクトリ、ユーザーと部門の共有、コンテンツ管理システムなど、幅広いワークロード向けに設計されています。SSD ストレージは、データベース、メディア処理ワークロード、データ分析アプリケーションなど、最もパフォーマンスが高く、レイテンシーの影響を受けやすいワークロード向けに設計されています。ストレージタイプと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、「FSx for Windows File Server のパフォーマンス」を参照してください。

データの重複排除 - 大規模なデータセットには冗長データが含まれていることが多く、データストレージのコストが増加します。例えば、ユーザーのファイル共有には、複数のユーザーによって保存された同じファイルのコピーが複数存在する場合があります。ソフトウェア開発共有には、ビルドごとに変更されないままの多くのバイナリを含めることができます。ファイルシステムの データ重複排除 を有効にすることで、データストレージのコストを削減することができます。重複排除機能を有効にすると、データセットの重複した部分を一度だけ保存することで、冗長データを自動的に削減または排除します。データ重複排除の詳細、および Amazon FSx ファイルシステムで簡単にそれを有効にする方法については、「データ重複排除によるストレージコストの削減」を参照してください。

ストレージ容量の管理

ストレージ要件の変化に応じて、FSx for Windows ファイルシステムのストレージ容量を増やすことができます。これを行うには、Amazon FSx コンソール、Amazon FSx API、または AWS Command Line Interface (AWS CLI) を使用します。ストレージ容量の増加を計画する際に考慮すべき要因には、ストレージ容量を増やす必要があるタイミングを把握すること、Amazon FSx がストレージ容量の増加を処理する方法を理解すること、ストレージの増加リクエストの進行状況を追跡することなどがあります。ファイルシステムのストレージ容量は増加のみが可能で、ストレージ容量を減らすことはできません。

> **Note**
>
> 2019 年 6 月 23 日より前に作成されたファイルシステムや、2019 年 6 月 23 日より前に作成されたファイルシステムに属するバックアップから復元されたファイルシステムでは、ストレージ容量を増やすことはできません。

Amazon FSx ファイルシステムのストレージ容量を増やすと、Amazon FSx は裏でファイルシステムに新しい大きなディスクセットを追加します。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透過的に移行します。ストレージタイプとその他の要因によってストレージの最適化には数時間から数日かかることがありますが、ワークロードのパフォーマンスに及ぼす影響は最小限です。この最適化では、古いストレージボリュームと新しいストレージボリュームの両方がファイルシステムレベルのバックアップに含まれるため、バックアップの使用量が一時的に高くなります。両方のストレージボリュームのセットが含まれているので、ストレージの拡張作業中にも Amazon FSx がバックアップを正常に取得して復元することができます。以前のストレージボリュームがバックアップ履歴に含まれていない場合、バックアップの使用量は、以前のベースラインレベルに戻ります。新しいストレージ容量が利用可能になると、新しいストレージ容量に対してのみ請求されます。

次の図は、Amazon FSx がファイルシステムのストレージ容量を増やすときに使用するプロセスの、4 つの主要ステップを示しています。

Amazon FSx コンソール、CLI、または API を使用して、ストレージ最適化、SSD ストレージ容量の増加、SSD IOPS の更新の進捗状況をいつでも追跡できます。詳細については、「ストレージ容量の拡張をモニタリングする」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増やす方法について知っておくべきこと

ストレージ容量を増やすときに考慮すべき重要な事項をいくつか挙げます。

- 増加のみ - ファイルシステムのストレージ容量は増加することのみ可能で、ストレージ容量は減らせません。
- 増加最小値 - 各ストレージ容量の増加は、ファイルシステムの現在のストレージ容量の最低 10% で、最大許容値 65,536 GiB までである必要があります。
- 最小スループットキャパシティ – ストレージキャパシティを増やすには、ファイルシステムの最小スループットキャパシティが 16 MBps である必要があります。これは、ストレージの最適化ステップがスループットを大量に消費するプロセスであるためです。
- 拡張するまでの時間 - 最後の拡張がリクエストされてから 6 時間経過するか、ストレージの最適化プロセスが完了するか、どちらが長い方は終わるまでは、ファイルシステムのストレージ容量をさらに増やすことはできません。ストレージの最適化には数時間から数日かかります。ストレージの最適化が完了するまでの時間を最小限に抑えるには、ストレージ容量を増やす前に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 (ストレージのスケーリング完了後にスループットキャパシティは元に戻せます)、ファイルシステムのトラフィックが最小である場合はストレージ容量を増やすことをお勧めします。

> **Note**
>
> 特定のファイルシステムイベントは、次の例のように、ディスク I/O のパフォーマンスリソースを消費する可能性があります。
> ストレージ容量のスケーリングの最適化フェーズでは、ディスクスループットが向上し、パフォーマンス警告が発生する可能性があります。詳細については、「パフォーマンスの警告と推奨事項」を参照してください。

ストレージ容量を増やすタイミングを知る

空きストレージ容量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します。`FreeStorageCapacity` CloudWatch メトリクスを使用して、ファイルシステム上で利用可能な空きストレージ容量をモニタリングします。このメトリクスで Amazon 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 によるモニターリング」を参照してください。

ファイルシステム上で常に 20% 以上の空きストレージ容量を維持することをお勧めします。ストレージ容量をすべて使用するとパフォーマンスに悪影響が生じ、データの不整合が生じる可能性があります。

空きストレージ容量が定義済みしきい値を下回った際にファイルシステムのストレージ容量を自動的に増やすことができます。が AWS開発したカスタム AWS CloudFormation テンプレートを使用して、自動化ソリューションの実装に必要なすべてのコンポーネントをデプロイします。詳細については、「ストレージ容量を動的に増やす」を参照してください。

ストレージ容量の拡張とファイルシステムのパフォーマンス

ほとんどのワークロードでは、パフォーマンスへの影響は最小限に抑えられますが、Amazon FSx は新しいストレージ容量が利用可能になった後、バックグラウンドでストレージ最適化プロセスを実行します。ただし、HDD ストレージタイプを持つファイルシステムや、多数のエンドユーザー、高レベルの I/O、または多数の小さなファイルを持つデータセットを含むワークロードでは、パフォーマンスが一時的に低下する可能性があります。このような場合は、ストレージ容量を増やす前に、まずファイルシステムのスループット容量を増やすことをお勧めします。これらのタイプのワークロードでは、ファイルシステムの負荷が最小限であるアイドル期間中にスループットキャパシティを変更することもお勧めします。これにより、アプリケーションのパフォーマンスニーズを満たすために、同じレベルのスループットを提供し続けることができます。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。

ファイルシステムのストレージタイプの管理

AWS Management Console および を使用して、ファイルシステムのストレージタイプを HDD から SSD に変更できます AWS CLI。ストレージタイプを SSD に変更する場合、最後の更新がリクエストされてから 6 時間後、またはストレージ最適化プロセスが完了するまでのどちらか長い方までは、ファイルシステム構成を再び更新できないことに注意してください。ストレージの最適化には数時間から数日かかります。この時間を最小限に抑えるために、ファイルシステムのトラフィックが最小のときにストレージタイプを更新することをお勧めします。詳細については、「FSx for Windows ファイルシステムのストレージタイプの更新」を参照してください。

ファイルシステムのストレージタイプは SSD から HDD には変更できません。ファイルシステムのストレージタイプを SSD から HDD に変更する場合は、HDD ストレージを使用するように設定した新しいファイルシステムにファイルシステムのバックアップを復元する必要があります。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。

ストレージタイプについて

FSx for Windows File Server ファイルシステムは、ソリッドステートドライブ (SSD) または磁気ハードディスクドライブ (HDD) ストレージタイプを使用するように設定できます。

SSD ストレージは、高いパフォーマンス要件とレイシンシーセンシティブを持つほとんどのプロダクション ワークロードに適します。これらのワークロードの例には、データベース、データ分析、

メディア処理、ビジネスアプリケーションなどがあります。また、多数のエンドユーザー、高レベルの I/O、またはデータセットに多数の小さなファイルが含まれるユースケースには、SSD をお勧めします。最後に、シャドウコピーを有効にする場合は SSD ストレージの使用をお勧めします。SSD ストレージを使用するファイルシステムの SSD IOPS は構成およびスケールできますが、HDD ストレージでは構成およびスケールできません。

HDD ストレージは、ホームディレクトリ、ユーザーおよび部門のファイル共有、コンテンツ管理システムなど、幅広いワークロードに対応するように設計されています。HDD ストレージは SSD ストレージに比べて低コストですが、レイテンシーが高く、ストレージ単位あたりのディスクスループットとディスク IOPS のレベルが低くなります。I/O 要件の低い汎用のユーザー共有やホームディレクトリ、データの取得頻度が低い大規模なコンテンツ管理システム (CMS)、またはサイズの大きいファイルの数が少ないデータセットに適する場合があります。

詳細については、「ストレージ構成とパフォーマンス」を参照してください。

SSD IOPS の管理

SSD ストレージで設定されたファイルシステムの場合、SSD IOPS の量は、キャッシュにあるデータではなく、ファイルシステムがディスクとの間でデータを読み取り、ディスクにデータを書き込む必要があるときに使用可能なディスク I/O の量を決定します。ストレージ容量とは別に SSD IOPS の量を選択してスケーリングできます。プロビジョニングできる最大 SSD IOPS は、ファイルシステムに選択したストレージ容量とスループットキャパシティによって異なります。SSD IOPS をスループットキャパシティでサポートされる制限を超えて増やそうとすると、その SSD IOPS のレベルに達するようにスループットキャパシティを増やす必要が生じる場合があります。詳細については、FSx for Windows File Server のパフォーマンスおよびスループット容量の管理を参照してください。

ファイルシステムのプロビジョニングされた SSD IOPS の更新について知っておくべき重要な項目を以下に示します。

- IOPS モードの選択 – 次の 2 つの IOPS モードから選択できます。
  - [自動] - このモードと Amazon FSx を選択すると、SSD IOPS を自動的にスケーリングして、ストレージ容量の GiB ごとに 3 つの SSD IOPS、ファイルシステムごとに最大 400,000 SSD IOPS を維持します。
  - [ユーザープロビジョニング] — このモードを選択すると、SSD IOPS の数を 96 ~ 400,000 の範囲で指定できます。Amazon FSx AWS リージョン が利用可能なすべての について、ストレージ容量の GiB あたり 3 ~ 50 IOPS、または米国東部 (バージニア北部) 、米国西部 (オレゴン) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、アジアパシフィック (東京) 、アジアパシ

フィック (シンガポール) でストレージ容量の GiB あたり 3 ~ 500 IOPS の数値を指定します。ユーザープロビジョンドモードを選択すると、指定した SSD IOPS の量が GiB あたり少なくとも 3 IOPS でない場合、リクエストは失敗します。プロビジョニングされた SSD IOPS のレベルが高い場合は、ファイルシステムごとに GiB あたり 3 IOPS を超える平均 IOPS に対して料金が発生します。

- ストレージ容量の更新 – ファイルシステムのストレージ容量を増やし、デフォルトで現在のユーザープロビジョニング SSD IOPS レベルを超える SSD IOPS 量を必要とする場合、Amazon FSx はファイルシステムを自動的に自動モードに切り替え、ファイルシステムにはストレージ容量の GiB あたり少なくとも 3 つの SSD IOPS があります。
- スループットキャパシティの更新 – スループットキャパシティを増やし、新しいスループット容量でサポートされる最大 SSD IOPS がユーザープロビジョニングの SSD IOPS レベルよりも高い場合、Amazon FSx は自動的にファイルシステムを自動モードに切り替えます。
- SSD IOPS 増加の時間間隔 – 最後に増加がリクエストされてから 6 時間後まで、またはストレージの最適化プロセスが完了するまでのどちらか長い期間は、SSD IOPS の増加も、スループットキャパシティの増加も、ファイルシステム上のストレージタイプの更新も、さらに行うことはできません。ストレージの最適化には数時間から数日かかります。ストレージの最適化が完了するまでの時間を最小限に抑えるために、ファイルシステムのトラフィックが最小限のときに SSD IOPS をスケーリングすることをお勧めします。

> **Note**
>
> 4,608 MBps 以上のスループットキャパシティレベルは、 AWS リージョン米国東部 (バージニア北部) 、米国西部 (オレゴン) 、米国東部 (オハイオ) 、欧州 (アイルランド) 、アジアパシフィック (東京) 、アジアパシフィック (シンガポール) でのみサポートされることに注意してください。

FSx for Windows File Server ファイルシステムのプロビジョニングされた SSD IOPS の量を更新する方法の詳細については、「ファイルシステムの SSD IOPS の更新」を参照してください。

データ重複排除によるストレージコストの削減

データ重複排除は、Dedup for Short とも呼ばれ、ストレージ管理者が重複データに関連するコストを削減するのに役立ちます。FSx for Windows File Server を使用すると、Microsoft Data Deduplication を使用して冗長データを特定して排除できます。大規模なデータセットは冗長なデータを持つことが多く、データストレージのコストが増加します。以下に例を示します。

- ユーザーファイル共有には、同じファイルまたは同様のファイルのコピーが多数ある場合があります。
- ソフトウェア開発共有には、ビルドごとに変更されないままの多くのバイナリを含めることができます。

ファイルシステムのデータ重複排除を有効にすることで、データストレージのコストを削減できます。データ重複除外 はデータセットの重複した部分を 1 回のみ保存することで、冗長データを削減または排除します。データ重複除外を有効にすると、重複除外後のデータ圧縮がデフォルトで有効になり、さらに節約ができます。重複排除は、データの忠実度や整合性を損なうことなく冗長性を最適化します。データ重複除外は、ファイルシステムを継続的に自動的にスキャンして最適化するバックグラウンドプロセスとして実行され、ユーザーや接続されたクライアントに対して透過的に実行されます。

データ重複除外によって達成できるストレージの節約は、ファイル間で重複する量など、データセットの性質によって異なります。一般的な汎用ファイル共有では、平均 50～60% 削減されます。共有内では、ユーザードキュメントの 30～50% からソフトウェア開発データセットの 70～80% が節約範囲です。重複除外による節約の可能性を測定するには、以下に説明する `Measure-FSxDedupFileMetadata` リモート PowerShell コマンドを使用します。

また、特定のストレージニーズに合わせてデータ重複除外をカスタマイズすることもできます。例えば、特定のファイルタイプでのみ実行するように重複除外を設定したり、カスタムジョブスケジュールを作成したりできます。重複除外ジョブはファイルサーバリソースを消費することがあるため、`Get-FSxDedupStatus` を使用して重複除外ジョブのステータスをモニタリングすることをお勧めします。

ファイルシステムでのデータ重複排除の設定については、「データ重複除外の管理」を参照してください。

データ重複排除に関連する問題の解決については、「

以下の情報を使用して、データ重複排除を設定および使用する際の一般的な問題のトラブルシューティングにお役立てください。

トピック

- データ重複排除が機能していない
- 重複排除の値が予期せず 0 に設定されている
- ファイルを削除した後、ファイルシステムのスペースが解放されません

データ重複排除が機能していない

データ重複排除の現在のステータスを確認するには、`Get-FSxDedupStatus` PowerShell コマンドを実行し、最新の重複排除ジョブの完了ステータスを表示します。1 つ以上のジョブが失敗している場合、ファイルシステム上で空きストレージ容量の増加が見られない場合があります。

重複排除ジョブが失敗する最も一般的な理由は、メモリ不足です。

- Microsoft は、1 TB の論理的なデータあたり 1 GB のメモリが最適にあることを推奨します (または、1 TB の論理的なデータあたり少なくとも 350 MB)。Amazon FSx パフォーマンステーブル を使用して、ファイルシステムのスループットキャパシティに関連付けられているメモリを特定し、メモリリソースがデータのサイズに対して十分であることを確認します。そうでない場合は、ファイルシステムのスループットキャパシティを、論理データの 1 TB あたり 1 GB のメモリ要件を満たすレベルまで増やす必要があります。
- 重複排除ジョブは、Windows が推奨するデフォルトの 25% のメモリ割り当てで設定されます。つまり、32 GB のメモリを備えたファイルシステムの場合、8 GB が重複排除に使用できます。メモリ割り当ては設定可能です (パラメータ `-Memory` で `Set-FSxDedupSchedule` コマンドを使用します)。重複排除にメモリ割り当てを増やすと、ファイルシステムのパフォーマンスに影響する可能性があることに注意してください。
- 重複排除のジョブの設定を変更して、必要なメモリ量を削減できます。例えば、特定のファイルタイプまたはフォルダーで実行するように最適化を制限したり、最適化のための最小ファイルサイズと経過時間を設定したりできます。また、ファイルシステムのロードが最小限であるアイドル期間中に重複排除ジョブが実行されるように設定することをお勧めします。

重複排除ジョブを完了するのに十分な時間がない場合にも、エラーが表示されることがあります。データ重複除外スケジュールの変更 で説明されているように、ジョブの最大期間を変更する必要がある場合があります。

重複排除ジョブが長期間失敗していて、この期間中にファイルシステム上のデータに変更があった場合、後続の重複排除ジョブを初めて正常に完了するには、より多くのリソースが必要になる場合があります。

重複排除の値が予期せず 0 に設定されている

データ重複排除を設定したファイルシステムでは、`SavedSpace` と `OptimizedFilesSavingsRate` の値が予期せず 0 になります。

これは、ファイルシステムのストレージ容量を増やす際、ストレージ最適化プロセス中に発生する可能性があります。ファイルシステムのストレージ容量を増やすと、Amazon FSx は、ストレー

ジ最適化プロセス中に既存のデータ重複排除ジョブをキャンセルします。これにより、以前のディスクから新しくより大きなディスクにデータが移行されます。ストレージ最適化ジョブが完了すると、Amazon FSx はファイルシステムでのデータ重複排除を再開します。ストレージ容量の増加とストレージの最適化の詳細については、「ストレージ容量の管理」を参照してください。

ファイルを削除した後、ファイルシステムのスペースが解放されません

データ重複排除の予想される動作は、重複排除がスペースを節約したデータが削除されたデータであった場合、ガベージコレクションのジョブが実行されるまでファイルシステムでスペースは解放されません。

役立つと思われるプラクティスとして、多数のファイルを削除した直後にガベージコレクションのジョブを実行するようにスケジュールを設定することができます。ガベージコレクションのジョブが終了したら、ガベージコレクションのスケジュールを元の設定に戻すことができます。これにより、削除により解放された容量をすぐに確認できます。

次の手順を使用して、ガベージコレクションジョブを 5 分で実行するように設定します。

1. データ重複排除が有効になっていることを確認するには、`Get-FSxDedupStatus` コマンドを使用します。コマンドとその期待される出力の詳細については、「保存スペースの量の表示」を参照してください。

2. 以下を使用して、5 分後にガベージコレクションのジョブを実行するスケジュールを設定します。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. ガベージコレクションのジョブが実行され、スペースが解放されたら、スケジュールを元の設定に戻します。

」を参照してください。

データ重複除外の詳細については、Microsoft の「データ重複除外について」ドキュメントを参照してください。

> **Warning**
>
> 特定の Robocopy コマンドをデータ重複除外で実行することは推奨されません。これらのコマンドはチャンクストアのデータ整合性に影響を与える可能性があるためです。詳細については、Microsoft のデータ重複除外の相互運用性に関するドキュメントを参照してください。

データ重複排除を使用する際のベストプラクティス

ここでは、Data Deduplication を使用するためのいくつかのベストプラクティスを以下に示します。

- ファイルシステムがアイドル状態のときに実行するように Data Deduplication ジョブをスケジュールする: デフォルトのスケジュールには、毎週土曜日の 2:45 UTC に実行される `GarbageCollection` ジョブが含まれています。ファイルシステムで大量のデータが流出している場合、完了するまでに数時間かかることがあります。この時間がワークロードにとって理想的でない場合は、ファイルシステムのトラフィックが少ないと予想される時間にこのジョブを実行するようにスケジュールします。
- Data Deduplication を完了するのに十分なスループットキャパシティを設定する: スループットキャパシティが大きいほど、メモリのレベルが高くなります。Microsoft では、Data Deduplication を実行するには、論理データの 1 TB あたり 1 GB のメモリを用意することを推奨します。Amazon FSx パフォーマンステーブルを使用して、ファイルシステムのスループットキャパシティに関連付けられているメモリを特定し、メモリリソースがデータのサイズに対して十分であることを確認します。
- Data Deduplication の設定をカスタマイズして、特定のストレージのニーズを満たし、パフォーマンス要件を緩和する: 特定のファイルタイプまたはフォルダーで実行するように最適化を制限したり、最適化のための最小ファイルサイズと経過時間を設定したりできます。詳細については、「データ重複排除によるストレージコストの削減」を参照してください。

ストレージクォータの管理

ファイルシステム上でユーザーストレージクォータを設定して、ユーザーが消費できるデータストレージの量を制限できます。クォータを設定した後、クォータの状態を追跡して使用状況をモニタリングし、ユーザーがクォータを上回るタイミングを確認できます。

また、クォータに達したユーザーがストレージに書き込むのを停止して、クォータを強制することもできます。クォータを強制すると、クォータを超えるユーザーに「ディスク容量が不十分です」というエラーメッセージが表示されます。

クォータ設定には、次のしきい値を設定できます。

- 警告 – ユーザーまたはグループがクォータ制限に近づいているかどうかを追跡するなど、追跡関連にのみ使用されます。
- 制限 – ユーザーまたはグループのストレージクォータ制限。

ファイルシステムにアクセスする新しいユーザーに適用されるデフォルトのクォータと、特定のユーザーまたはグループに適用されるクォータを設定できます。また、各ユーザーまたはグループが消費しているストレージの量、およびクォータを超えているかどうかについてのレポートを表示することもできます。

ユーザーレベルでのストレージ消費は、ファイルの所有権に基づいて追跡されます。ストレージ消費量は、ファイルが占める実際の物理ストレージ領域ではなく、論理的なファイルサイズを使用して計算されます。ユーザーストレージクォータは、データがファイルに書き込まれる時点で追跡されます。

複数のユーザーのクォータを更新するには、各ユーザーに対して更新コマンドを 1 回実行するか、ユーザーをグループに編成してそのグループのクォータを更新する必要があります。

PowerShell でのリモート管理の Amazon FSx CLI を使用して、ファイルシステム上のユーザーストレージクォータを管理できます。この CLI を使用する方法については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

ユーザーストレージクォータを管理するために使用できるコマンドは次のとおりです。

ユーザーストレージクォータコマンド	説明
Enable-FSxUserQuotas	ユーザーストレージクォータの追跡または強制、またはその両方を開始します。
Disable-FSxUserQuotas	ユーザーストレージクォータの追跡と強制を停止します。
Get-FSxUserQuotaSettings	ファイルシステムの現在のユーザーストレージクォータ設定を取得します。

ユーザーストレージクォータコマンド	説明
Get-FSxUserQuotaEntries	ファイルシステム上の個々のユーザーおよびグループの現在のユーザーストレージクォータエントリを取得します。
Set-FSxUserQuotas	個々のユーザーまたはグループのユーザーストレージクォータを設定します。クォータ値はバイト単位で指定します。

各コマンドのオンラインヘルプには、すべてのコマンドオプションのリファレンスが記載されています。このヘルプにアクセスするには、-? (例えば、Enable-FSxUserQuotas -?) コマンドを実行します。

ファイルシステムのストレージ容量の増加

ストレージ要件の変更に応じて、FSx for Windows File Server ファイルシステムのストレージ容量を増やせます。次の手順で説明するように、Amazon FSx コンソール AWS CLI、、または Amazon FSx API を使用して、ファイルシステムのストレージ容量を増やします。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。

ファイルシステムのストレージ容量を増やすには (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、ストレージ容量を増やしたい Windows ファイルシステムを選択します。
3. [Action] (アクション) で [Update storage] (ストレージの更新) 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 [Storage capacity] (ストレージ容量) の横にある [Update] (更新) を選択します。

   [Update storage capacity] (ストレージ容量の更新) ウィンドウが表示されます。
4. [Input type] (入力タイプ) には、[Percentage] (割合) を選択して現在値からの変化率として新しいストレージ容量を入力するか、[Absolute] (絶対) を選択して新しい値を GiB 単位で入力します。
5. 希望するストレージ容量 を入力します。

> **Note**
>
> 希望する容量値は、現在値よりも最低 10% 以上である必要があり、最大 65,536 GiB まで可能です。

6. [Update] (更新) を選択して、ストレージ容量の更新を開始します。
7. [Update] (更新)タブの ファイルシステム 詳細ページで、更新の進捗状況をモニタリングすることができます。

ファイルシステムのストレージ容量を増やすには (CLI)

FSx for Windows ファイルサーバーファイルシステムのストレージ容量を増やすには、 AWS CLI コマンド update-file-system を使用します。以下のパラメータを設定します。

- 更新するファイルシステムの ID への `--file-system-id`。
- 現在の値より少なくとも 10 パーセント大きい値への `--storage-capacity`。

コマンド describe AWS CLI describe-file-systems を使用して、更新の進行状況をモニタリングできます。出力で `administrative-actions` を探します。

詳細については、「AdministrativeAction」を参照してください。

ストレージ容量の拡張をモニタリングする

ファイルシステムのストレージ容量を増やしたら、次の手順で説明 AWS CLI するように、Amazon FSx コンソール、 API、または を使用してストレージ容量の増加の進行状況をモニタリングできます。

コンソールで拡張をモニタリングする

File system details (ファイルシステムの詳細) ウィンドウの [Update] (更新) タブでは、更新の種類ごとに最新の更新プログラムを 10 個表示できます。

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。

更新タイプ

可能な値は、[ストレージ容量] です。

ターゲット値

ファイルシステムのストレージ容量を更新する希望値です。

ステータス

更新の現在のステータス。ストレージ容量の更新では、指定できる値は次のとおりです。

- 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。
- 進行中 - Amazon FSx が更新リクエストを処理しています。
- 最適化の更新 - Amazon FSx により、ファイルシステムのストレージ容量が拡張しました。ストレージ最適化プロセスでは、ファイルシステムデータを新しい大きなディスクに移動しています。
- Completed - ストレージ容量の拡張は正常に完了しました。
- 失敗 - ストレージ容量の拡張に失敗しました。疑問符 (?) を選択し、ストレージの更新が失敗した理由の詳細を確認します。

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。

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。

モニタリングは、 AWS CLI と API で増加します。

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

次の例は、describe-file-systems CLI コマンドのレスポンスの抜粋を示しています。ファイルシステムのストレージ容量は 300 GB で、ストレージ容量を 1000 GB に増やすための保留中の管理アクションがあります。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
```

```
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "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。これは、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。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
```

```
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

ストレージ容量の拡張に失敗した場合、FILE_SYSTEM_UPDATE アクションが FAILED に変更されます。FailureDetails プロパティは、次の例に示すように、障害に関する情報を提供します。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

失敗したアクションのトラブルシューティングについては、「ストレージまたはスループットキャパシティの更新が失敗する」を参照してください。

FSx for Windows ファイルサーバーファイルシステムのストレージ容量の動的な拡張

FSx for Windows File Server ファイルシステムのストレージ容量を手動で増やす代わりに、 AWS CloudFormation テンプレートを使用してストレージを自動的に増やすことができます。このセクションのソリューションを使用すると、空きストレージ容量が指定したしきい値を下回った場合に、ファイルシステムの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、空きストレージ容量のしきい値、このしきい値に基づく Amazon CloudWatch アラーム、ファイルシステムのストレージ容量を増やす AWS Lambda 関数を定義するために必要なすべてのコンポーネントを自動的にデプロイします。

このソリューションは以下のパラメータを使用します。

- ファイルシステム ID
- 空きストレージ容量のしきい値 (数値)
- 測定単位 (パーセンテージ [デフォルト] または GiB)
- ストレージ容量の増加率 (%)
- SNS サブスクリプションの電子メールアドレス
- アラームしきい値の調整 (はい / いいえ)

トピック

- アーキテクチャの概要
- AWS CloudFormation テンプレート
- AWS 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 クラウドに次のリソースが構築されます。

この図表は以下のステップを示しています。

1. AWS CloudFormation テンプレートは、CloudWatch アラーム、 AWS Lambda 関数、Amazon Simple Notification Service (Amazon SNS) キュー、および必要なすべての 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空きストレージ容量が指定されたしきい値を下回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。
3. ソリューションによって、この Amazon SNS トピックに登録されている Lambda 関数がトリガーされます。
4. Lambda 関数は、指定された増加率の値に基づいて新しいファイルシステムのストレージ容量を計算し、新しいファイルシステムのストレージ容量を設定します。
5. Lambda 関数はオプションで、ファイルシステムの新しいストレージ容量の指定された割合に等しくなるように、空きストレージ容量しきい値を調整できます。
6. 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。

AWS CloudFormation テンプレート

このソリューションでは AWS CloudFormation 、 を使用して、FSx for Windows File Server 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、IncreaseFSxSize AWS CloudFormation テンプレートをダウンロードします。

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

FileSystemId

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

LowFreeDataStorageCapacityThreshold

デフォルト値はありません。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る空きストレージ容量の初期しきい値を、GiB で指定するか、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。パーセンテージで表すと、CloudFormation テンプレートは CloudWatch アラーム設定と一致するように GiB に再計算されます。

LowFreeDataStorageCapacityThresholdUnit

デフォルトは % です。`LowFreeDataStorageCapacityThreshold` の単位を GiB、または現在のストレージ容量に対するパーセンテージで指定します。

AlarmModificationNotification

デフォルトは [Yes] (はい) です。[はい] に設定すると、初期 `LowFreeDataStorageCapacityThreshold` は、後続のアラームしきい値の `PercentIncrease` の値に比例して増加します。

例えば、`PercentIncrease` が 20 に設定され、AlarmModificationNotification が Yes に設定されている場合、GiB で指定された使用可能な空き領域のしきい値 (`LowFreeDataStorageCapacityThreshold`) は、後続のストレージ容量増加イベントのために 20% 増加します。

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

デフォルト値はありません。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。

AWS CloudFormationによる自動デプロイ

次の手順では、FSx for Windows File Server ファイルシステムのストレージ容量を自動的に増やすように AWS CloudFormation スタックを設定してデプロイします。デプロイには約 5 分かかります。

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

開始する前に、 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 が必要です。Amazon FSx リソースの作成の詳細については、「Amazon FSx for Windows File Server 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. IncreaseFSxSize AWS 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**
   >
   > Amazon FSx は現在、特定の AWS リージョンでのみ使用できます。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. [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。

3. [Stack name] (スタック名) を入力します。
4. [Parameters] (パラメータ) では、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。次に、[Next] (次へ) を選択します。
5. 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。
6. [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。

7. [Create] (作成) を選択してスタックをデプロイします。

スタックのステータスは、 AWS CloudFormation コンソールの Status 列で確認できます。約 5 分で CREATE_COMPLETE 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。

FSx for Windows ファイルシステムのストレージタイプの更新

HDD ストレージを使用して SSD ストレージを使用するファイルシステムのストレージタイプを変更できます。次の手順に示すように、Amazon FSx コンソール AWS CLI、、または Amazon FSx API を使用して、ファイルシステムのストレージタイプを変更できます。詳細については、「ファイルシステムのストレージタイプの管理」を参照してください。

ファイルシステムのストレージタイプを更新するには (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. [ファイルシステム] に移動し、ストレージタイプを更新する Windows ファイルシステムを選択します。
3. [アクション] で [ストレージの更新] を選択します。または、[サマリー] パネルで、[HDD] の横にある [更新] ボタン選択します。[ストレージタイプの更新] ウィンドウが表示されます。
4. [希望するストレージタイプ] で、[SSD] を選択します。ストレージタイプの更新を開始するには、[更新] を選択します。

   コンソールと CLI を使用し、ストレージタイプの更新の進捗状況をモニタリングできます。

ファイルシステムのストレージタイプを更新するには (CLI)

FSx for Windows File Server ファイルシステムのストレージタイプを更新するには、 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` を更新するファイル システムの ID に。
- `--storage-type` から SSD へ。SSD ストレージタイプから HDD ストレージタイプには切り替えられません。

コマンド describe AWS CLI describe-file-systems を使用して、更新の進行状況をモニタリングできます。出力で `administrative-actions` を探します。

詳細については、「AdministrativeAction」を参照してください。

ストレージタイプの更新をモニタリング

ファイルシステムのストレージタイプを HDD から SSD ストレージに更新した後、次の手順で説明するように、Amazon FSx コンソール、、 AWS CLIまたは API を使用してストレージタイプの更新の進行状況をモニタリングできます。

コンソールでファイルシステムの更新をモニタリングする

[ファイルシステムの詳細] ウィンドウの [更新] タブに、更新の種類ごとに最近の 10 件の更新プログラムが表示されます。

ストレージタイプの更新については、次の情報を表示できます。

[Update type] (更新タイプ)

可能な値は、[ストレージタイプ] です。

[Target value] (ターゲット値)

[SSD]

[Status] (ステータス)

更新の現在のステータス。ストレージタイプの更新では、可能な値は次のとおりです。

- [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。
- [最適化の更新] – SSD ストレージのパフォーマンスを書き込みオペレーションに利用できます。更新は、[最適化の更新状態] に入りますが、通常は数時間かかり、その間の読み取りオペレーションは HDD と SSD の間のパフォーマンスレベルになります。更新処理が完了すると、新しい SSD パフォーマンスは読み取りと書き込みの両方に利用できるようになります。
- [完了] - ストレージタイプの更新が正常に完了しました。
- [失敗] — ストレージタイプの更新に失敗しました。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。

AWS CLI および API を使用した更新のモニタリング

describedescribe-file-systems AWS CLI コマンドと DescribeFileSystems API アクションを使用して、ファイルシステムのストレージタイプの更新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 SSD IOPS を増やすと、`FILE_SYSTEM_UPDATE` および `STORAGE_TYPE_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 IOPS の更新

SSD ストレージで設定されたファイルシステムでは、プロビジョニングされた SSD IOPS のレベルによって、キャッシュにあるデータの読み取りまたは書き込みではなく、ファイルシステムがディスクとの間でデータを読み取り、ディスクに書き込む必要があるときに使用可能なディスク I/O の量を決定します。次の手順で説明するように AWS CLI、Amazon FSx コンソール、、または Amazon FSx API を使用して、ファイルシステムの SSD IOPS を更新できます。SSD IOPS の管理の詳細については、「SSD IOPS の管理」を参照してください。

ファイルシステムの SSD IOPS を更新するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [ファイルシステム] に移動して、SSD IOPS を更新する Windows ファイルシステムを選択します。
3. [アクション] で、[SSD IOPS の更新] を選択します。または、[サマリー] パネルで、[プロビジョニングされた SSD IOPS] の横にある [更新] ボタンを選択します。[IOPS プロビジョニングを更新] ウィンドウが開きます。
4. [モード] で、[自動] または [ユーザープロビジョニング] を選択します。[自動] を選択した場合、Amazon FSx はファイルシステムのストレージ容量 1 GiB あたり 3 つの SSD IOPS を自動的にプロビジョニングします。[ユーザープロビジョニング] を選択した場合は、96 ~ 400,000 の範囲の任意の整数を入力します。
5. [更新] を選択して、プロビジョニングされた SSD IOPS 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。

ファイルシステムの SSD IOPS を更新するには (CLI)

FSx for Windows File Server ファイルシステムの SSD IOPS を更新するには、`--windows-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。

- SSD IOPS の数を指定する場合は、 を使用します。サポートされている AWS リージョンおよびでは`Iops=`*`number_of_IOPS`*最大 400,000 です`Mode=USER_PROVISIONED`。
- 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、ファイルシステムのストレージ容量の GiB あたり 3 SSD IOPS を自動的に維持し、サポートされている AWS リージョンでは最大 400,000 まで維持します。

AWS CLI コマンド describedescribe-file-systems を使用して、更新の進行状況をモニタリングできます。出力で `administrative-actions` を探します。

詳細については、「AdministrativeAction」を参照してください。

プロビジョニングされた SSD IOPS 更新のモニタリング

ファイルシステムのプロビジョニングされた SSD IOPS の量を更新した後、次の手順で説明するように、Amazon FSx コンソール、、 AWS CLIおよび API を使用して SSD IOPS 更新の進行状況をモニタリングできます。

コンソールで更新をモニタリングする

ファイルシステムの詳細 ウィンドウの [Updates] (更新) タブでは、更新の種類ごとに最新の更新プログラムを 10 個表示できます。

プロビジョニングされた SSD IOPS 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)

