



入门

Data Infrastructure Insights

NetApp
October 08, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/data-infrastructure-insights/task_cs_getting_started.html on October 08, 2025. Always check docs.netapp.com for the latest.

目录

入门	1
工作负载安全性入门	1
工作负载安全代理要求	1
其他建议	2
云网络访问规则	2
网络内规则	3
系统规模估算	4
安装工作负载安全代理	4
开始之前	4
安装代理的步骤	5
网络配置	7
"固定"当前版本的Agent	7
对代理错误进行故障排除	8
删除工作负载安全代理	10
删除代理	11
配置 Active Directory （AD）用户目录收集器	11
测试用户目录收集器配置	13
对用户目录收集器配置错误进行故障排除	14
配置 LDAP 目录服务器收集器	16
测试用户目录收集器配置	18
对 LDAP 目录收集器配置错误进行故障排除	19
配置 ONTAP SVM 数据收集器	20
开始之前	20
Test Connectivity for Data Collectors	22
阻止用户访问的前提条件	23
有关权限的注释	23
配置数据收集器	26
MetroCluster的建议配置	27
服务策略	27
播放-暂停Data Collector	27
永久性存储	28
迁移收集器	28
故障排除	29
对ONTAP SVM数据收集器进行故障排除	29
为NetApp ONTAP 收集器配置Cloud Volumes ONTAP 和Amazon FSX	36
Cloud Volumes ONTAP 存储配置	36
支持的平台	37
代理计算机配置	37
安装工作负载安全代理	37

故障排除	37
用户管理	38
SVM事件速率检查程序(代理规模估算指南)	38
要求	39
示例	40
故障排除	41

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

你必须"安装工作负载安全代理"以便从数据收集者那里获取信息。在安装代理之前，请确保您的环境满足操作系统、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。

组件	Linux 要求
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
内存	16 GB RAM
可用磁盘空间	应按以下方式分配磁盘空间：/opt/Filesystem 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	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	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	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	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，用于处理 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。
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。



全局变化可能会对您的ONTAP系统产生潜在影响。强烈建议在非高峰时段进行影响大量数据收集器的更改。

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：

Add an Agent [X]

Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

[Close]

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。

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：

cloudsecure_config.agents



GET	/v1/cloudsecure/agents	Retrieve all agents.	
POST	/v1/cloudsecure/agents/configuration	Pin all agents under tenant	
DELETE	/v1/cloudsecure/agents/configuration	Unpin all agents under tenant	
POST	/v1/cloudsecure/agents/{agentId}/configuration	Pin an agent under tenant	
DELETE	/v1/cloudsecure/agents/{agentId}/configuration	Unpin an agent under tenant	
GET	/v1/cloudsecure/agents/{agentUuid}	Retrieve an agent by agentUuid.	

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。

Installed Agents (15)

Name ↑	IP Address	Version	Status
agent-1396	10.128.218.124	1.625.0	Connected

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。	<p>通过 SSH 连接到代理计算机。通过检查代理服务状态 <code>sudo systemctl status cloudsecure-agent.service</code>。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。</p> <pre>sudo id cssys</pre> <pre>sudo groups cssys`</pre> <p>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。</p> <pre>`sudo useradd cssys</pre> <pre>`sudo groupadd cssys`</pre> <p>5.执行以下命令、然后重新启动代理服务：</p> <pre>`sudo systemctl restart cloudsecure-agent.service`</pre> <p>6.如果仍未运行，请检查其他故障排除选项。</p>
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。	<p>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：</p> <pre>sudo systemctl restart cloudsecure-agent.service`</pre> <p>3.通过检查代理服务的状态</p> <pre>`sudo systemctl status cloudsecure-agent.service。</pre> <p>4.座席应进入已连接状态。</p>
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。	<p>"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。</p>
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。	<p>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</p>

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。临时决策 将使用以下命令创建cssys用户并手动添加其登录目录： <code>sudo useradd user_name -m -d home_DIR-m</code> ：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、 <code>_sudo useradd cssys -m -d /cssys_</code> 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。 <code>systemctl status cloudsecure-agent.service</code> 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： <code>cd /opt/netapp/cloudsecurity/conf</code> 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： <code>agent_proxy_host=scspa1950329001.vm.vm.proxy.com</code> <code>NetApp agent_port=80</code> <code>agent_proxy_user=pxuser</code> <code>agent_proxy_password=pass1234</code> 4.保存文件。 5.重新启动代理： <code>sudo systemctl restart cloudsecure-agent.service</code>

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 <i>GlobalADCollector</i>
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	ThumbnailPhoto.

ManagerDN	管理器
组	成员

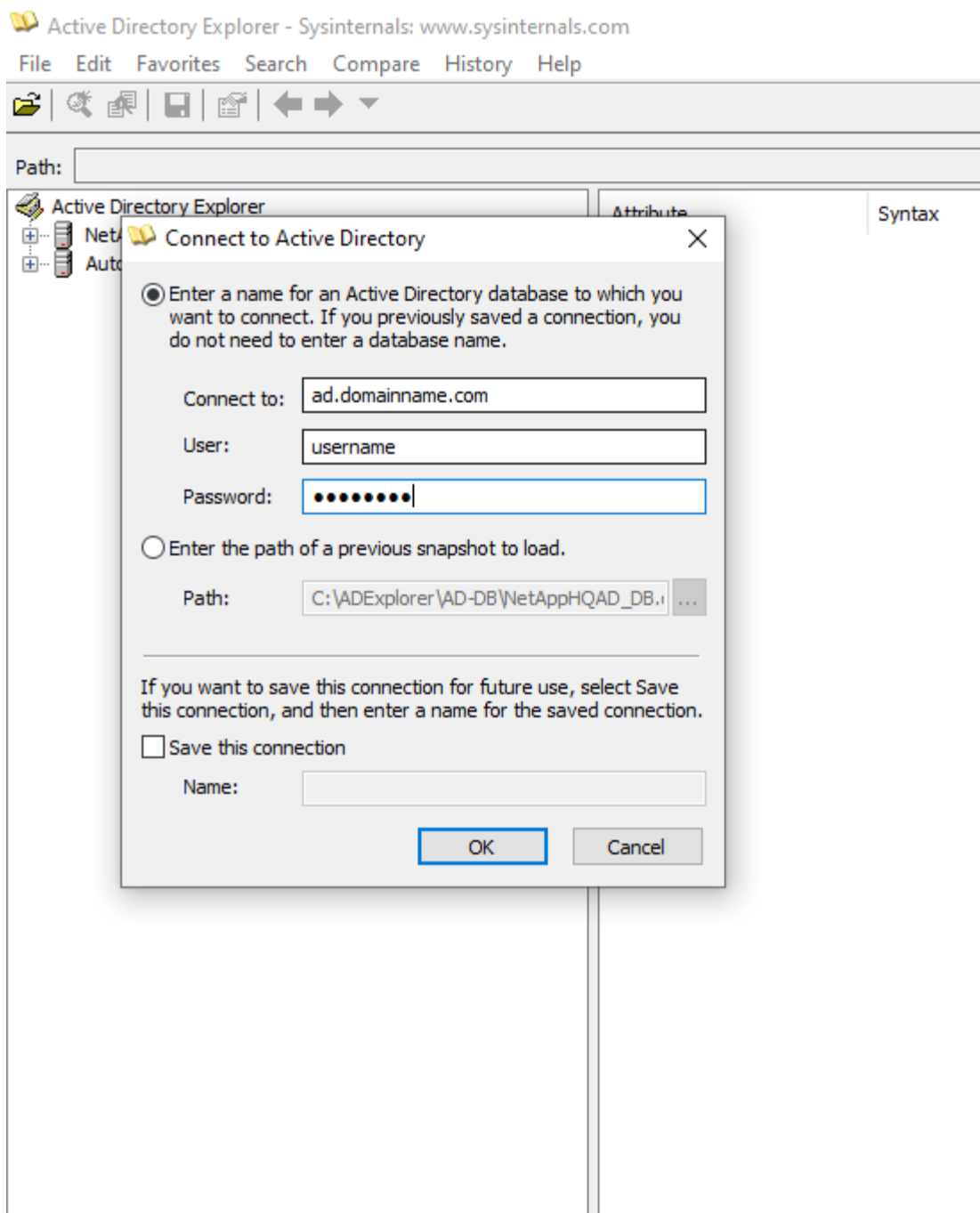
测试用户目录收集器配置

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 <i>Restart</i> 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.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 <i>GlobalLDAPCollector</i>
代理	从列表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.companyn.com 、以下命令为： uid=ldapUser、cn=users、cn=accounts、dc=domain、dc=companynName、dc=com uid=John、cn=users、cn=accounts、dc=dorp、dc=companyn、dc=com。dorp.companyn.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	电话号码
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。

The screenshot shows a 'Configuration' dialog box with five tabs: Configuration, Server, Connection, Option, and SSL/TLS. The 'Configuration' tab is active. It contains the following fields and controls:

- User DN:** A text box containing 'cn=admin,d'.
- Password:** A text box containing '*****'.
- Use SSL port:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Use TLS:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Base DN:** A text box containing 'dc=workgro'.
- Anonymous login:** An unchecked checkbox.
- Store password:** A checked checkbox.
- (TLS is only used on non SSL ports):** A note next to the TLS options.
- Guess value:** A button next to the Base DN field.
- Test connection:** A button at the bottom of the configuration section.
- Ok and Annuler buttons:** At the bottom of the dialog box.

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 <i>Restart</i> 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

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。



全局变化可能会对您的ONTAP系统产生潜在影响。强烈建议在非高峰时段进行影响大量数据收集器的更改。

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(最高为NFS 4.1、含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 有多个子类型。其中、仅支持 `_defaultsync_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 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。
 - 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 <vservename> -user-or-group
-name <username>
```

示例输出

```
Vserver: svmname
```

