



Amazon FSX for ONTAP のドキュメント

Amazon FSx for ONTAP

NetApp
July 04, 2022

目次

| | |
|-----------------------------------|----|
| Amazon FSX for ONTAP のドキュメント | 1 |
| Amazon FSX for ONTAP の新機能 | 2 |
| 2022年7月3日 | 2 |
| 2022 年 2 月 27 日 | 2 |
| 2021 年 10 月 31 日 | 2 |
| 2021 年 10 月 4 日 | 2 |
| 2021 年 9 月 2 日 | 3 |
| はじめに | 4 |
| Amazon FSX for ONTAP の詳細をご覧ください | 4 |
| Amazon FSX for ONTAP の利用を開始しましょう | 5 |
| ONTAP の FSX のアクセス許可を設定します | 5 |
| ONTAP の FSX のセキュリティグループルール | 7 |
| ONTAP には Amazon FSX を使用します | 16 |
| Amazon FSX for ONTAP 作業環境の作成と管理 | 16 |
| ONTAP 用の Amazon FSX ボリュームを作成します | 24 |
| Amazon FSX for ONTAP のボリュームを管理します | 29 |
| 知識とサポート | 31 |
| サポートに登録します | 31 |
| ヘルプを表示します | 32 |
| 法的通知 | 34 |
| 著作権 | 34 |
| 商標 | 34 |
| 特許 | 34 |
| プライバシーポリシー | 34 |
| オープンソース | 34 |

Amazon FSX for ONTAP のドキュメント

Amazon FSX for ONTAP の新機能

Amazon FSX for ONTAP の新機能をご確認ください。

2022年7月3日

- ・単一または複数のアベイラビリティゾーンHA導入モデルを選択できるようになりました。

["ONTAP 作業環境用の FSX を作成します"](#)

- ・AWS GovCloudアカウント認証はCloud Managerでサポートされるようになりました。

["IAM ロールを設定します"](#)

2022 年 2 月 27 日

IAM の役割を引き受けます

ONTAP 作業環境向け FSX を作成する場合、Cloud Manager が ONTAP 作業環境用の FSX を作成すると想定できる IAM ロールの ARN を指定する必要があります。以前は、AWS アクセスキーを指定する必要がありました。

["FSX for ONTAP のアクセス許可を設定する方法について説明します"](#)。

2021 年 10 月 31 日

Cloud Manager API を使用して **iSCSI** ボリュームを作成

Cloud Manager API を使用して FSX for ONTAP 用の iSCSI ボリュームを作成し、作業環境で管理できます。

ボリュームの作成時にボリュームの単位を選択します

可能です ["ボリュームの作成時にボリュームの単位（GiB または TiB）を選択します"](#) FSX for ONTAP の場合。

2021 年 10 月 4 日

Cloud Manager を使用して **CIFS** ボリュームを作成

できるようになりました。 ["Cloud Manager を使用して、FSX for ONTAP に CIFS ボリュームを作成します"](#)。

Cloud Manager を使用してボリュームを編集

できるようになりました。 ["Cloud Manager を使用して ONTAP ボリュームの FSX を編集します"](#)。

2021 年 9 月 2 日

Amazon FSX for ONTAP のサポート

- "ONTAP 対応の Amazon FSX" は、NetApp ONTAP ストレージ・オペレーティング・システムを搭載したファイル・システムの起動と実行を可能にするフルマネージド・サービスです。FSX for ONTAP は、ネットアップのお客様がオンプレミスで使用しているのと同じ機能、パフォーマンス、管理機能を、ネイティブの AWS サービスの簡易性、即応性、セキュリティ、拡張性で提供します。

["Amazon FSX for ONTAP の詳細をご覧ください"](#)。

- ONTAP 作業環境用に Cloud Manager で FSX を設定できます。

["ONTAP 作業環境用の Amazon FSX を作成します"](#)。

- AWS と Cloud Manager のコネクタを使用すると、ボリュームの作成と管理、データのレプリケート、および Data Sense や Cloud Sync などのクラウドサービス ONTAP との FSX の統合が可能です。

["Amazon FSX for ONTAP のクラウドデータセンスを今すぐ始めましょう"](#)。

はじめに

Amazon FSX for ONTAP の詳細をご覧ください

"[ONTAP 対応の Amazon FSX](#)" は、NetApp ONTAP ストレージ・オペレーティング・システムを搭載したファイル・システムの起動と実行を可能にするフルマネージド・サービスです。FSX for ONTAP は、ネットアップのお客様がオンプレミスで使用しているのと同じ機能、パフォーマンス、管理機能を、ネイティブの AWS サービスの簡易性、即応性、セキュリティ、拡張性で提供します。

の機能

- ストレージ・デバイス 'ソフトウェア' バックアップを構成または管理する必要はありません
- CIFS、NFSv3、NFSv4.x、SMB v2.v3.1.1 のプロトコルがサポートされます。
- 使用頻度の低い IA（ストレージ・ティア）を使用して '低コストで事実上無制限のデータ・ストレージ容量を実現します
- Oracle RAC を含むレイテンシの影響を受けやすいアプリケーションでの実行が保証されています。
- バンドル価格と従量課金制のいずれかを選択できます

Cloud Manager のその他の機能

- AWS と Cloud Manager のコネクタを使用すると、ボリュームの作成と管理、データのレプリケート、および Data Sense や Cloud Sync などのクラウドサービス ONTAP との FSX の統合が可能です。
- 人工知能（AI）ベースのテクノロジーを使用したクラウドデータセンスは、データコンテキストを理解し、FSX for ONTAP アカウントに存在する機密データを識別するのに役立ちます。"[詳細はこちら](#)。"
- NetApp Cloud Sync を使用すると、クラウド内やオンプレミス内のあらゆるターゲットへのデータ移行を自動化できます。"[詳細はこちら](#)。"

コスト

ONTAP 用の FSX アカウントは、Cloud Manager ではなく AWS で管理されます。 "[『Amazon FSX for ONTAP Getting Started Guide』](#)"

AWS でコネクタを使用する場合、および Cloud Sync や Data Sense などのオプションのデータサービスを使用する場合は、追加コストが発生します。

サポートされている地域

"[サポート対象の Amazon リージョンを表示します](#)。"

サポートを受ける

Amazon FSX for ONTAP は、AWS ファーストパーティの解決策です。AWS FSX ファイルシステム、インフラ、またはこのサービスを使用する AWS 解決策に関連する質問やテクニカルサポートの問題については、AWS コンソールのサポートセンターを使用して AWS へのサポートケースをオープンしてください。「FSX

for ONTAP」サービスと該当するカテゴリを選択します。AWS サポートケースの作成に必要な残りの情報を指定します。

Cloud Manager や Cloud Manager のマイクロサービスに関する一般的な質問については、Cloud Manager のインラインチャットから始めることができます。

内の Cloud Manager またはマイクロサービスに固有のテクニカルサポートの問題については、Cloud Manager アカウントレベルのシリアル番号を使用してネットアップサポートチケットを開くことができます。サポートを有効にするには、Cloud Manager のシリアル番号を登録する必要があります。

制限

- Cloud Manager は、オンプレミスまたは Cloud Volumes ONTAP から ONTAP 用 FSX にのみデータをレプリケートできます。
- この時点で、ONTAP CLI、ONTAP API、または Cloud Manager API を使用して iSCSI ボリュームを作成できます。
- この時点で、ONTAP の FSX からの SnapMirror レプリケーションはです ["ONTAP CLI を使用してサポート"](#)。

Amazon FSX for ONTAP の利用を開始しましょう

Amazon FSX for ONTAP の導入を開始するには、いくつかの手順を実行します。

FSX for ONTAP は、ほんの数ステップで開始できます。

ボリュームを追加する前に、ONTAP 作業環境用の Amazon FSX を作成する必要があります。する必要があります ["Cloud Manager SaaS で役割を引き受けることを可能にする IAM ロールを設定します"](#)。

を用意しておく必要があります ["AWS 用コネクタ"](#) FSX for ONTAP 作業環境を開くには、ボリュームを作成するか、その他の操作を実行します。コネクタが必要な場合、Cloud Manager はまだ追加されていないかどうかを尋ねます。

ONTAP ボリュームの FSX は、Cloud Manager を使用して作成できます。

Cloud Manager を使用してボリュームを管理し、レプリケーション、Cloud Sync、データセンスなどの追加サービスを設定します。

関連リンク

- ["Cloud Manager からコネクタを作成します"](#)
- ["AWS Marketplace から Connector を起動する"](#)
- ["Linux ホストへの Connector ソフトウェアのインストール"](#)

