



# Ports

## Setup and administration

NetApp  
April 26, 2024

# Sommaire

- Ports ..... 1
  - Règles du groupe de sécurité du connecteur dans AWS ..... 1
  - Règles du groupe de sécurité du connecteur dans Azure ..... 2
  - Règles de pare-feu du connecteur dans Google Cloud ..... 4
  - Ports pour le connecteur sur site ..... 5

# Ports

## Règles du groupe de sécurité du connecteur dans AWS

Le groupe de sécurité AWS du connecteur nécessite à la fois des règles entrantes et sortantes. BlueXP crée automatiquement ce groupe de sécurité lorsque vous créez un connecteur à partir de BlueXP. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	<ul style="list-style-type: none"><li>Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale</li><li>Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP</li></ul>
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale depuis les navigateurs Web client et des connexions à partir de l'instance de classification BlueXP
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. <a href="#">"Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"</a>
TCP	9060 février 9061	Permet d'activer et d'utiliser la classification BlueXP ainsi que la sauvegarde et la restauration BlueXP dans les régions du gouvernement.

### 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 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
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers AWS, vers ONTAP, vers la classification BlueXP et envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	ONTAP HA médiateur	Communication avec le médiateur ONTAP HA
	TCP	8080	Classification BlueXP	Sonde à instance de classification BlueXP pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

## Règles du groupe de sécurité du connecteur dans Azure

Le groupe de sécurité Azure pour le connecteur nécessite à la fois des règles entrantes et sortantes. BlueXP crée automatiquement ce groupe de sécurité lorsque vous créez un connecteur à partir de BlueXP. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	<ul style="list-style-type: none"><li>Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale</li><li>Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP</li></ul>
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale depuis les navigateurs Web client et des connexions à partir de l'instance de classification BlueXP

Protocole	Port	Objectif
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. <a href="#">"Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"</a>
TCP	9060 février 9061	Permet d'activer et d'utiliser la classification BlueXP ainsi que la sauvegarde et la restauration BlueXP dans les régions du gouvernement.

## 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 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
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers Azure, vers ONTAP, vers la classification BlueXP et envoi de messages AutoSupport à NetApp

Service	Protocole	Port	Destination	Objectif
Appels API	TCP	8080	Classification BlueXP	Sonde à instance de classification BlueXP pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

## Règles de pare-feu du connecteur dans Google Cloud

Les règles de pare-feu Google Cloud pour le connecteur exigent à la fois des règles entrantes et sortantes. BlueXP crée automatiquement ce groupe de sécurité lorsque vous créez un connecteur à partir de BlueXP. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	<ul style="list-style-type: none"> <li>Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale</li> <li>Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP</li> </ul>
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale à partir des navigateurs Web clients
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. <a href="#">"Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"</a>

### Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent 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

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous 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
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers Google Cloud, vers ONTAP, vers la classification BlueXP et envoi de messages AutoSupport à NetApp
Appels API	TCP	8080	Classification BlueXP	Sonde à instance de classification BlueXP pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

## Ports pour le connecteur sur site

Le connecteur utilise des ports *inbound* lorsqu'il est installé manuellement sur un hôte Linux sur site. Vous devrez peut-être vous référer à ces ports à des fins de planification.

Ces règles entrantes s'appliquent à tous les modèles de déploiement BlueXP.

Protocole	Port	Objectif
HTTP	80	<ul style="list-style-type: none"><li>Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale</li><li>Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP</li></ul>
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale à partir des navigateurs Web clients

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.