



Ports

NetApp Console setup and administration

NetApp
October 15, 2025

Sommaire

- Ports 1
 - Règles du groupe de sécurité de l’agent de console dans AWS 1
 - Règles entrantes 1
 - Règles de sortie 1
 - Règles du groupe de sécurité de l’agent de console dans Azure 2
 - Règles entrantes 2
 - Règles de sortie 3
 - Règles de pare-feu d’agent dans Google Cloud 4
 - Règles entrantes 4
 - Règles de sortie 4
- Ports pour l’agent de console sur site 5

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	<ul style="list-style-type: none">Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur localeUtilisé 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> 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

Copyright © 2025 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.