ONTAP の FSX のアクセス許可を設定します

ONTAP 作業環境用の Amazon FSX を作成または管理するには、Cloud Manager に ONTAP 作業環境用の FSX の作成に必要な権限を付与する IAM ロールの ARN を指定して、Cloud Manager に AWS クレデンシャルを追加する必要があります。

IAM ロールを設定します

Cloud Managerにロールを引き継ぐことができるようにIAMロールを設定します。

手順

1. ターゲットアカウントの IAM コンソールに移動します。
2. [アクセス管理] で、[役割]、[役割の作成 *] の順にクリックし、手順に従って役割を作成します。

必ず次の手順を実行してください。

- 信頼されるエンティティのタイプ * で、* AWS アカウント * を選択します。
- 別のAWSアカウント*を選択し、Cloud ManagerのIDを入力します。
 - Cloud Manager SaaSの場合：952013314444
 - AWS GovCloud（US）の場合：
- 次の権限を含むポリシーを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "kms:Describe*",
        "kms:List*",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

から Connector 展開ポリシーを表示します ["Cloud Manager Policies ページ"](#)。

3. IAM ロールのロール ARN をコピーして、次の手順で Cloud Manager に貼り付けることができます。

IAM ロールに必要な権限が割り当てられます。

クレデンシャルを追加します

IAM ロールに必要な権限を付与したら、Cloud Manager に ARN ロールを追加します。

IAM ロールを作成したばかりの場合は、使用できるようになるまで数分かかることがあります。Cloud Manager にクレデンシャルを追加するまで数分待ってから、

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、* クレデンシャル * を選択します。



2. [Add Credentials] をクリックし、ウィザードの手順に従います。
 - a. * クレデンシャルの場所 * : 「* Amazon Web Services > Cloud Manager *」を選択します。
 - b. * クレデンシャルの定義 * : IAM ロールの ARN (Amazon リソース名) を指定します。

- AWS GovCloud (US) アカウントを使用している場合は、* AWS GovCloud (US) アカウントを使用している*を確認します。



- AWS GovCloudを使用して認証すると、SaaSプラットフォームが無効になります。これはお客様のアカウントへの永続的な変更であり、元に戻すことはできません。

- c. * 確認 * : 新しいクレデンシャルの詳細を確認し、* 追加 * をクリックします。

ONTAP 作業環境で FSX を作成するときに、資格情報を使用できるようになりました。

関連リンク

- ["AWS のクレデンシャルと権限"](#)
- ["Cloud Manager 用の AWS クレデンシャルの管理"](#)

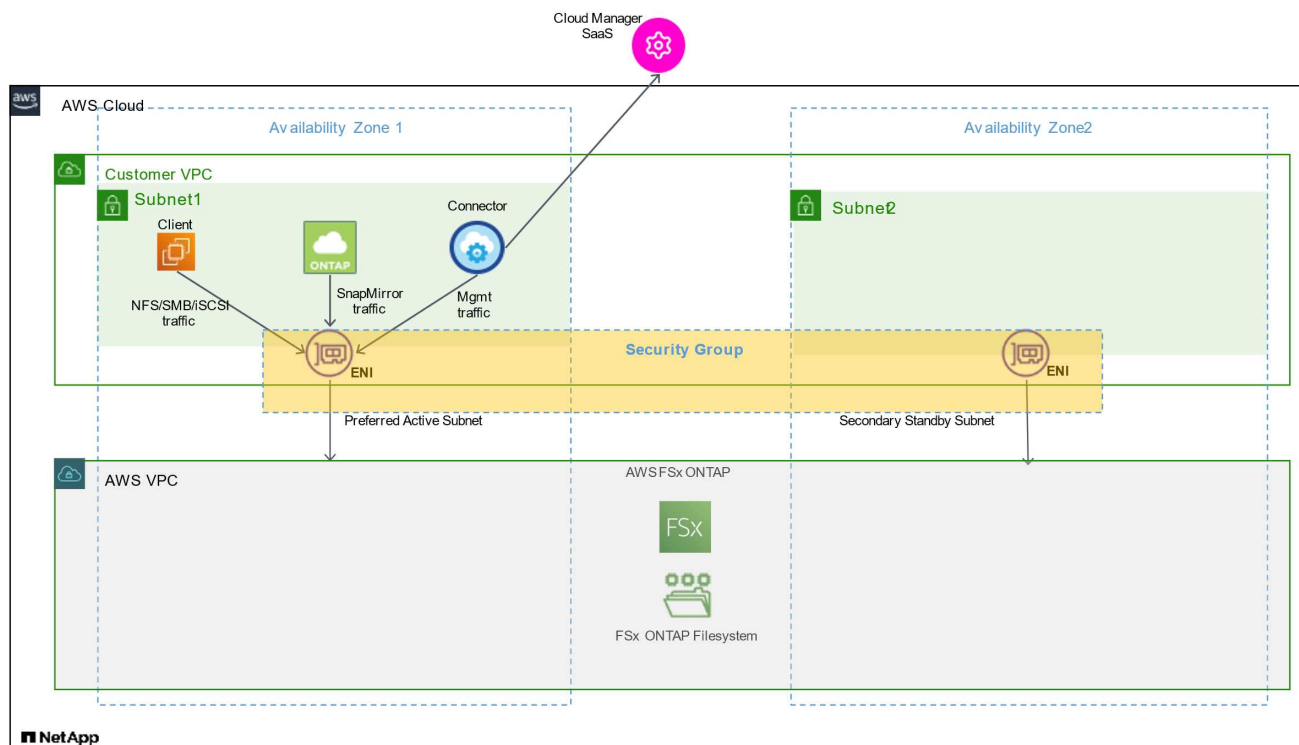
ONTAP の FSX のセキュリティグループルール

Cloud Manager で作成される AWS セキュリティグループには、Cloud Manager と FSX for ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールが含まれています。テスト目的または独自のポートを使用する必要がある場合には、ポートを参照してください。

ONTAP の FSX のルール

FSX for ONTAP セキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。こ

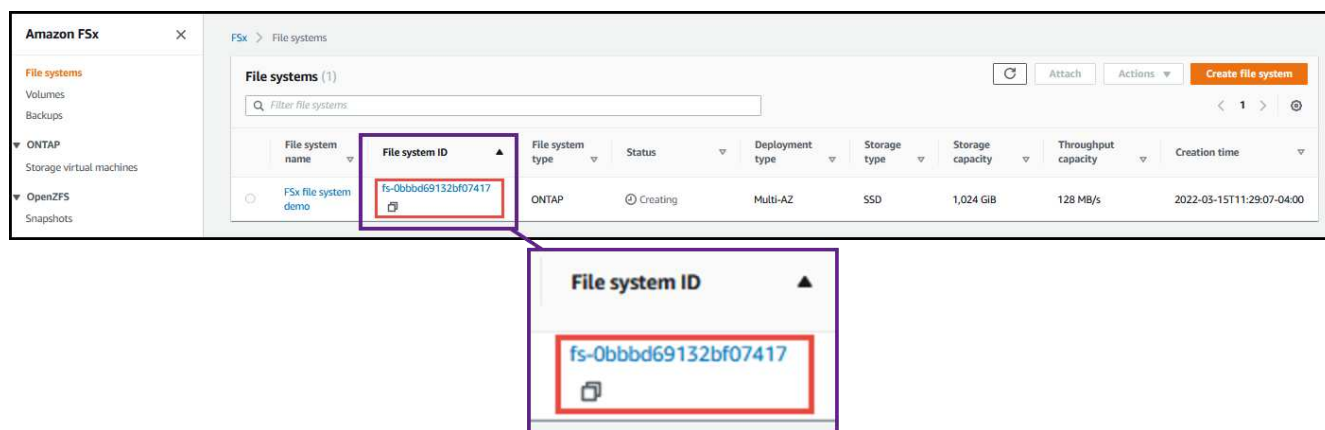
の図は、ONTAP ネットワーク構成およびセキュリティグループ要件の FSX を示しています。



