



工作负载安全性 Cloud Insights

NetApp
April 16, 2024


目录

- 工作负载安全性 1
 - 关于存储工作负载安全性 1
 - 入门 1
 - 警报 37
 - 取证 43
 - 自动响应策略 51
 - 允许的文件类型策略 53
 - 与ONTAP 自主勒索软件保护相集成 54
 - 与ONTAP集成访问被拒绝 56
 - 正在阻止用户访问 58
 - 工作负载安全性：模拟攻击 62
 - 为警报，警告和代理 / 数据源收集器运行状况配置电子邮件通知 66
 - 工作负载安全API 67

工作负载安全性

关于存储工作负载安全性

Cloud Insights 存储工作负载安全性(以前称为Cloud Secure)可通过针对内部威胁的可操作智能来帮助保护您的数据。它可以集中查看和控制混合云环境中的所有企业数据访问，以确保实现安全性和合规性目标。



Cloud Insights 联邦版不提供工作负载安全性。

可见性

集中查看和控制用户对存储在内部或云中的关键企业数据的访问。

更换无法及时准确地查看数据访问和控制情况的工具和手动流程。工作负载安全性在云和内部存储系统上都是唯一的、可为您提供有关恶意用户行为的实时警报。

保护

通过高级机器学习和异常检测功能，防止组织数据被恶意用户或被入侵用户滥用。

通过高级机器学习和用户行为异常检测，提醒您任何异常数据访问。


合规性

通过审核用户对存储在内部或云中的关键企业数据的数据访问，确保企业合规性。

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。



Cloud Insights 联邦版不提供工作负载安全性。

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 Vendor Reference 》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。

工作负载安全代理要求

您必须 ["安装代理"](#) 以便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。



Cloud Insights 联邦版不支持存储工作负载安全性。

组件	Linux 要求
操作系统	运行以下许可版本之一的计算机： Red Hat Enterprise Linux 7.x、8.x 64位、SELinux CentOS 7.x 64位、SELinux CentOS 8 Stream、SELinux Ubuntu 20至22 64位 Rocky 8.x 64位、Rocky 9.x 64位、SELinux SUSE Linux Enterprise Server 15 SP3、SUSE Linux Enterprise Server 15 SP4、SUSE 15 SP3上的SELinux 此计算机不应运行任何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使用"sudo su-"命令。
CPU	4 个 CPU 核
内存	16 GB RAM

组件	Linux 要求
可用磁盘空间	<p>磁盘空间应按以下方式分配： /opt/NetApp 35 GB (最低)</p> <p>注意：建议额外分配一点磁盘空间、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。</p> <p>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、则可能无法安装代理或数据收集器。请参见 "故障排除" 部分、了解更多详细信息。</p>
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：工作负载安全代理可以与Cloud Insights 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 Cloud Insights
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 Cloud Insights
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 Cloud Insights
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。
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

请参见 ["事件速率检查器"](#) 有关规模估算的信息的文档。

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。代理连接到环境中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"](#) 配置代理虚拟机。



Cloud Insights 联邦版不提供工作负载安全性。

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Cloud Insights安全性的信息 ["此处"](#)。

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 ?

CentOS

RHEL

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。

×

Agent Server Requirements

Installation Instructions

Open up a terminal window and run the following commands:

- ```
export https_proxy='USER:PASSWORD@PROXY_SERVER:PORT'
```

- ```
token='eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU4NCJ9.eyJvbmV0aWw1Ilg9
rZW5JZCdk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMy
IsInJvbnZlclVybyCkblw1I0sInNlcnZlclVybyCI6Imh0dHBzOi8vZwZ3M
rZW5JZCdk1Zi05YjU0WFJlLTQwNDYtNDk1Zi05YjU1LTdhYjZlODhmNDVlMy
IsInJvbnZlclVybyCkblw1I0sInNlcnZlclVybyCI6Imh0dHBzOi8vZwZ3M
xYmJmLTJhMDI0YjYjMC04ODY2LWYwN2JhMDI0YjYjcwMSIsIm1hdCI6MTY2Mz
```

Close

- ✔ New agent detected!

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
```

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，并可使用 <code>jlogalctl -u cloudsecure-agent.service</code> 命令在服务日志中看到。此命令可用于进一步对问题描述进行故障排除。
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。请参见 “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 <code>"yum install unzip"</code> 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"无法启动工作负载安全守护进程服务"。2. 检查 Agent 计算机中是否存在 <code>cssys</code> 用户。使用 <code>root</code> 权限逐个执行以下命令，并检查 <code>cssys</code> 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<code>cssys</code>用户。4. 执行以下命令手动创建 <code>cssys</code> 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. 如果它仍未运行、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 <code>not_connected</code> 状态。	重新启动代理的步骤。1. 通过 SSH 连接到代理计算机。2. 执行以下命令重新启动代理服务： <code>sudo systemctl restart cloudsecure-agent.service</code> 3.通过 <code>sudo systemctl status cloudsecure-agent.service</code> 检查代理服务的状态。4. 代理应处于已连接状态。
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 *。 <code>.cloudinsights.netapp.com</code> URL 的 SSL 检查。如果 Zscaler 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。	" <code>chmod 755 -rf</code> " 命令失败。如果代理安装命令由非 <code>root</code> <code>sudo</code> 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 <code>chmod</code> 命令失败，其余安装不会执行。1. 创建一个名为 <code>cloudsecure</code> 的新目录。2. 转到该目录。3. 复制并粘贴完整的 " <code>token=.....</code> ..." <code>./cloudsure-agent-install.sh</code> " 安装命令并按 <code>Enter</code> 键。4. 安装应能继续进行。
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 Cloud Insights 序列号以创建案例，并按照说明将日志附加到案例。	<p>将日志附加到案例： 1.使用 <code>root</code> 权限执行以下脚本并共享输出文件（<code>cloudsure-agent-sympy.zip</code>）。</p> <pre>答/opt/netapp/cloudsecurity/agent/bin/cloudsecure-agent-symptom-collector.sh</pre> <p>2.在 <code>root</code> 权限下逐个执行以下命令，并共享输出。答ID <code>cssys</code> b.组 <code>cssys</code> c.cat <code>/etc/os-release</code></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： <i>sudo useradd user_name -m -d home_DIR-m</i> ：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、 <i>_sudo useradd cssys -m -d /cssys</i> 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_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) Active：激活(自动重新启动)(结果：退出代码)自Cloudue 2021-08-03 21: 12: 26 PDT起；退出前代理进程：dbash /dbash /netapp=25bash /bash /bash：/dcc=bash：25889 (code=exited、status=126)、Aug 03 21: 12: 26 demo systemd1]: cloudsecure-agent.service: main process exited、code=exited、status=126/n/a Aug 03 21: 12: 26 demo systemd1]: unit cloudsecure-agent.service entered.Aug 03 21: 12: 26 demo systemd1]: 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： <i>cd /opt/netapp/cloudsecurity/conf</i> 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： <i>agent_proxy_host=scspa1950329001.vm.netapp.com agent_proxy_port=80 agent_proxy_user=pxuser agent_proxy_password=pass1234</i> 4.保存文件。5.重新启动代理： <i>sudo systemctl restart cloudsecure-agent.service</i>

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

- 要执行此任务，您必须是 Cloud Insights 管理员或帐户所有者。
- 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Workload Security菜单中、单击：
收集器>用户目录收集器>+用户目录收集器*并选择*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： <i>x.y.z</i> ⇒ SVM 上的直接域名。例如： <i>hq.companyname.com</i>] <i>dc=x</i> , <i>DC=y</i> , <i>DC=z</i> ⇒ 相对可分辨名称（例如： <i>DC=HQ</i> , <i>DC=CompanyName</i> , <i>DC=com</i> ），或者您可以指定为以下内容： <i>OU=engineering</i> , <i>DC=HQ</i> , <i>DC=CompanyName</i> , <i>DC=com</i> 【按特定 OU <i>engineering</i> 进行筛选】 <i>CN=username</i> , <i>OU=engineering</i> , <i>DC=CompanyName</i> , <i>DC=NetApp</i> , <i>DC=com</i> 【仅从 OU < <i>engineering</i> >] 中获取具有 < <i>username</i> > 的特定用户， <i>compcn=Acrobat</i> 用户， <i>CN=Users</i> , <i>DC=HQ</i> , <i>DC=com</i> , <i>DC=All Users</i> ,
绑定 DN	允许搜索目录的用户。例如： <i>username@companyname.com</i> 或 <i>username@domainname.com</i> 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	名称
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	电话号码
角色	标题
国家 / 地区	CO
状态	状态

部门	部门
照片	ThumbnailPhoto.
ManagerDN	管理器
组	成员

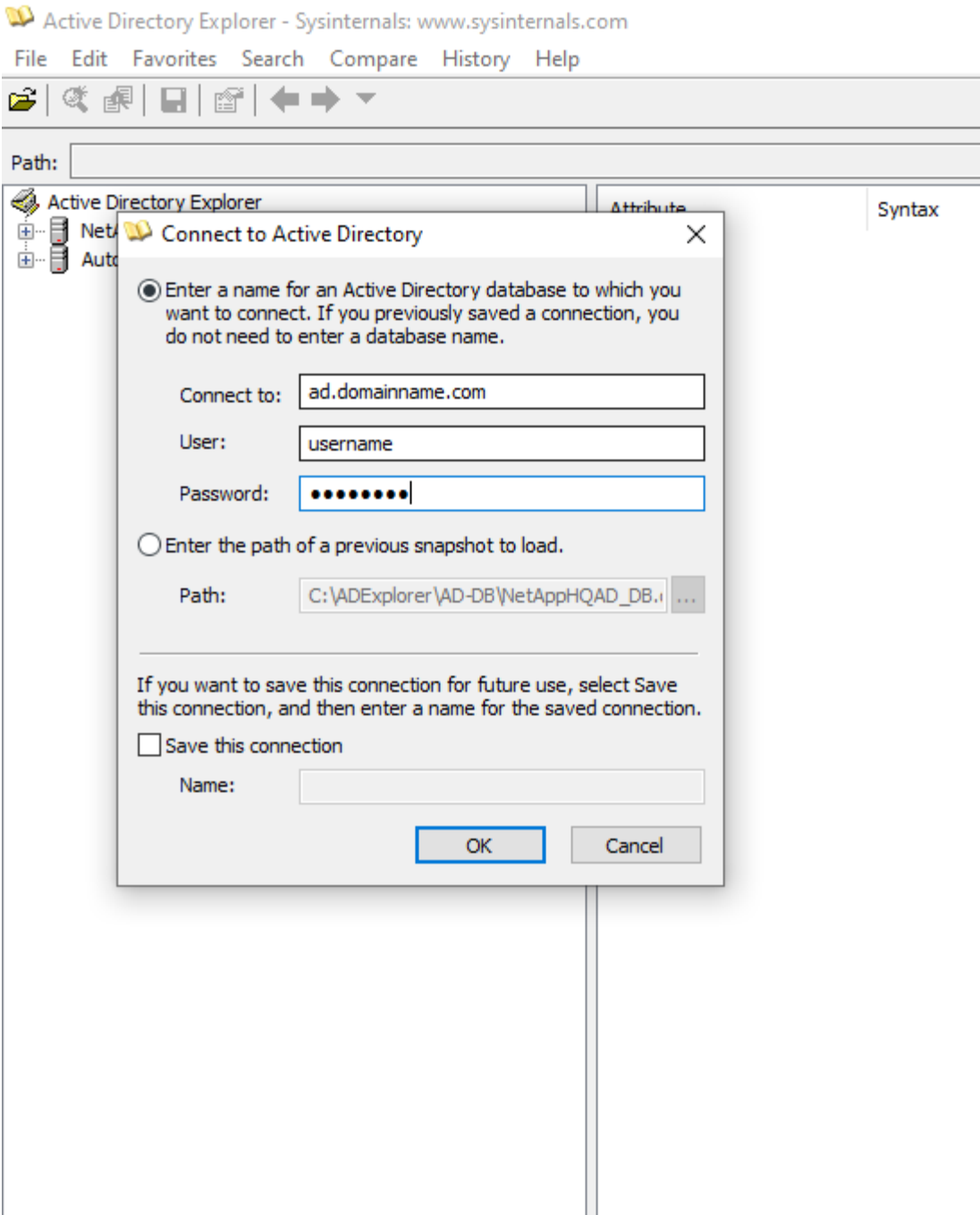
测试用户目录收集器配置

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 -ll -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](#)" 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.ldap-port has type string rather than 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。
用户数据将从 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. 编辑从 Active Directory 提取用户信息的特定 Active Directory 收集器。请注意，在可选属性下，字段名称 " 电话号码 " 映射到 Active Directory 属性 '电话号码'。4. 现在，请使用上述 Active Directory 资源管理器工具浏览 Active Directory 并查看正确的属性名称。3. 确保在 Active Directory 中有一个名为 'telphonenumber' 的属性，该属性确实包含用户的电话号码。5. 我们可以说，在 Active Directory 中，它已修改为 'phonenumber'。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 收集器后，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电话号码。
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

- 要执行此任务，您必须是 Cloud Insights 管理员或帐户所有者。
- 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Workload Security菜单中、单击：
收集器>用户目录收集器>+用户目录收集器*并选择*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：UID=LDAPUser , CN=Users , CN=accounts , dc=domain , dc=CompanyName , dc=com uid=john , cn=users , cn=accounts , dc=drep , dc=company、dc=com 。 john@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	名称
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	状态
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

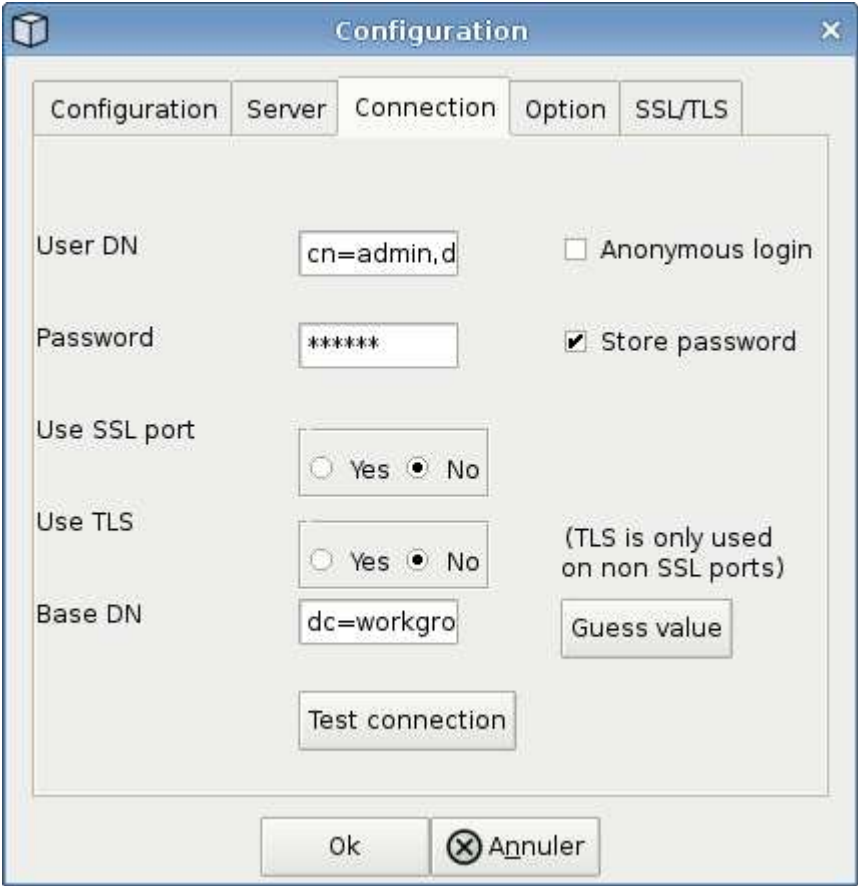
您可以使用以下过程验证 LDAP 用户权限和属性定义：

- 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。

- 安装 LDAP 资源管理器 或 Java LDAP 资源管理器 可连接到 LDAP 服务器的任何 Windows 计算机上。
- 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 <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.ldapport has type string rather than 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。
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。

问题：	解决方法：
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. 编辑从 Active Directory 提取用户信息的特定 Active Directory 收集器。请注意，在可选属性下，字段名称 " 电话号码 " 映射到 Active Directory 属性 '电话号码'。4. 现在，请使用上述 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 LDAP 目录中有一个名为 'telphonenumber' 的属性，该属性确实包含用户的电话号码。5. '在 LDAP 目录中将其修改为 "phonenummer"。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 'phonenummer'。7. 保存 Active Directory 收集器后，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电话号码。
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 协议 4.0 及更早版本
 - 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_defaultsinc_sourcesync_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）。
- 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管理员集群 /SVM 管理用户名和密码，则可以创建一个权限较低的自定义用户，如中所述 ["关于权限的注释"](#) 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          Authentication          Acct   Second
Name               Application Method      Role Name Locked Authentication
-----
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。clustershell::
: > ssecurity 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::: > ssecurity 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。clustershell::: > 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。

请参见 ["代理要求"](#) 有关配置信息，请参见。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

请记住以下内容 ["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
```

ONTAP ARP集成的权限：

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

ONTAP访问权限被拒绝：

```
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
```

注意：如果已添加一个REST角色--*arwrole_*或*_csrestrole*--则无需再添加另一个REST角色。您只需按照以下示例添加API权限即可。

示例：_csrestrole_已存在、因此我们只需启用反勒索软件保护并为现有_csrestrole_授予API权限：

```
security login rest-role create -role csrestrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
```

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 <vservname> 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>
```

ONTAP访问权限被拒绝:

```
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自主防兰软件保护的权限

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。

对于具有集群凭据的_CSUser_、请从ONTAP 命令行执行以下操作：

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

有关详细信息、请阅读 ["与ONTAP 自主勒索软件保护相集成"](#)

ONTAP访问权限被拒绝

如果使用集群管理凭据添加Data Collector、则无需新权限。

如果使用自定义用户(例如、-CsUser_)添加收集器并授予该用户权限、请按照以下步骤为工作负载安全性授予向ONTAP注册"拒绝访问"事件所需的权限。

对于具有_cluster- 凭据的CsUser、从ONTAP命令行执行以下命令。请注意、_csrestrolle_是自定义角色、而-CsUser_是ONTAP自定义用户。

```
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
```

对于凭据为_svm_的CsUser、从ONTAP命令行执行以下命令：

```
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>
```

有关详细信息、请阅读 ["与ONTAP集成访问被拒绝"](#)

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 Cloud Insights 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 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。

建议的Metro Cluster配置

对于Metro Cluster、建议使用以下配置：

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

如果要使用ONTAP 9.1.1版中的服务策略连接到数据源收集器、则需要_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、也不会从该数据收集器流向Cloud Insights。

请注意、如果在收集器暂停时在ONTAP上创建了新卷等、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、Cloud Insights工作负载安全性将无法获取该事件。
- 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。

故障排除

下表介绍了已知问题及其解决方法。

如果出现错误，请单击 *Status* 列中的 *More detail* 以了解有关该错误的详细信息。

Installed Data Collectors

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

问题：	解决方法：
Data Collector 会运行一段时间，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。 "	ONTAP 中的事件速率远远高于 Agent Box 可以处理的事件速率。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。如果此代理安装在 2021 年 3 月 4 日之前的 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 在调整收集器大小后重新启动系统。

问题：	解决方法：
<p>收集器报告错误消息： " 在可访问 SVM 数据接口的连接器上未找到本地 IP 地址 "。</p>	<p>这很可能是由于 ONTAP 端存在网络问题描述。请按照以下步骤操作：</p> <ol style="list-style-type: none"> 1.确保SVM数据If或管理If上没有阻止与SVM连接的防火墙。 2. 在通过集群管理 IP 添加 SVM 时，请确保 SVM 的数据 LIF 和管理 LIF 可从 Agent VM 执行 Ping 操作。如果出现问题，请检查网关，网络掩码和 LIF 路由。 <p>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：</p> <pre>network ping -vserver <vserver name>-Destination <Agent IP>-If <Lif Name>-show-DEBIL</pre> <p>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。</p> <ol style="list-style-type: none"> 3. 如果您尝试通过集群 IP 进行连接，但此连接无法正常工作，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. 如果此 LIF 仍不起作用，请创建一个新的 SVM LIF 并尝试通过此 LIF 进行连接。确保子网掩码设置正确。 6.高级调试： <ol style="list-style-type: none"> 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)等待直至出现错误。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 <pre>\https: <cluster_mgmt_ip> : //SPI/SPI/packet/etc/log/packet_traces/<clustername></pre> <ol style="list-style-type: none"> e)确保有一个从ONTAP到代理框的“SNT”。 F)如果没有来自ONTAP的问题描述，则它是中带有防火墙的ONTAP。 g)在ONTAP中打开防火墙，以便ONTAP能够连接代理盒。 7. 如果此功能仍不起作用，请咨询网络团队，以确保没有外部防火墙阻止从 ONTAP 到代理框的连接。 8.确认端口7已打开。

问题：	解决方法：
消息： Failed to determine ONTAP type for [hostname : <IP Address >] 。原因：与存储系统<IP 地址>的连接错误：主机不可访问（主机不可访问）	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 连接到要连接的 SVM 或集群。连接后，请确保 SVM 或集群名称正确无误。
错误消息："Connector is in error state.service.name：审核。失败原因：外部 fpolicy 服务器已终止。"	1. 防火墙很可能会阻止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，并确保端口范围处于打开状态。 <code>_sudo iptables-save</code>
<p><code>grep 3500* _</code> 示例输出应如下所示：<i>A in_public_allow -p tcp -m tcp -dport 35000 -m conntrack -ctstate new -j accept</i> 3. 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。<i>system services firewall show system services firewall policy show</i> "检查防火墙命令" 在 ONTAP 端。4. 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，NFS 协议），并确保 ping 操作正常：<code>_network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail</code> 如果无法执行 Ping 操作，请确保 ONTAP 中的网络设置正确，以便代理计算机可以执行 Ping 操作。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。6. 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 将始终成功。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。7. 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。</p>	活动页面中未显示任何事件。
<p>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. 如果未看到任何活动，请登录到 SVM 并输入以下命令。<code><svm> event log show -source fpolicy</code> 请确保没有与 fpolicy 相关的错误。3. 如果未看到任何活动，请登录到 SVM。输入以下命令 <code><svm> fpolicy show</code> 检查是否已设置以前缀 "cloudsecure _" 命名的 fpolicy 策略且状态为 "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。</p>	SVM Data Collector 处于错误状态，错误消息为 "Agent failed to connect to the collector"

