Requirements

Amazon FSx for NetApp ONTAP

NetApp
February 11, 2024

Table of Contents

Requirements

Set up permissions for FSx for ONTAP

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

Set up the IAM role

Set up an IAM role that enables BlueXP to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Grant BlueXP access to the AWS account. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.
   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the BlueXP **Account ID**:
     - For BlueXP SaaS: 952013314444
     - For AWS GovCloud (US): 033442085313

     For increased security, we suggest you specify an *External ID*. To access your AWS account, BlueXP will have to provide the role ARN (Amazon Resource Name) and the external ID you specified. This prevents the confused deputy problem.
3. Create a policy that includes the following required minimum permissions and optional permissions, as needed.

Required permissions

The following minimum permissions are required to allow BlueXP to create your FSx for NetApp ONTAP file system.

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

Automatic capacity

The following additional permissions are required to enable automatic capacity management.

```
"cloudwatch:GetMetricData",
"cloudwatch:GetMetricStatistics"
```

Security groups

The following additional permissions are required to allow BlueXP to generate security groups.

```
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"cloudformation:CreateStack",
"cloudformation:ValidateTemplate",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents"
```

4. Copy the role ARN of the IAM role so that you can paste it in BlueXP 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 BlueXP.

Before you get started

If you just created the IAM role, wait a few minutes for the new credentials to become available.

Steps

1. In the upper right of the BlueXP 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 > BlueXP**.
   b. **Define Credentials**: Provide a **Credentials name** and the **Role ARN** and **External ID** (if specified) you created when you Set up the IAM role.

- If you use an AWS GovCloud (US) account, check **I use an AWS GovCloud (US) account**.

- Authenticating using AWS GovCloud will disable the SaaS platform. This is a permanent change to your account and cannot be undone.

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

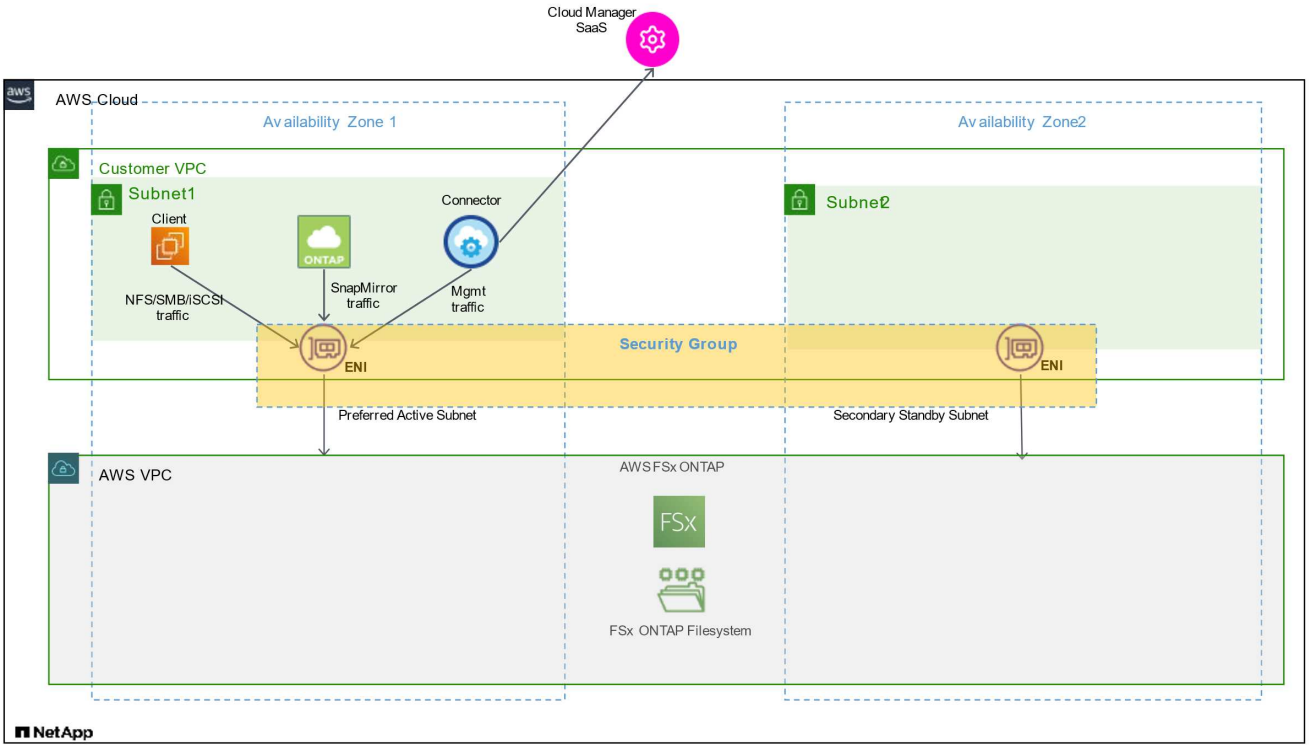
- AWS credentials and permissions
- Managing AWS credentials for BlueXP

Security group rules for FSx for ONTAP

BlueXP creates AWS security groups that include the inbound and outbound rules that BlueXP 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.

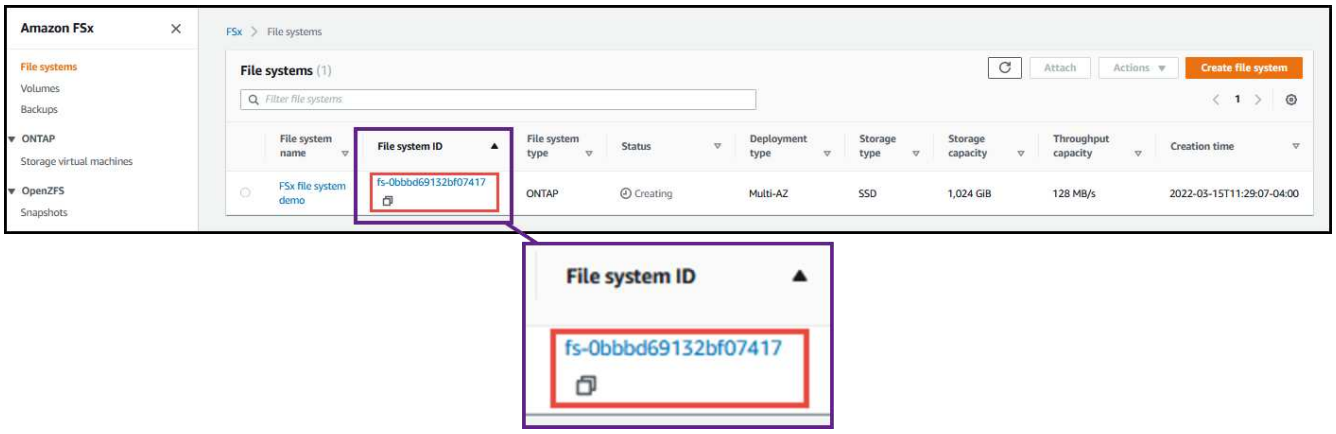


Before you begin

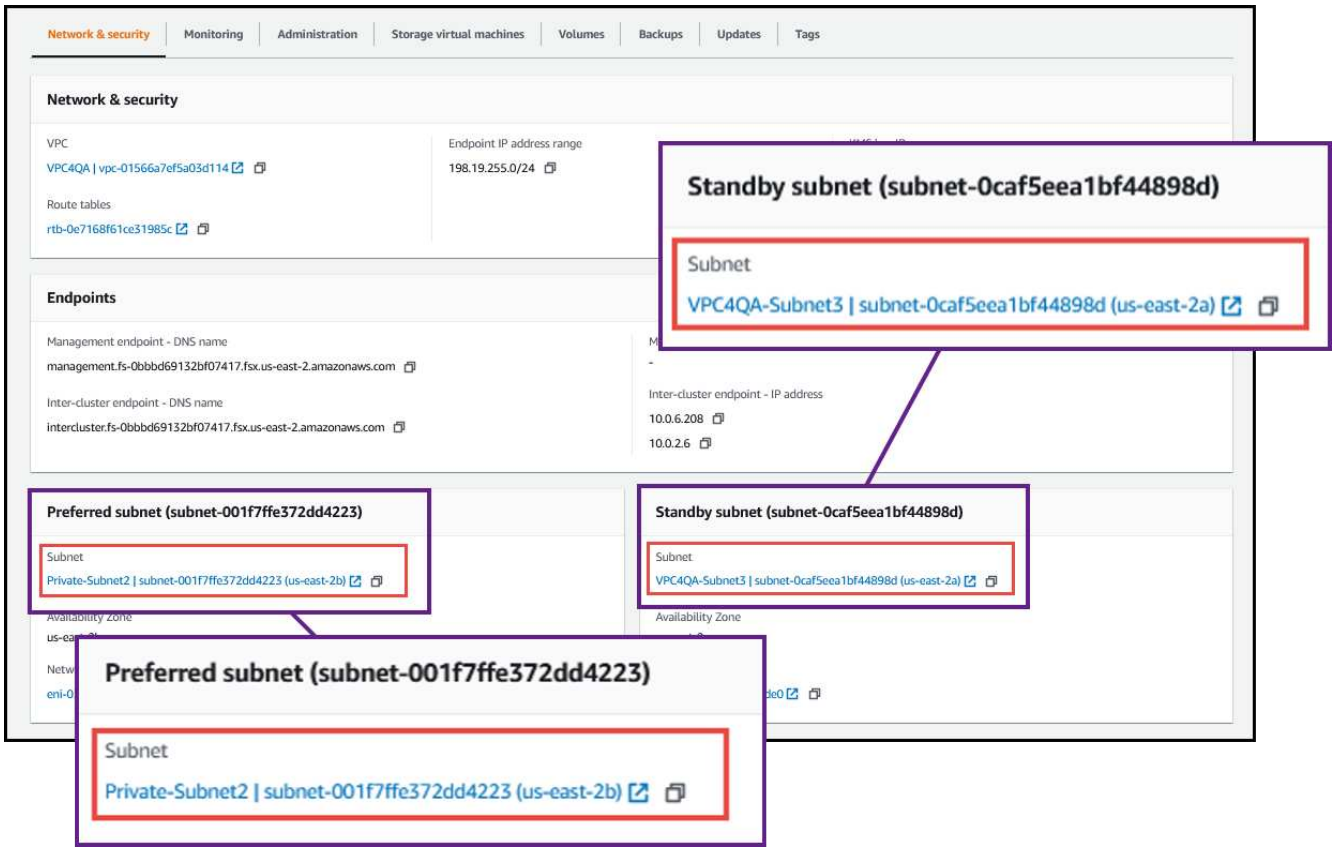
You need to locate the security groups associated with the ENIs using the AWS Management Console.

