入门

Data Infrastructure Insights

NetApp
January 17, 2025

目录

入门

工作负载安全性入门

在开始使用工作负载安全性监控用户活动之前、需要完成一些配置任务。

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" "* 视频 * ： 代理部署"
配置用户目录连接器	"添加 User Directory Connector" "* 视频 * ： Active Directory 连接"
配置数据收集器	单击*工作负载安全性>收集器*单击要配置的数据收集器。请参见文档中的《Data Collector供应商参考》一节。"* 视频 * ： ONTAP SVM 连接"
创建用户帐户	"管理用户帐户"
故障排除	"* 视频 * ： 故障排除"

工作负载安全性也可以与其他工具集成。例如、"请参见本指南"与Splunk集成时。

工作负载安全代理要求

您必须"安装代理"从数据收集器获取信息。在安装 Agent 之前，您应确保环境满足操作系统， CPU ，内存和磁盘空间要求。

组件	**Linux** 要求
操作系统	运行以下许可证版本之一的计算机：* CentOS 8 Stream (64位)、CentOS 9 Stream、SELinux * SUSE Leap 15.3到15.5 (64位)* Oracle Linux 8.6 - 8.8、9.1到9.4 (64位)* Red Hat Enterprise Linux 8.6到8.8、9.1到9.4 (64位)、SELinux * Rockit 9.2 - Debian (64位)、SELinux Enterprise Server 9.1-9.4 (64位)和其他64位Linux * Linux * Linux * 9.4 (20.04)的计算机应运行此Linux * Linux、Linux * Linux 9、64位和Linux 9、64位Linux 9、10 LTS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使用"sudo su–"命令。
CPU	4 个 CPU 核

组件	**Linux** 要求
内存	16 GB RAM
可用磁盘空间	应按以下方式分配磁盘空间：/opt/Filessystem NetApp 36 GB (创建文件系统后至少35 GB的可用空间)注：建议再分配一点磁盘空间、以便创建文件系统。确保文件系统中至少有35 GB的可用空间。如果/opt是NAS存储中的已挂载文件夹、请确保本地用户有权访问此文件夹。如果本地用户无权访问此文件夹、则代理或数据收集器可能无法安装。有关详细信息、请参阅一节。"故障排除"
网络	100 Mbps到1 Gbps以太网连接、静态IP地址、与所有设备的IP连接以及与工作负载安全实例(80或443)的所需端口。

请注意：Workload Security代理可以与Data Infrastructure Insight采集单元和/或代理安装在同一台计算机上。但是，最佳做法是在不同的计算机上安装这些软件。如果这些磁盘安装在同一台计算机上，请按如下所示分配磁盘空间：

可用磁盘空间	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 ） * 来同步 ONTAP 系统和代理计算机上的时间。

云网络访问规则

对于*基于美国*的工作负载安全环境：

协议	端口	源	目标	说明
TCP	443	工作负载安全代理	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	访问数据基础架构洞察力
TCP	443	工作负载安全代理	gateway.c01.cloudinsights.netapp.com 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	说明
TCP	443	工作负载安全代理	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	访问数据基础架构洞察力
TCP	443	工作负载安全代理	gateway.c01.cloudinsights.netapp.com 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	说明
TCP	443	工作负载安全代理	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	访问数据基础架构洞察力
TCP	443	工作负载安全代理	gateway.c01.cloudinsights.netapp.com 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	说明
TCP	389 （LDAP） 636 （LDAPS / START-TLS ）	工作负载安全代理	LDAP 服务器 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)	与 ONTAP 的 API 通信

协议	端口	源	目标	说明
TCP	35000 - 55000	SVM 数据 LIF IP 地址	工作负载安全代理	从ONTAP到工作负载安全代理的Fpolicy事件通信。必须向工作负载安全代理打开这些端口、ONTAP才能向其发送事件、包括工作负载安全代理本身(如果存在)上的任何防火墙。请注意、您无需预留*所有*这些端口、但为此预留的端口必须在此范围内。建议首先预留~100个端口、必要时增加。
TCP	7	工作负载安全代理	SVM 数据 LIF IP 地址	从代理到SVM数据Lifs的回显
SSH	22	工作负载安全代理	集群管理	CIFS/SMB用户阻止所需。

系统规模估算

有关规模估算的信息、请参见"事件速率检查器"相关文档。

安装工作负载安全代理

工作负载安全性(以前称为Cloud Secure)使用一个或多个代理收集用户活动数据。代理会连接到租户上的设备、并收集发送到工作负载安全SaaS层进行分析的数据。请参见"代理要求"以配置代理VM。

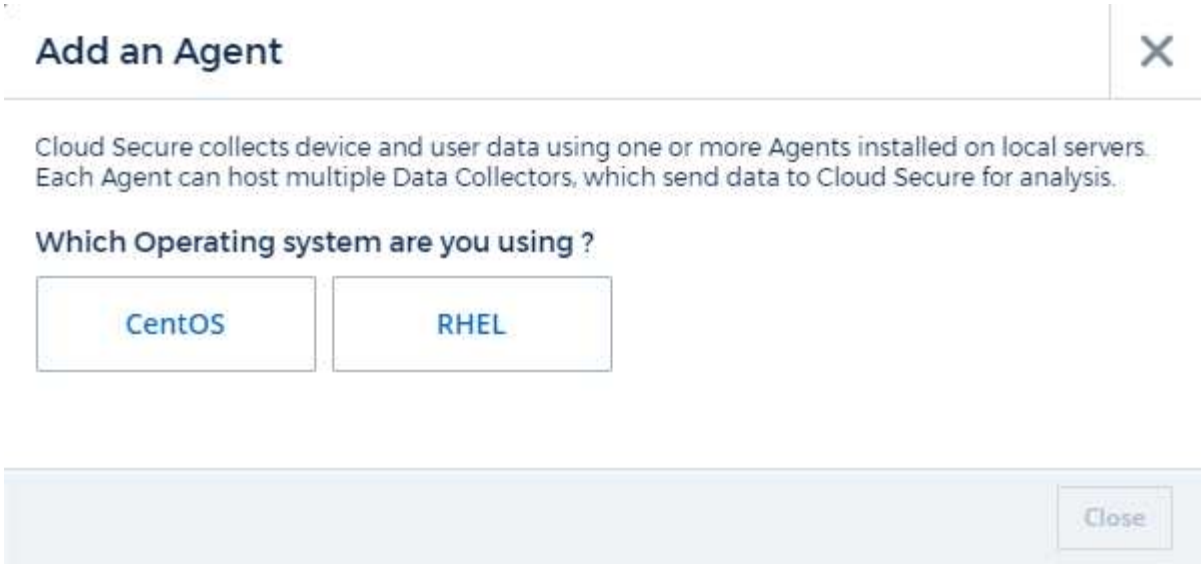
开始之前

- 安装，运行脚本和卸载需要 sudo 权限。
- 安装代理时、会在计算机上创建一个本地用户_cssys_和一个本地组_cssys_。如果权限设置不允许创建本地用户、而需要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 Insight安全性的"此处"信息。

