



入门

Amazon FSx for ONTAP

NetApp
June 01, 2022

目录

- 入门 1
 - 了解适用于 ONTAP 的 Amazon FSX 1
 - 开始使用适用于 ONTAP 的 Amazon FSX 2
 - 为适用于 ONTAP 的 FSX 设置权限 2
 - 适用于 ONTAP 的 FSX 的安全组规则 4

入门

了解适用于 ONTAP 的 Amazon FSX

"适用于 ONTAP 的 Amazon FSX" 是一项完全托管的服务，允许客户启动和运行由 NetApp ONTAP 存储操作系统提供支持的文件系统。FSX for ONTAP 提供了与 NetApp 客户在内部使用的相同的特性，性能和管理功能，并具有原生 AWS 服务的简单性，灵活性，安全性和可扩展性。

功能

- 无需配置或管理存储设备，软件或备份。
- 支持 CIFS，NFSv3，NFSv4.x 和 SMB v2.0 - v3.1.1 协议。
- 使用可用的不常访问（IA）存储层，可实现低成本，几乎无限制的数据存储容量。
- 经过认证，可在延迟敏感型应用程序上运行，包括 Oracle RAC。
- 可选择捆绑定价和按需购买定价

Cloud Manager 中的其他功能

- 使用 AWS 和 Cloud Manager 中的连接器，您可以创建和管理卷，复制数据，并将适用于 ONTAP 的 FSx 与 Data sense 和 Cloud Sync 等 NetApp 云服务集成。
- 利用人工智能（AI）驱动的技术，云数据感知可以帮助您了解数据环境，并识别 FSX for ONTAP 帐户中的敏感数据。"[了解更多信息。](#)"
- 使用 NetApp Cloud Sync，您可以自动将数据迁移到云中或内部环境中的任何目标。"[了解更多信息。](#)"

成本

您的 FSX for ONTAP 帐户由 AWS 维护，而不是由 Cloud Manager 维护。"[《适用于 ONTAP 的 Amazon FSX 入门指南》](#)"

在 AWS 中使用连接器以及 Cloud Sync 和 Data sense 等可选数据服务会产生额外成本。

支持的区域

"[查看支持的 Amazon 地区。](#)"

获取帮助

Amazon FSX for ONTAP 是 AWS 第一方解决方案。对于与 AWS FSX 文件系统，基础架构或使用此服务的任何 AWS 解决方案相关的问题或技术支持问题，请使用 AWS 控制台中的支持中心向 AWS 创建支持案例。选择 "FSX for ONTAP" 服务和相应的类别。提供创建 AWS 支持案例所需的其余信息。

对于 Cloud Manager 或 Cloud Manager 微服务特有的一般问题，您可以从在线 Cloud Manager 聊天开始。

对于 Cloud Manager 或中的微服务特有的技术支持问题，您可以使用 Cloud Manager 帐户级别序列号打开

NetApp 支持服务单。您需要注册 Cloud Manager 序列号才能激活支持。

限制

- Cloud Manager 只能将数据从内部或 Cloud Volumes ONTAP 复制到适用于 ONTAP 的 FSX 。
- 此时，可以使用 ONTAP 命令行界面， ONTAP API 或 Cloud Manager API 创建 iSCSI 卷。
- 目前、从适用于ONTAP 的FSX进行SnapMirror复制 "[支持使用ONTAP 命令行界面](#)"。

开始使用适用于 ONTAP 的 Amazon FSX

通过几个步骤开始使用适用于 ONTAP 的 Amazon FSx 。

只需几个步骤，即可开始使用适用于 ONTAP 的 FSX 。

在添加卷之前，您必须创建适用于 ONTAP 的 Amazon FSX 工作环境。您需要 "[设置一个 IAM 角色，使 Cloud Manager SaaS 能够承担此角色](#)"。

您必须具有 "[适用于 AWS 的连接器](#)" 要打开适用于 ONTAP 的 FSX 工作环境，请创建卷或执行其他操作。如果需要使用 Connector ， Cloud Manager 将提示您是否尚未添加。