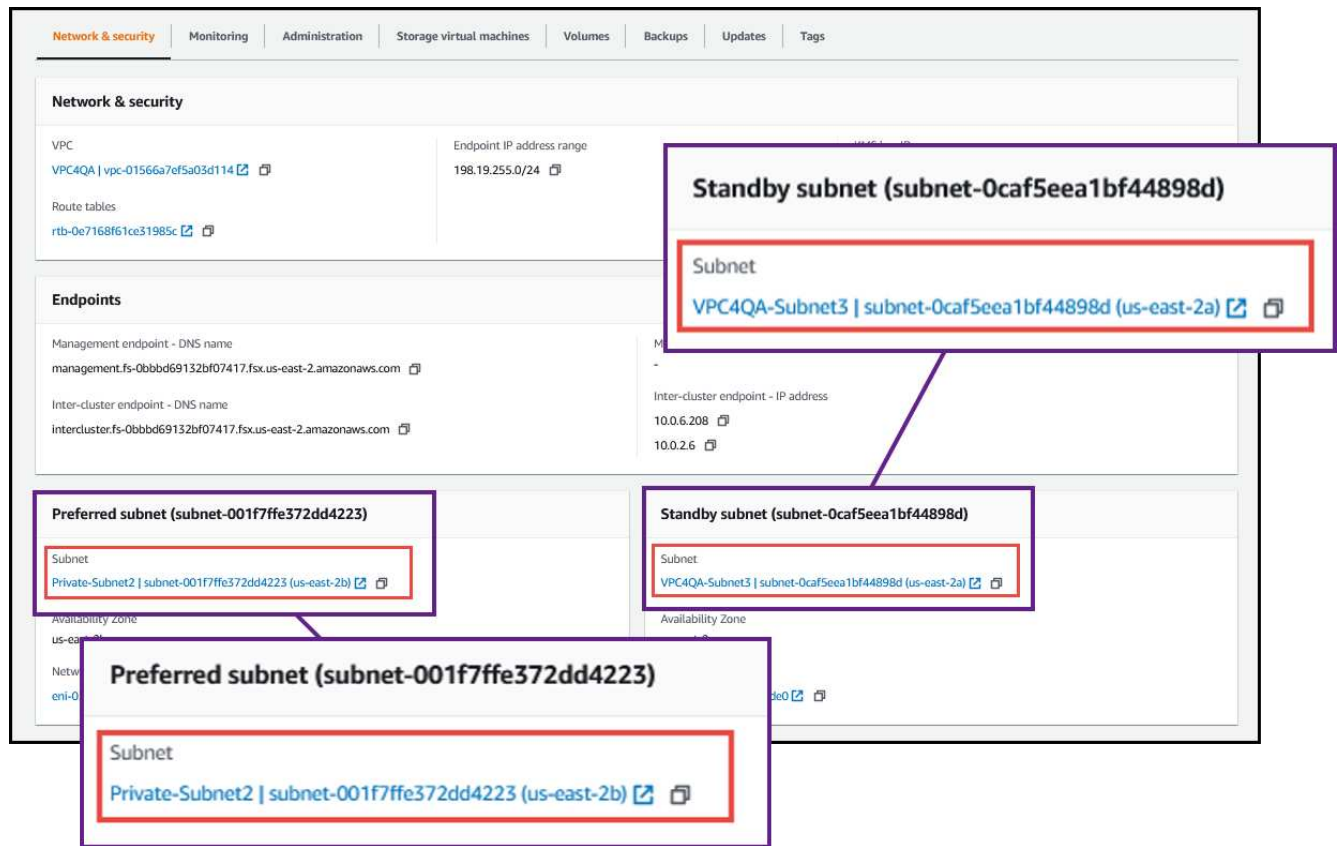
AWS 管理コンソールを使用して、ENI に関連付けられたセキュリティグループを見つける必要があります。

手順

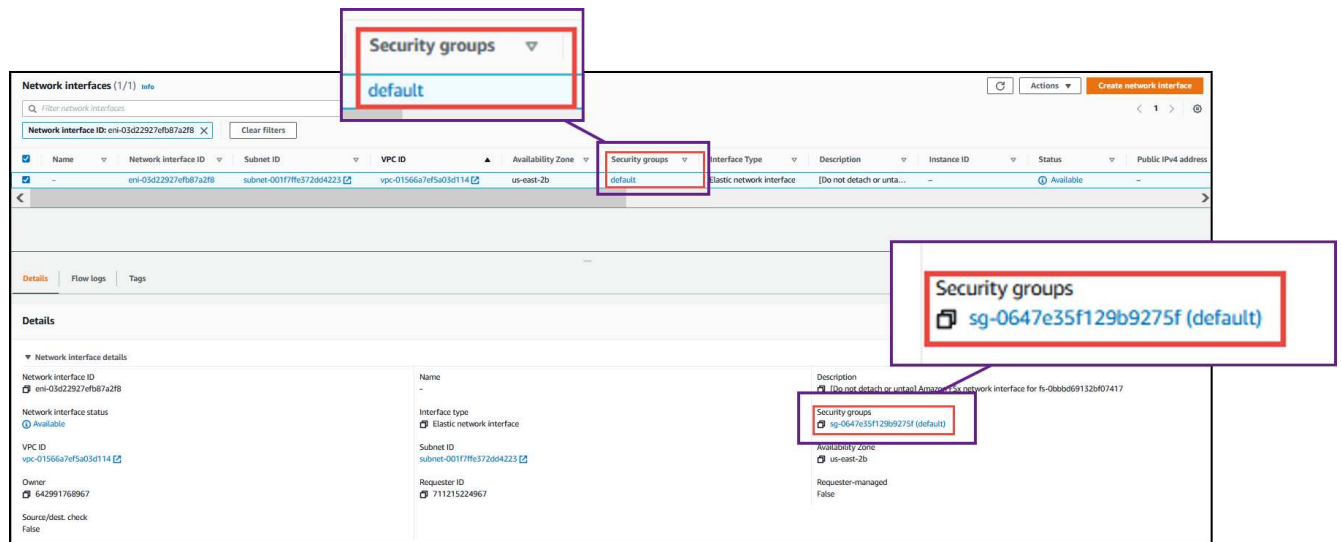
1. AWS 管理コンソールで FSX for ONTAP ファイルシステムを開き、ファイルシステム ID のリンクをクリックします。



2. [ネットワークとセキュリティ *] タブで、優先サブネットまたはスタンバイサブネットのネットワークインターフェイス ID をクリックします。



3. ネットワーク・インターフェイス・テーブルのセキュリティ・グループまたはネットワーク・インターフェイスの * 詳細 * セクションをクリックします。



インバウンドルール

| プロトコル | ポート | 目的 |
|-----------|-----|--|
| すべての ICMP | すべて | インスタンスの ping を実行します |
| HTTPS | 443 | fsxadmin管理LIFへのコネクタからアクセスし、API呼び出しをFSXに送信します |

| プロトコル | ポート | 目的 |
|-------|---------|--|
| SSH | 22 | クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス |
| TCP | 111 | NFS のリモートプロシージャコール |
| TCP | 139 | CIFS の NetBIOS サービスセッション |
| TCP | 161-162 | 簡易ネットワーク管理プロトコル |
| TCP | 445 | NetBIOS フレーム同期を使用した Microsoft SMB over TCP |
| TCP | 635 | NFS マウント |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS サーバデーモン |
| TCP | 3260 | iSCSI データ LIF を介した iSCSI アクセス |
| TCP | 4045 | NFS ロックデーモン |
| TCP | 4046 | NFS のネットワークステータスマニタ |
| TCP | 10000 | NDMP を使用したバックアップ |
| TCP | 11104 | SnapMirror のクラスタ間通信セッションの管理 |
| TCP | 11105 | クラスタ間 LIF を使用した SnapMirror データ転送 |
| UDP | 111 | NFS のリモートプロシージャコール |
| UDP | 161-162 | 簡易ネットワーク管理プロトコル |
| UDP | 635 | NFS マウント |
| UDP | 2049 | NFS サーバデーモン |
| UDP | 4045 | NFS ロックデーモン |
| UDP | 4046 | NFS のネットワークステータスマニタ |
| UDP | 4049 | NFS rquotad プロトコル |

アウトバウンドルール

FSX for ONTAP の事前定義されたセキュリティグループは、すべてのアウトバウンドトラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

FSX for ONTAP の事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

| プロトコル | ポート | 目的 |
|-----------|-----|--------------|
| すべての ICMP | すべて | すべての発信トラフィック |
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |

高度なアウトバウンドルール

メディアーターの特定のポートを開く必要はありませんまた 'FSX for ONTAP' のノード間でポートを開く必要もありません



ソースは、ONTAP システムの FSX 上のインターフェイス（IP アドレス）です。

| サービス | プロトコル | ポート | ソース | 宛先 | 目的 |
|------------------|-------------|------|----------------------------|-----------------------------|---|
| Active Directory | TCP | 88 | ノード管理 LIF | Active Directory フォレスト | Kerberos V 認証 |
| | UDP | 137 | ノード管理 LIF | Active Directory フォレスト | NetBIOS ネームサービス |
| | UDP | 138 | ノード管理 LIF | Active Directory フォレスト | NetBIOS データグラムサービス |
| | TCP | 139 | ノード管理 LIF | Active Directory フォレスト | NetBIOS サービスセッション |
| | TCP および UDP | 389 | ノード管理 LIF | Active Directory フォレスト | LDAP |
| | TCP | 445 | ノード管理 LIF | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP |
| | TCP | 464 | ノード管理 LIF | Active Directory フォレスト | Kerberos V パスワードの変更と設定 (SET_CHANGE) |
| | UDP | 464 | ノード管理 LIF | Active Directory フォレスト | Kerberos キー管理 |
| | TCP | 749 | ノード管理 LIF | Active Directory フォレスト | Kerberos V Change & Set Password (RPCSEC_GSS) |
| | TCP | 88 | データ LIF (NFS、CIFS、iSCSI) | Active Directory フォレスト | Kerberos V 認証 |
| | UDP | 137 | データ LIF (NFS、CIFS) | Active Directory フォレスト | NetBIOS ネームサービス |
| | UDP | 138 | データ LIF (NFS、CIFS) | Active Directory フォレスト | NetBIOS データグラムサービス |
| | TCP | 139 | データ LIF (NFS、CIFS) | Active Directory フォレスト | NetBIOS サービスセッション |
| | TCP および UDP | 389 | データ LIF (NFS、CIFS) | Active Directory フォレスト | LDAP |
| | TCP | 445 | データ LIF (NFS、CIFS) | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP |
| | TCP | 464 | データ LIF (NFS、CIFS) | Active Directory フォレスト | Kerberos V パスワードの変更と設定 (SET_CHANGE) |
| | UDP | 464 | データ LIF (NFS、CIFS) | Active Directory フォレスト | Kerberos キー管理 |
| | TCP | 749 | データ LIF (NFS、CIFS) | Active Directory フォレスト | Kerberos V Change & Set Password (RPCSEC_GSS) |
| S3 へのバックアップ | TCP | 5010 | クラスタ間 LIF | バックアップエンドポイントまたはリストアエンドポイント | S3 へのバックアップ処理とリストア処理 フィーチャー (Feature) |

| サービス | プロトコル | ポート | ソース | 宛先 | 目的 |
|------------|-------|---------------|---------------------------------|-----------------|--------------------------------|
| DHCP | UDP | 68 | ノード管理 LIF | DHCP | 初回セットアップ用の DHCP クライアント |
| DHCP | UDP | 67 | ノード管理 LIF | DHCP | DHCP サーバ |
| DNS | UDP | 53 | ノード管理 LIF とデータ LIF (NFS、CIFS) | DNS | DNS |
| NDMP | TCP | 18600 ~ 18699 | ノード管理 LIF | 宛先サーバ | NDMP コピー |
| SMTP | TCP | 25 | ノード管理 LIF | メールサーバ | SMTP アラート。 AutoSupport に使用できます |
| SNMP | TCP | 161 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | UDP | 161 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | TCP | 162 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | UDP | 162 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| SnapMirror | TCP | 11104 | クラスタ間 LIF | ONTAP クラスタ間 LIF | SnapMirror のクラスタ間通信セッションの管理 |
| | TCP | 11105 | クラスタ間 LIF | ONTAP クラスタ間 LIF | SnapMirror によるデータ転送 |
| syslog | UDP | 514 | ノード管理 LIF | syslog サーバ | syslog 転送メッセージ |

コネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

| プロトコル | ポート | 目的 |
|-------|------|---|
| SSH | 22 | コネクタホストへの SSH アクセスを提供します |
| HTTP | 80 | クライアント Web ブラウザからローカルユーザインターフェイスへの HTTP アクセス、および Cloud Data Sense からの接続を提供します |
| HTTPS | 443 | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |
| TCP | 3128 | AWS ネットワークで NAT やプロキシを使用していない場合に、 Cloud Data Sense インスタンスにインターネットアクセスを提供します |

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場

合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

| プロトコル | ポート | 目的 |
|----------|-----|--------------|
| すべての TCP | すべて | すべての発信トラフィック |
| すべての UDP | すべて | すべての発信トラフィック |

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス | プロトコル | ポート | 宛先 | 目的 |
|------------------|-------|-----|------------------------|---|
| Active Directory | TCP | 88 | Active Directory フォレスト | Kerberos V 認証 |
| | TCP | 139 | Active Directory フォレスト | NetBIOS サービスセッション |
| | TCP | 389 | Active Directory フォレスト | LDAP |
| | TCP | 445 | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP |
| | TCP | 464 | Active Directory フォレスト | Kerberos V パスワードの変更と設定 (SET_CHANGE) |
| | TCP | 749 | Active Directory フォレスト | Active Directory Kerberos v の変更とパスワードの設定 (RPCSEC_GSS) |
| | UDP | 137 | Active Directory フォレスト | NetBIOS ネームサービス |
| | UDP | 138 | Active Directory フォレスト | NetBIOS データグラムサービス |
| | UDP | 464 | Active Directory フォレスト | Kerberos キー管理 |

| サービス | プロトコル | ポート | 宛先 | 目的 |
|-------------------------|-------|------|--|---|
| API コールと AutoSupport | HTTPS | 443 | アウトバウンドインターネットおよび ONTAP クラスター管理 LIF | AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信 |
| API コール | TCP | 8088 | S3 へのバックアップ | S3 へのバックアップを API で呼び出します |
| DNS | UDP | 53 | DNS | Cloud Manager による DNS 解決に使用されます |
| クラウドデータの意味 | HTTP | 80 | Cloud Data Sense インスタンス | Cloud Volumes ONTAP に最適なクラウドデータ |

ONTAP には Amazon FSX を使用します

Amazon FSX for ONTAP 作業環境の作成と管理

Cloud Manager を使用すると、ボリュームや追加のデータサービスを追加および管理するために、ONTAP 作業環境用の FSX を作成および管理できます。

ONTAP 作業環境用の Amazon FSX を作成します

最初のステップは、ONTAP 作業環境用の FSX を作成することです。AWS 管理コンソールですでに ONTAP ファイルシステム用の FSX を作成している場合は、次の操作を実行できます ["Cloud Manager で IT を詳細に確認"](#)。

Cloud Manager で FSX for ONTAP の作業環境を作成する前に、次のものがが必要です。

- Cloud Manager に ONTAP 作業環境用の FSX の作成に必要な権限を付与する IAM ロールの ARN 。を参照してください ["Cloud Manager に AWS クレデンシャルを追加しています"](#) を参照してください。
- ONTAP インスタンスの FSX を作成する場所のリージョンおよび VPN 情報。

手順

1. Cloud Manager で、新しい作業環境を追加し、場所 * Amazon Web Services * を選択して、* Next * をクリックします。
2. Amazon FSX for ONTAP * を選択し、* Next * をクリックします。

The screenshot shows the 'Add Working Environment' dialog in the AWS Cloud Manager console. It is divided into two main sections: 'Choose a Location' and 'Choose Type'.

Choose a Location: This section contains four cards: 'Microsoft Azure', 'Amazon Web Services' (which is selected and has a blue checkmark), 'Google Cloud Platform', and 'On-Premises'.

Choose Type: This section contains four cards: 'Cloud Volumes ONTAP Single Node', 'Cloud Volumes ONTAP HA High Availability', 'Amazon FSx for ONTAP High Availability' (which is selected and has a blue checkmark), and 'Kubernetes Cluster Managed'.

At the bottom of the dialog, there is a search bar with the text 'If you want to discover an existing Amazon FSx for ONTAP in AWS, [Click Here](#)'. Below this is a large blue 'Next' button.