可能な値は、[IOPS モード] および [SSD IOPS] です。

[Target value] (ターゲット値)

ファイルシステムの IOPS モードと SSD IOPS へ更新するのに必要な値です。

[Status] (ステータス)

更新の現在のステータス。SSD IOPS 更新の場合、可能な値は以下の通りです。

- [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。
- 最適化の更新 – 新しい IOPS レベルをワークロードの書き込み操作に使用できます。更新は、最適化の更新 状態に入り、通常数時間続き、その間、ワークロードの読み取りオペレーションは、以前のレベルと新しいレベル間の IOPS パフォーマンスになります。更新処理が完了すると、新しい IOPS レベルは読み取りと書き込みの両方に使用できるようになります。
- [完了] - SSD IOPS の更新が正常に完了しました。
- [失敗] — SSD IOPS の更新に失敗しました。疑問符 (?) を選択し、ストレージの更新が失敗した理由の詳細を確認します。

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。

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。

AWS CLI および API を使用した更新のモニタリング

describe-file-systems AWS CLI コマンドと DescribeFileSystems API アクションを使用して、ファイルシステムの SSD IOPS 更新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 SSD IOPS を増やすと、`FILE_SYSTEM_UPDATE` および `IOPS_OPTIMIZATION` アクションの 2 つの `AdministrativeActions` が生成されます。

データ重複除外の管理

PowerShell でのリモート管理用の Amazon FSx CLI を使用して、ファイルシステムのデータ重複除外設定を管理できます。PowerShell での Amazon FSx CLI リモート管理の使用の詳細については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

データ重複除外に使用できるコマンドは次のとおりです。

データ重複除外コマンド	説明
Enable-FSxDedup	ファイル共有でデータ重複除外を有効にします。データ重複除外を有効にすると、重複除外後のデータ圧縮がデフォルトで有効になります。
Disable-FSxDedup	ファイル共有のデータ重複除外を無効にします。
Get-FSxDedupConfiguration	最適化の最小ファイルサイズと保存期間、圧縮設定、除外されたファイルタイプとフォルダなど、重複除外設定情報を取得します。
Set-FSxDedupConfiguration	最適化の最小ファイルサイズと保存期間、圧縮設定、除外されたファイルタイプとフォルダなど、重複除外の設定を変更します。
Get-FSxDedupStatus	重複除外ステータスを取得し、ファイルシステムの最適化の節約とステータス、時間、ファイルシステム上の最後の重複排除ジョブの完了ステータスを説明する読み取り専用プロパティを含めます。
Get-FSxDedupMetadata	重複除外最適化メタデータを取得します。
Update-FSxDedupStatus	更新されたデータ重複除外の節約情報を計算して取得します。
Measure-FSxDedupFileMetadata	フォルダのグループを削除した場合に、ファイルシステム上で再利用できる潜在的なストレージ領域を測定および取得します。多くの場合、ファイルには他のフォルダ間で共有されるチャンクがあり、重複除外エンジンは一意で削除されるチャンクを計算します。
Get-FSxDedupSchedule	現在定義されている重複除外スケジュールを取得します。
New-FSxDedupSchedule	データ重複除外スケジュールを作成およびカスタマイズします。
Set-FSxDedupSchedule	既存のデータ重複除外スケジュールの設定を変更します。
Remove-FSxDedupSchedule	重複除外スケジュールを削除します。

データ重複除外コマンド	説明
Get-FSxDedupJob	現在実行中またはキューに入っているすべての重複除外ジョブのステータスと情報を取得します。
Stop-FSxDedupJob	指定したデータ重複除外ジョブを 1 つ以上キャンセルします。

各コマンドのオンラインヘルプには、すべてのコマンドオプションのリファレンスが記載されています。このヘルプにアクセスするには、-? (例えば、Enable-FSxDedup -?) コマンドを実行します。

データ重複除外の有効化

Amazon FSx for Windows File Server ファイル共有でデータ重複除外を有効にするには、次のように `Enable-FSxDedup` コマンドを使用します。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

データ重複除外を有効にすると、デフォルトのスケジュールと設定が作成されます。以下のコマンドを使用して、スケジュールと設定を作成、変更、削除できます。

`Disable-FSxDedup` コマンドを使用して、ファイルシステムのデータ重複除外を完全に無効化できます。

データ重複除外スケジュールの作成

デフォルトのスケジュールはほとんどの場合うまく機能しますが、次のように `New-FsxDedupSchedule` コマンドを使用して、新しい重複除外スケジュールを作成することができます。データ重複除外スケジュールでは UTC 時間が使用されます。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

このコマンドは `CustomOptimization` という名前のスケジュールを作成します。これは、月曜日、水曜日、土曜日に実行され、毎日午前 8:00 (UTC) にジョブを開始し、最大期間は 7 時間で、ジョブがまだ実行されている場合はジョブを停止します。

新しいカスタム重複除外ジョブスケジュールを作成しても、既存のデフォルトスケジュールが上書きされたり、削除されたりすることはありません。デフォルトのジョブが不要な場合は、カスタム重複除外ジョブを作成する前に無効にすることができます。

以下に示すように、Set-FsxDedupSchedule コマンドを使用して、デフォルトの重複除外付けジュールを無効化できます。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

重複排除スケジュールは、Remove-FSxDedupSchedule -Name "ScheduleName" コマンドを使用して削除できます。デフォルトの BackgroundOptimization 重複排除スケジュールは変更または削除できないため、無効にする必要があります。

データ重複除外スケジュールの変更

次のように Set-FsxDedupSchedule コマンドを使用して、既存の重複除外スケジュールを変更できます。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

このコマンドは、既存の CustomOptimization スケジュールを修正します。これは、月曜日から水曜日と土曜日の日に実行され、毎日午前 9:00 (UTC) にジョブを開始し、最大期間は 9 時間で、ジョブがまだ実行されている場合はジョブを停止します。

最適化前のファイルの最小保存期間を変更するには、Set-FSxDedupConfiguration コマンドを使用します。

保存スペースの量の表示

データ重複除外を実行することで節約するディスク容量を表示するには、次のように Get-FSxDedupStatus コマンドを使用します。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
```

```
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> Capacity、FreeSpace、UsedSpace、UnoptimizedSize、SavingsRate のパラメータに対するコマンドレスポンスに表示される値は信頼できないため、使用しないでください。

データ重複排除のトラブルシューティング

以下の情報を使用して、データ重複排除を設定および使用する際の一般的な問題のトラブルシューティングにお役立てください。

トピック

- データ重複排除が機能していない
- 重複排除の値が予期せず 0 に設定されている
- ファイルを削除した後、ファイルシステムのスペースが解放されません

データ重複排除が機能していない

データ重複排除の現在のステータスを確認するには、`Get-FSxDedupStatus` PowerShell コマンドを実行し、最新の重複排除ジョブの完了ステータスを表示します。1 つ以上のジョブが失敗している場合、ファイルシステム上で空きストレージ容量の増加が見られない場合があります。

重複排除ジョブが失敗する最も一般的な理由は、メモリ不足です。

- Microsoft は、1 TB の論理的なデータあたり 1 GB のメモリが最適にあることを推奨します (または、1 TB の論理的なデータあたり少なくとも 350 MB)。Amazon FSx パフォーマンステーブル を使用して、ファイルシステムのスループットキャパシティに関連付けられているメモリを特定し、メモリリソースがデータのサイズに対して十分であることを確認します。そうでない場合は、ファイルシステムのスループットキャパシティを、論理データの 1 TB あたり 1 GB のメモリ要件を満たすレベルまで増やす必要があります。

- 重複排除ジョブは、Windows が推奨するデフォルトの 25% のメモリ割り当てで設定されます。つまり、32 GB のメモリを備えたファイルシステムの場合、8 GB が重複排除に使用できます。メモリ割り当ては設定可能です (パラメータ `-Memory` で `Set-FSxDedupSchedule` コマンドを使用します)。重複排除にメモリ割り当てを増やすと、ファイルシステムのパフォーマンスに影響する可能性があることに注意してください。
- 重複排除のジョブの設定を変更して、必要なメモリ量を削減できます。例えば、特定のファイルタイプまたはフォルダーで実行するように最適化を制限したり、最適化のための最小ファイルサイズと経過時間を設定したりできます。また、ファイルシステムのロードが最小限であるアイドル期間中に重複排除ジョブが実行されるように設定することをお勧めします。

重複排除ジョブを完了するのに十分な時間がない場合にも、エラーが表示されることがあります。データ重複除外スケジュールの変更 で説明されているように、ジョブの最大期間を変更する必要がある場合があります。

重複排除ジョブが長期間失敗していて、この期間中にファイルシステム上のデータに変更があった場合、後続の重複排除ジョブを初めて正常に完了するには、より多くのリソースが必要になる場合があります。

重複排除の値が予期せず 0 に設定されている

データ重複排除を設定したファイルシステムでは、`SavedSpace` と `OptimizedFilesSavingsRate` の値が予期せず 0 になります。

これは、ファイルシステムのストレージ容量を増やす際、ストレージ最適化プロセス中に発生する可能性があります。ファイルシステムのストレージ容量を増やすと、Amazon FSx は、ストレージ最適化プロセス中に既存のデータ重複排除ジョブをキャンセルします。これにより、以前のディスクから新しくより大きなディスクにデータが移行されます。ストレージ最適化ジョブが完了すると、Amazon FSx はファイルシステムでのデータ重複排除を再開します。ストレージ容量の増加とストレージの最適化の詳細については、「ストレージ容量の管理」を参照してください。

ファイルを削除した後、ファイルシステムのスペースが解放されません

データ重複排除の予想される動作は、重複排除がスペースを節約したデータが削除されたデータであった場合、ガベージコレクションのジョブが実行されるまでファイルシステムでスペースは解放されません。

役立つと思われるプラクティスとして、多数のファイルを削除した直後にガベージコレクションのジョブを実行するようにスケジュールを設定することができます。ガベージコレクションのジョブが

終了したら、ガベージコレクションのスケジュールを元の設定に戻すことができます。これにより、削除により解放された容量をすぐに確認できます。

次の手順を使用して、ガベージコレクションジョブを 5 分で実行するように設定します。

1. データ重複排除が有効になっていることを確認するには、`Get-FSxDedupStatus` コマンドを使用します。コマンドとその期待される出力の詳細については、「保存スペースの量の表示」を参照してください。
2. 以下を使用して、5 分後にガベージコレクションのジョブを実行するスケジュールを設定します。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. ガベージコレクションのジョブが実行され、スペースが解放されたら、スケジュールを元の設定に戻します。

DFS 名前空間の使用

DFS 名前空間は、異なるサーバーにある共有フォルダを 1 つ以上の論理的に構造化された名前空間にグループ化するために使用する Windows Server ロールサービスです。これにより、次の図に示すように、共有フォルダの仮想ビューをユーザーに付与できます。1 つのパスから複数のファイルシステムにあるファイルに移動できます。複数のファイルシステム間でファイル共有へのアクセスを整理および統合することに加えて、

複数の FSx for Windows File Server のファイルシステムと DFS 名前空間のグループ化

Microsoft 分散ファイルシステム (DFS) 名前空間を使用して、複数の FSx for Windows File Server ファイルシステム上のファイル共有を 1 つの一般的なフォルダ構造または名前空間にグループ化できます。DFS 名前空間を使用すると、大きなファイルデータセットの単一ファイルシステム (64

TiB) の最大ストレージ容量を超えて、数百ペタバイトまでのファイルストレージを拡張できます。このセクションでは、複数の FSx for Windows File Server ファイルシステムに DFS 名前空間を設定する方法を示します。

DFS 名前空間は、異なるサーバーにある共有フォルダを 1 つ以上の論理的に構造化された名前空間にグループ化するために使用する Windows Server ロールサービスです。これにより、次の図に示すように、共有フォルダの仮想ビューをユーザーに付与できます。1 つのパスから複数のファイルシステムにあるファイルに移動できます。複数のファイルシステム間でファイル共有へのアクセスを整理および統合することに加えて、

DFS 名前空間を使用して FSx for Windows ファイルシステムをグループ化するステップバイステップの手順については、「単一の名前空間で複数のファイルシステムをグループ化する」を参照してください。

シャードによるパフォーマンスの向上

Amazon FSx for Windows File Server は、Microsoft 配信ファイルシステム (DFS) の使用をサポートしています。DFS 名前空間を使用すると、ファイルデータを複数の Amazon FSx ファイルシステムに分散させて、入出力の負荷の高い I / O ワークロードに対応するためのパフォーマンス (読み取りと書き込みの両方) をスケールアウトすることができます。同時に、共通の名前空間下で統一されたビューをアプリケーションに表示することもできます。このソリューションには、ファイルデータをより小さなデータセットまたは シャード に分割したり、それらを異なるファイルシステム間に保存することが含まれています。複数のインスタンスからデータにアクセスするアプリケーションは、これらのシャードに対して並行して読み取りと書き込みを行うことで、高いレベルのパフォーマンスを設定できます。

スケールアウトパフォーマンスのための DFS 名前空間を使用したデータのシャーディング で提供されているソリューションを使用して、複数の FSx for Windows File Server ファイルシステムにデータへの読み取り/書き込みアクセスを均一に分散できます。

単一の名前空間で複数のファイルシステムをグループ化する

この手順では、複数の FSx for Windows ファイルシステム (財務、マーケティング、販売、home_directories) に保存されているファイル共有を統合するために、2 つの名前空間サーバーに 1 つのドメインベースの名前空間 (`example.com\corp`) を作成します。また、名前空間の下に 4 つのファイル共有を設定し、それぞれ別々の FSx for Windows ファイルシステムでホストされている共有に、ユーザーを透過的にリダイレクトさせます。これにより、ユーザーは、ファイル共有をホストする各ファイルシステムの DNS 名を指定しなくても、共通の名前空間を使用してファイル共有にアクセスできます。

> **Note**
>
> Amazon FSx を DFS 共有パスのルートに追加することはできません。

複数のファイルシステムを共通の DFS 名前空間にグループ化するには

1. DFS 名前空間サーバーをまだ実行していない場合は、setup-DFSN-servers.template テンプレートを使用して、高可用性 DFS AWS CloudFormation 名前空間サーバーのペアを起動できます。AWS 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。
2. 前のステップで起動した DFS 名前空間サーバーの 1 つに、AWS 委任管理者 グループのユーザーとして接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。
3. DFS 管理コンソールを開いてアクセスします。[Start] (スタート) メニューを開き、dfsmgmt.msc を実行します。これにより DFS 管理 GUI ツールが開きます。
4. [Action] (アクション)、それから [New Namespace] (新規名前空間) を選択し、[Server] (サーバー) で最初に起動した DFS 名前空間サーバーのコンピュータ名を入力し、[Next] (次へ) を選択します。
5. [Name] (名前) に、作成する名前空間を入力します (例えば、Corp)。
6. [Edit Settings] (設定の編集) を選択して、要件に応じて適切な許可を設定します。[Next] (次へ) を選択します。

7. デフォルトの[Domain-based namespace] (ドメインベースの名前空間) オプションが選択されたままにします。[Enable Windows Server 2008 mode] (Windows サーバー 2008 モードを有効化) オプションも選択したままで、[Next] (次へ) を選択します。

> **Note**
>
> Windows Server 2008 モードは、名前空間で使用可能な最新のオプションです。

8. 名前空間の設定を確認し、[Create] (作成) を選択します。
9. ナビゲーションバーの[Namespaces] (名前空間) で新規作成した名前空間が選択された状態で、[Action] (アクション)、[Add Namespace Server] (名前空間サーバーの追加) の順に選択します。
10. 名前空間サーバー に起動した 2 つ目の DFS 名前空間サーバーのコンピュータ名を入力します。
11. [Edit Settings] (設定の編集) を選択し、要件に基づいて適切な許可を設定し、[OK] を選択します。
12. 作成した名前空間のコンテキスト (右クリック) メニューを開き、[New Folder] (新しいフォルダ) を選択し、フォルダ名を入力し (例えば 名前 に `finance`)、[OK] を選択します。
13. フォルダーターゲットへのパス のために、DFS 名前空間フォルダを指定するファイル共有の DNS 名を UNC 形式で入力して (例えば `\\fs-0123456789abcdef0.example.com\finance`)、[OK] を選択します。
14. 共有が存在しない場合。
    a. [Yes] (はい) を選択して共有を作成します。
    b. [Create Share] (共有の作成) ダイアログから、[Browse] (参照) を選択します。
    c. 既存のフォルダを選択するか、[D$] の下に新しいフォルダを作成して、[OK] 選択します。
    d. 適切な共有許可を設定し、[OK] を選択します。
15. [New Folder] (新しいフォルダ) ダイアログで、[OK] を選択します。新しいフォルダーが名前空間の下に作成されます。
16. 最後の 4 つのステップを繰り返して、同じ名前空間で共有したい他のフォルダを作成します。

スケールアウトパフォーマンスのための DFS 名前空間を使用したデータのシャーディング

以下の手順では、スケールアウトパフォーマンスを実現するために、Amazon FSx 上で DFS ソリューションを作成する方法について説明します。この例では、*`corp`* 名前空間に保存されている

データがアルファベット順にシャードされています。データファイル「A-F」、「G-M」、「N-Z」はすべて異なるファイル共有に保存されます。データの種類、入出力 I / O サイズ、および入出力 I / O アクセスパターンに基づいて、複数のファイル共有間でデータをシャードさせる最適な方法を決定する必要があります。使用する予定のすべてのファイル共有に、入出力 I / O を均等に配信するシャーディング方式を選択します。各名前空間は、最大 50,000 のファイル共有と、全体で数百ペタバイトのストレージ容量をサポートすることに注意してください。

スケールアウトパフォーマンスに DFS 名前空間を設定するには

1. DFS 名前空間サーバーをまだ実行していない場合は、setup-DFSN-servers.template テンプレートを使用して、高可用性 DFS AWS CloudFormation 名前空間サーバーのペアを起動できます。AWS 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。
2. 前のステップで起動した DFS 名前空間サーバーの 1 つに、AWS 委任管理者 グループのユーザーとして接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。
3. DFS 管理コンソールにアクセスします。[Start] (スタート) メニューを開いて dfsmgmt.msc を実行します。これにより DFS 管理 GUI ツールが開きます。
4. [Action] (アクション)、それから [New Namespace] (新規名前空間) を選択し、[Server] (サーバー) で最初に起動した DFS 名前空間サーバーのコンピュータ名を入力し、[Next] (次へ) を選択します。
5. [Name] (名前) に、作成する名前空間を入力します (例えば、Corp)。
6. [Edit Settings] (設定の編集) を選択して、要件に応じて適切な許可を設定します。[Next] (次へ) を選択します。

7. デフォルトの[Domain-based namespace] (ドメインベースの名前空間) オプションが選択されたままにします。[Enable Windows Server 2008 mode] (Windows サーバー 2008 モードを有効化) オプションも選択したままで、[Next] (次へ) を選択します。

> **Note**
>
> Windows Server 2008 モードは、名前空間で使用可能な最新のオプションです。

8. 名前空間の設定を確認し、[Create] (作成) を選択します。
9. ナビゲーションバーの[Namespaces] (名前空間) で新規作成した名前空間が選択された状態で、[Action] (アクション)、[Add Namespace Server] (名前空間サーバーの追加) の順に選択します。
10. 名前空間サーバー に起動した 2 つ目の DFS 名前空間サーバーのコンピュータ名を入力します。
11. [Edit Settings] (設定の編集) を選択し、要件に応じて適切な許可を設定し、[OK] を選択します。
12. 作成した名前空間のコンテキスト (右クリック) メニューを開き、[New Folder] (新規フォルダ) を選択し、最初のシャードのフォルダ名 (例えば [Name] (名前) に `A-F`) を入力して、[Add] (追加) を選択します。
13. [Path to folder target] (フォルダーターゲットへのパス) に、このシャードをホストしているファイル共有の DNS 名を UNC 形式 (例えば `\\fs-0123456789abcdef0.example.com\A-F`) で入力し、[OK] を選択します。
14. 共有が存在しない場合。
    a. [Yes] (はい) を選択して共有を作成します。
    b. [Create Share] (共有の作成) ダイアログから、[Browse] (参照) を選択します。
    c. 既存のフォルダを選択するか、[D$] の下に新しいフォルダを作成して、[OK] 選択します。
    d. 適切な共有許可を設定し、[OK] を選択します。
15. このシャードにフォルダーターゲットが追加されたら、[OK] を選択します。
16. 同じ名前空間に追加したい他のシャードについても、後半の 4 つのステップを繰り返します。

スループット容量の管理

ファイルシステムのスループットキャパシティを増減して、いつでもパフォーマンスを管理できます。スループットキャパシティは、FSx for Windows File Server 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。スループットキャパシティでは、秒ごとの I/O オペレーション (IOPS) のレベルが高くなり、ファイルサーバー上のキャッ

シュメモリの量が増えます。詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。

トピック

- スループットスケーリングの仕組み
- スループットキャパシティを変更するタイミングを知る
- スループットキャパシティの変更
- スループットキャパシティの更新のモニタリング

スループットスケーリングの仕組み

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、バックグラウンドでスループットが増減するサーバーに切り替えます。マルチ AZ ファイルシステムの場合、Amazon FSx が優先ファイルサーバーとセカンダリファイルサーバーを切り替える間、自動フェイルオーバーとフェイルバックをトリガーする新しいファイルサーバーに切り替えます。シングル AZ システムでは、ファイルサーバーがスループットキャパシティのスケーリング中に切り替わる間にファイルシステムが数分間利用できなくなります。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キャパシティが課金されます。

> **Note**
>
> バックエンドでのメンテナンスオペレーション中に、システムの変更 (スループットキャパシティの変更を含む) が遅れる場合があります。メンテナンスオペレーションでは、システムの変更によってキューに入り、処理される可能性があります。

マルチ AZ ファイルシステムの場合、Amazon FSx が優先ファイルサーバーおよびセカンダリファイルサーバーを切り替える間、スループットキャパシティのスケーリングは自動フェイルオーバーおよびフェイルバックを引き起こします。スループットキャパシティのスケーリング、ファイルシステムのメンテナンス、および予期しないサービスの中断中に発生するファイルサーバーの置き換え中、ファイルシステムへの進行中のトラフィックは、残りのファイルサーバーによって処理されます。交換したファイルサーバーがオンラインに戻ると、FSx for Windows は再同期ジョブを実行し、データが新しく交換されたファイルサーバーに確実に同期されるようにします。

FSx for Windows は、この再同期アクティビティがアプリケーションとおよびーザーに与える影響を最小限に抑えるように設計されています。ただし、再同期プロセスでは大きなブロックでデータを

同期する必要があります。つまり、ごく一部のデータのみが更新された場合でも、データの大きなブロックを同期する必要があります。したがって、再同期の量はデータチャーンの量だけでなく、ファイルシステム上のデータチャーンの性質にも依存します。ワークロードの書き込みと IOPS が多い場合、データ同期処理に時間がかかり、追加のパフォーマンスリソースが必要になることがあります。

この間、ファイルシステムは引き続き使用可能になりますが、データ同期の期間を短縮するために、ファイルシステムの負荷が最小であるアイドル期間中にスループット容量を変更することをお勧めします。データ同期にかかる時間を短縮するため、ファイルシステムには、ワークロードに加えて同期ジョブも実行するために十分なスループットキャパシティがあるか確認することをお勧めします。最後に、ファイルシステムの負荷が軽いうちにフェイルオーバーの影響をテストすることをお勧めします。

スループットキャパシティを変更するタイミングを知る

Amazon FSx は Amazon CloudWatch と統合され、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パフォーマンス (スループットと IOPS) は、ファイルシステムのスループットキャパシティ、ストレージ容量、ストレージタイプと共に、特定のワークロードの特性によって異なります。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、「Amazon CloudWatch によるモニターリング」を参照してください。

FSx for Windows File Server は、Amazon FSx コンソールのファイルシステムの詳細ページのモニタリングとパフォーマンスダッシュボードで、ファイルシステムの CloudWatch メトリクスの値に基づいてパフォーマンスアラートを提供します。これには、スループットキャパシティ、およびスループットキャパシティの増加から恩恵を受ける可能性のあるその他のファイルシステムメトリクスが含まれます。詳細については、「パフォーマンスの警告と推奨事項」を参照してください。

ワークロードの予想されるトラフィックだけでなく、ファイルシステムで有効にする機能をサポートするために必要な追加のパフォーマンスリソースも満たすのに十分なスループットキャパシティでファイルシステムを設定します。例えば、データ重複排除を実行している場合、選択するスループットキャパシティは、使用しているストレージに基づいて重複排除を実行するのに十分なメモリを提供する必要があります。シャドウコピーを使用している場合は、Windows Server がシャドウコピーを削除しないように、スループットキャパシティをワークロードによって駆動されると予想される値の 3 倍以上の値に増やしてください。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。

スループットキャパシティの変更

次の手順で説明するように、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キャパシティを増減できます。

ファイルシステムのスループット容量を変更するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. [File systems] (ファイルシステム) に移動し、スループット容量を拡張する Windows ファイルシステムを選択します。
3. [Actions] (アクション) には、[Update throughput] (スループットの更新) 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。

   スループット容量の更新 ウィンドウが表示されます。
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。

   > **Note**
   >
   > マルチ AZ ファイルシステムは、スループットスケーリングの更新時にフェイルオーバーしてフェイルバックし、完全に利用可能になります。シングル AZ ファイルシステムは更新中、ごくわずかな期間利用できないことがあります。

6. [Updates] (更新) タブの [File systems] (ファイルシステム) 詳細ページで、更新の進捗状況をモニタリングできます。

   Amazon FSx コンソール、、および API を使用して AWS CLI、更新の進行状況をモニタリングできます。詳細については、「スループットキャパシティの更新のモニタリング」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キャパシティを増減するには、 AWS CLI コマンド update-file-system を使用します。以下のパラメータを設定します。

- 更新するファイルシステムの ID への `--file-system-id`。

- `ThroughputCapacity` を目的の値に指定します。有効な値は 8、16、32、64、128、256、512、1024、2048、4608、6144、9216、12288 MBps です。

Amazon FSx コンソール、、および API を使用して AWS CLI、更新の進行状況をモニタリングできます。詳細については、「スループットキャパシティの更新のモニタリング」を参照してください。

スループットキャパシティの更新のモニタリング

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 details] (ファイルシステムの詳細) ウィンドウの [Updates] (更新) タブで、更新アクションの種類ごとに最新の 10 件の更新アクションを表示できます。

Update type	Target value	Status	Progress %	Request time
Storage capacity	154	Completed	-	2020-05-22T12:14:58-04:00
Throughput capacity	64	Completed	-	2020-05-22T12:14:50-04:00
Throughput capacity	128	Completed	-	2020-05-21T13:55:58-04:00
Storage capacity	140	Completed	-	2020-05-21T13:55:30-04:00
Storage capacity	122	Completed	-	2020-05-18T11:36:33-04:00

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)

可能な値は、[スループットキャパシティ] 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。
- [最適化の更新] — Amazon FSx は、ファイルシステムのネットワーク I/O、CPU、メモリリソースを更新しました。新しいディスク I/O パフォーマンスレベルを書き込み操作に利用できます。読み取り操作では、ファイルシステムがこの状態ではなくなるまで、前のレベルと新しいレベル間でディスク I/O パフォーマンスが表示されます。
- [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 および API を使用した変更のモニタリング

describe-file-systems CLI コマンドおよび DescribeFileSystems API アクションを使用して、ファイルシステムのスループット容量変更リクエストを表示し、モニタリングできます。`AdministrativeActions` 配列には、管理アクションタイプごとに最新の更新アクションが 10 件を表示されます。ファイルシステムのスループット容量を変更すると、`FILE_SYSTEM_UPDATE` 管理アクションが生成されます。

次の例は、`describe-file-systems` CLI コマンドのレスポンスの抜粋を示しています。ファイルシステムのスループット容量は 8 MBps、ターゲットスループット容量は 256 MBps です。

