はじめに
Amazon FSx for ONTAP

NetApp
April 18, 2022

目次

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。

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 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。

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 SaaS の ID として 952013314444 を入力してください
   - 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": "*"
        }
    ]
}
```

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。
   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

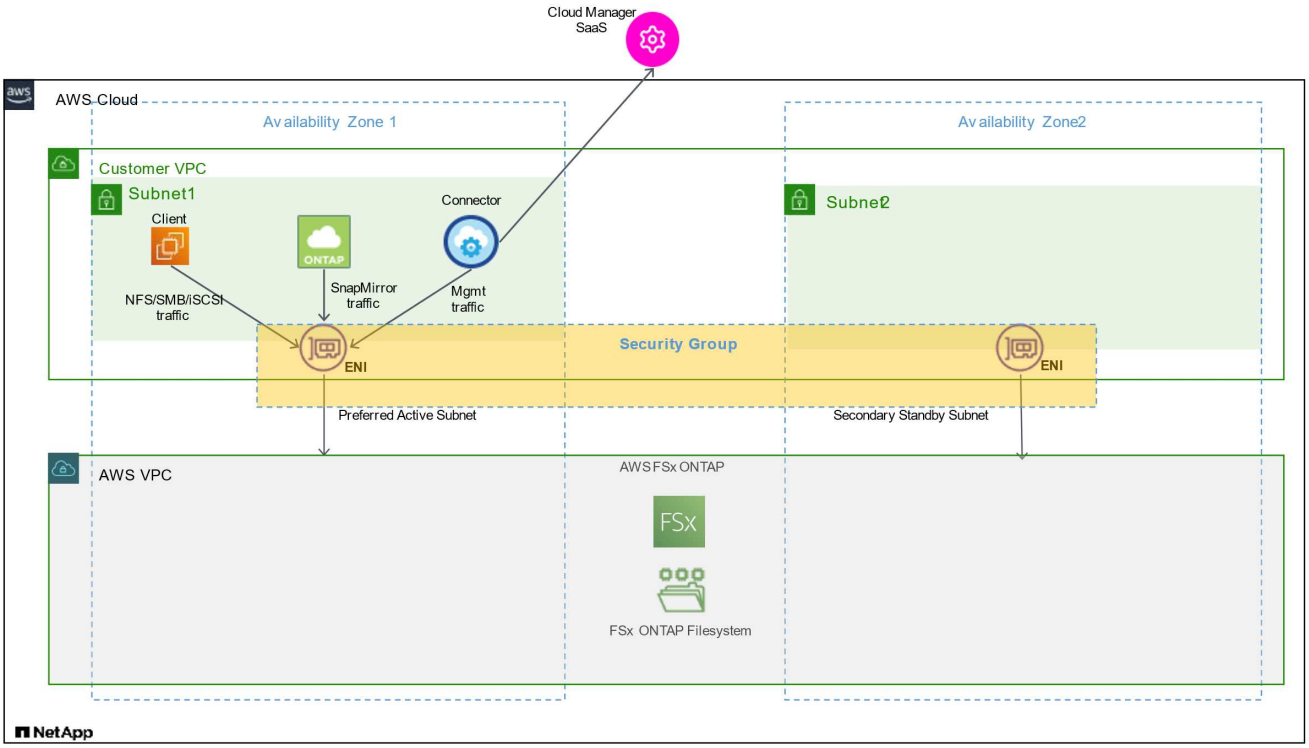
- "AWS のクレデンシャルと権限"
- "Cloud Manager 用の AWS クレデンシャルの管理"

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

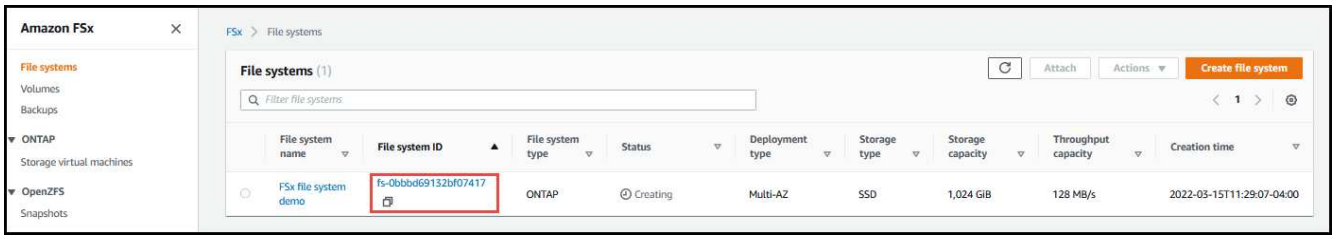
