# Security group rules for Azure

## Cloud Manager 3.5

NetApp

11/01/2018

# Table of Contents

# 1. Security group rules for Azure

Cloud Manager creates Azure security groups that include the inbound and outbound rules that Cloud Manager and Cloud Volumes ONTAP need to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own security groups.

## 1.1. Rules for Cloud Manager

The security group for Cloud Manager requires both inbound and outbound rules.

### 1.1.1. Inbound rules for Cloud Manager

The source for inbound rules in the predefined security group is 0.0.0.0/0.

| Protocol | Port | Purpose |
|---|---|---|
| SSH | 22 | Provides SSH access to the Cloud Manager host |
| HTTP | 80 | Provides HTTP access from client web browsers to the Cloud Manager web console |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the Cloud Manager web console |

### 1.1.2. Outbound rules for Cloud Manager

The predefined security group for Cloud Manager 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 Cloud Manager 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 Cloud Manager.

The source IP address is the Cloud Manager host.

| Service | Protocol | Port | Destination | Purpose |
|---|---|---|---|---|
| Active Directory | TCP | 88 | Active Directory forest | Kerberos V authentication |
| | TCP | 139 | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Active Directory forest | LDAP |
| | TCP | 445 | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | TCP | 749 | Active Directory forest | Active Directory Kerberos V change & set password (RPCSEC_GSS) |
| | UDP | 137 | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Active Directory forest | NetBIOS datagram service |
| | UDP | 464 | Active Directory forest | Kerberos key administration |
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP cluster management LIF | API calls to ONTAP |
| DNS | UDP | 53 | DNS | Used for DNS resolve by Cloud Manager |

# 1.2. Rules for Cloud Volumes ONTAP

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

## 1.2.1. Inbound rules for Cloud Volumes ONTAP

The source for inbound rules in the predefined security group is 0.0.0.0/0.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | Pinging the instance |
| HTTP | 80 | HTTP access to the System Manager web console using the IP address of the cluster management LIF |
| HTTPS | 443 | HTTPS access to the System Manager web console using the IP address of the cluster management LIF |
| SSH | 22 | SSH access to the IP address of the cluster management LIF or a node management LIF |
| TCP | 111 | Remote procedure call for NFS |
| TCP | 139 | NetBIOS service session for CIFS |

| Protocol | Port | Purpose |
|---|---|---|
| TCP | 161-162 | Simple network management protocol |
| TCP | 445 | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| TCP | 635 | NFS mount |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS server daemon |
| TCP | 3260 | iSCSI access through the iSCSI data LIF |
| TCP | 4045 | NFS lock daemon |
| TCP | 4046 | Network status monitor for NFS |
| TCP | 10000 | Backup using NDMP |
| TCP | 11104 | Management of intercluster communication sessions for SnapMirror |
| TCP | 11105 | SnapMirror data transfer using intercluster LIFs |
| UDP | 111 | Remote procedure call for NFS |
| UDP | 161-162 | Simple network management protocol |
| UDP | 635 | NFS mount |
| UDP | 2049 | NFS server daemon |
| UDP | 4045 | NFS lock daemon |
| UDP | 4046 | Network status monitor for NFS |
| UDP | 4049 | NFS rquotad protocol |

## 1.2.2. Outbound rules for Cloud Volumes ONTAP

The predefined security group for Cloud Volumes ONTAP 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 Cloud Volumes ONTAP includes the following outbound rules.

| Protocol | Port | Purpose |
|---|---|---|
| All ICMP | All | All outbound traffic |
| 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 Cloud Volumes ONTAP.

The source is the interface (IP address) on the Cloud Volumes ONTAP system.

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| Active Directory | TCP | 88 | Node management LIF | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Node management LIF | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Node management LIF | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Node management LIF | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Node management LIF | Active Directory forest | LDAP |
| | TCP | 445 | Node management LIF | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Node management LIF | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Node management LIF | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Node management LIF | Active Directory forest | Kerberos V change & set Password (RPCSEC_GSS) |
| | TCP | 88 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V authentication |
| | UDP | 137 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS name service |
| | UDP | 138 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS datagram service |
| | TCP | 139 | Data LIF (NFS, CIFS) | Active Directory forest | NetBIOS service session |
| | TCP | 389 | Data LIF (NFS, CIFS) | Active Directory forest | LDAP |
| | TCP | 445 | Data LIF (NFS, CIFS) | Active Directory forest | Microsoft SMB/CIFS over TCP with NetBIOS framing |
| | TCP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (SET_CHANGE) |
| | UDP | 464 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos key administration |
| | TCP | 749 | Data LIF (NFS, CIFS) | Active Directory forest | Kerberos V change & set password (RPCSEC_GSS) |

| Service | Protocol | Port | Source | Destination | Purpose |
|---|---|---|---|---|---|
| DHCP | UDP | 68 | Node management LIF | DHCP | DHCP client for first-time setup |
| DHCPS | UDP | 67 | Node management LIF | DHCP | DHCP server |
| DNS | UDP | 53 | Node management LIF and data LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | Node management LIF | Destination servers | NDMP copy |
| SMTP | TCP | 25 | Node management LIF | Mail server | SMTP alerts, can be used for AutoSupport |
| SNMP | TCP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 161 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | TCP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| | UDP | 162 | Node management LIF | Monitor server | Monitoring by SNMP traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |