要件
Amazon FSx for NetApp ONTAP

NetApp
November 28, 2023

目次

要件

ONTAP の FSX のアクセス許可を設定します

FSx for ONTAP作業環境を作成または管理するには、FSx for ONTAP作業環境の作成に必要な権限をBlueXPに付与するIAMロールのARNを指定して、AWSクレデンシャルをBlueXPに追加する必要があります。

IAM ロールを設定します

BlueXPが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. BlueXPにAWSアカウントへのアクセスを許可します。[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。
   - 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、BlueXP *のアカウントID *を入力します。
     - BlueXP SaaSの場合：952013314444
     - AWS GovCloud（US）の場合：033442085313

     セキュリティを強化するには、 "外部*ID*"。AWSアカウントにアクセスするには、BlueXPでロールARN（Amazon Resource Name）と指定した外部IDを指定する必要があります。これにより、 "混乱した副保安官問題"。
3. 必要に応じて、次の必須最小権限とオプションの権限を含むポリシーを作成します。

必要な権限

FSx for NetApp ONTAP ファイルシステムを作成するには、BlueXPで最小限の権限が必要です。

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

自動容量

を有効にするには、さらに次の権限が必要です "容量の自動管理"。

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

セキュリティグループ

BlueXPでを許可するには、次の追加権限が必要です "セキュリティグループを生成します"。

```
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"cloudformation:CreateStack",
"cloudformation:ValidateTemplate",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents"
```

4. IAMロールのARNをコピーして、次の手順でBlueXPに貼り付けられるようにします。

結果

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、BlueXPにARNロールを追加します。

始める前に

IAMロールを作成したばかりの場合は、新しいクレデンシャルが使用可能になるまで数分待ちます。

手順

1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[資格情報*]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. 資格情報の場所：「* Amazon Web Services > BlueXP *」を選択します。
   b. クレデンシャルの定義：*クレデンシャル名*と*ロールARN *および*外部ID *（指定されている場合）を指定します。 IAM ロールを設定します。

   - 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。

結果

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

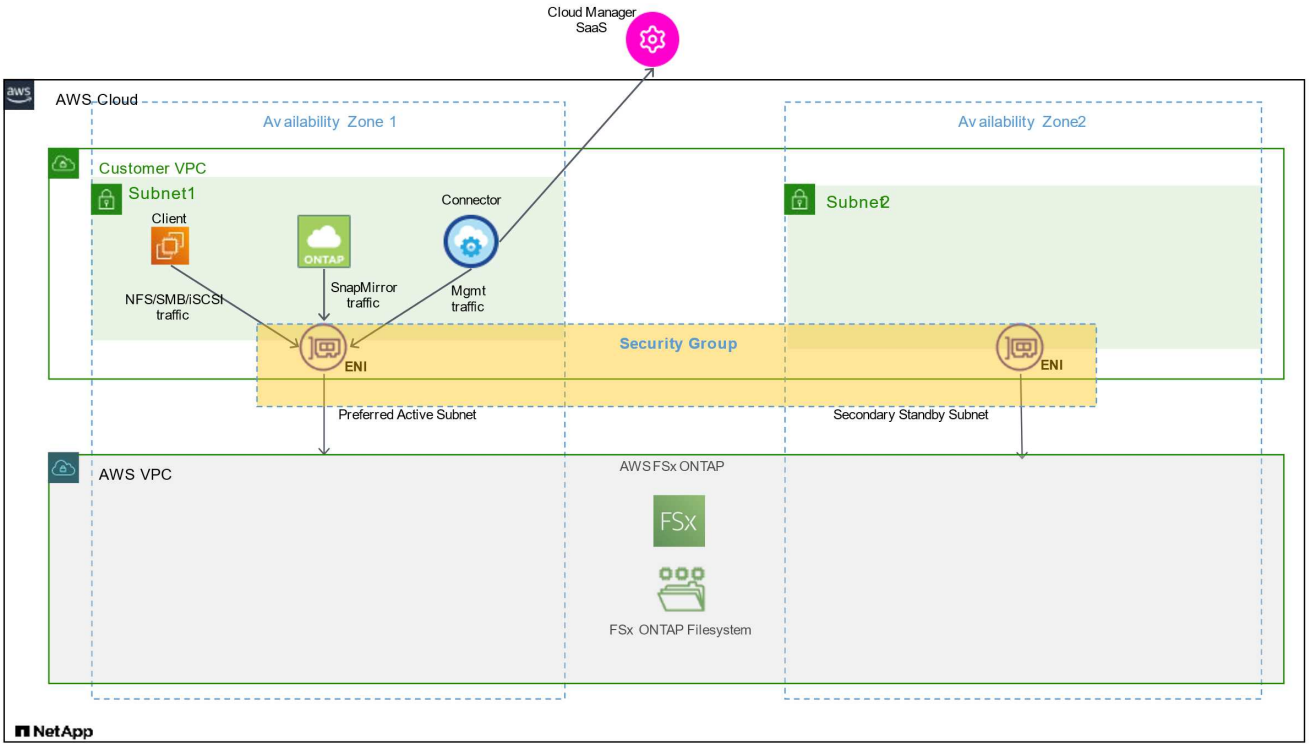
- "AWS のクレデンシャルと権限"
- "BlueXP用のAWS資格情報の管理"