Steps

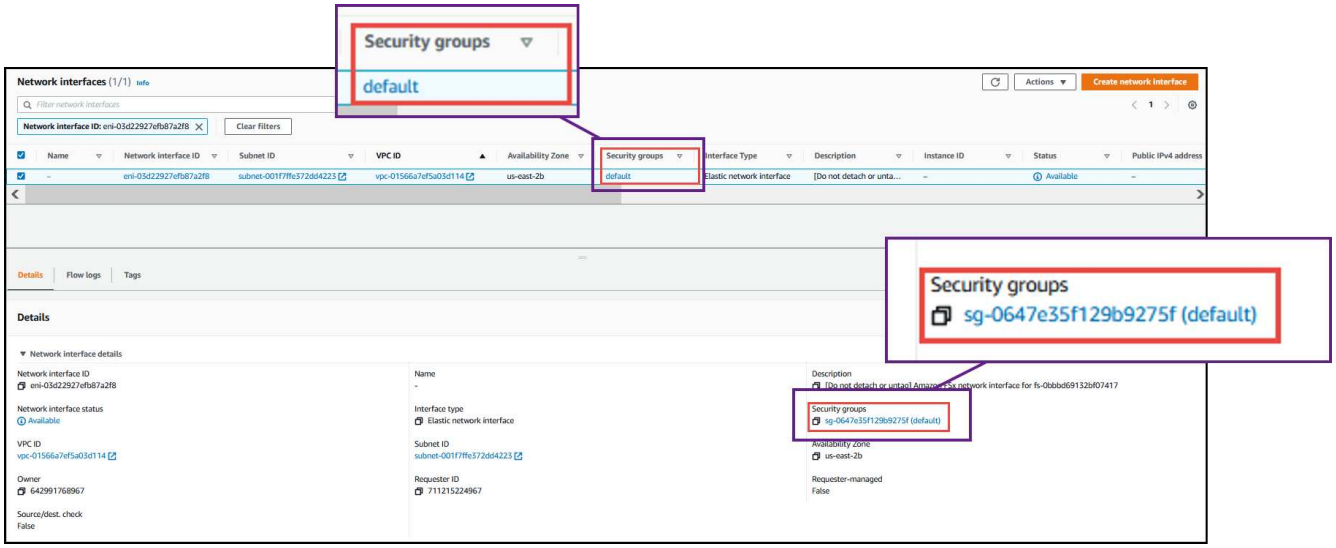
1. Open the FSx for ONTAP file system in the AWS Management Console and click the file system ID link.



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



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



Inbound rules

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTPS	443	Access from the Connector to fsxadmin management LIF to send API calls to FSx
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF

Protocol	Port	Purpose
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)
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
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

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 BlueXP classification instance
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides the BlueXP classification 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 BlueXP
BlueXP classification	HTTP	80	BlueXP classification	BlueXP classification for Cloud Volumes ONTAP

Copyright information

Trademark information