要求
Amazon FSx for ONTAP

NetApp
April 04, 2022

目录

要求

为适用于 ONTAP 的 FSX 设置权限

要创建或管理适用于 ONTAP 的 Amazon FSX 工作环境，您需要通过提供 IAM 角色的 ARN 将 AWS 凭据添加到 Cloud Manager ，以便为 Cloud Manager 提供创建适用于 ONTAP 的 FSX 工作环境所需的权限。

设置 IAM 角色

设置一个 IAM 角色，使 Cloud Manager SaaS 能够承担此角色。

步骤

1. 转到目标帐户中的 IAM 控制台。
2. 在访问管理下，单击 * 角色 > 创建角色 * ，然后按照步骤创建角色。

   请务必执行以下操作：

   - 在 * 可信实体类型 * 下，选择 * AWS 帐户 * 。
   - 选择 * 其他 AWS 帐户 * 并输入 Cloud Manager SaaS 的 ID： 952013314444
   - 创建包含以下权限的策略：

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

3. 复制 IAM 角色的角色 ARN ，以便您可以在下一步将其粘贴到 Cloud Manager 中。

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 Cloud Manager 中。

如果您刚刚创建了 IAM 角色，则可能需要几分钟的时间，直到这些角色可用为止。请等待几分钟，然后再将凭据添加到 Cloud Manager 。

步骤

1. 在 Cloud Manager 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 > Cloud Manager* 。
   b. * 定义凭据 * ： 提供 IAM 角色的 ARN （ Amazon 资源名称）。
   c. * 查看 * ： 确认有关新凭据的详细信息，然后单击 * 添加 * 。

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 Cloud Manager 的 AWS 凭据"

适用于 ONTAP 的 FSX 的安全组规则

Cloud Manager 会创建 AWS 安全组，其中包含 Cloud Manager 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

适用于 ONTAP 的 FSX 安全组需要入站和出站规则。

入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0 。

协议	Port	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问

协议	**Port**	目的
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

如果您需要对出站流量使用严格的规则，则可以使用以下信息仅打开 ONTAP 的 FSX 出站通信所需的端口。

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
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信（仅限 Cloud Volumes ONTAP HA ）
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用（仅适用于 Cloud Volumes ONTAP HA ）
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态（仅限 Cloud Volumes ONTAP HA ）
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 Cloud Data sense 建立的连接
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，则可为云数据感知实例提供 Internet 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

服务	协议	**Port**	目标	目的
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	3000	ONTAP HA 调解器	与 ONTAP HA 调解器通信
	TCP	8088	备份到 S3	对备份到 S3 进行 API 调用
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析
云数据感知	HTTP	80	云数据感知实例	适用于 Cloud Volumes ONTAP 的云数据感知