



Get started

Amazon FSx for ONTAP

NetApp
May 16, 2022

Table of Contents

- Get started 1
 - Learn about Amazon FSx for ONTAP 1
 - Get started with Amazon FSx for ONTAP 2
 - Set up permissions for FSx for ONTAP 2
 - Security group rules for FSx for ONTAP 4

Get started

Learn about Amazon FSx for ONTAP

[Amazon FSx for ONTAP](#) is a fully managed service allowing customers to launch and run file systems powered by NetApp's ONTAP storage operating system. FSx for ONTAP provides the same features, performance, and administrative capabilities NetApp customers use on premises, with the simplicity, agility, security, and scalability of a native AWS service.

Features

- No need to configure or manage storage devices, software, or backups.
- Support for CIFS, NFSv3, NFSv4.x, and SMB v2.0 - v3.1.1 protocols.
- Low cost, virtually unlimited data storage capacity using available Infrequently Accessed (IA) storage tier.
- Certified to run on latency-sensitive applications including Oracle RAC.
- Choice of bundled and pay-as-you-go pricing.

Additional features in Cloud Manager

- Using a Connector in AWS and Cloud Manager, you can create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as Data Sense and Cloud Sync.
- Using Artificial Intelligence (AI) driven technology, Cloud Data Sense can help you understand data context and identify sensitive data that resides in your FSx for ONTAP accounts. [Learn more](#).
- Using NetApp Cloud Sync, you can automate data migration to any target in the cloud or on premises. [Learn more](#)

Cost

Your FSx for ONTAP account is maintained by AWS and not by Cloud Manager. [Amazon FSx for ONTAP getting started guide](#)

There is an additional cost associated with using the Connector in AWS and the optional data services such as Cloud Sync and Data Sense.

Supported regions

[View supported Amazon regions.](#)

Getting help

Amazon FSx for ONTAP is an AWS first-party solution. For questions or technical support issues associated with your AWS FSx file system, infrastructure or any AWS solution using this service, use the Support Center in your AWS console to open a support case to AWS. Select the "FSx for ONTAP" service and appropriate category. Provide the remaining information required to create your AWS support case.

For general questions specific to Cloud Manager or Cloud Manager micro-services, you can start with the in-line Cloud Manager chat.

For technical support issues specific to Cloud Manager or micro-services within, you can open a NetApp support ticket using your Cloud Manager account level serial number. You will need to register your Cloud Manager serial number to activate support.

Limitations

- Cloud Manager can replicate data only from on-premises or Cloud Volumes ONTAP to FSx for ONTAP.
- At this time iSCSI volumes can be created using the ONTAP CLI, ONTAP API, or Cloud Manager API.

Get started with Amazon FSx for ONTAP

Get started with Amazon FSx for ONTAP in a few steps.

You can get started with FSx for ONTAP in just a few steps.

1

Create an FSx for ONTAP working environment

You must create an Amazon FSx for ONTAP working environment before adding volumes. You will need to [set up an IAM role that enables the Cloud Manager SaaS to assume the role](#).

2

Create a Connector

You must have a [Connector for AWS](#) to open the FSx for ONTAP working environment, create volumes, or perform other actions. When a Connector is required, Cloud Manager will prompt you if one is not already added.

3

Add volumes

You can create FSx for ONTAP volumes using Cloud Manager.

4

Manage your volumes

Use Cloud Manager to manage your volumes and configure additional services such as replication, Cloud Sync, and Data Sense.

Related links

- [Creating a Connector from Cloud Manager](#)
- [Launching a Connector from the AWS Marketplace](#)
- [Installing the Connector software on a Linux host](#)

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

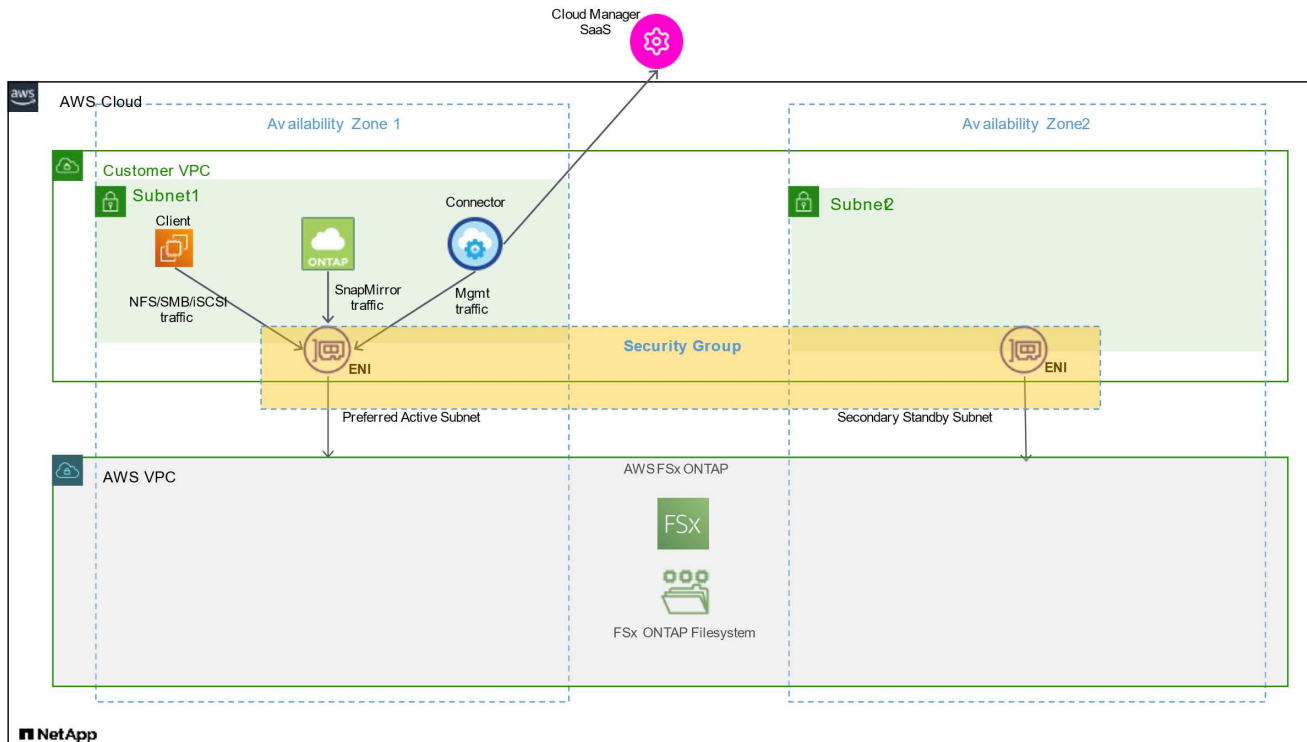
- [AWS credentials and permissions](#)
- [Managing AWS credentials for Cloud Manager](#)

