入门指南
Data Infrastructure Insights

NetApp
February 11, 2026

目录

入门指南

工作负载安全入门

工作负载安全功能可帮助您监控用户活动并检测存储环境中的潜在安全威胁。在开始监控之前，您需要配置代理、数据收集器和目录服务，为全面的安全监控奠定基础。

工作负载安全系统使用代理从存储系统收集访问数据并从目录服务服务器收集用户信息。

在开始收集数据之前，您需要配置以下内容：

任务	相关信息
配置代理	"代理要求" "添加代理"
配置用户目录连接器	"添加用户目录连接器"
配置数据收集器	单击*工作负载安全>收集器*单击要配置的数据收集器。有关收集器信息，请参阅文档中的“数据收集器供应商参考”部分。
创建用户帐户	"管理用户帐户"

工作负载安全也可以与其他工具集成。例如，"请参阅本指南"与 Splunk 集成。

工作负载安全代理要求

在满足最低操作系统、CPU、内存和磁盘空间要求的专用服务器上部署 Workload Security Agents，以确保最佳监控和威胁检测性能。本指南规定了 "安装 Workload Security Agent" 之前所需的硬件和网络要求，包括支持的 Linux 发行版、网络连接规则和系统规模调整指南。

组件	**Linux** 要求
操作系统	运行以下任一许可版本的计算机：* AlmaLinux 9.4（64 位）至 9.5（64 位）、10（64 位），包括 SELinux* CentOS Stream 9（64 位）* Debian 11（64 位）、12（64 位），包括 SELinux* OpenSUSE Leap 15.3（64 位）至 15.6（64 位）* Oracle Linux 8.10（64 位）、9.1（64 位）至 9.6（64 位），包括 SELinux* Red Hat Enterprise Linux 8.10（64 位）、9.1（64 位）至 9.6（64 位）、10（64 位），包括 SELinux* Rocky 9.4（64 位）至 9.6（64 位），包括 SELinux* SUSE Linux Enterprise Server 15 SP4（64 位）至 15 SP6（64 位），包括 SELinux * Ubuntu 20.04 LTS（64 位）、22.04 LTS（64 位）、24.04 LTS（64 位） 此计算机不应运行其他应用程序级软件。建议使用专用服务器。
命令	安装需要“unzip”。此外，安装、运行脚本和卸载都需要“sudo su –”命令。

组件	**Linux** 要求
CPU	4 个 CPU 核心
内存	16 GB 内存
可用磁盘空间	磁盘空间应按以下方式分配：/opt/netapp 36 GB（创建文件系统后至少有 35 GB 的可用空间）注意：建议分配一些额外的磁盘空间以允许创建文件系统。确保文件系统中至少有 35 GB 的可用空间。如果 /opt 是从 NAS 存储挂载的文件夹，请确保本地用户可以访问该文件夹。如果本地用户没有访问此文件夹的权限，代理或数据收集器可能无法安装。请参阅"故障排除"部分了解更多详情。
网络	100 Mbps 到 1 Gbps 以太网连接、静态 IP 地址、与所有设备的 IP 连接以及工作负载安全实例所需的端口（80 或 443）。

请注意：工作负载安全代理可以与Data Infrastructure Insights获取单元和/或代理安装在同一台机器上。但是，最佳做法是将它们安装在单独的机器上。如果将它们安装在同一台机器上，请按如下所示分配磁盘空间：

可用磁盘空间	50-55 GB 对于 Linux，应按以下方式分配磁盘空间：/opt/netapp 25-30 GB /var/log/netapp 25 GB

其他建议

- 强烈建议使用*网络时间协议 (NTP)* 或*简单网络时间协议 (SNTP)* 同步ONTAP系统和代理机器上的时间。

云网络访问规则

对于*美国*的工作负载安全环境：

协议	端口	源	目标	描述
TCP	443	工作负载安全代理	<站点名称>.cs01.cloudinsights.netapp.com <站点名称>.c01.cloudinsights.netapp.com <站点名称>.c02.cloudinsights.netapp.com	访问Data Infrastructure Insights
TCP	443	工作负载安全代理	agentlogin.cs01.cloudinsights.netapp.com	访问身份验证服务

对于*基于欧洲的*工作负载安全环境：

协议	端口	源	目标	描述
TCP	443	工作负载安全代理	<站点名称>.cs01-eu-1.cloudinsights.netapp.com <站点名称>.c01-eu-1.cloudinsights.netapp.com <站点名称>.c02-eu-1.cloudinsights.netapp.com	访问Data Infrastructure Insights
TCP	443	工作负载安全代理	agentlogin.cs01-eu-1.cloudinsights.netapp.com	访问身份验证服务

对于*基于亚太地区*的工作负载安全环境：

协议	端口	源	目标	描述
TCP	443	工作负载安全代理	<站点名称>.cs01-ap-1.cloudinsights.netapp.com <站点名称>.c01-ap-1.cloudinsights.netapp.com <站点名称>.c02-ap-1.cloudinsights.netapp.com	访问Data Infrastructure Insights
TCP	443	工作负载安全代理	agentlogin.cs01-ap-1.cloudinsights.netapp.com	访问身份验证服务

网络内规则

协议	端口	源	目标	描述
TCP	389（LDAP） 636（LDAP/启动-tls）	工作负载安全代理	LDAP Server URL	连接到 LDAP
TCP	443	工作负载安全代理	集群或 SVM 管理 IP 地址（取决于 SVM 收集器配置）	API 与ONTAP进行通信

协议	端口	源	目标	描述
TCP	35000 - 55000	SVM 数据 LIF IP 地址	工作负载安全代理	ONTAP与工作负载安全代理之间针对 Fpolicy 事件的通信。必须向工作负载安全代理打开这些端口，以便ONTAP向其发送事件，包括工作负载安全代理本身上的任何防火墙（如果存在）。请注意，您不需要保留所有这些端口，但为此保留的端口必须在此范围内。建议先预留约 100 个端口，然后根据需要增加。
TCP	35000-55000	集群管理 IP	工作负载安全代理	从ONTAP集群管理 IP 到工作负载安全代理的通信，用于 **EMS** 事件。必须向工作负载安全代理打开这些端口，以便ONTAP向其发送 **EMS** 事件，包括工作负载安全代理本身上的任何防火墙（如果存在）。请注意，您不需要保留所有这些端口，但为此保留的端口必须在此范围内。建议先预留约 100 个端口，然后根据需要增加。
SSH	22	工作负载安全代理	集群管理	需要 CIFS/SMB 用户阻止。

系统规模

查看"事件发生率检查器"有关尺寸的信息，请参阅文档。

部署工作负载安全代理

工作负载安全代理对于监控用户活动和检测存储基础架构中潜在的安全威胁至关重要。本指南提供分步安装说明、代理管理最佳实践（包括暂停/恢复和固定/取消固定功能）以及部署后配置要求。开始之前，请确保您的代理服务器满足以下条件： "系统要求"。

开始之前

- 安装、运行脚本和卸载都需要 sudo 权限。
- 安装代理时，会在机器上创建本地用户_cssys_和本地组_cssys_。如果权限设置不允许创建本地用户，而是需要 Active Directory，则必须在 Active Directory 服务器中创建用户名为 *cssys* 的用户。
- 您可以阅读有关Data Infrastructure Insights安全性的文章"此处"。

最佳实践

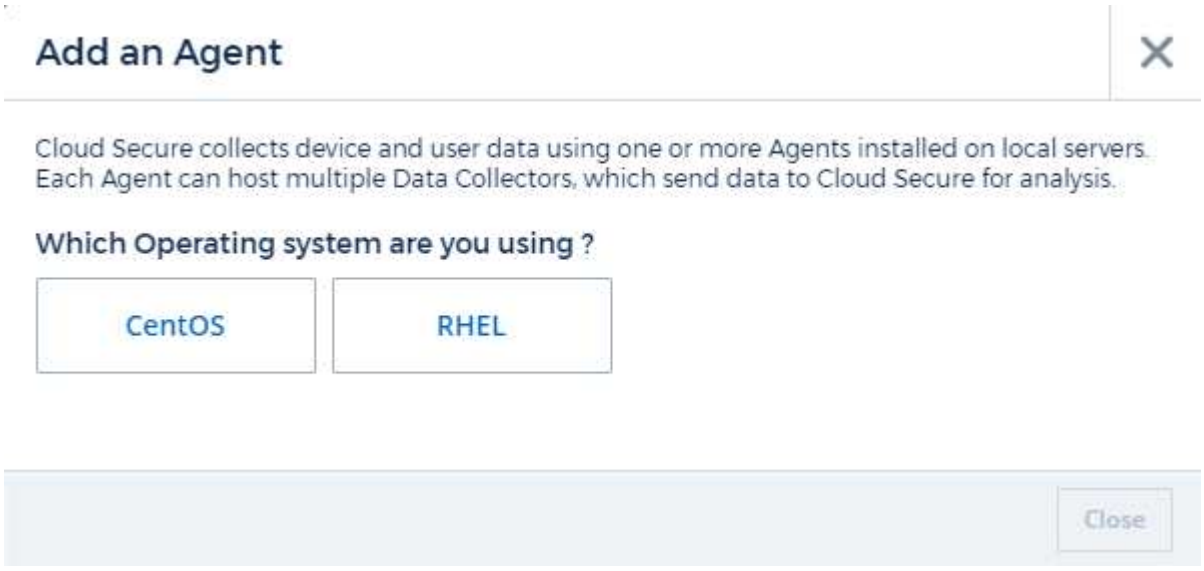
配置工作负载安全代理之前，请记住以下事项。

暂停和恢复	暂停：从ONTAP中移除 fpolicies。通常用于客户执行可能需要大量时间的长时间维护活动，例如代理虚拟机重启或存储更换。恢复：将 fpolicies 重新添加到 ONTAP。
别针和拔针	Unpin 会立即获取最新版本（如果可用），并升级代理和收集器。在此升级过程中，fpolicies 将断开连接并重新连接。此功能专为希望控制自动升级时间的客户而设计。请见下文插针/拔针说明。
推荐方法	对于大型配置，建议使用引脚和引脚断开操作，而不是暂停集电极。使用固定和取消固定功能时，无需暂停和恢复。客户可以保留其代理和收款员，并在收到有关新版本的电子邮件通知后，有 30 天的时间逐个选择性地升级代理。这种方法最大限度地减少了对 fpolicies 的延迟影响，并提供了对升级过程的更大控制。

