Ports

Setup and administration

NetApp
September 12, 2023

Table of Contents

Ports

Security group rules in AWS

The AWS security group for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages
TCP	9060, 9061	Provides the ability to enable and use BlueXP classification and BlueXP backup and recovery in Government regions.

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP HA mediator	Communication with the ONTAP HA mediator
	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Security group rules in Azure

The Azure security group for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages
TCP	9060, 9061	Provides the ability to enable and use BlueXP classification and BlueXP backup and recovery in Government regions.

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to Azure, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp
API calls	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Firewall rules in Google Cloud

The Google Cloud firewall rules for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages

Outbound rules

The predefined firewall rules for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined firewall rules for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to Google Cloud, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp
API calls	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Ports for the on-prem Connector

The Connector uses *inbound* ports when installed manually on an on-premises Linux host. You might need to refer to these ports for planning purposes.

These inbound rules apply to all BlueXP deployment models.

Protocol	Port	Purpose
HTTP	80	Provides HTTP access from client web browsers to the local user interface
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

Copyright information

Trademark information