



Puertos

Setup and administration

NetApp
August 13, 2024

Tabla de contenidos

- Puertos 1
 - Reglas de grupo de seguridad de conector en AWS 1
 - Reglas de grupo de seguridad de conector en Azure 2
 - Reglas de firewall de conector en Google Cloud 4
 - Puertos para el conector en las instalaciones 5

Puertos

Reglas de grupo de seguridad de conector en AWS

El grupo de seguridad de AWS para Connector requiere reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

Reglas de entrada

| Protocolo | Puerto | Específico |
|-----------|--------|--|
| SSH | 22 | Proporciona acceso SSH al host de Connector |
| HTTP | 80 | <ul style="list-style-type: none">• Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario• Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Ofrece acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de clasificación de BlueXP |
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. "Obtenga información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport" |

Reglas de salida

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

Reglas de salida básicas

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

| Protocolo | Puerto | Específico |
|---------------|--------|--------------------------|
| Todos los TCP | Todo | Todo el tráfico saliente |
| Todas las UDP | Todo | Todo el tráfico saliente |

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

| Servicio | Protocolo | Puerto | Destino | Específico |
|----------------------------|-----------|--------|--|--|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres de ONTAP y Internet saliente | Llamadas API a AWS, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 3000 | Mediador de alta disponibilidad de ONTAP | Comunicación con el mediador de alta disponibilidad de ONTAP |
| | TCP | 8080 | Clasificación de BlueXP | Sondee la instancia de clasificación de BlueXP durante la puesta en marcha |
| DNS | UDP | 53 | DNS | Utilizado para resolver DNS por BlueXP |

Reglas de grupo de seguridad de conector en Azure

El grupo de seguridad de Azure para Connector requiere reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

Reglas de entrada

| Protocolo | Puerto | Específico |
|-----------|--------|--|
| SSH | 22 | Proporciona acceso SSH al host de Connector |
| HTTP | 80 | <ul style="list-style-type: none"> Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Ofrece acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de clasificación de BlueXP |

| Protocolo | Puerto | Específico |
|-----------|--------|--|
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. "Obtenga información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport" |

Reglas de salida

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

Reglas de salida básicas

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

| Protocolo | Puerto | Específico |
|---------------|--------|--------------------------|
| Todos los TCP | Todo | Todo el tráfico saliente |
| Todas las UDP | Todo | Todo el tráfico saliente |

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

| Servicio | Protocolo | Puerto | Destino | Específico |
|----------------------------|-----------|--------|--|--|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres de ONTAP y Internet saliente | Llamadas API a Azure, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 8080 | Clasificación de BlueXP | Sondee la instancia de clasificación de BlueXP durante la puesta en marcha |
| DNS | UDP | 53 | DNS | Utilizado para resolver DNS por BlueXP |

Reglas de firewall de conector en Google Cloud

Las reglas de firewall de Google Cloud para el conector requieren reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

Reglas de entrada

| Protocolo | Puerto | Específico |
|-----------|--------|--|
| SSH | 22 | Proporciona acceso SSH al host de Connector |
| HTTP | 80 | <ul style="list-style-type: none">• Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario• Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario |
| TCP | 3128 | Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. "Obtenga información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport" |

Reglas de salida

Las reglas de firewall predefinidas para el conector abren todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

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

| Protocolo | Puerto | Específico |
|---------------|--------|--------------------------|
| Todos los TCP | Todo | Todo el tráfico saliente |
| Todas las UDP | Todo | Todo el tráfico saliente |

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

| Servicio | Protocolo | Puerto | Destino | Específico |
|----------------------------|-----------|--------|--|---|
| Llamadas API y AutoSupport | HTTPS | 443 | LIF de gestión de clústeres de ONTAP y Internet saliente | Llamadas API a Google Cloud, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp |
| Llamadas API | TCP | 8080 | Clasificación de BlueXP | Sondee la instancia de clasificación de BlueXP durante la puesta en marcha |
| DNS | UDP | 53 | DNS | Utilizado para resolver DNS por BlueXP |

Puertos para el conector en las instalaciones

El conector utiliza los puertos *inbound* cuando se instala manualmente en un host Linux local. Es posible que necesite consultar estos puertos para fines de planificación.

Estas reglas de entrada se aplican a todos los modelos de implementación de BlueXP.

| Protocolo | Puerto | Específico |
|-----------|--------|--|
| HTTP | 80 | <ul style="list-style-type: none"> Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP |
| HTTPS | 443 | Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario |

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.