3. Cloud Manager で ONTAP の FSX を認証します。
 - a. ご使用のアカウントに、FSX for ONTAP に対する適切な AWS 権限を持つ既存の IAM ロールがある

場合は、ドロップダウンからそのロールを選択します。

- b. アカウントに IAM ロールがない場合は、* クレデンシャルページ * をクリックし、ウィザードの手順に従って、ONTAP クレデンシャル用の FSX を使用して AWS IAM ロールの ARN を追加します。を参照してください "[Cloud Manager に AWS クレデンシャルを追加しています](#)" を参照してください。

4. ONTAP インスタンスの FSX に関する情報を入力します。
- a. 使用する作業環境名を入力します。
 - b. 必要に応じて、プラス記号をクリックし、タグの名前と値を入力してタグを作成できます。

- c. 使用する ONTAP クラスタのパスワードを入力し、確認のためにもう一度入力します。
- d. SVM ユーザに同じパスワードを使用するか、別のパスワードを設定するかを選択します。
- e. 「* 次へ *」をクリックします。

Add FSx for ONTAP Details and Credentials

Details

Working Environment Name ?

Tags Optional

[Add Tags](#)

Credentials

User Name

ONTAP Cluster Password

Confirm ONTAP Cluster Password

☒ Use the same password for SVM user (vsadmin)

5. リージョンと VPC の情報を指定します。

- a. 単一アベイラビリティゾーン*または*複数のアベイラビリティゾーン* HA配置モデルを選択します。

Select HA Deployment Model ☒ Single Availability Zone ☐ Multiple Availability Zones

- b. リージョンとVPCを選択します。

複数のアベイラビリティゾーンについては、各ノードが専用のアベイラビリティゾーンになるように、少なくとも2つのアベイラビリティゾーンのサブネットを選択してください。



Region: us-east-2 | US East (Ohio) VPC: VPC4QA - 10.0.0.0/16 Security Group: Default security group

Node 1

Availability Zone: us-east-2b

Subnet: 10.0.4.0/24

Node 2

Availability Zone: us-east-2c

Subnet: 10.0.3.0/24

- c. デフォルトのセキュリティグループをそのまま使用するか、別のセキュリティグループを選択します。"AWS セキュリティグループ" インバウンドおよびアウトバウンドトラフィックを制御します。これらの情報は AWS 管理者が設定し、に関連付けます "AWS Elastic Network Interface (ENI)"。
- d. 「* 次へ *」をクリックします。
6. `_cidr Range_Empty` を選択し、* Next * をクリックすると、使用可能な範囲が自動的に設定されます。必要に応じて、を使用できます "AWS 転送ゲートウェイ" 範囲を手動で設定します。

Add FSx for ONTAP
Floating IP

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access.

Floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an [AWS transit gateway](#).

CIDR Range

Optional

Example: 10.10.10.10/24

Notice: You must specify a CIDR block that is outside of the CIDR blocks for all VPCs in the selected AWS region.

Previous

Next

7. フローティング IP アドレスへのルートを含むルーティングテーブルを選択します。VPC 内のサブネット用のルーティングテーブルが 1 つ（メインルーティングテーブル）だけの場合は、Cloud Manager によってそのルーティングテーブルに自動的にフローティング IP アドレスが追加されます。「* 次へ *」をクリックして続行します。

Add FSx for ONTAP
Route Tables

Select the route tables that should include routes to the floating IP addresses. This enables client access to volumes. Clients associated with unselected route tables won't have access to volumes. [Learn More](#)

2 Route table

| <input type="checkbox"/> | Name | Main | ID | Associate with Subnets | Tags | |
|-------------------------------------|-------------|------|---------------------------|------------------------|------|---|
| <input checked="" type="checkbox"/> | VPC4QA | Yes | rtb-0880ec9d aeb55d630 | 2 Subnets | 2 | ▼ |
| <input type="checkbox"/> | No tag name | No | rtb-0e0c7d9e a4cf05d66 | 1 Subnet | 1 | ▼ |

Notice: The main route table is the default for the VPC


Previous

Next

8. デフォルトの AWS マスターキーを使用するか、* キーの変更 * をクリックして別の AWS カスタマーマスターキー（CMK）を選択します。CMK の詳細については、を参照してください "AWS KMS のセットアップ"。 「* 次へ *」をクリックして続行します。

Add FSx for ONTAP

Data Encryption

 AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/fsx [Change Key](#)

Previous

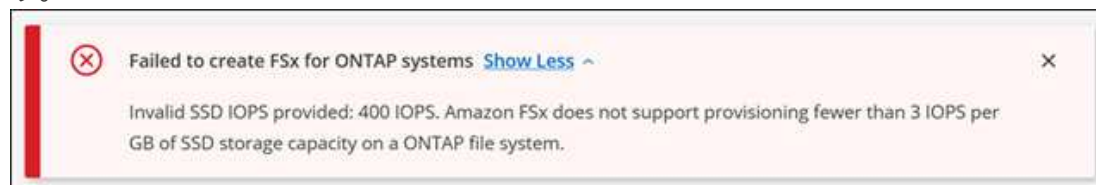
Next

9. ストレージを設定します。

- スループット、容量、単位を選択します。
- 必要に応じて、IOPS 値を指定できます。IOPS の値を指定しない場合、Cloud Manager は、入力した合計容量の 1GiB あたりの 3 IOPS に基づいてデフォルト値を設定します。たとえば、合計容量に 2、000GiB と入力した場合、IOPS の値が指定されていないければ、有効な IOPS の値は 6、000 に設定されます。



最小要件を満たしていない IOPS 値を指定すると、作業環境の追加時にエラーが発生します。



- 「* 次へ *」をクリックします。

Add FSx for ONTAP
Storage Configuration

SSD Disk Properties

Throughput
512 MBps

Capacity
3
Unit
TiB

IOPS Value
400
Optional ⓘ

Notice: The current version of FSx does not allow changing the capacity after creation. Also, note that the capacity drives the cost of the service.

Previous
Next

10. 構成を確認します。

- タブをクリックして、ONTAP のプロパティ、プロバイダのプロパティ、およびネットワーク構成を確認します。
- 任意の設定を変更するには、* 戻る * をクリックします。
- [* 追加 (Add)] をクリックして設定を確定し、作業環境を作成します。

Review

myfsxenvironment
FSx for ONTAP | HA | Multiple AZs

Overview

| ONTAP Properties | Provider Properties | Networking |
|---------------------|----------------------------|------------|
| HA Deployment Model | Multiple Availability Zone | |
| Capacity | 3 TiB | |
| Throughput | 512 MBps | |

Previous
Add

ONTAP 用 FSX の設定は、キャンバスページに表示されます。



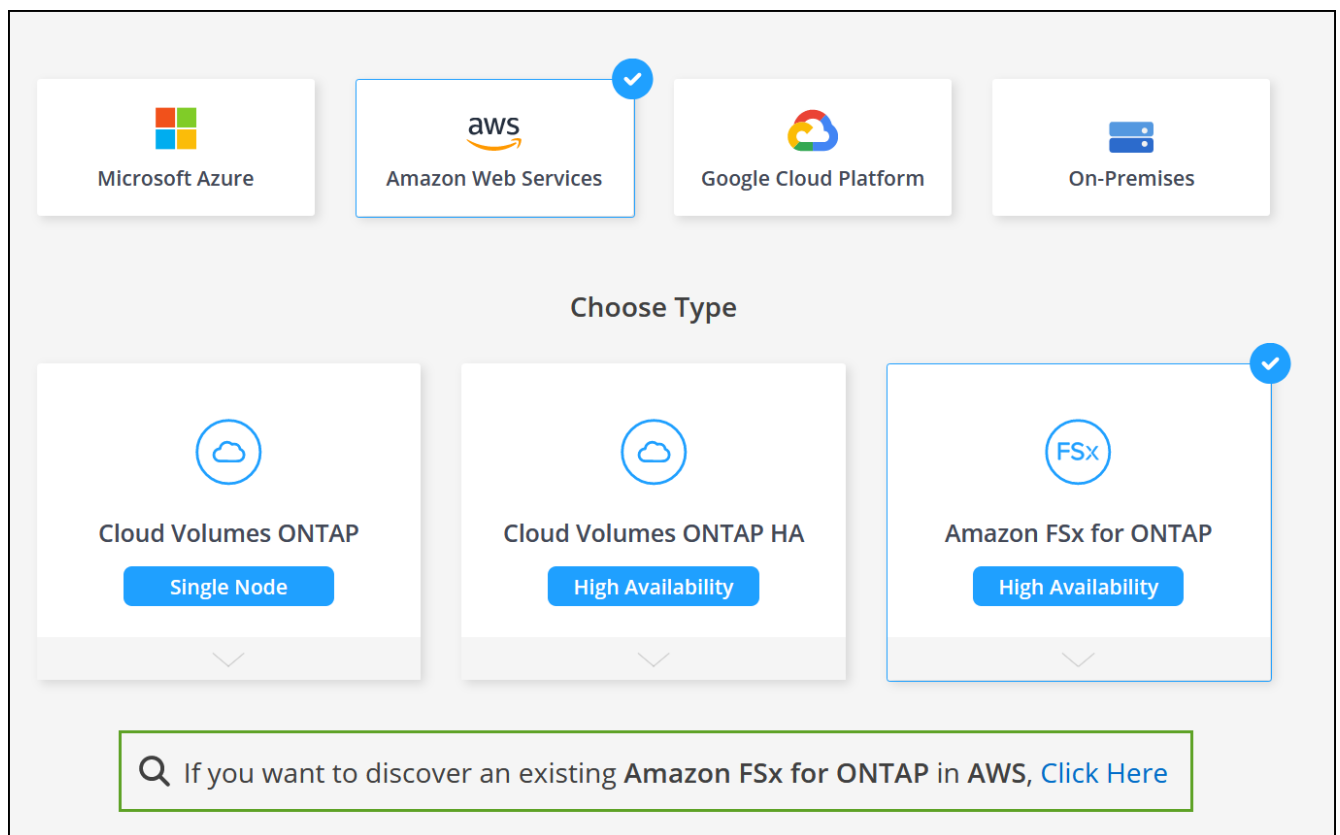
Cloud Manager を使用して、FSX for ONTAP 作業環境にボリュームを追加できるようになりました。

既存の **FSX for ONTAP** ファイルシステムを検出します

AWS 管理コンソールを使用して ONTAP ファイルシステムの FSX を作成した場合、または以前に削除した作業環境をリストアする場合は、Cloud Manager を使用して検出できます。

手順

1. Cloud Manager で、* 作業環境の追加 * をクリックし、* Amazon Web Services * を選択します。
2. Amazon FSX for ONTAP * を選択し、* ここをクリック * します。



3. 既存のクレデンシャルを選択するか、新しいクレデンシャルを「* 次へ *」をクリックします。
4. 追加する AWS リージョンと作業環境を選択します。
5. [追加 (Add)] をクリックします。

Cloud Manager に、検出された ONTAP ファイルシステムの FSX が表示されます。

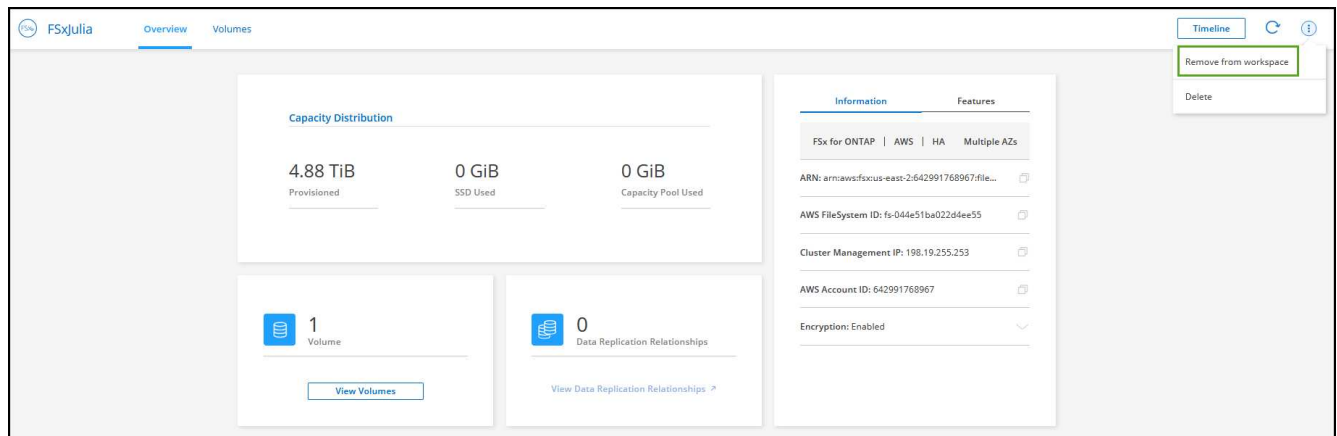


ワークスペースから **ONTAP** の **FSX** を削除します

ONTAP の FSX は、ONTAP アカウントまたはボリュームの FSX を削除することなく、Cloud Manager から削除できます。FSX for ONTAP の作業環境は、いつでも Cloud Manager に追加できます。

手順

1. 作業環境を開きます。AWS にコネクタがない場合は、プロンプト画面が表示されます。これは無視して作業環境の削除に進んでください。
2. ページの右上にあるアクションメニューを選択し、* ワークスペースから削除 * をクリックします。



3. ONTAP 用の FSX を Cloud Manager から削除するには、* Remove * をクリックします。

ONTAP 作業環境の **FSX** を削除します

ONTAP の FSX は、Cloud Manager から削除できます。

作業を開始する前に

- 実行する必要があります **"すべてのボリュームを削除します"** ファイルシステムに関連付けられています。



ボリュームを削除または削除するには、AWS でアクティブなコネクタが必要になります。

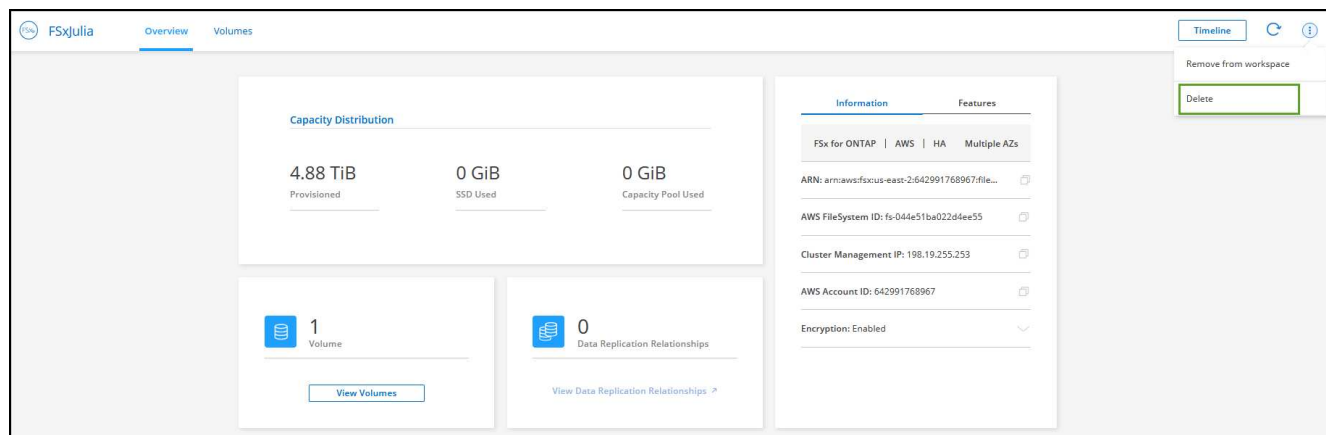
- 障害ボリュームが含まれている作業環境は削除できません。ONTAP ファイルシステムの FSX を削除する前に、AWS 管理コンソールまたは CLI を使用して障害ボリュームを削除する必要があります。



この操作を実行すると、作業環境に関連付けられているすべてのリソースが削除されます。この操作を元に戻すことはできません。

手順

1. 作業環境を開きます。AWS にコネクタがない場合は、プロンプト画面が表示されます。これは無視して作業環境の削除に進んでください。
2. ページの右上にあるアクションメニューを選択し、* 削除 * をクリックします。



3. 作業環境の名前を入力し、* 削除 * をクリックします。

ONTAP 用の Amazon FSX ボリュームを作成します

作業環境をセットアップしたら、ONTAP ボリュームの FSX を作成してマウントできます。

ボリュームを作成します

Cloud Manager では、FSX for ONTAP 作業環境から NFS ボリュームと CIFS ボリュームを作成および管理できます。ONTAP CLI を使用して作成された NFS ボリュームと CIFS ボリュームは、FSX for ONTAP の作業環境にも表示されます。