问题：	解决方法：
1. 代理很可能已过载，无法连接到数据源收集器。2. 检查连接到代理的数据源收集器数量。3. 另请在用户界面的 "所有活动" 页面中查看数据流速。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代理。	SVM Data Collector 显示错误消息，显示为 "fpolicy.server.connectError: Node failed to establish a connection with the FPolicy server "12.195.15.146" (reason : "select Timed Out") "
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 CLI 包括： event log show -source fpolicy ，其中显示错误事件日志 show -source fpolicy -fields event ， action ， description ，其中显示了更多详细信息。" 检查防火墙命令 " 在 ONTAP 端。	错误消息： "Connector is in error state.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）。 "
确保有一个可操作的接口（充当 CIFS/NFS 的数据和数据协议角色）。	数据收集器将进入 " 错误 " 状态，一段时间后进入 " 正在运行 " 状态，然后再次返回 " 错误 " 。此周期将重复。
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。	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-modify : "Federal " 中的 "share-to include" 元素指定的值无效
共享名称必须在不带任何引号的情况下提供。编辑 ONTAP SVM DSC 配置以更正共享名称。 <i>include</i> 和 <i>exclude shares</i> 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。	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？
建议删除所有现有未使用的 fpolicy 设置，即使它们处于已断开连接状态也是如此。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 CLI 命令： <i>fpolicy show-steps to delete fpolicy configurations :</i> <i>_fpolicy disable -vserver <svmname> -policy-name <policy_name> _fpolicy policy policy scope delete -vserver <svmname> -policy-name <policy_name> _fpolicy policy policy policy delete -vserver <svmname> -policy -policy -engine -<policy_name> -policy -<vmname> -node -engine -<policy_name> -policy_name -vserver -vserver -policy> <policy_name> -vpolicy -policy -engine -<vm> <policy_name> -node -policy_name> -vpolicy -engine -vpolicy -<policy_name> -vpolicy</i>	启用工作负载安全性后、ONTAP 性能将受到影响：延迟偶尔会高、IOPS偶尔会低。
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。	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。 "

问题：	解决方法：
从仅配置 NFS 服务的新 SVM 开始。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。请等待、直到工作负载安全性中的数据收集器显示错误。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。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。	Data Collector 显示错误消息：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）。

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 Cloud Insights 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。此时将安装工作负载安全代理、并提供所有 "代理前提条件" 已满足。

有关详细步骤，请参见以下链接：https://docs.netapp.com/us-en/cloudinsights/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

