要求

Amazon FSx for NetApp ONTAP

NetApp
November 28, 2023

目录

要求

为适用于 ONTAP 的 FSX 设置权限

要创建或管理FSx for ONTAP工作环境、您需要向BlueXP添加AWS凭据、方法是提供IAM角色的ARN、为BlueXP提供创建FSx for ONTAP工作环境所需的权限。

设置 IAM 角色

设置一个IAM角色、使BlueXP能够承担此角色。

步骤

1. 转到目标帐户中的 IAM 控制台。
2. 授予BlueXP对AWS帐户的访问权限。在访问管理下，单击 * 角色 > 创建角色 * ，然后按照步骤创建角色。
   - 在 * 可信实体类型 * 下，选择 * AWS 帐户 * 。
   - 选择*另一个AWS帐户*并输入BlueXP 帐户**ID**：
     - 对于BlueXP SaaS：952013314444
     - 对于AWS GovCloud (美国)：033442085313

     为了提高安全性、建议您指定 "外部ID_"。要访问您的AWS帐户、BlueXP必须提供角色ARN (Amazon资源名称)和您指定的外部ID。这会阻止 "令人困惑的副问题"。

3. 根据需要创建一个包含以下所需最低权限和可选权限的策略。

所需权限

要允许BlueXP创建FSx for NetApp ONTAP 文件系统、需要具备以下最低权限。

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

自动容量

要启用、需要具备以下附加权限 "自动容量管理"。

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

安全组

要允许BlueXP执行此操作、需要具备以下附加权限 "生成安全组"。

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

4. 复制IAM角色的角色ARN、以便在下一步中将其粘贴到BlueXP中。

结果

IAM 角色现在具有所需的权限。

添加凭据

为IAM角色提供所需权限后、将角色ARN添加到BlueXP中。

开始之前

如果您刚刚创建了IAM角色、请等待几分钟、以使新凭据可用。

步骤

1. 在BlueXP控制台的右上角、单击设置图标、然后选择*凭据*。

2. 单击 * 添加凭据 * ，然后按照向导中的步骤进行操作。
   a. 凭据位置：选择* Amazon Web Services > BlueX*。
   b. 定义身份凭证：提供*身份凭证名称*以及您在创建时创建的*角色ARN*和*外部ID*(如果已指定) 设置 IAM 角色。

   - 如果您使用的是AWS GovCloud (US)帐户、请选中*我使用的是AWS GovCloud (US)帐户*。

   - 使用AWS GovCloud进行身份验证将禁用SaaS平台。这是对您的帐户的永久更改、无法撤消。

   c. * 查看 * ：确认有关新凭据的详细信息，然后单击 * 添加 * 。

结果

现在，您可以在创建适用于 ONTAP 的 FSX 工作环境时使用这些凭据。

相关链接

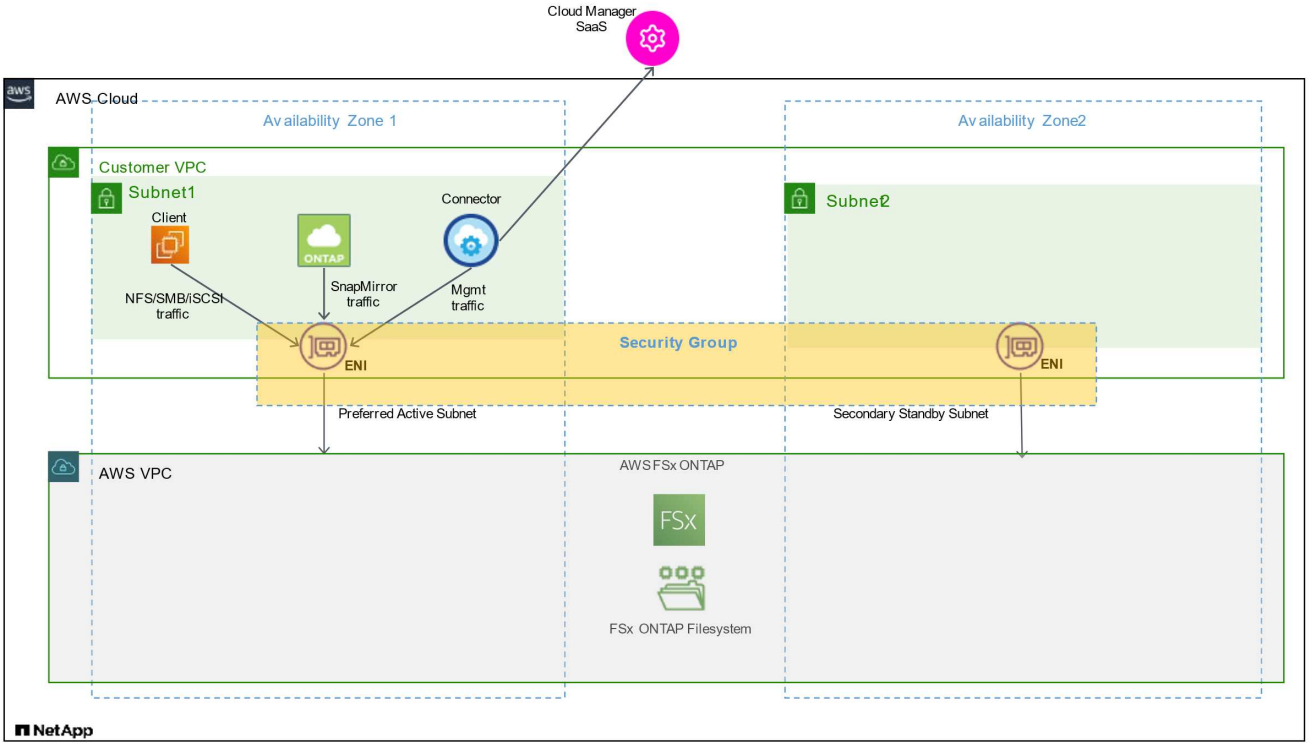
- "AWS 凭据和权限"
- "管理BlueXP的AWS凭据"

适用于 ONTAP 的 FSX 的安全组规则

BlueXP创建了AWS安全组、其中包含了BlueXP和适用于ONTAP 的FSX成功运行所需的入站和出站规则。您可能需要参考端口进行测试，或者需要使用自己的端口。

适用于 ONTAP 的 FSX 的规则

ONTAP 的 FSX 安全组需要入站和出站规则。此图显示了适用于 ONTAP 的 FSX 网络配置和安全组要求。

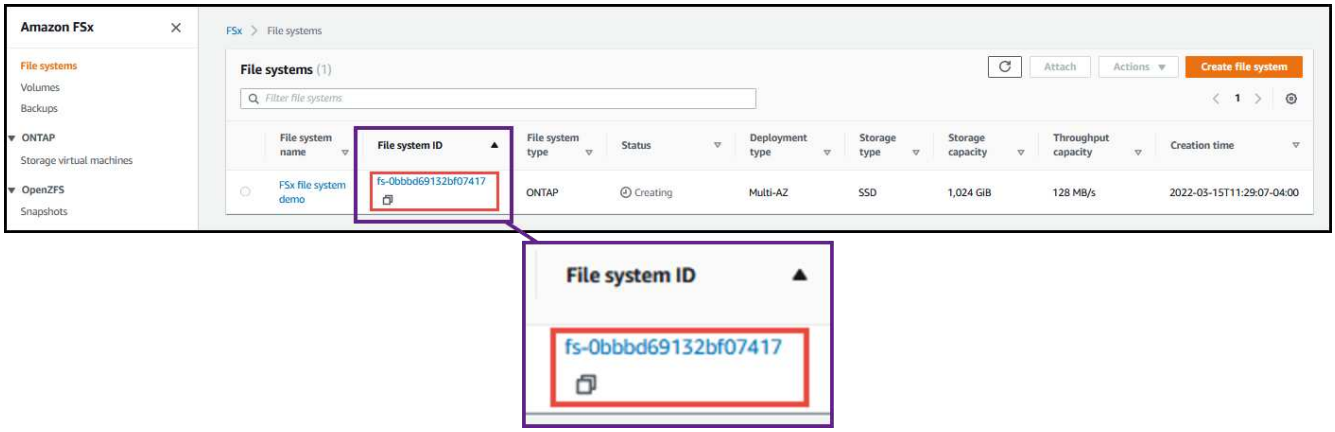


开始之前

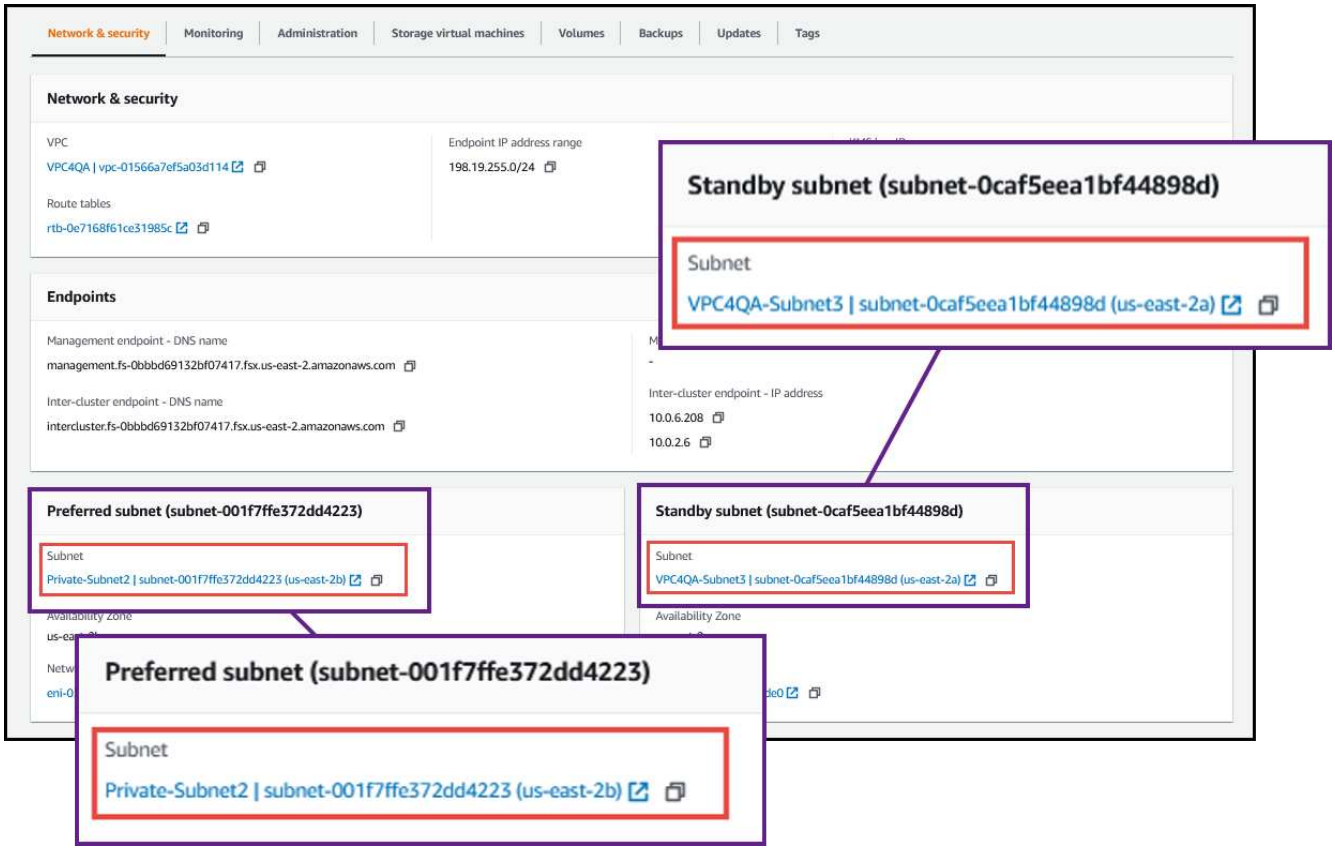
您需要使用 AWS 管理控制台查找与 Enis 关联的安全组。

步骤

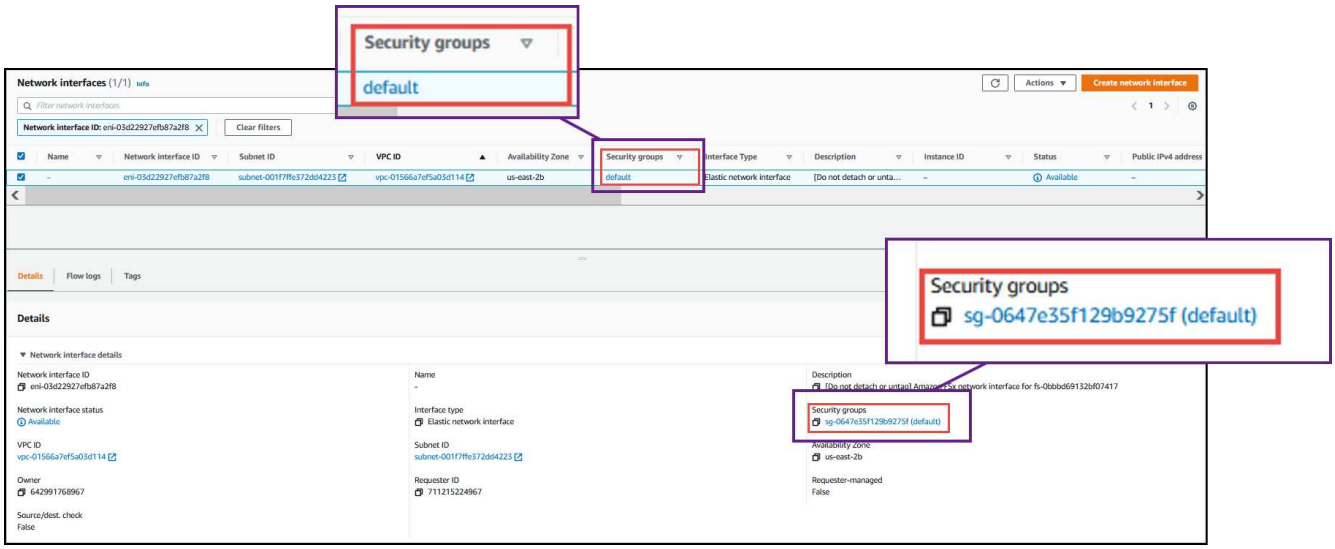
1. 在 AWS 管理控制台中打开适用于 ONTAP 的 FSX 文件系统，然后单击文件系统 ID 链接。



2. 在 * 网络和安全 * 选项卡上，单击首选子网或备用子网的网络接口 ID 。



3. 单击网络接口表中的安全组或网络接口的 * 详细信息 * 部分。



入站规则

协议	**Port**	目的
所有 ICMP	全部	Ping 实例

协议	**Port**	目的
HTTPS	443.	从Connector访问fsxadmin管理LIF、以便向FSX发送API调用
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049.	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049.	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

出站规则

FSX for ONTAP 的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

FSX for ONTAP 的预定义安全组包括以下出站规则。

协议	**Port**	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

您无需为调解器打开特定端口，也无需在适用于 ONTAP 的 FSx 中的节点之间打开特定端口。

源是 ONTAP 系统上的 FSX 接口（IP 地址）。