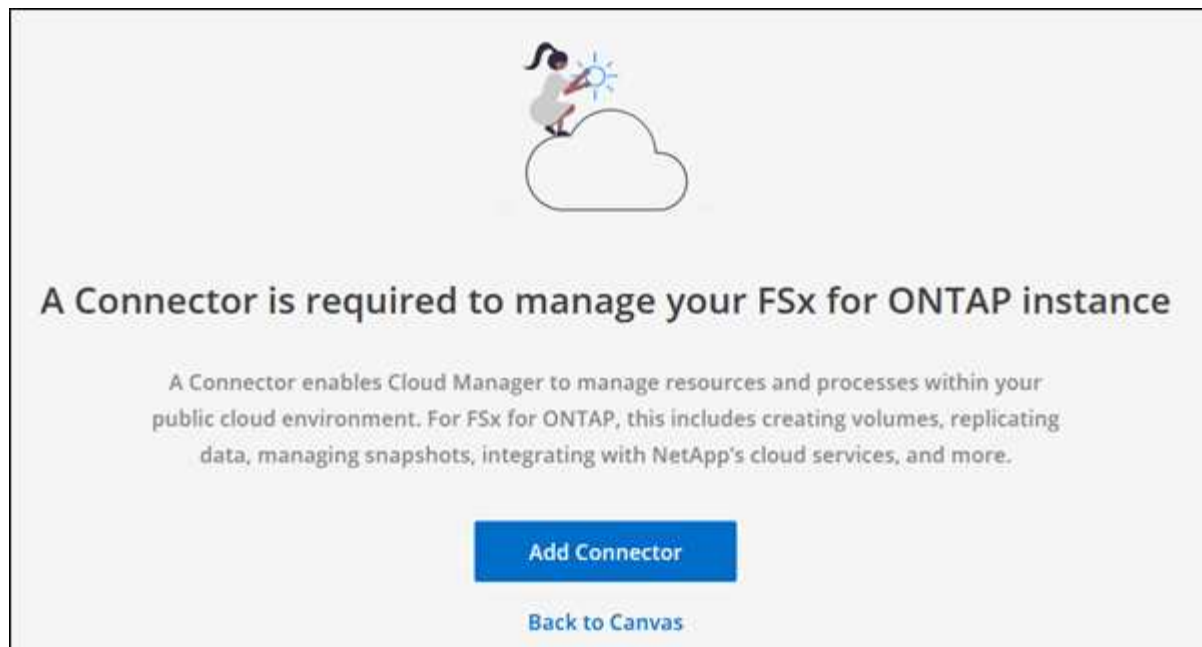
iSCSI ボリュームは、ONTAP CLI、ONTAP API、または Cloud Manager API を使用して作成し、FSX for ONTAP 作業環境で Cloud Manager を使用して管理できます。

必要なもの：

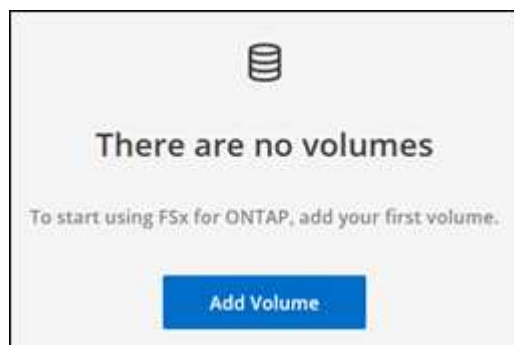
- アクティブです ["AWS のコネクタ"](#)。
- SMB を使用する場合は、DNS と Active Directory を設定しておく必要があります。DNS と Active Directory のネットワーク設定の詳細については、[を参照してください "AWS：自己管理型の Microsoft AD を使用するための前提条件"](#)。

手順

1. FSX for ONTAP 作業環境を開きます。
2. 有効になっているコネクタがない場合は、コネクタを追加するように求められます。



3. [* Volumes (ボリューム)] タブをクリックします
4. [ボリュームの追加] をクリックします。



5. * ボリュームの詳細と保護 * :
 - a. 新しいボリュームの名前を入力します。
 - b. Storage VM (SVM) のフィールドには、作業環境の名前に基づいて SVM が自動的に設定されます。
 - c. ボリュームサイズを入力して単位 (GiB または TiB) を選択します。ボリュームサイズは使用量とともに増加することに注意してください。
 - d. Snapshot ポリシーを選択します。デフォルトでは、Snapshot は 1 時間ごと (最新の 6 つのコピーを保持)、1 日ごと (最新の 2 つのコピーを保持)、および 1 週間ごと (最新の 2 つのコピーを保持) に作成されます。
 - e. 「* 次へ *」をクリックします。

Volume Details & Protection

Volume Name i

Storage VM (SVM)

Volume Size i Unit

Snapshot Policy

default policy i

6. * プロトコル * : NFS または CIFS ボリューム・プロトコルを選択します。

a. NFS の場合 :

- アクセス制御ポリシーを選択します。
- NFS バージョンを選択します。
- カスタムエクスポートポリシーを選択します。有効な値条件の情報アイコンをクリックします。

Volume Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol

Access Control

Select NFS Version ☒ NFSv3 ☒ NFSv4

Custom Export Policy i

b. CIFS の場合 :

- 共有名を入力します。
- ユーザまたはグループをセミコロンで区切って入力します。
- ボリュームの権限レベルを選択します。

✓ Details & Protection

2 Protocol

3 Usage Profile & Tiering Policy

4 Review

Volume Protocol

Select the volume's protocol:

☐ NFS Protocol
☒ CIFS Protocol

Share Name

<Volume name>_share

Users/Groups

Everyone;

Permissions

Full Control



この作業環境で最初に CIFS ボリュームを使用する場合は、_Active Directory_or_Workgroup_setup を使用して CIFS 接続を設定するように求められます。

- Active Directory の設定を選択した場合は、次の設定情報を入力する必要があります。

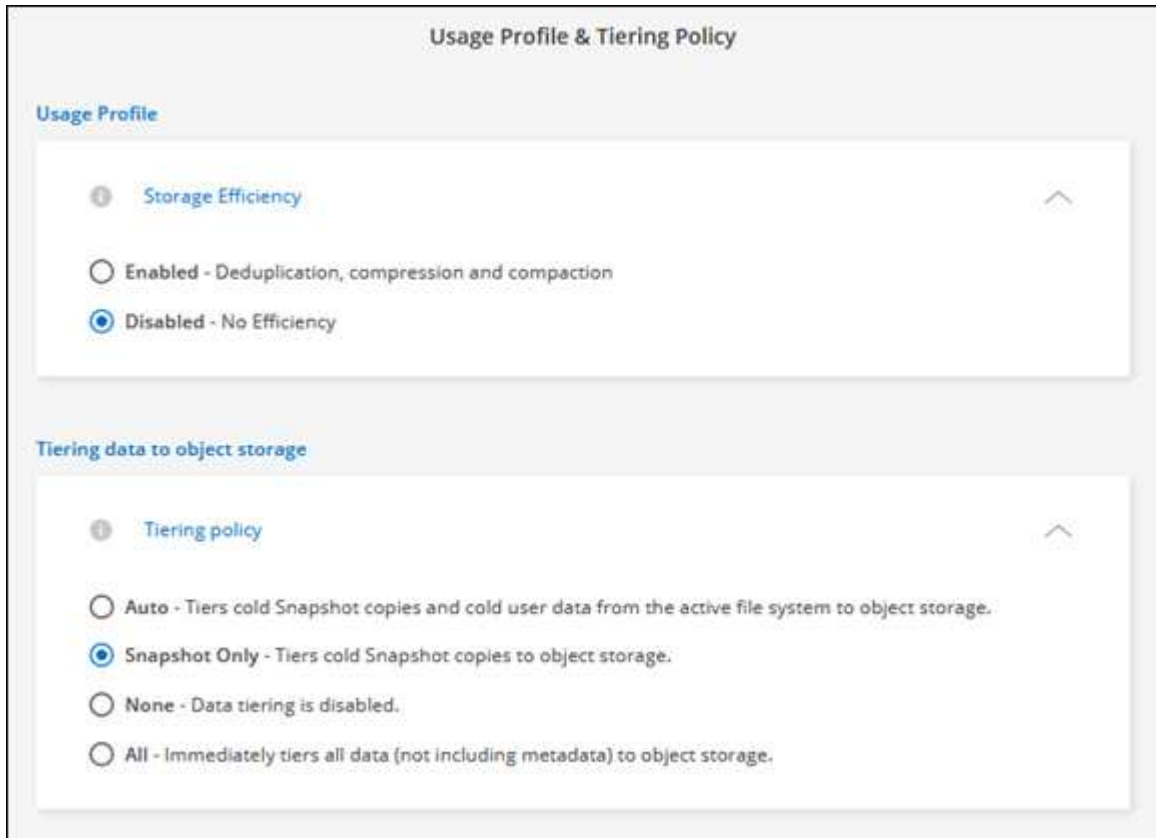
| フィールド | 説明 |
|----------------------------|--|
| DNS プライマリ IP アドレス | CIFS サーバの名前解決を提供する DNS サーバの IP アドレスです。これらの DNS サーバには、Active Directory の LDAP サーバと、CIFS サーバが参加するドメインのドメインコントローラを見つけるために必要なサービスロケーションレコード（SRV）が含まれている必要があります。 |
| 参加する Active Directory ドメイン | CIFS サーバを参加させる Active Directory（AD）ドメインの FQDN。 |
| ドメインへの参加を許可されたクレデンシャル | AD ドメイン内の指定した組織単位（OU）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。 |
| CIFS サーバの NetBIOS 名 | AD ドメイン内で一意の CIFS サーバ名。 |
| 組織単位 | CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 |
| DNS ドメイン | Storage Virtual Machine（SVM）の DNS ドメインです。ほとんどの場合、ドメインは AD ドメインと同じです。 |
| NTP サーバ | Active Directory DNS を使用して NTP サーバを設定するには、* NTP サーバ設定を有効にする * を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、API を使用してください。を参照してください "Cloud Manager 自動化に関するドキュメント" を参照してください。 |