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
```

```
    }
]
```

Amazon FSx でアクションの処理が正常に完了すると、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": {
          "WindowsConfiguration": {
            "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 プロパティは失敗に関する情報を提供します。失敗したアクションのトラブルシューティングについては、「ストレージまたはスループットキャパシティの更新が失敗する」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その他の FSx for Windows File Server リソースの管理に役立つように、タグの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、目的、所有者、環境など、さまざまな方法で AWS リソースを分類できます。これは同じタイプのリソースが多数ある場合に役立ちます。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

- タグの制限
- リソースにタグを付けるために必要なアクセス許可

タグの基本

タグは、 AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。

タグを使用すると、目的、所有者、環境など、さまざまな方法で AWS リソースを分類できます。たとえば、各インスタンスの所有者とスタックレベルを追跡するのに役立つ、アカウントの FSx for Windows File Server ファイルシステムのタグのセットを定義できます。

各リソースタイプ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。一貫性のある一連のタグキーを使用することで、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。効果的なリソースタグ付け戦略の実装方法の詳細については、 AWS ホワイトペーパー「タグ付けのベストプラクティス」を参照してください。

タグは Amazon FSx に対してセマンティックな意味は持たず、文字列として厳密に解釈されます。また、タグは自動的にリソースに割り当てられます。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。

FSx for Windows File Server API、 CLI、または AWS SDK を使用している場合は、 `TagResource` API AWS アクションを使用して既存のリソースにタグを適用できます。さらに、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できます。リソースの作成時にタグを適用できない場合はリソース作成プロセスがロールバックされます。これにより、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。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ティングを実行する必要がなくなります。作成時にユーザーがリソースにタグ付けできるようにする方法については、「リソース作成時にタグ付けするアクセス許可の付与」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 FSx for Windows File Server リソースにタグを付けることができます。Amazon FSx コンソールを使用している場合は、関連するリソース画面のタグタブを使用して、

リソースにタグを適用できます。リソースを作成するときは、Name キーに値を適用できます。また、新しいファイルシステムを作成するときに、選択したタグを適用できます。コンソールは Name タグに従ってリソースを整理できますが、このタグには FSx for Windows File Server サービスに対する意味論的な意味はありません。

IAM ポリシーのタグベースのリソースレベルのアクセス許可を、作成時のタグ付けをサポートする FSx for Windows File Server API アクションに適用して、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きめ細かく制御できます。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、リソースの使用を制御するタグベースのリソースレベルアクセス権限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。

IAM ポリシーの `TagResource`および `UntagResource` FSx for Windows File Server API アクションにリソースレベルのアクセス許可を適用して、既存のリソースに設定されているタグキーと値を制御することもできます。

請求用リソースへのタグ付けの詳細についてはAWS Billing ユーザーガイドの「コスト配分タグの使用」を参照してください。

タグの制限

タグには以下のような基本制限があります。

- リソースあたりのタグの最大数 - 50 件
- 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。
- キーの最大長 - UTF-8 の 128 Unicode 文字
- 値の最大長 - UTF-8 の 256 Unicode 文字
- FSx for Windows File Server タグに使用できる文字は、UTF-8 で表される文字、数字、スペース、および + - = . _ : / @ 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 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にはカウントされません。

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。削除するには、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され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。

パブリック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 でのみ使用でき AWS アカウント、他の AWS アカウント はそれらのタグにアクセスできなくなります。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 はリソースへのアクセスを制御するために独自のタグセットを割り当てる AWS アカウント 必要があります。

リソースにタグを付けるために必要なアクセス許可

作成時に Amazon FSx リソースにタグ付けする際に必要なアクセス許可の詳細については、「リソース作成時にタグ付けするアクセス許可の付与」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。

を使用してファイルシステムを更新する AWS CLI

このチュートリアルの手順を使用して更新できる 3 つの要素があります。これら以外の更新可能なファイルシステムの要素は、すべてコンソールから更新できます。これらの手順は、ローカルコンピュータに AWS CLI がインストールされ、設定されていることを前提としています。詳細については、「AWS Command Line Interface ユーザーガイド」の「インストールと設定」を参照してください。

- AutomaticBackupRetentionDays - ファイルシステムの自動バックアップを保持する日数。
- DailyAutomaticBackupStartTime - 日次自動バックアップ時間枠をスタートする協定世界時 (UTC) の時刻。期間はこの指定時刻から 30 分間です。この期間は、週 1 回のメンテナンスバックアップ時間枠と重複させることはできません。
- WeeklyMaintenanceStartTime - メンテナンス時間枠をスタートする週の時刻。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。

以下の手順では、ファイルシステムを AWS CLIで更新する方法を説明しています。

ファイルシステムの自動バックアップ保持期間を更新するには

1. コンピュータでコマンドプロンプトまたはターミナルを開きます。
2. 次のコマンドを実行し、ファイルシステム ID をユーザーのファイルシステムの ID に、そして自動バックアップを保持したい日数に置き換えます。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

ファイルシステムの日次バックアップ期間を更新するには

1. コンピュータでコマンドプロンプトまたはターミナルを開きます。
2. 次のコマンドを実行し、ファイルシステム ID をユーザーのファイルシステムの ID に置き換え、時刻をバックアップ期間を開始させたい時刻に置き換えます。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

ファイルシステムの毎週のメンテナンス期間を更新するには

1. コンピュータでコマンドプロンプトまたはターミナルを開きます。
2. 次のコマンドを実行し、ファイルシステム ID をユーザーのファイルシステムの ID に、日時をメンテナンス期間を開始する日時に置き換えます。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

バックアップ、シャドウコピー、およびスケジューラのレプリケーションによるデータの保護

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

- Amazon FSx のネイティブバックアップは、Amazon FSx 内のバックアップ保持およびコンプライアンスのニーズをサポートします。
- AWS Backup Amazon FSx ファイルシステムのバックアップは、クラウドおよびオンプレミス AWS のサービス全体で一元化され自動化されたバックアップソリューションの一部です。
- Windowsシャドウコピーを使用すことで、ユーザーは、ファイルの変更を簡単に取り消すことができ、ファイルを以前のバージョンに復元することで、ファイルのバージョンを比較することができます。
- AWS DataSync Amazon FSx ファイルシステムの 2 番目のファイルシステムへのスケジュールされたレプリケーションは、データ保護とリカバリを提供します。

トピック

- バックアップでデータを保護する。
- シャドウコピーによるデータの保護
- を使用したスケジュールされたレプリケーション AWS DataSync

バックアップでデータを保護する。

FSx for Windows File Server ファイルシステムのデータを保護するには、ファイルシステムの定期的なバックアップを実行します。Amazon FSx には、ファイルシステムをバックアップするための複数のオプションが用意されています。自動日次バックアップを使用して、毎日バックアップを取ることができます。ファイルシステムのユーザー主導のバックアップはいつでも実行できます。 AWS リソースの一元化されたバックアップソリューション AWS Backup の一部として を使用することもできます。これらのバックアップソリューションは、データ保持、ビジネス、コンプライアンスのニーズを満たすのに役立ちます。

ファイルシステムでデフォルトで有効になっている自動日次バックアップを使用し、 を 全体の一元化されたバックアップソリューション AWS Backup に使用することをお勧めします AWS のサービ

ス。 AWS Backup を使用すると、異なる頻度 (1 日に複数回、毎日、毎週など) と保持期間で追加のバックアッププランを設定できます。

Amazon FSx を使用すると、バックアップはファイルシステムの一貫性があり、高い耐久性、増分です。各バックアップには、新しいファイルシステムを作成するために必要なすべての情報が含まれているので、ファイルシステ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することができます。ファイルシステムの一貫性を確保するために、Amazon FSx は Microsoft Windows のボリュームシャドウコピーサービス (VSS) を使用します。高い耐久性を確保するために、Amazon FSx はバックアップを Amazon Simple Storage Service (Amazon S3) に保存します。

Amazon FSx バックアップは、自動の日次バックアップを使用して生成されるか、ユーザー主導のバックアップ機能を使用して生成されるかにかかわらず、増分します。つまり、最新のバックアップの後に変更されたファイルシステム上のデータのみが保存されます。これにより、バックアップの作成に必要な時間が最小限に抑えられ、データを複製しないことでストレージコストを節約できます。

バックアッププロセス中のある時点で、ストレージ I/O が一時的に中断されることがあります (一般的に数秒間)。VSS サービスは I/O を再開する前にすべてのキャッシュされた書き込みをディスクにフラッシュする必要があるため、ワークロードの 1 秒あたりの書き込みオペレーション (`DataWriteOperations`) の数が多い場合は、一時停止の時間が長くなることがあります。ほとんどのユーザーとアプリケーションでは、この I/O 中断が短時間の I/O 一時停止として発生します。アプリケーションのタイムアウトに対する感度は、その構成に応じて異なる場合があります。

ファイルシステムの定期的なバックアップを作成することは、Amazon FSx for Windows File Server がファイルシステムに対して実行するレプリケーションを補完するベストプラクティスです。Amazon FSx バックアップは、バックアップ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ちます。Amazon FSx バックアップの操作は、バックアップの作成、バックアップのコピー、バックアップからのファイルシステムの復元、バックアップの削除などを簡単に行えます。シングルファイルシステムのバックアップの使用状況を表示するには、その特定のバックアップのタグを有効にし、タグベースの請求レポートを有効にする必要があります。

トピック

- 自動の日次バックアップの操作
- ユーザー主導のバックアップ機能
- Amazon FSx AWS Backup での の使用
- バックアップのコピー
- 新しいファイルシステムへのバックアップの復元
- ユーザーによるバックアップの作成

- バックアップの削除
- バックアップのサイズ
- 同じアカウント内のバックアップのコピー
- 新しいファイルシステムへのバックアップの復元

自動の日次バックアップの操作

デフォルトで、Amazon FSx はファイルシステムの日次自動バックアップを実行します。自動の日次バックアップは、ファイルシステムの作成時に設定された日次バックアップウィンドウ中に実行されます。日次バックアップウィンドウを選択するときは、ファイルシステムを使用するアプリケーションに対して、通常の営業時間外の都合の良い時間帯を選択することをお勧めします。また、ファイルシステムのメンテナンスが進行中の場合、自動バックアップが発生しない可能性があるため、メンテナンスウィンドウの外部で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。

自動の日次バックアップは、保持期間と呼ばれる一定期間の間保持されます。Amazon FSx コンソールでファイルシステムを作成する場合、デフォルトの自動日次バックアップの保持期間は 30 日です。デフォルトの保持期間は Amazon FSx API と CLI で異なります。保持期間は、0 ~ 90 日間で設定できます。保持期間を 0 (ゼロ) 日 に設定すると、自動日次 バックアップが行われなくなります。自動日次バックアップは、ファイルシステムの削除時に削除されます。

> **Note**
>
> 保持期間を 0 日に設定すると、ファイルシステムが自動的にバックアップされることはありません。関連したすべてのレベルの重要な機能を持つファイルシステムには、自動日次バックアップを使用することを強くお勧めします。

AWS CLI またはいずれかの AWS SDKs を使用して、ファイルシステムのバックアップウィンドウとバックアップ保持期間を変更できます。`UpdateFileSystem` API オペレーションまたは `update-file-system` CLI コマンドを使用します。詳細については、「を使用してファイルシステムを更新する AWS CLI」を参照してください。

> **Important**
>
> 自動日次バックアップの保持期間を短くすると、新しい保持期間外にバックアップが永続的に削除されます。続行する前に、これらの古いバックアップが不要になったことを確認してください。

ユーザー主導のバックアップ機能

Amazon FSx では、いつでもファイルシステムのバックアップを手動で作成できます。これを行うには、Amazon FSx コンソール、API、または AWS Command Line Interface () を使用しますAWS CLI。ユーザーが作成した Amazon FSx ファイルシステムのバックアップは期限切れにならず、保存したい期間利用できます。ユーザーによるバックアップは、バックアップされたファイルシステムを削除した後も保持されます。ユーザーが作成したバックアップは、Amazon FSx コンソール、API、または CLI を使用してのみ削除できます。Amazon FSx によって自動的に削除されることはありません。詳細については、「バックアップの削除」を参照してください。

ファイルシステムの変更中 (スループット容量の更新中やファイルシステムのメンテナンス中など) にバックアップが開始された場合、バックアップリクエストはキューに入れられ、アクティビティが完了すると再開されます。

ファイルシステムのユーザー主導のバックアップを行う方法については、「ユーザーによるバックアップの作成」を参照してください。

Amazon FSx AWS Backup での の使用

AWS Backup は、Amazon FSx ファイルシステムをバックアップすることでデータを保護するシンプルで費用対効果の高い方法です。 AWS Backup は、作成を簡素化するために設計された統合バックアップサービスです。 コピー、 復元、 バックアップの削除 レポートと監査が改善されると同時に、 AWS Backup 規制、 また、 AWS Backup は AWS ストレージボリュームを保護します。 データベース、 と ファイルシステムは、以下を実行できる一元的な場所を提供することで、よりシンプルになります。

- バックアップする AWS リソースを設定して監査します。
- 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。
- AWS リージョン間および AWS アカウント間でバックアップをコピーします。
- 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 コンソールから取得したバックアップは、Amazon FSx コンソールから取得したバックアップと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、および同じ復元オプションを持ちます。から取得されたバックアップ AWS Backup は、ユーザーが開始または自動で取得する他の Amazon FSx バックアップと比較して増分的です。

AWS Backup を使用してこれらのバックアップを管理すると、無制限の保持オプションや、1 時間ごとにスケジュールされたバックアップを作成する機能などの追加機能を利用できます。さらに、ソースファイルシステムが削除された後でも、 はイミュータブルバックアップ AWS Backup を保持します。これにより、偶発的または悪意のある削除から保護されます。

によって作成されたバックアップ AWS Backup 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クォータにカウントされます。によって作成されたバックアップは、Amazon FSx コンソール、CLI、および API AWS Backup で表示および復元できます。ただし、Amazon FSx コンソール、CLI、または API AWS Backup で によって作成されたバックアップを削除することはできません。 AWS Backup を使用して Amazon FSx ファイルシステムをバックアップする方法の詳細については、 AWS Backup デベロッパーガイドの「Amazon FSx ファイルシステムの使用」を参照してください。

バックアップのコピー

Amazon FSx を使用して、同じ AWS アカウント内のバックアップを別の AWS リージョン (クロスリージョンコピー) または同じ AWS リージョン (リージョン内コピー) に手動でコピーできます。クロスリージョンコピーは、同じ AWS パーティション内でのみ作成できます。ユーザー主導のバックアップコピーは、Amazon FSx コンソール AWS CLI、または API を使用して作成できます。ユーザー主導バックアップコピーを作成するときは、タイプ `USER_INITIATED` があります。

AWS Backup を使用して、 AWS リージョン間および AWS アカウント間でバックアップをコピーすることもできます。 AWS Backup は、ポリシーベースのバックアッププランの一元的なインターフェイスを提供するフルマネージドバックアップ管理サービスです。クロスアカウント管理では、バックアップポリシーを自動的に使用して、組織内の アカウント全体にバックアッププランを適用できます。

クロスリージョンバックアップコピー は、クロスリージョン災害対策に特に役立ちます。プライマリ AWS リージョンで災害が発生した場合にバックアップから復元し、他の AWS リージョンですぐに可用性を回復できるように、バックアップを作成して別の AWS リージョンにコピーします。バックアップコピーを使用して、ファイルデータセットを別の AWS リージョンまたは同じ AWS リージョン内にクローンすることもできます。Amazon FSx コンソール、または Amazon FSx API を使用して AWS CLI、同じ AWS アカウント (クロスリージョンまたはインリージョン) 内にバックアップコピーを作成します。また、AWS Backup を使用して、オンデマンドまたはポリシーベースのバックアップコピーを実行することもできます。

クロスアカウントバックアップコピーは、バックアップを分離されたアカウントにコピーするための規制コンプライアンス要件を満たすために役立ちます。また、バックアップの偶発的または悪意のある削除、認証情報の喪失、または AWS KMS キーの侵害を防ぐためのデータ保護レイヤーも追加さ

れています。クロスアカウントバックアップは、ファンイン (複数のプライマリアカウントから 1 つの独立したバックアップ コピーアカウントにバックアップをコピーすること) および ファンアウト (1 つのプライマリアカウントから複数の独立したバックアップ コピーアカウントにバックアップをコピーすること) をサポートします。

サポート AWS Backup で を使用して、クロスアカウントバックアップコピーを作成できます AWS Organizations 。クロスアカウントコピーのアカウント境界は、 AWS Organizations ポリシーによって定義されます。 AWS Backup を使用してクロスアカウントバックアップコピーを作成する方法の詳細については、 AWS Backup デベロッパーガイドの「 でのバックアップコピーの作成 AWS アカウント」を参照してください。

バックアップコピーの制約

バックアップをコピーする際の制約は以下のとおりです。

- クロスリージョンバックアップコピーは、任意の 2 つの商用 AWS リージョン間、中国 (北京) と中国 (寧夏) リージョン間、および AWS GovCloud (米国東部) と AWS GovCloud (米国西部) リージョン間でのみサポートされますが、これらのリージョンのセット間ではサポートされません。
- クロスリージョンバックアップコピーは、オプトインリージョンではサポートされていません。
- リージョン内のバックアップコピーは、任意の AWS リージョン内で作成できます。
- コピーする前に、出典バックアップは、`AVAILABLE` のステータスである必要があります。
- コピー中の出典バックアップは削除できません。デスティネーション・ バックアップが利用可能になってから、出典バックアップを削除できるようになるまでの間に、短い遅延が発生する場合があります。出典バックアップの削除を再試行する場合は、この遅延に注意する必要があります。
- アカウントごとに 1 つの送信先 AWS リージョンに対して最大 5 つのバックアップコピーリクエストを実行できます。

クロスリージョンのバックアップコピーの許可

IAM ポリシーステートメントを使用して、バックアップコピー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。ソース AWS リージョンと通信してクロスリージョンバックアップコピーをリクエストするには、リクエスタ (IAM ロールまたは IAM ユーザー) がソースバックアップとソース AWS リージョンにアクセスできる必要があります。

ポリシーを使用して、バックアップコピーオペレーションの `CopyBackup` アクションにアクセス許可を付与します。次の例のように、ポリシーの `Action` フィールドでアクションを指定し、ポリシーの `Resource` フィールドでリソース値を指定します。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

IAM ポリシーの詳細については、IAM ユーザーガイド の「IAM ポリシーと許可」を参照してください。

フルコピーと増分コピー

ソースバックアップから別のコピー先 AWS リージョンまたはコピー先 AWS アカウントにバックアップをコピーする場合、同じ KMS キーを使用してバックアップのソースコピーとコピー先コピーの両方を暗号化した場合でも、最初のコピーはフルバックアップコピーになります。

最初のバックアップコピー後、同じ AWS アカウント内の同じコピー先リージョンへの後続のバックアップコピーはすべて増分されます。ただし、そのリージョンで以前にコピーされたすべてのバックアップを削除しておらず、同じ AWS KMS キーを使用していることが条件です。いずれかの条件が満たされていない場合、コピーオペレーションはフル (増分ではない) バックアップのコピーになります。

ファイルシステムのバックアップをコピーする方法については、「同じアカウント内のバックアップのコピー」を参照してください。

新しいファイルシステムへのバックアップの復元

可能なバックアップを使用して新しいファイルシステムを作成し、別のファイルシステムのポイントインタイム スナップショット を効果的に復元できます。コンソール AWS CLI、またはいずれかの AWS SDKs を使用してバックアップを復元できます。新しいファイルシステムへのバックアップの復元には、新しいファイルシステムの作成と同じ時間がかかります。バックアップから復元されたデータは、ファイルシステムにレイジーロードされ、その間、レイテンシーがわずかに長くなります。

復元されたファイルシステムにユーザーが引き続きアクセスできるようにするには、復元されたファイルシステムに関連付けられている Active Directory ドメインが、元のファイルシステムの Active Directory ドメインと同じであるか、元のファイルシステムの Active Directory ドメインによって信頼されていることを確認してください。Active Directory スキーマの詳細については、「Microsoft Active Directory の使用」を参照してください。

新しい FSx for Windows ファイルシステムにバックアップを復元する方法については、「新しいファイルシステムへのバックアップの復元」を参照してください。

> **Note**
>
> ファイルシステムバックアップは、元のファイルシステムと同じデプロイタイプとストレージ容量を持つ新しいファイルシステムにのみ復元できます。新しいファイルシステムのストレージ容量は、利用可能になった後、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。

バックアップを新しいファイルシステムに復元するときに、次のいずれかのファイルシステム設定を変更できます。

- ストレージタイプ
- スループット容量
- VPC
- アベイラビリティーゾーン
- サブネット
- VPC セキュリティグループ
- アクティブディレクトリの設定
- AWS KMS 暗号化キー
- 毎日の自動バックアップ開始時間
- 週次メンテナンス時間枠

ユーザーによるバックアップの作成

日次自動ファイルシステムバックアップに加えて、次の手順で説明するように、Amazon FSx コンソールを使用して、ユーザー主導のファイルシステムバックアップをいつでも作成できます。

ユーザーがファイルシステムのバックアップを作成するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. コンソールダッシュボードから、バックアップするファイルシステムの名前を選択します。
3. [Actions] (アクション)から、[Create backup] (バックアップの作成) を選択します。
4. 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。
5. [Create backup] (バックアップの作成) を選択します。

これで、ファイルシステムのバックアップが作成されました。左側のナビゲーションで、[Backups] (バックアップ を選択すると、Amazon FSx コンソールにすべてのバックアップの表を見つけることができます。新しいユーザー主導バックアップには `USER_INITIATED` タイプがあり、ステータスは `AVAILABLE` になるまで `CREATING` です。詳細については、「ユーザー主導のバックアップ機能」を参照してください。

バックアップの削除

以下の手順で説明されているように、Amazon FSx コンソール、CLI、または API を使用して、ファイルシステムのユーザー主導の日次自動バックアップを削除できます。Backup のタイプを持つ によって作成されたAWS バックアップを削除するには AWS Backup、 AWS Backup コンソール、CLI、または API を使用する必要があります。バックアップの削除は、永久的で回復不能なアクションです。削除されたバックアップ内のデータもすべて削除されます。今後そのバックアップが必要でないということが確かでない限り、バックアップを削除しないでください。

バックアップを削除するには (コンソール)

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. コンソールダッシュボードで、左側のナビゲーションから [Backups] (バックアップ) を選択します。
3. [Backups] (バックアップ) テーブルから削除するバックアップを選択してから、[Delete backup] (バックアップの 削除) を選択します。
4. 開いた [Delete backups] (バックアップの削除) ダイアログボックスで、バックアップの ID が削除するバックアップを識別してい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。

これで、バックアップと含まれているすべてのデータが完全に復元不能に削除されます。

バックアップのサイズ

バックアップサイズは、プロビジョニングされたストレージ容量の合計ではなく、ファイルシステムの使用済みストレージで決まります。バックアップのサイズは、使用済みのストレージ容量とファイルシステム上のデータチャーンの量に応じて異なります。ファイルシステムの複数のストレージボリュームでのデータの分散方法およびデータ変更の頻度に応じて、バックアップの合計サイズは、使用されているストレージ容量よりも大きくなる場合と小さくなる場合があります。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。

一貫したファイルシステム、高い耐久性、増分であるバックアップを実現するために、Amazon FSx ではブロックレベルでデータをバックアップします。ファイルシステムのストレージボリューム上のデータは、書き込みまたは上書きされたパターンに応じて、複数のブロックに分けて保存される場合があります。その結果、バックアップ使用量の合計が、ファイルシステム上のファイルやディレクトリの厳密なサイズと一致しなくなる可能性があります。全体的なバックアップの使用状況とコストは、 AWS Billing ダッシュボードまたは で確認できます AWS Cost Management Console。

タグを使用して AWS 請求書を整理し、独自のコスト構造を反映します。これを行うには、サインアップしてタグキー値を含む AWS アカウント 請求書を取得します。次に、結合したリソースのコストを見るには、同じタグキー値のリソースに従って請求書情報を整理します。例えば、複数のリソースに特定のアプリケーション名のタグを付け、請求情報を整理することで、複数のサービスを利用しているアプリケーションの合計コストを確認することができます。詳細については、AWS Billing ユーザーガイド の「コスト配分タグの使用」をご参照ください。

> **Note**
>
> ストレージ容量を増やすと、古いストレージディスクのセットから新しい大きなストレージディスクのセットにデータを移行するプロセスにより、古いストレージディスクのセットに関連付けられたバックアップが削除されるまで、バックアップ使用量が一時的に増加する可能性があります。ストレージ容量を増やす前にファイルシステムのストレージが部分的にしか使用されなかった場合、新しいディスクに移行する必要があるデータのサイズは、元のストレージディスクに存在するデータのサイズよりも大きくなる可能性があります。これにより、新しいストレージ容量レベルまでバックアップ使用量が増加する可能性があります。ストレージ容量の増加がバックアップ計画に与える影響を考慮する必要があります。

同じアカウント内のバックアップのコピー

AWS Management Console および を使用して AWS CLI 、次の手順を使用して、同じ AWS アカウント内のバックアップを別の AWS リージョン アカウント (クロスリージョンコピー) または同じアカウント内 AWS リージョン (リージョン内コピー) に手動でコピーできます。

コンソールを使用して、同じアカウント (クロスリージョンまたはインリージョン) 内のバックアップをコピーするには

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、[Backups] (バックアップ) を選択します。
3. [Backups] (バックアップ) テーブルで、コピーするバックアップを選択し、[Copy backup] (バックアップのコピー)を選択します。
4. [Settings] (設定) セクションで、以下の手順を実行します。
   - 送信先リージョンリストで、バックアップをコピーする送信先 AWS リージョンを選択します。送信先は、別の AWS リージョン (クロスリージョンコピー) または同じ AWS リージョン内 (リージョン内コピー) にすることができます。
   - (オプション) [Copy Tags] (タグのコピー) を選択して、出典バックアップから宛先バックアップにタグをコピーします。ステップ 6 で [Copy Tags] (タグのコピー) を選択し、タグを追加すると、すべてのタグがマージされます。
5. 暗号化 では、コピーしたバックアップを暗号化する AWS KMS 暗号化キーを選択します。
6. [Tags - optional] (タグ - オプション) で、キーと値を入力して、コピーしたバックアップにタグを追加します。ここにタグを追加し、またステップ 4 で [Copy Tags] (タグのコピー) を選択すると、すべてのタグがマージされます。
7. [Copy backup] (バックアップのコピー) を選択します。

バックアップは、同じ AWS アカウント内で選択した AWS リージョンにコピーされます。

CLI を使用して同じアカウント内 (クロスリージョンまたはインリージョン) 内でバックアップをコピーするには

- `copy-backup` CLI コマンドまたは CopyBackup API オペレーションを使用して、 AWS リージョン間または AWS リージョン内で、同じ AWS アカウント内のバックアップをコピーします。

次のコマンドは、us-east-1 リージョンからbackup-0abc123456789cba7 の ID でバックアップをコピーします。

```
aws fsx copy-backup \
  --source-backup-id backup-0abc123456789cba7 \
  --source-region us-east-1
```

レスポンスには、コピーされたバックアップの説明が表示されます。

Amazon FSx コンソールまたはプログラムで describe-backups CLI コマンドあるいは DescribeBackups (バックアップの説明) の API オペレーションを使用してバックアップを見ることができます。

新しいファイルシステムへのバックアップの復元

次の手順で説明するように AWS Management Console、、CLI、API を使用してファイルシステムのバックアップを復元して新しいファイルシステムを作成できます。

バックアップからファイルシステムを復元するには

1. https://console.aws.amazon.com/fsx/ で Amazon FSx コンソールを開きます。
2. 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) テーブルから復元するバックアップを選択し、[Restore backup] (バックアップの復元) を選択します。

   これにより、ファイルシステム作成ウィザードが開きます。このウィザードは、スタンダードのファイルシステム作成ウィザードと同じですが、デプロイタイプとストレージ容量は既に設定されており、変更できません。ただし、スループット容量、関連する VPC、その他の設定、およびストレージタイプは変更できます。ストレージタイプは、デフォルトでは SSD に設定されていますが、以下の条件で HDD に変更できます。

   - ファイルシステムのデプロイタイプがマルチ AZ またはシングル AZ 2 です。
   - ストレージ容量は少なくとも 2,000 GiB です。
4. 新しいファイルシステムを作成する場合と同様に、ウィザードを完了します。
5. レビューして作成 を選択します。

6. Amazon FSx ファイルシステムに選択した設定を確認し、ファイルシステムの作成を選択します。

   Amazon FSx は新しいファイルシステムを作成し、ステータスが `AVAILABLE` に変わったら、ファイルシステムを通常どおり使用できます。

シャドウコピーによるデータの保護

Microsoft Windows のシャドウコピーは、ある時点の Windows ファイルシステムのスナップショットです。シャドウコピーを有効にすると、ネットワークに保存されている削除または変更されたファイルをすばやく復元し、ファイルバージョンを比較できます。ストレージの管理者は、Windows PowerShell コマンドを使用して、定期的にシャドウコピーを取得するように、簡単にスケジュールすることができます。

シャドウコピーは、ファイルシステムのデータとともに保存され、ファイルの変更した部分のみのファイルシステムのストレージ容量が消費されます。ファイルシステムに保存されている、すべてのシャドウコピーは、ファイルシステムのバックアップに含まれます。

> **Note**
>
> FSx for Windows ファイルサーバーは、デフォルトではシャドウコピーが有効になっていません。シャドウコピーを使用しているファイルシステム上でデータを保護するには、シャドウコピーを有効にし、ファイルシステムにシャドウコピーのスケジュールを設定する必要があります。詳細については、「デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する」を参照してください。

> **Warning**
>
> シャドウコピーは、バックアップの代用にはなりません。シャドウコピーを有効にする場合は、必ず定期的なバックアップを継続して実行してください。

トピック

- シャドウコピーを使用する際のベストプラクティス
- シャドウコピーのセットアップ
- デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する

- シャドウコピーストレージの最大量の設定
- シャドウコピーストレージを表示する
- カスタムシャドウコピースケジュールを作成する
- シャドウコピースケジュールの表示
- シャドウコピーの作成
- 既存のシャドウコピーの表示
- シャドウコピーの削除
- シャドウコピースケジュールの削除
- シャドウコピーのストレージ、スケジュール、およびすべてのシャドウコピーを削除する
- シャドウコピーのトラブルシューティング

シャドウコピーを使用する際のベストプラクティス

ファイルシステムのシャドウコピーを有効にすると、エンドユーザーは Windows ファイルエクスプローラーで個々のファイルおよびフォルダを以前のスナップショットから表示または復元することができます。Amazon FSx は、Microsoft Windows Server が提供するシャドウコピー機能を利用しています。シャドウコピーには次のベストプラクティスを使用します。

- ファイルシステムに十分なパフォーマンスリソースがあることを確認する: Microsoft Windows では、最新のシャドウコピーポイント以降の変更を記録するためにコピーオンライト方式が使用され、このコピーオンライトアクティビティでは、ファイル書き込み操作ごとに対して最大 3 回の I/O オペレーションが発生する可能性があります。
- SSD ストレージを使用してスループットキャパシティを増やす: Windows ではシャドウコピーを維持するために高レベルの I/O パフォーマンスが必要なため、SSD ストレージを使用し、スループットキャパシティを予想されるワークロードの 3 倍まで増やすことをお勧めします。これにより、ファイルシステムに十分なリソースを確保して、シャドウコピーが不要に削除されるなどの問題を回避できます。
- 必要な数のシャドウコピーのみを維持する: 最新のシャドウコピーが 64 個を超える場合や多くのストレージ (TB スケール) を専有するシャドウコピーが 1 つのファイルシステムにある場合など、大量のシャドウコピーがある場合は、フェイルオーバーやフェイルバックなどの処理に余分な時間がかかる可能性があります。これは、FSx for Windows がシャドウコピーストレージで整合性チェックを実行する必要があるためです。また、FSx for Windows がシャドウコピーを維持しながら書き込み時コピーアクティビティを実行する必要があるため、I/O オペレーションのレイテンシーが長くなる可能性もあります。シャドウコピーによる可用性とパフォーマンスへの影響を最小

限に抑えるには、未使用のシャドウコピーを手動で削除するか、ファイルシステム上の古いシャドウコピーを自動的に削除するようにスクリプトを構成します。

> **Note**
>
> マルチ AZ ファイルシステムのフェイルオーバーイベント中、FSx for Windows は整合性チェックを実行します。この整合性チェックでは、新しいアクティブファイルサーバーがオンラインになる前にファイルシステム上のシャドウコピーストレージのスキャンが必要です。整合性チェックに要する時間は、ファイルシステム上のシャドウコピーの数と消費されるストレージに応じて異なります。フェイルオーバーとフェイルバックの遅延を防ぐために、ファイルシステム上のシャドウコピーの数を 64 未満にし、以下の手順に従って定期的にモニタリングを行って最も古いシャドウコピーを削除することをお勧めします。

シャドウコピーのセットアップ

Amazon FSx で定義された Windows PowerShell コマンドを使用して、ファイルシステム上の定期的なシャドウコピーを有効にし、スケジュールします。FSx for Windows File Server ファイルシステムでシャドウコピーを設定する場合の主な設定を以下に示します。

- シャドウコピーがファイルシステム上で消費できる最大のストレージ量の設定
- (オプション) ファイルシステムに保存できるシャドウコピーの最大数を設定します。デフォルト値は 20 です。
- (オプション) 毎日、毎週、毎月など、時間および間隔を定義してシャドウコピーを取得するスケジュールの設定

ファイルシステムごとに最大 500 のシャドウコピーを保存できますが、可用性とパフォーマンスを確保するために、いつでも 64 未満のシャドウコピーを維持することをお勧めします。この制限に達すると、次に取得したシャドウコピーが、最も以前のシャドウコピーに置き換えられます。同様に、シャドウコピーの最大ストレージ量に達した場合、最も以前のシャドウコピーの1つまたは複数が削除され、次のシャドウコピーのための十分なストレージスペースを確保することができます。

デフォルトの Amazon FSx 設定を使用して定期的なシャドウコピーをすばやく有効にしてスケジュールする方法については、「デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する」を参照してください。

シャドウコピーストレージの割り当てに関する注意事項

シャドウコピーは、前回のシャドウコピー以降に行われたファイル変更をブロックレベルでコピーしたものです。ファイル全体がコピーされず、変更箇所のみがコピーされます。したがって、以前のバージョンのファイルは、通常、現在のファイルほど多くのストレージスペースを占有しません。変更に使用されるボリュームスペースの量は、ワークロードに応じて異なります。ファイルが変更された場合、シャドウコピーが使用するストレージスペースは、ワークロードによって異なります。シャドウコピーに割り当てるストレージ容量を決定する際は、ワークロードのファイルシステムの使用パターンを考慮する必要があります。

シャドウコピーを有効にすると、シャドウコピーがファイルシステム上で消費できる最大容量のストレージ量を指定することができます。デフォルトの制限はファイルシステムの 10% です。ユーザーが頻繁にファイルの追加または変更する場合は、制限値を増やすことをお勧めします。制限値を小さく設定しすぎると、最も古いシャドウコピーがユーザーの予想以上に頻繁に削除されることになります。

シャドウコピーストレージを無制限に設定できます (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`)。ただし、無制限の設定では、多数のシャドウコピーがファイルシステムストレージを消費する可能性があります。その結果、ワークロードに対して十分なストレージ容量が確保できなくなる可能性があります。無制限のストレージを設定する場合は、シャドウコピーの制限に達したときにストレージ容量を必ずスケールするようにしてください。シャドウコピーストレージを特定のサイズまたは無制限として設定する方法については、シャドウコピーストレージの最大量の設定 を参照してください。

シャドウコピーを有効にした後、シャドウコピーが消費するストレージスペースの量をモニタリングすることができます。詳細については、「シャドウコピーストレージを表示する」を参照してください。

シャドウコピーの最大数を設定する際の考慮事項

シャドウコピーを有効にすると、ファイルシステム上で保存されるシャドウコピーの最大容量を指定することができます。デフォルトの制限は 20 で、シャドウコピーによる可用性とパフォーマンスへの影響を最小限に抑えるために、Microsoft はシャドウコピーの最大数を 64 未満に設定することをお勧めします。Windows ではシャドウコピーを維持するために高レベルの I/O パフォーマンスが必要なため、SSD ストレージを使用し、スループットキャパシティを予想されるワークロードの 3 倍まで増やすことをお勧めします。これにより、ファイルシステムに十分なリソースを確保して、シャドウコピーが不要に削除されるなどの問題を回避できます。

最大 500 のシャドウコピーを設定できます。ただし、1 つのファイルシステムで大量のストレージ (TB スケール) を占める多数のシャドウコピーまたはシャドウコピーがある場合、フェイルオーバーやフェイルバックなどのプロセスに予想以上に時間がかかることがあります。これは、Windows がシャドウコピーストレージで整合性チェックを実行する必要があるためです。また、Windows がシャドウコピーを維持しながら書き込み時コピーアクティビティを実行する必要があるため、I/O オペレーションのレイテンシーが長くなる可能性もあります。

シャドウコピーに関するファイルシステムのレコメンデーション

シャドウコピーの使用に関するファイルシステムのレコメンデーションを以下に示します。

- ワークロードのニーズに合わせて、ファイルシステム上に十分なパフォーマンス容量プロビジョンを提供していることを確認します。Amazon FSx は、Microsoft Windows Server によって与えられたシャドウコピー機能を提供します。設計上、Microsoft Windows では、最新のシャドウコピーポイント以降の変更を記録するためにコピーオンライト方式が使用され、このコピーオンライトアクティビティでは、ファイル書き込み操作ごとに対して最大 3 つの I/O 入出力オペレーションが発生する可能性があります。Windows が 1 秒間に入力される I/O オペレーションの速度に対応できない場合、書き込み時コピーを介してシャドウコピーを維持することができなくなるため、すべてのシャドウコピーが削除される可能性があります。したがって、ファイルシステムのワークロードのニーズに十分な I/O パフォーマンス容量をプロビジョニングすることが重要です (ファイルサーバーの I/O パフォーマンスを決定するスループット容量のディメンションと、ストレージ I/O パフォーマンス を決定するストレージタイプと容量の両方)。
- シャドウコピーを有効にする場合は、通常、シャドウコピーを維持するために Windows の方が高い入出力 I/O パフォーマンスを消費することと、HDD ストレージが入出力操作の I/O パフォーマンス容量が低いことを考慮して、HDD ストレージではなく SSD ストレージで設定されたファイルシステムを使用することをお勧めします。
- ファイルシステムには、設定されているシャドウコピーストレージ量の最大容量に加えて、少なくとも 320 MB の空き容量が必要です (`MaxSpace`)。例えば、シャドウコピーに 5 GB の `MaxSpace` を割り当てた場合、ファイルシステムには、5GB の `MaxSpace` に加えて常に少なくとも 320 MB の空き領域が必要です。

> **Warning**
>
> シャドウコピーのスケジュールを設定する際は、データの移行時またはデータ重複排除ジョブの実行がスケジュールされているときに、シャドウコピーをスケジュールしないようにしてください。ファイルシステムが動作停止状態になることを想定される場合は、シャドウコ

ピーをスケジュールする必要があります。カスタムシャドウコピースケジュールの設定については、「カスタムシャドウコピースケジュールを作成する」を参照してください。

個々のファイルとフォルダの復元

Amazon FSx ファイルシステムにシャドウコピーを設定すると、ユーザーは個々のファイルやフォルダの以前のバージョンをすばやく復元し、削除したフィアルを復旧することができます。

ユーザーは、使い慣れた Windows のファイルエクスプローラーの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します。ファイルを復元するには、復元するファイルを選択し、以前のバージョンの復元 コンテキスト (右クリック) メニューから選択します。

これにより、ユーザーは以前のバージョンリストより以前のバージョンを表示および復元することができます。

デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する

シャドウコピーのストレージ設定とスケジュールにデフォルトを使用することで、ファイルシステム上にシャドウコピーをすばやく設定することができます。シャドウコピーストレージのデフォルト設定では、シャドウコピーがファイルシステムストレージ容量の最大 10% を消費するようになっています。ファイルシステムのストレージ容量を増やすと、現在割り当てられているシャドウコピーストレージ容量は同様に増加しません。

デフォルトのスケジュールでは、毎週月曜日、火曜日、水曜日、木曜日、金曜日の午前 7:00 および午後 12:00 (UTC) に自動的にシャドウコピーが取得できます。

シャドウコピーストレージスペースのデフォルトレベルを設定するには

1. ファイルシステムとのネットワーク接続が可能な Windows コンピューティングインスタンスに接続します。
2. ファイルシステム管理者グループのメンバーとして Windows コンピューティングインスタンスにログインします。では AWS Managed Microsoft AD、そのグループはAWS 委任 FSx 管理者です。セルフマネージド Microsoft AD では、そのグループは ドメイン管理者、またはファイルシステムの作成時に管理用に指定したカスタムグループです。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。
3. 次のコマンドを使用して、シャドウストレージのデフォルトの量を設定します。*FSxFileSystem-Remote-PowerShell-Endpoint* を、管理するファイルシステムの Windows Remote PowerShell エンドポイントに置き換えます。Windows Remote PowerShell エンドポイントは、Amazon FSx コンソールのファイルシステムの詳細画面のネットワークおよびセキュリティセクション、または `DescribeFileSystem` API オペレーションのレスポンスの中で見つけることができます。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowStorage -Default}
```

レスポンスは以下のようになります。

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 10737418240                  20
```

デフォルトのシャドウコピーのスケジュールを設定するには

1. ファイルシステムとのネットワーク接続が可能な Windows コンピューティングインスタンスに接続します。
2. ファイルシステム管理者グループのメンバーとして Windows コンピューティングインスタンスにログインします。では AWS Managed Microsoft AD、そのグループはAWS 委任 FSx 管理者です。セルフマネージド Microsoft AD では、そのグループは ドメイン管理者、またはファイルシステムの作成時に管理用に指定したカスタムグループです。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。

3. 次のコマンドを使用して、デフォルトのシャドウコピーにスケジュールを設定します。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowCopySchedule -Default}
```

レスポンスには、現在設定されているデフォルトのスケジュールが表示されます。

```
FSx Shadow Copy Schedule

Start Time                Days of week                            WeeksInterval
----------                ------------                            -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday            1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday            1
```

追加のオプションとカスタムシャドウコピースケジュールの作成については、「カスタムシャドウコピースケジュールを作成する」を参照してください。

シャドウコピーストレージの最大量の設定

Set-FsxShadowStorage カスタム PowerShell コマンドを使用してシャドウコピーが消費できるストレージの最大容量を定義します。-Maxsize パラメータまたは -Default パラメータのいずれかを使用することにより、シャドウコピーが拡大できる最大サイズを指定できます。Default を使用すると、ファイルシステムのストレージ容量の最大値が 10% に設定されます。同じコマンド内で、-Maxsize パラメータと -Default パラメータを指定することはできません。

-Maxsize を使用して、シャドウコピーストレージを次のように定義できます。

- バイト単位: Set-FsxShadowStorage -Maxsize 2500000000
- キロバイト、メガバイト、ギガバイト、またはその他の単位: Set-FsxShadowStorage -Maxsize (2500MB) または Set-FsxShadowStorage -Maxsize (2.5GB)
- ストレージ全体のパーセンテージ: Set-FsxShadowStorage -Maxsize "20%"
- 無制限: Set-FsxShadowStorage -Maxsize "UNBOUNDED"

-Default を使用して、シャドウストレージがファイルシステムを最大 10% まで使用できるように設定します: Set-FsxShadowStorage -Default。デフォルトオプションの使用に関する詳細につ

いては、「デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する」を参照してください。

FSx for Windows ファイルサーバーのファイルシステムにシャドウコピーストレージ容量を設定するには

1. 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、ファイルシステムとのネットワーク接続があるコンピューティングインスタンスに接続します。では AWS Managed Microsoft AD、そのグループはAWS 委任 FSx 管理者です。セルフマネージド Microsoft AD では、そのグループは ドメイン管理者、またはファイルシステムの作成時に管理用に指定したカスタムグループです。詳細については、「Amazon EC2 ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。
2. コンピューティングインスタンスで Windows PowerShell ウィンドウを開きます。
3. 次のコマンドを使用して、Amazon FSx ファイルシステム上でリモート PowerShell セッションを開きます。*FSxFileSystem-Remote-PowerShell-Endpoint* を、管理したいファイルシステムの Windows Remote PowerShell エンドポイントに置き換えます。ファイルシステムの詳細画面の [Network & Security] (ネットワークとセキュリティ) セクション、または `DescribeFileSystem` API オペレーションのレスポンスに、Amazon FSx コンソールの Windows リモート PowerShell エンドポイントを見つけることができます。

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 次のコマンドを使用して、ファイルシステム上にシャドウコピーストレージが設定されていないことを確認します。