ONTAP の FSX のセキュリティグループルール

BlueXPでは、BlueXPおよび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を含むAWSセキュリティグループが作成されます。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。

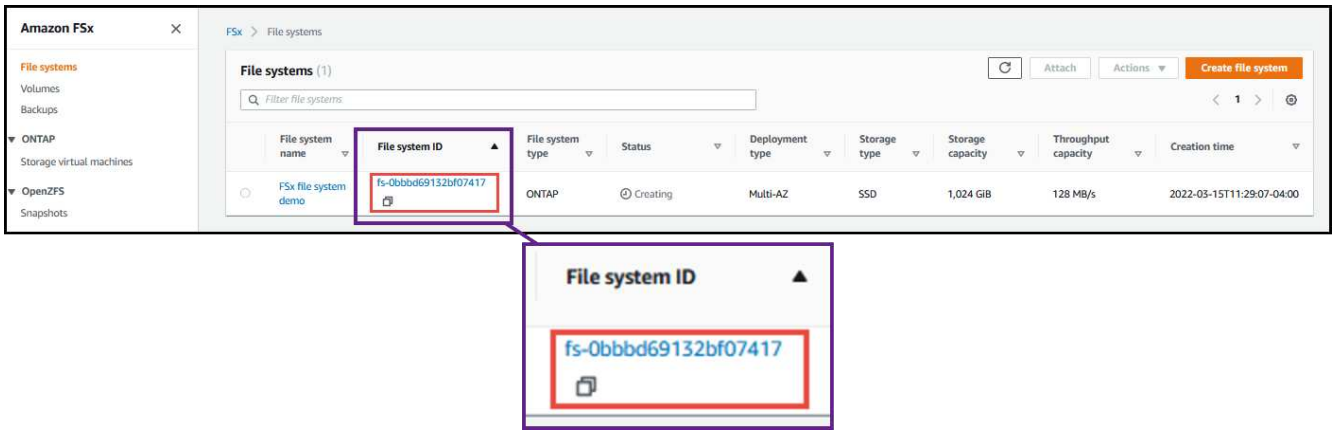


作業を開始する前に

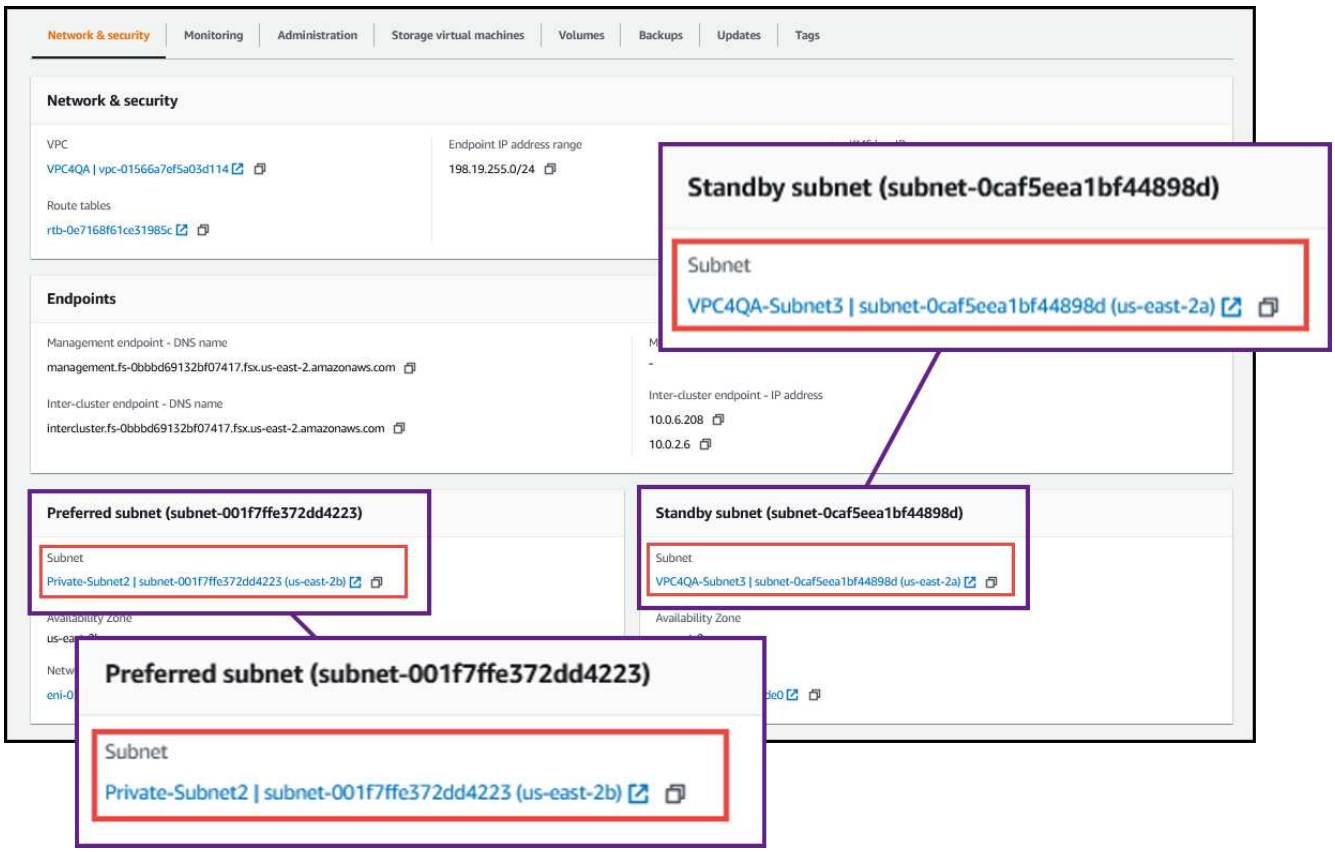
AWS 管理コンソールを使用して、 ENI に関連付けられたセキュリティグループを見つける必要があります。