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication 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"GMT"(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之间必须存在有效路由。

Test Connectivity for Data Collectors

The test connectivity feature (introduced March 2025) aims to help end users identify the specific causes of failures when setting up data collectors in Data Infrastructure Insights (DII) Workload Security. This allows the users to self-correct issues related to network communication or missing roles.

This feature will help users determine if all network-related checks are in place before setting up a data collector. Additionally, it will inform users about the features they can access based on the ONTAP version, roles, and permissions assigned to them in ONTAP.



Test connectivity is not supported for User Directory collectors

Prerequisites for Connection Testing

- Cluster level credentials are needed for this feature to work in full.
- Feature access check is not supported in SVM mode.
- 如果您使用的是集群管理凭据、则不需要任何新权限。
- If you are using a custom user (e.g., *csuser*), provide the mandatory permissions and feature specific permissions for the features you want to use.



Be sure to review the [权限](#) section below as well.

Test the Connection

The user can go to the add/edit collector page, enter the cluster level details (in Cluster Mode) or SVM level details (in SVM Mode), and click on the **Test Connection** button. Workload Security will then process the request and display an appropriate success or failure message.

Add ONTAP SVM

[Need Help?](#)

An Agent is required to fetch data from the ONTAP SVM in to Storage Workload Security

Network Checks:

Https: Connection successful on port 443 (AGENT -> ONTAP)

Ontap Version: 9.14.1

Data Lifs: Found 1 (10.10.10.10) data interfaces in the SVM which contains service name data-fpolicy-client, admin/oper status as up.

Agent IP: Determined agent IP address to be used (10.10.10.10)

✔ Fpolicy Server: Connection successful on Agent IP (10.10.10.10), ports [35037, 35038, 35039] (ONTAP -> AGENT)

Features (User has permissions):

Snapshot, Ems, Access Denied, Persistent Store, Ontap ARP, User Blocking

Features (User does not have permissions):

Protobuf: Ontap version 9.14.1 is below minimum supported version 9.15.0

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。

如果您使用的是自定义用户(例如、-CsUser_)并为该用户授予了权限、请按照中的步骤“[用户访问阻止](#)”为“工作负载安全性”授予权限以阻止用户。

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。

注意: 您可以创建一个角色、用于自定义用户的所有功能权限。如果存在现有用户、请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 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 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。

注意：您可以创建一个角色、用于自定义用户的所有功能权限。如果存在现有用户、请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
<vservename>
security login role delete -role csrole -cmddirname * -vserver
<vservename>
security login rest-role delete -role csrestrole -api * -vserver
<vservename>