您可以使用 Cloud Manager 为 ONTAP 卷创建 FSX 。

使用 Cloud Manager 管理卷并配置其他服务，例如复制， Cloud Sync 和 Data sense 。

相关链接

- "[使用 Cloud Manager 创建连接器](#)"
- "[从 AWS Marketplace 启动 Connector](#)"
- "[在 Linux 主机上安装 Connector 软件](#)"

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

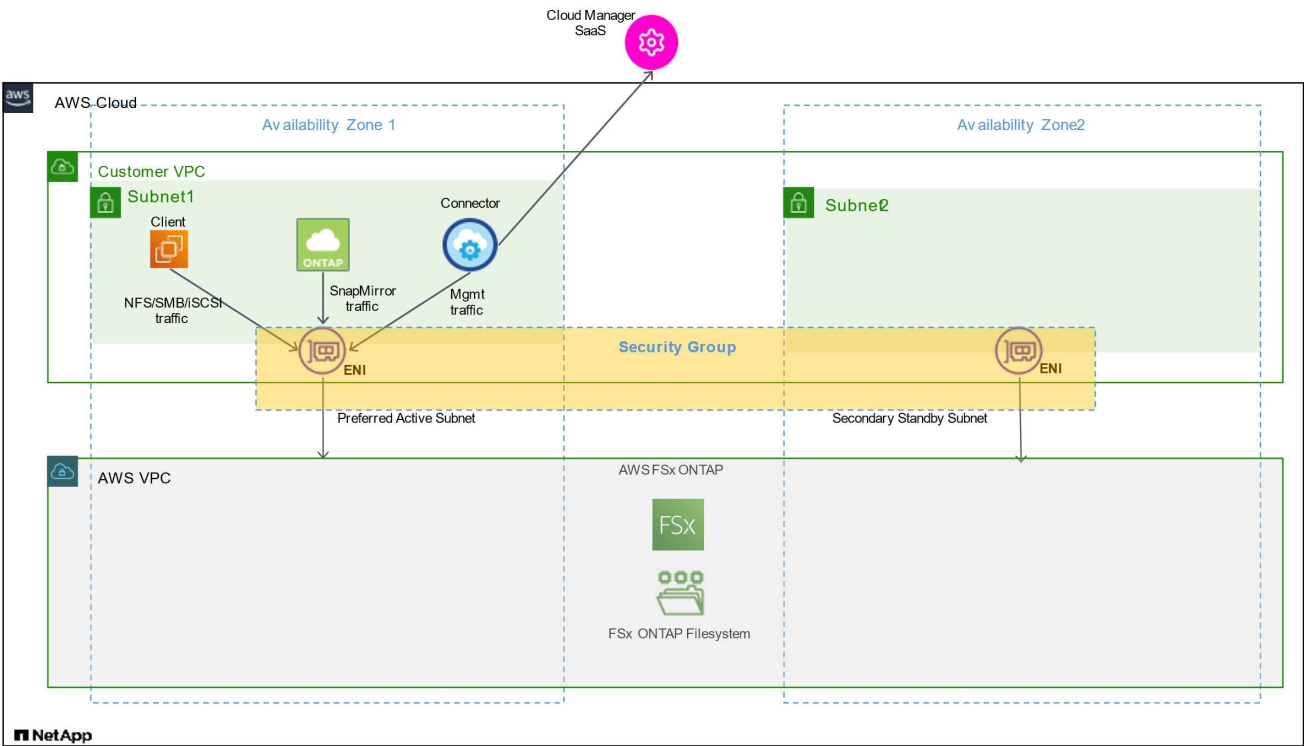
- ["AWS 凭据和权限"](#)
- ["管理 Cloud Manager 的 AWS 凭据"](#)