安装代理的步骤

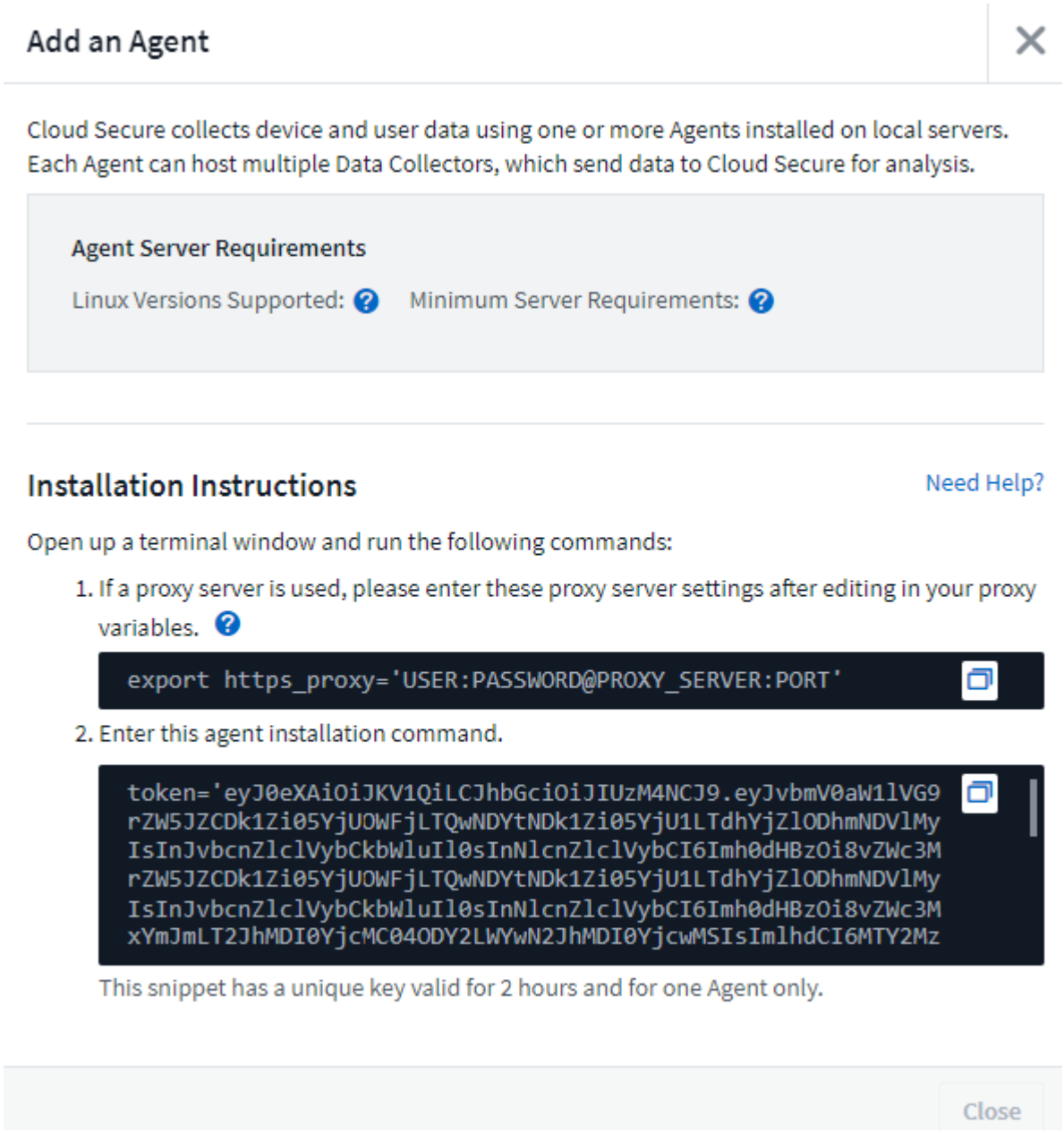
1. 以管理员或帐户所有者的身份登录到您的工作负载安全环境。
2. 选择*收藏家>代理>+代理*

   系统显示“添加代理”页面：



3. 验证代理服务器是否满足最低系统要求。
4. 要验证代理服务器是否正在运行受支持的 Linux 版本，请单击_支持的版本 (i)_。

5. 如果您的网络使用代理服务器，请按照代理部分中的说明设置代理服务器详细信息。



6. 单击“复制到剪贴板”图标以复制安装命令。
7. 在终端窗口中运行安装命令。
8. 安装成功完成后系统显示以下消息：

完成后

1. 您需要配置一个"用户目录收集器"。
2. 您需要配置一个或多个数据收集器。

网络配置

在本地系统上运行以下命令以打开工作负载安全将使用的端口。如果对端口范围存在安全问题，则可以使用较小的端口范围，例如 *35000:35100*。每个 SVM 使用两个端口。

步骤

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

根据您的平台执行以下步骤：

CentOS 7.x / RHEL 7.x：

1. `sudo iptables-save | grep 35000`

示例输出：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
CentOS 8.x / RHEL 8.x：
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`（适用于 CentOS 8）

示例输出：

```
35000-55000/tcp
```

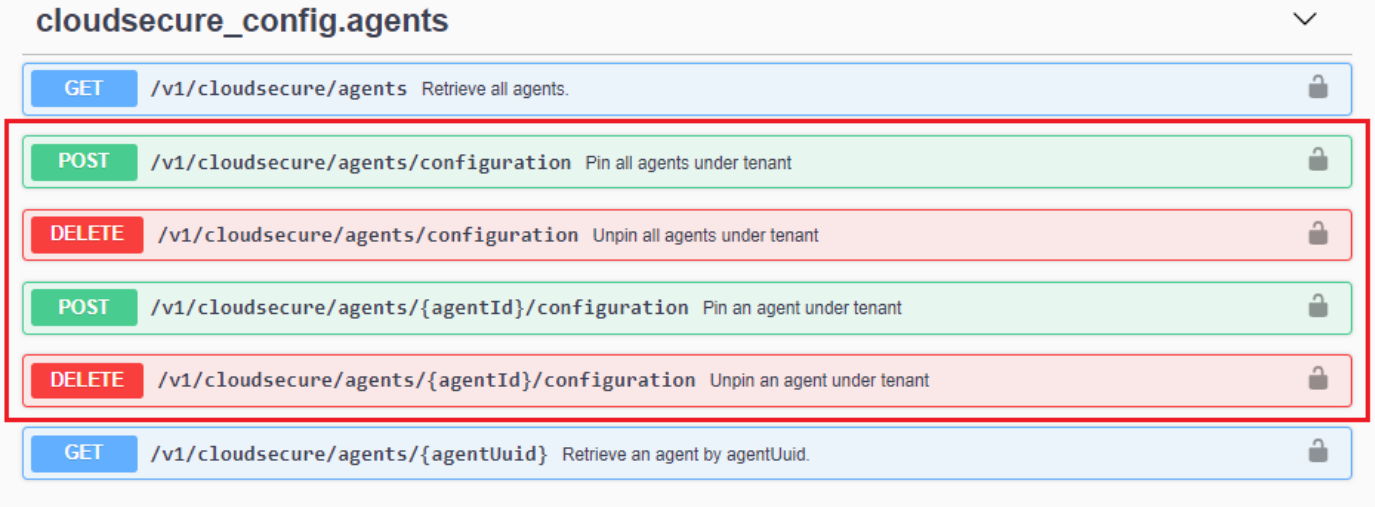
将代理“固定”在当前版本

默认情况下，Data Infrastructure Insights工作负载安全会自动更新代理。一些客户可能希望暂停自动更新，这将使代理保持其当前版本，直到发生以下情况之一：

- 客户恢复自动代理更新。
- 30天过去了。请注意，30 天从最近一次代理更新之日开始，而不是从代理暂停之日开始。

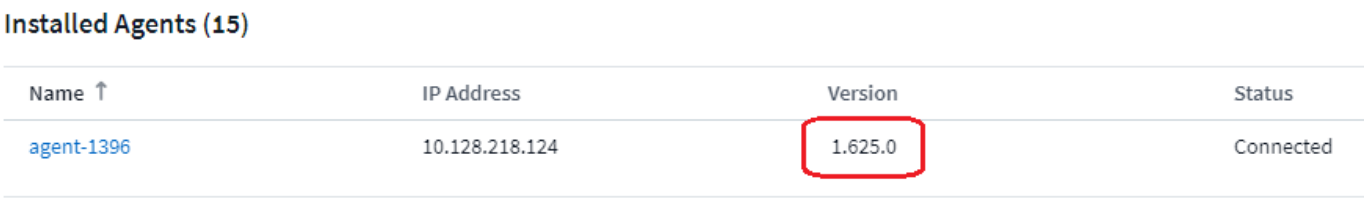
在每种情况下，代理都将在下一次工作负载安全刷新时更新。

要暂停或恢复自动代理更新，请使用 *cloudsecure_config.agents* API：



请注意，暂停或恢复操作可能需要最多五分钟才能生效。

您可以在“工作负载安全 > 收集器”页面的“代理”选项卡中查看当前的代理版本。



代理错误故障排除

下表描述了已知问题及其解决方法。

问题：	解决：
代理安装无法创建 /opt/netapp/cloudsecure/agent/logs/agent.log 文件夹，并且 install.log 文件未提供相关信息。	此错误发生在代理引导期间。该错误未记录在日志文件中，因为它发生在记录器初始化之前。错误被重定向到标准输出，并可使用以下方式在服务日志中查看 `journalctl -u cloudsecure-agent.service`命令。此命令可用于进一步解决问题。est
代理安装失败，并显示“不支持此 Linux 发行版”。退出安装”。	当您尝试在不受支持的系统上安装代理时会出现此错误。看"代理要求" 。
代理安装失败，错误为：“-bash：unzip：未找到命令”	安装unzip然后再次运行安装命令。如果机器上安装了 Yum，请尝试“yum install unzip”来安装解压缩软件。之后，从代理安装 UI 重新复制命令并将其粘贴到 CLI 中以再次执行安装。

