# Ports

## Set up and administration

NetApp
November 07, 2022

# Table of Contents

# Ports

## Security group rules in AWS

The AWS security group for the Connector requires both inbound and outbound rules.

### 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 Cloud Data Sense 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 more about the Connector's proxy server. |
| TCP | 9060 | Provides the ability to enable and use Cloud Data Sense and Cloud Backup in Government Cloud deployments. This port is also required for Cloud Backup if you disable the SaaS interface in your BlueXP account. |

### 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 and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |

| Service | Protocol | Port | Destination | Purpose |
|---|---|---|---|---|
| API calls | TCP | 3000 | ONTAP HA mediator | Communication with the ONTAP HA mediator |
| | TCP | 8088 | Backup to S3 | API calls to Backup to S3 |
| 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.

## 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 Cloud Data Sense 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 more about the Connector's proxy server. |
| TCP | 9060 | Provides the ability to enable and use Cloud Data Sense and Cloud Backup in Government Cloud deployments. This port is also required for Cloud Backup if you disable the SaaS interface in your BlueXP account. |

## 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 and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| 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.

## 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 more about the Connector's proxy server. |

## 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 GCP and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| DNS | UDP | 53 | DNS | Used for DNS resolve by BlueXP |

# Ports for the on-prem Connector

The Connector uses the following *inbound* ports when installed manually on an on-premises Linux host.

These inbound rules apply to both deployment models for the on-prem Connector: installed with internet access or without internet access.

| 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