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

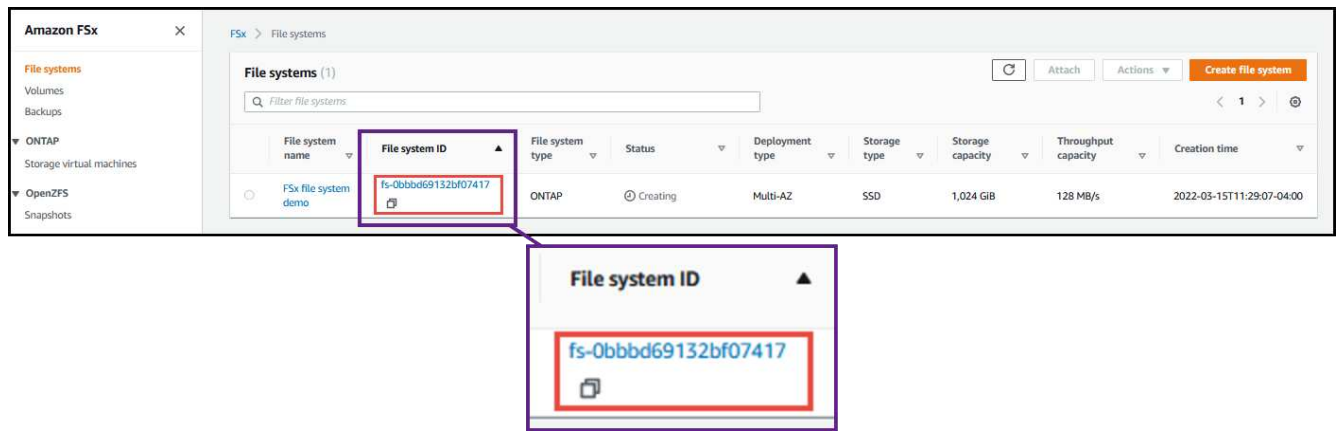
ONTAP 的 FSX 安全组需要入站和出站规则。此图显示了适用于 ONTAP 的 FSX 网络配置和安全组要求。