问题：	解决：
代理已安装并正在运行。然而代理却突然停止了。	通过 SSH 连接到代理机器。通过以下方式检查代理服务的状态 `sudo systemctl status cloudsecure-agent.service`。1.检查日志是否显示消息“无法启动工作负载安全守护程序服务”。2.检查代理机器中是否存在 cssys 用户。以root权限逐个执行以下命令，并检查cssys用户和组是否存在。`sudo id cssys` `sudo groups cssys`3.如果不存在，则集中监控策略可能已删除 `cssys` 用户。4.通过执行以下命令手动创建 `cssys` 用户和组。`sudo useradd cssys` `sudo groupadd cssys`5.然后通过执行以下命令重新启动代理服务：`sudo systemctl restart cloudsecure-agent.service` 6.如果仍然无法运行，请检查其他故障排除选项。
无法向代理添加超过 50 个数据收集器。	一个代理只能添加 50 个数据收集器。这可以是所有收集器类型的组合，例如 Active Directory、SVM 和其他收集器。
UI 显示代理处于 NOT_CONNECTED 状态。	重新启动代理的步骤。1.通过 SSH 连接到代理机器。2.然后通过执行以下命令重新启动代理服务：`sudo systemctl restart cloudsecure-agent.service` 3.通过以下方式检查代理服务的状态 `sudo systemctl status cloudsecure-agent.service`。4.代理应进入 CONNECTED 状态。
代理 VM 位于 Zscaler 代理后面，并且代理安装失败。由于 Zscaler 代理的 SSL 检查，工作负载安全证书以由 Zscaler CA 签名的形式呈现，因此代理不信任该通信。	在 Zscaler 代理中禁用 *.cloudinsights.netapp.com url 的 SSL 检查。如果 Zscaler 进行 SSL 检查并替换证书，Workload Security 将不起作用。
安装代理时，解压后安装在挂起。	“chmod 755 -Rf”命令失败。当代理安装命令由非 root sudo 用户运行，且工作目录中有属于另一个用户的文件，并且这些文件的权限无法更改时，命令将失败。由于 chmod 命令失败，其余安装无法执行。1.创建一个名为“cloudsecure”的新目录。2.转到该目录。3.复制并粘贴完整的“token=…… … ./cloudsecure-agent-install.sh”安装命令并按回车键。4.安装应该可以继续。
如果代理仍然无法连接到 Saas，请向NetApp支持部门提交案例。提供Data Infrastructure Insights序列号以打开案例，并按照说明将日志附加到案例中。	将日志附加到案例：1.使用 root 权限执行以下脚本并共享输出文件（cloudsecure-agent-symptoms.zip ）。a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2.使用 root 权限逐个执行以下命令并共享输出。a. id cssys b. groups cssys c. cat /etc/os-release

问题：	解决：
cloudsecure-agent-symptom-collector.sh 脚本失败并出现以下错误。 [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 收集服务日志 收集应用程序日志 收集代理配置 拍摄服务状态快照 拍摄代理目录结构快照…… …… /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh：第 52 行：zip：未找到命令错误：无法创建 /tmp/cloudsecure-agent-symptoms.zip	Zip 工具未安装..通过运行命令“yum install zip”安装zip工具。然后再次运行cloudsecure-agent-symptom-collector.sh。
代理安装因 useradd 而失败：无法创建目录 /home/cssys	如果由于缺乏权限而无法在 /home 下创建用户的登录目录，则可能会发生此错误。解决方法是创建 cssys 用户并使用以下命令手动添加其登录目录：*sudo useradd user_name -m -d HOME_DIR* -m：如果不存在，则创建用户的主目录。 -d ： 使用 HOME_DIR 作为用户登录目录的值来创建新用户。例如，*sudo useradd cssys -m -d /cssys*，添加用户 *cssys* 并在根目录下创建其登录目录。
安装后代理未运行。 *Systemctl status cloudsecure-agent.service* 显示以下内容：[root@demo ~]# systemctl status cloudsecure-agent.service agent.service – 工作负载安全代理守护进程服务已加载：已加载（/usr/lib/systemd/system/cloudsecure-agent.service；已启用；供应商预设：已禁用）活动：正在激活（自动重启）（结果：退出代码）自 2021 年 8 月 3 日星期二 21:12:26 PDT 起； 2 秒前 进程：25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent（代码=exited status=126） 主 PID：25889（代码=exited，状态=126），8 月 3 日 21:12:26 demo systemd[1]：cloudsecure-agent.service：主进程已退出，代码=exited，状态=126/n/a 8 月 3 日 21:12:26 demo systemd[1]：单元 cloudsecure-agent.service 进入失败状态。 8 月 3 日 21:12:26 demo systemd[1]: cloudsecure-agent.service 失败。	这可能会失败，因为_cssys_用户可能没有安装权限。如果 /opt/netapp 是 NFS 挂载，并且 *cssys* 用户无权访问此文件夹，则安装将失败。 *cssys* 是由 Workload Security 安装程序创建的本地用户，可能没有权限访问已安装的共享。您可以尝试使用 *cssys* 用户访问 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent 来检查这一点。如果返回“权限被拒绝”，则表示不存在安装权限。不要安装在已安装的文件夹中，而是安装在机器本地的目录中。
代理最初通过代理服务器连接，并且代理是在代理安装期间设置的。现在代理服务器已经改变。如何更改代理的代理配置？	您可以编辑 agent.properties 来添加代理详细信息。请遵循以下步骤：1.更改为包含属性文件的文件夹：cd /opt/netapp/cloudsecure/conf 2.使用您最喜欢的文本编辑器，打开_agent.properties_文件进行编辑。3.添加或修改以下行：AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4.保存文件。5.重新启动代理：sudo systemctl restart cloudsecure-agent.service

删除工作负载安全代理

删除工作负载安全代理时，必须先删除与该代理关联的所有数据收集器。

删除代理

删除代理会删除与该代理关联的所有数据收集器。如果您计划使用不同的代理配置数据收集器，则应在删除代理之前创建数据收集器配置的备份。

开始之前

1. 确保从工作负载安全门户中删除与代理相关的所有数据收集器。

   注意：如果所有相关收集器都处于 STOPPED 状态，请忽略此步骤。

删除代理的步骤：

1. 通过 SSH 进入代理虚拟机并执行以下命令。出现提示时，输入“y”继续。

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. 单击“工作负载安全”>“收集器”>“代理”*

   系统显示已配置的代理列表。

3. 单击要删除的代理的选项菜单。
4. 单击“删除”。

   系统显示“删除代理”页面。

5. 单击“删除”确认删除。

配置 Active Directory (AD) 用户目录收集器

可以配置工作负载安全以从 Active Directory 服务器收集用户属性。

开始之前

- 您必须是Data Infrastructure Insights管理员或帐户所有者才能执行此任务。
- 您必须拥有托管 Active Directory 服务器的服务器的 IP 地址。
- 在配置用户目录连接器之前，必须先配置代理。

配置用户目录收集器的步骤

1. 在“工作负载安全”菜单中，单击：收集器 **>** 用户目录收集器 **> +** 用户目录收集器，然后选择*Active Directory*

   系统显示添加用户目录屏幕。

通过在下表中输入所需数据来配置用户目录收集器：

名称	描述
名称	用户目录的唯一名称。例如_GlobalADColector_
代理人	从列表中选择一个已配置的代理
服务器IP/域名	托管活动目录的服务器的 IP 地址或完全限定域名 (FQDN)
森林名称	目录结构的森林级别。森林名称允许以下两种格式：*x.y.z* ⇒ 直接域名，与您在 SVM 上的一样。 [示例：hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 相对可分辨名称 [示例：DC=hq,DC= companyname,DC=com] 或者您可以指定如下：*OU=engineering,DC=hq,DC= companyname,DC=com* [按特定 OU engineering 过滤] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [从 OU <engineering> 获取具有 <username> 的特定用户] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [获取该组织内的用户内的所有 Acrobat 用户] 还支持受信任的 Active Directory 域。
绑定 DN	允许用户搜索目录。例如：*username@companyname.com* 或 *username@domainname.com* 此外，还需要域只读权限。用户必须是安全组“只读域控制器”的成员。
绑定密码	目录服务器密码（即绑定 DN 中使用的用户名的密码）
协议	ldap、ldaps、ldap-start-tls
端口	选择端口

如果在 Active Directory 中修改了默认属性名称，请输入以下 Directory Server 所需的属性。大多数情况下，这些属性名称在 Active Directory 中不会被修改，在这种情况下，您可以简单地使用默认属性名称。