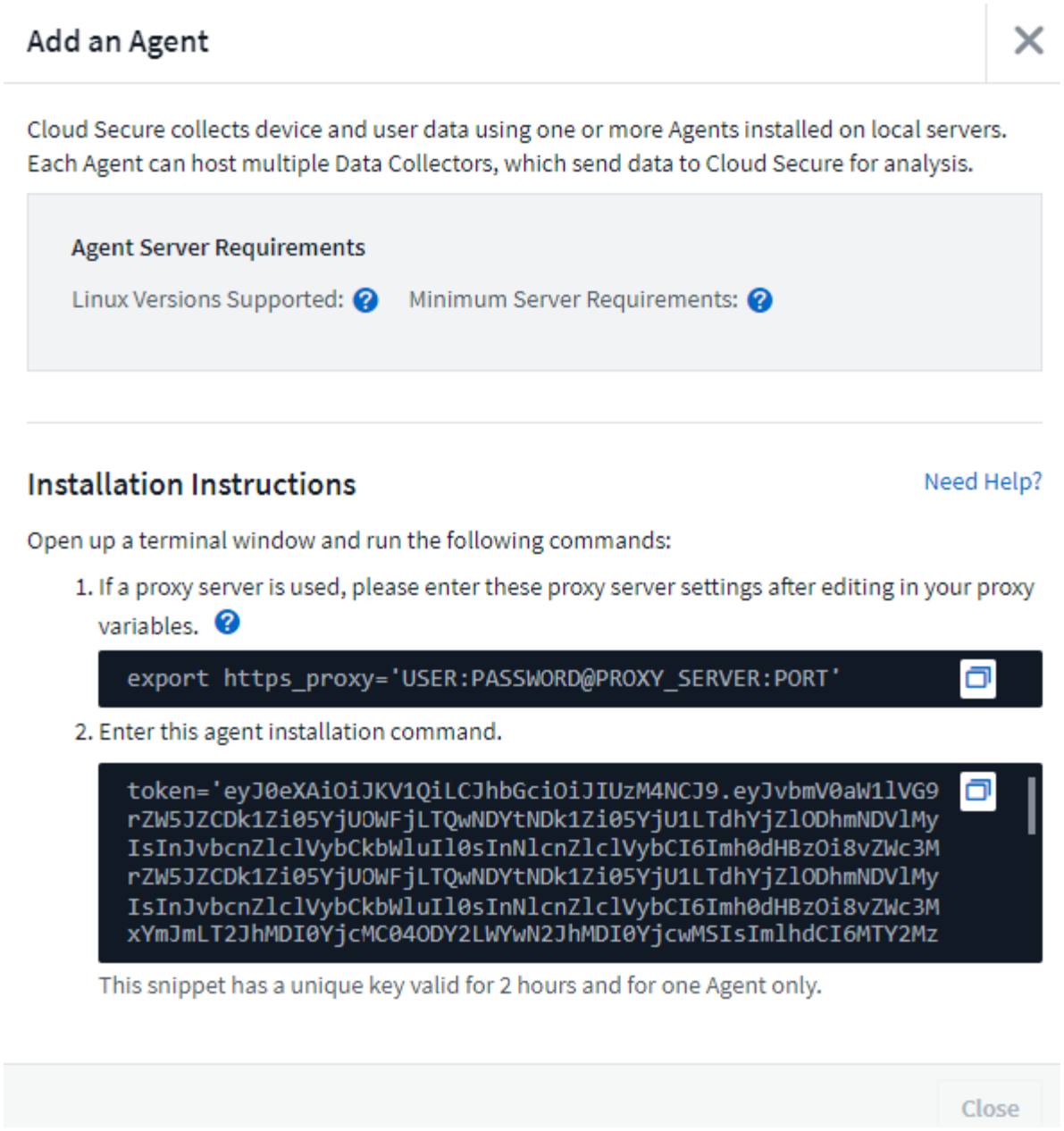
安装代理的步骤

1. 以管理员或帐户所有者身份登录到工作负载安全环境。
2. 选择*Collectors > Agents>+Agent*

   系统将显示 "Add an Agent" 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 _versions supported （ 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，系统将显示以下消息：

完成后

1. 您需要配置"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、以打开将由工作负载安全性使用的端口。如果对端口范围存在安全问题，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
```

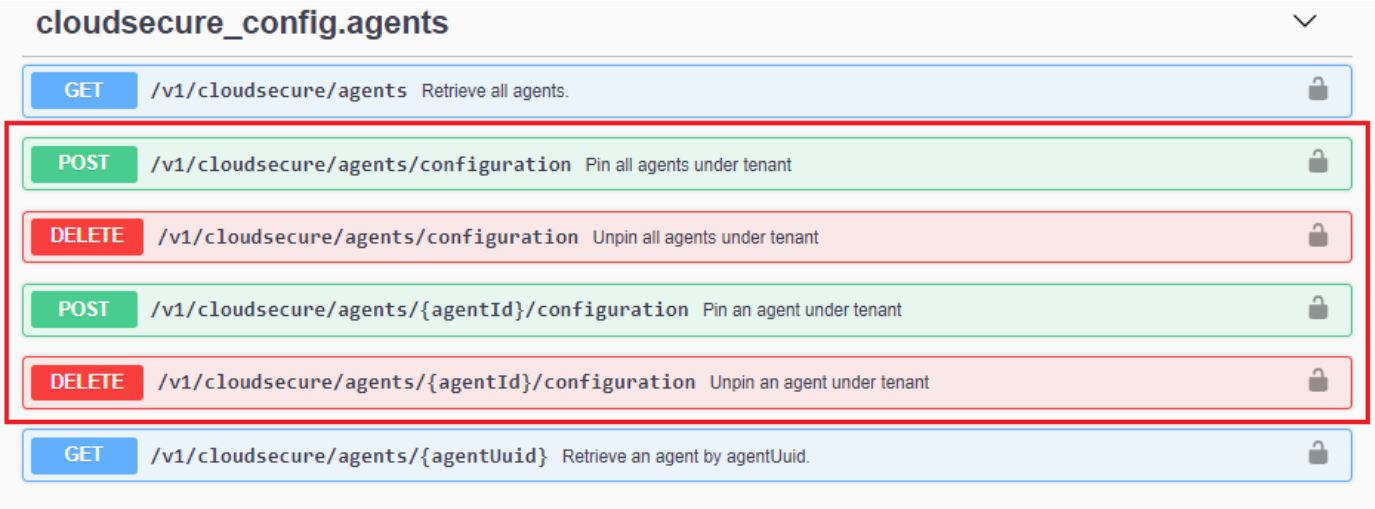
"固定"当前版本的**Agent**

默认情况下、Data Infrastructure Insight Workload Security会自动更新代理。某些客户可能希望暂停自动更新、这将使工程师保持其当前版本、直到出现以下情况之一：

- 客户恢复自动Agent更新。
- 30天过去了。请注意、这30天从最近一次Agent更新的那一天开始、而不是从Agent暂停的那一天开始。

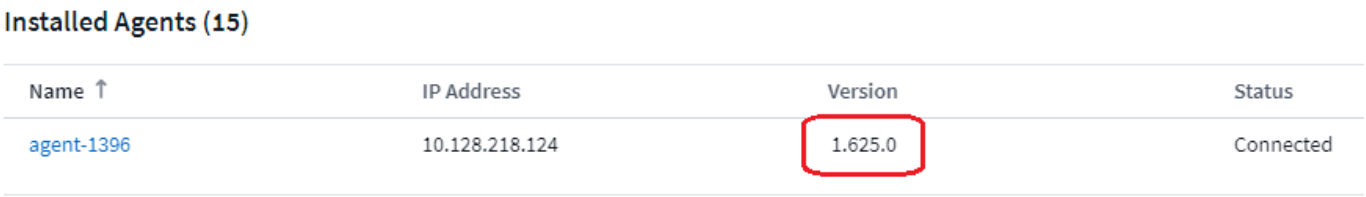
在上述每种情况下、代理都会在下次工作负载安全性刷新时进行更新。

要暂停或恢复自动代理更新、请使用_云 安全_config.agents_ API：



请注意、暂停或恢复操作可能需要长达五分钟才能生效。

您可以在*Agents*选项卡的*Workload Security > Collectors*页面上查看当前的Agent版本。



对代理错误进行故障排除

下表介绍了已知问题及其解决方法。

问题：	解决方法：
代理安装无法创建 /opt/netapp/cloudsecurity/agent/logs/agent.log 文件夹，并且 install.log 文件不提供任何相关信息。	在启动代理期间发生此错误。此错误不会记录在日志文件中，因为它会在日志程序初始化之前发生。此错误将重定向到标准输出、并可通过 `journalctl -u cloudsecure-agent.service`命令显示在服务日志中。此命令可用于进一步解决此问题。EST
代理安装失败，并显示 '不支持此 Linux 版本。正在退出安装。	如果您尝试在不受支持的系统上安装代理、则会出现此错误。请参阅。 "代理要求"
代理安装失败，并显示错误： "-bash： unzip：command not found"	安装 unzip ，然后再次运行安装命令。如果计算机上安装了 Yum ，请尝试 " yum install unzip " 以安装解压缩软件。然后，从代理安装 UI 中重新复制此命令并将其粘贴到命令行界面中以重新执行安装。

问题：	解决方法：

代理已安装并正在运行。但是，代理已突然停止。	通过 SSH 连接到代理计算机。通过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“Failed to start Workload Security daemon service”(无法启动工作负载安全守护进程服务)。2.检查代理计算机中是否存在cssys用户。使用 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，则集中式监控策略可能已删除 `cssys` 用户。4.执行以下命令、手动创建`cssys`用户和组。
	`sudo useradd cssys`
	`sudo groupadd cssys`5.执行以下命令、然后重新启动代理服务：
	`sudo systemctl restart cloudsecure-agent.service`6.如果仍未运行，请检查其他故障排除选项。

无法向代理添加 50 个以上的数据收集器。	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 Agent 处于 not_connected 状态。	重新启动代理的步骤。1.通过 SSH 连接到代理计算机。2.执行以下命令、然后重新启动代理服务： `sudo systemctl restart cloudsecure-agent.service`3.通过检查代理服务的状态 `sudo systemctl status cloudsecure-agent.service`。4.座席应进入已连接状态。
代理 VM 位于 Zscaler 代理之后，代理安装失败。由于Zscaler代理的SSL检查、工作负载安全证书会在Zscaler CA签名时显示出来、因此代理不会信任通信。	在 Zscaler 代理中禁用 * 。 .cloudinsights.netapp.com URL 的 SSL 检查。如果Zscaleer执行SSL检查并替换证书、则工作负载安全性将不起作用。
安装代理时，安装将在解压缩后挂起。	"chmod 755 -rf " 命令失败。如果代理安装命令由非 root sudo 用户运行，而该用户的文件位于工作目录中，属于另一个用户，并且无法更改这些文件的权限，则此命令将失败。由于 chmod 命令失败，其余安装不会执行。1.创建一个名为"云 安全"的新目录。2.转到该目录。3.复制并粘贴完整的"令牌=……./candsSecure 代理安装.sh"安装命令、然后按Enter键。4.安装应该能够继续。
如果工程师仍无法连接到 SaaS ，请向 NetApp 支持部门创建案例。提供用于创建案例的Data Infrastructure Insight序列号、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(volumece-agent-ssys.zip)。a. NetApp 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：	解决方法：
cloudsecure-agent-symptom-collector.sh脚本失败、并显示以下错误。根@计算机tmp]#/opt/netapp/cloudsecurity/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获取服务状态快照获取代理目录结构快照…… 。…… 。/opt/netapp/cloudsecurity/agent/bin/cloudsure-agent-smp-collector.sh：行52：zip：command not found error：failed to create /tmp/cloudsecure-agent-symptoms.zip	未安装zip工具。运行命令"yum install zip "来安装zip工具。然后再次运行cloudsecure-agent-symptom-collector.sh。
代理安装失败、并显示useradd：无法创建目录/home/cssys	如果由于缺少权限而无法在/home下创建用户的登录目录、则可能会发生此错误。临时解决策 将使用以下命令创建cssys用户并手动添加其登录目录：*sudo useradd user_name -m -d home_DIR*-m：如果用户的主目录不存在、请创建该用户的主目录。-d：使用home_DIR作为用户登录目录的值创建新用户。例如、_sudo useradd cssys -m -d /cssys_会添加一个用户_cssys_并在root下创建其登录目录。