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
No Fsx Shadow Storage Configured
```

5. `-Default` オプションを使用して、シャドウストレージの量をボリュームの 10% に、シャドウコピーの最大数を 20 に設定します。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 32530536858                  20
```

-MaxShadowCopyNumber パラメータで Set-FSxShadowStorage コマンドを使用し、1 ~ 500 の値を指定することで、ファイルシステムで許可されるシャドウコピーの最大数を制限できます。デフォルトでは、Microsoft がアクティブなワークロードに推奨しているように、シャドウコピーの最大数は 20 に設定されています。

シャドウコピーストレージを表示する

ファイルシステム上のリモート PowerShell セッションで Get-FsxShadowStorage コマンドを使用して、ファイルシステム上のシャドウコピーによって現在使用されているストレージの量を表示できます。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 10737418240                  20
```

出力には、シャドウストレージの設定が次のように表示されます。

- AllocatedSpace - シャドウコピーに現在割り当てられているファイルシステム上のストレージ容量 (バイト単位)。初期状態では、この値は 0 です。
- UsedSpace - シャドウコピーで現在使用されているストレージ容量 (バイト単位)。初期状態では、この値は 0 です。
- MaxSpace - シャドウストレージを拡張できるストレージの最大容量 (バイト単位)。これは、Set-FsxShadowStorage コマンドを使用して シャドウコピーストレージ に設定した値です。
- MaxShadowCopyNumber – ファイルシステムが保持できるシャドウコピーの最大数は 1 ~ 500 です。

UsedSpace 金額が設定された最大シャドウコピーストレージ量 (MaxSpace) に達するか、シャドウコピー数が設定された最大シャドウコピー数 (MaxShadowCopyNumber) に達すると、次に作成するシャドウコピーは最も古いシャドウコピーと置き換えられます。最も古いシャドウコピーを失いたくない場合は、シャドウコピーのストレージをモニタリングして、新しいシャドウコピー用の十分なストレージスペースがあることを確認してください。スペースを増やす必要がある場合は、既存のシャドウコピーを削除、または シャドウコピーストレージ の最大量を増やすことができます。

> **Note**
>
> シャドウコピーが自動または手動で作成される場合、それらは、ストレージ制限として設定したシャドウコピーストレージの量を使用します。シャドウコピーは時間の経過とともにサイズが大きくなり、CloudWatch `FreeStorageCapacity` メトリクスで表示される使用可能なストレージスペースを、設定された最大シャドウコピーストレージ量 (`MaxSpace`) まで活用します。

カスタムシャドウコピースケジュールを作成する

シャドウコピースケジュールでは、Microsoft Windows のスケジュールされたタスクトリガーを使用して、シャドウコピーが自動的に作成されるタイミングを指定します。シャドウコピースケジュールには複数のトリガーを設定できるため、スケジューリングの柔軟性が大幅に向上します。一度に存在できるシャドウコピースケジュールは 1 つだけです。シャドウコピースケジュールを作成する前に、まず シャドウコピーストレージ の容量を設定する必要があります。

ファイルシステムで `Set-FsxShadowCopySchedule` コマンドを実行すると、既存のシャドウコピースケジュールが上書きされます。クライアントコンピューターが UTC タイムゾーンにある場合は、Windows タイムゾーンと `-TimezoneId` オプションを使用して、トリガーのためのタイムゾーンを指定することもできます。Windows のタイムゾーンのリストについては、Microsoft の デフォルトのタイムゾーン のドキュメントを参照するか、Windows のコマンドプロンプトで次のコマンドを実行してください。`tzutil /l`。Windows タスクトリガーの詳細については、「Microsoft Windows Developer Center ドキュメント」の「タスクトリガー」を参照してください。

また、`-Default` オプションを使用して、デフォルトのシャドウコピースケジュールを迅速に設定することもできます。詳細については、「デフォルトのストレージとスケジュールを使用するようにシャドウコピーを設定する」を参照してください。

カスタムシャドウコピースケジュールを作成するには

1. シャドウコピーがシャドウコピースケジュールで作成される時期を定義する、一連の Windows スケジュールタスクトリガーを作成します。ローカルマシンの PowerShell で `new-scheduledTaskTrigger` コマンドを使用して、複数のトリガーを設定します。

   次の例では、毎週月曜日から金曜日の午前 6 時と午後 6 時 (UTC) にシャドウコピーを作成するカスタムシャドウコピースケジュールを作成します。デフォルトでは、作成した Windows のスケジュールタスクトリガーでタイムゾーンを指定しない限り、時刻は UTC で表されます。

```
PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. `invoke-command` を使用して `scriptblock` コマンドを実行します。実行すると、先ほど作成した `new-scheduledTaskTrigger` でシャドウコピースケジュールを設定するスクリプティングが書き込まれます。*`FSxFileSystem-Remote-PowerShell-Endpoint`* を、管理したいファイルシステムの Windows Remote PowerShell エンドポイントに置き換えます。ファイルシステムの詳細画面の [Network & Security] (ネットワークとセキュリティ) セクション、または `DescribeFileSystem` API オペレーションのレスポンスに、Amazon FSx コンソールの Windows リモート PowerShell エンドポイントを見つけることができます。

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. >> プロンプトで次の行を入力し、`set-fsxshadowcopyschedule` コマンドを使用してシャドウコピースケジュールを設定します。

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

レスポンスには、ファイルシステム上で設定したシャドウコピースケジュールが表示されます。

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

シャドウコピースケジュールの表示

ファイルシステム上の既存のシャドウコピースケジュールを表示するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                            WeeksInterval
----------                ------------                            -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

シャドウコピーの作成

シャドウコピーを手動で作成するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

既存のシャドウコピーの表示

ファイルシステム上で一連の既存のシャドウコピーを表示するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                        Creation Time
--------------                        -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

シャドウコピーの削除

ファイルシステム上のリモート PowerShell セッションでコマンドで `Remove-FsxShadowCopies` を使用して、ファイルシステム上の既存のシャドウコピーを削除できます。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

以下のいずれかの必須オプションを使用して、削除するシャドウコピーを指定します。

- `-Oldest` は最も古いシャドウコピーを削除します
- `-All` は既存のシャドウコピーをすべて削除します
- `-ShadowCopyId` は ID で特定のシャドウコピーを削除します

また、1 つのオプションのみでコマンドを使用することができます。削除するシャドウコピーを指定しない場合、複数のシャドウコピー ID を指定する場合、または無効なシャドウコピー ID を指定する場合は、エラーが発生します。

ファイルシステム上の最も古いシャドウコピーを削除するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

ファイルシステム上の特定のシャドウコピーを削除するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

ファイルシステム上の最も古いシャドウコピーを一定数削除するには、-MaxShadowCopyNumber パラメータを残したいシャドウコピーの必要数に更新します。ただし、この変更は、次のシャドウコピースナップショットが作成されてから、システムが自動的に余分なシャドウコピーを削除する場合にのみ有効になります。ファイルシステム上のリモート PowerShell セッションで次のコマンドを使用します。

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

シャドウコピースケジュールの削除

ファイルシステム上の既存のシャドウコピースケジュールを削除するには、ファイルシステムのリモート PowerShell セッションで次のコマンドを入力します。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
```

```
[fs-0123456789abcdef1]PS>
```

シャドウコピーのストレージ、スケジュール、およびすべてのシャドウコピーを削除する

既存のすべてのシャドウコピーとシャドウコピーのスケジュールを含むシャドウコピー設定を削除できます。同時に、ファイルシステム上のシャドウコピーストレージを解放できます。

これを行うには、ファイルシステム上のリモート PowerShell セッションで `Remove-FsxShadowStorage` コマンドを入力します。ファイルシステム上でリモート PowerShell セッションを起動する手順については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

シャドウコピーのトラブルシューティング

次のセクションで説明するように、シャドウコピーが欠落している場合やアクセスできない場合には、いくつかの考えられる原因があります。

トピック

- 最も古いシャドウコピーが欠落している
- すべてのシャドウコピーが欠落している
- 最近復元または更新されたファイルシステムで Amazon FSx バックアップを作成したり、シャドウコピーにアクセスしたりすることはできません

最も古いシャドウコピーが欠落している

最も古いシャドウコピーは、次のいずれかの状況で削除されます。

- 500 個のシャドウコピーがある場合、シャドウコピーに割り当てられている残りのストレージボリュームスペースに関係なく、次のシャドウコピーが最も古いシャドウコピーを置き換えます。
- 設定されているシャドウコピーの最大ストレージ量に達すると、シャドウコピーが 500 未満であっても、次のシャドウコピーが 1 つ以上の最も古いシャドウコピーを置き換えます。

どちらの結果も予想される動作です。シャドウコピーに割り当てられたストレージが不十分な場合は、割り当てたストレージを増やすことを検討してください。

すべてのシャドウコピーが欠落している

ファイルシステムの I/O パフォーマンス容量が不十分な場合 (例えば、HDD ストレージを使用している HDD ストレージのバースト容量が不足している、またはスループットキャパシティが不十分であるなどの理由で)、使用可能な I/O パフォーマンス容量でシャドウコピーを維持できないため、Windows サーバーによってすべてのシャドウコピーが削除される可能性があります。この問題を防ぐために、次のレコメンデーションを検討してください。

- HDD ストレージを使用している場合は、Amazon FSx コンソールまたは Amazon FSx API を使用して SSD ストレージの使用に切り替えます。詳細については、「ファイルシステムのストレージタイプの管理」を参照してください。
- ファイルシステムのスループットキャパシティを、予想されるワークロードの 3 倍の値に増やします。
- 設定されているシャドウコピーの最大ストレージ容量に加えて、ファイルシステムに少なくとも 320 MB の空き容量があることを確認してください。
- ファイルシステムがアイドル状態になると予想される場合は、シャドウコピーをスケジュールします。

詳細については、「シャドウコピーに関するファイルシステムのレコメンデーション」を参照してください。

最近復元または更新されたファイルシステムで Amazon FSx バックアップを作成したり、シャドウコピーにアクセスしたりすることはできません

これは想定される動作です。Amazon FSx は、最近復元されたファイルシステムでシャドウコピー状態を再構築し、再構築が進行中にシャドウコピーまたはバックアップへのアクセスを許可しません。

を使用したスケジュールされたレプリケーション AWS DataSync

AWS DataSync を使用して、FSx for Windows File Server ファイルシステムの 2 番目のファイルシステムへ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。詳細については、このガイドAWS DataSyncを使用して、既存のファイルを FSx for Windows File Server に移行するの「」および「 ユーザーガイド」のAWS 「ストレージサービス間のデータ転送」を参照してください。 AWS DataSync

FSx for Microsoft SQL Server で FSx for Windows File Server の使用

高可用性 (HA) Microsoft SQL Server は通常、Windows Server フェイルオーバークラスター (WSFC) 内の複数のデータベースノードにデプロイされ、各ノードは共有ファイルストレージにアクセスできます。FSx for Windows File Server は、高可用性 (HA) Microsoft SQL Server デプロイの共有ストレージとして、アクティブデータファイルのストレージとして、および SMB ファイル共有監視として使用できます。

> **Note**
>
> 現在、Amazon FSx は Microsoft SQL Server の IFI (インスタントファイル初期化) 機能をサポートしていません。

SQL Server には、SSD ストレージの使用をお勧めします。SSD ストレージは、データベースなど、最高のパフォーマンスでレイテンシーの影響を受けやすいワークロード向けに設計されています。

Amazon FSx を使用して、SQL Server の高可用性デプロイの複雑さとコストを削減する方法については、次のAWS ストレージブログの投稿を参照してください。

- 「Amazon FSx for Windows File Server を使用して、Microsoft SQL Server の高可用性デプロイメントを簡素化する」
- での高可用性 SQL Server デプロイのコストの最適化 AWS
- AWS Launch Wizard と Amazon FSx を使用して SQL Server Always On デプロイを簡素化する

アクティブ SQL Server データファイルに Amazon FSx を使用する

Microsoft SQL Server は、アクティブデータファイルのストレージオプションとして SMB ファイル共有を使用してデプロイできます。Amazon FSx は、継続的に利用可能な (CA) ファイル共有をサポートすることにより、SQL Server データベースの共有ストレージを提供するように最適化されています。これらのファイル共有は、SQL Server などの共有ファイルデータへの中断されないアクセスを必要とするアプリケーション向けに設計されています。シングル AZ 2 ファイルシステムで CA

共有を作成できますが、HA の有無にかかわらず、すべての SQL Server デプロイには CA 共有をマルチ AZ ファイルシステムで使用する必要があります。

継続的に利用可能な共有を作成する

PowerShell のリモート管理用の Amazon FSx CLI を使用して CA 共有を作成できます。継続して利用可能な共有を指定するには、`-ContinuouslyAvailable` オプションを `$True` に設定した状態で `New-FSxSmbShare` を使用します。詳細については、「継続的に利用可能な (CA) 共有を作成するには」を参照してください。

SMB のタイムアウト設定を構成する

フェイルオーバープロセス で説明したように、マルチ AZ のフェイルオーバーとフェイルバックによって、通常 30 秒未満で完了する I/O の一時停止が発生することがあります。SQL Server アプリケーションは、構成によってタイムアウト設定に対する感度が異なる場合があります。

SMB クライアント構成のセッションのタイムアウトを調整して、アプリケーションにマルチ AZ ファイルシステムのフェイルオーバーに対する回復力を持たせることができます。ファイルシステムのスループット容量を更新することで、フェイルオーバー時にアプリケーションの動作をテストできます。これにより、自動フェイルオーバーとフェイルバックが開始されます。

Amazon FSx を SMB ファイル共有監視として使用する

Windows Server フェイルオーバークラスターデプロイでは通常、クラスターのリソースの定足数を維持するために、SMB ファイル共有監視をデプロイします。ファイル共有監視は、定足数情報に少量のストレージしか必要としません。Amazon FSx ファイルシステムは、Windows Server フェイルオーバークラスターデプロイの SMB ファイル共有監視として使用できます。

既存のファイルストレージを Amazon FSx に移行する

Amazon FSx for Windows File Server は、エンタープライズアプリケーションを簡単に Amazon ウェブサービスクラウドにリフトアンドシフトするための機能、パフォーマンス、および互換性を備えています。オンプレミスの Microsoft Windows File Server ストレージを FSx for Windows File Server に移行するプロセスには、次の 4 つの主要なステップがあります。

1. FSx for Windows File Server にファイルを移行します。詳細については、「FSx for Windows File Server に既存のファイルストレージを移行する」を参照してください。
2. ファイル共有設定を FSx for Windows File Server に移行します。詳細については、「オンプレミスのファイル共有設定を Amazon FSx に移行する」を参照してください。
3. 既存の DNS 名を Amazon FSx ファイルシステムの DNS エイリアスとして関連付けます。詳細については、「DNS エイリアスを Amazon FSx に関連付ける」をご覧ください。
4. FSx for Windows File Server にカットオーバーします。詳細については、「Amazon FSx for Windows File Server へのオペレーションのカットオーバー」を参照してください。

次のセクションで、プロセスの各ステップの詳細を確認できます。

トピック

- FSx for Windows File Server に既存のファイルストレージを移行する
- オンプレミスのファイル共有設定を Amazon FSx に移行する
- オンプレミス DNS 設定の FSx for Windows File Server への移行
- Amazon FSx for Windows File Server へのオペレーションのカットオーバー

FSx for Windows File Server に既存のファイルストレージを移行する

既存のファイルを FSx for Windows File Server ファイルシステムに移行するには、 AWS ストレージサービスとの間で大量のデータのコピーを簡素化、自動化、高速化するように設計された AWS DataSyncオンラインデータ転送サービスである を使用することをお勧めします。DataSync はインターネットまたは AWS Direct Connect経由でデータをコピーします。フルマネージドサービスの DataSync は、アプリケーションの変更、スクリプティングの開発、インフラストラクチャの管理の必要性の大部分を排除します。詳細については、「AWS DataSyncを使用して、既存のファイルを FSx for Windows File Server に移行する」を参照してください。

別のソリューションとして、Robust File Copy、または Microsoft Windows 用のコマンドラインディレクトリおよびファイルレプリケーションコマンドセットである Robocopy を使用できます。Robocopy を使用してファイルストレージを FSx for Windows File Server に移行する方法の詳細な手順については、「Robocopy を使用して、既存のファイルを FSx for Windows File Server に移行する」を参照してください。

既存のファイルストレージを FSx for Windows File Server に移行するためのベストプラクティス

大量のデータを FSx for Windows File Server にできるだけ早く移行するには、ソリッドステートドライブ (SSD) ストレージで設定された Amazon FSx ファイルシステムを使用します。移行が完了したら、ハードディスクドライブ (HDD) ストレージを使用してデータを Amazon FSx ファイルシステムに移動できます (ユーザーのアプリケーションにとってこれが最良のソリューションの場合)。

SDD ストレージを使用して Amazon FSx ファイルシステムから HDD ストレージにデータを移動するために、次の操作を行うことができます。(HDD ファイルシステムには最低でも 2 TB のストレージ容量があり、バックアップから復元するときはストレージ容量を変更できないことに注意してください。)

1. SSD ファイルシステムのバックアップを作成します。詳細については、「ユーザーによるバックアップの作成」を参照してください。
2. HDD ストレージを使用して、バックアップをファイルシステムに復元します。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。

AWS DataSyncを使用して、既存のファイルを FSx for Windows File Server に移行する

AWS DataSync を使用して FSx for Windows File Server ファイルシステム間でデータを転送することをお勧めします。DataSync は、インターネットまたは を介したオンプレミスストレージシステムと他の AWS ストレージサービス間のデータの移動とレプリケーションを簡素化、自動化、および高速化するデータ転送サービスです AWS Direct Connect。DataSync は、所有権、タイムスタンプ、アクセス許可などのファイルシステムデータおよびメタデータを転送できます。

DataSync は、NTFS アクセスコントロールリスト (ACL) のコピーをサポートしており、ファイル監査コントロール情報のコピーもサポートしています。これは、NTFS システムアクセスコントロールリスト (SACL) とも呼ばれ、管理者がファイルにアクセスしようとするユーザーの監査ログをコントロールするために使用されます。

DataSync を使用して、2 つの FSx for Windows File Server ファイルシステム間でファイルを転送したり、別の AWS リージョン または AWS アカウントのファイルシステムにデータを移動したりできます。他のタスクのために DataSync を FSx for Windows File Server 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。

では AWS DataSync、FSx for Windows File Server の場所は FSx for Windows File Server のエンドポイントです。FSx for Windows File Server のロケーションと他のファイルシステムのロケーションとの間でファイルを転送できます。詳細については、「AWS DataSync ユーザーガイド」の「ロケーションの使用」を参照してください。

DataSync は、サーバーメッセージブロック (SMB) プロトコルを使用して FSx for Windows File Server にアクセスします。 AWS DataSync コンソールまたは で設定したユーザー名とパスワードで認証されます AWS CLI。

前提条件

Amazon FSx for Windows File Server の設定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。

大規模なデータ移行、または多数の小さなファイルを含む移行を行う場合は、SSD ストレージタイプの Amazon FSx ファイルシステムを使用することをお勧めします。これは、DataSync タスクにはファイルメタデータのスキャンが含まれるため、HDD ファイルシステムのディスク IOPS 制限が使い果たされ、移行に時間がかかり、ファイルシステムのパフォーマンスに影響が及ぶ可能性があるからです。詳細については、「既存のファイルストレージを FSx for Windows File Server に移行するためのベストプラクティス」を参照してください。

データセットのほとんどが小さなファイルで構成されていたり、ファイル数が数百万に上る場合や、1 つの DataSync タスクよりも利用可能なネットワーク帯域幅が消費量よりも多い場合は、スケールアウトアーキテクチャを使用してデータ転送を高速化することもできます。詳細については、AWS DataSync 「スケールアウトアーキテクチャを使用してデータ転送を高速化する方法」を参照してください。

FSx パフォーマンスメトリクスを使用して、ファイルシステムのディスク I/O 使用状況をモニタリングできます。

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、出典の場所から転送先の場所にファイルを転送するには、次のベーシックな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。
- ソースと宛先の場所を作成して設定します。
- タスクを作成し、設定します。
- 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。

既存のオンプレミスファイルシステムから FSx for Windows File Server にファイルを転送する方法については、 AWS DataSync ユーザーガイドの「セルフマネージドストレージと 間のデータ転送 AWS」、「SMB の場所の作成」、および「Amazon FSx for Windows File Server の場所の作成」を参照してください。

既存のクラウド内ファイルシステムから FSx for Windows File Server にファイルを転送する方法については、「AWS DataSync ユーザーガイド」の「Deploy your agent as an Amazon EC2 instance」(Amazon EC2 インスタンスとしてエージェントをデプロイする) を参照してください。

2 つの Amazon FSx ファイルシステム間の移行

DataSync を使用して、2 つの Amazon FSx ファイルシステム間でデータを移行できます。これは、既存のファイルシステムから、シングル AZ 設定からマルチ AZ 設定など、異なる設定の新しいファイルシステムにワークロードを移動する必要がある場合に役立ちます。DataSync を使用して、2 つのファイルシステム間でワークロードを分割することもできます。

移行プロセスの概要の例を次に示します。

1. ソースとターゲットのファイルシステムの DataSync の場所を作成します。ソースとターゲットの両方が同じ Active Directory ドメインに属しているか、ドメイン間の AD 信頼関係を持っている必要があることに注意してください。
2. ソースからターゲットにデータを転送する DataSync タスクを作成および設定します。1 回限りのインスタンスとしてタスクを実行することも、設定したスケジュールに従って自動的に実行するようにタスクを設定することもできます。
3. タスクが正常に完了すると、ターゲットファイルシステムのデータはソースの正確なコピーになります。タスクを完了するには、ソースファイルシステム上の書き込みアクティビティまたはファイル更新を一時的に停止する必要があることに注意してください。その後、ターゲットファイルシステムにカットオーバーし、ソースファイルシステムを削除できます。

本番稼働用環境のファイルシステムから移行する前に、最新のバックアップから復元されたファイルシステムで移行プロセスをテストできます。これにより、データ転送処理にかかる時間を見積もり、DataSync エラーを事前にトラブルシューティングできます。

カットオーバー時間を最小限に抑えるために、DataSync タスクを事前に実行して、データの大部分をソースファイルシステムからターゲットファイルシステムに移行できます。ソースファイルシステムへのトラフィックを停止したら、最後のタスク転送を実行して、トラフィックを停止した後に新しく更新されたデータを同期し、ターゲットファイルシステムにカットオーバーできます。

DataSync タスクは、特定のディレクトリでのみ実行するように設定できるほか、特定のパスを含めたり除外したりするように設定することもできます。これは、複数のタスクを並列実行している場合や、データのサブセットを移行する場合に便利です。

ソースファイルシステムの DNS 名と同じ DNS エイリアスをターゲットファイルシステムに作成できます。これにより、エンドユーザーとアプリケーションは、ソースファイルシステムの DNS 名を使用してファイルデータに引き続きアクセスできます。DNS エイリアスの設定方法の詳細については、「DNS エイリアスを使用したデータへのアクセス」を参照してください。

このタイプの移行を実行する場合、次のことをお勧めします。

- ファイルシステムのバックアップ、毎週のメンテナンスウィンドウ、および `Data Deduplication` ジョブを回避するように移行をスケジュールします。具体的には、計画された移行と一致する場合は、`Data Deduplication GarbageCollection` ジョブを無効にすることをお勧めします。
- ソースとターゲットのファイルシステムの両方に SSD ストレージタイプを使用します。バックアップから復元することで、HDD と SSD のストレージタイプを切り替えることができます。詳細については、「FSx for Windows File Server に既存のファイルストレージを移行する」を参照してください。
- 転送する必要のあるデータ量のために十分なスループットキャパシティがあるように、ソースとターゲットのファイルシステムを設定します。DataSync タスクのプロセス中、ソースファイルシステムとターゲットファイルシステムの両方のパフォーマンスの使用状況をモニタリングします。詳細については、「Amazon CloudWatch によるモニターリング」を参照してください。
- 進行中のタスクの進行状況を把握できるように、DataSync モニタリングを設定します。エラーが発生した場合にタスクのデバッグに役立てるために、DataSync ログを Amazon CloudWatch Logs グループに送信することもできます。

Robocopy を使用して、既存のファイルを FSx for Windows File Server に移行する

Microsoft Windows サーバー上に構築された Amazon FSx for Windows File Server では、既存のデータセットを Amazon FSx ファイルシステムに完全に移行できます。各ファイルのデータを移行できます。属性、タイムスタンプ、アクセスコントロールリスト (ACL)、所有者情報、監査情報など、関連するすべてのファイルメタデータを移行することもできます。この移行のトータルサポートにより、Amazon FSx では、これらのファイルデータセットに依存する Windows ベースのワークロードとアプリケーションを Amazon ウェブサービスクラウドに移動できます。

既存のファイルデータをコピーするプロセスのガイドとして、次のトピックを使用します。このコピーを実行すると、オンプレミスのデータセンターまたは Amazon EC2 のセルフマネージドファイルサーバーのすべてのファイルメタデータが保持されます。

Robocopy を使用したファイル移行の前提条件

始める前に、次のことを確認してください。

- オンプレミスの Active Directory と Amazon FSx ファイルシステムを作成する VPC 間のネットワーク接続を確立します (AWS Direct Connect または VPN を使用) 。
- コンピュータをドメインを結合させるための委任されたアクセス許可を使用して、アクティブディレクトリにサービスアカウントを作成します。詳細については、「AWS Directory Service 管理ガイド」の「サービスアカウントへの特権の委任」を参照してください。
- Amazon FSx ファイルシステムを作成し、セルフマネージド (オンプレミス) Microsoft AD ディレクトリに結合します。
- Amazon FSx に転送する既存の`\\Source\Share`ファイルが含まれているファイル共有の場所 (オンプレミスまたは 内 AWS) を書き留めます。
- 既存のファイルを転送したい Amazon FSx ファイルシステム上のファイル共有の場所を、書き留めます (例えば `\\Target\Share`)。

次の表は、3 つの移行ユーザーアクセスモデルに関する出典および宛先ファイルシステムのアクセシビリティ要件をまとめたものです。

移行ユーザーアクセスモデル	出典ファイルシステムのアクセシビリティ要件	宛先 FSx ファイルサーバーのアクセシビリティ要件
直接読み取り / 書き込みするアクセス許可モデル	ユーザーは少なくとも、移行するファイルおよびフォルダに対する読み取り許可 (NTFS ACL) を持っている必要があります。	ユーザーは少なくとも、移行するファイルとフォルダに対する少なくとも書き込み許可 (NTFS ACL) を持っている必要があります。
アクセス許可を上書きするためのバックアップ/復元特権モデル	ユーザーは、オンプレミスのアクティブディレクトリのバックアップオペレータグループのメンバーで、RoboCopy で /b フラグを使用する必要があります。	ユーザーは、Amazon FSx ファイルシステムの 管理者グループ* のメンバーである必要があり、Robo Copy で /b フラグを使用する必要があります。
アクセス許可を上書きするドメイン管理者 (フル) 特権モデル	ユーザーは、オンプレミスのアクティブディレクトリのドメイン管理者グループのメンバーである必要があります。	ユーザーは、Amazon FSx ファイルシステムの 管理者グループ* メンバーで、Robo oCopy で /b フラグを使用する必要があります。

> **Note**
>
> * AWS Managed Microsoft AD に参加しているファイルシステムの場合、Amazon FSx ファイルシステム管理者グループはAWS 委任 FSx 管理者です。セルフマネージド Microsoft AD では、Amazon FSx ファイルシステム管理者グループは、ドメイン管理者、またはファイルシステムの作成時に管理用に指定したカスタムグループです。

Robocopy を使用したファイルの移行

以下の手順を使用して、オンプレミスファイルシステムから既存のファイルを FSx for Windows File Server ファイルシステムに移行できます。

Robocopy を使用して既存のファイルを Amazon FSx に移行するには

1. Amazon FSx ファイルシステムと同じ Amazon VPC で、Windows Server 2016 Amazon EC2 インスタンスを起動します。
2. Amazon EC2 インスタンスに接続します。詳細については、「Windows インスタンスの 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. コマンドプロンプトを開き、次のように既存のファイルサーバー (オンプレミスまたは 内 AWS) のソースファイル共有をドライブ文字 (*Y*: など) にマッピングします。この一環として、オンプレミスアクティブディレクトリの ドメイン管理者 グループのメンバーに認証情報を指定します。

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

The command completed successfully.
```

4. 以下のように、Amazon EC2 インスタンスで Amazon FSx ファイルシステム上のターゲットファイル共有を別のドライブ文字にマッピングします (例えば、*Z*:)。この一環として、オンプレミスアクティブディレクトリのドメイン管理者グループと Amazon FSx ファイルシステムの管理者グループのメンバーであるユーザーアカウントの認証情報を指定します。 AWS Managed Microsoft AD に参加しているファイルシステムの場合、そのグループは ですAWS **Delegated FSx Administrators**。セルフマネージド Microsoft AD では、そのグループは **Domain Admins**、またはファイルシステム作成時にユーザーが管理用に指定したカスタムグループです。

詳細については、「Robocopy を使用したファイル移行の前提条件」の「出典および宛先のファイルシステムのアクセシビリティ要件」の表を参照してください。

```
C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
Enter the password for 'amznfsxabcdef1.mydata.com': _

Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

The command completed successfully.
```

5. コンテキストメニューから [Run as Administrator] (管理者として実行) を選択します。管理者として [Command Prompt] (コマンドプロント) または Windows PowerShell を開き、次の Robocopy コマンドを実行して、出典共有からターゲット共有にファイルをコピーします。

   ROBOCOPY コマンドは、データ転送プロセスをコントロールするための複数のオプションを備えた柔軟なファイル転送ユーティリティです。この ROBOCOPY コマンドプロセスにより、ソース共有のすべてのファイルとディレクトリが Amazon FSx ターゲット共有にコピーされます。このコピーは、ファイルとフォルダの NTFS ACL、属性、タイムスタンプ、所有者情報、そして監査情報を保持します。

```
robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
```

   前述のコマンド例では、次の要素とオプションを使用します。

   - Y - オンプレミスのアクティブディレクトリフォレスト mydata.com にある出典共有を指します。
   - Z - Amazon FSx 上のターゲット共有 \\amznfsxabcdef1.mydata.com\share を指します。
   - /copy - コピーする次のファイルプロパティを指定します。
     - D - データ
     - A - 属性
     - T - タイムスタンプ
     - S - NTFS ACL
     - O - 所有者情報
     - U - 監査情報。

- /secfix - スキップされたファイルも含む、すべてのファイルのファイルセキュリティを修正します。
- /e - 空のものを含むサブディレクトリをコピーします。
- /b - NTFS ACL が現在のユーザーに対する許可を拒否した場合でも、Windows のバックアップと復元特権を使用してファイルをコピーします。
- /MT:8 - マルチスレッドコピーの実行に使用するスレッド数を指定します。

> **Note**
>
> 低速の、または信頼性の低い接続で大きなファイルをコピーする場合は、/b オプション の代わりに robocopy で /zb を使用して再起動可能モードを有効にできます。再起動可能モードでは、大きなファイルの転送が中断された場合、最初からファイル全体を再コピーしなくても、転送の途中で後続の Robocopy オペレーションを再開できます。再起動可能モードを有効にすると、データ転送速度が低下する可能性があります。

オンプレミスのファイル共有設定を Amazon FSx に移行する

次の手順を使用して、既存のファイル共有設定を Amazon FSx に移行できます。この手順では、出典ファイルサーバーは Amazon FSx に移行するファイル共有設定のファイルサーバーです。

> **Note**
>
> ファイル共有設定を移行する前に、まずファイルを Amazon FSx に移行します。詳細については、「FSx for Windows File Server に既存のファイルストレージを移行する」を参照してください。

FSx for Windows File Server に、既存のファイル共有を移行するには

1. 出典ファイルサーバーで、コンテキストメニューから [Run as Administrator] (管理者として実行) を選択します。管理者として Windows PowerShell を開きます。
2. PowerShell で次のコマンドを実行して、出典ファイルサーバーのファイル共有を `SmbShares.xml` という名前のファイルにエクスポートします。この例では、ファイル共有のエクスポート元になるファイルサーバー上で、F: をドライブ文字に置き換えます。

```
$shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
$shareFolder | Export-Clixml -Path F:\SmbShares.xml
```

3. `SmbShares.xml` ファイルを編集し、Amazon FSx ファイルシステムは D: 上にあるため、F: (ドライブ文字) へのすべてのリファレンスを D:\share に置き換えます。
4. 既存のファイル共有設定を FSx for Windows File Server にインポートします。宛先の Amazon FSx ファイルシステムおよび出典ファイルサーバーにアクセスできるクライアントで、保存したファイル共有設定をコピーします。次に、以下のコマンドを使用して、可変にインポートします。

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. 次のいずれかのオプションを使用して、FSx for Windows File Server でファイル共有を作成するために必要な認証情報オブジェクトを準備します。

   認証情報オブジェクトをインタラクティブに生成するには、次のコマンドを使用します。

```
$credential = Get-Credential
```

   AWS Secrets Manager リソースを使用して認証情報オブジェクトを生成するには、次のコマンドを使用します。

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

6. 次のスクリプティングを使用して、ファイル共有設定を Amazon FSx ファイルサーバーに移行します。

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
 "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
 "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
 "Path", "Name", "EncryptData")
ForEach ($item in $shares) {
    $param = @{};
    Foreach ($property in $item.psObject.properties) {
        if ($property.Name -In $FSxAcceptedParameters) {
            $param[$property.Name] = $property.Value
```

```
        }
    }
    Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
 amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
Credential $Using:credential @Using:param }
}
```

オンプレミス DNS 設定の FSx for Windows File Server への移行

FSx for Windows ファイルサーバーは、ファイルシステム上のデータにアクセスするために使用できるすべてのファイルシステムに、デフォルトのドメインネームシステム (DNS) 名を提供します。Amazon FSx ファイルシステムの DNS エイリアスとして代替 DNS 名を設定することで、任意の DNS 名を使用してファイルシステムにアクセスすることもできます。

DNS エイリアスを使用すると、ファイルシステムストレージをオンプレミスから Amazon FSx に移行する際、既存の DNS 名を引き続き使用して Amazon FSx に保存されたデータにアクセスできます。これにより、Amazon FSx への移行時に DNS 名を使用するツールやアプリケーションを更新する必要がなくなります。DNS エイリアスは、新しいファイルシステムを作成する際、およびバックアップから新しいファイルシステムを作成する際に、既存の FSx for Windows File Server ファイルシステムに関連付けることができます。ファイルシステムには、最大 50 個の DNS エイリアスを一度に関連付けることができます。詳細については、「DNS エイリアスを管理する」を参照してください。

DNS 名は、次の要件を満たしている必要があります。

- 例えば `accounting.example.com` のように、完全修飾ドメイン名 (FQDN) としてフォーマットされる必要がある。
- 英数字とハイフン (-) を含めることができます。
- ハイフンで開始または終了することはできません。
- 数字で始めることができます。

DNS エイリアス名の場合、Amazon FSx は、アルファベット文字を、大文字、小文字、またはエスケープコード内の対応する文字として指定する方法に関係なく、小文字 (a〜z) として格納します。

次の手順では、Amazon FSx コンソール、CLI、および API を使用して、既存の FSx for Windows File Server のファイルシステムに DNS エイリアスを関連付ける方法について説明します。バックアップからの新しいファイルシステムを含む、新しいファイルシステムを作成する際のDNSエイリ

アスの関連付けの詳細については、「DNS エイリアスとファイルシステムの関連付け」を参照してください。

既存のファイルシステムに DNS エイリアスを関連付けるには (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、DNS エイリアスを関連付ける Windows 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) タブで、DNS エイリアス の [Manage] (管理) を選択し、[Manage DNS aliases] (DNS エイリアスの管理) ダイアログボックスを開きます。

4. [Associate new aliases] (新しいエイリアスの関連付け) ボックスに、関連付ける DNS エイリアスを入力します。
5. [Associate] (関連付け) を選択して、エイリアスをファイルシステムに追加します。

   [Current aliases] (現在のエイリアス) リストで、関連付けたエイリアスのステータスをモニタリングできます。ステータスが [Available] (使用可能) を読み取る場合、エイリアスはファイルシステムに関連付けらています (最大 2.5 分かかるプロセス)。

既存のファイルシステムに DNS エイリアスを関連付けるには (CLI)

- `associate-file-system-aliases` CLI コマンド、または AssociateFileSystemAliases API オペレーションを使用して、既存のファイルシステムに DNS エイリアスを関連付けます。

  次の CLI リクエストは、指定されたファイルシステムに 2 つのエイリアスを関連付けます。