```

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 <vservename> 替换为您的 Vserver 名称，然后在 ONTAP 上执行这些命令：

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

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

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

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

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 role create -role csrole -cmddirname "vserver fpolicy"  
-access all  
Vserver模式：
```

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

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.'CSUser' 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.'CSUser' 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

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。



如果某个收集器的用户受限、则无法暂停此收集器。暂停收集器之前、请恢复用户访问权限。

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将无法获取该事件。
- 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 role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Vserver模式：

```
security login role create -vserver <vservename> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservename> -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、从而在代理之间实现高效的收集器负载平衡。

前提条件

- 源业务代表必须处于_connected状态。
- 要迁移的收集器必须处于_running"状态。

注意：

- 数据和用户目录收集器均支持迁移。
- 手动管理的租户不支持迁移收集器。

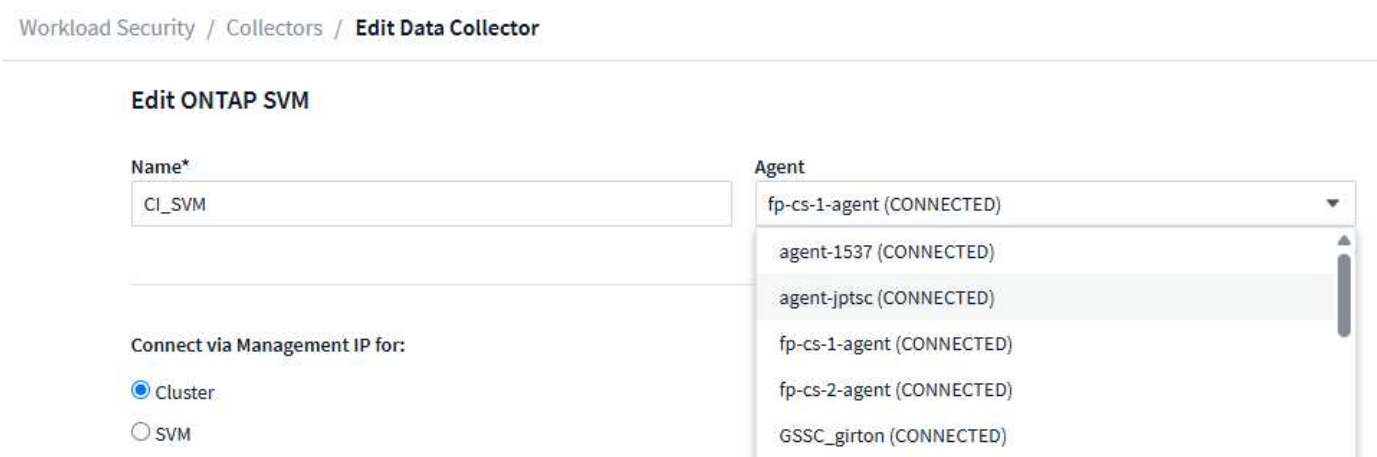
迁移收集器

要迁移收集器、请执行以下步骤：

1. 转到"编辑收集器"页面。
2. 从业务代表下拉列表中选择目标业务代表。
3. 单击"保存收集器"按钮。

Workload Security将处理此请求。成功迁移后、用户将重定向到收集器列表页面。如果失败、编辑页面上将显示相应的消息。

注意：在将收集器成功迁移到目标代理后、先前在"编辑收集器"页面上所做的任何配置更改将保持应用。



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。

对ONTAP SVM数据收集器进行故障排除


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。您可以在此处找到有关对此收集器问题进行故障排除的提示。

