De formation

Amazon FSx for NetApp ONTAP

NetApp
August 26, 2024

Sommaire

De formation 1
Configurez les autorisations de FSX pour ONTAP 1
Règles de groupe de sécurité pour FSX pour ONTAP 4

De formation

Configurez les autorisations de FSX pour ONTAP

Pour créer ou gérer un environnement de travail FSX pour ONTAP, vous devez ajouter des informations d'identification AWS à BlueXP en fournissant l'ARN d'un rôle IAM qui donne à BlueXP les autorisations nécessaires pour créer un environnement de travail FSX pour ONTAP.

Configurer le rôle IAM

Configurez un rôle IAM qui permet à BlueXP d'assumer le rôle.

Étapes

1. Accédez à la console IAM dans le compte cible.
2. Accordez l'accès BlueXP au compte AWS. Sous gestion des accès, cliquez sur **rôles > Créer un rôle** et suivez les étapes pour créer le rôle.
   - Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
   - Sélectionnez **un autre compte AWS** et entrez l'identifiant de compte BlueXP **ID** :
     - Pour BlueXP SaaS : 952013314444
     - Pour AWS GovCloud (USA) : 033442085313

     Pour une sécurité accrue, nous vous recommandons de spécifier un "*ID externe*". Pour accéder à votre compte AWS, BlueXP doit fournir le rôle ARN (Amazon Resource Name) et l'identifiant externe que vous avez spécifié. Cela empêche le "problème adjoint confus".
3. Créez une stratégie qui inclut les autorisations minimales requises et facultatives suivantes, si nécessaire.

Autorisations requises

Les autorisations minimales suivantes sont requises pour permettre à BlueXP de créer votre système de fichiers FSX pour NetApp ONTAP.

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

Capacité automatique

Les autorisations supplémentaires suivantes sont requises pour l'activation "gestion automatique de la capacité".

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

Groupes de sécurité

Les autorisations supplémentaires suivantes sont requises pour permettre à BlueXP de "générer des groupes de sécurité".

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

4. Copiez l'ARN du rôle IAM afin de pouvoir le coller dans BlueXP à l'étape suivante.

Résultat

Le rôle IAM dispose désormais des autorisations requises.

Ajoutez les informations d'identification

Une fois que vous avez autorisé le rôle IAM, ajoutez le rôle ARN à BlueXP.

Avant de commencer

Si vous venez de créer le rôle IAM, attendez quelques minutes pour que les nouvelles informations d'identification deviennent disponibles.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.

2. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Informations d'identification Location** : sélectionnez **Amazon Web Services > BlueXP**.
   b. **Définir les informations d'identification** : fournissez un **nom d'identification** et le **rôle ARN** et **ID externe** (si spécifié) que vous avez créés Configurer le rôle IAM.

- Si vous utilisez un compte AWS GovCloud (USA), consultez **j'utilise un compte AWS GovCloud (USA)**.

- L'authentification à l'aide d'AWS GovCloud désactive la plateforme SaaS. Il s'agit d'une modification permanente de votre compte et ne peut pas être annulée.

c. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

Résultat

Vous pouvez maintenant utiliser les informations d'identification lors de la création d'un environnement de travail FSX pour ONTAP.