安装后代理未运行。*systemctl status cloudsecure-agent.service* cloudsecure-agent.service:显示以下内容：[root ~ demo@]# systemctl status cloudsecure-agent.service agent.service cloudsecure-agent.service–Workload Security Agent Daemon Service loaded：loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled；vendor preset：disabled) Active：activating (auto-restart)(reside-code)(rescue 2021-08：12：26；2s ago Process：25889/excenter=126/system、deport=12：deed NetApp、depresent状态：d=126/d=12：d=126/d=126/12。Aug 03 21：12：26 demo systemd[1]：cloudsecure-agent.service失败。	此操作可能会失败、因为_cssys_用户可能没有安装权限。如果/opt/netapp是NFS挂载、而_cssys_用户无权访问此文件夹、则安装将失败。_cssys_是工作负载安全安装程序创建的本地用户、该用户可能无权访问挂载的共享。要检查此问题、您可以尝试使用_cssys_用户访问/opt/netapp/cloudsecurity/agent/bin/cloudsure-agent。如果返回"permission denies"、则安装权限不存在。安装在计算机本地的目录上、而不是挂载的文件夹。
代理最初是通过代理服务器连接的、代理是在安装期间设置的。现在、代理服务器已更改。如何更改代理的代理配置?	您可以编辑agent.properties以添加代理详细信息。请按照以下步骤操作：1.更改为包含属性文件的文件夹：cd /opt/netapp/cloudsecurity/conf 2。使用您喜爱的文本编辑器、打开_agent.properties_文件进行编辑。3.添加或修改以下行：agent_proxy_host=scspa1950329001.vm.vm.proxy.com NetApp agent_port=80 agent_proxy_user=pxuser agent_proxy_password=pass1234 4.保存文件。5.重新启动代理：sudo systemc联系 重新启动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

删除代理将删除与该代理关联的所有数据收集器。如果您计划使用其他代理配置数据收集器，则应在删除此代理之前为 Data Collector 配置创建备份。

开始之前

1. 确保从工作负载安全门户中删除与代理关联的所有数据收集器。

   注意：如果所有关联的收集器都处于 stopped 状态，请忽略此步骤。

删除代理的步骤：

1. 通过 SSH 连接到代理 VM 并执行以下命令。出现提示时，输入 "y" 以继续。

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

2. 单击*工作负载安全性>收集器>代理*

   系统将显示已配置代理的列表。

3. 单击要删除的代理的选项菜单。
4. 单击 * 删除 * 。

   系统将显示 * 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

可以将工作负载安全性配置为从Active Directory服务器收集用户属性。

开始之前

- 您必须是Data Infrastructure Insight管理员或帐户所有者才能执行此任务。
- 您必须具有托管 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. 在工作负载安全性菜单中，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*

   系统将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	说明

名称	用户目录的唯一名称。例如 *GlobalADCollector*
代理	从列表中选择一个已配置的代理
服务器 IP/ 域名	托管 Active Directory 的服务器的 IP 地址或完全限定域名（ FQDN ）
林名称	目录结构的林级别。林名称支持以下两种格式： *x.y.z* ⇒ SVM 上的直接域名。例如：hq.companyname.com] *dc=x* ， *DC=y* ， *DC=z* ⇒ 相对可分辨名称（例如： DC=HQ ， DC=CompanyName ， DC=com ），或者您可以指定为以下内容： *OU=engineering* ， *DC=HQ* ， *DC=CompanyName* ， *DC=com* 【按特定 OU engineering 进行筛选】 *CN=username* ， *OU=engineering* ， *DC=CompanyName* ， *DC=NetApp* ， *DC=com* 【仅从 OU <engineering>] 中获取具有 <username> 的特定用户， compcn=Acrobat 用户， CN=Users ， DC=HQ ， DC=com ， DC=All Users ，
绑定 DN	允许搜索目录的用户。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_read-only Domain Controllers_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

如果已在 Active Directory 中修改默认属性名称，请输入以下目录服务器所需属性。大多数情况下，这些属性名称在 Active Directory 中都是 *not* 修改的，在这种情况下，您只需继续使用默认属性名称即可。

属性	目录服务器中的属性名称
显示名称	name
SID	对象 SID
用户名	sAMAccountName

单击包括可选属性以添加以下任何属性：

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	电话编号
角色	标题
国家/地区	CO
状态	state
部门	部门
照片	ThumbnailPhote.

ManagerDN	管理器
组	成员

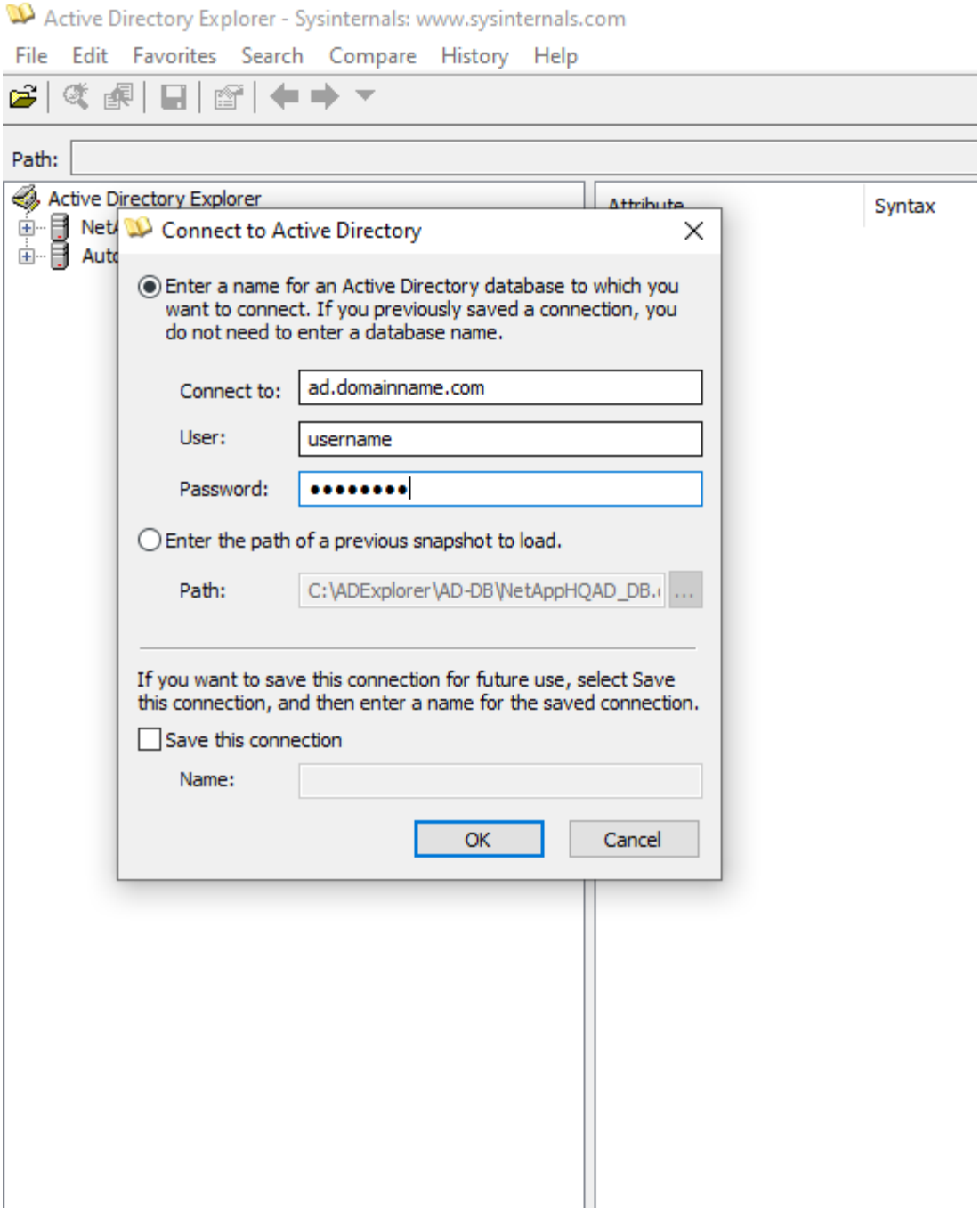
测试用户目录收集器配置

您可以使用以下过程验证 LDAP 用户权限和属性定义：

- 使用以下命令验证工作负载安全性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 资源管理器导航 AD 数据库，查看对象属性和属性，查看权限，查看对象架构，执行复杂的搜索，您可以保存这些搜索并重新执行这些搜索。
  - 安装"AD 资源管理器"在可连接到AD服务器的任何Windows计算机上。
  - 使用 AD 目录服务器的用户名 / 密码连接到 AD 服务器。



对用户目录收集器配置错误进行故障排除

下表介绍了在收集器配置期间可能发生的已知问题和解决方法：

问题：	解决方法：
添加用户目录连接器会导致 ‘Error ' 状态。错误消息为 " 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 ‘Error ' 状态。错误显示： " 无法获取作为林名称提供的 DN=DC=HQ ， DC=DOMAINNAME ， DC=com 对应的对象。 "	提供的林名称不正确。编辑并提供正确的林名称。

问题：	解决方法：
域用户的可选属性未显示在工作负载安全用户配置文件页面中。	这可能是因为在 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。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，并显示 "Failed to retrieve LDAP users.失败原因：无法在服务器上连接，连接为空 "	单击 *Restart* 按钮重新启动收集器。
添加用户目录连接器会导致 ‘Error ' 状态。	确保为所需字段（服务器，林名称，绑定 DN ，绑定密码）提供了有效值。确保绑定 DN 输入始终以 ‘Administrator@ <domain_for林 _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出现 ‘retrying ' 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 ）] 失败，因为 java.net.ConnectionException:Connection 被拒绝。 "	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 ‘Error ' 状态。错误消息为 " 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 ‘Error ' 状态。错误显示： " 无法加载设置。原因：数据源配置出错。具体原因： /connector/conf/application.conf： 70： ldap.ldap-port has type string rather than number "	提供的端口值不正确。尝试使用默认端口值或正确的 AD 服务器端口号。
我先从必备属性入手，然后它便可正常运行。添加可选属性后，无法从 AD 提取可选属性数据。	这可能是因为在 CloudSecure 中添加的可选属性与 Active Directory 中的实际属性名称不匹配。编辑并提供正确的必填或可选属性名称。
重新启动收集器后，何时会进行 AD 同步？	收集器重新启动后，将立即进行 AD 同步。提取大约 30 万个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。
用户数据已从 AD 同步到 CloudSecure 。何时删除数据？	如果不刷新，用户数据将保留 13 个月。如果删除租户，则数据将被删除。
User Directory 连接器会导致 ‘Error ' 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"	提供的林名称不正确。请参见上文，了解如何提供正确的林名称。

问题：	解决方法：
未在用户配置文件页面中填充电话号码。	这很可能是由于 Active Directory 存在属性映射问题。1.编辑要从Active Directory中提取用户信息的特定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“电话号码”。4.现在、请按照上述说明使用Active Directory资源管理器工具浏览Active Directory并查看正确的属性名称。3.‘Active Directory中有一个名为“Telephonenumber”的属性，该属性确实包含用户的电话号码。5.‘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。在可选属性部分中，将 ‘telphonenumber ' 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、并在用户配置文件页面中显示相同的号码。
如果在Active Directory (AD)服务器上启用了加密证书(SSL)、则工作负载安全用户目录收集器无法连接到AD服务器。	在配置用户目录收集器之前禁用 AD 服务器加密。提取用户详细信息后，该详细信息将在 13 个月内显示。如果在提取用户详细信息后 AD 服务器断开连接，则不会提取 AD 中新添加的用户。要重新提取、需要将用户目录收集器连接到AD。
来自Active Directory的数据存在于CloudInsights Security中。希望从CloudInsights中删除所有用户信息。	不能只从CloudInsights Security中删除Active Directory用户信息。要删除此用户、需要删除整个租户。

配置 LDAP 目录服务器收集器

您可以将工作负载安全性配置为从LDAP目录服务器收集用户属性。

开始之前

- 您必须是Data Infrastructure Insight管理员或帐户所有者才能执行此任务。
- 您必须具有托管 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. 在工作负载安全性菜单中，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*

   系统将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	说明
名称	用户目录的唯一名称。例如 *GlobalLDAPCollector*
代理	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 ）

搜索库	LDAP 服务器搜索库的搜索库支持以下两种格式：*x.y.z* ⇒ SVM 上的直接域名。例如：hq.companyname.com] *dc=x* ， *DC=y* ， *DC=z* ⇒ 相对可分辨名称（例如： DC=HQ ， DC=CompanyName ， DC=com ），或者您可以指定为以下内容： *OU=engineering* ， *DC=HQ* ， *DC=CompanyName* ， *DC=com* 【按特定 OU engineering 进行筛选】 *CN=username* ， *OU=engineering* ， *DC=CompanyName* ， *DC=NetApp* ， *DC=com* 【仅从 OU <engineering>> 获取 < 用户名 > 的特定用户】 _CN=Acrobat 用户， CN=Users ， DC=HQ ， DC=com ， DC=All Users ， DC=US ，
绑定 DN	允许搜索目录的用户。例如：对于用户john@dorp.company.com、以下命令为：uid=ldapUser、cn=users、cn=accounts、dc=domain、dc=companyName、dc=com uid=John、cn=users、cn=accounts、dc=dorp、dc=company、dc=com。dorp.company.com
—帐户	-users
— John	-Anna
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

如果已在 LDAP 目录服务器中修改默认属性名称，请输入以下目录服务器所需属性。大多数情况下，这些属性名称在 LDAP 目录服务器中都是 *not* 修改的，在这种情况下，您只需继续使用默认属性名称即可。

属性	目录服务器中的属性名称
显示名称	name
UNIX ID	uidNumber
用户名	UID

单击包括可选属性以添加以下任何属性：

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	电话编号
角色	标题
国家/地区	CO
状态	state
部门	部门编号
照片	照片
ManagerDN	管理器

组	成员

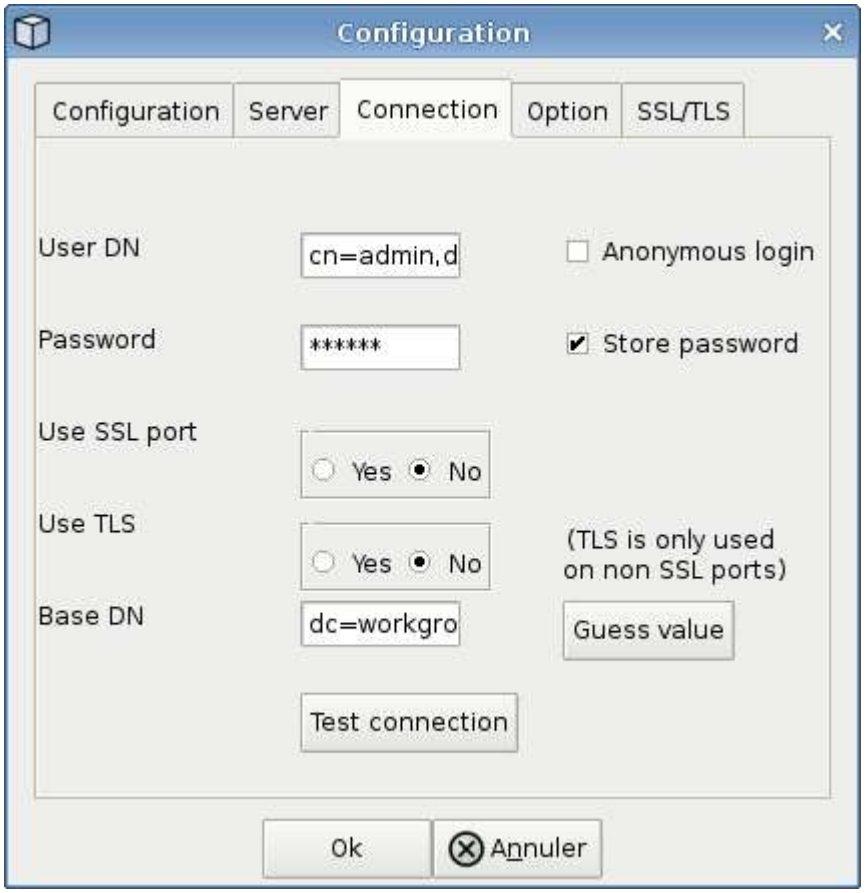
测试用户目录收集器配置

您可以使用以下过程验证 LDAP 用户权限和属性定义：

- 使用以下命令验证工作负载安全性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 资源管理器导航 LDAP
数据库，查看对象属性和属性，查看权限，查看对象架构，执行复杂的搜索，您可以保存这些搜索
并重新执行这些搜索。
```