工作负载安全性用户帐户通过Cloud Insights 进行管理。

Cloud Insights 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 Cloud Insights 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 Cloud Insights ["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
请参见 xref:{relative_path}concept_cs_agent_requirements.html["代理要求"]
第页、了解其他前提条件和要求。
```

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？	是的。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？	否即使 SVM 数量增加，该脚本也将最多运行 5 分钟。
是否可以增加可运行此脚本的SVM数量？	是的。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？	否即使 SVM 数量增加，该脚本也将最多运行 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。

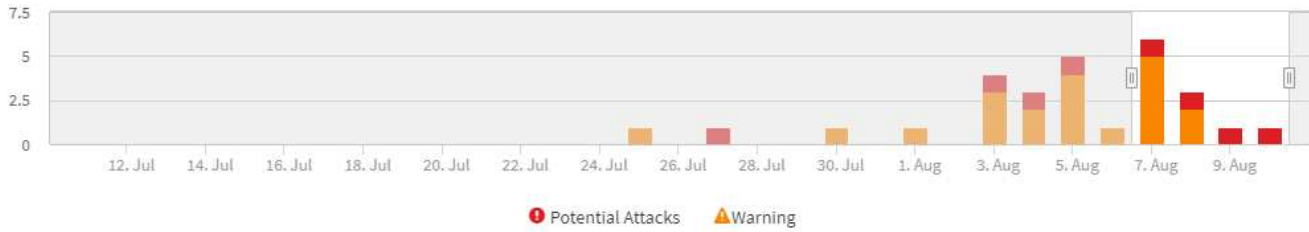
警报

"工作负载安全警报"页面显示了近期攻击和/或警告的时间线、并可用于查看每个问题描述的详细信息。



Cloud Insights 联邦版不提供工作负载安全性。

Filter By Status New



Potential Attacks (3)

Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
Ransomware Attack	5 hours ago Aug 10, 2020 4:38 AM	New	Iris McIntosh	> 700 Files Encrypted	Snapshots Taken
Ransomware Attack	a day ago Aug 9, 2020 3:51 AM	New	Christy Santos	> 500 Files Encrypted	Snapshots Taken
Ransomware Attack	2 days ago Aug 8, 2020 4:29 AM	New	Safwan Langley	> 700 Files Encrypted	Snapshots Taken

Warnings (7)

Abnormal Behaviour	Detected ↓	Status	User	Change	Action Taken
User Activity Rate	2 days ago Aug 8, 2020 7:49 PM	New	Iris McIntosh	↑ 192.46%	None
User Activity Rate	2 days ago Aug 8, 2020 7:32 PM	New	Jenny Bryan	↑ 73.64%	None
User Activity Rate	3 days ago Aug 7, 2020 8:07 PM	New	Szymon Owen	↑ 189.88%	None

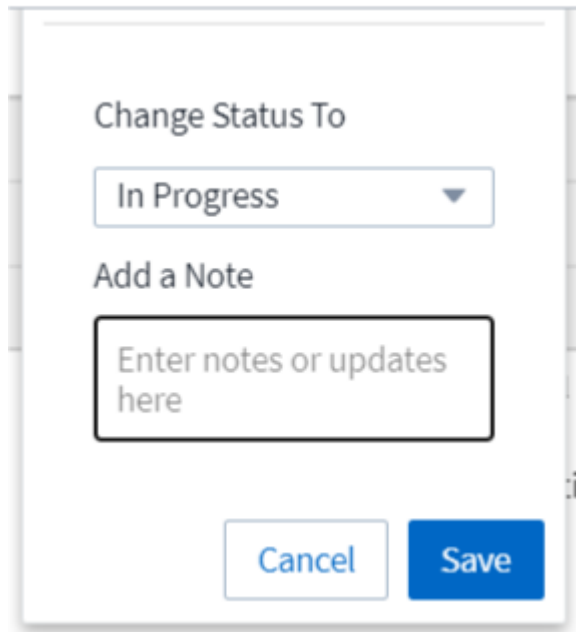
警报

警报列表显示一个图形，其中显示了选定时间范围内引发的潜在攻击和 / 或警告总数，然后列出了该时间范围内发生的攻击和 / 或警告。您可以通过调整图中的开始时间和结束时间滑块来更改时间范围。

对于每个警报，将显示以下内容：

- 潜在攻击： *
- 潜在攻击类型（例如勒索软件或破坏）
- 检测到潜在攻击的日期和时间
- 警报的 *Status* ：
 - * 新增 *：这是新警报的默认设置。
 - * 进行中 *：某个或多个团队成员正在调查此警报。
 - * 已解决 *：警报已被团队成员标记为已解决。
 - * 已取消 *：已将警报视为误报或预期行为而解除。

管理员可以更改警报状态并添加注释以协助调查。



- 其行为触发警报的 *User*
- 攻击的 *Event* （例如，大量文件已加密）
- 已执行操作 _ （例如，已创建快照）
- 警告： *
- 触发警告的 _Abnormal behavior _
- 检测到行为的日期和时间
- 警报的 *Status* （新建，正在进行等）
- 其行为触发警报的 *User*
- *Change* 的问题描述（例如，文件访问异常增加）
- 已采取操作 _

筛选器选项

您可以按以下方式筛选警报：

- 警报的 *Status*
- *Note* 中的特定文本
- _ 攻击 / 警告 _ 的类型
- 操作触发警报 / 警告的 *User*

警报详细信息页面

您可以单击警报列表页面上的警报链接以打开警报的详细信息页面。警报详细信息可能因攻击或警报类型而异。例如，勒索软件攻击详细信息页面可能会显示以下信息：

摘要部分：

- 攻击类型(勒索软件、破坏)和警报ID (由工作负载安全性分配)
- 检测到攻击的日期和时间
- 已执行操作（例如，已创建自动快照。Snapshot 时间显示在摘要部分的正下方）
- 状态（新增，正在进行等）

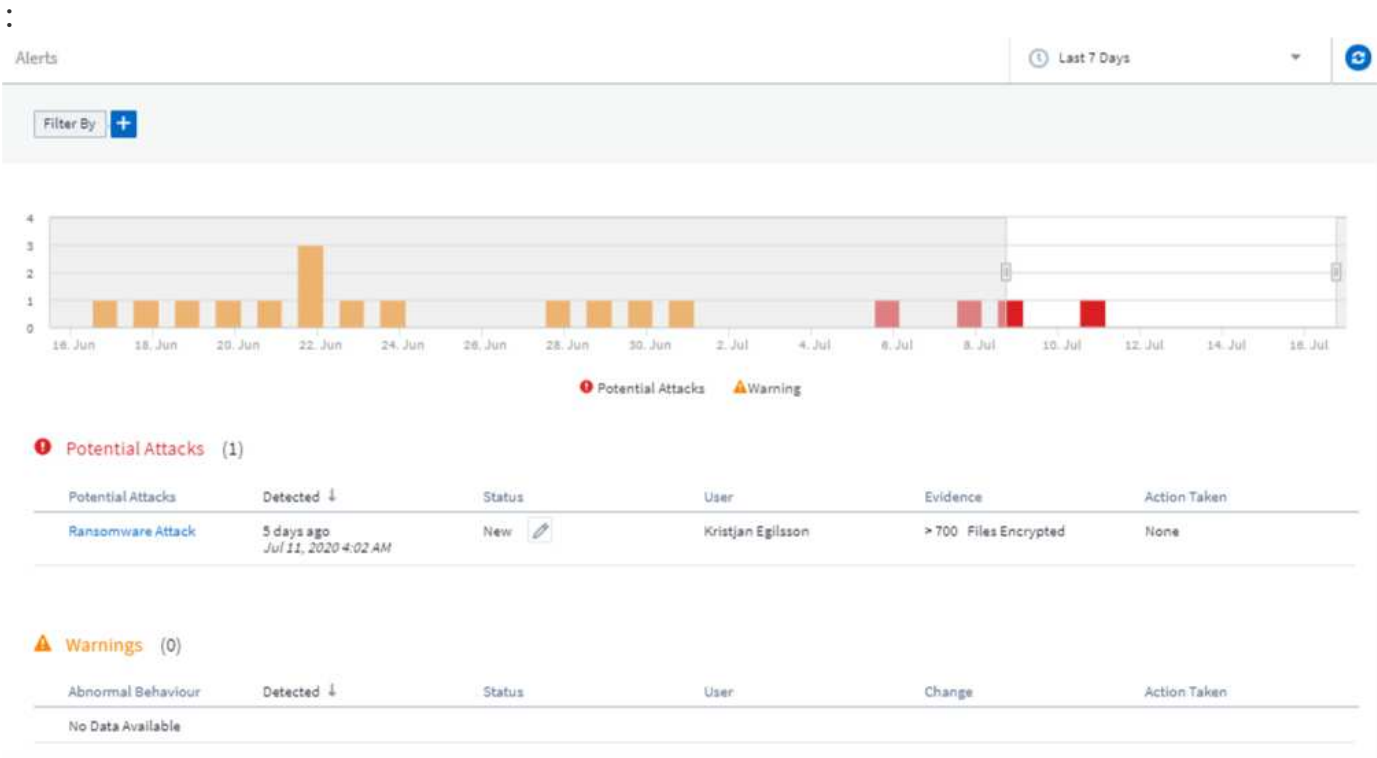
攻击结果部分：

- 受影响卷和文件的数量
- 随附的检测摘要
- 显示攻击期间文件活动的图形

相关用户部分：

此部分显示有关参与潜在攻击的用户的详细信息，包括用户的 "Top Activity" 图形。

警报页面（此示例显示了潜在的勒索软件攻击）



详细信息页面（此示例显示了潜在的勒索软件攻击）

：



POTENTIAL ATTACK: AL_305
Ransomware Attack

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None

Status
New

Total Attack Results

Affected Volumes	Deleted Files	Encrypted Files
1	0	4173

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Kristjan Egilsson
Accountant
Finance

4173
Encrypted Files

Detected
5 days ago
Jul 11, 2020 4:02 AM

Action Taken
None



Username
us035

Email
Egilsson@netapp.com

Phone
387224312607

Department
Finance

Manager
Lyndsey Maddox

Top Activity Types

Activity per minute
Last access location: 10.197.144.115

[View Activity Detail](#)



执行Snapshot_操作

工作负载安全性可通过在检测到恶意活动时自动创建快照来保护您的数据、并确保安全地备份您的数据。

您可以定义 "自动响应策略" 在检测到勒索软件攻击或其他异常用户活动时创建快照。您也可以从警报页面手动创建快照。

自动创建快照
:



POTENTIAL ATTACK: AL_307
Ransomware Attack

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken

Status
In Progress

Last snapshots taken by
Amit Schwartz
Jul 30, 2020 2:54 PM

How To:
[Restore Entities](#)

[Re-Take Snapshots](#)

Total Attack Results

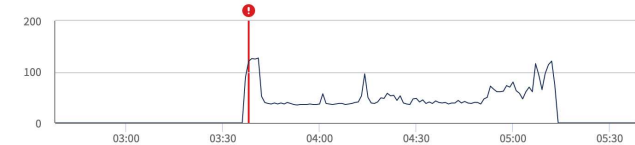
1 Affected Volumes | 0 Deleted Files | 5148 Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.
The extension "crypt" was added to each file.

Encrypted Files

Activity per minute



Related Users



Ewen Hall
Developer
Engineering

5148
Encrypted Files

Detected
4 days ago
Jul 26, 2020 3:38 AM

Action Taken
Snapshots Taken



手动快照

Cloud Insights

Abhi Basu Thakur

MONITOR & OPTIMIZE Alerts / Nabilah Howell had an abnormal change in activity rate

Jul 23, 2020 - Jul 26, 2020
1:44 AM 1:44 AM

Alert Detail

WARNING: AL_306
Nabilah Howell had an abnormal change in activity rate.

Detected
5 days ago
Jul 25, 2020 1:44 PM

Action Taken
None

Status
New

Recommendation: Setup an Automated Response Policy
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots

How To:
Restore Entities

Nabilah Howell's Activity Rate Change

Typical	Alert	