属性	目录服务器中的属性名称
显示名称	name
SID	对象标识符
用户名	sAM账户名称

单击“包括可选属性”以添加以下任意属性：

属性	目录服务器中的属性名称
电子邮件地址	邮件
电话号码	电话号码
角色	标题
国家/地区	公司
状态	状态

部门	部门
照片	缩略图
经理DN	经理
组	成员

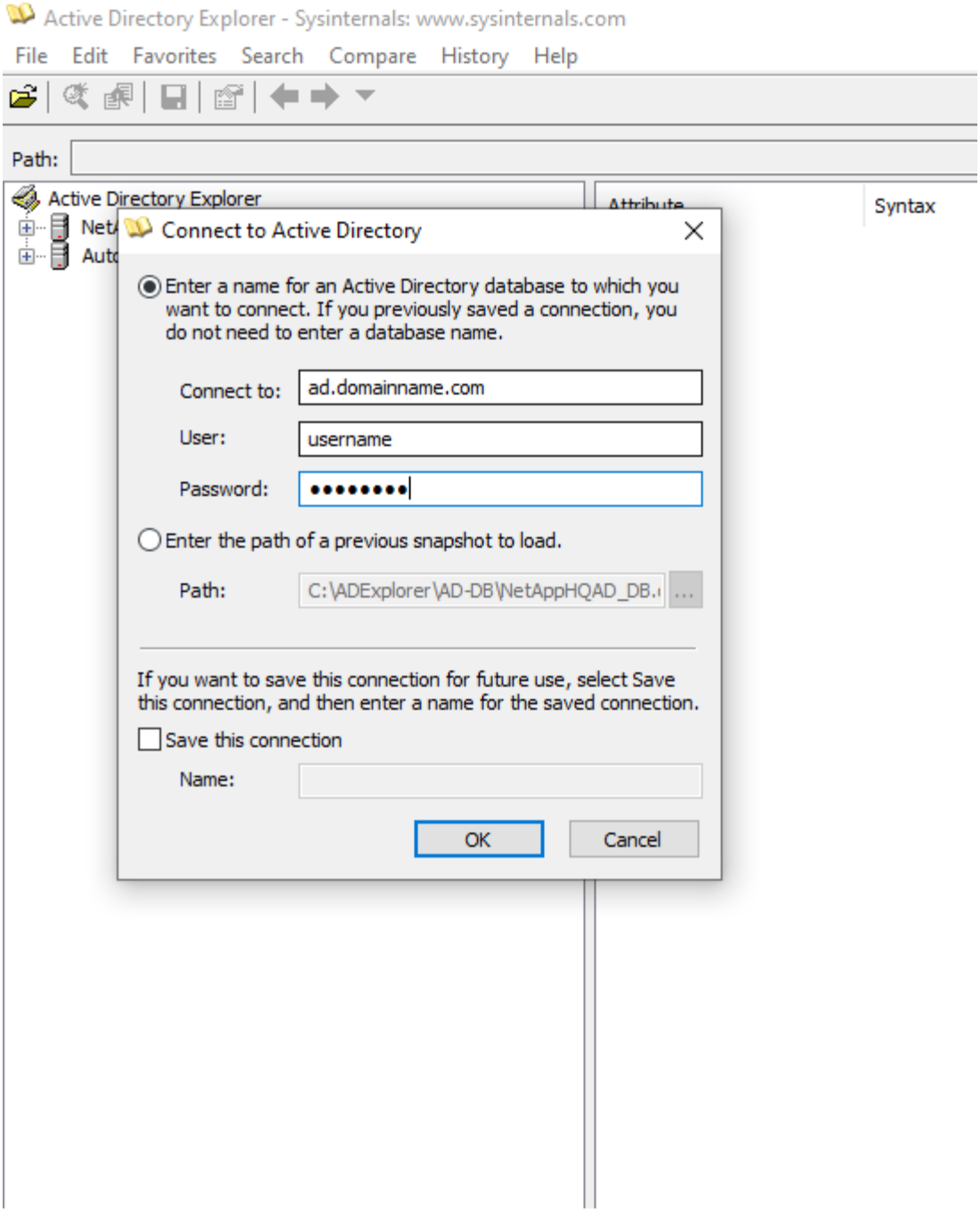
测试您的用户目录收集器配置

您可以使用以下步骤验证 LDAP 用户权限和属性定义：

- 使用以下命令验证 Workload Security LDAP 用户权限：

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
389 -D Administrator@netapp.com -W
```

- 使用 AD Explorer 浏览 AD 数据库、查看对象属性和特性、查看权限、查看对象的模式、执行可以保存和重新执行的复杂搜索。
  - 安装"AD 浏览器"在任何可以连接到 AD 服务器的 Windows 机器上。
  - 使用 AD 目录服务器的用户名/密码连接到 AD 服务器。



排除用户目录收集器配置错误

下表描述了收集器配置期间可能出现的已知问题和解决方法：

问题：	解决：
添加用户目录连接器会导致“错误”状态。错误提示“为 LDAP 服务器提供的凭据无效”。	提供的用户名或密码不正确。编辑并提供正确的用户名和密码。
添加用户目录连接器会导致“错误”状态。错误提示：“无法获取与作为林名称提供的 DN=DC=hq,DC=domainname,DC=com 对应的对象。”	提供的森林名称不正确。编辑并提供正确的森林名称。

问题：	解决：
域用户的可选属性未出现在工作负载安全用户配置文件页面中。	这可能是由于 CloudSecure 中添加的可选属性名称与 Active Directory 中的实际属性名称不匹配造成的。编辑并提供正确的可选属性名称。
数据收集器处于错误状态，显示“无法检索 LDAP 用户。失败原因：无法连接到服务器，连接为空”	单击“重新启动”按钮重新启动收集器。
添加用户目录连接器会导致“错误”状态。	确保您已为必填字段（服务器、林名称、绑定 DN、绑定密码）提供了有效值。确保 bind-DN 输入始终以“Administrator@<domain_forest_name>”或具有域管理员权限的用户帐户的形式提供。
添加用户目录连接器会导致“重试”状态。显示错误“无法定义收集器的状态，原因 Tcp 命令 [Connect(localhost:35012,None,List(),Some(,seconds),true)] 因 java.net.ConnectionException:Connection 被拒绝而失败。”	为 AD 服务器提供的 IP 或 FQDN 不正确。编辑并提供正确的 IP 地址或 FQDN。
添加用户目录连接器会导致“错误”状态。错误提示“无法建立 LDAP 连接”。	为 AD 服务器提供的 IP 或 FQDN 不正确。编辑并提供正确的 IP 地址或 FQDN。
添加用户目录连接器会导致“错误”状态。错误提示：“无法加载设置。原因：数据源配置错误。具体原因：/connector/conf/application.conf: 70: ldap.ldap-port 的类型为 STRING 而不是 NUMBER”	提供的端口值不正确。尝试使用 AD 服务器的默认端口值或正确的端口号。
我从强制属性开始，并且它起作用了。添加可选项后，可选属性数据不会从 AD 中获取。	这可能是由于 CloudSecure 中添加的可选属性与 Active Directory 中的实际属性名称不匹配造成的。编辑并提供正确的强制或可选属性名称。
重新启动收集器后，AD 同步何时发生？	收集器重启后，AD 同步将立即发生。获取约30万用户的用户数据大约需要15分钟，并且每12小时自动刷新一次。
用户数据从 AD 同步到 CloudSecure。数据何时会被删除？	如果没有刷新，用户数据将保留13个月。如果租户被删除，那么数据也将被删除。
用户目录连接器导致“错误”状态。 “连接器处于错误状态。服务名称：usersLdap。失败原因：无法检索 LDAP 用户。失败原因：80090308：LdapErr：DSID-0C090453，注释：AcceptSecurityContext 错误，数据 52e，v3839”	提供的森林名称不正确。请参阅上文，了解如何提供正确的森林名称。

问题：	解决：
用户资料页面中未填写电话号码。	这很可能是由于 Active Directory 的属性映射问题造成的。1.编辑从 Active Directory 获取用户信息的特定 Active Directory 收集器。2.请注意，在可选属性下，有一个字段名称“电话号码”映射到 Active Directory 属性“telephonenumber”。4.现在，请使用上面描述的 Active Directory Explorer 工具浏览 Active Directory 并查看正确的属性名称。3.确保 Active Directory 中有一个名为“telephonenumber”的属性，其中确实包含用户的电话号码。5.假设在 Active Directory 中它已被修改为“电话号码”。6.然后编辑 CloudSecure 用户目录收集器。在可选属性部分，将“telephonenumber”替换为“phonenumber”。7.保存 Active Directory 收集器，收集器将重新启动并获取用户的电话号码，并将其显示在用户个人资料页面中。
如果在 Active Directory (AD) 服务器上启用了加密证书 (SSL)，则 Workload Security User Directory Collector 无法连接到 AD 服务器。	在配置用户目录收集器之前禁用 AD 服务器加密。一旦获取用户详细信息，它将保留 13 个月。如果 AD 服务器在获取用户详细信息后断开连接，则不会获取 AD 中新添加的用户。要再次获取，用户目录收集器需要连接到 AD。
CloudInsights Security 中存在来自 Active Directory 的数据。想要从 CloudInsights 中删除所有用户信息。	无法仅从 CloudInsights Security 中删除 Active Directory 用户信息。为了删除用户，需要删除整个租户。

配置 LDAP 目录服务器收集器

您配置工作负载安全以从 LDAP 目录服务器收集用户属性。

开始之前

- 您必须是Data Infrastructure Insights管理员或帐户所有者才能执行此任务。
- 您必须拥有托管 LDAP 目录服务器的服务器的 IP 地址。
- 在配置 LDAP 目录连接器之前，必须先配置代理。

配置用户目录收集器的步骤

1. 在工作负载安全菜单中，单击：收集器 **>** 用户目录收集器 **> +** 用户目录收集器，然后选择*LDAP 目录服务器*

   系统显示添加用户目录屏幕。

通过在下表中输入所需数据来配置用户目录收集器：

名称	描述
名称	用户目录的唯一名称。例如 *GlobalLDAPCollector*
代理人	从列表中选择一个已配置的代理
服务器IP/域名	托管 LDAP 目录服务器的服务器的 IP 地址或完全限定域名 (FQDN)

搜索基础	LDAP 服务器的搜索基础搜索基础允许以下两种格式：*x.y.z* ⇒ 直接域名，就像您在 SVM 上拥有的那样。 [示例：hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 相对可分辨名称 [示例：DC=hq,DC=companyname,DC=com] 或者您可以指定如下：*OU=engineering,DC=hq,DC= companyname,DC=com* [按特定 OU engineering 过滤] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [从 OU <engineering> 获取具有 <username> 的特定用户] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [获取该组织内用户的所有 Acrobat 用户]
绑定 DN	允许用户搜索目录。例如：uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com 对于用户 john@dorp.company.com 。dorp.company.com
--账户	--用户
--约翰	--安娜
绑定密码	目录服务器密码（即绑定 DN 中使用的用户名的密码）
协议	ldap、ldaps、ldap-start-tls
端口	选择端口

如果 LDAP 目录服务器中的默认属性名称已被修改，请输入以下目录服务器所需的属性。大多数情况下，这些属性名称在 LDAP 目录服务器中不会被修改，在这种情况下，您可以简单地使用默认属性名称。

属性	目录服务器中的属性名称
显示名称	name
UNIXID	uid 号
用户名	uid

单击“包括可选属性”以添加以下任意属性：

属性	目录服务器中的属性名称
电子邮件地址	邮件
电话号码	电话号码
角色	标题
国家/地区	公司
状态	状态
部门	部门编号
照片	照片

经理DN	经理
组	成员

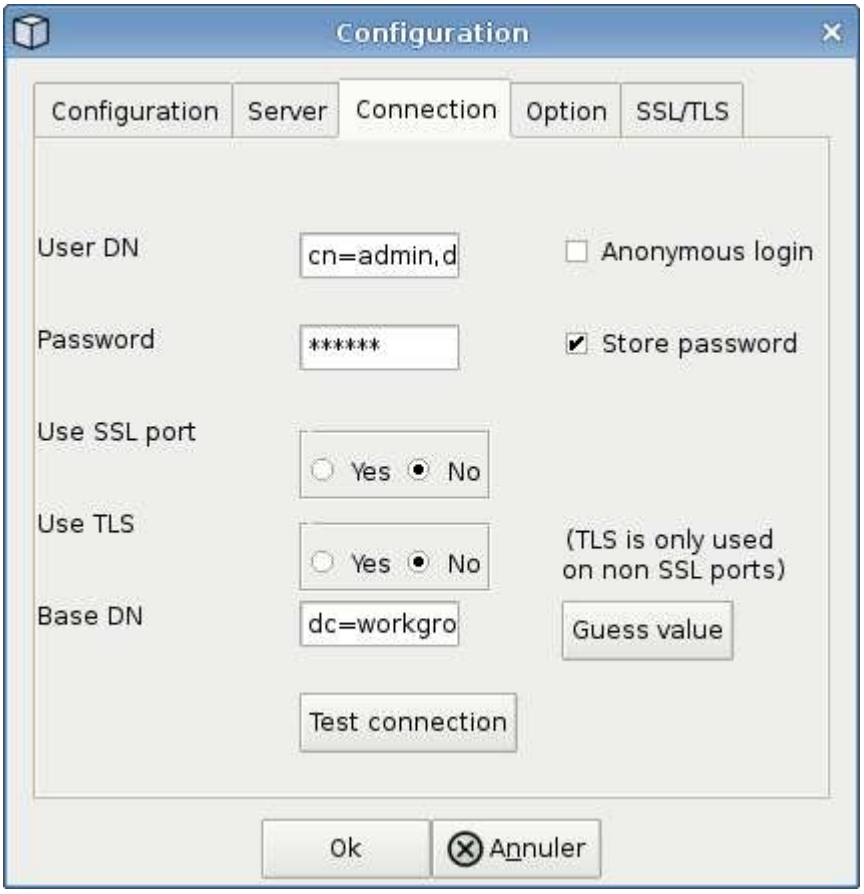
测试您的用户目录收集器配置

您可以使用以下步骤验证 LDAP 用户权限和属性定义：

- 使用以下命令验证 Workload Security LDAP 用户权限：

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* 使用 LDAP Explorer 浏览 LDAP
数据库、查看对象属性和特性、查看权限、查看对象的模式、执行可以保存和重新执行的复杂搜索
。
```

  - 安装 LDAP Explorer(http://ldaptool.sourceforge.net/ ）或 Java LDAP 资源管理器(http://jxplorer.org/) 在任何可以连接到 LDAP 服务器的 Windows 机器上。
  - 使用 LDAP 目录服务器的用户名/密码连接到 LDAP 服务器。



排除 **LDAP** 目录收集器配置错误

下表描述了收集器配置期间可能出现的已知问题和解决方法：

问题：	解决：
添加 LDAP 目录连接器会导致“错误”状态。错误提示“为 LDAP 服务器提供的凭据无效”。	提供的绑定 DN、绑定密码或搜索基础不正确。编辑并提供正确的信息。
添加 LDAP 目录连接器会导致“错误”状态。错误提示：“无法获取与作为林名称提供的 DN=DC=hq,DC=domainname,DC=com 对应的对象。”	提供的搜索基础不正确。编辑并提供正确的森林名称。
域用户的可选属性未出现在工作负载安全用户配置文件页面中。	这可能是由于 CloudSecure 中添加的可选属性名称与 Active Directory 中的实际属性名称不匹配造成的。字段区分大小写。编辑并提供正确的可选属性名称。
数据收集器处于错误状态，显示“无法检索 LDAP 用户。失败原因：无法连接到服务器，连接为空”	单击“重新启动”按钮重新启动收集器。
添加 LDAP 目录连接器会导致“错误”状态。	确保您已为必填字段（服务器、林名称、绑定 DN、绑定密码）提供了有效值。确保绑定 DN 输入始终为 uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com。
添加 LDAP 目录连接器会导致“重试”状态。显示错误“无法确定收集器的健康状况，因此请重试”	确保提供正确的服务器 IP 和搜索库 ////
添加 LDAP 目录时显示以下错误：“无法在 2 次重试内确定收集器的健康状况，请尝试重新启动收集器（错误代码：AGENT008）”	确保提供正确的服务器 IP 和搜索库
添加 LDAP 目录连接器会导致“重试”状态。显示错误“无法定义收集器的状态，原因 Tcp 命令 [Connect(localhost:35012,None,List(),Some(,seconds),true)] 因 java.net.ConnectionException:Connection 被拒绝而失败。”	为 AD 服务器提供的 IP 或 FQDN 不正确。编辑并提供正确的 IP 地址或 FQDN。 ////
添加 LDAP 目录连接器会导致“错误”状态。错误提示“无法建立 LDAP 连接”。	为 LDAP 服务器提供的 IP 或 FQDN 不正确。编辑并提供正确的 IP 地址或 FQDN。或者提供的端口值不正确。尝试使用 LDAP 服务器的默认端口值或正确的端口号。
添加 LDAP 目录连接器会导致“错误”状态。错误提示：“无法加载设置。原因：数据源配置错误。具体原因：/connector/conf/application.conf: 70: ldap.ldap-port 的类型为 STRING 而不是 NUMBER”	提供的端口值不正确。尝试使用 AD 服务器的默认端口值或正确的端口号。
我从强制属性开始，并且它起作用了。添加可选项后，可选属性数据不会从 AD 中获取。	这可能是由于 CloudSecure 中添加的可选属性与 Active Directory 中的实际属性名称不匹配造成的。编辑并提供正确的强制或可选属性名称。
重新启动收集器后，LDAP 同步何时发生？	收集器重启后，LDAP 同步将立即发生。获取约30万用户的用户数据大约需要15分钟，并且每12小时自动刷新一次。
用户数据从 LDAP 同步到 CloudSecure。数据何时会被删除？	如果没有刷新，用户数据将保留13个月。如果租户被删除，那么数据也将被删除。

问题：	解决：
LDAP 目录连接器导致“错误”状态。 “连接器处于错误状态。服务名称：usersLdap。失败原因：无法检索 LDAP 用户。失败原因：80090308：LdapErr：DSID-0C090453，注释：AcceptSecurityContext 错误，数据 52e，v3839”	提供的森林名称不正确。请参阅上文，了解如何提供正确的森林名称。
用户资料页面中未填写电话号码。	这很可能是由于 Active Directory 的属性映射问题造成的。1.编辑从 Active Directory 获取用户信息的特定 Active Directory 收集器。2.请注意，在可选属性下，有一个字段名称“电话号码”映射到 Active Directory 属性“telephonenumber”。4.现在，请使用上面描述的 Active Directory Explorer 工具浏览 LDAP 目录服务器并查看正确的属性名称。3.确保 LDAP 目录中有一个名为“telephonenumber”的属性，其中确实包含用户的电话号码。5.假设在 LDAP 目录中它已被修改为“电话号码”。6.然后编辑 CloudSecure 用户目录收集器。在可选属性部分，将“telephonenumber”替换为“phonenumber”。7.保存 Active Directory 收集器，收集器将重新启动并获取用户的电话号码，并将其显示在用户个人资料页面中。
如果在 Active Directory (AD) 服务器上启用了加密证书 (SSL)，则 Workload Security User Directory Collector 无法连接到 AD 服务器。	在配置用户目录收集器之前禁用 AD 服务器加密。一旦获取用户详细信息，它将保留 13 个月。如果 AD 服务器在获取用户详细信息后断开连接，则不会获取 AD 中新添加的用户。要再次获取用户目录收集器，需要连接到 AD。

配置ONTAP SVM 数据收集器

ONTAP SVM 数据收集器使工作负载安全能够监控NetApp ONTAP存储虚拟机 (SVM) 上的文件和用户访问活动。本指南将指导您完成 SVM 数据收集器的配置和管理，以便为您的ONTAP环境提供全面的安全监控。

开始之前

- 该数据收集器支持以下功能：
  - Data ONTAP 9.2 及更高版本。为了获得最佳性能，请使用高于 9.13.1 的Data ONTAP版本。
  - SMB 协议版本 3.1 及更早版本。
  - NFS 版本最高可达 NFS 4.1（请注意， ONTAP 9.15 或更高版本支持 NFS 4.1）。
  - ONTAP 9.4 及更高版本支持 Flexgroup
  - ONTAP 9.7 及更高版本的 NFS 支持FlexCache 。
  - ONTAP 9.14.1 及更高版本的 SMB 支持FlexCache 。
  - 支持ONTAP Select
- 仅支持数据类型 SVM。不支持具有无限卷的 SVM。
- SVM 有几种子类型。其中，仅支持_default_、*sync_source*_和_*sync_destination*。

- 一名特工"必须配置"然后才可以配置数据收集器。
- 确保您具有正确配置的用户目录连接器，否则事件将在“活动取证”页面中显示编码的用户名而不是用户的实际名称（存储在 Active Directory 中）。
- ONTAP持久存储从 9.14.1 版本开始受支持。
- 为了获得最佳性能，您应该将 FPolicy 服务器配置为与存储系统位于同一子网。
- 有关工作负载安全策略配置的全面最佳实践和建议，请参阅"知识库文章：FPolicy最佳实践"。
- 您必须使用以下两种方法之一添加 SVM：
  - 通过使用集群 IP、SVM 名称以及集群管理用户名和密码。 这是推荐的方法。
    - SVM 名称必须与ONTAP中显示的完全一致，并且区分大小写。
  - 使用 SVM Vserver 管理 IP、用户名和密码
  - 如果您无法或不愿意使用完整的管理员集群/SVM 管理用户名和密码，您可以创建一个具有较低权限的自定义用户，如“关于权限的说明”下面的部分。可以为 SVM 或集群访问创建此自定义用户。
    - 您还可以使用具有至少 csrole 权限的角色的 AD 用户，如下面的“关于权限的说明”部分所述。另请参阅"ONTAP 文档"。
- 通过执行以下命令确保为 SVM 设置了正确的应用程序：

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

示例输出

```
Vserver: svmname
                                                                  Second
User/Group                 Authentication                 Acct   Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
vsadmin        http        password      vsadmin          no     none
vsadmin        ontapi      password      vsadmin          no     none
vsadmin        ssh         password      vsadmin          no     none
3 entries were displayed.
```

:

- 确保 SVM 已配置 CIFS 服务器：clustershell:> `vserver cifs show`

  系统返回 Vserver 名称、CIFS 服务器名称和其他字段。

- 为 SVM vsadmin 用户设置密码。如果使用自定义用户或集群管理员用户，请跳过此步骤。clustershell:> `security login password -username vsadmin -vserver svmname`
- 解锁 SVM vsadmin 用户以进行外部访问。如果使用自定义用户或集群管理员用户，请跳过此步骤。clustershell:> `security login unlock -username vsadmin -vserver svmname`
- 确保数据 LIF 的防火墙策略设置为“mgmt”（而不是“数据”）。如果使用专用管理生命周期来添加 SVM，请跳过此步骤。clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall -policy mgmt`
- 启用防火墙后，您必须定义例外以允许使用Data ONTAP数据收集器的端口的 TCP 流量。

看"代理要求"获取配置信息。这适用于本地代理和安装在云中的代理。

- 当在 AWS EC2 实例中安装代理来监控 Cloud ONTAP SVM 时，代理和存储必须位于同一个 VPC 中。如果它们位于不同的 VPC 中，则 VPC 之间必须有有效的路由。

测试数据收集器的连通性

测试连接功能（于 2025 年 3 月推出）旨在帮助最终用户在Data Infrastructure Insights(DII) 工作负载安全中设置数据收集器时识别故障的具体原因。这使得用户能够自行纠正与网络通信或缺失角色相关的问题。

此功能将帮助用户在设置数据收集器之前确定所有与网络相关的检查是否已到位。此外，它还会根据ONTAP版本、角色以及在ONTAP中分配给他们的权限，告知用户可以访问的功能。