  - (http://jxplorer.org/在可以连接到LDAP服务器(http://ldaptool.sourceforge.net/的任何Windows计算机上安装LDAP资源管理器()或Java LDAP资源管理器()。
  - 使用 LDAP 目录服务器的用户名 / 密码连接到 LDAP 服务器。



对 LDAP 目录收集器配置错误进行故障排除

下表介绍了在收集器配置期间可能发生的已知问题和解决方法：

问题：	解决方法：
添加 LDAP 目录连接器会导致 ‘Error ' 状态。错误消息为 " 为 LDAP 服务器提供的凭据无效 " 。	提供的绑定 DN ，绑定密码或搜索库不正确。编辑并提供正确的信息。
添加 LDAP 目录连接器会导致 ‘Error ' 状态。错误显示： " 无法获取作为林名称提供的 DN=DC=HQ ， DC=DOMAINNAME ， DC=com 对应的对象。 "	提供的搜索库不正确。编辑并提供正确的林名称。
域用户的可选属性未显示在工作负载安全用户配置文件页面中。	这可能是因为在 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。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，并显示 "Failed to retrieve LDAP users.失败原因：无法在服务器上连接，连接为空 "	单击 *Restart* 按钮重新启动收集器。
添加 LDAP 目录连接器会导致 ‘Error ' 状态。	确保为所需字段（服务器，林名称，绑定 DN ，绑定密码）提供了有效值。确保绑定 DN 输入始终以 uid=ldapUser ， cn=users ， cn=accounts ， dc=domain ， dc=CompanyName ， dc=com 的形式提供。
添加 LDAP 目录连接器会导致出现 ‘retrying ' 状态。显示错误 "Failed to determine the health of the collector hence retrying age"	确保提供了正确的服务器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运行状况，请重新尝试重新启动收集器（错误代码： AGENT008 ） "	确保提供了正确的服务器 IP 和搜索库
添加 LDAP 目录连接器会导致出现 ‘retrying ' 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 ）] 失败，因为 java.net.ConnectionException:Connection 被拒绝。 "	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 ‘Error ' 状态。错误消息为 " 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 。或提供的端口值不正确。尝试使用默认端口值或正确的 LDAP 服务器端口号。
添加 LDAP 目录连接器会导致 ‘Error ' 状态。错误显示： " 无法加载设置。原因：数据源配置出错。具体原因： /connector/conf/application.conf： 70： ldap.ldap-port has type string rather than number "	提供的端口值不正确。尝试使用默认端口值或正确的 AD 服务器端口号。
我先从必备属性入手，然后它便可正常运行。添加可选属性后，无法从 AD 提取可选属性数据。	这可能是因为在 CloudSecure 中添加的可选属性与 Active Directory 中的实际属性名称不匹配。编辑并提供正确的必填或可选属性名称。
重新启动收集器后，何时会进行 LDAP 同步？	收集器重新启动后，将立即进行 LDAP 同步。提取大约 30 万个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。

问题：	解决方法：
用户数据已从 LDAP 同步到 CloudSecure 。何时删除数据?	如果不刷新，用户数据将保留 13 个月。如果删除租户，则数据将被删除。
LDAP 目录连接器会导致 ‘Error ' 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"	提供的林名称不正确。请参见上文，了解如何提供正确的林名称。
未在用户配置文件页面中填充电话号码。	这很可能是由于 Active Directory 存在属性映射问题。1.编辑要从Active Directory中提取用户信息的特定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“电话号码”。4.现在、请按照上述说明使用Active Directory资源管理器工具浏览LDAP目录服务器并查看正确的属性名称。3.确保在LDAP目录中有一个名为“‘Telephonenumber”的属性，该属性确实包含用户的电话号码。5.‘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。在可选属性部分中，将 ‘telphonenumber ' 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、并在用户配置文件页面中显示相同的号码。
如果在Active Directory (AD)服务器上启用了加密证书(SSL)、则工作负载安全用户目录收集器无法连接到AD服务器。	在配置用户目录收集器之前禁用 AD 服务器加密。提取用户详细信息后，该详细信息将在 13 个月内显示。如果在提取用户详细信息后 AD 服务器断开连接，则不会提取 AD 中新添加的用户。要重新提取，需要将用户目录收集器连接到 AD 。

配置 ONTAP SVM 数据收集器

工作负载安全性使用数据收集器从设备收集文件和用户访问数据。

开始之前

- 此数据收集器支持以下功能：
  - Data ONTAP 9.2 及更高版本为获得最佳性能、请使用9.13.1.以上的Data ONTAP版本。
  - SMB协议3.1及更早版本。
  - NFS版本(不低于NFS 4.1且安装了ONTAP 9.15.1或更高版本)。
  - ONTAP 9.4 及更高版本支持 FlexGroup
  - 支持ONTAP Select
- 仅支持数据类型 SVM 。不支持具有无限卷的 SVM 。
- SVM 有多个子类型。其中、仅支持_default*sync_source*sync_destination_.
- 代理"必须进行配置"、然后才能配置数据收集器。
- 请确保已正确配置 User Directory Connector ，否则事件将在 " 活动取证 " 页面中显示编码的用户名，而不