  ```
  aws fsx associate-file-system-aliases \
      --file-system-id fs-0123456789abcdef0 \
      --aliases financials.corp.example.com transfers.corp.example.com
  ```

  レスポンスには、Amazon FSx がファイルシステムに関連付けているエイリアスのステータスが表示されます。

  ```
  {
        "Aliases": [
            {
                "Name": "financials.corp.example.com",
                "Lifecycle": CREATING
            },
            {
                "Name": "transfers.corp.example.com",
                "Lifecycle": CREATING
            }
        ]
    }
  ```

  関連付けているエイリアスのステータスをモニタリングするには、`describe-file-system-aliases` CLI コマンドを使用します (DescribeFileSystemAliases は同等の API オペレーション

です)。エイリアスの `Lifecycle` に [AVELABLE] (利用可能) の値がある場合は、それを使用してファイルシステムにアクセスできます (最大で 2.5 分かかるプロセス)。

Amazon FSx for Windows File Server へのオペレーションのカットオーバー

オンプレミスのファイルストレージ、ファイル共有設定、および DNS 設定を移行したら、次のステップは FSx for Windows File Server ファイルシステムにオペレーションを引き継ぐことです。FSx for Windows File Server のファイルシステムにカットオーバーするには、次のステップを実行します。

- カットオーバーの準備をします。
  - SMB クライアントを元のファイルシステムから一時的に切断します。
  - 最終ファイルとファイル共有設定の同期を実行します。
- Amazon FSx ファイルシステムのサービスプリンシパル名 (SPN) を設定します。
- DNS CNAME レコードを更新して、Amazon FSx ファイルシステムを指定します。

これらの各ステップを実行する手順は、後に続くセクションで説明します。

トピック

- Amazon FSx へのカットオーバーの準備
- Kerberos 認証用の SPN の設定
- Amazon FSx ファイルシステムの DNS CNAME レコードを更新する

Amazon FSx へのカットオーバーの準備

Amazon FSx ファイルシステムへのカットオーバーを準備するには、次の操作を行う必要があります。

- 元のファイルシステムに書き込むすべてのクライアントを切断します。
- AWS DataSync または Robocopy を使用して最終ファイル同期を実行します。詳細については、「FSx for Windows File Server に既存のファイルストレージを移行する」を参照してください。
- 最終ファイル共有設定の同期を実行します。詳細については、「オンプレミスのファイル共有設定を Amazon FSx に移行する」を参照してください。

Kerberos 認証用の SPN の設定

Amazon FSx との転送中に、Kerberos ベースの認証と暗号化を使用することをお勧めします。Kerberos は、ファイルシステムにアクセスするクライアントに最も安全な認証を提供します。DNS エイリアスを使用して Amazon FSx にアクセスするクライアントの Kerberos 認証を有効にするには、Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトの DNS エイリアスに対応するサービスプリンシパル名 (SPN) を追加する必要があります。

Kerberos 認証には必要な SPN が 2 つあります。

```
HOST/alias
HOST/alias.domain
```

例として、エイリアスが `finance.domain.com` の場合、必要な 2 つの SPN は以下の通りです。

```
HOST/finance
HOST/finance.domain.com
```

SPN は、一度に 1 つのアクティブディレクトリコンピュータオブジェクトにのみ関連付けることができます。元のファイルシステムの アクティブディレクトリコンピュータオブジェクトに設定された DNS 名の既存 SPN がある場合は、Amazon FSx ファイルシステムの SPN を作成する前にそれらを削除する必要があります。

次の手順では、既存の SPN を検索して削除し、Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトの既存 SPN を作成する方法について説明します。

必要な PowerShell アクティブディレクトリモジュールをインストールするには

1. Amazon FSx ファイルシステムをを結合しているアクティブディレクトリを結合している Windows インスタンスにログオンします。
2. 管理者として PowerShell を開きます。
3. 次のコマンドを使用して、PowerShell アクティブディレクトリのモジュールをインストールします。

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

元のファイルシステムのアクティブディレクトリコンピュータオブジェクト上で、既存の DNS エイリアス SPN を検索して削除するには

1. 次のコマンドを使用して、既存の SPN を検索します。*alias_fqdn* を、オンプレミス DNS 設定の FSx for Windows File Server への移行 のファイルシステムに関連付けた DNS エイリアスと置き換えます。

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 次のスクリプティング例を使用して、前のステップで返された既存の HOST SPN を削除します。

   - *alias_fqdn* を、オンプレミス DNS 設定の FSx for Windows File Server への移行 のファイルシステムに関連付けた完全な DNS エイリアスと置き換えます。
   - *file_system_DNS_name* を、元のファイルシステムの DNS 名に置き換えます。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. オンプレミス DNS 設定の FSx for Windows File Server への移行 のファイルシステムに関連付けた各 DNS エイリアスで、これらのステップを繰り返します。

Amazon FSx ファイルシステムの アクティブディレクトリコンピュータオブジェクトに SPN を設定するには

1. 次のコマンドを実行して、Amazon FSx ファイルシステムの新しい SPN を設定します。

   - *file_system_DNS_name* を、Amazon FSx がファイルシステムに割り当てた DNS エイリアスに置き換えます。

Amazon FSx コンソールでファイルシステムの DNS 名を検索するには、[File Systems] (ファイルシステム) を選択し、ユーザーのファイルシステムを選択します。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) ペインを選択します。DNS 名は、DescribeFileSystems 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。

- *alias_fqdn* を、オンプレミス DNS 設定の FSx for Windows File Server への移行 のファイルシステムに関連付けた完全な DNS エイリアスと置き換えます。

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> 元のファイルシステムのコンピュータオブジェクトの AD に DNS エイリアスの SPN が存在する場合、Amazon FSx ファイルシステムの SPN の設定は失敗します。既存の SPN の検索および削除については、「元のファイルシステムのアクティブディレクトリコンピュータオブジェクト上で、既存の DNS エイリアス SPN を検索して削除するには」を参照してください。

2. 次のスクリプティング例を使用して、新しい SPN が DNS エイリアス用に設定されていることを確認します。レスポンスに 2 つの HOST SPN、HOST/*alias* および HOST/*alias_fqdn* が含まれていることを確認します。

   file_system_DNS_name を、Amazon FSx がファイルシステムに割り当てた DNS エイリアスに置き換えます。Amazon FSx コンソールでファイルシステムの DNS 名を検索するには、[Files systems] (ファイルシステム) を選択し、ファイルシステムを選択してから、ファイルシステムの詳細ページで [Network & security] (ネットワークとセキュリティ) ペインを選択します。

DNS 名は、DescribeFileSystems 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。

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. オンプレミス DNS 設定の FSx for Windows File Server への移行 でファイルシステムに関連付けた DNS エイリアスごとに、前のステップを繰り返します。

> **Note**
>
> アクティブディレクトリで次のグループポリシーオブジェクト (GPO) を設定することにより、DNS エイリアスを使用してファイルシステムに接続しているクライアントとの転送中に Kerberos 認証と暗号化を適用できます。
>
> - NTLM の制限: リモートサーバーへの発信 NTLM トラフィック
> - NTLM の制限: NTLM 認証のリモートサーバー例外の追加
>
> 詳細については、「チュートリアル 5: DNS エイリアスを使用してファイルシステムにアクセスする」の「グループポリシーオブジェクト (GPO) を使用した Kerberos 認証の強制」を参照してください。

Amazon FSx ファイルシステムの DNS CNAME レコードを更新する

ファイルシステムの SPN を適切に設定した後、元のファイルシステムに解決された各 DNS レコードを、Amazon FSx ファイルシステムのデフォルトの DNS 名に解決する DNS レコードに置き換えることによって、Amazon FSx にカットオーバーできます。

必要な PowerShell cmdlets をインストールするには

1. Amazon FSx ファイルシステムが参加している Active Directory に参加している Windows インスタンスに、DNS 管理権限を持つグループのメンバーであるユーザーとしてログオンします (AWS Managed Microsoft Active Directory AWS の委任されたドメインネームシステム管理者、

およびドメイン管理者、またはセルフマネージド Active Directory で DNS 管理権限を委任した別のグループ) 。

詳細については、「Amazon EC2 ユーザーガイド」の「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 PowerShell を開きます。
3. この手順の指示を実行するには、PowerShell DNS サーバーモジュールが必要です。次のコマンドを使用してインストールします。

```
Install-WindowsFeature RSAT-DNS-Server
```

既存の DNS CNAME レコードを更新するには

1. 次のスクリプティングは、Amazon FSx ファイルシステムのコンピュータオブジェクトに、*alias_fqdn* の既存 DNS CNAME レコードを更新します。見つからない場合は、DNS エイリアス *alias_fqdn* の新しい DNS CNAME レコードが作成され、これは Amazon FSx ファイルシステムのデフォルトの DNS 名に解決します。

   スクリプティングを実行するには。

   - *alias_fqdn* を、ファイルシステムに関連付けた DNS エイリアスに置き換えます。
   - *file_system_DNS_name* を、Amazon FSx がファイルシステムに割り当てたデフォルトの DNS に置き換えます。

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. オンプレミス DNS 設定の FSx for Windows File Server への移行 でファイルシステムに関連付けた DNS エイリアスごとに、前述のステップを繰り返します。

FSx for Windows File Server ファイルシステムのモニタリング

モニタリングは、FSx for Windows File Server と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。障害が発生した場合は、障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、FSx for Windows File Server のモニタリングを開始する前に、以下の質問に対する回答を含むモニタリング計画を作成する必要があります。

- モニタリングの目的は何ですか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- どのモニタリングツールを利用しますか?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

FSx for Windows File Server での口グ記録とモニタリングの詳細については、次のトピックを参照してください。

トピック

- 自動モニタリングと手動モニタリング
- Amazon CloudWatch によるモニターリング
- を使用した Amazon FSx for Windows File Server API コールの口グ記録 AWS CloudTrail

自動モニタリングと手動モニタリング

AWS には、FSx for Windows File Server のモニタリングに使用できるさまざまなツールが用意されています。これらのツールの一部はモニタリングを行うように設定できますが、一部のツールは手動による介入が必要です。モニタリングタスクはできるだけ自動化することをお勧めします。

自動モニタリングツール

次の自動モニタリングツールを使用して、FSx for Windows File Server を監視し、問題が発生したときに報告できます。

- Amazon CloudWatch アラーム - 指定した期間にわたって単一のメトリクスをモニタリングし、複数の期間にわたる特定のしきい値に対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します。アクションは、Amazon Simple Notification Service (Amazon SNS) のトピックまたは Amazon EC2 Auto Scaling のポリシーに送信される通知です。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ている必要があります。詳細については、「Amazon CloudWatch によるモニターリング」を参照してください。
- Amazon CloudWatch Logs - AWS CloudTrail またはその他の出典からログファイルをモニタリング、保存、およびアクセスします。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「Amazon CloudWatch Logs とは?」を参照してください。
- AWS CloudTrail ログモニタリング – アカウント間でログファイルを共有し、CloudWatch Logs に送信CloudWatch CloudTrail ログファイルをリアルタイムでモニタリングし、Java でログ処理アプリケーションを書き込み、CloudTrail による配信後にログファイルが変更されていないことを確認します。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail ログファイルの使用」を参照してください。

手動モニタリングツール

FSx for Windows File Server をモニタリングするもう 1 つの重要な点は、Amazon CloudWatch アラームでカバーされていない項目を手動でモニタリングすることです。FSx for Windows File Server、CloudWatch、およびその他の AWS コンソールダッシュボードには、 AWS 環境の状態が at-a-glanceビューが表示されます。

Amazon FSx [モニタリングとパフォーマンス] ダッシュボードには、以下が表示されます。

- 現在の警告と CloudWatch アラーム
- ファイルシステムのアクティビティの概要
- ファイルシステムのストレージ容量と使用率
- ファイルサーバーおよびストレージボリュームのパフォーマンス
- CloudWatch アラーム

Amazon CloudWatch ダッシュボードには、次の内容が表示されます。

- 現在のアラームとステータス
- アラームとリソースのグラフ

- サービスのヘルスステータス

さらに、CloudWatch を使用して次のことを行うことができます。

- カスタマイズダッシュボード を作成して、使用するサービスをモニタリングします。
- メトリクスデータをグラフ化して、問題のトラブルシューティングと傾向の発見を行います。
- すべての AWS リソースメトリクスを検索して参照します。
- 問題があることを通知するアラームを作成および編集する。

Amazon FSx の [Monitoring & performance] (モニタリングとパフォーマンス) ダッシュボードの詳細については、「ファイルシステムのメトリクスの使用」を参照してください。

Amazon CloudWatch によるモニターリング

Amazon CloudWatch は、FSx for Windows File Server から raw データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工することができます。これらの統計は 15 か月間保持されるため、履歴情報へのアクセス許可を与え、ワークフローまたはファイルシステムのパフォーマンスを把握できます。

FSx for Windows File Server は、次のドメインで CloudWatch メトリクスを発行します。

- ネットワーク I/O メトリクスは、ファイルシステムにアクセスしているクライアントとファイルサーバー間のアクティビティを測定します。
- ファイルサーバーのメトリクスは、ネットワークスループット使用率、ファイルサーバーの CPU とメモリ、およびファイルサーバーのディスクスループット使用率と IOPS 使用率を測定します。
- ディスク I/O メトリクスは、ファイルサーバーとストレージボリューム間のアクティビティを測定します。
- ストレージボリュームのメトリクスは、HDD ストレージボリュームのディスクスループット使用率と SSD ストレージボリュームの IOPS 使用率を測定します。
- ストレージ容量のメトリクスは、データ重複排除によるストレージ節約を含めたストレージ使用状況を測定します。

次の図は、FSx for Windows File Server ファイルシステム、そのコンポーネント、およびメトリクスドメインを示しています。

デフォルトでは、Amazon FSx for Windows File Server は、メトリクスデータを 1 分間隔で CloudWatch に送信しますが、次のような例外は 5 分間隔で送信されます。

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

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。

メトリクスは、シングル AZ ファイルシステムではファイルシステムのメンテナンス中や、インフラストラクチャコンポーネントの交換時、マルチ AZ ファイルシステムではプライマリファイルサーバーとセカンダリファイルサーバー間のフェイルオーバー中およびフェイルバック中に発行されない場合があります。

Amazon FSx CloudWatch メトリクスは raw バイトとしてレポートされます。バイトは、単位の 10 進数または 2 進数の倍数に丸められません。

トピック

- CloudWatch メトリクスとディメンション
- ファイルシステムのメトリクスの使用
- パフォーマンスの警告と推奨事項
- ファイルシステムメトリクスへのアクセス
- CloudWatch アラームの作成

CloudWatch メトリクスとディメンション

FSx for Windows File Server は、すべてのファイルシステムに対して、次のメトリクスを Amazon CloudWatch 内の `AWS/FSx` 名前空間に発行します。

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx for Windows File Server は、少なくとも 32 MBps のスループットキャパシティで設定されたファイルシステムに対して、次のセクションで説明するメトリクスを Amazon CloudWatch 内の `AWS/FSx` 名前空間に発行します。

ネットワーク I/O メトリクス

`AWS/FSx` 名前空間には、次のネットワーク I/O メトリクスが含まれます。

メトリクス	説明
`DataReadBytes`	ファイルシステムにアクセスするクライアントでの読み込み操作のバイト数。 単位: バイト 有効な統計: `Sum`
`DataWriteBytes`	ファイルシステムにアクセスするクライアントでの書き込み操作のバイト数。 単位: バイト 有効な統計: `Sum`
`DataReadOperations`	ファイルシステムにアクセスするクライアントでの読み込み操作の回数。

メトリクス	説明
	単位: カウント 有効な統計: Sum
DataWrite Operations	ファイルシステムにアクセスするクライアントでの書き込み操作の回数。 単位: カウント 有効な統計: Sum
MetadataOperations	ファイルシステムにアクセスするクライアントでのメタデータ操作の回数。 単位: カウント 有効な統計: Sum
ClientConnections	クライアントとファイルサーバー間のアクティブな接続の数。 単位: カウント

ファイルサーバーのメトリクス

AWS/FSx 名前空間には、次のファイルサーバーのメトリクスが含まれます。

メトリクス	説明
NetworkThroughputUtilization	ファイルシステムにアクセスするクライアントのネットワークスループットを、プロビジョニングされた制限に対する割合 (%) で表したものです。 単位: パーセント
CPUUtilization	ファイルサーバーの CPU リソースの使用率 (%)。 単位: パーセント
MemoryUtilization	ファイルサーバーのメモリリソースの使用率 (%)。

メトリクス	説明
	単位: パーセント
FileServerDiskThroughputUtilization	ファイルサーバーとそのストレージボリューム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された制限に対する割合 (%) で表したものです。 単位: パーセント
FileServerDiskThroughputBalance	ファイルサーバーとそのストレージボリューム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 (%)。256 MBps 以下のスループットキャパシティでプロビジョニングされたファイルシステムに有効です。 単位: パーセント
FileServerDiskIopsUtilization	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、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された制限に対する割合 (%) で表したものです。 単位: パーセント
FileServerDiskIopsBalance	ファイルサーバーとそのストレージボリューム間のディスク IOPS に使用できるバーストクレジットの割合 (%)。256 MBps 以下のスループットキャパシティでプロビジョニングされたファイルシステムに有効です。 単位: パーセント

ディスク I/O メトリクス

AWS/FSx 名前空間には、次のディスク I/O メトリクスが含まれます。

メトリクス	説明
DiskReadBytes	ストレージボリュームにアクセスする読み込み操作のバイト数。

メトリクス	説明
	単位: バイト 有効な統計: Sum
DiskWriteBytes	ストレージボリュームにアクセスする書き込み操作のバイト数。 単位: バイト 有効な統計: Sum
DiskReadOperations	ストレージボリュームにアクセスするファイルサーバーでの読み込み操作の回数。 単位: カウント 有効な統計: Sum
DiskWriteOperations	ストレージボリュームにアクセスするファイルサーバーでの書き込み操作の回数。 単位: カウント 有効な統計: Sum

FSx for Windows ストレージボリュームのメトリクス

AWS/FSx 名前空間には、次のストレージボリュームのメトリクスが含まれます。

メトリクス	説明
DiskThroughputUtilization	(HDD のみ) ファイルサーバーとそのストレージボリューム間のディスクスループットを、ストレージボリュームによって決定されるプロビジョニングされた制限に対する割合 (%) で表したものです。 単位: パーセント

メトリクス	説明
DiskThroughputBalance	(HDD のみ) ストレージボリュームのディスクスループットおよびディスク IOPS に使用できるバーストクレジットの割合 (%)。 単位: パーセント
DiskIopsUtilization	(SSD のみ) 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、ストレージボリュームによって決定されるプロビジョンド IOPS 制限に対する割合 (%) で表したものです。 単位: パーセント

ストレージ容量のメトリクス

AWS/FSx 名前空間には、次のストレージ容量のメトリクスが含まれます。

メトリクス	説明
FreeStorageCapacity	使用できるストレージ容量。 単位: バイト 有効な統計: Average、Minimum
StorageCapacityUtilization	合計ストレージ容量に対する使用済み物理ストレージ容量の割合 (%)。 単位: パーセント
DeduplicationSavedStorage	データ重複排除が有効になっている場合、それによって節約されるストレージ領域の量。 単位: バイト

FSx for Windows File Server メトリクスの名前空間とディメンション

FSx for Windows ファイルサーバーのメトリクスは `FSx` 名前空間を使用し、単一のディメンション `FileSystemId` のメトリクスを提供します。ファイルシステムの ID は、describe-file-systems AWS CLI コマンド、または DescribeFileSystems API コマンドを使用して見つけることができます。ファイルシステム ID は、*`fs-0123456789abcdef0`* の形式です。

ファイルシステムのメトリクスの使用

各 Amazon FSx ファイルシステムには、2 つの主要なアーキテクチャコンポーネントがあります。

- ファイルシステムにアクセスするクライアントにデータを提供するファイルサーバー。
- ファイルシステム内のデータをホストするストレージボリューム。

FSx for Windows File Server は、ファイルシステムのファイルサーバーとストレージボリュームのパフォーマンスおよびリソース使用率を追跡するメトリクスを CloudWatch でレポートします。次の図は、Amazon FSx ファイルシステムとそのアーキテクチャコンポーネント、およびモニタリングに使用できるパフォーマンスとリソースの CloudWatch メトリクスを示しています。メトリクスのセットで表示される主なプロパティは、それらのメトリクスの容量を決定するファイルシステムのプロパティです。このプロパティを調整すると、そのメトリクスのセットに対応するファイルシステムのパフォーマンスが変更されます。

Amazon FSx コンソールの [Monitoring & performance] (モニタリングとパフォーマンス) パネルを使用して、次の表で説明されている FSx for Windows File Server の CloudWatch メトリクスを表示できます。

[Monitoring & performance] (モニタリングとパフォーマンス) パネル	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	ファイルシステムの合計 IOPS を判別するにはどうすればよいですか?	合計 IOPS	SUM(DataReadOperations + DataWriteOperations + MetadataOperations)/Period (秒単位)
	ファイルシステムの合計スループットを判別するにはどうすればよいですか?	合計スループット	SUM(DataReadBytes + DataWriteBytes)/Period (秒単位)
	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?	使用可能なストレージ容量	FreeStorageCapacity
	クライアントとファイルサーバー間で確立されている接続の数を判別するにはどうすればよいですか?	クライアント接続	ClientConnections
[Storage (ストレージ)]	ファイルシステムの合計ストレージ容量に対する、使用済み物理ディスク領域の量の割合 (%) を判別するにはどうすればよいですか?	ストレージ容量の使用率	StorageCapacityUtilization

[Monitoring & performance] (モニタリングとパフォーマンス) パネル	方法を教えてください	チャート	関連するメトリクス
	データ重複排除によって節約される物理ディスク領域の量を判別するにはどうすればよいですか?	データ重複排除によるストレージの節約	DeduplicationSavedStorage
パフォーマンス – ファイルサーバー	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対する、ファイルシステムにアクセスするクライアントのネットワークスループットの割合 (%) を判別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 [1]
	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された制限に対する、ファイルサーバーとそのストレージボリューム間のディスクスループットの割合 (%) を判別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 [1]
	ファイルサーバーとそのストレージボリューム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 (%) を判別するにはどうすればよいですか?	ディスクスループットのバーストバランス	FileServerDiskThroughputBalance

[Monitoring & performance] (モニタリングとパフォーマンス) パネル	方法を教えてください	チャート	関連するメトリクス
	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された制限に対する、ファイルサーバーとストレージボリュームの間のディスク IOPS の回数の割合 (%) を判別するにはどうすればよいですか?	ディスク IOPS 使用率	`FileServerDiskIopsUtilization`
	ファイルサーバーとストレージボリューム間のディスク IOPS に使用できるバーストクレジットの割合 (%) を判別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`
	ファイルサーバーの CPU 使用率 (%) を判別するにはどうすればよいですか?	CPU 使用率	`CPUUtilization`
	ファイルサーバーのメモリ使用率 (%) を判別するにはどうすればよいですか?	メモリ使用率	`MemoryUtilization`

[Monitoring & performance] (モニタリングとパフォーマンス) パネル	方法を教えてください	チャート	関連するメトリクス
パフォーマンス – ストレージボリューム	HDD ストレージ容量によって決定されるプロビジョニングされた制限に対する、ストレージボリュームにアクセスする操作でのスループットの割合 (%) を判別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 (HDD)	`DiskThroughputUtilization`
	HDD ストレージボリュームにアクセスする操作での利用可能なスループットと IOPS バーストクレジットの割合 (%) を決定しますか?	ディスクスループットのバーストバランス (HDD)	`DiskThroughputBalance` [2]
	HDD ストレージ容量によって決定されるプロビジョニングされた制限に対する、ストレージボリュームにアクセスする操作での IOPS の割合 (%) を決定しますか?	ディスク IOPS 使用率 (HDD)	SUM(`DiskReadOperations` + `DiskWriteOperations`)/`Period` (秒単位)/(TiB で 12 * プロビジョニングされた HDD ストレージ容量)
	SSD ストレージ容量によって決定されるプロビジョニングされた制限に対する、ストレージボリュームにアクセスする操作での IOPS の割合 (%) を判別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**
>
> [1]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 Windows ストレージオペレーション (ストレージ同期、重複除外、シャドウコピーなど) に対して、十分な予備スループットキャパシティを確保するために、平均スループットキャパシティを 50% 未満に維持することをお勧めします。
> [2]HDD ストレージボリュームでは、ワークロードに応じてパフォーマンスに大きなばらつきが生じる可能性があります。IOPS またはスループットが急激に急増すると、ディスクのパフォーマンスが低下する可能性があります。詳細については、「HDD バーストパフォーマンス」を参照してください。

パフォーマンスの警告と推奨事項

FSx for Windows では、少なくとも 32 MBps のスループットキャパシティで設定されたファイルシステムに対して、パフォーマンスの警告が表示されます。Amazon FSx 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 CloudWatch メトリクスのセットに対応する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、「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。

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
ネットワークスループット – 使用率	スループットキャパシティを増やす
ファイルサーバー > ディスク IOPS – 使用率	
ファイルサーバー > ディスクスループット – 使用率	
ファイルサーバー > ディスク IOPS – バーストバランス	
ファイルサーバー > ディスクスループット – バーストバランス	
ストレージ容量の使用率	ストレージ容量を増やす
ストレージボリューム > ディスクスループット – 使用率 (HDD)	ストレージ容量を増やす または SDD ストレージタイプに切り替え
ストレージボリューム > ディスクスループット – バーストバランス (HDD)	
ストレージボリューム > ディスク IOPS – 使用率 (SSD)	SSD IOPS を増やす

> **Note**
>
> 特定のファイルシステムイベントは、ディスク I/O パフォーマンスリソースを消費し、パフォーマンスの警告をトリガーする可能性があります。例:
>
> - ストレージ容量のスケーリングの最適化フェーズでは、ストレージ容量の拡張とファイルシステムのパフォーマンス で説明されているように、ディスクスループットが向上する可能性があります。
> - マルチ AZ ファイルシステムでは、スループットキャパシティのスケーリング、ハードウェアの交換、アベイラビリティーゾーンの中断などのイベントにより、自動的にフェイルオーバーとフェイルバックのイベントが発生します。この期間内に発生したデータ変更は、プライマリファイルサーバーとセカンダリファイルサーバー間で同期させる必要があ

るため、Windows Server はディスク I/O リソースを消費するデータ同期ジョブを実行します。詳しくは、「スループット容量の管理」を参照してください。

ファイルシステムのパフォーマンスに関する詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。

ファイルシステムメトリクスへのアクセス

CloudWatch の Amazon FSx メトリクスは、次の方法で確認できます。

- Amazon FSx コンソール
- CloudWatch コンソール
- CloudWatch CLI
- CloudWatch API

次の手順は、これらのさまざまなツール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示しています。

Amazon FSx コンソールを使用してファイルシステムの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. [File system details] (ファイルシステムの詳細) ページを表示するには、ナビゲーションペインで [File systems] (ファイルシステム) を選択します。
3. メトリクスを表示するファイルシステムを選択します。
4. ファイルシステムのメトリクスのグラフを表示するには、2 番目のパネルで [Monitoring & performance] (モニタリングとパフォーマンス) を選択します。

- [Summary] (概要) メトリクスは、デフォルトで表示され、[File system activity] (ファイルシステムのアクティビティ) メトリクスとともに、アクティブな警告および CloudWatch アラームが表示されます。
- [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。
- [Performance] (パフォーマンス) を選択して、ファイルサーバーおよびストレージのパフォーマンスメトリクスを表示します
- [CloudWatch alarms] (CloudWatch アラーム) を選択して、ファイルシステム用に設定されたアラームのグラフを表示します。

詳細については、「ファイルシステムのメトリクスの使用」を参照してください。

CloudWatch コンソールでメトリクスを表示する

1. Amazon CloudWatch コンソールの [Metrics] (メトリクス) ページでファイルシステムのメトリクスを表示する場合は、Amazon FSx コンソールの [Monitoring & performance] (モニタリングとパフォーマンス) パネルのメトリクスに移動します。
2. 次の図に示すように、メトリクスグラフの右上にある [Actions] (アクション) メニューから [View in metrics] (メトリクスで表示) を選択します。

これにより、CloudWatch コンソールの [Metrics] (メトリクス) ページが開き、次の図に示すような、メトリクスグラフが表示されます。

CloudWatch ダッシュボードにメトリクスを追加するには

1. CloudWatch コンソールのダッシュボードに FSx for Windows ファイルシステムのメトリクスのセットを追加するには、Amazon FSx コンソールの [Monitoring & performance] (モニタリングとパフォーマンス) パネルに表示されたメトリクスのセット ([Summary] (概要)、[Storage] (ストレージ)、または [Performance] (パフォーマンス)) を選択します。
2. パネルの右上にある [Add to dashboard] (ダッシュボードに追加) を選択すると、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。

からメトリクスにアクセスするには AWS CLI

- `--namespace "AWS/FSx"` 名前空間で `list-metrics` 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。

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
    "Metrics": [
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DataWriteOperationTime",
```

```
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CapacityPoolWriteBytes",
            "Dimensions": [
                {
                    "Name": "VolumeId",
                    "Value": "fsvol-0cb2281509f5db3c2"
                },
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DiskReadBytes",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CompressionRatio",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-0f84c9a176a4d7c92"
                }
            ]
        },
.
.
.
```

```
}
```

CloudWatch API の使用

CloudWatch API からメトリクスにアクセスするには

- `GetMetricStatistics` 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。

CloudWatch アラームの作成

アラームの状態が変わったら、Amazon SNS メッセージを送信する Amazon CloudWatch のアラームを作成することができます。アラームは、指定期間にわたって単一のメトリクスを監視し、指定したしきい値に対応したメトリクスの値に基づいて、期間数にわたって 1 つ以上のアクションを実行します。アクションは、Amazon SNS のトピックまたはオートスケーリングのポリシーに送信される通知です。

アラームは、持続した状態の変化に対してのみアクションを呼び出します。CloudWatch のアラームは、メトリクスが特定の状態になっただけではアクションを呼び出しません。アクションを呼び出すには、状態が変化して、指定し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 CloudWatch コンソールからアラームを作成できます。

次の手順は、コンソール、 AWS CLI、および API を使用して Amazon FSx のアラームを作成する方法を示しています。

CloudWatch アラームを設定するには (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、[File systems] (ファイルシステム) を選択し、アラームに対して作成したいファイルシステムを選択します。
3. [Actions] (アクション) メニューを選択し、[View details] (詳細の表示) を選択します。
4. [Summary] (概要) ページで、[Monitoring] (モニタリング) を選択します。
5. [CloudWatch アラーム] を選択します。
6. [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。
7. [Select metrics] (メトリクスの選択) を選択し、[Next] (次へ) を選択します。

8. [メトリクス] セクションで、[FSX] を選択します。
9. [File System Metrics] (ファイルシステムメトリクス) を選択し、アラームを設定するメトリクスを選択し、[Select metrics] (メトリクスの選択) を選択します。
10. [Conditions] (条件) セクションで、アラームに使用する条件を選択し、[Next] (次へ) を選択します。

> **Note**
>
> メトリクスは、シングル AZ ファイルシステムではファイルシステムのメンテナンス中や、マルチ AZ ファイルシステムではプライマリサーバーまたはセカンダリサーバーとの間のフェイルオーバー中およびフェイルバック中に発行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「CludWatch 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トリガーした際に、CloudWatch から E メール または SNS 通知を受け取りたい場合は、アラーム状態に [Whenever this alarm state is] (このアラーム状態がいかなる場合も) を選択します。

    [select an SNS topic] (SNS トピックの選択) で、既存の SNS トピックを選択します。[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。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際に、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. [Name] (名前)、[Description] (説明)、[Whenever] (いつでも) のそれぞれにメトリクスの値を入力し、[Next] (次へ) を選択します。
13. [Preview and create] (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、[Create Alarm] (アラームの作成) を選択します。

CloudWatch コンソールを使用してアラームを設定するには

1. にサインイン AWS Management Console し、https://https://console.aws.amazon.com/cloudwatch/://www.com で CloudWatch コンソールを開きます。
2. [Create Alarm] (アラームの作成) を選択して、[Create Alarm Wizard] (アラームウィザードの作成) を起動します。
3. [FSx Metrics] を選択し、Amazon FSx メトリクスをスクロールして、アラームを設定するメトリクスを見つけます。このダイアログボックスに Amazon FSx メトリクスのみを表示するには、ファイルシステムのファイルシステム ID で検索します。アラームを作成するメトリクスを選択し、[Next] (次へ) をクリックします。
4. [Name] (名前)、[Description] (説明)、[Whenever] (いつでも) のそれぞれにメトリクスの値を入力します。
5. アラーム状態に達したときに CloudWatch から E メールを受け取るには、[Whenever this alarm] (アラームが次の時:) で、[State is ALARM] (状態: 警告) を選択します。[Send notification to] (通知の宛先) に、既存の SNS トピックを選択します。[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。

   > **Note**
   >
   > [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。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際に、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。

6. この段階で、[Alarm Preview] (アラームの確認) エリアで作成しているアラームを確認することができます。[Create Alarm] (アラームの作成) を選択します。

CloudWatch アラームを設定するには (CLI)

- `put-metric-alarm` 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。

アラームを設定するには (API)

- `PutMetricAlarm` 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。

を使用した Amazon FSx for Windows File Server API コールのログ記録 AWS CloudTrail

Amazon FSx for Windows File Server は AWS CloudTrail、Amazon FSx のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Amazon FSx へのすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Amazon FSx コンソールからの呼び出しと、Amazon FSx API オペレーションへのコード呼び出しが含まれます。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。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail により収集された情報を使用して、Amazon FSx に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエストが行われた日時、および追加の詳細を特定することができます。

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、アカウントの作成 AWS アカウント 時に で有効になります。Amazon FSx でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。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、 のイベントの継続的な記録については、証跡を作成します。追跡により、CloudTrail はログファイルを 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きに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要

- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

すべての Amazon FSx アクションは、CloudTrail によりログ記録され、Amazon FSx API リファレンスで文書化されます。例えば、`CreateFileSystem`、`CreateBackup`、`TagResource` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