用户目录收集器不支持测试连接

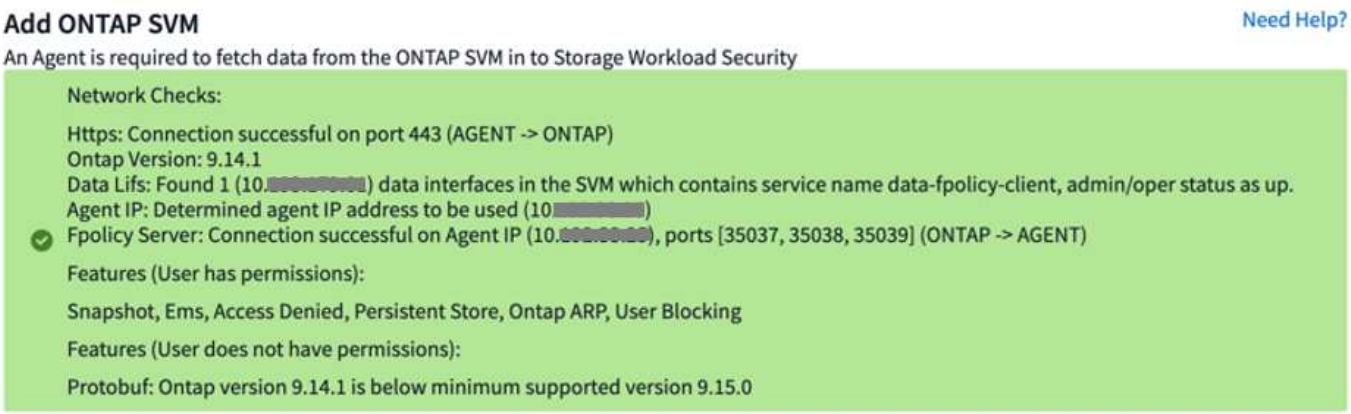
连接测试的先决条件

- 此功能要完全发挥作用，需要集群级凭证。
- SVM 模式不支持功能访问检查。
- 如果您使用集群管理凭据，则不需要新的权限。
- 如果您使用自定义用户（例如，*csuser*），请为您想要使用的功能提供强制权限和特定功能权限。

请务必查看权限下面的部分也是如此。

测试连接

用户可以转到添加/编辑收集器页面，输入集群级别详细信息（在集群模式下）或 SVM 级别详细信息（在 SVM 模式下），然后单击 测试连接 按钮。然后，工作负载安全将处理该请求并显示适当的成功或失败消息。



ONTAP Multi Admin Verify (MAV) 注意事项

某些功能，例如创建和删除快照或用户阻止 (SMB)，可能无法根据您的 ONTAP 版本中添加的 MAV 命令正常工

作。

请按照以下步骤将排除项添加到 MAV 命令中，以允许 Workload Security 创建或删除快照并阻止用户。

允许创建和删除快照的命令：

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

允许用户阻止的命令：

```
multi-admin-verify rule delete -operation set
```

用户访问阻止的先决条件

请记住以下几点"用户访问阻止"：

此功能需要集群级别凭证才能运行。

如果您使用集群管理凭据，则不需要新的权限。

如果您使用自定义用户（例如 *csuser*）并赋予该用户权限，请按照"用户访问阻止"授予 Workload Security 阻止用户的权限。

关于权限的说明

通过*集群管理 **IP***添加时的权限：

如果您无法使用集群管理员用户允许工作负载安全访问ONTAP SVM 数据收集器，则可以创建一个名为“csuser”的新用户，并使用以下命令所示的角色。配置工作负载安全数据收集器以使用集群管理 IP 时，请使用用户名“csuser”和密码“csuser”。

注意：您可以创建一个角色来用于自定义用户的所有功能权限。如果存在现有用户，则首先使用以下命令删除现有用户和角色：

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

要创建新用户，请使用集群管理管理员用户名/密码登录ONTAP ，然后在ONTAP服务器上执行以下命令：

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

通过 **Vserver** 管理 **IP** 添加时的权限：

如果您无法使用集群管理员用户允许工作负载安全访问ONTAP SVM 数据收集器，则可以创建一个名为“csuser”的新用户，并使用以下命令所示的角色。配置工作负载安全数据收集器以使用 Vserver 管理 IP 时，请使用用户名“csuser”和密码“csuser”。

注意：您可以创建一个角色来用于自定义用户的所有功能权限。如果存在现有用户，则首先使用以下命令删除现有用户和角色：

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

要创建新用户，请使用集群管理管理员用户名/密码登录ONTAP ，然后在ONTAP服务器上执行以下命令。为方便起见，请将这些命令复制到文本编辑器，然后将 <vservername> 替换为您的 Vserver 名称，然后在ONTAP上

执行这些命令：

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Protobuf模式

当在收集器的“高级配置”设置中启用此选项时，工作负载安全将在 protobuf 模式下配置 FPolicy 引擎。 ONTAP 9.15 及更高版本支持 Protobuf 模式。

关于此功能的更多详细信息，请参阅"ONTAP 文档"。

protobuf 需要特定的权限（其中一些或全部可能已经存在）：

集群模式：

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
```

虚拟服务器模式：

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

ONTAP自主勒索软件防护和**ONTAP**访问的权限被拒绝

如果您使用集群管理凭据，则不需要新的权限。

如果您使用具有指定权限的自定义用户（例如 *csuser*），则请按照以下步骤授予 Workload Security 从ONTAP收集 ARP 相关信息的权限。

欲了解更多信息，请阅读"与ONTAP集成访问被拒绝"

和"与ONTAP自主勒索软件防护集成"

配置数据收集器

配置步骤

1. 以管理员或帐户所有者的身份登录到您的Data Infrastructure Insights环境。
2. 单击“工作负载安全**>**收集器**>+**数据收集器”

   系统显示可用的数据收集器。

3. 将鼠标悬停在 * NetApp SVM 图块上，然后单击 **+Monitor**。

   系统显示ONTAP SVM 配置页面。为每个字段输入所需的数据。

字段	描述
名称	数据收集器的唯一名称
代理人	从列表中选择一个已配置的代理。
通过管理 IP 连接：	选择集群 IP 或 SVM 管理 IP
集群/SVM 管理 IP 地址	集群或 SVM 的 IP 地址，取决于您上面的选择。
SVM 名称	SVM 的名称（通过 Cluster IP 连接时需要此字段）
用户名	用于访问 SVM/集群的用户名通过集群 IP 添加时，选项为：1.集群管理员 2。 'csuser' 3. AD 用户具有与 csuser 类似的角色。通过 SVM IP 添加时，选项为：4. vsadmin 5. 'csuser' 6. AD 用户名具有与 csuser 类似的角色。
密码	上述用户名的密码
筛选股份/交易量	选择是否在事件收集中包含或排除股票/交易量
输入要排除/包含的完整共享名称	以逗号分隔的共享列表，用于从事件收集中排除或包含（视情况而定）
输入要排除/包含的完整卷名称	以逗号分隔的卷列表，用于从事件收集中排除或包含（视情况而定）

监控文件夹访问	选中后，启用文件夹访问监控事件。请注意，即使未选择此选项，文件夹的创建/重命名和删除也会受到监控。启用此功能将增加监控的事件数量。
设置ONTAP发送缓冲区大小	设置ONTAP Fpolicy 发送缓冲区大小。如果使用 9.8p7 之前的ONTAP版本并发现性能问题，则可以更改ONTAP发送缓冲区大小以提高ONTAP性能。如果您没有看到此选项并希望探索它，请联系NetApp支持。

完成后

- 在已安装的数据收集器页面中，使用每个收集器右侧的选项菜单来编辑数据收集器。您可以重新启动数据收集器或编辑数据收集器配置属性。

MetroCluster的推荐配置

以下是针对MetroCluster的建议：

1. 连接两个数据收集器，一个连接到源 SVM，另一个连接到目标 SVM。
2. 数据收集器应通过_集群 IP_ 连接。
3. 在任何时间点，当前“正在运行”的 SVM 的数据收集器将显示为“正在运行”。当前“停止”的 SVM 数据收集器将显示为“已停止”。
4. 每当发生切换时，数据收集器的状态将从_Running_变为_Stopped，反之亦然。
5. 数据收集器从_停止_状态转变为_运行_状态最多需要两分钟。

服务策略

如果使用ONTAP **9.9.1** 版或更新版本 的服务策略，为了连接到数据源收集器，需要 *data-fpolicy-client* 服务以及数据服务 *data-nfs* 和/或 *data-cifs*。

示例：

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

在ONTAP 9.9.1 之前的版本中，无需设置 *data-fpolicy-client* 。

播放-暂停数据收集器

如果数据收集器处于_运行_状态，您可以暂停收集。打开收集器的“三个点”菜单并选择暂停。当收集器暂停时，不会从ONTAP收集任何数据，也不会从收集器向ONTAP发送任何数据。这意味着没有 Fpolicy 事件会从ONTAP流向数据收集器，再从那里流向Data Infrastructure Insights。

请注意，如果在收集器暂停时在ONTAP上创建任何新卷等，则工作负载安全性将不会收集数据，并且这些卷等将不会反映在仪表板或表格中。

如果收集器有限制用户，则无法暂停收集器。在暂停收集器之前恢复用户访问权限。

请记住以下几点：

- 快照清除不会按照暂停收集器上配置的设置进行。
- EMS 事件（如 ONTAP ARP）不会在暂停的收集器上处理。这意味着，如果 ONTAP 识别出文件篡改攻击，Data Infrastructure Insights Workload Security 将无法获取该事件。
- 对于已暂停的收集器，将不会发送健康通知电子邮件。
- 暂停的收集器不支持手动或自动操作（例如快照或用户阻止）。
- 在代理或收集器升级、代理 VM 重新启动/重启或代理服务重新启动时，暂停的收集器将保持_暂停_状态。
- 如果数据收集器处于_Error_状态，则收集器无法更改为_Paused_状态。仅当收集器的状态为“正在运行”时，“暂停”按钮才会启用。
- 如果代理断开连接，则收集器无法更改为_Paused_状态。收集器将进入_停止_状态并且暂停按钮将被禁用。

持久存储

ONTAP 9.14.1 及更高版本支持持久存储。请注意，卷名称说明从ONTAP 9.14 到 9.15 有所不同。

可以通过选择收集器编辑/添加页面中的复选框来启用持久存储。选中复选框后，将显示一个用于接受卷名称的文本字段。卷名称是启用持久存储的必填字段。

- 对于ONTAP 9.14.1，您必须在启用该功能之前创建卷，并在“卷名称”字段中提供相同的名称。建议的卷大小为 16GB。
- 对于ONTAP 9.15.1，收集器将使用“卷名称”字段中提供的名称自动创建大小为 16 GB 的卷。

持久存储需要特定权限（其中一些或全部可能已经存在）：

集群模式：

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

虚拟服务器模式：

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

迁移收集器

您可以轻松地将工作负载安全收集器从一个代理迁移到另一个代理，从而实现跨代理的收集器的有效负载平衡。

前提条件

- 源代理必须处于_连接_状态。
- 要迁移的收集器必须处于_running_状态。

注:

- 数据和用户目录收集器均支持迁移。
- 不支持手动管理的租户迁移收集器。

迁移收集器

要迁移收集器，请按照以下步骤操作：

1. 转到“编辑收藏家”页面。
2. 从代理下拉菜单中选择目标代理。
3. 点击“保存收集器”按钮。

工作负载安全将处理该请求。迁移成功后，用户将被重定向到收藏家列表页面。如果失败，编辑页面上将显示相应的消息。

注意：当收集器成功迁移到目标代理时，“编辑收集器”页面上之前所做的任何配置更改都将保留应用。

故障排除

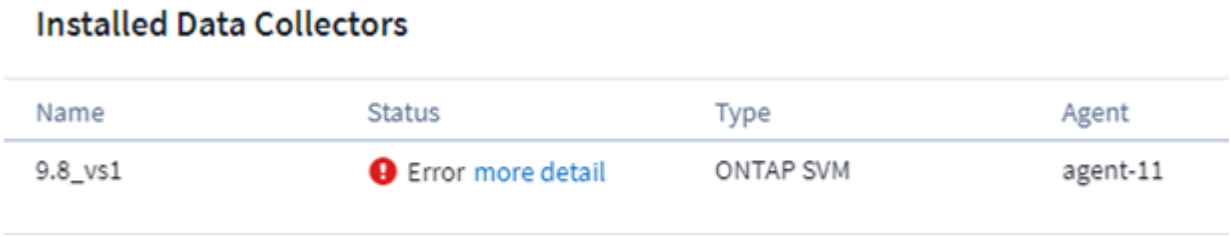
查看"SVM 收集器故障排除"页面以获取故障排除提示。

ONTAP SVM 数据收集器故障排除

工作负载安全使用数据收集器从设备收集文件和用户访问数据。您可以在这里找到解决此收集器问题的提示。

查看"配置 SVM 收集器"页面以获取有关配置此收集器的说明。

如果出现错误，您可以单击“已安装的数据收集器”页面的“状态”列中的“更多详细信息”来了解有关错误的详细信息。



已知问题及其解决方案如下所述。

问题：*数据收集器运行一段时间后在随机时间后停止，并出现故障：“错误消息：连接器处于错误状态。服务名称：审计。失败原因：外部 **fpolicy** 服务器超载。”*尝试一下： ONTAP的事件率远远高于代理盒可以处理的事件率。因此连接被终止。

检查断开连接时 CloudSecure 中的峰值流量。您可以从 **CloudSecure > Activity Forensics > All Activity** 页面进行检查。

如果峰值聚合流量高于代理箱可以处理的流量，请参阅事件速率检查器页面，了解如何确定代理箱中收集器的部署规模。

如果代理是在 2021 年 3 月 4 日之前安装在代理框中的，请在代理框中运行以下命令：

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

调整大小后从 UI 重新启动收集器。

{空的}

*问题：*收集器报告错误消息：“在连接器上未找到可以到达 SVM 数据接口的本地 IP 地址”。 *尝试一下：*这很可能是由于ONTAP端的网络问题造成的。请按照以下步骤操作：

1. 确保 SVM 数据生命周期或管理生命周期上没有防火墙阻止来自 SVM 的连接。
2. 通过集群管理 IP 添加 SVM 时，请确保 SVM 的数据 lif 和管理 lif 可以从代理 VM ping 通。如果出现问题，请检查网关、网络掩码和路由。

   您还可以尝试使用集群管理 IP 通过 ssh 登录集群，并 ping 代理 IP。确保代理 IP 可 ping 通：

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

如果无法 ping 通，请确保ONTAP中的网络设置正确，以便 Agent 机器可以 ping 通。

3. 如果您尝试通过 Cluster IP 连接但不成功，请尝试直接通过 SVM IP 连接。请参阅上文了解通过 SVM IP 连接的步骤。
4. 通过 SVM IP 和 vsadmin 凭据添加收集器时，检查 SVM Lif 是否启用了数据加管理角色。在这种情况下，ping 到 SVM Lif 将会起作用，但是 SSH 到 SVM Lif 将不起作用。如果是，请创建一个 SVM Mgmt Only Lif 并尝试通过此 SVM 管理专用 Lif 进行连接。
5. 如果仍然不起作用，请创建一个新的 SVM Lif 并尝试通过该 Lif 进行连接。确保子网掩码设置正确。
6. 高级调试：
   a. 在ONTAP中启动数据包跟踪。
   b. 尝试从 CloudSecure UI 将数据收集器连接到 SVM。
   c. 等待直到错误出现。在ONTAP中停止数据包跟踪。
   d. 从ONTAP打开数据包跟踪。可在此位置获取

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
. . 确保从ONTAP到代理框有一个 SYN。
. . 如果没有来自ONTAP的 SYN，那么这是ONTAP中的防火墙存在问题。
. . 在ONTAP中打开防火墙，以便ONTAP能够连接代理盒。
```

