



Puertos

NetApp Console setup and administration

NetApp

November 10, 2025

Tabla de contenidos

- Puertos 1
 - Reglas del grupo de seguridad del agente de consola en AWS 1
 - Reglas de entrada 1
 - Reglas de salida 1
 - Reglas del grupo de seguridad del agente de consola en Azure 2
 - Reglas de entrada 2
 - Reglas de salida 3
 - Reglas de firewall del agente en Google Cloud 4
 - Reglas de entrada 4
 - Reglas de salida 4
 - Puertos para el agente de consola local 5

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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> 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. "Descubre 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.