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または AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- 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、「CloudTrail userIdentity エレメント」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。イベントは任意ソースからの単一リクエストを表し、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の情報を含みます。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"
}
```

Amazon FSx 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を活用できます。

セキュリティは、 AWS お客様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して説明しています。

- クラウドのセキュリティ – AWS は、Amazon Web Services Cloud 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。 は、お客様が安全に使用できるサービス AWS も提供します。AWS コンプライアンスプログラム の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon FSx for Windows File Server に適用されるコンプライアンスプログラムについては、「コンプライアンスプログラムによるスコープ内のAWS サービス」 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、ユーザーは、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 for Windows File Server を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように Amazon FSx for Windows File Server を設定する方法について説明します。また、Amazon FSx for Windows File Server 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 Windows File Server でのデータ保護
- Windows ACLs を使用したファイルレベルおよびフォルダレベルのアクセスコントロール
- Amazon VPC を使用したファイルシステムアクセスコントロール
- ファイルアクセス監査によるエンドユーザーアクセスのログ記録
- Amazon FSx for Windows File Server の Identity and Access Management
- Amazon FSx for Windows File Server のコンプライアンス検証
- Amazon FSx for Windows File Server およびインターフェイス VPC エンドポイント

Amazon FSx for Windows File Server でのデータ保護

AWS 責任共有モデル、Amazon FSx for Windows File Server 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 Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- 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 FSx for Windows File Server 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 Windows File Server のデータ暗号化

Amazon FSx for Windows File Server は、保管中のデータの暗号化と転送中のデータの暗号化をサポートしています。保管中のデータの暗号化は、Amazon FSx ファイルシステムの作成時に自動的に有効になります。転送中のデータの暗号化は、SMB プロトコル 3.0 以降をサポートす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ます。Amazon FSx は、アプリケーションを変更することなく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。

暗号化を使用するタイミング

保存中のデータとメタデータの暗号化をリクエストする企業ポリシーまたは規制ポリシーの影響をユーザーの組織が受ける場合は、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暗号化ファイルシステムを作成することをお勧めします。

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。

保管中のデータの暗号化

すべての Amazon FSx ファイルシステムは、 AWS Key Management Service (AWS KMS) を使用して管理されるキーを使用して保存時に暗号化されます。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 の の使用方法 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、 AWS KMS key を使用してファイルシステムを暗号化します。ファイルシステム (データとメタデータの両方) の暗号化と復号化に使用する KMS キーを選択します。この KMS キーの許可は、有効化、無効化、または削除することができます。この KMS キーは、以下の 2 つのタイプのいずれかになります。

- AWS マネージドキー - これはデフォルトの KMS キーで、無料で使用できます。
- 顧客管理キー - これは、複数のユーザーまたはサービスに対してキーポリシーと付与を設定できるため、使用するのに最も柔軟な KMS キーです。カスタマーマネージド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。

ファイルデータ暗号化と復号化の KMS キーとして顧客管理キーを使用する場合は、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。さらに、カスタマーマネージドキーを使用すると、いつでも KMS キーへのアクセスを無効化、再有効化、削除、または取り消すタイミングを選択できます。詳細については、「 デベロッパーガイド」の「ロー AWS KMS keysテーション」を参照してください。AWS Key Management Service

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平文です。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:ReEncrypt - (オプション) クライアント側にデータのプレーンテキストを公開することなく、サーバー側で新しい KMS キーを使用してデータを暗号化します。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。許可の詳細については、 AWS Key Management Service デベロッパーガイドの「許可の使用」を参照してください。このアクセス許可は、デフォルトのキーポリシーに含まれています。
- kms:DescribeKey - (必須) 指定された KMS キーに関する詳細情報を提供します。この許可は、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。この許可は、デフォルトのキーポリシーに含まれています。

転送中のデータの暗号化

転送中のデータの暗号化は、SMB プロトコル 3.0 以降をサポートす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ます。これには、Windows Server 2012 および Windows 8 以降のすべての Windows バージョンと、Samba クライアントバージョン 4.2 以降を搭載したすべての Linux クライアントが含まれます。Amazon FSx for Windows File Server は、アプリケーションを変更することなくファイルシステムにアクセスするときに、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。

SMB 暗号化は、暗号化アルゴリズムとして AES-128-GCM または AES-128-CCM (クライアントが SMB 3.1.1 をサポートしている場合は GCM バリアントが選択されます) を使用し、SMB Kerberos セッションキーを使用した署名によるデータ整合性も提供します。AES-128-GCM を使用すると、パフォーマンスが向上します。例えば、暗号化された SMB 接続を介して大きなファイルをコピーする場合のパフォーマンスが最大 2 倍向上します。

転送中のデータを常に暗号化するためのコンプライアンス要件を満たすために、ファイルシステムへのアクセスを制限して、SMB 暗号化をサポートするクライアントへのアクセスのみを許可することができます。ファイル共有ごと、またはファイルシステム全体への転送中の暗号化を有効または無効にすることもできます。これにより、同じファイルシステム上で暗号化されたファイル共有と暗号化されていないファイル共有を混在させることができます。

転送時の暗号化の管理

一連のカスタム PowerShell コマンドを使用して、 FSx for Windows File Server ファイルシステムおよびクライアント間の転送中のデータの暗号化をコントロールできます。SMB 暗号化をサポートするクライアントのみにファイルシステムアクセスを制限して、送信中のデータが常に暗号化されるようにできます。転送中のデータの暗号化の強制を有効にすると、SMB 3.0 暗号化をサポートしてい

ないクライアントからファイルシステムにアクセスするユーザーは、暗号化が有効になっているファイル共有にアクセスできなくなります。

また、ファイルサーバーレベルの代わりに、ファイル共有レベルで転送中のデータの暗号化をコントロールすることもできます。機密データを含む一部のファイル共有に対して転送中の暗号化を強制し、すべてのユーザーが他のファイル共有にアクセスできるようにする場合は、ファイル共有レベルの暗号化コントロールを使用して、暗号化されているファイル共有と暗号化されていないファイル共有を同じファイルシステム上に混在させることができます。サーバー全体の暗号化は、共有レベルの暗号化よりも優先されます。グローバル暗号化が有効になっている場合、特定の共有の暗号化を選択的に無効にすることはできません。

PowerShell でのリモート管理に Amazon FSx CLI を使用して、ファイルシステムの転送時の暗号化を管理できます。この CLI を使用する方法については、「PowerShell での Amazon FSx CLI の使用」を参照してください。

ファイルシステム上でユーザーの転送中の暗号化を管理するために使用できるコマンドは次のとおりです。

転送コマンドの暗号化	説明
Get-FSxSmbServerConfiguration	サーバーメッセージブロック (SMB) サーバー設定を取得します。システムレスポンスでは、`EncryptData` および `RejectUnencryptedAccess` プロパティの値に基づいて、ファイルシステムの転送時の暗号化設定を決定できます。
Set-FSxSmbServerConfiguration	このコマンドには、ファイルシステムで転送時の暗号化をグローバルに設定するための 2 つのオプションがあります。 • `-EncryptData $True\|$False` – このパラメータを `True` に設定して、転送中のデータ暗号化をオンにします。このパラメータを `False` に設定して、転送中のデータ暗号化をオフにします。 • `-RejectUnencryptedAccess $True\|$False` – このパラメータを `True` に設定して、暗号化をサポートしていないクライアントがファイルシステムにアクセスすることを許可しないようにします。暗号化をサポートしていないクライアントがファイルシステムにアクセスできるようにするには、このパラメータを `False` に設定します。

転送コマンドの暗号化	説明
Set-FSxSmbShare -name ***name*** -EncryptData $True	このパラメータを に設定`True`して、共有の転送中のデータ暗号化を有効にします。このパラメータを に設定`False`して、共有の転送中のデータ暗号化をオフにします。

各コマンドのオンラインヘルプには、すべてのコマンドオプションのリファレンスが記載されています。このヘルプにアクセスするには、-? (例えば、 Get-FSxSmbServerConfiguration -?) のコマンドを実行します。

Windows ACLs を使用したファイルレベルおよびフォルダレベルのアクセスコントロール

Amazon FSx for Windows File Server は、Microsoft アクティブディレクトリを介したサーバーメッセージブロック (SMB) プロトコルへのアイデンティティベースの認証をサポートしています。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簡単に見つけて使用できるようにする Microsoft 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。Amazon FSx でのアクティブディレクトリサポートの詳細については、「Microsoft Active Directory の使用」を参照してください。

ドメインを結合しているコンピューティングインスタンスは、アクティブディレクトリ認証情報を使用して Amazon FSx ファイル共有にアクセスできます。きめ細かい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には、スタンダードの Windows アクセスコントロールリスト (ACL) を使用します。Amazon FSx ファイルシステムは、ファイルシステムデータにアクセスするユーザーの認証情報を自動的に検証して、これらの Windows ACL を適用します。

すべての Amazon FSx ファイルシステムには、`share` と呼ばれるデフォルトの Windows ファイル共有が付属しています。この共有フォルダーの Windows ACL は、ドメインユーザーに読み取り/書き込みアクセスを許可するように設定されています。また、ファイルシステムで管理アクションを実行するように委任されたアクティブディレクトリ内の委任された管理者グループを完全にコントロールできます。ファイルシステムを AWS Managed Microsoft AD と統合する場合、このグループは委任 AWS FSx 管理者です。ファイルシステムをセルフマネージドの Microsoft AD セットアップと統合する場合、このグループはドメイン管理者になることができます。または、ファイルシステムの作成時に指定したカスタムの委任された管理者グループにすることもできます。ACL を変更するには、委任された管理者グループのメンバーであるユーザーとして共有をマッピングできます。

> **Warning**
>
> Amazon FSx では、SYSTEM ユーザーがファイルシステム内のすべてのフォルダーに対する フルコントロール の NTFS ACL アクセス許可を持っている必要があります。フォルダでこのユーザーの NTFSACL アクセス許可を変更しないでください。これを行うと、ファイル共有にアクセスできなくなり、ファイルシステムのバックアップを使用できなくなる可能性があります。

関連リンク

- 「 管理ガイド」の AWS 「 Directory Service とは」。 AWS Directory Service
- AWS Directory Service 管理ガイドの AWS Managed Microsoft AD ディレクトリを作成します。
- 「AWS Directory Service 管理ガイド」で「信頼関係を作成するタイミング」。
- ステップ 1. Active Directory のセットアップ.

Amazon VPC を使用したファイルシステムアクセスコントロール

Elastic Network Interface を介して Amazon FSx のファイルシステムにアクセスします。この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 Virtual Private Cloud (Amazon VPC) サービスに基づく仮想プライベートクラウド (VPC) に存在します。ドメインネームサービス (DNS) 名を介して Amazon FSx ファイルシステムに接続します。DNS 名は、VPC 内のファイルシステムの Elastic Network Interface のプライベート 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、 AWS Direct Connect または VPN によって関連付けられた VPC に接続されたリソース、またはピア接続された VPCs 内のリソースのみが、ファイルシステムのネットワークインターフェイス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。

FSx for Windows File Server は VPC 共有をサポートしています。これにより、別の AWS アカウントが所有する VPC の共有サブネット内のリソースを表示、作成、変更、削除できます。詳細については、「Amazon VPC ユーザーガイド」の「共有VPCの操作」を参照してください。

Amazon VPC セキュリティグループ

VPC 内のファイルシステムの Elastic Network Interface を通過するネットワークトラフィックをさらにコントロールするには、セキュリティグループを使用してファイルシステムへのアクセスを制限します。セキュリティグループ は、関連するネットワークインターフェイスとの間のトラフィックをコントロールするステートフルファイアウォールです。この場合、関連するリソースはファイルシステムのネットワークインターフェイスです。

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の詳細については、「Amazon EC2 ユーザーガイド」の「セキュリティグループルール」を参照してください。

Amazon 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 については、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. 以下のルールを追加して、次のポートでアウトバウンドネットワークトラフィックを許可します。

   a. VPC セキュリティグループ の場合、デフォルトの Amazon VPC のデフォルトのセキュリティグループは、コンソールのファイルシステムにすでに追加されています。FSx 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と VPC ネットワーク ACL

が、次の図表に示す方向のポートでのトラフィックを許可していることを確認してください。

以下の表に、各ポートのロールを示します。

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	464	パスワードを変更 / 設定する
TCP / UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Computing Environment / End Point Mapper (DCE / EPMAP)
TCP	445	Directory Services SMB ファイル共有

プロトコル	ポート	ロール
TCP	636	TLS/SSL (LDAPS) を介した Lightweight Directory Access Protocol (LDAPS)
TCP	3268	Microsoft グローバルカタログ
TCP	3269	SSL 経由の Microsoft グローバルカタログ
TCP	5985	WinRM 2.0 (Microsoft Windows リモート管理)
TCP	9389	Microsoft AD DS ウェブサービス、PowerShell
TCP	49152 - 65535	RPC 用のエフェメラルポート

> **Important**
>
> シングル AZ2 およびすべてのマルチ AZ ファイルシステムのデプロイには、TCP ポート 9389 でのアウトバウンドトラフィックを許可する必要があります。

b. これらのトラフィックルールが、AD ドメインコントローラー、DNS サーバー、FSx クライアント、および 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ことを確認してください。

> **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に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VPCネットワーク ACL では、ポートを両方向に開く必要があります。

> **Note**
>
> アクティブディレクトリのサイトを定義している場合は、Amazon FSx ファイルシステムに関連付けられている VPC のサブネットがアクティブディレクトリサイトで定義されていること、および VPC のサブネットおよび他のサイトのサブネットの間に競合が

存在しないことを確認する必要があります。これらの設定は、アクティブディレクトリのサイトとサービス MMC スナップインを使用して表示および変更できます。

> **Note**
>
> 場合によっては、 AWS Managed Microsoft AD セキュリティグループのルールをデフォルト設定から変更した可能性があります。その場合、このセキュリティグループに Amazon FSx ファイルシステムからのトラフィックを許可するために必要なインバウンドルールがあることを確認してください。必要なインバウンドルールの詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD 前提条件」を参照してください。

セキュリティグループを作成したので、それを Amazon FSx ファイルシステムの Elastic Network Interface に関連付けることができます。

セキュリティグループを Amazon FSx ファイルシステムに関連付けるには

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、ファイルシステムを選択して詳細を表示します。
3. [Network & Security] (ネットワークとセキュリティ) タブを選択し、ファイルシステムのネットワークインターフェイス (例えば、[ENI-01234567890123456]) を選択します。シングル AZ ファイルシステムの場合、1 つのネットワークインターフェイスが表示されます。マルチ AZ ファイルシステムの場合、優先サブネットとスタンバイサブネットに 1 つずつ、ネットワークインターフェイスが表示されます。
4. ネットワークインターフェイスごとにネットワークインターフェイスを選択し、[Actions] (アクション) で [Change Security Groups] (セキュリティグループを変更) を選択します。
5. [Change Security Groups] (セキュリティグループの変更) ダイアログボックスで、使用するセキュリティグループを選択し、[Save] (保存) を選択します。

ファイルシステムへのアクセスを停止する

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禁止するには、ファイルシステムの Elastic Network Interface 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のないグループに置き換えます。

Amazon VPC ネットワーク ACL

VPC 内のファイルシステムへのアクセスを保護するためのもう 1 つのオプションは、ネットワークアクセスコントロールリスト (ネットワーク ACL) を確立することです。ネットワーク ACL はセキュリティグループとは別のものですが、VPC のリソースにセキュリティのレイヤーを追加するための同様の機能があります。ネットワーク ACL の詳細については、「Amazon VPC ユーザーガイド」の「ネットワーク ACL」を参照してください。

ファイルアクセス監査によるエンドユーザーアクセスのログ記録

Amazon FSx for Windows File Server は、ファイル、フォルダ、およびファイル共有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。ファイルシステムの監査イベントログを、豊富な機能を提供する他の AWS サービスに送信することを選択できます。これには、ログのクエリ、処理、保存、アーカイブの有効化、通知の発行、セキュリティとコンプライアンスの目標をさらに前進させるためのアクションのトリガーが含まれます。

ファイルアクセス監査を使用してアクセスパターンを把握し、エンドユーザーのアクティビティに関するセキュリティ通知を実装する方法の詳細については、「File storage access patterns insights」と「Implementing security notifications for end user activity」を参照してください。

> **Note**
>
> ファイルアクセス監査は、32 MBps 以上のスループットキャパシティを持つ FSx for Windows のファイルシステムでのみサポートされます。既存のファイルシステムの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、「スループット容量の管理」を参照してください。

ファイルアクセス監査を使用すると、ユーザーが定義した監査管理に基づいて、個々のファイル、フォルダ、およびファイル共有のエンドユーザーアクセスをレコードできます。監査コントロールは、NTFS システムアクセスコントロールリスト (SACL) とも呼ばれます。既存のファイルデータに監査コントロールがすでに設定されている場合は、ファイルアクセス監査を利用して新しい Amazon FSx for Windows File Server のファイルシステムを作成したり、データを移行することができます。

Amazon FSx は、ファイル、フォルダー、およびファイル共有アクセスのために次の Windows 監査イベントをサポートしています。

- ファイルアクセスに関しては、次がサポートされます: すべて、フォルダのスキャン / ファイルの実行、フォルダ一覧 / データの読み取り、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、サブフォルダとファイルの削除、削除、許可の読み取り、許可の変更、および所有権の取得。

- ファイル共有アクセスに関しては、次がサポートされます: ファイル共有に接続。

Amazon FSx は、ファイル、フォルダー、およびファイル共有へのアクセス全体で、成功した試行 (ファイルまたはファイル共有に正常にアクセスするための十分なアクセス許可を持つユーザーなど)、失敗した試行、またはその両方のロギングをサポートします。

アクセス監査をファイルとフォルダでのみ行うか、ファイル共有のみ、またはその両方で行うかを設定できます。ログに記録するアクセスの種類 (成功した試行のみ、失敗した試行のみ、またはその両方) を設定することもできます。また、ファイルアクセス監査はいつでも無効にできます。

> **Note**
>
> ファイルアクセスの監査では、有効化される時点からのエンドユーザーアクセスデータのみが記録されます。つまり、ファイルアクセスの監査では、ファイルアクセスの監査が有効化される前に発生したエンドユーザーのファイル、フォルダ、ファイル共有アクセスアクティビティの監査イベントログは生成されません。

サポートされるアクセス監査イベントの最大レートは、1 秒あたり 5,000 イベントです。アクセス監査イベントは、ファイルの読み取りおよび書き込みオペレーションごとに生成されるのではなく、ユーザーがファイルを作成したり、開いたり、削除したときなどの、ファイルメタデータオペレーションごとに 1 回生成されます。

トピック

- 監査イベントログの宛先
- 監査コントロールの移行
- イベントログの表示
- ファイルとフォルダの監査コントロールの設定
- ファイルアクセス監査の管理

監査イベントログの宛先

ファイルアクセス監査を有効にするときは、Amazon FSx が監査イベントログを送信する AWS サービスを設定する必要があります。この監査イベントログを、CloudWatch Logs ロググループ内の

Amazon CloudWatch Logs ログストリーミングか、Amazon Data Firehose 配信ストリームのいずれかに送信することができます。Amazon FSx for Windows File Server のファイルシステムを作成する際、または既存のファイルシステムを更新する際に、監査イベントログの宛先を選択できます。詳細については、「ファイルアクセス監査の管理」を参照してください。

以下は、選択する監査イベントログの宛先を決定するのに役立つ推奨事項になります。

- Amazon CloudWatch コンソールで監査イベントログを保存、表示、検索し、CloudWatch Logs インサイトを使用してログに対してクエリを実行し、CloudWatch アラームまたは Lambda 関数をトリガーする場合は、CloudWatch Logs を選択します。
- Amazon S3 のストレージ、Amazon Redshift のデータベース、Amazon OpenSearch Service、または詳細な分析のために Splunk や Datadog などの AWS パートナーソリューションにイベントを継続的にストリーミングする場合は、Amazon Data Firehose を選択します。

デフォルトでは、Amazon FSx はアカウントにデフォルトの CloudWatch Logs ロググループを作成し、監査イベントログの宛先として使用します。監査イベントログの宛先としてカスタム CloudWatch Logs ロググループ、または Firehose を使用する場合、監査イベントログの宛先の名前と場所の要件は次のとおりです。

- CloudWatch Logs ロググループの名前は、`/aws/fsx/` プレフィックスで始まる必要があります。コンソールでファイルシステムを作成または更新する際に既存の CloudWatch Logs ロググループがない場合、Amazon FSx は CloudWatch Logs `/aws/fsx/windows` ロググループでデフォルトのログストリーミングを作成して使用します。デフォルトのロググループを使用しない場合は、コンソールでファイルシステムを作成または更新する際に、設定 UI を使用して CloudWatch Logs ロググループを作成できます。
- Firehose の配信ストリーム名は、`aws-fsx-` プレフィックスで始まる必要があります。既存の Firehose 配信ストリームがない場合は、コンソールでファイルシステムを作成または更新する際に作成できます。
- Firehose の配信ストリームは、`Direct PUT` を出典として使用するように設定する必要があります。既存の Kinesis Data Stream を配信ストリームのデータソースとして使用することはできません。
- 送信先 (CloudWatch Logs ロググループまたは Firehose 配信ストリーム) は AWS リージョン、Amazon FSx ファイルシステム AWS アカウント と同じ AWS パーティションにある必要があります。

監査イベントログの宛先はいつでも変更できます (例えば CloudWatch Logs から Firehose)。これを実行すると、新しい監査イベントログは新たな宛先にのみ送信されます。

ベストエフォート監査イベントログ配信

通常、監査イベントログレコードは宛先に数分で配信されますが、時間がかかることもあります。ごく稀に、監査イベントログレコードが失われることがあります。ユーザーのユースケースで特定のセマンティクスが必要になる場合 (例えば、監査イベントを必ず見逃さないなど)、ワークフローを設計する際に見逃したイベントを考慮することをお勧めします。ファイルシステム上のファイルおよびフォルダ構造をスキャンして、見逃したイベントを監査できます。

監査コントロールの移行

既存のファイルデータに監査コントロール (SACL) がすでに設定されている場合は、Amazon FSx ファイルシステムを作成し、データを新しいファイルシステムに移行できます。を使用して AWS DataSync 、Amazon FSx ファイルシステムにデータと関連する SACLs を転送することをお勧めします。別の解決策として、Robocopy (ロバストファイルコピー) を使用できます。詳細については、「既存のファイルストレージを Amazon FSx に移行する」を参照してください。

イベントログの表示

Amazon FSx が監査イベントログの発行を開始した後、それらを表示できます。ログの表示場所と方法は、監査イベントログの宛先によって異なります。

- CloudWatch Logs を表示するには、CloudWatch コンソールに移動し、監査イベントログの宛先となるロググループとログストリーミングを選択します。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「CloudWatch Logs に送信されたログデータを表示する」を参照してください。

  CloudWatch Logs Insights を使用してログデータをインタラクティブに検索および分析できます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「[Analyzing Log Data with CloudWatch Logs Insights]」(CloudWatch Logs Insights でログデータを分析) を参照してください。

  監査イベントログを Simple Storage Service (Amazon S3) にエクスポートすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「[Exporting Log Data to Amazon S3]」(Simple Storage Service (Amazon S3) にログデーターをエキスポート) を参照してください。

- Firehose では、監査イベントログを表示できません。ただし、読み取り可能な宛先にログを転送するように Firehose を設定できます。目的地には Simple Storage Service (Amazon S3)、Amazon Redshift、Amazon OpenSearch Service、および Splunk や Datadog などのパートナーソリューションが含まれます。詳細については、「Amazon Data Firehose デベロッパーガイド」の「[Choose destination]」(宛先を選択) を参照してください。

監査イベントフィールド

このセクションでは、監査イベントログの情報と、監査イベントの例について説明します。

以下は Windows 監査イベントの顕著なフィールドについての説明になります。

- EventID は、Microsoft 定義の Windows イベントのログイベント ID を指します。ファイルシステムイベント および ファイル共有イベント の情報については、Microsoft のドキュメントを参照してください。
- [subjectUsername] (サブジェクトユーザー名) は、アクセスを実行しているユーザーを指します。
- [objectName] (オブジェクト名) は、アクセスされたターゲットファイル、フォルダ、またはファイル共有を指します。
- [shareName] (共有名) は、ファイル共有アクセス用に生成されたイベントで使用できます。例えば、`EventID 5140` はネットワーク共有オブジェクトにアクセスしたときに生成されます。
- [IpAddress] (IP アドレス) は、ファイル共有イベントのイベントを開始したクライアントを指します。
- [Keywords] (キーワード) は、使用可能な場合に、ファイルアクセスが成功したか障害だったかを指します。成功したアクセスの場合、値は `0x8020000000000000` です。失敗したアクセスの場合、値は `0x8010000000000000` です。
- [TimeCreated SystemTime] (作成時刻 システム時間) は、システム内でイベントが生成さた時刻を指し、<YYYY-MM-DDThh:mm:ss.s>Z 形式で表示されます。
- [Computer] (コンピュータ) は、ファイルシステムの Windows リモート PowerShell エンドポイントの DNS 名を参照し、ファイルシステムを識別するために使用できます。
- [AccessMask] (アクセスマスク) は、使用可能な場合、実行されたファイルアクセスの種類 (例えば readData、WriteData など) を指します。
- [AccessList] (アクセスリスト) は、オブジェクトに対してリクエストされた、または許可されたアクセスを指します。詳細については、下記の表および Microsoft のドキュメント (「イベント 4556」など) を参照してください。

アクセスタイプ	アクセスマスク	値
データまたはリストディレクトリの読み取り	0x1	%%4416
データの書き込みまたはファイルの追加	0x2	%%4417
データの付加またはサブディレクトリの追加	0x4	%%4418
拡張属性の読み取り	0x8	%%4419
拡張属性の書き込み	0x10	%%4420
実行 / トラバース	0x20	%%4421
子の削除	0x40	%%4422
属性の読み取り	0x80	%%4423
属性の書き込み	0x100	%%4424
削除	0x10000	%%1537
ACL の読み取り	0x20000	%%1538
ACL の書き込み	0x40000	%%1539
所有者の書き込み	0x80000	%%1540
同期	0x100000	%%1541
セキュリティ ACL にアクセスする	0x1000000	%%1542

以下は、実例を挙げたいくつかのキーイベントです。XML は読みやすさい形式にフォーマットされていることに注意してください。

イベント ID 4660 は、オブジェクトが削除されたときにログに記録されます。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

イベント ID 4659 は、ファイルの削除リクエストでログに記録されます。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
```

```
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

イベント ID 4663 は、オブジェクトに対して特定の操作が実行されたときにログに記録されます。次の例はファイルからのデータの読み取りを示しており、これは AccessList %%4416 で解釈されます。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

次の例はファイルからのデータの書き込み/付加を示しており、これは AccessList %%4417 で解釈されます。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
```

```
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

イベント ID 4656 は、オブジェクトに対して特定のアクセスがリクエストされたことを示します。次の例では、0x8010000000000000 の Keywords 値で確認できる通り、ObjectName「permtest」に対して読み取りリクエストが開始され、失敗した試行となっています。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
```

```
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

イベント ID 4670 は、オブジェクトの許可が変更された際にログに記録されます。
次の例は、ユーザー「admin」が ObjectName「permtest」に対する許可を変更して、SID「S-1-5-21-658495921-4185342820-3824891517-1113」にアクセス許可を追加したことを示しています。アクセス許可の解釈方法の詳細については、Microsoft のドキュメントを参照してください。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

イベント ID 5140 は、ファイル共有にアクセスするたびにログに記録されます。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
```

```
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

イベント ID 5145 は、ファイル共有レベルでアクセスが拒否されたときにログに記録されます。次の例は、ShareName「demosshare01」へのアクセスが拒否されたことを示しています。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

CloudWatch Logs Insights を使用してログデータを検索する場合は、次の例に示すように、イベントフィールドに対してクエリを実行できます。

- 特定のイベント ID をクエリするには。

```
fields @message
   | filter @message like /4660/
```

- 特定のファイル名と一致するすべてのイベントをクエリするには。

```
fields @message
   | filter @message like /event.txt/
```

CloudWatch Logs Insights の問い合わせ言語の詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「[Analyzing Log Data with CloudWatch Logs Insights]」(CloudWatch Logs Insights によるログデータ分析) を参照してください。

ファイルとフォルダの監査コントロールの設定

ユーザーアクセスの試行を監査するファイルおよびフォルダーに、監査コントロールを設定する必要があります。監査コントロールは、NTFS システムアクセスコントロールリスト (SACL) とも呼ばれます。

監査コントロールは、Windows ネイティブ GUI インターフェイスを使用するか、プログラムで Windows PowerShell コマンドを使用して設定します。継承が有効になっている場合は通常、アクセスをログに記録する最上位フォルダに対してのみ監査コントロールを設定する必要があります。

Windows GUI を使用した監査アクセスの設定

GUI を使用してファイルとフォルダーに監査コントロールを設定するには、Windows ファイルエクスプローラを使用します。特定のファイルまたはフォルダで、Windows ファイルエクスプローラを開き、[Properties] (プロパティ) > [Security] (セキュリティ) > [Advanced] (詳細設定) > Auditing] (監査) タブを選択します。

次の監査コントロールの例では、フォルダの成功したイベントを監査します。Windows イベントログエントリは、そのハンドルが読み取りのため、管理者ユーザーによって正常に開かれるたびに発行されます。

[Type] (タイプ) フィールドは、監査するアクションを示します。成功した試みを監査するにはこのフィールドを [Success] (成功) に、失敗した試みを監査するには [Fail] (失敗) に、成功と失敗の両方の試みを監査するには [All] (すべて) に設定します。

監査エントリフィールドの詳細については、Microsoft ドキュメントの「ファイルまたはフォルダに基本的な監査ポリシーを適用する」を参照してください。

PowerShell コマンドを使用した監査アクセスの設定

Microsoft Windows `Set-Acl` コマンドを使用して、任意のファイルまたはフォルダで監査 SACL を設定できます。このコマンドの設定の詳細については、「Microsoft の Set-Acl ドキュメント」を参照してください。

以下は、一連の PowerShell コマンドと可変を使用して、正常な試行に監査アクセスを設定する例になります。これらのサンプルコマンドは、ユーザーのファイルシステムのニーズに合わせて調整できます。

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List
```

```
$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

ファイルアクセス監査の管理

新しい Amazon FSx for Windows File Server のファイルシステムを作成する際に、ファイルアクセス監査を有効にできます。Amazon FSx コンソールからファイルシステムを作成すると、ファイルアクセス監査はデフォルトでオフになります。

ファイルアクセス監査が有効になっている既存のファイルシステムでは、ファイルおよびファイル共有アクセスのアクセス試行の種類変更や、監査イベントログの宛先など、ファイルアクセス監査の設定を変更できます。これらのタスクは、Amazon FSx コンソール AWS CLI、または API を使用して実行できます。

> **Note**
>
> ファイルアクセス監査は、32 MBps 以上のスループットキャパシティを持つ Amazon FSx for Windows File Server のファイルシステムでのみサポートされます。ファイルアクセス監査が有効になっている場合、32 MBps 未満のスループットキャパシティを持つファイルシステムを作成または更新することはできません。スループットキャパシティは、ファイルシステムを作成した後いつでも変更できます。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。

ファイルシステムの作成時にファイルアクセス監査を有効にするには (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. 「開始方法」セクションの「ステップ 5. ファイルシステムを作成」で説明されている新しいファイルシステムを作成するための手順に従います。
3. 監査 - オプション セクションを開きます。ファイルアクセスの監査は、デフォルトで無効になっています。

4. ファイルアクセス監査を有効にして設定するには、次の手順を実行します。
   - ファイルやフォルダへのアクセスログを記録する には、成功および / または失敗した試行のロギングを選択します。選択しないと、ファイルとフォルダのロギングは無効になります。
   - ファイル共有へのアクセスを記録する には、成功および/または失敗した試行のロギングを選択します。選択しないと、ファイル共有のロギングは無効になります。
   - [監査イベントログの宛先を選択する] には、[CloudWatch Logs] または [Firehose] を選択します。次に、既存のログまたは配信ストリームを選択するか、新しいログまたは配信ストリームを作成します。CloudWatch Logs の場合、Amazon FSx は CloudWatch Logs `/aws/fsx/windows` ロググループでデフォルトのログストリーミングを作成して使用します。

以下は、エンドユーザーによるファイル、フォルダ、およびファイル共有への成功および失敗したアクセス試行を監査する、ファイルアクセス監査設定の例になります。監査イベントログは、デフォルトの CloudWatch Logs `/aws/fsx/windows` ロググループの宛先に送信されます。

5. ファイルシステム作成ウィザードの次のセクションに進みます。

ファイルシステムが [Available] (利用可能) の場合は、ファイルアクセス監査機能が有効になります。

ファイルシステムの作成時にファイルアクセス監査を有効にするには (CLI)

1. 新しいファイルシステムを作成する場合は、CreateFileSystem API オペレーションで `AuditLogConfiguration` プロパティを使用し、新しいファイルシステムのファイルアクセス監査を有効にします。

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

2. ファイルシステムが [Available] (利用可能) の場合は、ファイルアクセス監査機能が有効になります。

ファイルアクセス監査の設定を変更するには (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. [Files systems] (ファイルシステム) に移動し、ファイルアクセス監査を管理する Windows 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. [File Access Auditing] (ファイルアクセスの監査) パネルで、[Manage] (管理) を選択します。

5. [Manage file access auditing settings] (ファイルアクセス監査設定の管理) ダイアログで、希望の設定を変更します。

- ファイルやフォルダへのアクセスログを記録する には、成功および / または失敗した試行のロギングを選択します。選択しないと、ファイルとフォルダのロギングは無効になります。
- ファイル共有へのアクセスを記録する には、成功および/または失敗した試行のロギングを選択します。選択しないと、ファイル共有のロギングは無効になります。
- [監査イベントログの宛先を選択する] には、[CloudWatch Logs] または [Firehose] を選択します。次に、既存のログまたは配信ストリームを選択するか、新しいログまたは配信ストリームを作成します。

6. [Save] (保存) を選択します。

ファイルアクセス監査設定を変更するには (CLI)

- `update-file-system` CLI コマンドまたは同等の `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 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Amazon FSx for Windows File Server の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に FSx for Windows File Server リソースの使用を許可する (アクセス許可を付与する) かを制御します。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

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon FSx for Windows File Server と IAM の連携の仕組み
- Amazon FSx for Windows File Server のアイデンティティベースのポリシー例
- AWS Amazon FSx for Windows File Server の マネージドポリシー
- Amazon FSx for Windows File Server のアイデンティティとアクセスのトラブルシューティング
- Amazon FSx でのタグの使用
- FSx for Windows File Server のサービスにリンクされたロールの使用

対象者

AWS Identity and Access Management (IAM) の使用方法は、FSx for Windows File Server で行う作業によって異なります。

サービスユーザー – FSx for Windows File Server サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が提供されます。さらに多くの FSx for Windows File Server 機能を使用して作業を行う場合は、追加のアクセス許可が必要になる場合があります。アクセスの

管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。FSx for Windows File Server の機能にアクセスできない場合は、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の FSx for Windows File Server リソースを担当している場合は、通常、FSx for Windows File Server へのフルアクセスがあります。サービスユーザーがどの FSx for Windows File Server の機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。FSx for Windows File Server で IAM を使用する方法の詳細については、「」を参照してくださいAmazon FSx for Windows File Server と IAM の連携の仕組み。

IAM 管理者 – IAM 管理者は、FSx for Windows File Server へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる FSx for Windows File Server 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、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティベースのポリシー例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、、AWS Directory Serviceアイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的

な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー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 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「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 ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサー

ビス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM 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。

- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」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 AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は 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。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「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。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所

有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。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 Windows File Server と IAM の連携の仕組み

IAM を使用して FSx for Windows File Server へのアクセスを管理する前に、FSx for Windows File Server で使用できる IAM 機能について説明します。

Amazon FSx for Windows File Server で使用できる IAM の機能

IAM の機能	FSx のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	いいえ
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	はい
転送アクセスセッション	はい
サービスロール	いいえ
サービスリンクロール	はい

FSx およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

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 ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。ID ベースの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。プリンシパルは、それが添付されている

ユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

FSx のアイデンティティベースのポリシー例

FSx for Windows File Server 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、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティベースのポリシー例。

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

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。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。

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。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

FSx のアクションの一覧を確認するには、サービス認可リファレンスの「Amazon FSx for Windows File Server で定義されるアクション」を参照してください。

FSx のポリシーアクションでは、アクションの前に以下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"
         ]
```

FSx for Windows File Server 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、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティベースのポリシー例。

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。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限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": "*"
```

FSx リソースのタイプとその ARN の一覧を確認するには、サービス認可リファレンスの「Amazon FSx for Windows File Server によって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 を指定するためのアクションについては、「Amazon FSx for Windows File Server で定義されるアクション」を参照してください。

FSx for Windows File Server 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、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティベースのポリシー例。

FSx 向け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 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、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。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS では `AND` 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理`OR`オペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。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。

FSx 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「Amazon FSx for Windows File Server の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「Amazon FSx for Windows File Server で定義されるアクション」を参照してください。

FSx for Windows File Server 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、「」を参照してくださいAmazon FSx for Windows File Server のアイデンティティベースのポリシー例。

FSx の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

FSx での 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、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) と多くの AWS リソースにタグをアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。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。

FSx での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する場合などの詳細については、IAM ユーザーガイドの「IAM AWS のサービス と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 の一時的セキュリティ認証情報」を参照してください。

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

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

FSx のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

> **Warning**
> サービスロールのアクセス許可を変更すると、FSx の機能が阻害される可能性があります。FSx が指示する場合にのみ、サービスロールを編集します。

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、編集することはできません。

FSx for Windows File Server 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、「」を参照してください[FSx for Windows File Server のサービスにリンクされたロールの使用](#)。

Amazon FSx for Windows File Server のアイデンティティベースのポリシー例

デフォルトでは、ユーザーとロールには FSx for Windows File Server リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「[IAM ポリシーを作成する (コンソール)](#)」を参照してください。

リソースタイプごとの ARN の形式を含む、FSx で定義されるアクションとリソースタイプの詳細については、サービス認可リファレンスの「[Amazon FSx for Windows File Server のアクション、リソース、および条件キー](#)」を参照してください。

トピック

- [ポリシーに関するベストプラクティス](#)
- [FSx コンソールの使用](#)

- 自分の権限の表示をユーザーに許可する

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、アカウントで FSx for Windows File Server リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – 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。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、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 AWS 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 Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer 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。

FSx コンソールの使用

Amazon FSx for Windows File Server コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、 の FSx for Windows File Server 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 FSx コンソールを使用できるようにするには、FSx `AmazonFSxConsoleReadOnlyAccess` AWS 管理ポリシーもエンティティにアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

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": "*"
        }
    ]
}
```