FSX for ONTAP セキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。この図は、 ONTAP ネットワーク構成およびセキュリティグループ要件の FSX を示しています。



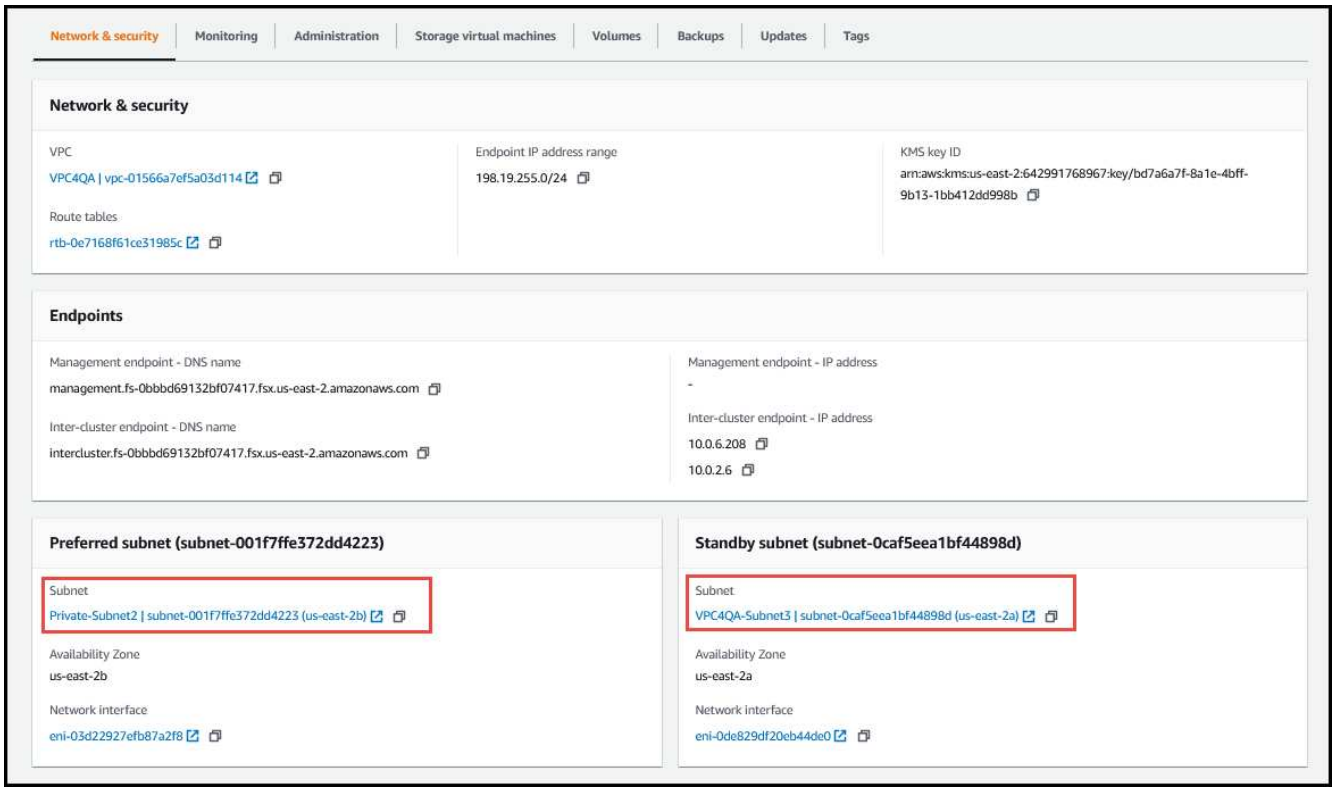
AWS 管理コンソールを使用して、 ENI に関連付けられたセキュリティグループを見つける必要があります。

手順

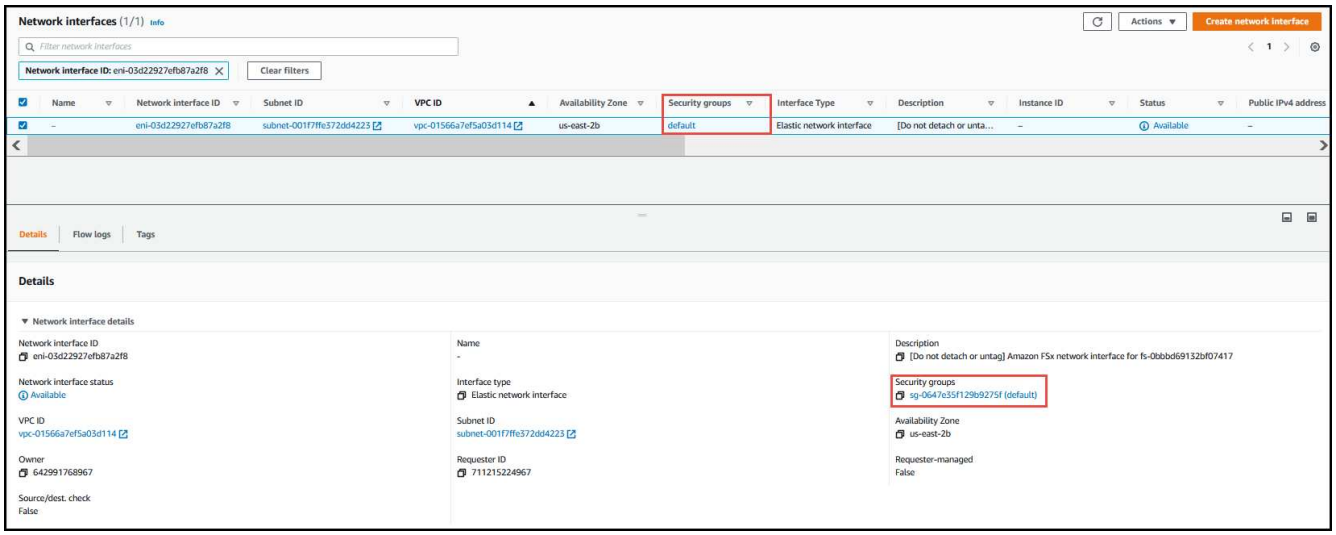
1. AWS 管理コンソールで FSX for ONTAP ファイルシステムを開き、ファイルシステム ID のリンクをクリックします。



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
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス

プロトコル	ポート	目的
HTTPS	443	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
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モニタ
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モニタ
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

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

メディエ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