Liens connexes

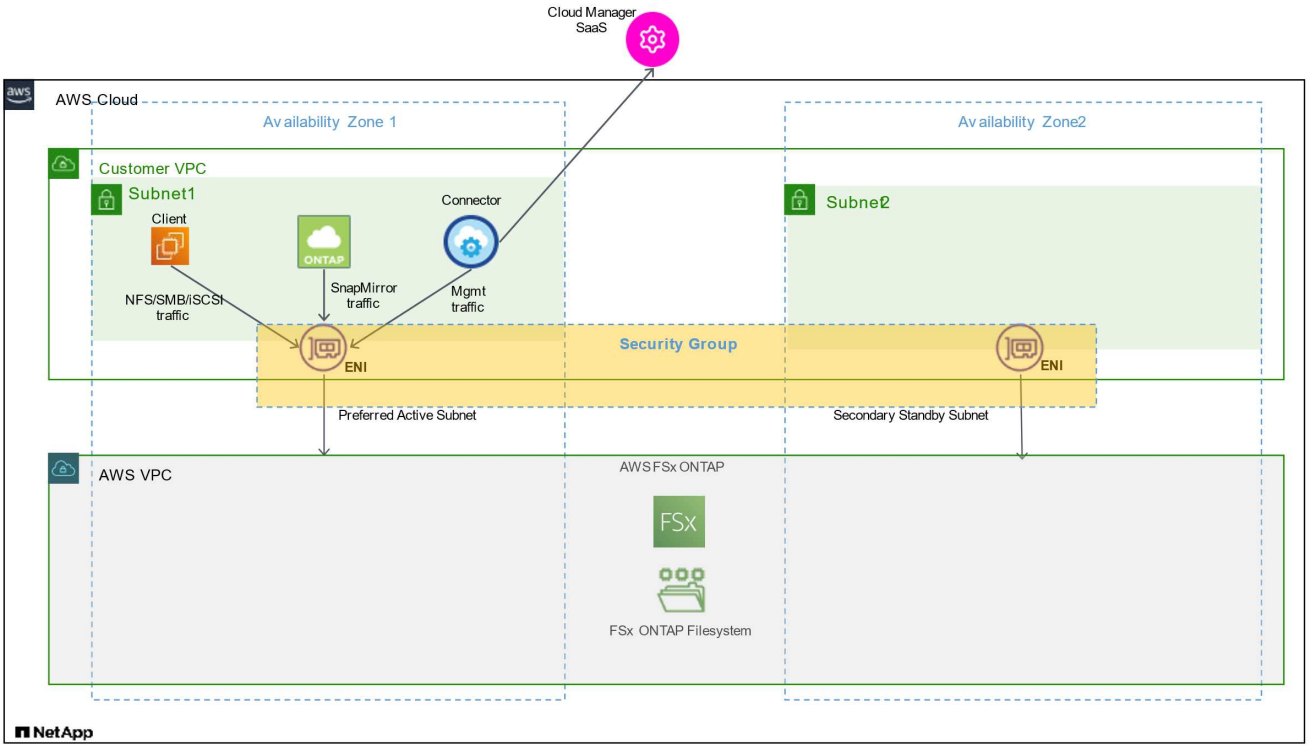
- "Identifiants et autorisations AWS"
- "Gestion des identifiants AWS pour BlueXP"

Règles de groupe de sécurité pour FSX pour ONTAP

BlueXP crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes que BlueXP et FSX pour ONTAP doivent fonctionner correctement. Vous pouvez vous référer aux ports à des fins de test ou si vous devez utiliser votre propre.

Règles pour FSX pour ONTAP

Le groupe de sécurité FSX pour ONTAP requiert des règles entrantes et sortantes. Ce schéma illustre la configuration de la mise en réseau de la solution FSX pour ONTAP et les exigences des groupes de sécurité.