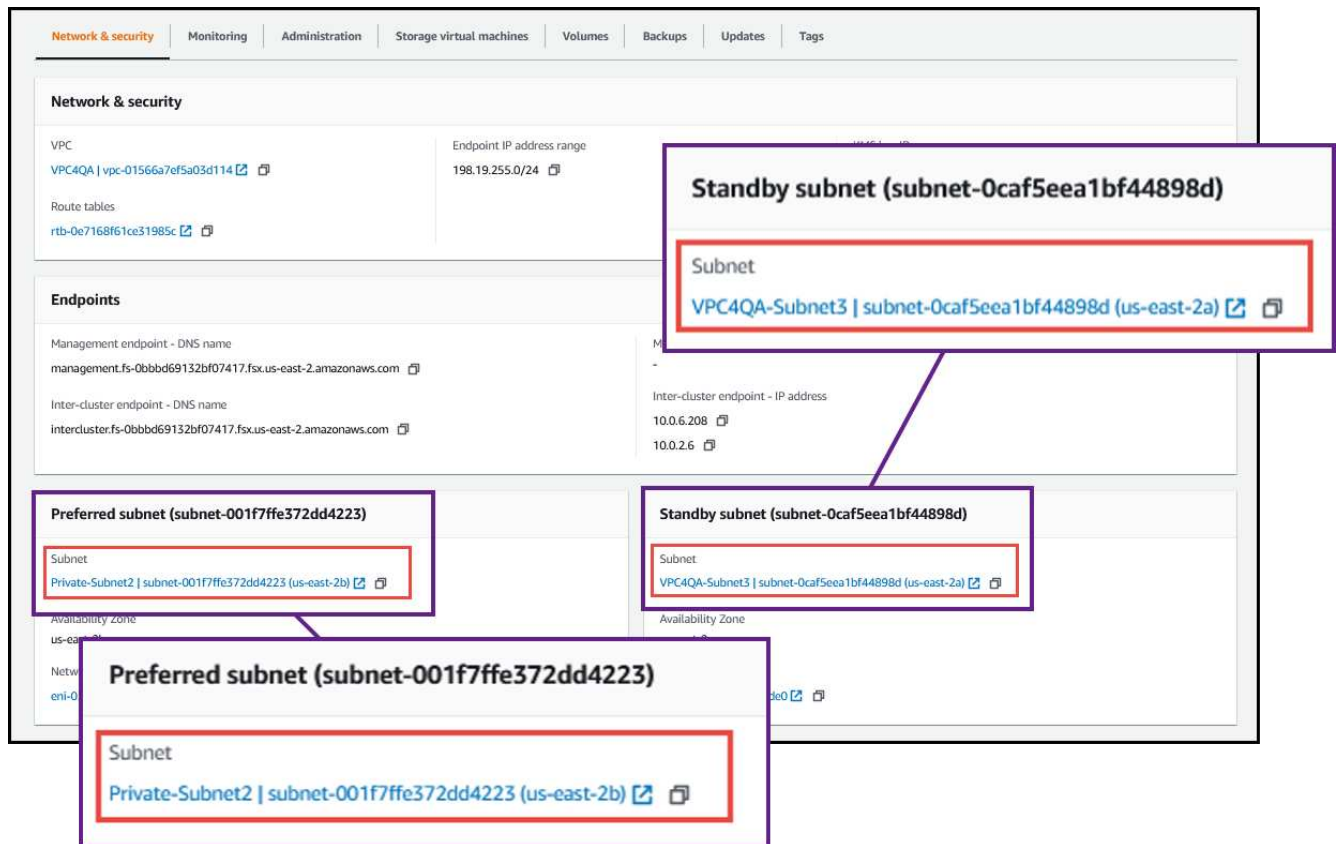
您需要使用 AWS 管理控制台查找与 Enis 关联的安全组。

步骤

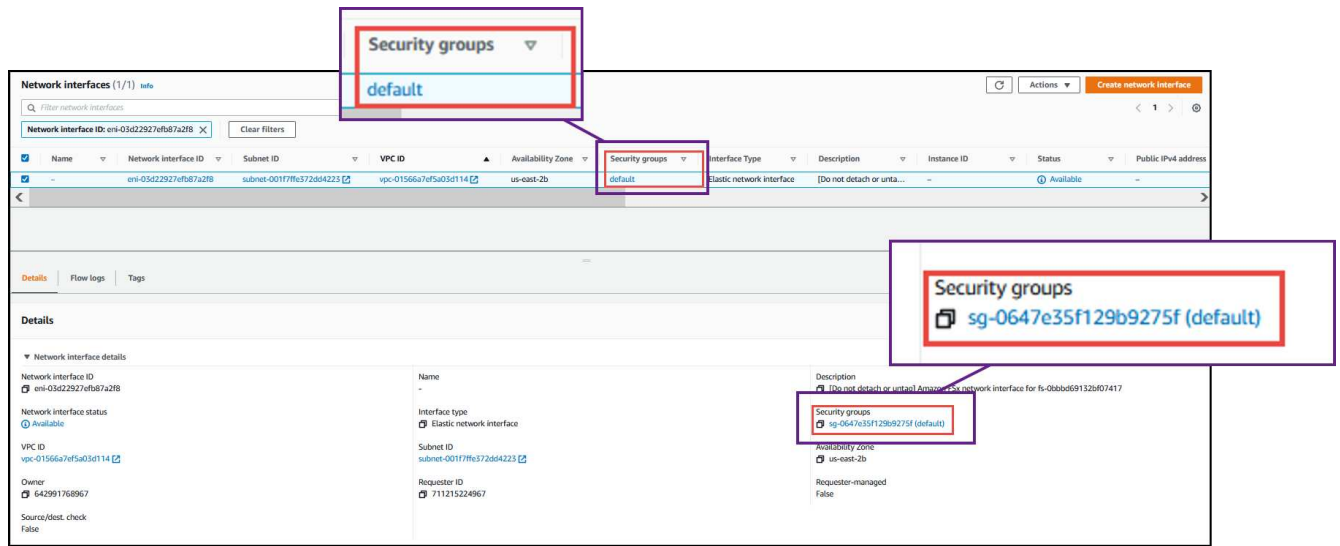
1. 在 AWS 管理控制台中打开适用于 ONTAP 的 FSX 文件系统，然后单击文件系统 ID 链接。



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 |
| 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 |

| 协议 | Port | 目的 |
|-----|-------|----------------|
| 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 ） |
| 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 |

| 服务 | 协议 | Port | 源 | 目标 | 目的 |
|------------|-----|---------------|---------------------------------|---------------|-------------------------|
| 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 |

| | | |
|--------|-------------|--------|
| 协议 | Port | 目的 |
| 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 |

版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。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).

商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 是NetApp、Inc.的商标。其他公司和产品名称可能是其各自所有者的商标。