是实际用户名（存储在 Active Directory 中）。

- •从9.14.1版开始支持ONTAP持久存储。
- 为了获得最佳性能，您应将 FPolicy 服务器配置为与存储系统位于同一子网中。
- 您必须使用以下两种方法之一添加 SVM：
  - 使用集群 IP ， SVM 名称以及集群管理用户名和密码。。这是建议的方法。_
    - SVM 名称必须与 ONTAP 中显示的名称完全相同，并且区分大小写。
  - 使用 SVM SVM 管理 IP ，用户名和密码
  - 如果您不能或不愿意使用完整的管理员集群/SVM管理用户名和密码、则可以创建一个Privileges较低的自定义用户、如下一节所述" 关于权限的注释 "。可以为 SVM 或集群访问创建此自定义用户。
    - o 您还可以使用具有至少具有 csrole 权限的角色的 AD 用户，如下面的 " 权限说明 " 一节所述。另请参见"ONTAP 文档"。
- 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.
```

:

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

  系统将返回 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。cluster shell：：> `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。cluster shell：：> `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 'data ' ）。如果使用专用管理lif添加SVM、请跳过此步骤 `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- 启用防火墙后，必须定义一个异常，以允许使用 Data ONTAP 数据收集器的端口传输 TCP 流量。

  有关配置信息、请参见。"代理要求"此适用场景内部部署代理和代理安装在云中。

- 在 AWS EC2 实例中安装代理以监控 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。

阻止用户访问的前提条件

请注意以下事项"用户访问阻止"：

要使此功能正常运行、需要集群级别的凭据。

如果您使用的是集群管理凭据、则不需要任何新权限。

如果您使用的自定义用户(例如_CSUser_)具有为该用户授予的权限、请按照以下步骤为工作负载安全性授予权限以阻止用户。

对于具有集群凭据的 CSUser ，请从 ONTAP 命令行执行以下操作：

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

有关权限的注释

通过*集群管理**IP***添加时的权限：

如果您无法使用集群管理管理员用户允许工作负载安全性访问ONTAP SVM数据收集器、则可以创建一个名为"CSUser"的新用户、其角色如下命令所示。将工作负载安全数据收集器配置为使用集群管理IP时、请使用"CSUser"的用户名和"CSUser"的密码。

要创建新用户，请使用集群管理管理员用户名 / 密码登录到 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 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 Management IP***添加时的权限：

如果您无法使用集群管理管理员用户允许工作负载安全性访问ONTAP SVM数据收集器、则可以创建一个名为"CSUser"的新用户、其角色如下命令所示。将工作负载安全数据收集器配置为使用Vserver管理IP时、请使用"CSUser"的用户名和"CSUser"的密码。

要创建新用户，请使用集群管理管理员用户名 / 密码登录到 ONTAP ，然后在 ONTAP 服务器上执行以下命令。为了方便，请将这些命令复制到文本编辑器中，并将 <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

如果在收集器的_Advanced Configuration_设置中启用了FPolicy引擎选项、则"Workload Security"将在protobuf模式下配置FPolicy引擎。ONTAP 9.15及更高版本支持原始缓冲区模式。

有关此功能的详细信息，请参见"ONTAP 文档"。

protobuf需要特定权限(其中部分或全部可能已存在)：

集群模式：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Vserver模式：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

ONTAP自动防网络软件保护和**ONTAP**访问权限被拒绝

如果您使用的是集群管理凭据、则不需要任何新权限。

如果您使用的自定义用户(例如_CSUser_)具有为该用户授予的权限、请按照以下步骤为工作负载安全性授予权限、以便从ONTAP 收集与ARP相关的信息。

有关详细信息、请阅读"与ONTAP集成访问被拒绝"

和 "与ONTAP 自主勒索软件保护相集成"

配置数据收集器

配置步骤

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

   系统将显示可用的数据收集器。

3. 将鼠标悬停在 * NetApp SVM 磁贴上，然后单击 * + 监控 * 。

   系统将显示 ONTAP SVM 配置页面。为每个字段输入所需数据。

字段	说明
名称	Data Collector 的唯一名称
代理	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，具体取决于您的上述选择。
SVM名称	SVM 的名称（通过集群 IP 进行连接时，此字段为必填字段）
用户名	通过集群 IP 添加时用于访问 SVM/ 集群的用户名选项为： 1.集群管理员 2.'用户的 3.与 CsUser 具有类似角色的 AD 用户。通过SVM IP添加时、选项为：4. vsadmin 5.'用户的 6.与 CsUser 角色类似的 AD-username 。
密码	上述用户名的密码
筛选共享 / 卷	选择是在事件收集中包含还是排除共享 / 卷
输入要排除 / 包括的完整共享名称	要在事件收集中排除或包括（根据需要）的共享的逗号分隔列表
输入要排除 / 包括的完整卷名称	要从事件收集中排除或包括（根据需要）的卷的逗号分隔列表
监控文件夹访问	选中后，将启用文件夹访问监控事件。请注意，即使未选择此选项，也会监控文件夹的创建 / 重命名和删除。启用此选项将增加受监控事件的数量。

设置 ONTAP 发送缓冲区大小	设置 ONTAP Fpolicy 发送缓冲区大小。如果使用的是 9.8p7 之前的 ONTAP 版本，并且显示了性能问题描述，则可以更改 ONTAP 发送缓冲区大小以提高 ONTAP 性能。如果您未看到此选项，但希望了解此选项，请联系 NetApp 支持部门。

完成后

- 在 "Installed Data Collectors" 页面中，使用每个收集器右侧的选项菜单编辑数据收集器。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的建议配置

对于MetroCluster、建议执行以下操作：

1. 将两个数据收集器连接起来、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_Cluster IP_进行连接。
3. 在任何时刻、一个数据收集器应正在运行、另一个数据收集器将出现错误。

   当前的‘Running ' SVM的数据收集器将显示为_running。当前‘s的SVM数据收集器将显示为_Error_。
4. 只要发生切换、数据收集器的状态就会从‘running '更改为‘error '、反之亦然。
5. 数据收集器需要长达两分钟的时间才能从"错误"状态变为"正在运行"状态。

服务策略

如果将服务策略与ONTAP * 9.9.1或更高版本*结合使用、则要连接到数据源收集器、需要使用_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9.1.1之前的ONTAP 版本中、不需要设置_data-fpolicy-client_。

播放-暂停Data Collector

现在、2个新操作显示在收集器的"CAE"菜单上(暂停和恢复)。

如果Data Collector处于_running"状态、则可以暂停收集。打开收集器的"三点"菜单、然后选择暂停。暂停收集器时、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、不会有Fpolicy事件从ONTAP流向数据收集器、也不会从数据收集器流向数据基础架构洞察。

请注意、如果在收集器暂停时在ONTAP上创建了任何新卷等、则"工作负载安全性"不会收集数据、这些卷等也不会反映在信息板或表中。

请记住以下几点：

- 根据已暂停收集器上配置的设置、不会执行Snapshot清除。
- 暂停的收集器不会处理EMS事件(如ONTAP ARP)。这意味着、如果ONTAP发现勒索软件攻击、Data Infrastructure Insight Workload Security将无法获得该事件。
- 不会为已暂停的收集器发送运行状况通知电子邮件。
- 暂停的收集器不支持手动或自动操作(例如Snapshot或用户阻止)。
- 在代理或收集器升级、代理VM重新启动/重新启动或代理服务重新启动时、暂停的收集器将保持_Paused.
- 如果数据收集器处于_Error_状态、则无法将此收集器更改为_Paused _状态。只有当收集器的状态为_running"时、暂停按钮才会启用。
- 如果代理已断开连接、则无法将收集器更改为_Paused _状态。收集器将进入_STOPPED _状态、暂停按钮将被禁用。

永久性存储

ONTAP 9.14.1及更高版本支持永久性存储。请注意、卷名称说明从ONTAP 9.14到9.15不等。

通过选中收集器编辑/添加页面中的复选框、可以启用永久性存储。选中此复选框后、将显示一个文本字段、用于接受卷名称。卷名称是启用永久性存储的必填字段。

- 对于ONTAP 9.14.1、必须先创建卷、然后再启用此功能、并在_Volume Name_字段中提供相同的名称。建议的卷大小为16 GB。
- 对于ONTAP 9.151、收集器将使用_Volume Name_字段中提供的名称自动创建大小为16 GB的卷。

永久性存储需要特定权限(其中部分或全部可能已存在)：

集群模式：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Vserver模式：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

故障排除

有关故障排除提示、请参见"SVM收集器故障排除"页面。

为NetApp ONTAP 收集器配置Cloud Volumes ONTAP 和Amazon FSX

工作负载安全性使用数据收集器从设备收集文件和用户访问数据。

Cloud Volumes ONTAP 存储配置

要配置单节点/HA AWS实例以托管工作负载安全代理、请参见OnCommand Cloud Volumes ONTAP文档：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中均受支持。例如：Amazon、Azure、Google Cloud。
- ONTAP Amazon FSX

代理计算机配置

必须在云服务提供商的相应子网中配置代理计算机。请在"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Agent的步骤。在Azure或Google Cloud中、可以按照适用于云服务提供商的等效步骤进行安装。

在AWS中、按照以下步骤配置要用作工作负载安全代理的计算机：

按照以下步骤配置要用作工作负载安全代理的计算机：

步骤

1. 登录到 AWS 控制台并导航到 EC2-Instances 页面，然后选择 *Launch Instance* 。
2. 选择具有此页面中所述的相应版本的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 个 vCPU 和 16 GB RAM ）作为已分配的资源。
    a. 创建 EC2 实例。
5. 使用 YUM 软件包管理器安装所需的 Linux 软件包：
    a. 安装 *wget* 和 _unzip _ 原生 Linux 软件包。

安装工作负载安全代理

1. 以管理员或帐户所有者身份登录到您的Data Infrastructure Insight环境。
2. 导航到工作负载安全性*Collectors*并单击*Agents*选项卡。
3. 单击 * + 代理 * 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已登录的 RHEL EC2 实例中。此操作将安装Workload Security代理、前提是满足所有"代理前提条件"要求。

有关详细步骤、请访问此链接：https://docs。NetApp．com/us-en/ldinsights /Task _cs_add_agent.html#Steps-to－install-agent

故障排除

下表介绍了已知问题及其解决方法。

问题	解决方法
数据收集器显示"工作负载安全性：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数据收集器添加到工作负载安全性中。从代理通过端口443连接到FSxN集群时超时。防火墙和AWS安全组启用了允许通信所需的规则。代理已部署且位于同一AWS帐户中。同一代理用于连接和监控其余NetApp设备(并且所有设备均正常运行)。	通过将fsxadmin LIF网段添加到代理的安全规则来解决此问题描述。如果不确定端口、则允许使用所有端口。

用户管理

Workload Security用户帐户通过Data Infrastructure Insight进行管理。

Data Infrastructure Insight提供了四个用户帐户级别：帐户所有者、管理员、用户和来宾。系统会为每个帐户分配特定的权限级别。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、自动化响应策略以及工作负载安全API等功能。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以及查看取证。用户角色可以更改警报状态，添加注释，手动创建快照以及限制用户访问。
来宾	可以查看警报和取证。来宾角色不能更改警报状态，添加备注，手动创建快照或限制用户访问。

步骤

1. 登录到工作负载安全性
2. 在菜单中，单击 * 管理员 > 用户管理 *

   您将被转发到Data Infrastructure Insight的User Management页面。

3. 为每个用户选择所需的角色。

添加新用户时，只需选择所需角色（通常为用户或来宾）即可。

有关用户帐户和角色的详细信息、请参见Data Infrastructure Insight"用户角色"文档。

SVM事件速率检查程序(代理规模估算指南)

事件速率检查器用于在安装 ONTAP SVM 数据收集器之前检查 SVM 中的 NFS/SMB 组合事件速率，以查看一个代理计算机能够监控的 SVM 数量。使用事件速率检查器作为规模估算指南、帮助您规划安全环境。

一个代理最多可支持50个数据收集器。

要求

- 集群IP
- 集群管理员用户名和密码

运行此脚本时，不应为要确定事件速率的 SVM 运行任何 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
. 此脚本要求在 Linux 计算机中安装 _sshpass_ 。可通过两种方式安装它：
```