有关配置此收集器的说明、请参见"[配置SVM收集器](#)"页面。

如果出现错误、您可以单击已安装数据收集器页面的_Status_列中的_more详细信息_以了解有关此错误的详细

信息。

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

下面介绍了已知问题及其解决方法。

问题：Data Collector运行一段时间、并在随机时间后停止、失败并显示："错误消息：连接器处于错误状态。服务名称：audit。失败原因：外部 fpolicy 服务器过载。"

尝试此操作：ONTAP的事件速率远远高于Agent Box所能处理的事件速率。因此，此连接已终止。

检查断开连接时 CloudSecure 中的峰值流量。您可以从 * CloudSecure > 活动取证 > 所有活动 * 页面查看此信息。

如果聚合流量峰值高于 Agent Box 可以处理的流量，请参阅 Event Rate Checker 页面，了解如何在 Agent Box 中估算收集器部署的规模。

如果此代理在2021年3月4日之前安装在Agent框中、请在Agent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。

*问题：*收集器报告错误消息："在可访问SVM数据接口的连接器上找不到本地IP地址"。*请尝试以下操作：
：*这很可能是由于ONTAP端的网络问题。请按照以下步骤操作：

1. 确保 SVM 数据 LIF 或管理 LIF 上没有防火墙阻止与 SVM 的连接。
2. 通过集群管理IP添加SVM时、请确保SVM的数据LIP和管理LIP可从此代理VM执行ping。如果出现问题，请检查网关，网络掩码和 LIF 路由。

您也可以尝试使用集群管理 IP 通过 ssh 登录到集群，并对代理 IP 执行 ping 操作。确保代理IP可执行pingable：

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

如果无法执行pingable，请确保ONTAP中的网络设置正确，以便Agent计算机可以执行pingable。

3. 如果您尝试通过集群IP进行连接、但该连接不起作用、请尝试直接通过SVM IP进行连接。有关通过 SVM IP 进行连接的步骤，请参见上文。
4. 通过SVM IP和vsadmin凭据添加收集器时、请检查SVM LIF是否已启用数据加管理角色。在这种情况下，对 SVM LIF 执行 ping 操作将有效，但对 SVM LIF 执行 SSH 将不起作用。如果是，请创建一个仅 SVM 管理 LIF ，并尝试通过此仅 SVM 管理 LIF 进行连接。
5. 如果仍然无法正常工作、请创建一个新的SVM LIF、然后尝试通过该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. 请等待、直到出现错误。停止 ONTAP 中的数据包跟踪。
 - d. 从ONTAP打开数据包跟踪。可从该位置获取

```
https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
```

```
.. 确保有一个从ONTAP到Agent框的SNT。  
.. 如果没有来自ONTAP的任何Synology认证系统、则表示  
ONTAP中的防火墙存在问题。  
.. 打开ONTAP中的防火墙、以便ONTAP能够连接代理盒。
```

7. 如果它仍然不工作、请咨询网络团队、以确保没有外部防火墙阻止从ONTAP到Agent Box的连接。
8. 如果上述方法均无法解决问题、请向创建案例以"[NetApp 支持](#)"获得进一步帮助。

