Ports

Set up and administration

NetApp
December 15, 2022

Inhaltsverzeichnis

Ports

Sicherheitsgruppenregeln in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz
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 mehr über den Proxy-Server des Connectors.
TCP	9060	Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren.

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 und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport-Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Für Sicherheitsgruppen gibt es in Azure Regeln

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz
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 mehr über den Proxy-Server des Connectors.

Protokoll	Port	Zweck
TCP	9060	Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren.

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 Azure und ONTAP, Cloud Data Sense, zum Ransomware-Service und Senden von AutoSupport-Nachrichten an NetApp
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
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 mehr über den Proxy-Server des Connectors.

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 bei GCP und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport Nachrichten an NetApp

Service	Protokoll	Port	Ziel	Zweck
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Anschlüsse für den On-Prem Connector

Der Connector verwendet die folgenden *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird.

Diese eingehenden Regeln gelten für beide Bereitstellungsmodelle für den On-Prem Connector: Installiert mit Internetzugang oder ohne Internetzugang.

Protokoll	Port	Zweck
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche