Ports

NetApp Console setup and administration

NetApp
October 15, 2025

Sommaire

Ports

Règles du groupe de sécurité de l'agent de console dans AWS

Le groupe de sécurité AWS pour l'agent nécessite des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients 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 et aux connexions à partir de l'instance de NetApp Data Classification
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

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

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes 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 l'agent

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers AWS, ONTAP, NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	3000	Médiateur ONTAP HA	Communication avec le médiateur ONTAP HA
	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Règles du groupe de sécurité de l'agent de console dans Azure

Le groupe de sécurité Azure pour l'agent nécessite des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d'installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients à l'interface utilisateur locale et des connexions depuis l'instance de NetApp Data Classification

Protocole	Port	But
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet pour envoyer des messages AutoSupport au support NetApp . Vous devez ouvrir manuellement ce port après le déploiement. "Découvrez comment l'agent est utilisé comme proxy pour les messages AutoSupport"

Règles de sortie

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

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

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

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Azure, vers ONTAP, vers NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Règles de pare-feu d’agent dans Google Cloud

Les règles de pare-feu Google Cloud pour l’agent nécessitent des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d’installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l’hôte de l’agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l’interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers l’interface utilisateur locale
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

Les règles de pare-feu prédéfinies de l’agent ouvrent tout le trafic sortant. Suivez les règles sortantes de base si elles sont acceptables, ou utilisez des règles sortantes avancées pour des exigences plus strictes.

Règles de base pour les voyages sortants

Les règles de pare-feu prédéfinies pour l’agent incluent les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

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

L’adresse IP source est l’hôte de l’agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Google Cloud, vers ONTAP, vers NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par classification des données

Ports pour l'agent de console sur site

L'agent de console utilise les ports *inbound* lorsqu'il est installé manuellement sur un hôte Linux local. Consultez ces ports à des fins de planification.

Ces règles entrantes s'appliquent à tous les modes de déploiement de la NetApp Console .

Protocole	Port	But
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers l'interface utilisateur locale

Informations sur le copyright

Informations sur les marques commerciales