7. 如果仍然不起作用，请咨询网络团队，以确保没有外部防火墙阻止从ONTAP到代理盒的连接。
8. 如果以上方法都无法解决问题，请提交案例"Netapp 支持"以获得进一步的帮助。

{空的}

问题：*消息：“无法确定 [主机名：**<IP** 地址**>]** 的**ONTAP**类型。原因：与存储系统 **<IP** 地址**>** 的连接错误：主机无法访问（主机无法访问）”*尝试此操作：

1. 验证是否提供了正确的 SVM IP 管理地址或集群管理 IP。
2. 通过 SSH 连接到您要连接的 SVM 或集群。连接后，请确保 SVM 或集群名称正确。

{空的}

问题：*错误消息：“连接器处于错误状态。服务名称：审计。失败原因：外部 **fpolicy** 服务器终止。” *试试这个：

1. 最有可能的是防火墙阻止了代理机器中的必要端口。验证端口范围 35000-55000/tcp 是否已打开，以便代理计算机从 SVM 进行连接。还要确保ONTAP端没有启用防火墙来阻止与代理机器的通信。

---

2. 在代理框中输入以下命令并确保端口范围是开放的。

```
sudo iptables-save | grep 3500*
```

示例输出应如下所示：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
```

. 登录 SVM，输入以下命令并检查是否没有设置防火墙来阻止与ONTAP 的通信。

```
system services firewall show
system services firewall policy show
```

"检查防火墙命令"在ONTAP方面。

3. 通过 SSH 连接到您要监控的 SVM/集群。从 SVM 数据生命周期 (支持 CIFS、NFS 协议) 对代理盒执行 ping 操作，并确保 ping 操作正常：

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

如果无法 ping 通，请确保ONTAP中的网络设置正确，以便 Agent 机器可以 ping 通。

4. 如果通过 2 个数据收集器将单个 SVM 两次添加到租户，则会显示此错误。通过 UI 删除其中一个数据收集器。然后通过 UI 重新启动其他数据收集器。然后数据收集器将显示“RUNNING”状态并开始从 SVM 接收事件。

   基本上，在一个租户中，应该只通过 1 个数据收集器添加 1 个 SVM 一次。 1 个 SVM 不应通过 2 个数据收集器添加两次。

5. 如果在两个不同的工作负载安全环境（租户）中添加了相同的 SVM，则最后一个 SVM 始终会成功。第二个收集器将使用自己的 IP 地址配置 fpolicy，并踢出第一个收集器。因此第一个收集器将停止接收事件，并且其“审计”服务将进入错误状态。为防止这种情况，请在单个环境上配置每个 SVM。
6. 如果服务策略配置不正确，也可能会出现此错误。使用ONTAP 9.8 或更高版本时，为了连接到数据源收集器，需要 data-fpolicy-client 服务以及数据服务 data-nfs 和/或 data-cifs 。此外，data-fpolicy-client 服务必须与受监控 SVM 的数据生命周期相关联。

{空的}

问题：*活动页面中未显示任何事件。 *试试这个：

1. 检查ONTAP收集器是否处于“正在运行”状态。如果是，则通过打开一些文件确保在 cifs 客户端虚拟机上生成一些 cifs 事件。

2. 如果没有看到任何活动，请登录 SVM 并输入以下命令。

```
<SVM>event log show -source fpolicy
```

请确保没有与 fpolicy 相关的错误。

3. 如果没有看到任何活动，请登录 SVM。输入以下命令：

```
<SVM>fpolicy show
```

检查以“cloudsecure_”为前缀的 fpolicy 策略是否已设置且状态为“on”。如果未设置，那么代理很可能无法执行 SVM 中的命令。请确保已遵循页面开头所述的所有先决条件。

{空的}

问题： SVM 数据收集器处于错误状态，错误消息为“代理无法连接到收集器” 尝试以下操作：

1. 最有可能的是代理超载并且无法连接到数据源收集器。
2. 检查有多少个数据源收集器连接到代理。
3. 还可以检查 UI 中“所有活动”页面的数据流量。
4. 如果每秒的活动数量非常高，请安装另一个代理并将一些数据源收集器移动到新的代理。

{空的}

问题： SVM 数据收集器显示错误消息为“fpolicy.server.connectError：节点无法与 FPolicy 服务器“12.195.15.146”建立连接（原因：“选择超时”）” 尝试此操作： SVM/Cluster 中启用了防火墙。因此 fpolicy 引擎无法连接到 fpolicy 服务器。 ONTAP中可用于获取更多信息的 CLI 包括：

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"检查防火墙命令"在ONTAP方面。

{空的}

*问题：*错误消息：“连接器处于错误状态。服务名称：审计。失败原因：在 SVM 上未找到有效的数据接口（角色：数据、数据协议：NFS 或 CIFS 或两者、状态：启动）。 *尝试一下：*确保有一个操作接口（具有数据角色和 CIFS/NFS 数据协议）。

{空的}

---

*问题：*数据收集器进入错误状态，一段时间后进入运行状态，然后再次返回错误状态。如此循环往复。 *尝试一下：*这通常发生在以下场景中：

1. 添加了多个数据收集器。
2. 表现出这种行为的数据收集器将会有 1 个 SVM 添加到这些数据收集器中。意思是 2 个或更多数据收集器连接到 1 个 SVM。
3. 确保 1 个数据收集器仅连接到 1 个 SVM。
4. 删除连接到同一 SVM 的其他数据收集器。

{空的}

问题：*连接器处于错误状态。服务名称：审计。失败原因：无法配置（**SVM svmname** 上的策略）。原因：在**“fpolicy.policy.scope-modify: "Federal"** 中为**“shares-to-include”**元素指定的值无效 *尝试此操作： *共享名称需要不带任何引号。编辑ONTAP SVM DSC 配置以更正共享名称。

_包括和排除共享_不适用于较长的共享名称列表。如果您需要包含或排除大量股票，请使用按数量过滤。

{空的}

---

*问题：*集群中存在未使用的现有 fpolicies。在安装 Workload Security 之前应该做什么？ *尝试一下：*建议删除所有现有的未使用的 fpolicy 设置，即使它们处于断开连接状态。工作负载安全将创建带有前缀“cloudsecure_”的 fpolicy。所有其他未使用的 fpolicy 配置都可以删除。

显示 fpolicy 列表的 CLI 命令：