- ワークグループセットアップを選択した場合は、CIFS 用に設定されているワークグループのサーバとワークグループ名を入力します。

a. 「* 次へ *」をクリックします。

7. * 使用状況プロファイルと階層化 * :

- a. デフォルトでは、* Storage Efficiency * は無効になっています。この設定を変更して、重複排除と圧縮を有効にすることができます。
- b. デフォルトでは、* 階層化ポリシー * は * Snapshot のみ * に設定されています。ニーズに応じて別の階層化ポリシーを選択できます。
- c. 「* 次へ *」をクリックします。



8. * 確認 * : ボリューム構成を確認します。設定を変更するには * 戻る * をクリックし、ボリュームを作成するには * 追加 * をクリックします。

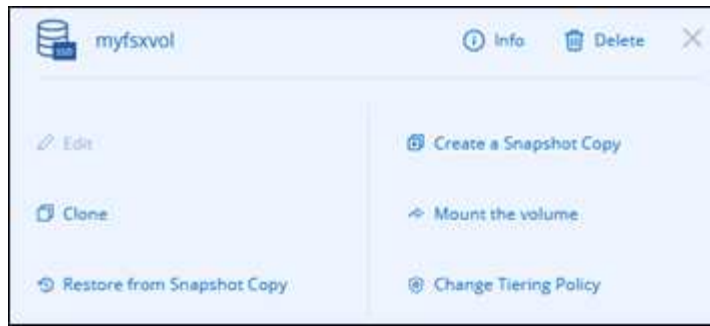
新しいボリュームが作業環境に追加されます。

ボリュームをマウント

Cloud Manager でのマウント手順を参照して、ホストにボリュームをマウントできるようにします。

手順

1. 作業環境を開きます。
2. 音量メニューを開き、「* 音量をマウントする *」を選択します。



3. 指示に従ってボリュームをマウントします。

Amazon FSX for ONTAP のボリュームを管理します

Cloud Manager を使用して、ONTAP のボリューム、クローン、Snapshot の管理、および FSX for の階層化ポリシーの変更を行うことができます。

ボリュームを編集します

作成したボリュームはいつでも変更できます。

手順

1. 作業環境を開きます。
2. 音量メニューを開き、「* 編集 *」を選択します。
 - a. NFS の場合、サイズとタグを変更できます。
 - b. CIFS の場合、共有名、ユーザ、権限、および Snapshot ポリシーを必要に応じて変更できます。
3. [適用 (Apply)] をクリックします。

ボリュームをクローニングする

ボリュームを作成したら、新しい Snapshot から読み書き可能な新しいボリュームを作成できます。

手順

1. 作業環境を開きます。
2. 音量メニューを開き、* Clone * を選択します。
3. クローンボリュームの名前を入力します。
4. [* Clone*] をクリックします。

Snapshot コピーを管理します

Snapshot コピーは、ボリュームのポイントインタイムコピーを提供します。Snapshot コピーを作成し、そのデータを新しいボリュームにリストアします。

手順

1. 作業環境を開きます。

2. ボリュームメニューを開き、Snapshot コピーの管理に使用できるオプションのいずれかを選択します。
 - * Snapshot コピーを作成します *
 - * Snapshot コピーからのリストア *
3. プロンプトに従って、選択した操作を完了します。

階層化ポリシーを変更します

ボリュームの階層化ポリシーを変更します。

手順

1. 作業環境を開きます。
2. ボリュームメニューを開き、* 階層化ポリシーの変更 * を選択します。
3. 新しいボリューム階層化ポリシーを選択し、* Change * をクリックします。

データをレプリケートして同期

Cloud Manager を使用して、ストレージ環境間でデータをレプリケートできます。ONTAP レプリケーション用に FSX を構成するには、を参照してください ["システム間でのデータのレプリケーション"](#)。

Cloud Manager の Cloud Sync を使用して、同期関係を作成できます。同期関係を設定するには、を参照してください ["同期関係を作成する"](#)。

ボリュームを削除します

不要になったボリュームを削除します。

以前に SnapMirror 関係に含まれていたボリュームは、Cloud Manager を使用して削除することはできません。SnapMirror ボリュームは、AWS 管理コンソールまたは CLI を使用して削除する必要があります。

手順

1. 作業環境を開きます。
2. 音量メニューを開き、「* 削除」を選択します。
3. 作業環境の名前を入力し、ボリュームを削除することを確認します。ボリュームが Cloud Manager から完全に削除されるまでに最大 1 時間かかることがあります。



クローンボリュームを削除しようとするエラーが表示されます。

知識とサポート

サポートに登録します

ネットアップテクニカルサポートでサポートケースをオープンするには、事前に Cloud Manager にネットアップサポートサイトのアカウントを追加し、サポートに登録しておく必要があります。

NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

手順

1. ネットアップサポートサイトのアカウントがない場合は、**"1 名で登録します"**。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、*** Support *** を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

3. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、**[* Continue (続行)]** をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

Cloud Manager で NSS アカウントを使用することができます。

注：お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。

アカウントを登録してサポートを受けてください

サポートの登録は、Cloud Manager のサポートダッシュボードで実行できます。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、* Support * を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [* リソース] タブで、[* サポートに登録 *] をクリックします。
3. 登録する NSS 資格情報を選択し、* 登録 * をクリックします。

ヘルプを表示します

ネットアップでは、Cloud Manager とその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

セルフサポート

次のオプションは、1 日 24 時間、週 7 日間無料でご利用いただけます。

- **"ナレッジベース"**

Cloud Manager のナレッジベースで問題のトラブルシューティングに役立つ記事を検索してください。

- **"コミュニティ"**

Cloud Manager コミュニティに参加して、進行中のディスカッションに参加したり、新しいコミュニティを作成したりできます。

- **ドキュメント**

現在表示している Cloud Manager のドキュメント。

- mailto : ng-cloudmanager-feedback@netapp.com [フィードバックメール]

お客様のご意見をお考えください。Cloud Manager の改善に役立つフィードバックを送信します。

ネットアップサポート

上記のセルフサポートオプションに加え、サポートを有効にしたあとに問題が発生した場合は、ネットアップサポートエンジニアと協力して解決できます。

手順

1. Cloud Manager で、 * Help > Support * の順にクリックします。
2. テクニカルサポートで利用可能なオプションのいずれかを選択します。
 - a. [* お問い合わせ *] をクリックして、ネットアップ・テクニカル・サポートの電話番号を検索してください。
 - b. [* 問題 を開く *] をクリックし、いずれかのオプションを選択して、[* 送信 *] をクリックします。

ネットアップの担当者がケースを確認し、すぐに対応を開始します。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

<http://www.netapp.com/us/legal/copyright.aspx>

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/us/media/patents-page.pdf>

プライバシーポリシー

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

- ["Cloud Manager 3.9 に関する注意事項"](#)
- ["Cloud Backup に関する通知です"](#)
- ["クラウドの同期に関する注意事項"](#)
- ["Cloud Tiering への通知"](#)
- ["Cloud Data Sense の通知"](#)

著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp、Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。