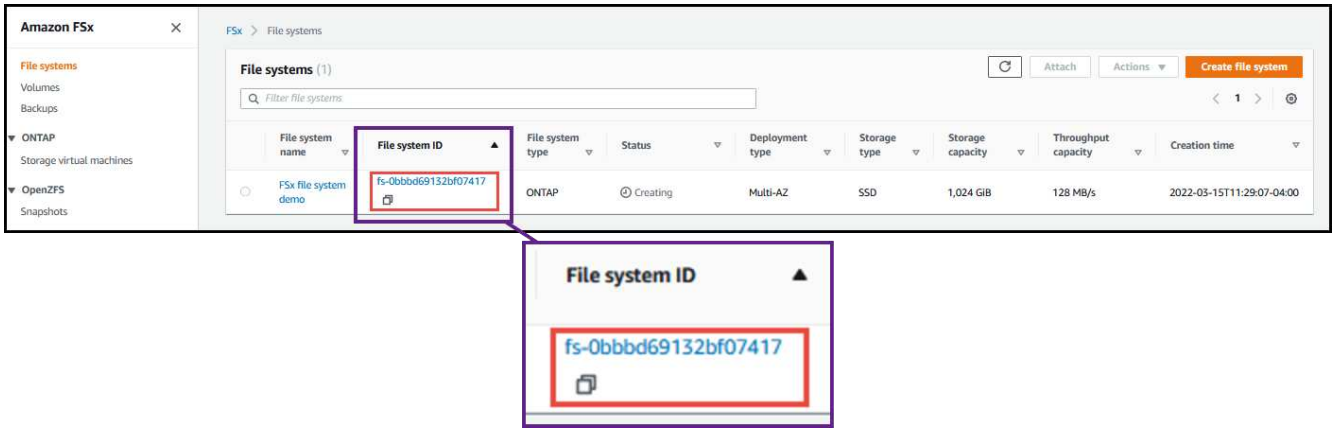


Avant de commencer

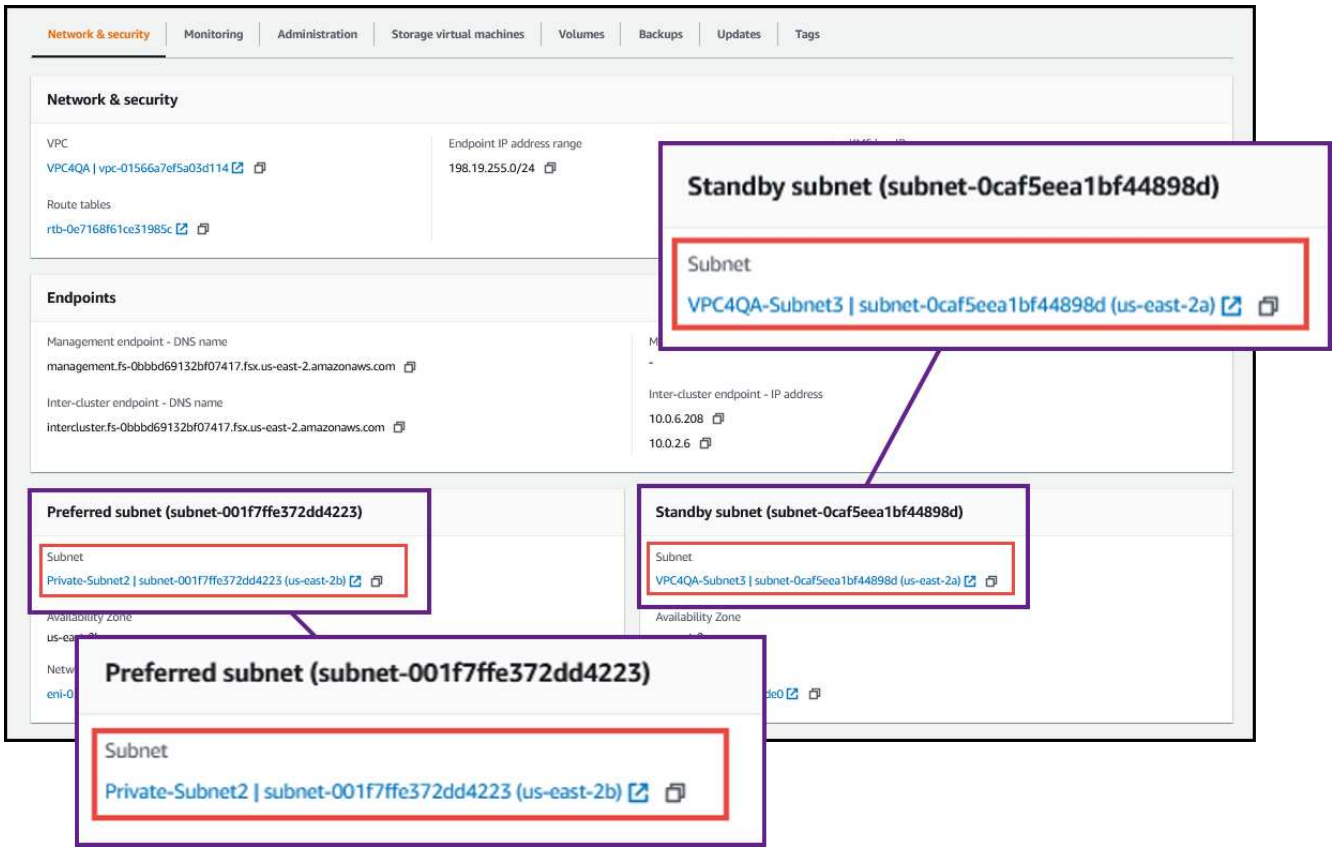
Vous devez localiser les groupes de sécurité associés à Enis à l'aide de la console de gestion AWS.