服务	协议	Port	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	节点管理 LIF	Active Directory 目录林	LDAP
	TCP	445	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（set_change ）
	UDP	464.	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（RPCSEC_GSS ）
	TCP	88	数据 LIF （NFS ，CIFS ， iSCSI ）	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	LDAP
	TCP	445	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（set_change ）
	UDP	464.	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	数据 LIF （NFS 、CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（RPCSEC_GSS ）

服务	协议	**Port**	源	目标	目的
备份到 S3	TCP	5010	集群间 LIF	备份端点或还原端点	备份到 S3 功能的备份和还原操作
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53.	节点管理 LIF 和数据 LIF （NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	节点管理 LIF	目标服务器	NDMP 副本
SMTP	TCP	25.	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	TCP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104.	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	TCP	11105.	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	UDP	514.	节点管理 LIF	系统日志服务器	系统日志转发消息

Connector 的规则

Connector 的安全组需要入站和出站规则。

入站规则

协议	**Port**	目的
SSH	22.	提供对 Connector 主机的 SSH 访问
HTTP	80	提供从客户端Web浏览器到本地用户界面的HTTP访问以及从BlueXP分类实例进行的连接
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问
TCP	3128	如果您的AWS网络不使用NAT或代理、则为BlueXP分类实例提供互联网访问

出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

Connector 的预定义安全组包括以下出站规则。

协议	**Port**	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。

源 IP 地址是 Connector 主机。

服务	协议	**Port**	目标	目的
Active Directory	TCP	88	Active Directory 目录林	Kerberos V 身份验证
	TCP	139.	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	Active Directory 目录林	LDAP
	TCP	445	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	TCP	749	Active Directory 目录林	Active Directory Kerberos V 更改和设置密码（ RPCSEC_GSS ）
	UDP	137.	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	Active Directory 目录林	NetBIOS 数据报服务
	UDP	464.	Active Directory 目录林	Kerberos 密钥管理
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP 、并将 AutoSupport 消息发送到 NetApp
API 调用	TCP	8088	备份到 S3	对备份到 S3 进行 API 调用
DNS	UDP	53.	DNS	用于BlueXP的DNS解析

服务	协议	**Port**	目标	目的
BlueXP分类	HTTP	80	BlueXP分类	Cloud Volumes ONTAP的BlueXP分类