Ports

Setup and administration

NetApp
April 26, 2024

Sommaire

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	• Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
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. "Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"
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	• Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
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. "Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"
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	• Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
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. "Découvrez comment le connecteur est utilisé comme proxy pour les messages AutoSupport"

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	• Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale à partir des navigateurs Web clients