122.8	210	↑ 71%
Activities Per Minute	Activities Per Minute	

Nabilah Howell's activity rate grew 71% over their typical average.

Activity Rate
Activity per 5 minutes

警报通知

警报的电子邮件通知会发送到警报的每个操作的警报收件人列表。要配置警报收件人，请单击 * 管理员 > 通知 * 并为每个收件人输入一个电子邮件地址。

保留策略

警报和警告保留 13 个月。超过 13 个月的警报和警告将被删除。如果删除了工作负载安全环境、则与该环境关

联的所有数据也将被删除。

故障排除

问题：	请尝试以下操作：
有时，ONTAP 每天每小时创建一次快照。工作负载安全(WS)快照是否会影响它？WS快照是否采用每小时快照的位置？默认每小时快照是否会停止？	工作负载安全快照不会影响每小时快照。WS快照不会占用每小时的快照空间、应像以前一样继续。默认的每小时快照不会停止。
如果在ONTAP中达到最大快照数，会发生什么情况？	如果达到最大Snapshot计数、则后续的Snapshot生成将失败、而工作负载安全性将显示一条错误消息、指出Snapshot已满。用户需要定义Snapshot策略以删除最早的快照，否则不会创建快照。在ONTAP 9.3及更早版本中，一个卷最多可包含255个Snapshot副本。在ONTAP 9.4及更高版本中，一个卷最多可以包含1023个Snapshot副本。有关的信息，请参见ONTAP文档 "正在设置Snapshot删除策略" 。
工作负载安全性根本无法创建快照。	确保用于创建快照的角色具有链接：已分配 proper 权限 。确保为csrole创建了用于创建快照的正确访问权限： security login role create -vserver <vservname> -role csrole -cmddirname "volume snapshot" -access all
对于SVM上较早的警报、快照失败、这些警报已从工作负载安全性中删除并随后重新添加。对于在重新添加SVM后出现的新警报，将创建快照。	这种情况极少。如果您遇到这种情况，请登录到ONTAP并为较早的警报手动创建快照。
在Alert Details页面中，在Take Snapshot按钮下方会显示消息"Last Attempt Failed" 错误。将鼠标悬停在错误上会显示"invoke API command has timed out for the data collector with id"。	如果通过SVM管理IP将数据收集器添加到工作负载安全性中、则在ONTAP中SVM的LIF处于_disabled_状态时、可能会发生这种情况。在ONTAP中启用特定LIF并从工作负载安全性中触发_Take Snapshot Manually_。然后，Snapshot操作将成功。

取证

取证—所有活动

所有活动页面可帮助您了解对工作负载安全环境中的实体执行的操作。

检查所有活动数据


单击 * 取证 > 活动取证 *，然后单击 * 所有活动 * 选项卡以访问所有活动页面。此页面概述了您环境中的活动，并重点介绍了以下信息：

- 显示 *Activity History*（根据选定全局时间范围，每分钟 / 每 5 分钟 / 每 10 分钟访问一次）的图形

您可以通过在图形中拖动一个方框来缩放图形。此时将加载整个页面以显示缩放的时间范围。放大后，将显示一个按钮，用户可以通过该按钮进行缩小。

- 活动类型图表。要按活动类型获取活动历史记录数据，请单击相应的 x 轴标签链接。
- 实体类型_上的活动图表。要按实体类型获取活动历史记录数据，请单击相应的 x 轴标签链接。

- 所有活动数据的列表

_ * 所有活动 * _ 表显示了以下信息。请注意，默认情况下并不会显示所有这些列。您可以单击齿轮图标来选择要显示的列 。

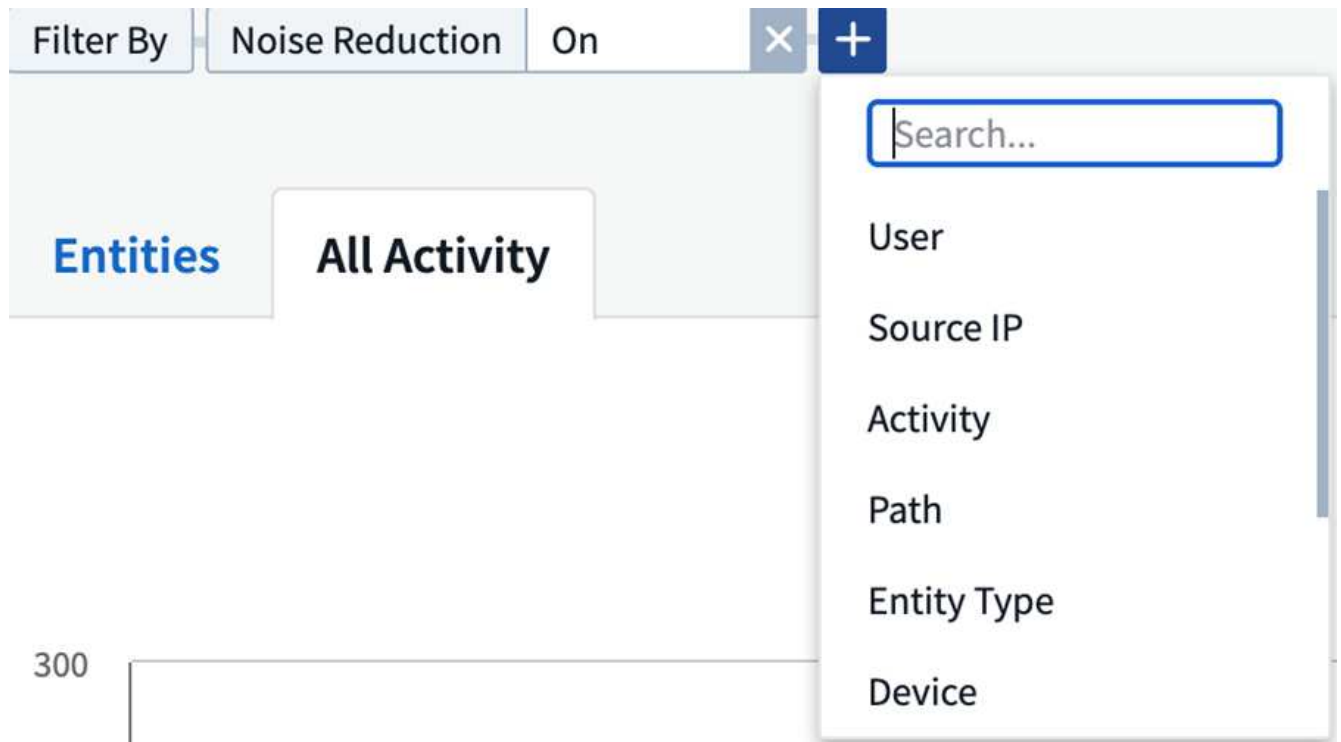
- 访问实体的 * 时间 *，包括上次访问的年份，月份，日期和时间。
- 通过指向的链接访问实体的 * 用户 * "[用户信息](#)"。
- 用户执行的 * 活动 *。支持的类型包括：
 - * 更改组所有权 * - 文件或文件夹的组所有权已更改。有关组所有权的详细信息，请参见 "[此链接](#)。"
 - * 更改所有者 * —文件或文件夹的所有权已更改为其他用户。
 - * 更改权限 * - 文件或文件夹权限已更改。
 - * 创建 * - 创建文件或文件夹。
 - * 删除 * - 删除文件或文件夹。如果删除某个文件夹，则会为该文件夹和子文件夹中的所有文件获取 *delete* 事件。
 - * 读取 * - 文件已读取。
 - * 读取元数据 * - 仅在启用文件夹监控选项时才显示。将在 Windows 上打开文件夹或在 Linux 中的文件夹内运行 "ls" 时生成。
 - * 重命名 * - 重命名文件或文件夹。
 - * 写入 * - 将数据写入文件。
 - * 写入元数据 * - 写入文件元数据，例如，权限已更改。
 - * 其他更改 * —上述未提及的任何其他事件。所有未映射的事件都会映射到 "其他更改" 活动类型。适用于文件和文件夹。
- 指向实体的 * 路径 *，并带有指向的链接 "[实体详细信息数据](#)"
- 实体类型 *，包括实体（即文件）扩展名（.doc，.docx，.tmp 等）
- 实体所在的 * 设备 *
- 用于提取事件的 * 协议 *。
- 重命名原始文件时用于重命名事件的 * 原始路径 *。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。
- 实体所在的 * 卷 *。默认情况下，此列在表中不可见。使用列选择器将此列添加到表中。

筛选取证活动历史记录数据

您可以使用两种方法筛选数据。

1. 将鼠标悬停在表中的字段上，然后单击显示的筛选器图标。该值将添加到 Top _Filter by" 列表中的相应筛选器中。
2. 通过在 _Filter by" 字段中键入来筛选数据：

通过单击 * +] * 按钮从顶部的 Filter by ' 小工具中选择相应的筛选器：



输入搜索文本

按 Enter 或单击筛选器框外侧以应用筛选器。

您可以按以下字段筛选取证活动数据：

- * 活动 * 类型。
- 访问实体的 * 源 IP*。您必须使用双引号提供有效的源 IP 地址，例如 "10.1.1.1."。诸如 "10.1.*"，"10.1.*。*" 等不完整的 IP 将不起作用。
- 提取协议专用活动的 * 协议 *。
- 执行活动的用户的 * 用户名 *。您需要提供确切的用户名以进行筛选。使用部分用户名或部分用户名预先设置或后缀为 '*' 的搜索将不起作用。
- * 降噪 * 用于筛选用户在过去 2 小时内创建的文件。它还用于筛选用户访问的临时文件（例如 .tmp 文件）。

以下字段受特殊筛选规则的约束：

- * 实体类型 *，使用实体（文件）扩展名
- 实体的 * 路径 *
- * 用户 * 正在执行活动
- 实体所在的 * 设备 *（SVM）
- 实体所在的 * 卷 *
- 重命名原始文件时用于重命名事件的 * 原始路径 *。

筛选时，上述字段受以下限制：

- 确切值应在引号内：示例："searchText"

- 通配符字符串不能包含任何引号：例如： `searchText` ， `* searchText*` 将筛选包含 'searchtext' 的任何字符串。
- 带有前缀的字符串示例： `searchText*` 将搜索以 'searchtext' 开头的任何字符串。

对取证活动历史记录数据进行排序

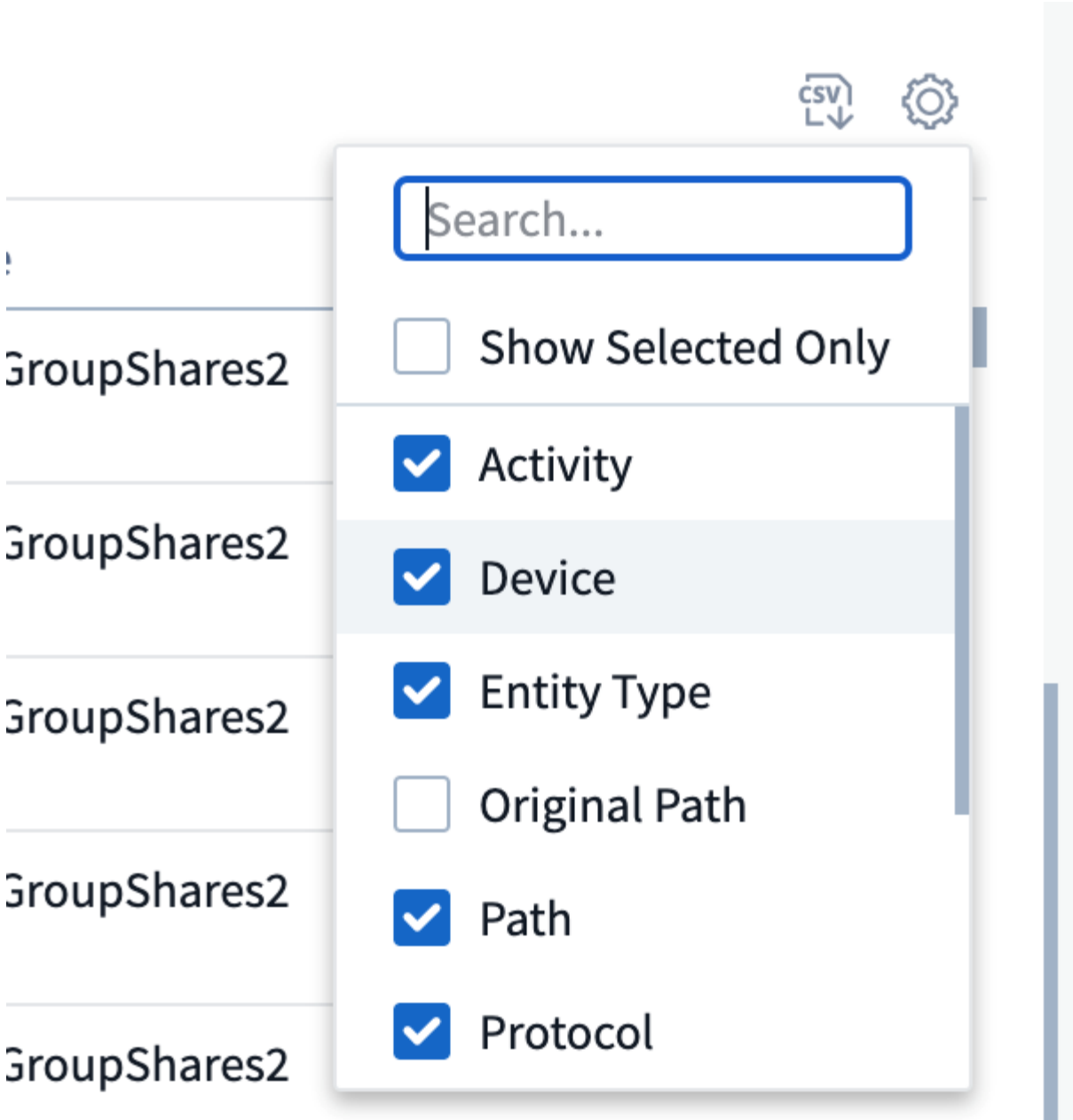
您可以按 *time* ， 用户， 源 *IP* ， 活动， 路径 *_* 和 *_Entity Type* 对活动历史记录数据进行排序。默认情况下，此表按降序 *time* 顺序排序，这意味着将首先显示最新数据。已对 *Device* 和 *Protocol* 字段禁用排序。

导出所有活动

您可以单击 "Activity History" 表上方的 *Export* 按钮将活动历史记录导出到 .CSV 文件。请注意、仅导出排名前10万位的记录。根据数据量的不同、导出可能需要几秒钟到几分钟才能完成。

为所有活动选择列

默认情况下， *all activity* 表会显示 *SELECT* 列。要添加，删除或更改列，请单击表右侧的齿轮图标，然后从可用列列表中进行选择。



活动历史记录保留

对于活动工作负载安全环境、活动历史记录保留13个月。

取证页面中的筛选器适用性

筛选器	功能	示例	适用于哪些筛选器？	不适用于哪些筛选器	结果
（星号）	用于搜索所有内容	Auto 03172022	用户、路径、实体类型、设备类型、卷、原始路径		返回以"Auto"开头、以"03172022 "结尾的所有资源

？（问号）	用于搜索特定数量的字符	AutoSabotageUser1_03172022?	用户、实体类型、设备、卷		返回AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022AB、AutoSabotageUser1_031720225等
或	用于指定多个实体	AutoSabotageUser1_03172022或AutoRansomUser4_03162022	用户、域、用户名、路径、实体类型、设备、原始路径		返回任意AutoSabotageUser1_03172022或AutoRansomUser4_03162022
不是	用于从搜索结果中排除文本	非AutoRansomUser4_03162022	用户、域、用户名、路径、实体类型、原始路径、卷	设备	返回不以"AutoRansomUser4_03162022"开头的所有内容
无	在所有字段中搜索空值	无	domain		返回目标字段为空的结果

路径/原始路径搜索

使用和不使用/的搜索结果将有所不同

/AutoDir1/AutoFile	工作正常