手順

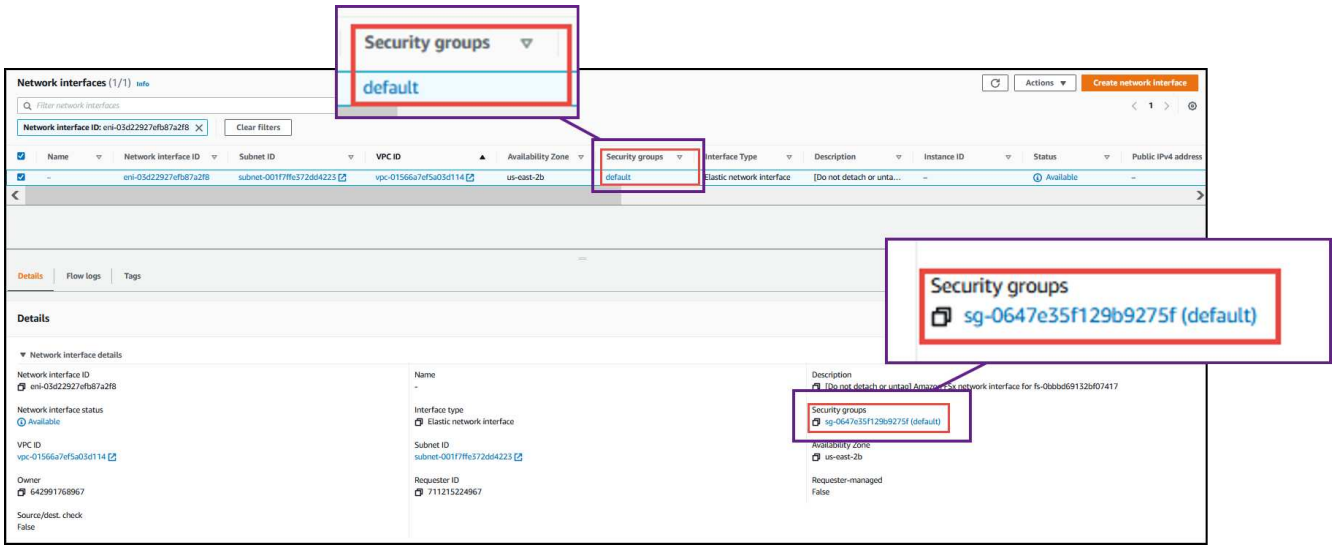
1. AWS 管理コンソールで FSX for ONTAP ファイルシステムを開き、ファイルシステム ID のリンクをクリックします。



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
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

プロトコル	ポート	目的
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
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BlueXP分類インスタンス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、BlueXP分類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	BlueXPによるDNS解決に使用されます
BlueXPの分類	HTTP	80	BlueXPの分類	Cloud Volumes ONTAPではBlueXPに分類されます