AWS Amazon FSx for Windows File Server 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、「FSx for Windows File Server のサービスにリンクされたロールの使用」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、「FSx for Windows File Server のサービスにリンクされたロールの使用」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 AWS Directory Service ディレクトリに関する情報を表示できるようにします。
- `ec2`
  - プリンシパルが指定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 Management Console。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `fsx` – プリンシパルに、Amazon FSx マネジメントコンソールのすべてのアクション (`BypassSnaplockEnterpriseRetention` を除く) を実行することを許可します。
- `cloudwatch` – プリンシパルが、Amazon FSx マネジメントコンソールで CloudWatch 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 AWS Directory Service ディレクトリに関する情報を一覧表示できるようにします。
- `ec2`
  - プリンシパルが、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。

  - プリンシパルが 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るようにします。
  - プリンシパルが Amazon FSx ファイルシステムに関連付けられた Elastic Network Interface を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)。
- `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への読み取り専用アクセス許可を付与します AWS Management Console。

アクセス許可の詳細

このポリシーには、以下の許可が含まれています。

- `fsx` - プリンシパルが Amazon FSx マネジメントコンソールで、すべてのタグを含む Amazon FSx ファイルシステムに関する情報を表示できるようにします。
- `cloudwatch` – プリンシパルが、Amazon FSx マネジメントコンソールで CloudWatch 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 AWS Directory Service ディレクトリに関する情報を表示できるようにします。
- `ec2`
  - 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。

  - プリンシパルが 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るようにします。
  - プリンシパルが Amazon FSx ファイルシステムに関連付けられた Elastic Network Interface を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。
- `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 ドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
AmazonFSxServiceRolePolicy— 既存のポリシーへの更新	Amazon FSx は、プリンシパル`ec2:AssignIpv6Addresses` 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を追加しました。	2025 年 7 月 22 日
AmazonFSxServiceRolePolicy - 既存のポリシーへの更新	Amazon FSx は、プリンシパル`ec2:UnassignIpv6Addresses` 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が追加されました。`fsx:CreateAndAttachS3AccessPoint` 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	2025 年 6 月 25 日

変更	説明	日付
	を追加 AWS アカウント しました AWS リージョン。	
AmazonFSxConsoleFullAccess - 既存のポリシーへの更新	Amazon FSx は、プリンシパル`fsx:DetachAndDeleteS3AccessPoint` が S3 アクセスポイントを削除できるようにする新しいアクセス許可を追加しました。	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が追加されました。`fsx:CreateAndAttachS3AccessPoint` 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 に新しいアクセス許可が追加されました。`fsx:DescribeS3AccessPointAttachments` これにより、プリンシパルは 内のすべての S3 アクセスポイントを AWS アカウント に一覧表示できます 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 は、プリンシパル`fsx:DetachAndDeleteS3AccessPoint` が S3 アクセスポイントを削除できるようにする新しいアクセス許可を追加しました。	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が追加されました。`ec2:DescribeNetworkInterfaces` 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が追加されました。`ec2:DescribeNetworkInterfaces` 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 ログのロググループ、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 ロン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 FSx for Windows File Server のアイデンティティとアクセスのトラブルシューティング

次の情報は、FSx for Windows File Server と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- FSx でアクションを実行する権限がない
- 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 FSx リソース AWS アカウント へのアクセスを許可したい

FSx でアクションを実行する権限がない

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 FSx for Windows File Server にロールを渡すことができ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、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 という IAM ユーザーがコンソールを使用して `marymajor` FSx for Windows File Server でアクションを実行しようとすると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
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 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:

- FSx for Windows File Server がこれらの機能をサポートしているかどうかを確認するには、「」を参照してください[Amazon FSx for Windows File Server と IAM の連携の仕組み](#)。
- 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 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制御したり、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。ユーザーは、作成時に Amazon FSx リソースにタグを適用する権限を持っている必要があります。

リソース作成時にタグ付けするアクセス許可の付与

一部のリソース作成 FSx for Windows File Server 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「AWSの ABAC とは」を参照してください。

ユーザーが作成時にリソースにタグを付けることができるようにするには、`fsx:CreateFileSystem` や `fsx:CreateBackup` などのリソースを作成するアクションを使用するためのアクセス許可が必要です。タグがリソース作成アクションで指定されている場合、Amazon は `fsx:TagResource` アクションで追加の認可を実行してユーザーがタグを作成するアクセス許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権限が必要です。

次の例は、特定の での作成時に、ユーザーがファイルシステムを作成し、ファイルシステムにタグを適用できるようにするポリシーを示しています AWS アカウント。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

同様に、次のポリシーにより、ユーザーは特定のファイルシステムにバックアップを作成し、バックアップの作成中に任意のタグをバックアップに適用できます。

```
{
  "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、リソース作成アクション中にタグが適用された場合にのみ評価されます。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っているユーザー (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、ユーザーがタグを使用して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 FSx リソースへのアクセスをコントロールするためには「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。

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 リソースとアクションへのアクセスを制御するには、タグに基づいて AWS Identity and Access Management (IAM) ポリシーを使用できます。コントロールは 2 つの方法で提供できます。

1. 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します。
2. IAM リクエストの条件でどのタグを渡せるかをコントロールする。

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、「リソース作成時にタグ付けするアクセス許可の付与」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することが必要な場合があります。

Example ポリシー - 特定のタグを指定するときに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バリューのペア (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 - 特定のタグを持つ Amazon FSx ファイルシステムのみでバックアップを作成する

このポリシーにより、ユーザーはキーと値のペア `key=Department, value=Finance` でタグ付けされたファイルシステムのみでバックアップを作成でき、バックアップはタグ `Deparment=Finance` 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:file-system/*",
            "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 - 特定のタグを持つバックアップから特定のタグを持つ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、`Department=Finance` でタグ付けされたバックアップからのみ `Department=Finance` でタグ付けされたファイルシステムを作成できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
```

```
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example ポリシー - 特定のタグを持つファイルシステムを削除する

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"
                }
            }
        }
    ]
}
```

FSx for Windows File Server のサービスにリンクされたロールの使用

Amazon FSx for Windows File Server 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。サービスにリンクされたロールは、FSx for Windows File Server に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、FSx for Windows File Server 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、必要なアクセス許可を手動で追加する必要がなくなるため、FSx for Windows File Server の設定が簡単になります。FSx for Windows File Server は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、FSx for Windows File Server のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチ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、最初に関連リソースを削除する必要があります。これにより、リソースへのアクセス許可が誤って削除されないため、FSx for Windows File Server リソースが保護されます。

サービスにリンクされた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」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。サービスにリンクされた役割に関するドキュメントをサービスで表示するには[はい] リンクを選択してください。

FSx for Windows File Server のサービスにリンクされたロールのアクセス許可

FSx for Windows File Server 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の Elastic Network Interface の作成など、アカウントで特定のアクションを実行します。

ロールのアクセス許可ポリシーにより、FSx for Windows File Server は該当するすべての AWS リソースに対して次のアクションを実行できます。

IAM エンティティに AmazonFSxServiceRolePolicy をアタッチすることはできません。このポリシーは、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サービスにリンクされたロールにアタッチされます。詳細については、「FSx for Windows File Server のサービスにリンクされたロールの使用」を参照してください。

このポリシーの更新については、「AmazonFSxServiceRolePolicy」を参照してください

このポリシーは、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管理アクセス許可を付与します。

アクセス許可の詳細

AmazonFSxServiceRolePolicy 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。AmazonFSxServiceRolePolicy には次のアクセス許可があります。

> **Note**
>
> AmazonFSxServiceRolePolicy 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。記載されているアクセス許可の一部は、FSx for Windows には適用されない場合があります。

- `ds` – FSx が AWS 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` - 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` – 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` - FSx に Amazon VPC をプライベートホストゾーンに関連付けることを許可します。
- `logs` - FSx が CloudWatch Logs のログストリームを記述して書き込むことを許可します。これは、ユーザーが FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを CloudWatch Logs ストリーミングに送信できるようにするためです。
- `firehose` - FSx に Amazon Data Firehose 配信ストリームを記述して書き込むことを許可します。これは、ユーザーが FSx for Windows File Server ファイルシステムのファイルアクセス監査ログを Amazon Data Firehose 配信ストリームに公開できるようにするためです。

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"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
```

```
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

本ポリシーの更新については、AWS マネージドポリシーに対する Amazon FSx の更新 に記載されています。

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) 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「サービスリンクロールの許可」を参照してください。

FSx for Windows File Server のサービスにリンクされたロールの作成

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。 AWS Management Console、IAM CLI、または IAM API でファイルシステムを作成すると、FSx for Windows File Server 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。ファイルシステムを作成すると、FSx for Windows File Server によってサービスにリンクされたロールが再度作成されます。

FSx for Windows File Server のサービスにリンクされたロールの編集

FSx for Windows File Server では、サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照す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。

FSx for Windows File Server のサービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、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と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 FSx for Windows File Server サービスが ロールを使用している場合、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

サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。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。

FSx for Windows File Server サービスリンクロールでサポートされているリージョン

FSx for Windows File Server 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ています。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 for Windows File Server のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスAWS のサービス プログラムによる対象範囲内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 「 Compliance ProgramsAssurance」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 AWS Artifact Reports 」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と場所に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、セキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅

威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。

- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon FSx for Windows File Server およびインターフェイス VPC エンドポイント

インターフェイス VPC エンドポイントを使用するように Amazon FSx を設定することで、VPC のセキュリティ体制を強化できます。インターフェイス VPC エンドポイントは、インターネットゲートウェイAWS PrivateLink、NAT デバイス、VPN 接続、 AWS Direct Connect 接続のいずれも必要とせずに Amazon FSx APIs にプライベートにアクセスできるテクノロジーである を利用しています。VPC のインスタンスは、パブリック IP アドレスがなくても Amazon FSx API と通信できます。VPC と Amazon FSx 間のトラフィックは、 AWS ネットワークを離れません。

各インターフェイス VPC エンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。ネットワークインターフェイスは、Amazon FSx API へのトラフィックのエントリポイントとなるプライベート IP アドレスを提供します。Amazon FSx 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「Creating an interface VPC endpoint」(インターフェイス VPC エンドポイントの作成) を参照してください。

Amazon FSx インターフェイス VPC エンドポイントに関する考慮事項

Amazon FSx のインターフェイス VPC エンドポイントを設定する前に、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプロパティと制限」を確認してください。

VPC から任意の Amazon FSx API オペレーションを呼び出すことができます。例えば、VPC 内で CreateFileSystem API を呼び出すことで、FSx for Windows File Server ファイルシステムを作成できます。Amazon FSx API の詳細なリストについては、「Amazon FSx API Reference」(Amazon FSx API リファレンス) の「Actions」(アクション) を参照してください。

VPC ピアリングに関する考慮事項

他の VPC には、インターフェイス VPC エンドポイントを使用して、VPC ピアリングによって接続できます。VPC ピアリングは2 つの VPC 間のネットワーク接続です。自分が所有者である 2 つの

VPC 間や、他の AWS アカウントアカウント内の VPC との間で、VPC ピアリング接続を確立できます。VPCs 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「Creating an interface VPC endpoint」(インターフェイス VPC エンドポイントの作成) を参照してください。

Amazon FSx のインターフェイス VPC エンドポイントを作成するには、次のいずれかを使用します。

- **`com.amazonaws.`*`region`*`.fsx`** – Amazon FSx API オペレーションのエンドポイントを作成します。
- **`com.amazonaws.`*`region`*`.fsx-fips`** — 連邦情報処理規格 (FIPS) 140-2 に準拠した Amazon FSx API のエンドポイントを作成します。

オプションとしてプライベート DNS を使用するには、VPC の `enableDnsHostnames` および `enableDnsSupport` 属性を設定する必要があります。詳細については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性の表示と更新」を参照してください。

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、 のデフォルト DNS 名を使用して VPC エンドポイントで Amazon FSx に API リクエストを行うことができます。たとえば AWS リージョン、 ですfsx.us-east-1.amazonaws.com。中国 (北京) と中国 (寧夏) では AWS リージョン、fsx-api.cn-northwest-1.amazonaws.com.cnそれぞれ fsx-api.cn-north-1.amazonaws.com.cnと を使用して VPC エンドポイントで API リクエストを行うことができます。

詳細については、「Amazon VPC ユーザーガイド」の「Accessing a service through an interface VPC endpoint」(インターフェイス VPC エンドポイントを介したサービスへのアクセス) を参照してください。

Amazon FSx 用の VPC エンドポイントポリシーの作成

Amazon FSx API へのアクセスをさらに制御するには、オプションで AWS Identity and Access Management (IAM) ポリシーを VPC エンドポイントにアタッチできます。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 エンドポイントによるサービスのアクセスコントロール」を参照してください。

他の サービスでの使用

Amazon CloudWatch、 AWS Identity and Access Management AWS CloudTrail、および に加えて AWS DataSync、FSx for Windows File Server は以下とも統合されます AWS のサービス。

- Amazon AppStream 2.0 – AppStream 2.0 は、デスクトップアプリケーションに即座にアクセスできるようにする、完全マネージド型のアプリケーションストリーミングサービスです。AppStream 2.0 は、アプリケーションのホストと実行に必要な AWS リソースを管理し、自動的にスケーリングして、オンデマンドでユーザーにアクセスできるようにします。AppStream 2.0 を使用して、個々のユーザー用の永続ストレージを作成し、FSx for Windows File Server ファイルシステム上の多くのユーザー間でストレージを共有する方法について説明します。詳細については、「Amazon AppStream 2.0 で Amazon FSx を使用する」を参照してください。
- Amazon Kendra – Amazon Kendra は、自然言語処理と高度な機械学習アルゴリズムを使用して、データから検索に関する質問に対する特定の回答を返すインテリジェントな検索サービスです。Amazon Kendra では、複数のデータリポジトリをインデックスに接続し、ドキュメントを取り込んでクローリングすることにより、統一された検索エクスペリエンスを実現できます。FSx for Windows File Server での Amazon Kendra の使用の詳細については、「Amazon Kendra で FSx for Windows ファイルサーバーを使用する」を参照してください。

トピック

- Amazon AppStream 2.0 で Amazon FSx を使用する
- Amazon Kendra で FSx for Windows ファイルサーバーを使用する

Amazon AppStream 2.0 で Amazon FSx を使用する

Server Message Block (SMB) プロトコルをサポートすることで、Amazon FSx for Windows File Server はAmazon EC2、VMware Cloud on、 AWS Amazon WorkSpaces、Amazon AppStream 2.0 インスタンスからのファイルシステムへのアクセスをサポートします。AppStream 2.0 は、フルマネージド型アプリケーションストリーミングサービスです。AppStream 2.0 でデスクトップアプリケーションを一元管理し、どのコンピュータのブラウザにも安全に配信することができます。AppStream 2.0 の詳細については、「Amazon AppStream 2.0 管理ガイド」を参照してください。Amazon AppStream 2.0 イメージとフリートの管理を効率化する方法については、 AWS ブログ記事「カスタマイズされた AppStream 2.0 Windows イメージを自動的に作成」を参照してください。

次の手順では、Amazon FSx を AppStream 2.0 で使用する方法と、各ユーザーに個人用永続ストレージを提供し、複数のユーザーが共通のファイルにアクセスできるように共有フォルダを提供する方法を示します。

個人用の永続的ストレージを各ユーザーに提供する

Amazon FSx を使用すると、AppStream 2.0 ストリーミングセッション内で組織内のすべてのユーザーに固有のストレージドライブを提供できます。ユーザーには、自分のフォルダのみへのアクセス許可が付与されます。ドライブはストリーミングセッションのスタートに自動的にマウントされ、ドライブに追加または更新されたファイルは、ストリーミングセッション間で自動的に保持されます。

このタスクを完了するには、3 つの手順を実行する必要があります。

Amazon FSx を使用してドメインユーザーのホームフォルダを作成するには

1. Amazon FSx ファイルシステムを作成します。詳細については、「Amazon FSx for Windows File Server の開始方法」を参照してください。
2. ファイルシステムが使用可能になったら、Amazon FSx ファイルシステム内のすべてのドメイン AppStream 2.0 ユーザー用のフォルダを作成します。次の例では、ユーザーのドメインユーザー名を、対応するフォルダの名前として使用します。これを行うと、Windows 環境可変 `%username%` を使用して、マッピングするファイル共有の UNC 名を容易に構築することができます。
3. これらの各フォルダを共有フォルダとして共有します。詳細については、「ファイル共有の作成、更新、削除」を参照してください。

ドメインに接続している AppStream 2.0 Image Builder を起動するには

1. AppStream 2.0 コンソール (https://console.aws.amazon.com/appstream2) にサインインします。
2. ナビゲーションメニューから [Directory Configs] (ディレクトリ設定) を選択し、ディレクトリ設定オブジェクトを作成します。詳細については、「Amazon AppStream 2.0 管理ガイド」の「AppStream2.0 でアクティブディレクトリを使用する」を参照してください。
3. [Images] (イメージ)、[Image Builder] を選択し、新しい Image Builder を起動します。
4. Image Builder の起動ウィザードで以前に作成したディレクトリ設定オブジェクトを選択して、Image Builder をアクティブディレクトリのドメインに結合させます。
5. Amazon FSx ファイルシステムと同じ VPC で Image Builder を起動します。Image Builder は、Amazon FSx ファイルシステムが結合されているのと同じ AWS Managed Microsoft AD

ディレクトリに関連付けてください。Image Builder に関連付ける VPC セキュリティグループは、Amazon FSx ファイルシステムへのアクセスを許可する必要があります。

6. Image Builder が使用可能になったら、Image Builder に接続し、ドメイン管理者アカウントを使用してログインします。
7. アプリケーションをインストールします。

Amazon FSx ファイル共有を AppStream 2.0 にリンクするには

1. Image Builder で、次のコマンドを使用してバッチスクリプトを作成し、既知のファイルの場所 (C:\Scripts\map-fs.bat など) に保存します。次の例では、S: をドライブ文字として使用し、Amazon FSx ファイルシステム上の共有フォルダをマッピングします。このスクリプティングでは、Amazon FSx ファイルシステムの DNS 名またはファイルシステムに関連付けられた DNS エイリアスを使用します。このエイリアスは、Amazon FSx コンソールのファイルシステムの詳細ビューから取得できます。

   ファイルシステムの DNS 名を使用している場合は、次の手順を実行します。

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   ファイルシステムに関連付けられた DNS エイリアスを使用している場合は、次の手順を実行します。

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```

2. PowerShell プロンプトを開き、`gpedit.msc` を実行します。
3. ユーザー設定から [Windows 設定]、[Logon] (ログオン) の順に選択します。
4. この手順の最初のステップで作成したバッチスクリプティングに移動し、それを選択します。
5. コンピュータ設定から、[Windows Administrative Templates] (Windows 管理テンプレート)、[System] (システム)、[Group Policy] (グループポリシー) の順に選択します。
6. [Configure Logon Script delay] (ログオンスクリプト遅延の設定) ポリシーを選択します。ポリシーを有効にして、時間遅延を `0` に引き下げます。この設定は、ユーザーがストリーミングセッションをスタートした際に、すぐにユーザーログオンスクリプトが実行されるようにするのに役立ちます。

7. イメージを作成し、AppStream 2.0 フリートに割り当てます。AppStream 2.0 フリートが Image Builder で使用したものと同じアクティブディレクトリのドメインに接続していることを確認します。Amazon FSx ファイルシステムで使用されているものと同じ VPC でフリートを起動します。フリートに関連付ける VPC セキュリティグループは、Amazon FSx ファイルシステムへのアクセスを提供する必要があります。
8. SAML SSO を使用してストリーミングセッションを起動します。アクティブディレクトリに接続しているフリートに接続するには、SAML プロバイダーを使用してシングルサインオンフェデレーションを設定します。詳細については、「Amazon AppStream 2.0 管理ガイド」の「SSAML2.0 を使用した AppStream2.0 へのシングルサインオンアクセス」を参照してください。
9. Amazon FSx ファイル共有は、ストリーミングセッション内の S: ドライブ文字にマッピングされます。

ユーザー間で共有フォルダを提供する

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、すべてのユーザーが必要とする共通ファイル (デモファイル、コード例、取扱説明書など) を管理するために使用できます。

このタスクを完了するには、3 つの手順を実行する必要があります。

Amazon FSx を使用して共有フォルダーを作成するには

1. Amazon FSx ファイルシステムを作成します。詳細については、「Amazon FSx for Windows File Server の開始方法」を参照してください。
2. すべての Amazon FSx ファイルシステムには、デフォルトで共有フォルダが含まれており、DNS エイリアスを使用している場合は、*file-system-DNS-name*\share または *fqdn-DNS-alias*\share というアドレスを使用してアクセスできます。デフォルトの共有を使用することも、別の共有フォルダを作成することもできます。詳細については、「ファイル共有の作成、更新、削除」を参照してください。

AppStream 2.0 Image Builder を起動する

1. AppStream 2.0 コンソールから、新しい Image Builder を起動するか、既存の Image Builder に接続します。Amazon FSx ファイルシステムで使用されているものと同じ VPC で Image Builder を起動します。Image Builder に関連付ける VPC セキュリティグループは、Amazon FSx ファイルシステムへのアクセスを許可する必要があります。

2. Image Builder が使用可能になったら、管理者ユーザーとして Image Builder に接続します。
3. アプリケーションを管理者としてインストールまたは更新します。

共有フォルダを AppStream 2.0 にリンクするには

1. 前の手順で説明したように、ユーザーがストリーミングセッションを起動したときに共有フォルダを自動的にマウントするバッチスクリプティングを作成します。スクリプティングを完了するには、ファイルシステムの DNS 名またはファイルシステムに関連付けられた DNS エイリアス (Amazon FSx コンソールのファイルシステムの詳細ビューから取得できます)、および共有フォルダにアクセスするための認証情報が必要です。

   ファイルシステムの DNS 名を使用している場合は、次の手順を実行します。

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   ファイルシステムに関連付けられた DNS エイリアスを使用している場合は、次の手順を実行します。

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. グループポリシーを作成して、ユーザーのログオンごとにこのバッチスクリプティングを実行します。前のセクションで説明したように、同じ手順に従うことができます。
3. イメージを作成し、フリートに割り当てます。
4. ストリーミングセッションを起動します。ドライブ文字に自動的にマッピングされた共有フォルダが表示されます。

Amazon Kendra で FSx for Windows ファイルサーバーを使用する

Amazon Kendra は、高精度かつインテリジェントな検索サービスです。FSx for Windows ファイルサーバーのファイルシステムを Amazon Kendra のデータソースとして使用できます。これにより、

ファイルシステムに保存されているドキュメントに含まれる情報のインデックス作成とインテリジェントな検索が可能になります。

- Amazon Kendra の詳細については、「Amazon Kendra デベロッパーガイド」の「What is Amazon Kendra」(Amazon Kendra の概要) を参照してください。
- Amazon Kendra データソースとしてファイルシステムを追加する方法の詳細については、「Amazon Kendra デベロッパーガイド」の「Amazon FSx データソースの開始方法 (コンソール)」を参照してください。
- Amazon Kendra の詳細については、Amazon Kendra ウェブサイトを参照してください。
- Amazon Kendra を使用してファイルシステムを検索する方法のチュートリアルについては、「AWS 機械学習ブログ」の「Amazon FSx for Windows File Server の Amazon Kendra コネクタを使用して、Windows ファイルシステムの非構造データを安全に検索する」を参照してください。

ファイルシステムのパフォーマンス

FSx for Windows ファイルサーバーのファイルシステムをデータソースとして追加すると、Amazon Kendra はファイルシステム上のファイルとフォルダーを定期的に同期頻度でクローリングし、検索インデックスを作成および維持します。(統合を確立するときに、同期頻度を選択できます。) Amazon Kendra からのこのファイルアクセスアクティビティは、ファイルシステムにアクセスするユーザー独自のワークロードからのアクティビティと同様に、ファイルシステムリソースを消費します。

ワークロードのパフォーマンスに影響を与えないように、ファイルシステムが十分なリソースで設定されていることを確認してください。具体的には、多数のファイルのインデックスを作成する場合は、SSD ストレージタイプのファイルシステムを使用することをお勧めします。これにより、ストレージボリュームにアクセスする必要のあるリクエストの最大スループットと IOPS レベルが高くなります。Amazon FSx パフォーマンスモデルの詳細については、「FSx for Windows File Server のパフォーマンス」を参照してください。

クォータ

以下で、Amazon FSx for Windows File Server を使用する場合のクォータについて説明します。

トピック

- 増やすことができるクォータ
- ファイルシステムあたりのリソースクォータ
- 追加の考慮事項
- Microsoft Windows 固有のクォータ

増やすことができるクォータ

以下は、引き上げることができる AWS アカウント各 の Amazon FSx for Windows File Server AWS リージョンのクォータです。

リソース	デフォルト	説明
Windows ファイルシステム	100	このアカウントで作成できる Amazon FSx for Windows サーバーのファイルシステムの最大数。
Windows スループット容量	10240	このアカウントのすべての Amazon FSx for Windows ファイルシステムで許可されるスループット容量の合計 (MBps 単位)。
Windows HDD ストレージ容量	524288	このアカウントのすべての Amazon FSx for Windows File Server のシステムで許可される HDD ストレージ容量 (GiB 単位) の最大容量。
Windows SSD ストレージ容量	524288	このアカウントのすべての Amazon FSx for Windows File

リソース	デフォルト	説明
		Server のシステムで許可される SSD ストレージ容量 (GiB 単位) の最大容量。
Windows 合計 SSD IOPS	500,000	このアカウントのすべての Amazon FSx for Windows File Server ファイルシステムに対して許可される SSD IOPS の合計量。
Windows バックアップ	500	このアカウントで保持できるすべての Amazon FSx for Windows File Server ファイルシステムの最大ユーザー起動バックアップ数。

クォータの増加をリクエストするには

1. Service Quotas コンソール を開きます。
2. ナビゲーションペインで、AWS サービス を選択します。
3. Amazon FSx を選択します。
4. クォータを選択します。
5. [Request quota increase] (クォータ引き上げリクエスト) を選択して、指示に従ってクォータの引き上げをリクエストします。
6. クォータリクエストのステータスを表示するには、コンソールのナビゲーションペインの [Quota request history] (クォータ依頼履歴) を選択します。

詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

ファイルシステムあたりのリソースクォータ

以下は、 AWS リージョン内の各ファイルシステムに対する Amazon FSx for Windows File Server のリソースのクォータです。

リソース	ファイルシステムあたりの制限
タグの最大数	50
自動バックアップの最大保持期間	90 日間
単一の宛先リージョンに対して同時に送信できるバックアップコピーリクエストの 1 アカウントあたりの最大数。	5
最小ストレージ容量、SSD ファイルシステム	32 GiB
最小ストレージ容量、HDD ファイルシステム	2,000 GiB
最大ストレージ容量、SSD、HDD	64 TiB
最小 SSD IOPS	96
最大 SSD IOPS	400,000
最小スループット容量	8 MBps
最大スループット容量	12,288 MBps
ファイル共有の最大数	100,000

追加の考慮事項

以下の点にも注意してください。

- 各 AWS Key Management Service（AWS KMS) キーは、最大 125 個の Amazon FSx ファイルシステムで使用できます。
- ファイルシステムを作成できる AWS リージョン のリストについては、「」の「Amazon FSx エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。
- ドメインネームサービス (DNS) 名で、仮想プライベートクラウド (VPC) 内の Amazon EC2 インスタンスからファイル共有をマッピングします。

Microsoft Windows 固有のクォータ

詳細については、「Microsoft Windows Dev Center」の「NTFS 制限」を参照してください。

Amazon FSx のトラブルシューティング

以下のシナリオを使用して、Amazon FSx で発生する問題をトラブルシューティングします。

Amazon FSx の使用中に以下に記載されていない問題が発生した場合は、Amazon FSx フォーラムで質問してみてください。

トピック

- ファイルシステムにアクセスできない
- 新しい Amazon FSx ファイルシステムの作成が失敗する
- ファイルシステムが正しく設定されていない状態です
- マルチ AZ またはシングル AZ 2 ファイルシステムで DFS-R を設定することができない
- ストレージまたはスループットキャパシティの更新が失敗する

ファイルシステムにアクセスできない

次のように、ファイルシステムにアクセスできない原因はいくつか考えられますが、それぞれ独自の解決方法があります。

トピック

- ファイルシステム Elastic Network Interface が変更または削除されました
- ファイルシステム 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セキュリティグループには、必要なインバウンドまたは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
- アクティブディレクトリに結合していないコンピューティングインスタンス
- ファイル共有は存在しません
- アクティブディレクトリユーザーに必要な許可がありません
- 削除されたフルコントロール許可の NTFS ACL 許可
- オンプレミスのクライアントを使用してファイルシステムにアクセスできない
- 新しいファイルシステムは DNS に登録されていません
- DNS エイリアスを使用してファイルシステムにアクセスできない

- IP アドレスを使用してファイルシステムにアクセスすることができない

ファイルシステム 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 変更または削除しないでください。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 Elastic Network Interface は変更または削除しないでください。詳細については、「Amazon VPC を使用した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 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、ファイルシステムの Elastic Network Interface に接続される Elastic IP アドレス (インターネットから到達可能なパブリック IP アドレス) を自動的にデタッチします。詳細については、「データへのアクセス」を参照してください。

ファイルシステムのセキュリティグループには、必要なインバウンドまたは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 で指定されている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。

アクティブディレクトリに結合していないコンピューティングインスタンス

コンピューティングインスタンスが、次の 2 種類のアクティブディレクトリのいずれかに正しく結合されていない可能性があります。

- ファイルシステムが結合されている AWS Managed Microsoft AD ディレクトリ。
- AWS Managed Microsoft AD ディレクトリと一方向のフォレストの信頼関係が確立されている Microsoft アクティブディレクトリのディレクトリ。

コンピューティングインスタンスが 2 種類のディレクトリのいずれかに結合していることを確認してください。1 つのタイプは、ファイルシステムが結合されている AWS Managed Microsoft AD ディレクトリです。もう 1 つのタイプは、ディレクトリと一方向のフォレスト信頼関係が確立されている Microsoft Active Directory AWS Managed Microsoft AD ディレクトリです。詳細については、「での Amazon FSx の使用 AWS Directory Service for Microsoft Active Directory」を参照してください。

ファイル共有は存在しません

アクセスしようとしている Microsoft Windows ファイル共有は存在しません。

既存のファイル共有を使用している場合は、ファイルシステムの DNS 名と共有名が正しく指定されていることを確認してください。ファイル共有を管理する方法については、「ファイル共有の作成、更新、削除」を参照してください。

アクティブディレクトリユーザーに必要な許可がありません

ファイル共有にアクセスしているアクティブディレクトリユーザーには、必要なアクセス許可がありません。

共有フォルダのファイル共有および Windows アクセスコントロールリスト (ACL) のアクセス許可が、そのフォルダにアクセスする必要があるアクティブディレクトリユーザーへのアクセスを許可していることを確認します。

削除されたフルコントロール許可の NTFS ACL 許可

共有しているフォルダに対して SYSTEM ユーザーの [Allow Full control] (フルコントロールを許可) の NTFS ACL 許可を削除すると、その共有にアクセスできなくなり、それ以降のファイルシステムのバックアップが使用できなくなることがあります。

影響を受けるファイル共有を再作成する必要があります。詳細については、「ファイル共有の作成、更新、削除」を参照してください。フォルダまたは共有を再作成した後、コンピューティングインスタンスから Windows ファイル共有をマッピングして使用できます。

オンプレミスのクライアントを使用してファイルシステムにアクセスできない

AWS Direct Connect または VPN を使用してオンプレミスから Amazon FSx ファイルシステムを使用し、オンプレミスクライアントに非プライベート IP アドレス範囲を使用している。

Amazon FSx は、2020 年 12 月 17 日以降に作成されたファイルシステム上の非プライベート IP アドレスを持つオンプレミスクライアントからのアクセスのみをサポートします。

2020 年 12 月 17 日以前に作成された FSx for Windows ファイルサーバーのファイルシステムに、非プライベート IP アドレス範囲を使用してアクセスする必要がある場合は、ファイルシステムのバックアップを復元して、新しいファイルシステムを作成します。詳細については、「バックアップでデータを保護する。」を参照してください。

新しいファイルシステムは DNS に登録されていません

セルフマネージドアクティブディレクトリに結合しているファイルシステムの場合、カスタマーネットワークは Microsoft DNS を使用しないため、Amazon FSx は作成時にファイルシステム DNS を登録していません。

ネットワークが Microsoft DNS ではなくサードパーティーの DNS サービスを使用している場合、Amazon FSx はファイルシステムを DNS に登録しません。Amazon FSx ファイルシステムの DNS A エントリをマニュアルで設定する必要があります。シングル AZ 1 ファイルシステムの場合は、DNS A エントリを 1 つ追加する必要があります。シングル AZ 2 およびマルチ AZ ファイルシステムの場合は、2 つの DNS A エントリを追加する必要があります。DNS A エントリをマニュアルで追加する際に使用するファイルシステムの IP アドレスを取得するには、次の手順を実行します。

1. https://console.aws.amazon.com/fsx/ で、IP アドレスを取得したいファイルシステムを選択すると、ファイルシステムの詳細ページが表示されます。
2. [Network & security] (ネットワークとセキュリティ) タブで、次のいずれかを実行します。
   - シングル AZ 1 ファイルシステムの場合:
     - [Subnet] (サブネット) パネルで、[Network Interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
     - [Primary private IPv4 IP] (プライマリプライベート IPv4 IP) 列には、シングル AZ 1 ファイルシステムが使用する IP アドレスが表示されます。
   - シングル AZ 2 またはマルチ AZ ファイルシステムの場合:

- [Preferred subnet] (優先サブネット) パネルで、[Network Interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
- 使用する優先サブネットの IP アドレスは、[Secondary private IPv4 IP] (セカンダリプライベート IPv4 IP) 列に表示されます。
- Amazon FSx の [Standby subnet] (スタンバイサブネット) パネルで、[Network Interface] (ネットワークインターフェイス) に表示されている Elastic Network Interface を選択して、Amazon EC2 コンソールの [Network Interfaces] (ネットワークインターフェイス) ページを開きます。
- 使用するスタンバイサブネットの IP アドレスは、[Secondary private IPv4 IP] (セカンダリプライベート IPv4 IP) 列に表示されます。

DNS エイリアスを使用してファイルシステムにアクセスできない

DNS エイリアスを使用してファイルシステムにアクセスできない場合は、次の手順を使用して問題のトラブルシューティングを行います。

1. 次のいずれかの手順を実行して、エイリアスが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。

   a. Amazon FSx コンソールの使用 - アクセスしようとしているファイルシステムを選択します。[File system details] (ファイルシステムの詳細) ページでは、[DNS aliases] (DNS エイリアス) は [Network & security] (ネットワークとセキュリティ) タブに表示されます。

   b. CLI または API の使用 - `describe-file-system-aliases` CLI コマンド、または DescribeFileSystemAliases API オペレーションを使用して、ファイルシステムに現在関連付けられているエイリアスを取得します。

2. DNS エイリアスが一覧表示されていない場合は、それをファイルシステムに関連付ける必要があります。詳細については、「既存のファイルシステム上の DNS エイリアスを管理する」を参照してください。

3. DNS エイリアスがファイルシステムに関連付けられている場合は、次の必須項目も設定されていることを確認します。

   - Amazon FSx ファイルシステムのアクティブディレクトリコンピュータオブジェクトに DNS エイリアスに対応するサービスプリンシパル名 (SPN) を作成している。

詳細については、「Kerberos のサービスプリンシパル名 (SPN) を設定する」を参照してください。

- Amazon FSx ファイルシステムのデフォルトの DNS 名に解決される DNS エイリアスの DNS CNAME レコードを作成している。

  詳細については、「DNS CNAME レコードを更新または作成する」を参照してください。

4. 有効な SPN と DNS CNAME レコードを作成した場合は、クライアントの DNS に正しいファイルシステムに解決される DNS CNAME レコードがあることを確認します。

   a. `nslookup` を実行して、レコードが存在し、ファイルシステムのデフォルト DNS 名に解決していることを確認します。

   b. DNS CNAME が別のファイルシステムに解決された場合は、クライアントの DNS キャッシュが更新されるのを待ってから、CNAME レコードを再度確認します。次のコマンドを使用して、クライアントの DNS キャッシュをフラッシュすることで、プロセスを高速化できます。

```
ipconfig /flushdns
```