问题：*消息："无法确定[主机名：<IP Address>的ONTAP类型。原因：存储系统<IP Address>连接错误：无法访问主机(无法访问主机)"*请尝试此操作：

1. 验证是否已提供正确的SVM IP管理地址或集群管理IP。
2. 通过SSH连接到要连接的SVM或集群。连接后，请确保 SVM 或集群名称正确无误。

问题:*错误消息:"连接器处于错误状态。**service.name** : 审核。失败原因: 外部 **fpolicy** 服务器已终止。
" 请尝试此操作: *

1. 很可能是防火墙阻止了代理计算机中的必要端口。验证是否已为代理计算机打开端口范围 35000-55000/TCP, 以便从 SVM 进行连接。此外, 请确保 ONTAP 端未启用防火墙, 从而无法与代理计算机进行通信。
2. 在代理框中键入以下命令、并确保端口范围已打开。

```
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  
. 登录到 SVM , 输入以下命令并检查是否未设置防火墙以阻止与 ONTAP 的通信。
```

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

"[检查防火墙命令](#)"在ONTAP端。

3. 通过SSH连接到要监控的SVM/集群。从SVM数据Lif对Agent框执行Ping操作(支持CIFS和NFS协议)、并确保Ping操作正常:

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

如果无法执行pingable, 请确保ONTAP中的网络设置正确, 以便Agent计算机可以执行pingable。

4. 如果通过2个数据收集器将一个SVM添加到租户中两次、则会显示此错误。通过用户界面删除其中一个数据收集器。然后, 通过 UI 重新启动另一个数据收集器。然后, 数据收集器将显示 "正在运行" 状态, 并开始从 SVM 接收事件。

基本上, 在租户中, 1 个 SVM 只能通过 1 个数据收集器添加一次。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)中添加了同一个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, 并启动第一个收集器。因此, 第一个收集器将停止接收事件, 其 "审核" 服务将进入错误状态。要防止这种情况发生, 请在一个环境中配置每个 SVM。
6. 如果服务策略配置不正确、也可能发生此错误。对于ONTAP 9.8或更高版本、要连接到数据源收集器、需要提供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LIF关联。

问题:*活动页面中未显示任何事件。 请尝试此操作: *

1. 检查ONTAP收集器是否处于"正在运行"状态。如果是, 请通过打开某些文件确保在 CIFS 客户端 VM 上生成某些 CIFS 事件。
2. 如果未发现任何活动、请登录到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. 如果未发现任何活动、请登录到SVM。输入以下命令:

```
<SVM>fpolicy show
```

检查是否已设置以"云 安全_"前缀命名的fpolicy策略、并且状态是否为"on"。如果未设置, 则代理很可能无法在 SVM 中执行这些命令。请确保已遵循页面开头所述的所有前提条件。

问题: SVM Data Collector处于错误状态、并且错误消息为"Agent failed to connect to the Collector (代理无法连接到收集器)"请尝试此操作:

1. 代理很可能过载、无法连接到数据源收集器。
2. 检查有多少数据源收集器连接到代理。
3. 此外、还可以在用户界面的"All Active"(所有活动)页面中查看数据流速率。
4. 如果每秒的活动数非常高, 请安装另一个代理并将某些数据源收集器移动到新的代理。

