



# Ports

## Set up and administration

NetApp

November 07, 2022

# Table of Contents

- Ports ..... 1
  - Security group rules in AWS ..... 1
  - Security group rules in Azure ..... 2
  - Firewall rules in Google Cloud ..... 3
  - Ports for the on-prem Connector ..... 4

# 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. <a href="#">Learn more about the Connector's proxy server.</a> |
| 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. <a href="#">Learn more about the Connector's proxy server.</a> |
| 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 | HTTP     | 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. <a href="#">Learn more about the Connector's proxy server.</a> |

### 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

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.