Étapes

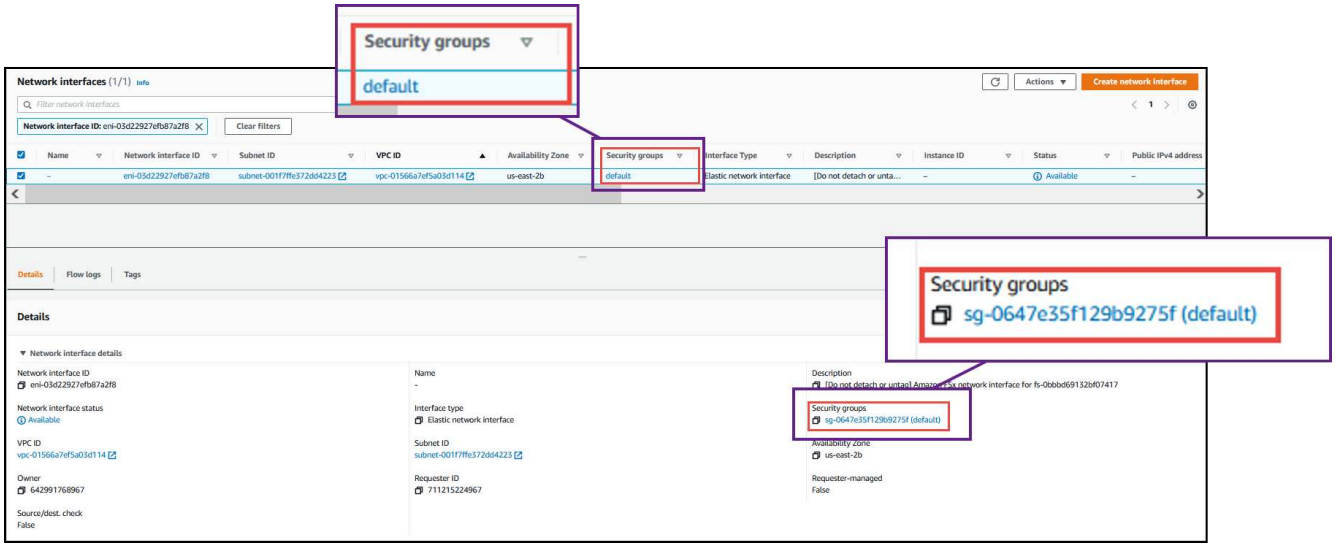
1. Ouvrez le système de fichiers FSX pour ONTAP dans la console de gestion AWS et cliquez sur le lien ID du système de fichiers.



2. Dans l'onglet **réseau et sécurité**, cliquez sur l'ID de l'interface réseau pour le sous-réseau préféré ou de secours.



3. Cliquez sur le groupe de sécurité dans le tableau de l'interface réseau ou dans la section **Détails** de l'interface réseau.



Règles entrantes

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance

Protocole	Port	Objectif
HTTPS	443	Accès depuis le connecteur à la LIF de gestion fsxadmin pour envoyer des appels API à FSX
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour FSX pour ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour FSX pour ONTAP inclut les règles sortantes suivantes.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Tout le trafic sortant

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Il n’est pas nécessaire d’ouvrir des ports spécifiques pour le médiateur ou entre les nœuds de FSX pour ONTAP.

La source est l’interface (adresse IP) du système FSX pour ONTAP.

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3

Service	Protocole	Port	Source	Destination	Objectif
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles pour le connecteur

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à l'interface utilisateur locale depuis les navigateurs Web client et des connexions à partir de l'instance de classification BlueXP

Protocole	Port	Objectif
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Fournit l'instance de classification BlueXP avec un accès Internet, si votre réseau AWS n'utilise pas de NAT ou de proxy

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP
Classification BlueXP	HTTP	80	Classification BlueXP	Classification BlueXP pour Cloud Volumes ONTAP

Informations sur le copyright

Informations sur les marques commerciales