问题: SVM数据收集器显示错误消息"fpolicy.server.connectError:节点无法与FPolicy服务器建立连接12.195.15.146(原因: "选择超时")"*尝试此操作: *已在SVM/集群中启用防火墙。因此, fpolicy 引擎无法连接到 fpolicy 服务器。ONTAP中可用于获取详细信息的命令行界面包括:

```
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端。

*问题: *错误消息: "连接器处于错误状态。服务名称: audit。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: 已启动)。"*请尝试以下操作: *确保有一个操作接口(角色为数据、数据协议为CIFS或NFS)。

*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。此周期将重复。*请尝试以下操作: *这通常发生在以下情形中:

1. 添加了多个数据收集器。
2. 显示此类行为的数据收集器将向这些数据收集器添加1个SVM。表示将 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。

问题: *连接器处于错误状态。服务名称: **audit**。失败原因: 无法配置 (**SVM svmname** 上的策略。原因: 为"**fpolicy.policy.scope**修改"中的"**shares-to include**"元素指定的值无效: "**fedified**"*尝试此操作: *共享名称必须不带任何引号。编辑 ONTAP SVM DSC 配置以更正共享名称。

include 和 *exclude shares* 不适用于长列表的共享名称。如果要包含或排除大量共享, 请改用按卷筛选。

*问题: *集群中存在未使用的现有fpolicies.在安装工作负载安全性之前、应如何处理这些问题? *请尝试以下操作: *建议删除所有现有的未使用的fpolicy设置, 即使这些设置处于断开状态也是如此。工作负载安全性将创建前缀为"cloudsure_"的fpolicy。可以删除所有其他未使用的 fpolicy 配置。

用于显示fpolicy list的命令行界面命令:

```
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>
```

|启用工作负载安全性后、ONTAP性能会受到影响: 延迟偶尔会很高、IOPS偶尔会很低。|在将ONTAP与工作负载安全性结合使用时、有时可能会在ONTAP中出现延迟问题。出现这种情况的可能原因如下: "[第1294.](#)"、"[1415152](#)"、"[1438207](#)"、"[1479704](#)" "[1354659](#)"。所有这些问题在ONTAP 9.13.1.及更高版本中均已修复; 强烈建议使用这些更高版本之一。

问题:*数据收集器出错,显示此错误消息。" 错误: 连接器处于错误状态。服务名称: **audit**。失败原因: 无法在 **SVM SVM_test** 上配置策略。原因: **ZAPI** 字段: **Events** 缺少值。"*请尝试此操作:

1. 从仅配置 NFS 服务的新 SVM 开始。
2. 在工作负载安全性中添加ONTAP SVM数据收集器。在工作负载安全性中添加ONTAP SVM数据收集器时、CIFS会配置为SVM的允许协议。
3. 请等待、直到工作负载安全性中的数据收集器显示错误。
4. 由于未在SVM上配置CIFS服务器、因此Workload Security将显示左侧所示的此错误。
5. 编辑 ONTAP SVM 数据收集器并取消选中 CIFS 作为允许的协议。保存数据收集器。它将在仅启用 NFS 协议的情况下开始运行。

问题: *数据收集器显示错误消息: "错误: 无法在2次重试中确定收集器的运行状况、请尝试重新启动收集器(错误代码: **AGENT008**)"。请尝试此操作: *

1. 在数据收集器页面上, 滚动到出现错误的收集器右侧, 然后单击 3 点菜单。选择 *Edit*。再次输入数据收集器的密码。按 **Save** 按钮保存数据收集器。Data Collector 将重新启动, 并应解决此错误。
2. Agent计算机可能没有足够的CPU或RAM余量、这就是DSC出现故障的原因。请检查添加到计算机中代理的数据收集器的数量。如果超过20、请增加Agent计算机的CPU和RAM容量。增加CPU和RAM后、DSCS将自动进入Initializing状态、然后自动进入Running状态。查看上的规模估算指南["此页面"](#)。

*问题: *选择SVM模式后、Data Collector出现错误。*Try this: *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。

*问题:*启用“拒绝访问”功能时, 数据收集器显示错误消息: “连接器处于错误状态。服务名称: **audit**。失败原因: 无法在SVM test_SVM上配置fpolicy。原因: 用户未获得授权。"*请尝试以下操作: *用户可能缺少“拒绝访问”功能所需的REST权限。请按照上的说明["此页面"](#)设置权限。

设置权限后、重新启动收集器。

如果您仍遇到问题, 请访问 * 帮助 > 支持 * 页面中提到的支持链接。

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。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 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。