5. DNS CNAME レコードが Amazon FSx ファイルシステムのデフォルト DNS に解決したにもかかわらず、クライアントがまだファイルシステムにアクセスできない場合、「ファイルシステムにアクセスできない 」で追加のトラブルシューティング手順を参照してください。

IP アドレスを使用してファイルシステムにアクセスすることができない

IP アドレスを使用してファイルシステムにアクセスできない場合は、代わりに DNS 名または関連する DNS エイリアスを使用してみます。

ファイルシステムの DNS 名と関連する DNS エイリアスは、Amazon FSx コンソール で Windows ファイルサーバー、ネットワークとセキュリティ を選択して見つけることができます。または、CreateFileSystem ないし DescribeFileSystems API オペレーションのレスポンスにもあります。DNS エイリアスの使用については、「DNS エイリアスを管理する」を参照してください。

- AWS Managed Microsoft Active Directory に結合されたシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
fs-0123456789abcdef0.ad-domain.com
```

- すべてのマルチ AZ ファイルシステムおよびセルフマネージド型 Active Directory に結合しているシングル AZ ファイルシステムの場合、DNS 名は次のようになります。

```
amznfsxaa11bb22.ad-domain.com
```

新しい Amazon FSx ファイルシステムの作成が失敗する

ファイルシステムの作成リクエストが失敗する場合、次のセクションで説明するように、いくつかの原因が考えられます。

トピック

- VPC セキュリティグループとネットワーク ACL の設定ミス
- ファイルシステム管理者グループ名の重複
- DNS サーバーまたはドメインコントローラーに到達できない
- サービスアカウントの認証情報が無効
- サービスアカウントのアクセス許可が不十分
- サービスアカウントの容量超過
- Amazon FSx は組織単位 (OU) にアクセスできない
- サービスアカウントが管理者グループにアクセスできない
- ドメインで Amazon FSx の接続が失われた
- サービスアカウントに正しいアクセス許可がない
- 作成パラメータで使用される Unicode 文字
- バックアップの復元中にストレージタイプを HDD に切り替えると失敗する

VPC セキュリティグループとネットワーク ACL の設定ミス

VPC セキュリティグループとネットワーク ACL が、推奨されるセキュリティグループ設定を使用して設定されていることを確認してください。詳細については、「セキュリティグループの作成」を参照してください。

ファイルシステム管理者グループ名の重複

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx は、同じ名前のドメインに複数の管理者グループがあるため、ファイルシステムを作成しませんでした。

グループ名を指定しない場合、Amazon FSx は管理者グループとしてデフォルト値の「ドメイン管理者」を使用しようとします。デフォルトの「ドメイン管理者」名を使用するグループが複数ある場合、リクエストは失敗します。

以下のステップを使用し、問題を解決します。

1. ファイルシステムをセルフマネージド Active Directory に結合させるための前提条件を確認します。
2. セルフマネージド Active Directory に結合している FSx for Windows File Server ファイルシステムを作成する前に、Amazon FSx Active Directory 検証ツールを使用して、セルフマネージド Active Directory 設定を検証します。
3. AWS Management Console または を使用して新しいファイルシステムを作成します AWS CLI。詳細については、「セルフマネージド Microsoft アクティブディレクトリドメインへの Amazon FSx ファイルシステムの結合」を参照してください。
4. セルフマネージド Active Directory のドメインで一意のファイルシステム管理者グループの名前を指定します。

DNS サーバーまたはドメインコントローラーに到達できない

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
```

```
traffic from the file system to the domain controller.
```

以下のステップでトラブルシューティングを行い、問題を解決します。

1. Amazon FSx ファイルシステムを作成するサブネットとセルフマネージドアクティブディレクトリとの間でネットワーク接続とルーティングを確立するための前提条件に従っていることを確認します。詳細については、「前提条件」を参照してください。

   Amazon FSx アクティブディレクトリ検証ツール を使用して、これらのネットワーク設定をテストおよび検証します。

   > **Note**
   >
   > 複数のアクティブディレクトリサイトが定義されている場合、Amazon FSx ファイルシステムに関連する VPC 内のサブネットがアクティブディレクトリのサイトで定義されており、VPC 内のサブネットと他のサイトのサブネットの間に IP の競合が存在しないことを確認してください。これらの設定は、アクティブディレクトリサイトとサービス MMC スナップインを使用して、表示および変更することができます。

2. Amazon FSx ファイルシステムに関連付けた VPC セキュリティグループと VPC ネットワーク ACL を設定して、すべてのポートでアウトバウンドネットワークトラフィックを許可していることを確認します。

   > **Note**
   >
   > 最小特権を実装する場合は、アクティブディレクトリのドメインコントローラーとの通信に必要な特定のポートへの送信トラフィックのみを許可できます。詳細については、「Microsoft アクティブディレクトリのドキュメント」を参照してください。

3. Microsoft Windows ファイルサーバーまたはネットワーク管理プロパティの値に Latin-1 以外の文字が含まれていないことを確認します。例えば、ファイルシステム管理者グループの名前に `Domänen-Admins` を使用すると、ファイルシステムの作成に失敗します。
4. アクティブディレクトリドメインの DNS サーバーおよびドメインコントローラーがアクティブで、提供されたドメインに対するリクエストにレスポンスできることを確認します。
5. アクティブディレクトリドメインの機能レベルが Windows Server 2008 R2 以上であることを確認します。

6. アクティブディレクトリドメインのドメインコントローラーのファイアウォールルールで、Amazon FSx ファイルシステムからのトラフィックが許可されていることを確認します。詳細については、「Microsoft アクティブディレクトリのドキュメント」を参照してください。

サービスアカウントの認証情報が無効

セルフマネージド Active Directory に接続しているファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

以下のステップでトラブルシューティングを行い、問題を解決します。

1. セルフマネージドアクティブディレクトリの設定で、サービスアカウントのユーザーネームに `ServiceAcct` などのユーザー名のみを入力していることを確認します。

   > **Important**
   >
   > サービスアカウントのユーザー名を入力する際は、ドメインプレフィックス (`corp.com\ServiceAcct`) またはドメインサフィックス (`ServiceAcct@corp.com`) 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) を入力するときは、識別名 (DN) を使用しないでください。

2. 指定したサービスアカウントがアクティブディレクトリドメインに存在することを確認します。
3. 必要な許可が、指定したサービスアカウントに委任されていることを確認してください。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

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、「Amazon FSx サービスアカウント」を参照してください。

サービスアカウントのアクセス許可が不十分

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

次の手順を使用して、問題のトラブルシューティングと解決を行います。

- 必要な許可が、指定したサービスアカウントに委任されていることを確認してください。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

  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、「Amazon FSx サービスアカウント」を参照してください。

サービスアカウントの容量超過

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

この問題を解決するには、提供したサービスアカウントが、ドメインに結合できるコンピュータの最大数に達していることを確認します。上限に達した場合は、適切な許可で新しいサービスアカウントを作成してください。新しいサービスアカウントを使用して、新しいファイルシステムを作成します。詳細については、「Amazon FSx サービスアカウント」を参照してください。

Amazon FSx は組織単位 (OU) にアクセスできない

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

以下のステップでトラブルシューティングを行い、問題を解決します。

1. 指定した OU がアクティブディレクトリのドメインにあることを確認します。
2. 必要な許可が、指定したサービスアカウントに委任されていることを確認してください。サービスアカウントは、ファイルシステムに結合しているドメインの OU 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。またサービスアカウントには、少なくとも以下を実行するための許可が必要です。
   - 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ためのコントロールを委任されます
- 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

正しい許可でサービスアカウントを作成する方法の詳細については、「Amazon FSx サービスアカウント」を参照してください。

サービスアカウントが管理者グループにアクセスできない

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

以下のステップでトラブルシューティングを行い、問題を解決します。

1. 管理者グループパラメータの文字列として、グループの名前だけを指定していることを確認してください。

   > **Important**
   > グループ名パラメータを指定するときは、ドメインプレフィックス (`corp.com\FSxAdmins`) またはドメインサフィックス (`FSxAdmins@corp.com`) を含めないでください。
   > グループには識別名 (DN) を使用しないでください。識別名の例は、CN=FSxAdmins、OU=example、DC=corp、DC=com です。

2. 提供された管理者グループが、ファイルシステムに結合するドメインと同じアクティブディレクトリドメインに存在することを確認してください。

3. 管理者グループのパラメータを指定しなかった場合、Amazon FSx はアクティブディレクトリドメインの `Builtin Domain Admins` グループを使用しようとします。このグループ名が変更された場合、またはドメイン管理に別のグループを使用している場合は、そのグループ名を指定する必要があります。

ドメインで Amazon FSx の接続が失われた

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

ファイルシステムを作成した際に、Amazon FSx はアクティブディレクトリドメインの DNS サーバーとドメインコントローラーに到達し、ファイルシステムをアクティブディレクトリドメインに正常に結合させることができました。しかし、ファイルシステムの作成が完了している間に、Amazon FSx はドメインへの接続またはメンバーシップを失っています。以下のステップでトラブルシューティングを行い、問題を解決します。

1. Amazon FSx ファイルシステムとアクティブディレクトリの間にネットワーク接続が存在していることを確認します。また、ルーティングルール、VPC セキュリティグループルール、VPC ネットワーク ACL、およびドメインコントローラーファイアウォールのルールを使用して、ネットワークトラフィックが引き続き許可されるようにします。
2. Amazon FSx がアクティブディレクトリのドメインでファイルシステム用に作成したコンピュータオブジェクトが、まだアクティブで、削除されたり操作されたりしていないことを確認します。

サービスアカウントに正しいアクセス許可がない

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
```

```
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

必要な許可が、指定したサービスアカウントに委任されていることを確認してください。以下のステップでトラブルシューティングを行い、問題を解決します。

サービスアカウントには、少なくとも次のアクセス許可が必要です。

- ファイルシステムに接続している OU 内のコンピュータオブジェクトを作成および削除するためのコントロールを委任する
- ファイルシステムに接続している OU 内で次の許可が必要です。
  - 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
  - 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機能(委任可)
  - 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
  - アクセス許可を変更する機能

  正しい許可でサービスアカウントを作成する方法の詳細については、「Amazon FSx サービスアカウント」を参照してください。

作成パラメータで使用される Unicode 文字

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ファイルシステムの作成に失敗すると、次のエラーメッセージが表示されます。

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx は Unicode 文字をサポートしていません。作成パラメータにアクセント記号などの Unicode 文字が含まれていないことを確認します。これには、デフォルト値が自動的に入力される場

所で空白のままにできるパラメータが含まれます。アクティブディレクトリの対応するデフォルト値にも Unicode 文字が含まれていないことを確認します。

バックアップの復元中にストレージタイプを HDD に切り替えると失敗する

バックアップからのファイルシステムの作成に失敗し、次のエラーメッセージが表示されます。

```
Switching storage type to HDD while creating a file system from backup
backup_id is not supported because a storage scaling activity was still
under way on the source file system to increase storage capacity from less
than 2000 GiB when the backup backup_id was taken, and the minimum storage
capacity for HDD storage is 2000 GiB.
```

この問題は、バックアップを復元し、ストレージタイプを SSD から HDD に変更した場合に発生します。復元するバックアップは、元のファイルシステム上でストレージ容量が増加している間に作成されたため、バックアップからの復元は失敗します。増加リクエスト前のファイルシステムの SSD ストレージ容量は 2000 GiB 未満でした。これは、HDD ファイルシステムの作成に必要な最小ストレージ容量です。

この問題を解決するには、次の手順を使用します。

1. ストレージ容量の増加リクエストが完了するのを待ちます。ファイルシステムには、少なくとも 2000 GiB の SSD ストレージ容量があります。詳細については、「ストレージ容量の拡張をモニタリングする」を参照してください。
2. ユーザーが開始したファイルシステムのバックアップを取ります。詳細については、「ユーザー主導のバックアップ機能」を参照してください。
3. HDD ストレージを使用して、ユーザーが開始したバックアップを新しいファイルシステムに復元します。詳細については、「新しいファイルシステムへのバックアップの復元」を参照してください。

ファイルシステムが正しく設定されていない状態です

アクティブディレクトリ環境の変更が原因で、FSx for Windows ファイルサーバーのファイルシステムが [Misconfigured] (接続ミス) 状態になる場合があります。この状態では、ファイルシステムは使用できないか、アベイラビリティーを失うリスクがあり、バックアップが成功しない可能性があります。

接続ミス状態には、Amazon FSx コンソール、API、または AWS CLIを使用してアクセスできるエラーメッセージと推奨される修正措置が含まれます。修正措置を行った後、ファイルシステムの状態が最終的に `Available` に変わることを確認します。この変更が完了するまでに数分かかる場合があることに注意してください。

次のようないくつかの理由で、ファイルシステムが 接続ミス 状態になる可能性があります。

- DNS サーバーの IP アドレスは無効です。
- サービスアカウントの認証情報が有効でないか、必要な許可がありません。
- 無効な VPC セキュリティグループ、VPC ネットワーク ACL またはルーティングテーブルの設定、またはドメインコントローラーのファイアウォール設定などのネットワーク接続の問題が原因で、アクティブディレクトリのドメインコントローラーに到達できません。

> **Important**
>
> ファイルシステムの作成後に 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。これを行うと、ファイルシステムが正しく設定されなくなります。

(アクティブディレクトリ要件の完全なリストについては、「前提条件」を参照してください。Amazon FSx アクティブディレクトリ検証ツールを使用して、アクティブディレクトリ環境がこれらの要件を満たすように適切に設定されていることを検証することもできます。)

これらの問題のいくつかを解決するには、DNS サーバーの IP アドレスの変更や、サービスアカウントのユーザーネームまたはパスワードの変更など、ファイルシステムのアクティブディレクトリ設定のパラメータを 1 つ以上、直接更新する必要があります。このような場合、是正措置には、Amazon FSx コンソール、API、または を使用して必要な設定パラメータを更新 AWS CLI する必要があります。

ドメインコントローラーのファイアウォール設定や VPC セキュリティグループの変更など、アクティブディレクトリ設定パラメータを変更する必要がない問題もあります。ただし、これらの場合、ファイルシステムが `Available` になる前に、追加アクションを実行する必要があります。アクティブディレクトリ環境が適切に設定されていることを確認したら、Amazon FSx コンソールの [設定ミス] ステータスの横にある [回復を試みる] ボタンを選択するか、Amazon FSx コンソール、API、または AWS CLIで `StartMisconfiguredStateRecovery` コマンドを使用します。

トピック

- 誤って設定されたファイルシステム: Amazon FSx は、ドメインの DNS サーバーまたはドメインコントローラーのいずれにも到達できません。
- ファイルシステムの設定ミス: サービスアカウントの認証情報が無効です
- ファイルシステムの設定ミス: 提供されたサービスアカウントには、ファイルシステムをドメインに結合させる許可がありません
- ファイルシステムの設定ミス: サービスアカウントは、これ以上コンピュータをドメインに結合させることができません
- ファイルシステムの設定ミス: サービスアカウントが OU にアクセスできません

誤って設定されたファイルシステム: Amazon FSx は、ドメインの DNS サーバーまたはドメインコントローラーのいずれにも到達できません。

Amazon FSx が Microsoft アクティブディレクトリのドメインコントローラーと通信できない場合、ファイルシステムは `Misconfigured` 状態になります。

この状況を解決するには、以下の手順を実行します。

1. ネットワーク設定で、ファイルシステムからドメインコントローラーへのトラフィックが許可されていることを確認します。
2. Amazon FSx アクティブディレクトリ検証ツール を使用して、セルフマネージドアクティブディレクトリのネットワーク設定をテストし、検証します。詳細については、「セルフマネージド Microsoft Active Directory を使用する」を参照してください。
3. Amazon FSx コンソールで、ファイルシステムのセルフマネージドアクティブディレクトリの設定を確認します。
4. ファイルシステムのセルフマネージドアクティブディレクトリの設定を更新するには、Amazon FSx コンソールを使用します。

   a. ナビゲーションペインで ファイルシステム を選択し、更新するファイルシステムを選択すると、ファイルシステムの詳細 ページが表示されます。

   b. [File system details] (ファイルシステムの詳細) ページで、[Networking and security] (ネットワークとセキュリティ) タブの [Update] (更新) を選択します。

   また、Amazon FSx CLI `update-file-system` コマンドまたは API オペレーション UpdateFileSystem を使用することもできます。

ファイルシステムの設定ミス: サービスアカウントの認証情報が無効です

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、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です。詳細については、「セルフマネージド Microsoft Active Directory を使用する」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。

1. 正しいサービスアカウントを使用していること、およびそのアカウントに正しい認証情報を使用していることを確認してください。
2. 次に、Amazon FSx コンソールを使用して正しいサービスアカウントまたはアカウントの認証情報でファイルシステムの設定を更新します。

   a. ナビゲーションペインで ファイルシステム を選択し、更新する設定ミスのあるファイルシステムを選択します。

   b. ファイルシステムの詳細 ページで ネットワークとセキュリティ タブの 更新 を選択します。

   Amazon FSx API オペレーション `update-file-system` を使用することもできます。詳細については、Amazon FSx API リファレンスの「UpdateFileSystem」を参照してください。

ファイルシステムの設定ミス: 提供されたサービスアカウントには、ファイルシステムをドメインに結合させる許可がありません

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への接続を確立できません。これは、提供されたサービスアカウントに、指定された OU のあるドメインにファイルシステムを参加させる許可がないためです。

設定ミスを解決するには、次の手順を実行します。

1. 必要な許可を Amazon FSx サービスアカウントに追加するか、必要な許可のある新しいサービスアカウントを作成します。これを行う方法については、「Amazon FSx サービスアカウント」を参照してください。
2. 次に、ファイルシステムのセルフマネージドアクティブディレクトリ設定を新しいサービスアカウントの認証情報で更新します。Amazon FSx コンソールを使用して、設定を更新できます。

a. ナビゲーションペインで ファイルシステム を選択し、更新するファイルシステムを選択すると、ファイルシステムの詳細 ページが表示されます。
b. ファイルシステムの詳細 ページで、ネットワークとセキュリティ タブの 更新 を選択します。

Amazon FSx API オペレーション `update-file-system` を使用することもできます。詳細については、Amazon FSx API リファレンスの「UpdateFileSystem」を参照してください。

ファイルシステムの設定ミス: サービスアカウントは、これ以上コンピュータをドメインに結合させることができません

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への接続を確立できません。この場合の原因は、提供されたサービスアカウントが、ドメインに結合させれるコンピュータの最大数に達したためです。

設定ミスを解決するには、次の手順を実行します。

1. 別のサービスアカウントを特定するか、新しいコンピュータをドメインに結合させることができる新しいサービスアカウントを作成します。
2. 次に、Amazon FSx コンソールを使用して、ファイルシステムのセルフマネージドアクティブディレクトリ設定を新しいサービスアカウントの認証情報で更新します。

   a. ナビゲーションペインで ファイルシステム を選択し、更新するファイルシステムを選択すると、ファイルシステムの詳細 ページが表示されます。
   b. ファイルシステムの詳細 ページで、ネットワークとセキュリティ タブの 更新 を選択します。

   Amazon FSx API オペレーション `update-file-system` を使用することもできます。詳細については、Amazon FSx API リファレンスの「UpdateFileSystem」を参照してください。

ファイルシステムの設定ミス: サービスアカウントが OU にアクセスできません

提供されたサービスアカウントが指定された OU にアクセスできないため、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への接続を確立できません。

設定ミスを解決するには、次の手順を実行します。

1. 別のサービスアカウントを特定するか、OU にアクセスできる新しいサービスアカウントを作成します。
2. 次に、ファイルシステムのセルフマネージドアクティブディレクトリ設定を新しいサービスアカウントの認証情報で更新します。

   a. ナビゲーションペインで ファイルシステム を選択し、更新するファイルシステムを選択すると、ファイルシステムの詳細 ページが表示されます。
   b. ファイルシステムの詳細 ページで、ネットワークとセキュリティ タブの 更新 を選択します。

   Amazon FSx API オペレーション `update-file-system` を使用することもできます。詳細については、Amazon FSx API リファレンスの「UpdateFileSystem」を参照してください。

マルチ AZ またはシングル AZ 2 ファイルシステムで DFS-R を設定することができない

Microsoft 分散ファイルシステムレプリケーション (DFS-R) は、マルチ AZ およびシングル AZ 2 ファイルシステムではサポートされていません。

マルチ AZ ファイルシステムは、複数のアクセスゾーンにわたる冗長性にネイティブで設定されています。複数のアベイラビリティーゾーンで高可用性を実現するには、マルチ AZ 配置タイプを使用します。詳細については、「可用性および耐久性: シングル AZ およびマルチ AZ のファイルシステム」を参照してください。

ストレージまたはスループットキャパシティの更新が失敗する

ファイルシステムのストレージとスループットキャパシティの更新リクエストが失敗する原因はいくつか考えられますが、それぞれ独自の解像度方法があります。

Amazon FSx がファイルシステムの にアクセスできないため、ストレージ容量の増加は失敗します。 AWS KMS key

Amazon FSx がファイルシステムを暗号化するために使用される KMS キーにアクセスできなかったため、ストレージ容量増加リクエストが失敗しました。

管理アクションを実行するには、Amazon FSx がファイルシステムを暗号化するために使用される KMS キーにアクセスできることを確認する必要があります。次の情報を使用して、キーアクセスの問題を解決します。

- KMS キーが削除された場合、削除された KMS キーを使用したファイルシステムとそのバックアップは復元できません。詳細については、「 AWS Key Management Service デベロッパーガイド」のAWS KMS key「 の削除」を参照してください。
- KMS キーが無効になっており、カスタマーマネージドキーである場合は、再度有効にしてから、ストレージ容量の増加リクエストを再試行してください。詳細については、「 AWS Key Management Service デベロッパーガイド」の「キーの有効化と無効化」を参照してください。
- 削除が保留中のためキーが無効である場合は、キーの削除が `PendingDeletion` 状態のうちに、まキー削除をキャンセルする必要があります。KMS キーが `Enabled` になったら、リクエストを再試行できます。
- インポートが保留されているためにキーが無効である場合は、インポートが完了するまで待ってから、ストレージの増加リクエストを再試行する必要があります。
- キーの付与制限を超えた場合は、キーの付与数の増加をリクエストする必要があります。詳細については、「 AWS Key Management Service デベロッパーガイド」の「リソースクォータ」を参照してください。クォータの増加が認められたら、ストレージの増加リクエストを再試行します。

セルフマネージドアクティブディレクトリの設定ミスのため、ストレージまたはスループットキャパシティの更新に失敗する

ファイルシステムのセルフマネージドアクティブディレクトリが誤って設定されているため、ストレージ容量またはスループットキャパシティの更新リクエストに失敗しました。

特定の設定ミスの状態を解決するには、「ファイルシステムが正しく設定されていない状態です」を参照してください。

スループットキャパシティが不十分なため、ストレージ容量の増加に失敗する

ファイルシステムのスループットキャパシティが 8 MBps に設定されているため、ストレージ容量の増加リクエストに失敗しました。

ファイルシステムのスループット容量を最低 16 MBps に増やし、リクエストを再試行します。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。

スループットキャパシティを 8 MBps に更新できない

ファイルシステムのスループットキャパシティを 8 MBps に変更するリクエストが失敗しました。

これは、ストレージ容量の増加リクエストが保留中または進行中の場合に発生する可能性があります。ストレージ容量を増やすには、16 MBps の最小スループットが必要です。ストレージ容量の増加リクエストが完了するまで待ってから、スループットキャパシティ変更リクエストを再試行します。

ドキュメント履歴

- API バージョン: 2018 年 3 月 1 日
- ドキュメントの最終更新日: 2025 年 7 月 22 日

以下の表は、「Amazon FSx Windows ユーザーガイド」の重要な変更点を記したものです。RSS フィードに登録して、ドキュメントの更新に関する通知を得ることができます。

変更	説明	日付
Amazon FSx が AmazonFSxServiceRolePolicy AWS 管理ポリシーを更新しました	Amazon FSx は、AmazonFSxServiceRolePolicy に `ec2:AssignIpv6Addresses` および アクセス`ec2:UnassignIpv6Addresses` 許可を追加しました。詳細については、「AmazonFSxServiceRolePolicy」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 アクセス`fsx:DetachAndDeleteS3AccessPoint` 許可が追加されました。	2025 年 6 月 25 日
Amazon FSx が AmazonFSxConsoleFullAccess 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:CreateAndAttachS3Access`	2025 年 6 月 25 日

	Point 、fsx:DescribeS3AccessPointAttachments 、および アクセスfsx:DetachAndDeleteS3AccessPoint 許可が追加されました。	
Amazon FSx が AmazonFSxConsoleReadOnlyAccess AWS 管理ポリシーを更新しました	Amazon FSx は、AmazonFSxConsoleReadOnlyAccess ポリシーを更新して、 アクセスec2:DescribeNetworkInterfaces 許可を追加しました。詳細については、AmazonFSxConsoleReadOnlyAccess ポリシーを参照してください。	2025 年 2 月 25 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	IPv4 と IPv6 の両方の IP アドレスと DNS 名を使用して、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作成できるようになりました。詳細については、FSx for Windows File Server」と「インターフェイス VPC エンドポイント」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 リファレンス」の「API エンドポイント」を参照してください。	2025 年 2 月 7 日

Amazon FSx が AmazonFSxConsoleFullAccess AWS 管理ポリシーを更新しました	Amazon FSx は、AmazonFSxConsoleFullAccess ポリシーを更新して、 アクセス`ec2:DescribeNetworkInterfaces` 許可を追加しました。詳細については、「AmazonFSxConsoleFullAccess」のポリシーを参照してください。	2025 年 2 月 7 日
FSx for Windows File Server Active Directory 検証ツールの更新バージョン	FSx for Windows File Server Active Directory 検証ツールの更新バージョンが利用可能になりました。詳細については、「Active Directory 設定の検証」を参照してください。	2024 年 11 月 6 日
スループット容量が 4 GBps 以上のファイルシステムでより高いレベルの IOPS のサポートを追加	FSx for Windows File Server は、スループットキャパシティが 4 GBps 以上のファイルシステムでは最大 IOPS を 130K から 150K に、スループットキャパシティが 6 GBps 以上のファイルシステムでは 175K から 200K に、スループットキャパシティが 9 GBps 以上のファイルシステムでは 260K から 300K に、スループットキャパシティが 12 GBps 以上のファイルシステムでは 350K から 400K に増加しています。 200K 詳細については、「FSx for Windows ファイルサーバーのパフォーマンス」を参照してください。	2024 年 1 月 17 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
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、`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 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、`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 AWS 管理ポリシーの更新」を参照してください。	2023 年 11 月 14 日
ファイルシステムのストレージタイプの更新のサポートを追加	FSx for Windows ファイルサーバーファイルシステムは、HDD ストレージタイプから SSD ストレージタイプへの更新をサポートするようになりました。詳細については、「ストレージタイプの管理」を参照してください。	2023 年 8 月 9 日
最大スループットキャパシティを増やすためのサポートを追加	FSx for Windows ファイルサーバーファイルシステムは、最大 12 GBps のスループットキャパシティをサポートするようになりました。詳細については、「FSx for Windows ファイルサーバーのパフォーマンス」を参照してください。	2023 年 8 月 9 日

SSD IOPS プロビジョニングのサポートを追加	FSx for Windows ファイルサーバーファイルシステムは、ストレージ容量に関係なく、最大 350,000 IOPS まで SSD IOPS プロビジョニングをサポートするようになりました。詳細については、「SSD IOPS の管理」を参照してください。	2023 年 8 月 9 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、「AmazonFSxServiceRolePolicy」を参照してください。	2023 年 7 月 24 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

Amazon FSx for Windows File Server 用の新しい CloudWatch メトリクスの追加	FSx for Windows File Server では、ファイルサーバーとストレージボリュームのパフォーマンスおよび容量の使用量をモニタリングする CloudWatch メトリクスが追加されました。詳細については、「Metrics and dimensions」(メトリクスとディメンション) を参照してください。	2022 年 9 月 22 日
ファイルシステムのパフォーマンス警告の追加	Amazon FSx では、CloudWatch メトリクスのセットのいずれかが事前に設定されたしきい値に近づくか超えた場合、[Performance & monitoring] (パフォーマンスとモニタリング) ウィンドウに警告が表示されるようになりました。各警告では、ファイルシステムのパフォーマンスを向上させるための実用的な推奨事項も提供されます。詳細については、「Performance warnings and recommendations」(パフォーマンスの警告と推奨事項)を参照してください。	2022 年 9 月 22 日

強化されたファイルシステムのパフォーマンスモニタリングの追加	FSx for Windows File Server ファイルシステム用の Amazon FSx コンソールのファイルシステムモニタリングダッシュボードに、[Summary] (概要)、[Storage] (ストレージ)、および[Performance] (パフォーマンス) のセクションが新しく追加されました。これらのセクションでは、強化されたパフォーマンスのモニタリングをサポートする新しい CloudWatch メトリクスのグラフが表示されます。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。	2022 年 9 月 22 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

Amazon Kendra の追加	FSx for Windows File Server のファイルシステムを Amazon Kendra のデータソースとして使用できるようになりました。これにより、ファイルシステムに保存されているドキュメントに含まれる情報のインデックス作成と検索が可能になります。詳細については、「Amazon Kendra で FSx for Windows File Server を使用する」を参照してください。	2022 年 3 月 26 日
ファイルアクセス監査の追加	ファイル、フォルダ、およびファイル共有に対するエンドユーザーアクセスの監査を有効にできるようになりました。監査イベントログを Amazon CloudWatch Logs または Amazon Data Firehose サービスに送信することを選択できます。詳細については、「ファイルアクセスの管理」を参照してください。	2021 年 6 月 8 日
バックアップのコピーの追加	Amazon FSx を使用して、同じ AWS アカウント内のバックアップを別の AWS リージョン (クロスリージョンコピー) または同じ AWS リージョン (リージョン内コピー) にコピーできるようになりました。詳細については、「バックアップのコピー」を参照してください。	2021 年 4 月 12 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	が AWS開発したカスタマイズ可能な AWS CloudFormation テンプレートを使用して、指定したしきい値に達すると、ファイルシステムのストレージ容量が自動的に増加します。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。	2021 年 2 月 17 日
非プライベート IP アドレスを使用したクライアントアクセスの追加	非プライベート IP アドレスを使用して、オンプレミスのクライアントで FSx for Windows File Server ファイルシステムにアクセスできます。詳細については、「サポート環境」を参照してください。非プライベート IP アドレスを使用する DNS サーバーおよび AD ドメインコントローラーを使用して、FSx for Windows File Server ファイルシステムをセルフマネージド Microsoft アクティブディレクトリ に結合できます。詳細については、「セルフマネージドアクティブディレクトリ での Amazon FSx の使用」を参照してください。	2020 年 12 月 17 日

DNS エイリアスの使用の追加	ファイルシステム上のデータへアクセスするために使用する FSx for Windows File Server ファイルシステムに、DNS エイリアスを関連付けできるようになりました。詳細については、「DNS エイリアスの管理」および「チュートリアル 5: DNS エイリアスを使用したファイルシステムへのアクセス」を参照してください。	2020 年 11 月 9 日
Amazon Elastic Container Service の追加	Amazon ECS で FSx for Windows File Server を使用できるようになりました。詳細については、「 サポートされるクライアント」を参照してください。	2020 年 11 月 9 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 での AWS Backup の使用」を参照してください。	2020 年 11 月 9 日

スループットキャパシティスケーリングの追加	スループット要件の進展に応じて、既存の FSx for Windows File Server ファイルシステムの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。	2020 年 6 月 1 日
ストレージ容量のスケーリングの追加	ストレージ要件の進展に応じて、既存の FSx for Windows File Server ファイルシステムのストレージ容量を増やせ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」を参照してください。	2020 年 6 月 1 日
ハードディスクドライブ (HDD) ストレージの追加	HDDストレージは、FSx for Windows File Server を使用する場合に、料金とパフォーマンスの柔軟性を提供します。詳細については、「Amazon FSx でコストを最適化する」をご覧ください。	2020 年 3 月 26 日
を使用したファイル転送のサポートが追加されました AWS DataSync	AWS DataSync を使用して、FSx for Windows File Server との間でファイルを転送できるようになりました。詳細については、「AWS DataSync を使用して Amazon FSx for Windows File Server にファイルを移行する」を参照してください。	2020 年 2 月 4 日

FSx for Windows File Server は追加の Windows ファイルシステム管理タスクのサポートをリリースします	PowerShell 上でのリモート管理のため、Amazon FSx CLI を使用してファイル共有、データ重複、ストレージクォータ、および転送中の暗号化を管理運用できるようになりました。詳細については、「ファイルシステムの運用」を参照してください。	2019 年 11 月 20 日
FSx for Windows File Server はネイティブマルチAZ サポートをリリースします	FSx for Windows File Server 用のマルチ AZ 配置を使用すると、複数のアベイラビリティーゾーン (AZ) にまたがる高可用性のファイルシステムを、より簡単に作成できます。詳細については、「Availability and Durability: Single-AZ and Multi-AZ File Systems」(可用性と耐久性: シングル AZ とマルチ AZ ファイルシステム) を参照してください。	2019 年 11 月 20 日
FSx for Windows File Server はユーザーセッションとオープンファイルの管理サポートをリリースします	Microsoft Windows ネイティブの共有フォルダツールを使用して、ユーザーセッションの管理や、FSx for Windows File Server ファイルシステム上のファイルを開くことができるようになりました。詳細については、「ユーザーセッションとオープンファイルの管理」を参照してください。	2019 年 10 月 17 日

Amazon FSx は、Microsoft Windows シャドウコピーのサポートをリリースします	FSx for Windows File Server ファイルシステムで Windows シャドウコピーを設定できるようになりました。シャドウコピーを使用すると、ユーザーはファイルを以前のバージョンに復元することで、ファイルの変更を元に戻し、ファイルのバージョンを比較することができます。詳細については、「シャドウコピーの使用」を参照してください。	2019 年 7 月 31 日
Amazon FSx は共有された Microsoft アクティブディレクトリのサポートをリリースします	FSx for Windows File Server ファイルシステムを、別の VPC またはファイルシステム AWS アカウント とは異なる にある AWS Managed Microsoft AD ディレクトリに結合できるようになりました。詳細については、「アクティブディレクトリのサポート」を参照してください。	2019 年 6 月 25 日
Amazon FSx は強化された Microsoft アクティブディレクトリのサポートをリリースします	FSx for Windows File Server ファイルシステムを、オンプレミスまたはクラウド上のセルフマネージド Microsoft アクティブディレクトリドメインに結合できるようになりました。詳細については、「アクティブディレクトリのサポート」を参照してください。	2019 年 6 月 24 日

Amazon FSx は SOC 認定に準拠しています	Amazon FSx は SOC 認定に準拠していると査定されています。詳細については、「セキュリティおよびデータの保護」を参照してください。	2019 年 5 月 16 日
AWS Direct Connect、VPN、およびリージョン間の VPC ピアリング接続のサポートに関する明確な注意事項を追加	2019 年 2 月 22 日以降に作成された Amazon FSx ファイルシステムは、 AWS Direct Connect、VPN、およびリージョン間 VPC ピアリングを使用してアクセスできます。詳細については、「サポートされたアクセス方法」を参照してください。	2019 年 2 月 25 日
AWS Direct Connect、VPN、およびリージョン間 VPC ピアリング接続に追加されたサポート	オンプレミスのリソース、および別の Amazon VPC または AWS アカウント内のリソースから Amazon FSx for Windows File Server のファイルシステムにアクセスできるようになりました。詳細については、「サポートされたアクセス方法」を参照してください。	2019 年 2 月 22 日

Amazon FSx が一般提供になりました	Amazon FSx for Windows File Server は、フルマネージド Microsoft Windows ファイルサーバーを提供し、完全ネイティブの Windows ファイルシステムによってバックアップされます。Amazon FSx for Windows File Server は、エンタープライズアプリケーションを AWSに簡単にリフトアンドシフトするための機能、パフォーマンス、および互換性を備えています。	2018 年 11 月 28 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。