Puertos

NetApp Console setup and administration

NetApp
November 10, 2025

Tabla de contenidos

Puertos

Reglas del grupo de seguridad del agente de consola en AWS

El grupo de seguridad de AWS para el agente requiere reglas entrantes y salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando usted crea un agente de consola desde la consola. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
HTTP	80	• Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS a la interfaz de usuario local y conexiones desde la instancia de NetApp Data Classification
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación.

Reglas de salida

El grupo de seguridad predefinido para el agente abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de salida. Si necesita reglas más rígidas, utilice las reglas de salida avanzadas.

Reglas básicas de salida

El grupo de seguridad predefinido para el agente incluye las siguientes reglas de salida.

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede usar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a AWS, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	Mediador de HA de ONTAP	Comunicación con el mediador de ONTAP HA
	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Utilizado para la resolución de DNS por la consola

Reglas del grupo de seguridad del agente de consola en Azure

El grupo de seguridad de Azure para el agente requiere reglas de entrada y de salida. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
HTTP	80	• Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de NetApp Data Classification

Protocolo	Puerto	Objetivo
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp . Debe abrir este puerto manualmente después de la implementación. "Descubra cómo se utiliza el agente como proxy para los mensajes de AutoSupport"

Reglas de salida

El grupo de seguridad predefinido para el agente abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de salida. Si necesita reglas más rígidas, utilice las reglas de salida avanzadas.

Reglas básicas de salida

El grupo de seguridad predefinido para el agente incluye las siguientes reglas de salida.

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a Azure, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Utilizado para la resolución de DNS por la consola

Reglas de firewall del agente en Google Cloud

Las reglas de firewall de Google Cloud para el agente requieren reglas tanto entrantes como salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
HTTP	80	• Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación.

Reglas de salida

Las reglas de firewall predefinidas del agente abren todo el tráfico saliente. Siga las reglas básicas de salida si es aceptable o utilice reglas avanzadas de salida para requisitos más estrictos.

Reglas básicas de salida

Las reglas de firewall predefinidas para el agente incluyen las siguientes reglas de salida.

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a Google Cloud, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Se utiliza para la resolución de DNS mediante clasificación de datos

Puertos para el agente de consola local

El agente de consola utiliza puertos *entrantes* cuando se instala manualmente en un host Linux local. Consulte estos puertos para fines de planificación.

Estas reglas de entrada se aplican a todos los modos de implementación de la NetApp Console .

Protocolo	Puerto	Objetivo
HTTP	80	• Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local