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 FSx for ONTAP security group requires both inbound and outbound rules. This diagram illustrates FSx for ONTAP networking configuration and security group requirements.

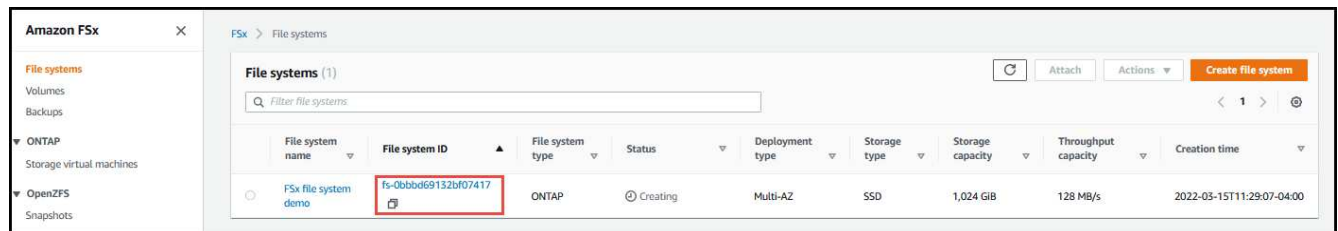


Before you begin

You need to locate the security groups associated with the ENIs using the AWS Management Console.

Steps

1. Open the FSx for ONTAP file system in the AWS Management Console and click the file system ID link.



2. On the **Network & security** tab, click the network interface ID for the preferred or standby subnet.

Network & security | Monitoring | Administration | Storage virtual machines | Volumes | Backups | Updates | Tags

Network & security

VPC VPC4QA vpc-01566a7ef5a03d114	Endpoint IP address range 198.19.255.0/24	KMS key ID arn:aws:kms:us-east-2:642991768967:key/bd7a6a7f-8a1e-4bff-9b13-1bb412dd998b
Route tables rtb-0e7168f61ce31985c		

Endpoints

Management endpoint - DNS name management.fs-0bbbd69132bf07417.fsx.us-east-2.amazonaws.com	Management endpoint - IP address -
Inter-cluster endpoint - DNS name intercluster.fs-0bbbd69132bf07417.fsx.us-east-2.amazonaws.com	Inter-cluster endpoint - IP address 10.0.6.208 10.0.2.6

Preferred subnet (subnet-001f7fe372dd4223)

Subnet
Private-Subnet2 | subnet-001f7fe372dd4223 (us-east-2b)

Availability Zone
us-east-2b

Network interface
eni-03d22927efb87a2f8

Standby subnet (subnet-0caf5eea1bf44898d)

Subnet
VPC4QA-Subnet3 | subnet-0caf5eea1bf44898d (us-east-2a)

Availability Zone
us-east-2a

Network interface
eni-0de829df20eb44de0

3. Click the security group in the network interface table or the **Details** section for the network interface.

Network interfaces (1/1) info

Filter network interfaces

Network interface ID: eni-03d22927efb87a2f8

Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security groups	Interface Type	Description	Instance ID	Status	Public IPv4 address
-	eni-03d22927efb87a2f8	subnet-001f7fe372dd4223	vpc-01566a7ef5a03d114	us-east-2b	default	Elastic network interface	[Do not detach or untag]	-	Available	-

Details | Flow logs | Tags

Details

Network interface details

<p>Network interface ID eni-03d22927efb87a2f8</p> <p>Network interface status Available</p> <p>VPC ID vpc-01566a7ef5a03d114</p> <p>Owner 642991768967</p> <p>Source/dest. check False</p>	<p>Name -</p> <p>Interface type Elastic network interface</p> <p>Subnet ID subnet-001f7fe372dd4223</p> <p>Requester ID 711215224967</p>	<p>Description [Do not detach or untag] Amazon FSx network interface for fs-0bbbd69132bf07417</p> <p>Security groups sg-0647c35f129b9275f (default)</p> <p>Availability Zone us-east-2b</p> <p>Requester-managed False</p>
---	---	--

Inbound rules

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

Protocol	Port	Purpose
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

You do not need to open specific ports for the mediator or between nodes in 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)

Service	Protocol	Port	Source	Destination	Purpose
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
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
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

Protocol	Port	Purpose
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
API calls	TCP	8088	Backup to S3	API calls to Backup to S3
DNS	UDP	53	DNS	Used for DNS resolve by Cloud Manager

Service	Protocol	Port	Destination	Purpose
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.