a. 运行以下命令：

```
 linux_prompt> yum install sshpass
.. 如果不起作用，请从 Web 将 _sshpass_ 下载到 Linux 计算机并运行以下命令：
```

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

3. 出现提示时，请提供正确的值。请参见以下示例。
4. 运行此脚本大约需要 5 分钟。
5. 运行完成后，此脚本将从 SVM 中打印事件速率。您可以在控制台输出中检查每个 SVM 的事件速率：

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

每个 ONTAP SVM 数据收集器都可以与一个 SVM 相关联，这意味着每个数据收集器都能够接收单个 SVM 生成

的事件数量。

请记住以下几点：

a)使用此表作为一般规模估算指南。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数量、最多可增加50个数据收集器：

代理计算机配置	SVM 数据收集器的数量	Agent Machine 可以处理的最大事件速率
4 核， 16 GB	10 个数据收集器	每秒 20 ， 000 个事件
4 核， 32 GB	20 个数据收集器	每秒 20 ， 000 个事件

b ）要计算事件总数，请添加为该代理的所有 SVM 生成的事件。

c ）如果脚本未在高峰时段运行，或者流量峰值难以预测，请保留 30% 的事件速率缓冲区。

B + C 应小于 A ，否则 Agent 计算机将无法监控。

换言之，可添加到单个代理计算机的数据收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
```

有关其他前提条件和要求、请参见link:concept_cs_agent_requirements.html["代理要求"]页面。

示例

假设我们有三个 SVMS ，每秒生成的事件速率分别为 100 ， 200 和 300 个。

我们将应用以下公式：

```
 (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.
```

控制台输出可在 Agent 计算机中的当前工作目录中的文件名 *fpolicy_stat*<SVM Name>.log__ 中找到。

在以下情况下，此脚本可能会提供错误的结果：

- 提供的凭据， IP 或 SVM 名称不正确。
- 如果已存在具有相同名称，序列号等的 fpolicy ，则会出现错误。
- 脚本在运行时会突然停止。

下面显示了一个脚本运行示例：

```
[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性的SVM上运行此脚本、它是仅使用SVM上的现有fpolicy配置还是设置一个临时脚本并运行此过程?	即使已为工作负载安全性配置SVM、事件速率检查器也可以正常运行。不应产生任何影响。
是否可以增加可运行此脚本的SVM数量?	是。只需编辑脚本并将 SVM 的最大数量从 5 更改为任何所需数量即可。
如果增加SVM的数量、是否会增加脚本的运行时间?	不会。即使增加了SVM数量、该脚本也将运行最长5分钟。
是否可以增加可运行此脚本的SVM数量?	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。
如果增加SVM的数量、是否会增加脚本的运行时间?	不会。即使增加了SVM数量、该脚本也将运行最长5分钟。
如果我使用现有代理运行事件速率检查程序、会发生什么情况?	对现有代理运行事件速率检查发生原因 程序可能会增加SVM上的延迟。这种增加在事件速率检查程序运行期间是临时的。