AutoDir1/AutoFile	不起作用
/AutoDir1/AutoFile (Dir1)	dir1部分子字符串不起作用
"/AutoDir1/AutoFile03242022"	精确搜索有效
Auto* 03242022	不起作用
AutoSabotageUser1_03172022?	不起作用
/AutoDir1/AutoFile03242022 或/AutoDir1/AutoFile03242022	工作正常
非/AutoDir1/AutoFile03242022	工作正常
非/AutoDir1	工作正常
非/AutoFile03242022	不起作用
*	显示所有条目

故障排除

问题	请尝试此操作
----	--------

在 "All actives" 表的 'User' 列下，用户名显示为： "ldap： HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" 或 "ldap： default： 80038003"	可能的原因包括： 1.尚未配置任何用户目录收集器。要添加一个，请转到*工作负载安全性>收集器>用户目录收集器*，然后单击*+用户目录收集器*。选择 <i>Active Directory</i> 或 <i>LDAP Directory Server</i> 。 2. 已配置用户目录收集器，但它已停止或处于错误状态。请进入*收集器>用户目录收集器*并检查状态。请参见 " 用户目录收集器故障排除 " 文档中有关故障排除提示的章节。 正确配置后，此名称将在 24 小时内自动解析。 如果仍无法解决此问题，请检查您是否添加了正确的用户数据收集器。确保用户确实属于添加的 Active Directory/LDAP 目录服务器。
UI 中未显示某些 NFS 事件。	检查以下内容： 1.运行设置了 POSIX 属性的 AD 服务器的用户目录收集器时，应通过 UI 启用 unixid 属性。2. 在 UI 3 的用户页面中搜索时，应看到执行 NFS 访问的任何用户。NFS 4 不支持原始事件（尚未发现用户的事件）。不会监控对 NFS 导出的匿名访问。5. 确保使用的 NFS 版本低于 NFS4.1。
在Forsics_All Activity_或_indices_页面的筛选器中键入包含通配符(如星号(*))的某些字母后、页面加载速度非常慢。	搜索字符串中的星号(*)将搜索所有内容。但是，诸如_*<searchTerm>_或_*<searchTerm>_*之类的前导通配符字符串会导致查询速度较慢。 要获得更好的性能，请改用前缀字符串，格式为<searchTerm>*(换言之，请附加星号(*)_after_搜索词)。 示例：使用字符串_testvolume*，而不是_*testvolume_或_*test*volume_。 使用基于前缀的搜索以递归方式查看给定文件夹下的所有活动(分层搜索)。例如、/path1/path2/path3_或"/path1/path2/path3"将以递归方式列出/path1/path2/path3_下的所有活动。 或者、使用所有活动选项卡下的"Add to Filter"(添加到筛选器)选项。
使用路径筛选器时遇到"Request failed with status code 500/503"错误。	请尝试使用较小的日期范围来筛选记录。

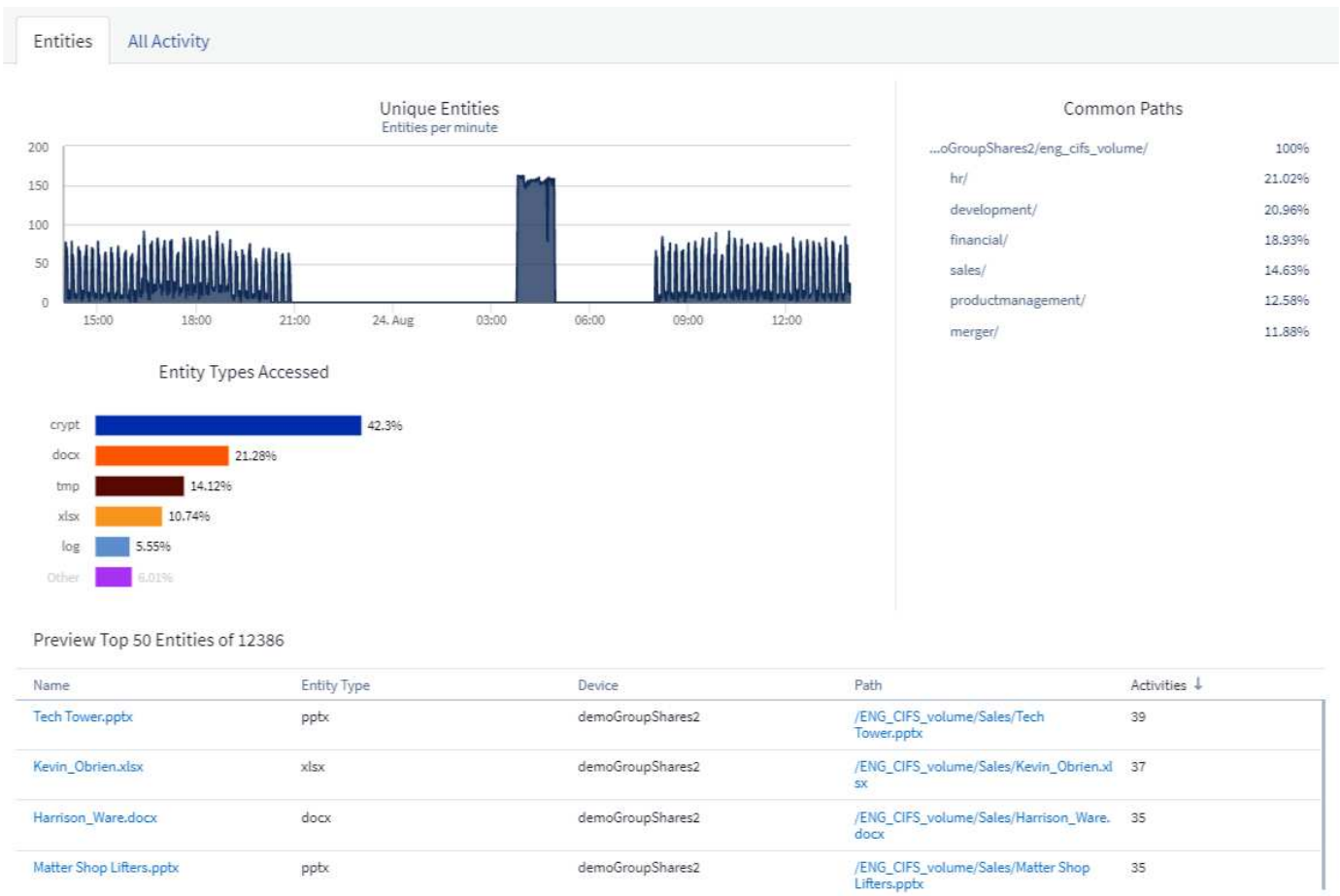
取证实体页面

" 取证实体 " 页面提供了有关环境中实体活动的详细信息。

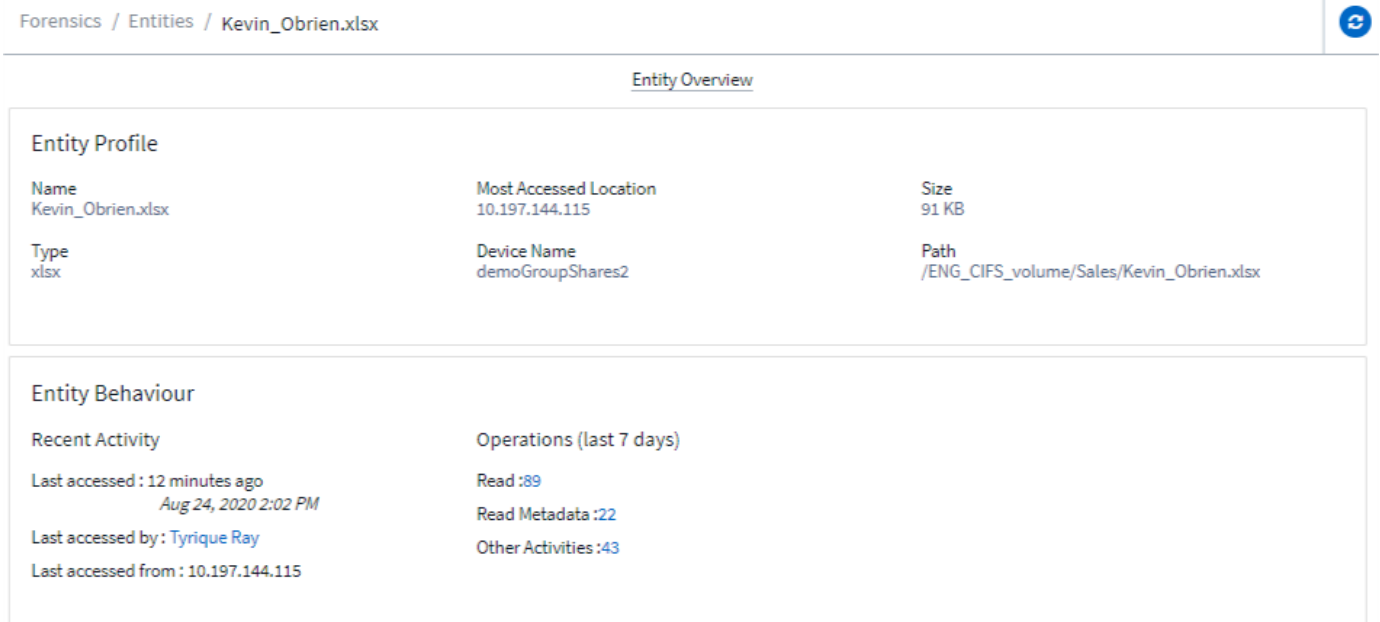
检查实体信息

单击 * 取证 > 活动取证 *，然后单击 *entities* 选项卡以访问实体页面。

此页面简要介绍了环境中的实体活动，并重点介绍了以下信息： * 显示每分钟访问的 *unique entities* 的图形 * 已访问的 _Entity types 的图表 * _ 通用路径 _ 的细分 * 在实体总数中排名前 50 位的实体 _ 的列表



单击列表中的某个实体将打开该实体的概述页面，其中显示了该实体的配置文件，其中包含名称，类型，设备名称，最常访问的位置 IP 和路径等详细信息，以及用户，IP，和上次访问实体的时间。



取证用户概述

用户概述中提供了每个用户的信息。使用这些视图可以了解用户特征，关联实体和近期活动。

用户配置文件

用户配置文件信息包括用户的联系信息和位置。配置文件提供以下信息：

- 用户的名称
- 用户的电子邮件地址
- 用户的经理
- 用户的电话联系人
- 用户的位置

用户行为

用户行为信息用于标识用户最近执行的活动和操作。这些信息包括：

- 近期活动
 - 上次访问位置
 - 活动图
 - 警报
- 过去七天的操作
 - 操作数

刷新间隔

用户列表每 12 小时刷新一次。

保留策略

如果未再次刷新，则用户列表将保留 13 个月。13 个月后，数据将被删除。如果删除了工作负载安全环境，则会删除与该环境关联的所有数据。

自动响应策略

响应策略会触发一些操作，例如在发生攻击或用户行为异常时创建快照或限制用户访问。



Cloud Insights 联邦版不提供工作负载安全性。

您可以在特定设备或所有设备上设置策略。要设置响应策略，请选择*管理>自动响应策略*，然后单击相应的*+Policy*按钮。您可以为攻击或警告创建策略。

Add Attack Policy

Policy Name*

Unique New Policy Name

For Attack Type(s) *

☐ Ransomware Attack

☐ Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

☒ Take Snapshot ?

☐ Block User File Access ?

Time Period

12 hours

Cancel

Save

您必须使用唯一名称保存策略。

要禁用自动响应操作（例如，创建 Snapshot），只需取消选中该操作并保存策略即可。

当针对指定设备（或所有设备，如果已选择）触发警报时，自动响应策略将为您的数据创建快照。您可以在上查看快照状态 ["警报详细信息页面"](#)。

请参见 ["限制用户访问"](#) 第页，了解有关通过 IP 限制用户访问的更多详细信息。

您可以通过在策略的下拉菜单中选择相应选项来修改或暂停自动响应策略。

工作负载安全性将根据Snapshot清除设置每天自动删除一次快照。

Snapshot Purge Settings



Define purge periods to automatically delete snapshots taken by Cloud Secure.

Attack Automated Response

Delete Snapshot after 30 Days ▼

Warning Automated Response

Delete Snapshot after 7 Days ▼

User Created

Delete Snapshot after 30 Days ▼

Cancel

Save

允许的文件类型策略

如果检测到已知文件扩展名的勒索软件攻击、并且在"警报"屏幕上生成警报、则可以将该文件扩展名添加到_允许的文件类型_列表中、以防止发出不必要的警报。

导航到*工作负载安全性>策略*并转到_允许的文件类型策略_选项卡。

[Automated Response Policies](#)

[Allowed File Types Policies](#)

Allowed File Types Policies

Ransomware alerts will not be triggered for the following file types:

.abc ✕ .123 ✕ .*safe ✕ |

添加到_ALLOWED FILE Types_列表后、不会为该允许的文件类型生成任何勒索软件攻击警报。请注意、_Allowed File Types_策略仅适用于勒索软件检测。

例如、如果名为_test.txt的文件重命名为_test.txt. abc_、并且工作负载安全性由于扩展名_.abc_而检测到勒索

软件攻击、则可以将 `_abc_` 扩展名添加到 `_ALLOWED FILE Types_` 列表中。添加到列表后、将不再对扩展名为 `_abc_` 的文件生成勒索软件攻击。

允许的文件类型可以是完全匹配(例如 `".abc"`)或表达式(例如 `".type"`、`".type"` 或 `"type"`)。不支持类型为 `".A*c"`、`".p*f"` 的表达式。

与ONTAP 自主勒索软件保护相集成

ONTAP 自主勒索软件保护(ARP)功能可利用NAS (NFS和SMB)环境中的工作负载分析功能主动检测并警告可能指示勒索软件攻击的异常文件活动。

有关ARP的其他详细信息和许可证要求、请参见 ["此处"](#)。

工作负载安全性可与ONTAP 集成以接收ARP事件、并提供额外的分析和自动响应层。

工作负载安全性从ONTAP 接收ARP事件并执行以下操作：

1. 将卷加密事件与用户活动关联起来、以确定导致损坏的人员。
2. 实施自动响应策略(如果已定义)
3. 提供取证功能：
 - 允许客户执行数据泄露调查。
 - 确定哪些文件受到影响、有助于加快恢复速度并执行数据违规调查。

前提条件

1. 最低ONTAP 版本：9.11.1
2. 已启用ARP的卷。有关启用ARP的详细信息、请参见 ["此处"](#)。必须通过OnCommand 系统管理器启用ARP。工作负载安全性无法启用ARP。
3. 应通过集群IP添加工作负载安全收集器。
4. 要使此功能正常运行、需要集群级别的凭据。换言之、添加SVM时必须使用集群级别的凭据。

需要用户权限

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。

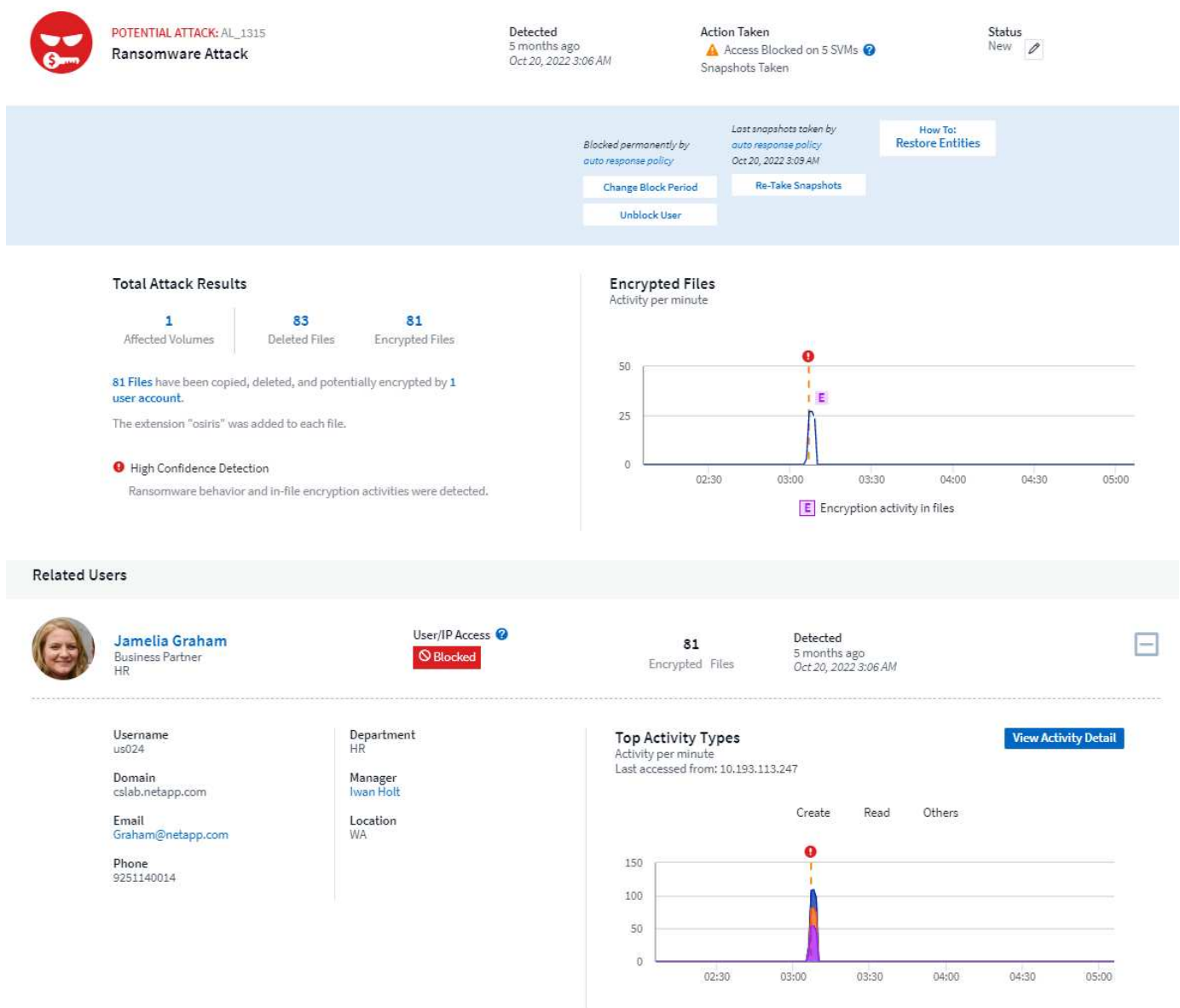
对于具有集群凭据的 `_CSUser_`、请从ONTAP 命令行执行以下操作：