```
 fpolicy show
```

删除 `fpolicy` 配置的步骤：

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{空的}

---

*问题：*启用工作负载安全后， ONTAP性能受到影响：延迟偶尔会升高，IOPS 偶尔会降低。 *试试这个：*在

使用ONTAP和工作负载安全时，有时会在ONTAP中看到延迟问题。造成这种情况可能有以下几个原因："1372994"， "1415152"， "1438207"， "1479704"， "1354659"。所有这些问题均已在ONTAP 9.13.1 及更高版本中修复；强烈建议使用其中一个更高版本。

{空的}

问题：*数据收集器显示错误消息："错误：两次重试后无法确定收集器的健康状况，请尝试重新启动收集器（错误代码：**AGENT008**）"。 *试试这个：

1. 在数据收集器页面上，滚动到出现错误的数据收集器的右侧，然后单击 3 个点菜单。选择"编辑"。再次输入数据采集器的密码。按下"保存"按钮保存数据收集器。数据收集器将重新启动并且错误应该得到解决。
2. 代理机器可能没有足够的 CPU 或 RAM 空间，这就是 DSC 失败的原因。请检查机器中添加到代理的数据收集器的数量。如果超过20，请增加Agent机器的CPU和RAM容量。一旦 CPU 和 RAM 增加，DSC 将自动进入初始化状态，然后进入运行状态。查看尺码指南"本页"。

{空的}

---

*问题：*选择 SVM 模式时数据收集器出错。 *尝试一下：*在 SVM 模式下连接时，如果使用集群管理 IP 而不是 SVM 管理 IP 进行连接，则连接将出错。确保使用正确的 SVM IP。

{空的}

---

*问题：*启用"拒绝访问"功能时，数据收集器显示一条错误消息："连接器处于错误状态。服务名称：审计。失败原因：无法在 SVM test_svm 上配置 fpolicy。原因：用户未获得授权。" *尝试一下：*用户可能缺少"拒绝访问"功能所需的 REST 权限。请按照"本页"设置权限。

设置权限后重新启动收集器。

{空的}

问题： 收集器处于错误状态，消息为：连接器处于错误状态。 失败原因：无法在 SVM <SVM 名称> 上配置持久存储。 原因：无法在 SVM"<SVM 名称>"中找到卷"<volumeName>"的合适聚合。 原因：聚合"<aggregateName>"的性能信息目前不可用。服务名称：审计。失败原因: 无法在 SVM 上配置持久性存储<SVM Name>。原因: 无法为卷"找到合适的聚合"<volumeName> " 在 SVM 中"<SVM Name> "。原因: 聚合的性能信息 "<aggregateName> " 当前不可用。请稍等几分钟，然后重试此命令。

*试试这个方法：*等待几分钟，然后重新启动收集器。

{空的}

如果您仍然遇到问题，请联系*帮助>支持*页面中提到的支持链接。

配置Cloud Volumes ONTAP和Amazon FSx for NetApp ONTAP收集器

通过为Cloud Volumes ONTAP和Amazon FSx for NetApp ONTAP配置 Workload Security 数据收集器，监控整个云存储基础架构中的文件和用户访问。本指南提供了在 AWS 中部署代理并将其连接到云存储实例的分步说明。

Cloud Volumes ONTAP存储配置

请参阅OnCommand Cloud Volumes ONTAP文档，以配置单节点/HA AWS 实例来托管工作负载安全代理：https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

配置完成后，按照以下步骤设置您的 SVM：https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

支持的平台

- Cloud Volumes ONTAP，在所有可用的云服务提供商处均受支持。例如：Amazon、Azure、Google Cloud。
- ONTAPAmazon FSx

代理机器配置

代理机器必须在云服务提供商的各自子网中配置。在[代理要求]中阅读有关网络访问的更多信息。

以下是在 AWS 中安装代理的步骤。可以在 Azure 或 Google Cloud 中按照适用于云服务提供商的等效步骤进行安装。

在 AWS 中，使用以下步骤将机器配置为用作工作负载安全代理：

使用以下步骤将机器配置为工作负载安全代理：

步骤

1. 登录 AWS 控制台并导航到 EC2-Instances 页面并选择_启动实例_。
2. 选择具有此页面中提到的适当版本的 RHEL 或 CentOS AMI：https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. 选择 Cloud ONTAP实例所在的 VPC 和子网。
4. 选择 *t2.xlarge*（4 vcpus 和 16 GB RAM）作为分配的资源。
    a. 创建 EC2 实例。
5. 使用 YUM 包管理器安装所需的 Linux 包：
    a. 安装 *wget* 和 *unzip* 本机 Linux 包。

安装工作负载安全代理

1. 以管理员或帐户所有者的身份登录到您的Data Infrastructure Insights环境。

2. 导航到工作负载安全*收集器*并单击*代理*选项卡。
3. 单击 **+Agent** 并指定 RHEL 作为目标平台。
4. 复制代理安装命令。
5. 将代理安装命令粘贴到您登录的 RHEL EC2 实例中。这将安装 Workload Security 代理，提供所有"代理先决条件"均已满足。

有关详细步骤，请参阅此链接： https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

故障排除

下表描述了已知问题及其解决方法。

问题	解决方法
数据收集器显示“工作负载安全：无法确定 Amazon FxSN 数据收集器的ONTAP类型”错误。客户无法将新的 Amazon FSxN 数据收集器添加到 Workload Security 中。从代理到端口 443 上的 FSxN 集群的连接超时。防火墙和 AWS 安全组已启用所需规则以允许通信。代理已部署并且也位于同一个 AWS 账户中。同一代理用于连接和监控其余的NetApp设备（并且所有设备都在运行）。	通过将 fsxadmin LIF 网络段添加到代理的安全规则来解决此问题。如果您不确定端口，请允许所有端口。

用户管理

工作负载安全用户帐户通过Data Infrastructure Insights进行管理。

Data Infrastructure Insights提供四个用户帐户级别：帐户所有者、管理员、用户和访客。每个帐户都分配有特定的权限级别。具有管理员权限的用户帐户可以创建或修改用户，并为每个用户分配以下工作负载安全角色之一：

角色	工作负载安全访问
管理员	可以执行所有工作负载安全功能，包括警报、取证、数据收集器、自动响应策略和工作负载安全 API。管理员还可以邀请其他用户，但只能分配工作负载安全角色。
用户	可以查看和管理警报并查看取证。用户角色可以更改警报状态、添加注释、手动拍摄快照以及限制用户访问。
访客	可以查看警报和取证。来宾角色不能更改警报状态、添加注释、手动拍摄快照或限制用户访问。

步骤

1. 登录工作负载安全
2. 在菜单中，单击“管理”>“用户管理”

   您将被转发到数据基础设施洞察的用户管理页面。

3. 为每个用户选择所需的角色。

添加新用户时，只需选择所需的角色（通常是用户或访客）。

有关用户帐户和角色的更多信息，请参阅Data Infrastructure Insights"用户角色"文档。

Event Rate Checker：Agent 规模调整指南

在部署数据收集器之前，通过测量 SVM 生成的 NFS 和 SMB 事件率来确定最佳 Agent 计算机大小。Event Rate Checker 脚本可帮助您了解容量限制（每个 Agent 最多 50 个数据收集器），并确保您的 Agent 基础架构可以处理您的预期事件量以进行可靠的威胁检测。

要求：

- 集群 IP
- 集群管理员用户名和密码

运行此脚本时，不应为正在确定事件率的 SVM 运行ONTAP SVM 数据收集器。

步骤：

1. 按照 CloudSecure 中的说明安装代理。
2. 安装代理后，以 sudo 用户身份运行 *server_data_rate_checker.sh* 脚本：

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. 该脚本需要在 Linux 机器上安装 _sshpass_。有两种安装方法：
```

   a. 运行以下命令：

```
 linux_prompt> yum install sshpass
.. 如果这不起作用，则从网络下载 _sshpass_ 到 Linux 机器并运行以下命令：
```

```
linux_prompt> rpm -i sshpass
```

3. 出现提示时提供正确的值。请参阅下面的示例。
4. 该脚本大约需要 5 分钟才能运行。
5. 运行完成后，脚本将从 SVM 打印事件率。您可以在控制台输出中检查每个 SVM 的事件率：

```
“Svm svm_rate is generating 100 events/sec”.
```

每个 Ontap SVM 数据收集器可以与单个 SVM 关联，这意味着每个数据收集器将能够接收单个 SVM 生成的事件数量。

请记住以下几点：

A) 使用此表作为一般尺寸指南。您可以增加核心和/或内存的数量来增加支持的数据收集器的数量，最多可增加 50 个数据收集器：

代理机器配置	SVM 数据收集器的数量	代理机器可以处理的最大事件速率
4核，16GB	10名数据收集员	20K 个事件/秒
4核，32GB	20名数据收集员	20K 个事件/秒

B) 要计算总事件数，请将该代理的所有 SVM 生成的事件数相加。

C) 如果脚本不在高峰时段运行，或者高峰流量难以预测，则保持 30% 的事件率缓冲。

B+C应该小于A，否则Agent机器会监控失败。

也就是说，单台代理机器上可以添加的数据采集器数量应遵循以下公式：

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

查看link:concept_cs_agent_requirements.html["代理要求"]页面以了解其他先决条件和要求。

示例

假设我们有三个 SVMS，分别每秒生成 100、200 和 300 个事件。

我们应用公式：

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

控制台输出在代理机器的当前工作目录中的文件名 *fpolicy_stat_<SVM Name>.log* 中可用。

在以下情况下，脚本可能会给出错误的结果：

- 提供的凭据、IP 或 SVM 名称不正确。
- 具有相同名称、序列号等的已存在 fpolicy 将会出现错误。
- 脚本在运行时突然停止。

示例脚本运行如下所示：

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

故障排除

问题	问题解答
如果我在已配置工作负载安全的 SVM 上运行此脚本，它是否仅使用 SVM 上现有的 fpolicy 配置，还是设置一个临时配置并运行该过程?	即使对于已经配置了工作负载安全性的 SVM，事件率检查器也可以正常运行。应该不会有影响。

我可以增加可运行该脚本的 SVM 数量吗？	是只需编辑脚本并将 SVM 的最大数量从 5 更改为任何所需的数量。
如果我增加 SVM 的数量，会增加脚本的运行时间吗？	不会。即使 SVM 的数量增加，该脚本最多也会运行 5 分钟。
我可以增加可运行该脚本的 SVM 数量吗？	是您需要编辑脚本并将 SVM 的最大数量从 5 更改为任何所需的数量。
如果我增加 SVM 的数量，会增加脚本的运行时间吗？	不会。即使 SVM 的数量增加，该脚本最多也会运行 5 分钟。
如果我使用现有代理运行事件率检查器会发生什么情况？	针对已存在的代理运行事件率检查器可能会导致 SVM 上的延迟增加。当事件率检查器运行时，这种增加将是暂时的。