



Ports

Setup and administration

NetApp
April 26, 2024

Inhalt

- Ports 1
 - Regeln für die Connector-Sicherheitsgruppe in AWS 1
 - Regeln für die Connector-Sicherheitsgruppe in Azure 2
 - Connector-Firewall-Regeln in Google Cloud 4
 - Anschlüsse für den On-Prem Connector 5

Ports

Regeln für die Connector-Sicherheitsgruppe in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	<ul style="list-style-type: none">• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche• Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS, ONTAP, BlueXP Klassifizierung und das Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Regeln für die Connector-Sicherheitsgruppe in Azure

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	<ul style="list-style-type: none">• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche• Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet

Protokoll	Port	Zweck
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe zu Azure, zu ONTAP, zur BlueXP Klassifizierung und zum Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Connector-Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	<ul style="list-style-type: none"> Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an Google Cloud, an ONTAP, an BlueXP Klassifizierung und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Anschlüsse für den On-Prem Connector

Der Connector verwendet *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Möglicherweise müssen Sie diese Ports zu Planungszwecken verwenden.

Diese Inbound Regeln gelten für alle BlueXP Implementierungsmodelle.

Protokoll	Port	Zweck
HTTP	80	<ul style="list-style-type: none">• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche• Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.