```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

阅读有关配置其他的更多信息 ["ONTAP 权限"](#)。

警报示例

下面显示了因ARP事件生成的警报示例：



Access Limitation History for This User (3)					
Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	 Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	 Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes					
Device ↑	Volume	Encrypted Files	Associated Snapshot Taken		
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM	cloudsecure_attack_auto Automatic _1666249787062	Take Snapshot

高度可信的横幅表示此攻击已显示勒索软件行为以及文件加密活动。加密文件图形指示ARP解决方案 检测到卷加密活动的时间戳。

限制

如果SVM不受工作负载安全性监控、但ONTAP 生成了ARP事件、则工作负载安全性仍会接收和显示这些事件。但是、不会捕获或显示与警报相关的取证信息以及用户映射。

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：
检测到攻击后24小时收到电子邮件警报。在UI中、当Cloud Insights 工作负载安全收到电子邮件时、警报会在24小时之前显示。	当ONTAP 将_勒索 软件检测到_事件发送到Cloud Insights 工作负载安全(即工作负载安全)时、系统会发送电子邮件。事件包含一系列攻击及其时间戳。工作负载安全UI会显示第一个受攻击文件的警报时间戳。对特定数量的文件进行编码后、ONTAP 会将_勒索 软件检测到_事件发送到Cloud Insights。因此、在UI中显示警报的时间与发送电子邮件的时间可能会有所不同。

与ONTAP集成访问被拒绝

ONTAP访问被拒绝功能会在NAS环境(NFS和SMB)中使用工作负载分析来主动检测文件操作失败(即尝试执行其无权限操作的用户)并发出警告。这些失败的文件操作通知(尤其是在出现与安全相关的故障时)将进一步有助于在早期阶段阻止内部攻击。

Cloud Insights工作负载安全性与ONTAP相集成、可接收"拒绝访问"事件、并提供额外的分析和自动响应层。

前提条件

- 最低ONTAP版本： 9.13.0。
- 工作负载安全管理员必须在添加新收集器或编辑现有收集器时启用"访问被拒绝"功能、方法是选中"高级配置"下的_Monitor Access Denied Events_复选框。

需要用户权限

如果使用集群管理凭据添加Data Collector、则无需新权限。

如果使用自定义用户(例如、-CsUser_)添加收集器并授予该用户权限、请按照以下步骤为工作负载安全性授予向ONTAP注册"拒绝访问"事件所需的权限。

对于具有_cluster-凭据的CsUser、从ONTAP命令行执行以下命令。请注意、_csrestrolle_是自定义角色、而-CsUser_是ONTAP自定义用户。

```
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
```

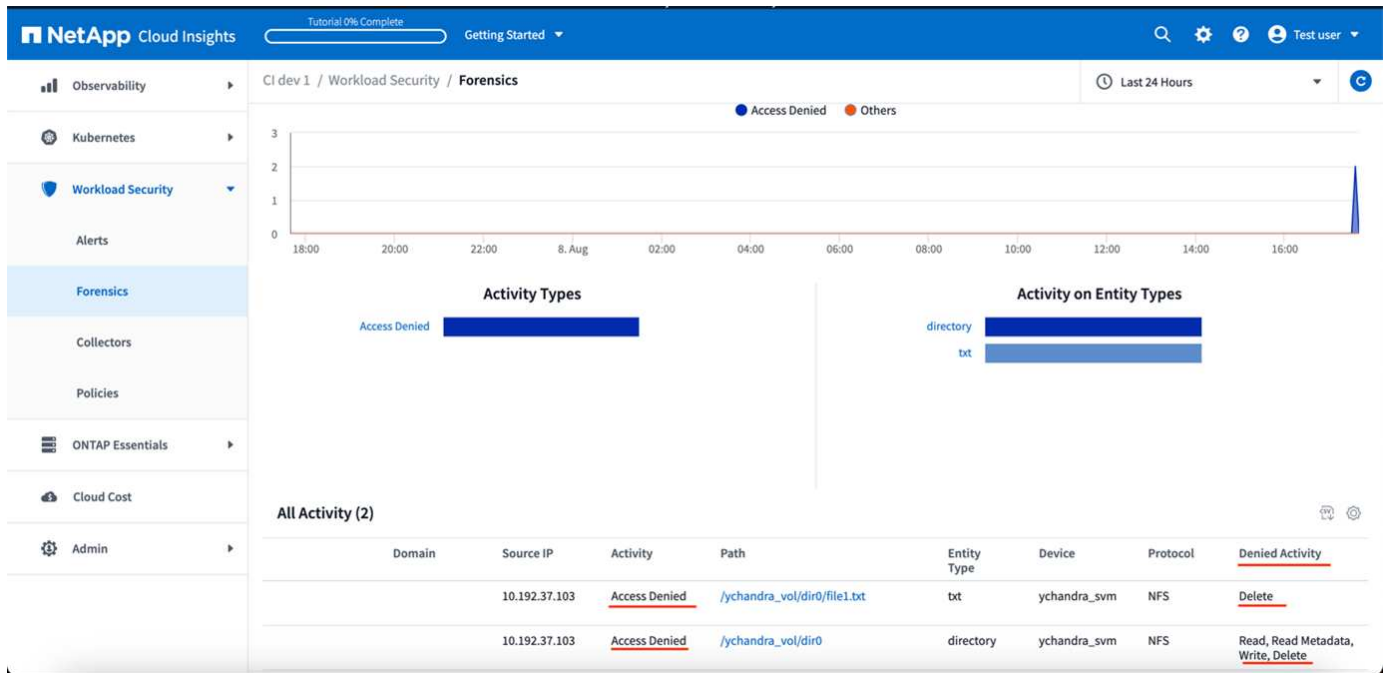
对于凭据为_svm_的CsUser、从ONTAP命令行执行以下命令：

```
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>
```

阅读有关配置其他的更多信息 ["ONTAP 权限"](#)。

拒绝访问事件

从ONTAP系统获取事件后、Workload Security Foreness页面将显示Access Denied Events。除了显示的信息之外、您还可以通过将_Desired Activity_列从齿轮图标添加到表中来看特定操作缺少的用户权限。



正在阻止用户访问

检测到攻击后、工作负载安全性可以通过阻止用户访问文件系统来阻止攻击。可以使用自动响应策略自动阻止访问、也可以从警报或用户详细信息页面手动阻止访问。



Cloud Insights 联邦版不提供工作负载安全性。

在阻止用户访问时、您应定义一个阻止时间段。选定时间段结束后，系统将自动还原用户访问权限。SMB和NFS协议均支持访问阻止。

SMB会直接阻止用户访问、NFS会阻止导致攻击的主机的IP地址。这些计算机IP地址将被阻止访问工作负载安全性监控的任何Storage Virtual Machine (SVM)。

例如、假设工作负载安全性管理10个SVM、并且为其中4个SVM配置了自动响应策略。如果攻击源自四个SVM中的一个、则用户的访问将在所有10个SVM中被阻止。仍会在源 SVM 上创建 Snapshot。

如果有四个SVM、其中一个SVM配置为SMB、一个配置为NFS、其余两个SVM配置为NFS和SMB、则如果攻击源自四个SVM中的任何一个、则所有SVM都将被阻止。

阻止用户访问的前提条件

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
```

请务必查看的权限部分 ["配置 ONTAP SVM 数据收集器"](#) 页面。

如何启用此功能？

- 在工作负载安全性中，导航到*工作负载安全性>策略>自动响应策略*。选择*+攻击策略*。
- 选择(选中)*Block User File Access*。

如何设置自动用户访问阻止？

- 创建新的攻击策略或编辑现有攻击策略。
- 选择应监控攻击策略的 SVM 。
- 单击"阻止用户文件访问"复选框。选择此选项后，此功能将启用。
- 在"时间段"下、选择应用阻止的截止时间。
- 要测试自动用户阻止、您可以通过模拟攻击 ["模拟脚本"](#)。

如何知道系统中是否存在被阻止的用户？

- 在警报列表页面中、如果任何用户被阻止、则屏幕顶部将显示一个横幅。
- 单击此横幅将转到"用户"页面、在此可以看到被阻止的用户列表。
- 在"用户"页面中、有一列名为"用户/IP访问"。在该列中、将显示用户阻止的当前状态。

手动限制和管理用户访问

- 您可以转到警报详细信息或用户详细信息屏幕、然后从这些屏幕手动阻止或还原用户。

用户访问限制历史记录

在警报详细信息和用户详细信息页面的用户面板中、您可以查看对用户访问限制历史记录的审核：时间、操作(阻止、取消阻止)、持续时间、采取的操作、NFS的手动/自动IP以及受影响的IP。

如何禁用此功能？

您可以随时禁用此功能。如果系统中存在受限用户，则必须先还原其访问权限。

- 在工作负载安全性中，导航到*工作负载安全性>策略>自动响应策略*。选择*+攻击策略*。
- 取消选择(取消选中)*Block User File Access*。

此功能将在所有页面中隐藏。

手动还原NFS的IP

如果您的工作负载安全试用版已过期或代理/收集器已关闭、请按照以下步骤手动从ONTAP 还原任何IP。

1. 列出 SVM 上的所有导出策略。

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm1	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm3	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

4 entries were displayed.

2. 通过指定相应的RuleIndex、删除SVM上所有策略中的规则、这些策略将"cloudsure_rule"设置为客户端匹配。工作负载安全规则通常为1。

```
contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

• 确保已删除工作负载安全规则 (确认的可选步骤)。

```

contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>

```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

2 entries were displayed.

手动还原SMB用户

如果您的工作负载安全试用版已过期或代理/收集器已关闭、请按照以下步骤手动从ONTAP 还原任何用户。

您可以从"用户"列表页面获取"工作负载安全性"中阻止的用户列表。

1. 使用cluster_admin_凭据登录到ONTAP 集群(要解除对用户的阻止)。(对于Amazon FSX、使用FSX凭据登录)。
2. 运行以下命令以列出所有SVM中受SMB工作负载安全性阻止的所有用户：

```

vserver name-mapping show -direction win-unix -replacement " "

```

```

Vserver:    <vservename>
Direction: win-unix
Position Hostname          IP Address/Mask
-----
1          -               -               Pattern: CSLAB\\US040
                                     Replacement:
2          -               -               Pattern: CSLAB\\US030
                                     Replacement:
2 entries were displayed.

```

在上述输出中、域CSL阻止了2个用户(US030、US040)。

1. 从上述输出中确定位置后、运行以下命令以解除对用户的阻止：

```

vserver name-mapping delete -direction win-unix -position <position>
. 运行命令以确认用户未被阻止：

```

```
vserver name-mapping show -direction win-unix -replacement " "
```

对于先前已阻止的用户、不应显示任何条目。

故障排除

问题	请尝试此操作
尽管存在攻击，但某些用户并未受到限制。	1. 确保 SVM 的数据收集器和代理处于 <code>_running</code> 状态。如果停止了 Data Collector 和代理、则工作负载安全性将无法发送命令。2. 这是因为用户可能已使用以前未使用的新 IP 从计算机访问存储。限制通过用户访问存储的主机的 IP 地址进行。在 UI（"Alert Details"（警报详细信息）>"Access Limitation History"（此用户的访问限制历史记录）>"Affected IPs"（受影响的 IP））中检查受限 IP 地址列表。如果用户要从 IP 与受限 IP 不同的主机访问存储，则用户仍可通过非受限 IP 访问存储。如果用户尝试从 IP 受限的主机访问，则无法访问存储。
手动单击限制访问会显示 "此用户的 IP 地址已受限制"。	要限制的 IP 已被其他用户限制。
无法修改策略。原因：未获得该命令的授权。	检查是否使用 <code>CsUser</code> 、是否已按上述方式为用户授予权限。
NFS 的用户 (IP 地址) 阻止正常工作、但对于 SMB/CIFS、我看到错误消息："SID 到 DomainName 转换失败。原因超时：未建立套接字"	如果 <code>_CSUser</code> 无权执行 <code>ssh</code> 、则可能会发生这种情况。(确保在集群级别连接、然后确保用户可以执行 <code>ssh</code>)。 <code>CSUser</code> 角色需要这些权限。 https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking 对于具有集群凭据的 <code>_CSUser</code> 、请从 ONTAP 命令行执行以下操作： <pre>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"-all security login logline. role create -role csrole -cmddirname "vserver name-mapping"-access all</pre> 如果未使用 <code>_csUser</code> 、并且使用了集群级别的管理员用户、请确保管理员用户对 ONTAP 具有 <code>ssh</code> 权限。

工作负载安全性：模拟攻击

您可以使用此页面上的说明来模拟攻击、以便使用随附的勒索软件模拟脚本测试或演示工作负载安全性。



开始之前需要注意的事项

- 勒索软件模拟脚本仅适用于 Linux。
- 此脚本随工作负载安全代理安装文件一起提供。它可在安装了工作负载安全代理的任何计算机上使用。
- 您可以在工作负载安全代理计算机本身上运行此脚本；无需准备其他Linux计算机。但是，如果您希望在其他系统上运行此脚本，只需复制此脚本并在其中运行即可。

至少具有 1,000 个示例文件

此脚本应在包含要加密的文件的文件夹的 SVM 上运行。建议在该文件夹和任何子文件夹中至少有 1,000 个文件。这些文件不能为空。请勿使用同一用户创建文件并对其进行加密。工作负载安全性会将此视为低风险活动，因此不会生成警报(即同一用户修改其刚刚创建的文件)。

有关说明，请参见下面的 ["以编程方式创建非空文件"](#)。

运行模拟器之前的准则：

1. 确保加密文件不为空。
2. 请确保对50个以上的文件进行加密。少量文件将被忽略。
3. 请勿多次使用同一用户进行攻击。几次后、Workload Security将了解此用户行为并假设这是用户的正常行为。
4. 不要对同一用户刚刚创建的文件进行加密。更改用户刚刚创建的文件不会被视为一项风险活动。而是使用另一用户创建的文件、或者在创建文件 and 对其进行加密之间等待几个小时。

准备系统

首先，将目标卷挂载到计算机。您可以挂载 NFS 挂载或 CIFS 导出。

要在 Linux 中挂载 NFS 导出，请执行以下操作：

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

请勿挂载 NFS 4.1；Fpolicy 不支持此版本。

要在 Linux 中挂载 CIFS，请执行以下操作：

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

接下来，设置数据收集器：

1. 如果尚未配置工作负载安全代理、请进行配置。

2. 如果尚未配置 SVM 数据收集器，请进行配置。

运行勒索软件模拟器脚本

1. 登录(ssh)到工作负载安全代理计算机。
2. 导航到： `/opt/netapp/cloudsecure/agent/install`
3. 调用不带参数的模拟器脚本以查看用法：

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

对测试文件进行加密

要对文件进行加密，请运行以下命令：

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

还原文件

要解密，请运行以下命令：

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/  
File /root/for/File000.txt is restored.  
File /root/for/File001.txt is restored.  
File /root/for/File002.txt is restored.  
...
```

多次运行此脚本

在为用户生成勒索软件攻击后，切换到另一个用户以生成额外的攻击。工作负载安全性可了解用户行为、不会在短时间内对同一用户的重复勒索软件攻击发出警报。

以编程方式创建文件

在创建文件之前、必须先停止或暂停数据收集器处理。

在将数据收集器添加到代理之前，请执行以下步骤。如果您已添加数据收集器，只需编辑数据收集器，输入无效密码并保存即可。此操作将暂时使数据收集器处于错误状态。注意：请务必记下原始密码！



建议的选项为 **"暂停收集器"** 创建文件之前。]

在运行模拟之前，您必须先添加要加密的文件。您可以手动将要加密的文件复制到目标文件夹中，也可以使用脚本（请参见以下示例）以编程方式创建文件。无论使用哪种方法，至少复制 1,000 个文件。

如果您选择以编程方式创建文件，请执行以下操作：

1. 登录到代理框。
2. 将 NFS 导出从存储器的 SVM 挂载到代理计算机。将 CD 复制到该文件夹。
3. 在该文件夹中，创建一个名为 createfiles.sh 的文件
4. 将以下行复制到该文件。

```
for i in {000..1000}  
do  
    echo hello > "File${i}.txt"  
done  
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. 保存文件。
6. 确保对文件具有执行权限：

```
chmod 777 ./createfiles.sh  
. 执行脚本：
```

```
./createfiles.sh
```

此时将在当前文件夹中创建 1000 个文件。

7. 重新启用数据收集器

如果您在步骤 1 中禁用了数据收集器，请编辑该数据收集器，输入正确的密码并保存。确保数据收集器重新处于运行状态。

8. 如果您在执行这些步骤之前暂停了收集器、请确保 ["恢复收集器"](#)。

为警报，警告和代理 / 数据源收集器运行状况配置电子邮件通知

要配置工作负载安全警报收件人、请单击*管理员>通知*、然后在相应的部分中为每个收件人输入电子邮件地址。



Cloud Insights 联邦版不提供工作负载安全性。

潜在攻击警报和警告

要发送 *potential agres*攻击 _ 警报通知，请在 *_Send potential Attack Alerts* 部分输入收件人的电子邮件地址。对于对警报执行的每个操作，系统会将电子邮件通知发送到警报收件人列表。

要发送 *Warning* 通知，请在 *Send Warning Alerts* 部分中输入收件人的电子邮件地址。

代理和数据收集器运行状况监控

您可以通过通知监控代理和数据源的运行状况。

要在代理或数据源收集器未运行时接收通知，请在 *Data Collection Health Alerts* 部分中输入收件人的电子邮件地址。

请记住以下几点：

- 只有在代理 / 收集器停止报告至少一小时后，才会发送运行状况警报。
- 在给定的 24 小时时间段内，仅向目标收件人发送一封电子邮件通知，即使代理或数据收集器断开连接的时间较长也是如此。
- 如果代理发生故障，将发送一个警报（而不是每个收集器发送一个警报）。此电子邮件将列出所有受影响的 SVM。
- Active Directory 收集失败会报告为警告；它不会影响勒索软件检测。
- 现在，Getting Started 设置列表包括一个新的 *_Configure email notifications* 阶段。

正在接收代理和**Data Collector**升级通知

- 在"Data Collection Health Alerts"(数据收集运行状况警报)中输入电子邮件ID。

- 此时、"Enable upgrade通知"复选框将变为启用状态。
- 代理和Data Collector升级电子邮件通知会在计划升级的前一天发送到电子邮件ID。

故障排除

* 问题: *	* 请尝试此操作: *
"Data Collector运行状况警报"中存在电子邮件ID、但我未收到通知。	通知电子邮件从NetApp Cloud Insights域发送、即从_accounts@service.cloudinsights.netapp.com_发送。某些公司会阻止来自外部域的传入电子邮件。确保来自NetApp Cloud Insights域的外部通知已列入白名单。

工作负载安全API

通过工作负载安全API、NetApp客户和独立软件供应商(ISV)可以将工作负载安全与其他应用程序(例如CMDB或其他票证系统)集成在一起。



Cloud Insights 联邦版不提供工作负载安全性。

API 访问要求:

- API 访问令牌模型用于授予访问权限。
- API令牌管理由具有管理员角色的工作负载安全用户执行。

API 文档 (Swagger)

要查看最新的API信息、请登录到工作负载安全性并导航到*管理> API访问*。单击 * API Documentation" 链接。API 文档基于 Swagger ，其中提供了 API 的简短问题描述和使用情况信息，您可以在环境中试用这些文档。

API 访问令牌

在使用工作负载安全API之前、必须创建一个或多个* API访问令牌*。访问令牌授予读取权限。您还可以为每个访问令牌设置到期时间。

创建访问令牌:

- 单击 * 管理 > API 访问 *
- 单击 * + API 访问令牌 *
- 输入 * 令牌名称 *
- 指定 * 令牌到期 *



您的令牌只能在创建过程中复制到剪贴板并进行保存。令牌创建后无法检索，因此强烈建议复制令牌并将其保存在安全位置。系统将提示您单击复制 API 访问令牌按钮，然后才能关闭令牌创建屏幕。

您可以禁用，启用和撤消令牌。可以启用已禁用的令牌。

令牌可从客户的角度授予对 API 的通用访问权限，并可在其自身环境范围内管理对 API 的访问。

在用户成功进行身份验证并授权访问后，应用程序会收到访问令牌，然后在调用目标 API 时将访问令牌作为凭据传递。传递的令牌将通知 API 令牌的持有人已获得访问 API 的授权，并根据授权期间授予的范围执行特定操作。

传递访问令牌的 HTTP 标头为 *。X-CloudInsights ApiKey： *

例如，使用以下命令检索存储资产：

```
curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-CloudInsights-ApiKey: <API_Access_Token>'
```

其中， `<API_Access_Token>` 是您在创建 API 访问密钥期间保存的令牌。

有关详细信息，请参见 *API Documentation* 链接中的 * 管理 > API 访问 *。

版权信息

版权所有 © 2024 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。