



Requirements

Amazon FSx for ONTAP

NetApp
April 05, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-fsx-ontap/requirements/task-setting-up-permissions-fsx.html> on April 05, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Requirements 1
 - Set up permissions for FSx for ONTAP 1
 - Security group rules for FSx for ONTAP 2

Requirements

Set up permissions for FSx for ONTAP

To create or manage an Amazon FSx for ONTAP working environment, you need to add AWS credentials to Cloud Manager by providing the ARN of an IAM role that gives Cloud Manager the permissions needed to create an FSx for ONTAP working environment.

Set up the IAM role

Set up an IAM role that enables the Cloud Manager SaaS to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

Be sure to do the following:

- Under **Trusted entity type**, select **AWS account**.
- Select **Another AWS account** and enter the ID of the Cloud Manager SaaS: 952013314444
- Create a policy that includes the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "kms:Describe*",
        "kms:List*",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

3. Copy the Role ARN of the IAM role so that you can paste it in Cloud Manager in the next step.

Result

The IAM role now has the required permissions.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to Cloud Manager.

Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



2. Click **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location:** Select **Amazon Web Services > Cloud Manager**.
 - b. **Define Credentials:** Provide the ARN (Amazon Resource Name) of the IAM role.
 - c. **Review:** Confirm the details about the new credentials and click **Add**.

Result

You can now use the credentials when creating an FSx for ONTAP working environment.

Related links

- [AWS credentials and permissions](#)
- [Managing AWS credentials for Cloud Manager](#)

Security group rules for FSx for ONTAP

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

Rules for FSx for ONTAP

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

Inbound rules

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 |

| Protocol | Port | Purpose |
|----------|---------|---|
| 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 |
| 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 |

Outbound rules

The predefined security group for FSx for 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 FSx for 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 FSx for ONTAP.



The source is the interface (IP address) on the FSx for 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 & UDP | 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, iSCSI) | 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 & UDP | 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) |
| Backup to S3 | TCP | 5010 | Intercluster LIF | Backup endpoint or restore endpoint | Back up and restore operations for the Backup to S3 feature |

| Service | Protocol | Port | Source | Destination | Purpose |
|------------|-------------|---------------------|--|----------------------------|--|
| Cluster | All traffic | All traffic | All LIFs on one node | All LIFs on the other node | Intercluster communications (Cloud Volumes ONTAP HA only) |
| | TCP | 3000 | Node management LIF | HA mediator | ZAPI calls (Cloud Volumes ONTAP HA only) |
| | ICMP | 1 | Node management LIF | HA mediator | Keep alive (Cloud Volumes ONTAP HA only) |
| 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 | 1860 0–18 699 | 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 | 1110 4 | Intercluster LIF | ONTAP intercluster LIFs | Management of intercluster communication sessions for SnapMirror |
| | TCP | 1110 5 | Intercluster LIF | ONTAP intercluster LIFs | SnapMirror data transfer |
| Syslog | UDP | 514 | Node management LIF | Syslog server | Syslog forward messages |

Rules for the Connector

The 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 |

| Protocol | Port | Purpose |
|----------|------|---|
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface and connections from Cloud Data Sense |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface |
| TCP | 3128 | Provides the Cloud Data Sense instance with internet access, if your AWS network doesn't use a NAT or proxy |

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 |
|---------------------------|----------|------|--|--|
| 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 |

| 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 Cloud Manager |
| Cloud Data Sense | HTTP | 80 | Cloud Data Sense instance | Cloud Data Sense for Cloud Volumes ONTAP |

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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.