配置和管理适用于 Cisco Secure Workload 的连接器

连接器使 Cisco Secure Workload 能够与外部资源（例如网络交换机、路由器、防火墙和终端管理系统）集成，以收集遥测数据、注入流观察结果并丰富资产和终端情景。

什么是连接器

Cisco Secure Workload 中的连接器是允许 Cisco Secure Workload 与各种资源交互并从各种资源收集数据以用于不同目的的集成。要配置和使用连接器，请从导航窗格中选择**管理 (Manage)** > **连接器 (Connectors)**。

Note 连接器需要使用虚拟设备。有关详细信息，请参阅连接器的虚拟设备。

用于流注入的连接器

连接器会将来自不同网络交换机、路由器和其他中间设备（例如负载均衡器和防火墙）的流观察结果流传输到 Cisco Secure Workload，以便进行流注入。

Cisco Secure Workload 支持通过 NetFlow v9、IPFIX 和自定义协议进行流注入。除了流观察结果之外，中间件连接器还会主动拼接客户端和服务器端的流，以了解哪些客户端流与哪些服务器流相关。

连接器	说明	已在虚拟设备上部署
NetFlow	从路由器和交换机等网络设备收集 NetFlow V9 和/或 IP-FIX 遥测数据。	Cisco Secure Workload 注入
F5 BIG-IP	收集来自 F5 BIG-IP、拼接客户端和服务器端流的遥测数据，利用用户属性丰富客户端资产。	Cisco Secure Workload 注入
Citrix NetScaler	从 Citrix ADC、拼接客户端和服务器端流收集遥测数据。	Cisco Secure Workload 注入
Cisco Secure 连接器防火墙	从 Cisco Secure Firewall ASA、Cisco Secure Firewall Threat Defense、拼接客户端和服务器端流收集遥测数据。	Cisco Secure Workload 注入
Meraki	从 Meraki 防火墙收集遥测数据。	Cisco Secure Workload 注入
ERSPAN	从支持 ERSPAN 的网络设备收集 ERSPAN 遥测数据	Cisco Secure Workload 注入
另请参阅	云连接器	–

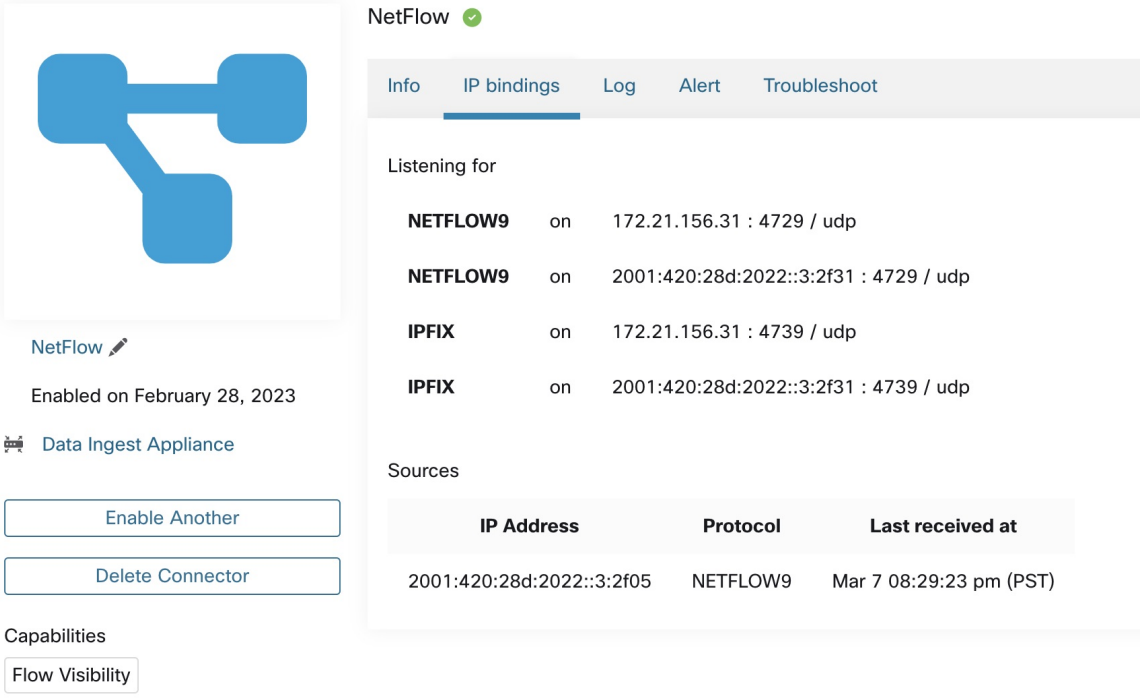
有关所需虚拟设备的详细信息，请参阅连接器的虚拟设备。

NetFlow 连接器

NetFlow 连接器允许 Cisco Secure Workload 从网络中的路由器和交换机注入流观察结果。

此解决方案使主机能够避免运行软件代理，因为思科交换机会将 NetFlow 记录中继到 Cisco Secure Workload 注入设备中托管的 NetFlow 连接器进行处理。

Figure 1: NetFlow 连接器



什么是 NetFlow

NetFlow 协议允许路由器和交换机将通过它们的流量汇聚到流中，然后将这些流导出到流收集器。

流收集器接收这些流记录并将其存储在流存储中，以供进行离线查询和分析。思科路由器和交换机支持 NetFlow。

设置通常包括以下步骤：

1. 在一台或多台网络设备上启用 NetFlow 功能，并配置设备应导出的流模板。
2. 配置远程网络设备上的 NetFlow 收集器终端信息。此 NetFlow 收集器会侦听已配置的终端，以便接收和处理 NetFlow 流记录。

到 Cisco Secure Workload 的流注入

NetFlow 连接器本质上是一个 NetFlow 收集器。连接器会接收来自网络设备的流记录，并将其转发到 Cisco Secure Workload 进行流分析。您可以在 Cisco Secure Workload 注入设备上启用 NetFlow 连接器，并将其作为 Docker 容器运行。

NetFlow 连接器还会作为 Cisco Secure Workload NetFlow 代理向 Cisco Secure Workload 注册。NetFlow 连接器会解封 NetFlow 协议数据包（即流记录）；然后，像常规 Cisco Secure Workload 代理一样处理和报告流。与深度可视性代理不同，它不报告任何进程或接口信息。

注释 NetFlow 连接器支持 NetFlow v9 和 IPFIX 协议。

注释 每个 NetFlow 连接器应仅报告一个 VRF 的流。连接器会导出流，并根据 Cisco Secure Workload 集群中的代理 VRF 配置将其放置在 VRF 中。

要为连接器配置 VRF，请依次选择**管理 (Manage)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的代理远程 *VRF* 配置 *(Agent Remote VRF Configurations)* 部分下，点击创建配置 *(Create Config)* 并提供有关连接器的详细信息。

此表单要求您提供：VRF 名称、连接器的 IP 子网以及可能向集群发送流记录的端口号范围。

速率限制

NetFlow 连接器每秒最多可接受 15000 个流。请注意，某个 NetFlow v9 或 IPFIX 数据包可能包含一个或多个流和模板记录。NetFlow 连接器会解析数据包并识别流。如果连接器每秒解析的流超过 15000 个，则会丢弃额外的流记录。

另请注意，Cisco Secure Workload 客户仅在流速保持在此可接受限制内时才支持 NetFlow 连接器。

如果流速超过每秒 15000 个流，建议先将流速调整到限制范围内，并将此级别至少保持三天（以排除与较高传入流速相关的问题）。

如果原先的问题仍然存在，客户支持将开始调查问题并确定适当的解决方法和/或解决方案。

支持的信息元素

NetFlow 连接器仅支持 NetFlow v9 和 IPFIX 协议中的以下信息元素。有关详细信息，请参阅 IP 流信息导出 (IPFIX) 实体。

元素 ID	名称	说明	必需
1	octetDeltaCount	此流的传入数据包中的八位组数。	是
2	packetDeltaCount	此流的传入数据包数。	是
4	protocolIdentifier	IP 数据包标头中协议号的值。	是
6	tcpControlBits	为此流的数据包观察到的 TCP 控制位。代理可处理 FIN、SYN、RST、PSH、ACK 和 URG 标志。	不兼容
7	sourceTransportPort	传输标头中的源端口标识符。	是

元素 ID	名称	说明	必需
8	sourceIPv4Address	IP 数据包标头中的 IPv4 源地址。	8 或 27
11	destinationTransportPort	传输标头中的目标端口标识符。	是
12	destinationIPv4Address	IP 数据包标头中的 IPv4 目标地址。	12 或 28
27	sourceIPv6Address	IP 数据包标头中的 IPv6 源地址。	8 或 27
28	destinationIPv6Address	IP 标头中的 IPv6 目标地址。	12 或 28
150	flowStartSeconds	流的第一个数据包的绝对时间戳（以秒为单位）。	不兼容
151	flowEndSeconds	流的最后一个数据包的绝对时间戳（以秒为单位）。	不兼容
152	flowStartMilliseconds	流的第一个数据包的绝对时间戳（以毫秒为单位）。	不兼容
153	flowEndMilliseconds	流的最后一个数据包的绝对时间戳（以毫秒为单位）。	不兼容
154 种	flowStartMicroseconds	流的第一个数据包的绝对时间戳（以微秒为单位）。	不兼容
155	flowEndMicroseconds	流的最后一个数据包的绝对时间戳（以微秒为单位）。	不兼容
156	flowStartNanoseconds	流的第一个数据包的绝对时间戳（以纳秒为单位）。	不兼容
157	flowEndNanoseconds	流的最后一个数据包的绝对时间戳（以纳秒为单位）。	否

如何在交换机上配置 NetFlow

以下步骤适用于 Nexus 9000 交换机。对于其他思科平台，配置可能略有不同。无论如何，请参阅您所配置的思科平台的官方思科配置指南。

Procedure

步骤 1 进入全局配置 模式。

```
switch# configure terminal
```

步骤 2 启用 Netflow 功能。

```
switch(config)# feature netflow
```

步骤 3 配置流记录。

下面的配置示例显示了如何在 NetFlow 记录中生成流的五个元组信息。

```
switch(config)# flow record ipv4-records
switch(config-flow-record)# description IPv4Flow
switch(config-flow-record)# match ipv4 source address
switch(config-flow-record)# match ipv4 destination address
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match transport source-port
switch(config-flow-record)# match transport destination-port
switch(config-flow-record)# collect transport tcp flags
switch(config-flow-record)# collect counter bytes
switch(config-flow-record)# collect counter packets
```

步骤 4 配置流导出器。

以下示例配置指定了 NetFlow 协议版本、NetFlow 模板交换间隔和 NetFlow 收集器终端详细信息。指定要在 Cisco Secure Workload 注入设备上启用 NetFlow 连接器的 IP 和端口。

```
switch(config)# flow exporter flow-exporter-one
switch(config-flow-exporter)# description NetFlowv9ToNetFlowConnector
switch(config-flow-exporter)# destination 172.26.230.173 use-vrf management
switch(config-flow-exporter)# transport udp 4729
switch(config-flow-exporter)# source mgmt0
switch(config-flow-exporter)# version 9
switch(config-flow-exporter-version-9)# template data timeout 20
```

步骤 5 配置流监控器。

创建流监控器，并将其与流记录和流导出器相关联。

```
switch(config)# flow monitor ipv4-monitor
switch(config-flow-monitor)# description IPv4FlowMonitor
switch(config-flow-monitor)# record ipv4-records
switch(config-flow-monitor)# exporter flow-exporter-one
```

步骤 6 将流监控器应用到接口。

```
switch(config)# interface Ethernet 1/1
switch(config-if)# ip flow monitor ipv4-monitor input
```

以上步骤在 Nexus 9000 上配置 NetFlow，为通过接口 1/1 的入口流量导出 NetFlow v9 协议数据包。它通过 UDP 协议将流记录发送到 172.26.230.173:4729。每个流记录包括流的五个元组信息和流的字节/数据包计数。

Figure 2: 在 *Cisco Nexus 9000* 交换机上运行 *NetFlow* 配置

```
switch# show running-config netflow

!Command: show running-config netflow
!Time: Wed Mar 21 04:25:21 2018

version 7.0(3)I7(1)
feature netflow

flow timeout 60
flow exporter flow-exporter-173
  destination 172.26.230.173 use-vrf management
  transport udp 4729
  source mgmt0
  version 9
    template data timeout 20
flow record ipv4-records
  match ipv4 source address
  match ipv4 destination address
  match ip protocol
  match transport source-port
  match transport destination-port
  collect transport tcp flags
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
flow monitor ipv4-monitor
  record ipv4-records
  exporter flow-exporter-173


interface Ethernet1/1
  ip flow monitor ipv4-monitor input

interface Ethernet1/2
  ip flow monitor ipv4-monitor input

switch#
```

如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。对于 NetFlow 连接器，支持 IPv4 和 IPv6（双栈模式）地址。但请注意，双堆栈支持是一项测试功能。

连接器上允许以下配置。

- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许的命令在 Cisco Secure Workload 注入设备中的 Docker 容器上更新连接器上 IPFIX 协议的侦听端口。通过提供连接器的连接器 ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。有关详细信息，请参阅 update-listing-ports。

限制

指标	限制
单个 Cisco Secure Workload 注入设备上的最大 NetFlow 连接器数	3
一个租户（根范围）上的最大 NetFlow 连接器数	10
Cisco Secure Workload 上的最大 NetFlow 连接器数	100

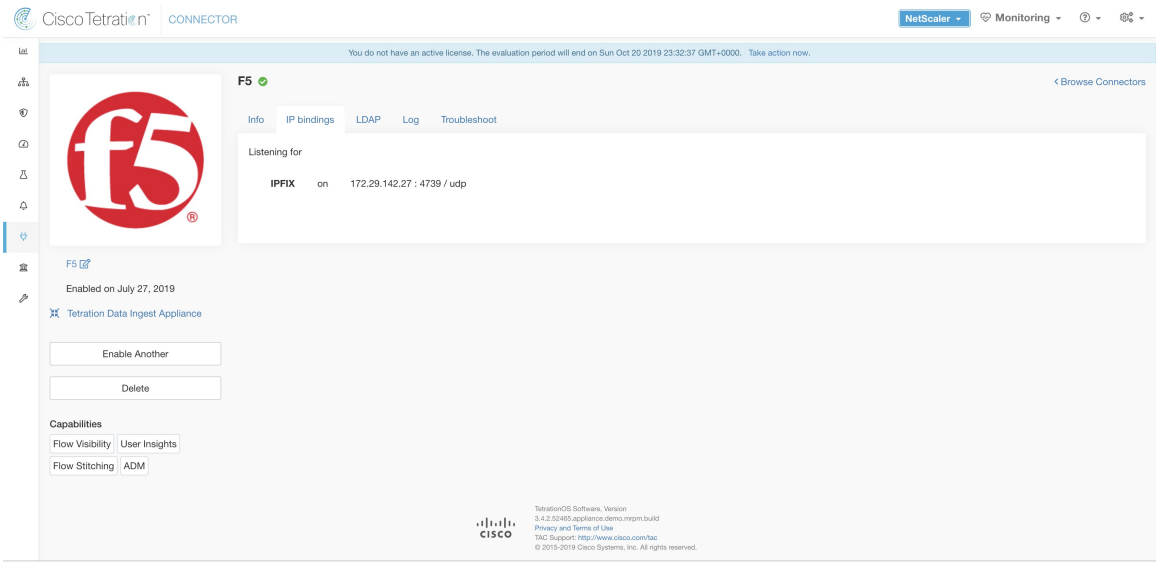
F5 连接器

F5 连接器允许 Cisco Secure Workload 从 F5 BIG-IP ADC 注入流观察结果。

它允许 Cisco Secure Workload 远程监控 F5 BIG-IP ADC 上的流观察结果，拼接客户端和服务器端流，以及在客户端 IP 上注释用户（如果有可用的用户信息）。

使用此解决方案，主机无需运行软件代理，因为 F5 BIG-IP ADC 会配置将 IPFIX 记录导出到 F5 连接器进行处理。

Figure 3: F5 连接器



什么是 F5 BIG-IP IPFIX

F5 BIG-IP IPFIX 日志记录会收集流经 F5 BIG-IP 的流量的流数据，并将 IPFIX 记录导出到流收集器。

设置通常包括以下步骤：

1. 在 F5 BIG-IP 设备上创建 IPFIX 日志发布服务器。
2. 在 F5 BIG-IP 设备上配置 IPFIX 日志目标。此日志目标会侦听已配置的终端，以接收和处理流记录。
3. 创建将 IPFIX 流记录发布到日志发布服务器的 F5 iRule。
4. 将 F5 iRule 添加到所需的虚拟服务器。

注释 F5 连接器支持 F5 BIG-IP 软件 12.1.2 及更高版本。

到 Cisco Secure Workload 的流注入

F5 BIG-IP 连接器本质上是一个 IPFIX 收集器。连接器会接收来自 F5 BIG-IP ADC 的流记录，拼接 NATed 流，并将其转发到 Cisco Secure Workload 以进行流分析。此外，如果向 F5 连接器提供了 LDAP 配置，它还会确定与事务相关的用户的 LDAP 属性配置值（如果 F5 在处理事务前对用户进行了身份验证）。这些属性与发生流的客户端 IP 地址相关联。

注释 F5 连接器仅支持 IPFIX 协议。

注释 每个 F5 连接器仅报告一个 VRF 的流。连接器会根据思科 Cisco Secure Workload 集群中的代理 VRF 配置将其导出的流放入 VRF 中。

要为连接器配置 VRF，请依次选择**管理 (Manage)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的代理远程 *VRF* 配置 *(Agent Remote VRF Configurations)* 部分下，点击创建配置 *(Create Config)* 并提供有关连接器的详细信息。此表单要求您提供：VRF 名称、连接器的 IP 子网以及可能向集群发送流记录的端口号范围。

如何在 F5 BIG-IP 上配置 IPFIX

以下步骤适用于 F5 BIG-IP 负载均衡器。（参考：为 IPFIX 配置 F5 BIG-IP）

目的	说明
1. 创建一个 IPFIX 收集器池。	在 F5 BIG-IP 设备上，创建一个 IPFIX 收集器池。这些是与 Cisco Secure Workload 注入设备上的 F5 连接器关联的 IP 地址。在 VM 上的 Docker 容器中运行的 F5 连接器会在端口 4739 上侦听 IPFIX 数据包。
2. 创建一个日志目标。	F5 BIG-IP 设备上的日志目标配置会指定所使用的实际 IPFIX 收集器池。
3. 创建一个日志发布服务器。	日志发布服务器会指定 F5 BIG-IP 将 IPFIX 消息发送到何处。发布服务器与日志目标绑定。
4. 添加 F5 和 Cisco Secure Workload 批准的 iRule。	Cisco Secure Workload 和 F5 开发了 iRules，可将流记录导出到 F5 连接器。这些 iRule 将导出有关给定事务的完整信息：包括所有终端、字节和数据包计数、流开始和结束时间（以毫秒为单位）。F5 连接器将创建 4 个独立流，然后将每个流与其相关流进行匹配。
5. 将 iRule 添加到虚拟服务器。	在虚拟服务器的 iRule 设置中，将经过 Cisco Secure Workload 批准的 iRule 添加到虚拟服务器。

上述步骤在 F5 BIG-IP 负载均衡器上配置 IPFIX，以便为通过设备的流量导出 IPFIX 协议数据包。以下是 F5 的示例配置。

Figure 4: F5 BIG-IP 负载均衡器上 *IPFIX* 的运行配置

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm  pool ipfix-pool-1
ltm pool ipfix-pool-1 {
    members {
        10.28.118.6:ipfix {
            address 10.28.118.6
            session monitor-enabled
            state up
        }
    }
    monitor gateway_icmp
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config ltm virtual vip-1 rules
ltm virtual vip-1 {
    rules {
        ipfix-rule-1
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show running-config sys  log-config
sys log-config destination ipfix ipfix-collector-1 {
    pool-name ipfix-pool-1
    transport-profile udp
}
sys log-config publisher ipfix-pub-1 {
    destinations {
        ipfix-collector-1 { }
    }
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

在上面的示例中，流记录将发布到 *ipfix-pub-1*。*ipfix-pub-1* 配置了 log-destination *ipfix-collector-1*，它会将 IPFIX 消息发送到 IPFIX 池 *ipfix-pool-1*。*ipfix-pool-1* 将 10.28.118.6 作为 IPFIX 收集器之一。虚拟服务器 *vip-1* 使用 IPFIX iRule *ipfix-rule-1* 进行配置，该规则指定 IPFIX 模板以及模板的填充和发送方式。

- F5 和 Cisco Secure Workload 已批准用于 TCP 虚拟服务器的 iRule。有关详细信息，请参阅 TCP 虚拟服务器的 L4 iRule。
- F5 和 Cisco Secure Workload 已批准用于 UDP 虚拟服务器的 iRule。有关详细信息，请参阅 UDP 虚拟服务器的第 4 层 iRule。
- F5 和 Cisco Secure Workload 已批准用于 HTTPS 虚拟服务器的 iRule。有关详细信息，请参阅 HTTPS 虚拟服务器的 iRule。

Note 在使用从本指南下载的 iRule 之前，请更新**日志发布服务器**，以指向您在其中添加 iRule 的 F5 连接器中配置的日志发布服务器。

Note F5 已发布 GitHub 存储库 f5-tetration 来帮助您从流拼接开始。用于将各种协议类型的 IPFIX 记录发布到 F5 连接器的 iRules 位于：f5-tetration/irules。

访问站点以获取最新的 iRule 定义。此外，F5 还会开发一个脚本来执行以下操作：

1. 为虚拟服务器安装正确的 iRule。
2. 添加 IPFIX 收集器终端池（F5 连接器会在其中侦听 IPFIX 记录）。
3. 配置日志收集器和日志发布服务器。
4. 将正确的 iRule 绑定到虚拟服务器。

此工具可尽可能减少手动配置和用户错误，同时启用流拼接使用案例。该脚本位于 f5-tetration/scripts 中。

如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。

连接器上允许以下配置。

- LDAP：LDAP 配置支持发现 LDAP 属性，并提供工作流程来选择与用户名对应的属性以及要为每位用户获取的最多 6 个属性的列表。有关更多信息，请参阅“发现”。
- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许在容器上运行的命令在 Cisco Secure Workload 注入设备中的 Docker 容器上更新连接器上 IPFIX 协议的侦听端口。通过提供连接器的连接器 ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。有关详细信息，请参阅 update-listing-ports。

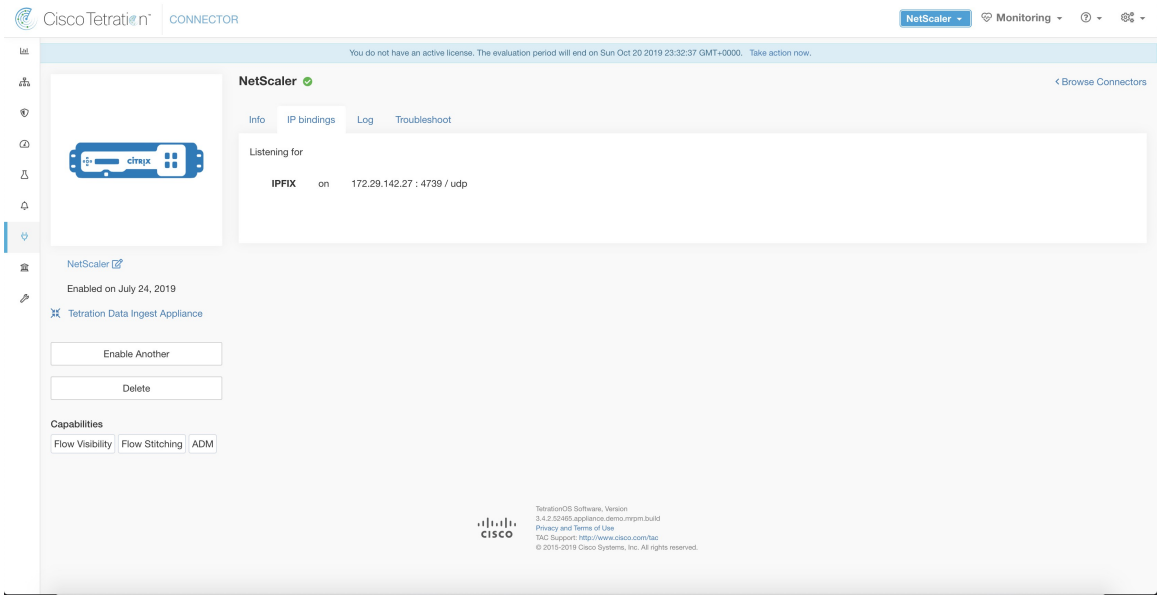
限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 F5 连接器数	3
一个租户（根范围）上的最大 F5 连接器数	10
Cisco Secure Workload 上的最大 F5 连接器数	100

NetScaler 连接器

NetScaler 连接器允许 Cisco Secure Workload 从 Citrix ADC (Citrix NetScaler) 注入流观察结果。它允许 Cisco Secure Workload 远程监控 Citrix ADC 上的流观察结果，同时拼接客户端和服务器端流。使用此解决方案，主机无需运行软件代理，因为 Citrix ADC 会被配置为将 IPFIX 记录导出到 NetScaler 连接器进行处理。

Figure 5: NetScaler 连接器



什么是 Citrix NetScaler AppFlow

Citrix NetScaler AppFlow 会收集流经 NetScaler 的流量的流数据，并将 IPFIX 记录导出到流收集器。Citrix AppFlow 协议会使用 IPFIX 将流导出到流收集器。Citrix NetScaler 负载均衡器支持 Citrix AppFlow。

设置通常包括以下步骤：

1. 在一个或多个 Citrix NetScaler 实例上启用 AppFlow 功能。
2. 配置远程网络设备上的 AppFlow 收集器终端信息。此 AppFlow 收集器将侦听已配置的终端，以接收和处理流记录。
3. 配置 AppFlow 操作和策略，以将流记录导出到 AppFlow 收集器。

Note NetScaler 连接器支持 Citrix ADC 软件版本 11.1.51.26 及更高版本。

到 Cisco Secure Workload 的流注入

NetScaler 连接器本质上是一个 Citrix AppFlow (IPFIX) 收集器。连接器会接收来自 Citrix ADC 的流记录，拼接 NATed 流，并将其转发到 Cisco Secure Workload 以进行流分析。NetScaler 连接器可以在思科 Cisco Secure Workload 注入设备上启用，并作为 Docker 容器运行。NetScaler 连接器还会作为 Cisco Secure Workload NetScaler 代理向 Cisco Secure Workload 注册。

Note NetScaler 连接器仅支持 IPFIX 协议。

Note 每个 NetScaler 连接器应只报告一个 VRF 的流。连接器导出的流将根据 Cisco Secure Workload 集群中的代理 VRF 配置放入 VRF 中。要为连接器配置 VRF，请转至：**管理 (Manage)** > **代理 (Agents)**，然后点击“配置”(Configuration) 选项卡。在此页面的代理远程 *VRF* 配置 *(Agent Remote VRF Configurations)* 部分下，点击创建配置 *(Create Config)* 并提供有关连接器的详细信息。此表单要求用户提供以下内容：VRF 的名称、连接器的 IP 子网以及可能向集群发送流记录的端口号范围。

如何在 NetScaler 上配置 AppFlow

以下步骤适用于 NetScaler 负载均衡器。（参考：配置 AppFlow）

Procedure

步骤 1 在 NetScaler 上启用 AppFlow。

```
enable ns feature appflow
```

步骤 2 添加 AppFlow 收集器终端。

收集器从 NetScaler 接收 AppFlow 记录。指定在作为 AppFlow 收集器的 Cisco Secure Workload 注入设备上启用的 NetScaler 连接器的 IP 和端口。

```
add appflow collector c1 -IPAddress 172.26.230.173 -port 4739
```

步骤 3 配置 AppFlow 操作。

这将列出在关联的 AppFlow 策略匹配时将获取 AppFlow 记录的收集器。

```
add appflow action a1 -collectors c1
```

步骤 4 配置 AppFlow 策略。

必须匹配此规则才能生成 AppFlow 记录。

```
add appflow policy p1 CLIENT.TCP.DSTPORT(22) a1
add appflow policy p2 HTTP.REQ.URL.SUFFIX.EQ("jpeg") a1
```

步骤 5 将 AppFlow 策略绑定到虚拟服务器。

系统将评估到达虚拟服务器 IP (VIP) 的流量是否与 AppFlow 策略匹配。一旦匹配，就会生成一条流记录，并发送到相关 AppFlow 操作中列出的所有收集器。

```
bind lb vserver lb1 -policyname p1 -priority 10
```

步骤 6 或者，全局绑定 AppFlow 策略（适用于所有虚拟服务器）。

AppFlow 策略也可以全局绑定到所有虚拟服务器。此策略适用于流经 Citrix ADC 的所有流量。

```
bind appflow global p2 1 NEXT -type REQ_DEFAULT
```

步骤 7 （可选）模板刷新间隔。

模板刷新的默认值为 60 秒。

```
set appflow param -templatereferesh 60
```

上述步骤在 Citrix NetScaler 负载均衡器上配置 AppFlow，以便导出通过 NetScaler 的流量的 IPFIX 协议数据包。流记录将被发送到 172.26.230.173:4739（适用于通过 vserver lb1 的流量）和 172.26.230.184:4739（适用于通过 NetScaler 的所有流量）。每个流记录包括流的 5 个元组信息和流的字节/数据包计数。

以下屏幕截图显示了 Citrix NetScaler 负载均衡器上 AppFlow 的运行配置。

Figure 6: 在 ***Citrix NetScaler*** 负载均衡器上运行 ***AppFlow*** 配置

```
MAARUMUG-M-M1PB:~ maarumug$ ssh nsroot@172.26.231.131
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Password:
Last login: Fri Dec 15 12:32:45 2017 from 10.128.140.136
 Done
> sh run | grep appflow
add appflow collector c1 -IPAddress 172.26.230.174
add appflow collector c2 -IPAddress 172.26.230.173
set appflow param -templateRefresh 60 -connectionChaining ENABLED
add appflow action act1 -collectors c1 c2
add appflow policy pol1 true act1
bind appflow global pol1 1 NEXT -type REQ_DEFAULT
>
```

如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。连接器上允许以下配置。

- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许的命令在 Cisco Secure Workload 注入设备中的 Docker 容器上更新连接器上 IPFIX 协议的侦听端口。通过提供连接器的连接器 ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。。有关详细信息，请参阅 update-listing-ports。

限制

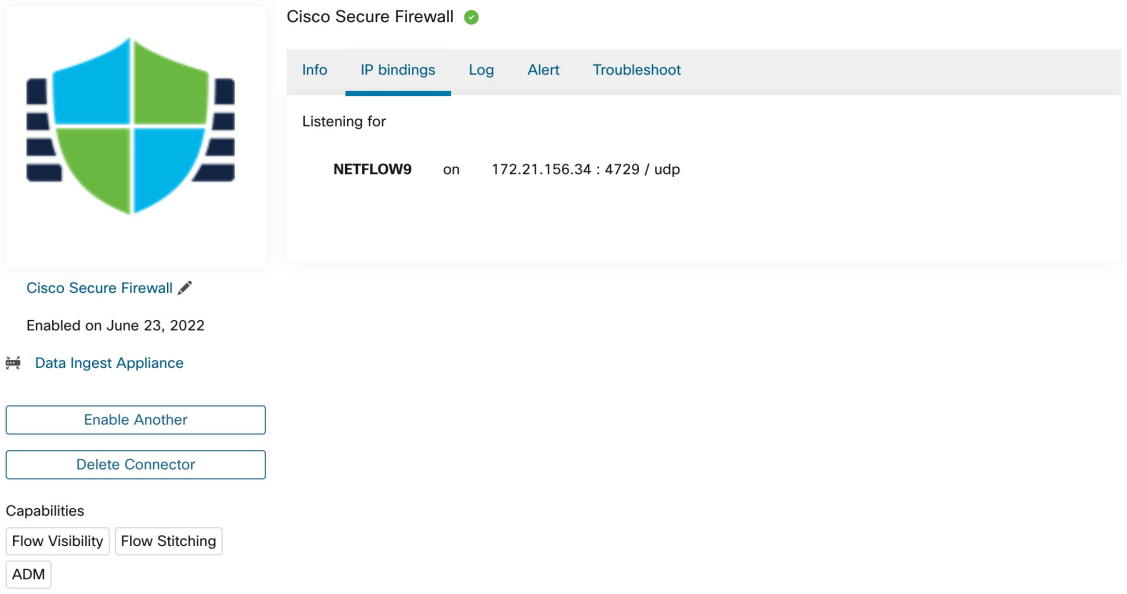
表 *1:* 限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 NetScaler 连接器数	3
一个租户（根范围）上的最大 NetScaler 连接器数	10
Cisco Secure Workload 上的最大 NetScaler 连接器数	100

Cisco Secure Firewall 连接器

Cisco Secure Firewall 连接器（以前称为 ASA 连接器）允许 Cisco Secure Workload 从 Cisco Secure Firewall ASA（以前称为 Cisco ASA）和 Cisco Secure Firewall Threat Defense（以前称为 Firepower Threat Defense 或 FTD）注入流观察结果。使用此解决方案，主机无需运行软件代理，因为思科交换机会将 NetFlow 安全事件日志记录 (NSEL) 记录中继到 Cisco Secure Workload 注入设备中托管的 Cisco Secure Firewall 连接器进行处理。

***Figure 7: Cisco Secure Firewall* 连接器**



Cisco Secure Firewall ASA NetFlow 安全事件日志 (NSEL) 提供有状态的 IP 流监控，可将流中的重要事件导出到 NetFlow 收集器中。当某一事件导致流的状态发生变化时，NSEL 事件就会被触发，该事件会将流观察结果和导致状态变化的事件一起发送到 NetFlow 收集器。流收集器接收这些流记录并将其存储在流存储中，以供进行离线查询和分析。

设置通常包括以下步骤：

1. 在 Cisco Secure Firewall ASA 和/或 Cisco Secure Firewall Threat Defense 上启用 NSEL 功能。
2. 在 Cisco Secure Firewall ASA 和/或 Cisco Secure Firewall Threat Defense 上配置 Cisco Secure Firewall 连接器终端信息。Cisco Secure Firewall 连接器将侦听已配置的终端，以接收和处理 NSEL 记录。

到 Cisco Secure Workload 的流注入

Cisco Secure Firewall 连接器本质上是一个 NetFlow 收集器。连接器从 Cisco Secure Firewall ASA 和 Cisco Secure Firewall Threat Defense 接收 NSEL 记录，并将其转发到 Cisco Secure Workload 以进行流量分析。Cisco Secure Firewall 连接器可以在 Cisco Secure Workload 注入设备上启用，并作为 Docker 容器运行。

Cisco Secure Firewall 连接器还会向 Cisco Secure Workload 注册为 Cisco Secure Workload 代理。Cisco Secure Firewall 连接器解封 NSEL 协议数据包（即流记录）；然后，像常规 Cisco Secure Workload 代理一样处理和报告流。与深度可视性代理不同，它不报告任何进程或接口信息。

Note Cisco Secure Firewall 连接器支持 NetFlow v9 协议。

Note 每个 Cisco Secure Firewall 连接器应仅报告一个 VRF 的流。连接器导出的流会根据 Cisco Secure Workload 集群中的代理 VRF 配置放入 VRF 中。要为连接器配置 VRF，请转至：**管理 (Manage)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的代理远程 *VRF* 配置 *(Agent Remote VRF Configurations)* 部分下，点击创建配置 *(Create Config)* 并提供有关连接器的详细信息。此表单要求用户提供以下内容：VRF 的名称、连接器的 IP 子网以及可能向集群发送流记录的端口号范围。

处理 NSEL 事件

下表显示了 Cisco Secure Firewall 连接器如何处理各种 NSEL 事件。有关这些元素的详细信息，请参阅 IP 流信息导出 (IPFIX) 实体文档。

流事件元素 ID：233 元素名称：*NF_F_FW_EVENT*	扩展流事件元素 ID：33002 元素名称：*NF_F_FW_EXT_EVENT*	对 Cisco Secure Firewall 连接器执行的操作
0（默认值，忽略此值）	无关	无操作
1（已创建流）	无关	发送流至 Cisco Secure Workload
2（已删除流）	> 2000（表示终止原因）	发送流至 Cisco Secure Workload

流事件元素 ID：233 元素名称：*NF_F_FW_EVENT*	扩展流事件元素 ID：33002 元素名称：*NF_F_FW_EXT_EVENT*	对 Cisco Secure Firewall 连接器执行的操作
3（流被拒绝）	1001（入口 ACL 拒绝流）	将处理结果标记为已拒绝的流发送到 Cisco Secure Workload
	1002（出口 ACL 拒绝流）	
	1003（ASA 接口拒绝连接或 ICMP(v6) 拒绝与设备的连接）	
	1004（TCP 上的第一个数据包不是 SYN）	
4（流警报）	无关	无操作
5（流更新）	无关	发送流至 Cisco Secure Workload

根据 NSEL 记录，Cisco Secure Firewall 连接器会将流观察结果发送到 Cisco Secure Workload。NSEL 流记录是双向的。因此，Cisco Secure Firewall 连接器会向 Cisco Secure Workload 发送 2 个流：正向流和反向流。

以下是 Cisco Secure Firewall 连接器向 Cisco Secure Workload 发送的流观察结果的详细信息。

转发流观察结果

字段	NSEL 元素 ID	NSEL 元素名称
协议	4	*NF_F_PROTOCOL*
源地址	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
源端口 (Source Port)	7	*NF_F_SRC_PORT*
目标地址	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
目标端口 (Destination Port)	11	*NF_F_DST_PORT*
流开始时间	152	*NF_F_FLOW_CREATE_TIME_MSEC*
字节计数	231	*NF_F_FWD_FLOW_DELTA_BYTES*
数据包计数 (Packet Count)	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

反向流信息

字段	NSEL 元素 ID	NSEL 元素名称
协议	4	*NF_F_PROTOCOL*
源地址	12	*NF_F_DST_ADDR_IPV4*
	28	*NF_F_DST_ADDR_IPV6*
源端口 (Source Port)	11	*NF_F_DST_PORT*
目标地址	8	*NF_F_SRC_ADDR_IPV4*
	27	*NF_F_SRC_ADDR_IPV6*
目标端口 (Destination Port)	7	*NF_F_SRC_PORT*
流开始时间	152	*NF_F_FLOW_CREATE_TIME_MSEC*
字节计数	232	*NF_F_REV_FLOW_DELTA_BYTES*
数据包计数 (Packet Count)	299	*NF_F_REV_FLOW_DELTA_PACKETS*

NAT

如果客户端到 ASA 的流经过 NAT，则 NSEL 流记录指明服务器端经过 NAT 的 IP/端口。Cisco Secure Firewall 连接器使用此信息将服务器流拼接到 ASA 以及将 ASA 流拼接到客户端。

以下是正向 NATed 流记录。

字段	NSEL 元素 ID	NSEL 元素名称
协议	4	*NF_F_PROTOCOL*
源地址	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
源端口 (Source Port)	227	*NF_F_XLATE_SRC_PORT*
目标地址	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
目标端口 (Destination Port)	228	*NF_F_XLATE_DST_PORT*
流开始时间	152	*NF_F_FLOW_CREATE_TIME_MSEC*
字节计数	231	*NF_F_FWD_FLOW_DELTA_BYTES*
数据包计数 (Packet Count)	298	*NF_F_FWD_FLOW_DELTA_PACKETS*

正向流将被标记为与正向 NATed 流记录相关（反之亦然）

这是反向 NATed 流记录

字段	NSEL 元素 ID	NSEL 元素名称
协议	4	*NF_F_PROTOCOL*
源地址	226	*NF_F_XLATE_DST_ADDR_IPV4*
	282	*NF_F_XLATE_DST_ADDR_IPV6*
源端口 (Source Port)	228	*NF_F_XLATE_DST_PORT*
目标地址	225	*NF_F_XLATE_SRC_ADDR_IPV4*
	281	*NF_F_XLATE_SRC_ADDR_IPV6*
目标端口 (Destination Port)	227	*NF_F_XLATE_SRC_PORT*
流开始时间	152	*NF_F_FLOW_CREATE_TIME_MSEC*
字节计数	232	*NF_F_REV_FLOW_DELTA_BYTES*
数据包计数 (Packet Count)	299	*NF_F_REV_FLOW_DELTA_PACKETS*

反向流将被标记为与反向上的 NATed 流记录相关（反之亦然）。

Note Cisco Secure Firewall 连接器仅支持本节中列出的 NSEL 元素 ID。

TCP 标志启发式

NSEL 记录没有 TCP 标志信息。Cisco Secure Firewall 连接器使用以下启发式方法设置 TCP 标志，以便可以通过自动策略发现进一步分析流：

- 如果至少有一个转发数据包，将 `SYN` 添加到正向流 TCP 标志。
- 如果至少有两个正向数据包和一个反向数据包，将 `ACK` 添加到正向流 TCP 标志，并将 `SYN-ACK` 添加到反向流 TCP 标志。
- 如果上一个条件成立并且流事件为“流已删除”，将 `FIN` 添加到正向和反向 TCP 标志。

如何在 Cisco Secure Firewall ASA 上配置 NSEL

以下步骤是有关如何配置 NSEL 并将 NetFlow 数据包导出到收集器（即 Cisco Secure Firewall 连接器）的指南。有关详细信息，请参阅《Cisco Secure Firewall ASA NetFlow 实施指南》中的官方思科配置指南。

以下是 NSEL 配置示例。

```
flow-export destination outside 172.29.142.27 4729
flow-export template timeout-rate 1
!
```

```
policy-map flow_export_policy
  class class-default
  flow-export event-type flow-create destination 172.29.142.27
  flow-export event-type flow-teardown destination 172.29.142.27
  flow-export event-type flow-denied destination 172.29.142.27
  flow-export event-type flow-update destination 172.29.142.27
  user-statistics accounting
service-policy flow_export_policy global
```

在本示例中，Cisco Secure Firewall ASA 设备配置为在端口 *4729* 上将 NetFlow 数据包发送到 *172.29.142.27*。此外，还会对 *flow-create*、*flow-teardown*、*flow-denied* 和 *flow-update* 事件启用 *flow-export* 操作。当这些流量事件在 ASA 上发生时，就会生成 NetFlow 记录并发送到配置中指定的目标。

假设在 Cisco Secure Workload 上启用了 Cisco Secure Firewall 连接器，并在 Cisco Secure Workload 注入设备中侦听 *172.29.142.27:4729*，则连接器将接收来自 Cisco Secure Firewall ASA 设备的 NetFlow 数据包。连接器按处理 NSEL 事件中的说明处理 NetFlow 记录，并将流观察结果导出到 Cisco Secure Workload。此外，对于 NAT 流，连接器会拼接相关流（客户端和服务器端）。

如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。连接器上允许以下配置。

- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许的命令在Cisco Secure Workload注入设备中的Docker容器上更新连接器上IPFIX协议的侦听端口。通过提供连接器的连接器ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。有关详细信息，请参阅update-listing-ports。

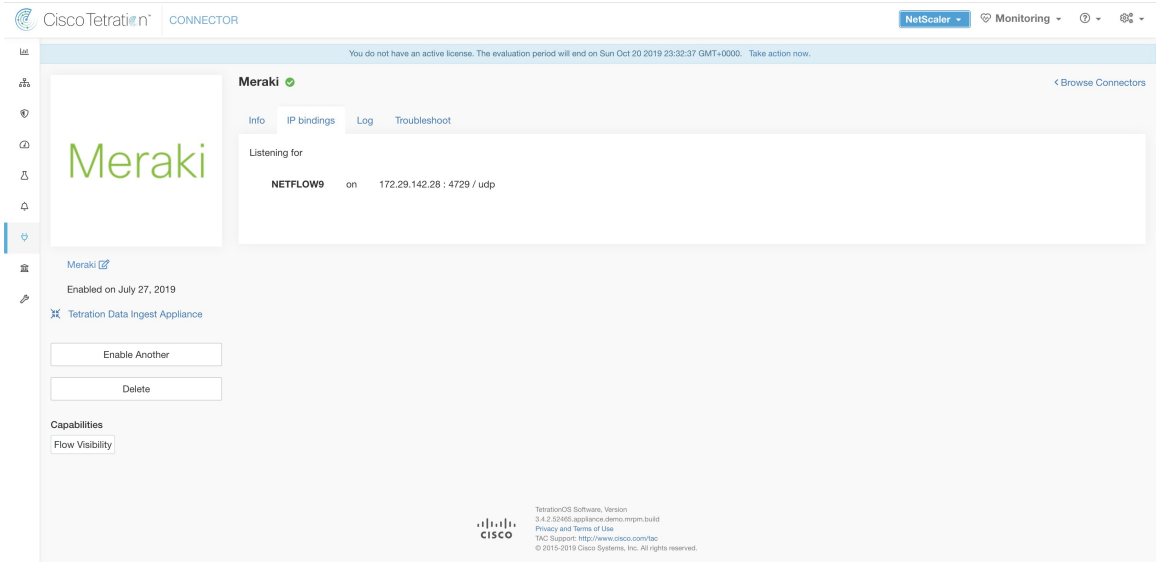
限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 Cisco Secure Firewall 连接器数	1
一个租户（根范围）上的最大 Cisco Secure Firewall 连接器数	10
Cisco Secure Workload 上的最大 Cisco Secure Firewall 连接器数	100

Meraki 连接器

Meraki 连接器允许 Cisco Secure Workload 从 Meraki 防火墙（Meraki MX 安全设备和无线接入点中包含）注入流观察结果。使用此解决方案，主机无需运行软件代理，因为思科交换机会将 NetFlow 记录中继到 Cisco Secure Workload 注入设备中托管的 Meraki 连接器进行处理。

***Figure 8: Meraki* 连接器**



什么是 NetFlow

NetFlow 协议允许网络设备（例如 Meraki 防火墙）将通过它们的流量汇聚到流中，并将这些流导出到流收集器。流收集器接收这些流记录并将其存储在流存储中，以供进行离线查询和分析。

设置通常包括以下步骤：

1. 在 Meraki 防火墙上启用 NetFlow 统计信息报告。
2. 在 Meraki 防火墙上配置 NetFlow 收集器终端信息。

到 Cisco Secure Workload 的流注入

Meraki 连接器本质上是一个 NetFlow 收集器。连接器从配置为导出 NetFlow 流量统计信息的 Meraki 防火墙接收流记录。它会处理 NetFlow 记录，并将 Meraki 防火墙报告的流观察结果发送到 Cisco Secure Workload 进行流分析。Meraki 连接器可以在 Cisco Secure Workload 注入设备上启用，并作为 Docker 容器运行。

Meraki 连接器还会向 Cisco Secure Workload 注册为 Cisco Secure Workload Meraki 代理。Meraki 连接器解封 NetFlow 协议数据包（即流记录）；然后，像常规 Cisco Secure Workload 代理一样处理和报告流。与深度可视性代理不同，它不报告任何进程或接口信息。

Note Meraki 连接器支持 NetFlow v9 协议。

Note 每个 Meraki 连接器应仅报告一个 VRF 的流量。连接器导出的流会根据 Cisco Secure Workload 集群中的代理 VRF 配置放入 VRF 中。要为连接器配置 VRF，请转至：**管理 (Manage)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的代理远程 *VRF* 配置 *(Agent Remote VRF Configurations)* 部分下，点击创建配置 *(Create Config)* 并提供有关连接器的详细信息。此表单要求用户提供以下内容：VRF 的名称、连接器的 IP 子网以及可能向集群发送流记录的端口号范围。

处理 NetFlow 记录

根据 NetFlow 记录，Meraki 连接器会将流观察结果发送到 Cisco Secure Workload。Meraki NetFlow 流记录是双向的。因此，Meraki 连接器向 Cisco Secure Workload 发送 2 个流：正向流和反向流。

以下是 Meraki 连接器向 Cisco Secure Workload 发送的流观察结果的详细信息。

转发流观察结果

字段	元素 ID	元素名称
协议 (Protocol)	4	*protocolIdentifier*
源地址 (Source Address)	8	*sourceIPv4Address*
源端口 (Source Port)	7	*sourceTransportPort*
目标地址 (Destination Address)	12	*destinationIPv4Address*
目标端口 (Destination Port)	11	*destinationTransportPort*
字节计数 (Byte Count)	1	*octetDeltaCount*
数据包计数 (Packet Count)	2	*packetDeltaCount*
流开始时间 (Flow Start Time)		根据连接器何时收到此流的 NetFlow 记录来设置

反向流信息

字段	元素 ID	
协议 (Protocol)	4	*protocolIdentifier*
源地址 (Source Address)	8	*sourceIPv4Address*
源端口 (Source Port)	7	*sourceTransportPort*
目标地址 (Destination Address)	12	*destinationIPv4Address*
目标端口 (Destination Port)	11	*destinationTransportPort*

字段	元素 ID	
字节计数 (Byte Count)	23	*postOctetDeltaCount*
数据包计数 (Packet Count)	24	*postPacketDeltaCount*
流开始时间 (Flow Start Time)		根据连接器何时收到此流的 NetFlow 记录来设置

如何在 Meraki 防火墙上配置 NetFlow

以下步骤显示如何在 Meraki 防火墙上配置 NetFlow 报告。

Procedure

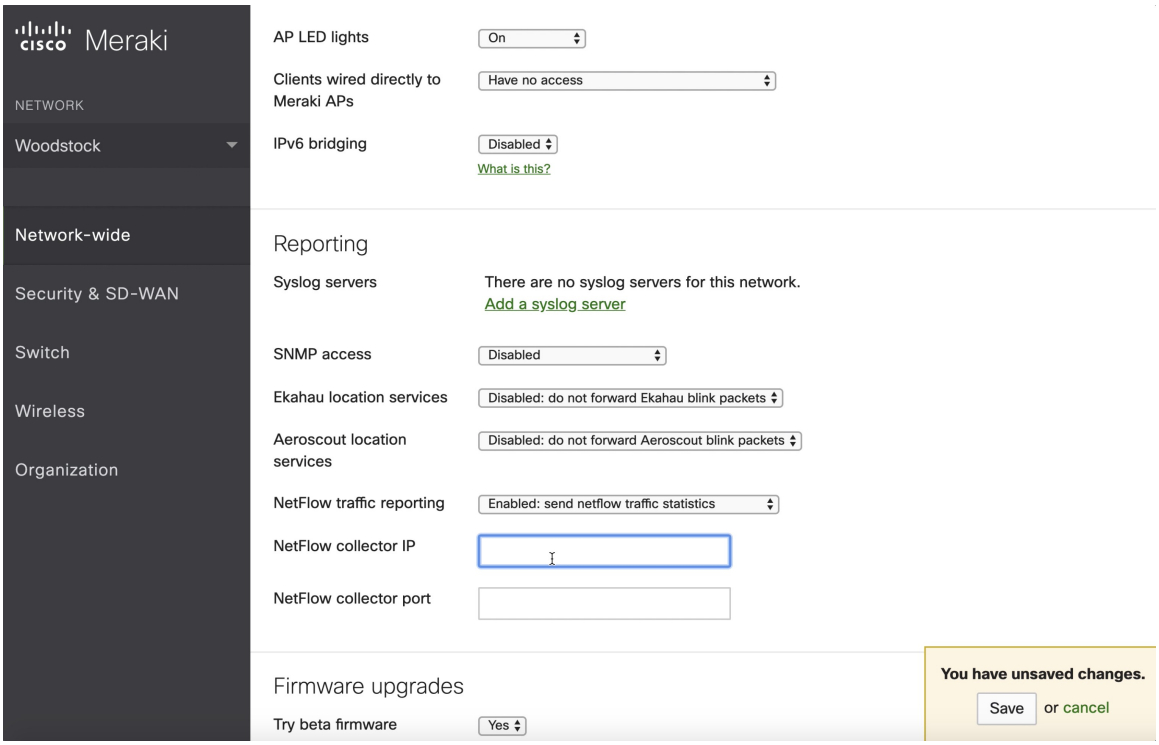
步骤 1 登录 Meraki UI 控制台。

步骤 2 导航至**全网范围 (Network-wide)** > **常规 (General)**。在报告 *(Reporting)* 设置中，启用 **NetFlow 流量报告 (NetFlow traffic reporting)**，并确保将值设置为启用：发送 *NetFlow* 流量统计信息 *(Enabled: send NetFlow traffic statistics)*。

步骤 3 将 **NetFlow 收集器 IP (NetFlow collector IP)** 和 **NetFlow 收集器端口 (NetFlow collector port)** 设置为 Meraki 连接器在 Cisco Secure Workload 注入设备中侦听的 IP 和端口。Meraki 连接器用于侦听 NetFlow 记录的默认端口为 4729。

步骤 4 保存更改。

Figure 9: 在 ***Meraki*** 防火墙上启用 ***NetFlow***



如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。连接器上允许以下配置。

- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许的命令在 Cisco Secure Workload 注入设备中的 Docker 容器上更新连接器上 NetFlow v9 协议的侦听端口。通过提供连接器的连接器 ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。有关详细信息，请参阅 update-listing-ports。

限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 Meraki 连接器数	1
一个租户（根范围）上的最大 Meraki 连接器数	10
Cisco Secure Workload 上的最大 Meraki 连接器数	100

ERSPAN 连接器

ERSPAN 连接器允许 Cisco Secure Workload 从网络中的路由器和交换机注入流观察结果。通过使用此解决方案，主机无需运行软件代理，因为思科交换机会将主机的流量中继到 ERSPAN 连接器进行处理。

什么是 ERSPAN

封装远程交换机端口分析器 (ERSPAN) 是大多数思科交换机的一项功能。它会镜像网络设备看到的帧，将其封装在 IP 数据包中，然后再发送到远程分析仪。用户可以选择要监控的交换机接口和/或 VLANS 列表。

通常，设置涉及在一个或多台网络设备上配置源 ERSPAN 监控会话，以及在直接连接到流量分析器的远程网络设备上配置目标 ERSPAN 监控会话。

Cisco Secure Workload ERSPAN 连接器提供目标 ERSPAN 会话和流量分析器功能；因此，无需使用 Cisco Secure Workload 解决方案在交换机上配置任何目标会话。

什么是 SPAN 代理

每个 ERSPAN 连接器都会向集群注册一个 SPAN 代理。Cisco Secure Workload SPAN 代理是配置为仅处理 ERSPAN 数据包的常规 Cisco Secure Workload 代理：与思科目标 ERSPAN 会话一样，它们解封镜像帧；然后，它们会像常规 Cisco Secure Workload 代理一样处理和报告流量。与深度可视性代理不同，它们不会报告任何进程或接口信息。

什么是 ERSPAN 注入设备

ERSPAN 的 Cisco Secure Workload 注入设备是在内部运行三个 ERSPAN Cisco Secure Workload 连接器的 VM。它使用与正常注入设备相同的 OVA 或 QCOW2。

每个连接器都在专用的 Docker 容器中运行，其中专门分配了一个 vNIC 和两个 vCPU 内核，没有配额限制。

ERSPAN 连接器使用容器主机名向集群注册 SPAN 代理： <VM hostname>-<interface IP address>。

在 VM、Docker 后台守护程序或 Docker 容器崩溃/重启时，连接器和代理将被保留/恢复。

注释 ERSPAN 连接器的状态将报告回“连接器”(Connector) 页面。请参阅“代理列表”页面并检查相应的 SPAN 代理状态。

有关所需虚拟设备的详细信息，请参阅连接器的虚拟设备。ERSPAN 连接器支持 IPv4 和 IPv6（双栈模式）地址。但请注意，双堆栈支持是一项测试功能。

如何配置源 ERSPAN 会话

以下步骤适用于 Nexus 9000 交换机。对于其他思科平台，配置可能略有不同。有关配置思科平台的信息，请参阅《Cisco Secure Workload 用户指南》。

图 *10:* 在 *Cisco Nexus 9000* 上配置 *ERSPAN* 源

```
Enter the configuration mode
# config terminal

Configure the erspan source IP address
(config)# monitor erspan origin ip-address 172.28.126.1 global

Create and configure the source erspan session
(config)# monitor session 10 type erspan-source
(config-erspan-src)# source interface ethernet 1/23 both
(config-erspan-src)# source vlan 315, 512
(config-erspan-src)# destination ip 172.28.126.194

Turn on the monitor session
(config-erspan-src)# no shut

Persist the configuration
# copy runnin-config startup-config
```

上述步骤创建了 ID 为 10 的源 ERSPAN 会话。交换机将镜像进出接口 eth1/23 的帧以及 VLANS 315 和 512 上的帧。承载镜像帧的外部 GRE 数据包的源 IP 地址为 172.28.126.1（必须是此交换机 L3 接口的地址），目标 IP 地址为 172.28.126.194。这是 ERSPAN VM 上配置的 IP 地址之一。

支持的 ERSPAN 格式

Cisco Secure Workload SPAN 代理可以处理提议的 ERSPAN RFC 中所述的 ERSPAN I、II 和 III 类数据包。因此，它们可以处理思科设备所生成的 ERSPAN 数据包。在不符合 RFC 标准的格式中，它们可以处理 VMware vSphere 分布式交换机 (VDS) 生成的 ERSPAN 数据包。

配置 ERSPAN 源时的性能注意事项

仔细选择 ERSPAN 源的端口/VLAN 列表。虽然 SPAN 代理有两个专用 vCPU，但会话可能会产生大量数据包，从而使代理的处理能力达到饱和。如果代理接收的数据包超过其处理能力，则会显示在集群“深度可视性代理”(Deep Visibility Agent) 页面的“代理数据包丢失”(Agent Packet Misses) 图中。

对于 ERSPAN 源将镜像哪些帧，可以通过 ACL 策略（通常通过 filter 配置关键字）进行更精细的调整。

如果交换机支持，则可以配置 ERSPAN 源会话，以修改 ERSPAN 数据包的最大传输单元 (MTU)（默认值通常为 1500 字节），通常是通过 mtu 关键字。减少该值将限制网络基础设施中 ERSPAN 带宽的使用，但不会影响 SPAN 代理的负载，因为代理的工作负载是按数据包计算的。减少该值时，应为镜像帧预留 160 字节的空间。有关 ERSPAN 标头开销详细信息，请参阅提议的 ERSPAN RFC。

ERSPAN 有三个版本。版本越低，ERSPAN 标头开销越低。版本 II 和 III 允许对 ERSPAN 数据包应用 QOS 策略，并提供一些 VLAN 信息。第 3 版包含更多设置。版本 II 通常是思科交换机的默认版本。虽然 Cisco Secure Workload SPAN 代理支持所有三个版本，但目前它们不会使用 ERSPAN 版本 II 和III 数据包携带的任何额外信息。

安全考虑事项

ERSPAN 访客操作系统的注入虚拟机是 CentOS 7.9，其中的 OpenSSL 服务器/客户端软件包已被删除。

注释 CentOS 7.9 是 Cisco Secure Workload 3.8.1.19 及更早版本中注入和边缘虚拟设备的访客操作系统。从 Cisco Secure Workload 3.8.1.36 开始，操作系统为 AlmaLinux 9.2。

启动 VM 并部署 SPAN 代理容器后（仅首次启动时需要几分钟时间），虚拟机中除了环回接口外将不存在任何网络接口。因此，访问设备的唯一途径是通过其控制台。

VM 网络接口现在被移到了 Docker 容器内。容器运行基于 centos:7.9.2009 的 Docker 映像，未打开 TCP/UDP 端口。

注释 从 Cisco Secure Workload 3.8.1.36 开始，容器运行 almalinux/9-base:9.2。

此外，容器使用基本权限（无 –privileged 选项）加上 NET_ADMIN 功能运行。

万一容器被入侵，虚拟机客户操作系统也无法从容器内部入侵。

适用于在主机内运行的 Cisco Secure Workload 代理的所有其他安全注意事项也适用于在 Docker 容器内运行的 Cisco Secure Workload SPAN 代理。

故障排除

SPAN 代理在“集群监控/代理概述”(Monitoring/Agent Overview) 页面中显示为活动状态后，无需对 ERSPAN 虚拟机执行任何操作，用户也无需登录该虚拟机。如果这没有发生，或者流未报告给集群，以下信息将有助于查明部署问题。

正常情况下，在 VM 上：

- `systemctl status tet_vm_setup` 报告具有 *SUCCESS* 退出状态的非活动服务；
- `systemctl status tet-nic-driver` 报告活动服务；
- `docker network ls` 报告五个网络：`host`、`none` 和三个 `erspan-<iface name>`；
- `ip link` 仅报告环回接口；
- `docker ps` 报告三个正在运行的容器；
- `docker logs <cid>` 包含以下消息：`INFO success: tet-sensor entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)`
- `docker exec <cid> ifconfig` 只报告一个接口（环回接口除外）；
- `docker exec <cid> route -n` 报告默认网关；
- `docker exec <cid> iptables -t raw -S PREROUTING` 报告规则 `-A PREROUTING -p gre -j DROP`；

如果上述任一项不成立，请检查 `/local/tetration/logs/ tet_vm_setup.log` 中的部署脚本日志，了解 SPAN 代理容器部署失败的原因。

任何其他代理注册/连接问题都可以通过 *docker exec* 命令来对主机上运行的代理进行故障排除：

- `docker exec <cid> ps -ef` 报告两个 `tet-engine, tet-engine check_conf` 实例和两个 `/usr/local/tet/tet-sensor -f /usr/local/tet/conf/.sensor_config` 实例（一个是 root user，另一个是 tet-sensor 用户），以及进程管理器 `/usr/bin/ python /usr/bin/supervisord -c /etc/supervisord.conf -n` 实例。
- `docker exec <cid> cat /usr/local/tet/log/tet-sensor.log` 显示代理的日志；
- `docker exec <cid> cat /usr/local/tet/log/fetch_sensor_id.log` 显示代理的注册日志；
- `docker exec <cid> cat /usr/local/tet/log/check_conf_update.log` 显示配置更新轮询日志；

  如有必要，在设置容器的网络命名空间后，可以使用 tcpdump 监控进出容器的流量：

  1. 通过 docker inspect <cid> | grep SandboxKey 检索容器的网络命名空间 (SandboxKey)；
  2. 设置到容器的网络命名空间中 nsenter --net=/var/run/docker/netns/...；
  3. 监控 eth0 流量 tcpdump -i eth0 -n。

限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 ERSPAN 连接器数	3
一个租户（根范围）上的最大ERSPAN连接器数	24（TaaS 为 12）
Cisco Secure Workload 上的最大 ERSPAN 连接器数	450

面向终端的连接器

终端的连接器会为 Cisco Secure Workload 提供终端情景。

连接器	说明	已在虚拟设备上部署
AnyConnect	从思科 AnyConnect 网络可视性模块 (NVM) 收集遥测数据，并丰富具有用户属性的终端资产	Cisco Secure Workload 注入
ISE	收集有关由 Cisco ISE 设备管理的终端和资产的信息，并使用用户属性和安全组标签 (SGL) 丰富终端资产。	Cisco Secure Workload 边缘

有关所需虚拟设备的详细信息，请参阅连接器的虚拟设备。

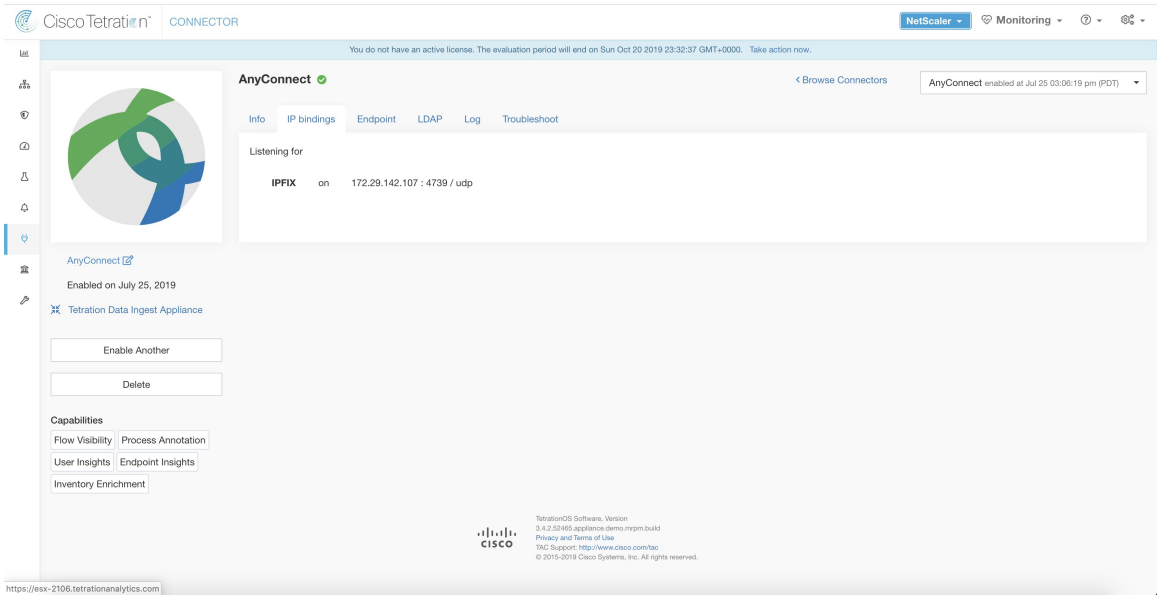
AnyConnect 连接器

AnyConnect 连接器监控运行带有网络可视性模块 (NVM) 的思科 AnyConnect 安全移动客户端的终端。通过使用此解决方案，主机无需在终端上运行任何软件代理，因为 NVM 会以 IPFIX 格式向收集器（如 AnyConnect 连接器）发送主机、接口和流记录。

AnyConnect 连接器可执行以下高级功能。

1. 在思科 Cisco Secure Workload 上将每个终端（支持的用户设备，例如台式机、笔记本电脑或智能手机）注册为 AnyConnect 代理。
2. 使用 Cisco Secure Workload 从这些终端更新接口快照。
3. 将这些终端导出的流信息发送到 Cisco Secure Workload 收集器。
4. 定期发送在 AnyConnect 连接器跟踪的终端上生成流的进程的进程快照。
5. 使用与每个终端上的登录用户相对应的轻量级目录访问协议 (LDAP) 属性来标记终端接口 IP 地址。

***Figure 11: AnyConnect* 连接器**



什么是 AnyConnect NVM

AnyConnect NVM 提供对内部和外部终端和用户行为的可视性和监控。它从终端收集包括以下情景的信息。

1. **设备/终端情景**：设备/终端特定信息。
2. **用户情景**：与流关联的用户。

3. **应用情景**：与流关联的进程。
4. **位置情景**：位置特定属性（如果可用）。
5. **目标情景**：目标的 FQDN。AnyConnect NVM 会生成 3 种类型的记录。

NVM 记录	说明
终端记录	设备/终端信息，包括唯一设备标识符 (UDID)、主机名、操作系统名称、操作系统版本和制造商。
接口记录	终端中每个接口的相关信息，包括终端 UDID、接口唯一标识符 (UID)、接口索引、接口类型、接口名称和 MAC 地址。
流记录器	在终端上看到的流的相关信息，包括终端 UDID、接口 UID、五元组（源/目标 IP/端口和协议）、入/出字节计数、进程信息、用户信息和目标的 FQDN。

每条记录都以 IPFIX 协议格式生成和导出。当设备处于受信任网络（内部/VPN）中时，AnyConnect NVM 会将记录导出到配置的收集器中。AnyConnect 连接器是一个 IPFIX 收集器示例，可接收和处理来自 AnyConnect NVM 的 IPFIX 数据流。

Note AnyConnect 连接器支持 4.2 及以上版本的思科 AnyConnect 安全移动客户端的 AnyConnect NVM。

如何配置 AnyConnect NVM

有关如何使用 Cisco Secure Firewall ASA 或 Cisco Identity Services engine (ISE) 来实施 AnyConnect NVM 的分步说明，请参阅如何实施 AnyConnect NVM 文档。部署 NVM 模块后，应指定 NVM 配置文件并将其推送到运行思科 AnyConnect 安全移动客户端的终端上，并将其安装在终端上。在指定 NVM 配置文件时，应将 IPFIX 收集器配置为指向端口 4739 上的 AnyConnect 连接器。

AnyConnect 连接器还会作为 Cisco Secure Workload AnyConnect 代理向 Cisco Secure Workload 注册。

处理 NVM 记录

AnyConnect 连接器会处理 AnyConnect NVM 记录，如下所示。

终端记录

收到终端记录后，AnyConnect 连接器会将该终端注册为 Cisco Secure Workload 上的 AnyConnect 代理。AnyConnect 连接器使用 NVM 记录中存在的终端特定信息以及 AnyConnect 连接器的证书来注册终端。注册终端后，通过在 Cisco Secure Workload 中创建与其中一个收集器的新连接，即可启用该终端的数据平面。AnyConnect 连接器会根据该终端的活动（流记录），定期（20-30 分钟）将该终端对应的 AnyConnect 代理与集群进行签入。

AnyConnect NVM 从 4.9 开始发送代理版本。默认情况下，AnyConnect 终端将在 Cisco Secure Workload 上注册为版本 4.2.x。此版本表示支持的最低 AnyConnect NVM 版本。对于版本为 4.9 或更高版本的 AnyConnect 终端，Cisco Secure Workload 上相应的 AnyConnect 代理将显示实际安装的版本。

Note AnyConnect 代理安装的版本不受 Cisco Secure Workload 控制。在 Cisco Secure Workload UI 上升级 AnyConnect 终端代理的尝试不会奏效。

接口记录

接口记录接口的 IP 地址不是 AnyConnect NVM 接口记录的一部分。接口的 IP 地址是在该接口的流记录开始从终端流出时确定的。 一旦确定了接口的 IP 地址，AnyConnect 连接器就会将该终端所有接口的完整快照（其 IP 地址已确定）发送到 Cisco Secure Workload 的配置服务器。这样就将 VRF 与接口数据关联起来，通过这些接口输入的数据流现在将标记为该 VRF。

流记录器

收到流记录后，AnyConnect 连接器将记录转换为 Cisco Secure Workload 能够理解的格式，并通过与该终端对应的数据平面发送 FlowInfo。此外，它还会在本地存储流记录中包含的进程信息。此外，如果 LDAP 配置提供给 AnyConnect 连接器，它将确定终端登录用户的已配置 LDAP 属性的值。这些属性与发生流的终端 IP 地址相关联。进程信息和用户标签会被定期推送到 Cisco Secure Workload。

Note 每个 AnyConnect 连接器将只报告一个 VRF 的终端/接口/流量。AnyConnect 连接器报告的终端和接口根据 Cisco Secure Workload 中的代理 VRF 配置与 VRF 关联。AnyConnect 连接器代理代表 AnyConnect 终端导出的流属于同一 VRF。要为代理配置 VRF，请转至：**管理 (Manage)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的“代理远程 VRF 配置”(Agent Remote VRF Configurations) 部分下，点击“创建配置”(Create Config) 并提供有关 AnyConnect 连接器的详细信息。该表单要求用户提供：VRF 名称、安装代理的主机 IP 子网，以及可能向集群发送流记录的端口号范围。

Windows 终端中的重复 UDID

如果端点计算机是从同一个黄金镜像克隆的，那么所有克隆终端的 UDID 都有可能是相同的。在这种情况下，AnyConnect 连接器使用相同的 UDID 从这些终端接收终端记录，并使用相同的 UDID 在 Cisco Secure Workload 上注册这些记录。当连接器从这些终端接收接口/流记录时，连接器无法确定 Cisco Secure Workload 上的正确 AnyConnect 代理来关联数据。连接器将所有数据关联到一个终端（且不确定）。

为了解决此问题，AnyConnect NVM 4.8 版本提供了一个名为 *dartcli.exe* 的工具，用于在终端上查找和重新生成 UDID。

- *dartcli.exe -u* 检索终端的 UDID。
- *dartcli.exe -nu* 重新生成终端的 UDID。要运行此工具，请执行以下步骤。

```
    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 8D0D1E8FA0AB09BE82599F10068593E41EF1BFFF

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-nu
    Are you sure you want to re-generate UDID [y/n]: y
    Adding nonce success
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5

    C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\DART>dartcli.exe
-u
    UDID : 29F596758941E606BD0AFF49049216ED5BB9F7A5
```

定期任务

AnyConnect 连接器会定期发送 AnyConnect 终端资产上的进程快照和用户标签。

1. **进程快照**：每隔 5 分钟，AnyConnect 连接器会检查其在本地维护的该间隔的进程，并发送在该间隔内具有流的所有终端的进程快照。
2. **用户标签**：每隔 2 分钟，AnyConnect 连接器会检查其在本地维护的 LDAP 用户标签，并更新这些 IP 地址上的用户标签。

对于用户标签，AnyConnect连接器会创建组织内所有用户的LDAP属性本地快照。启用AnyConnect连接器后，可提供 LDAP 配置（服务器/端口信息、为用户获取的属性、包含用户名的属性）。此外，还可以提供用于访问 LDAP 服务器的 LDAP 用户凭证。在 AnyConnect 连接器中，LDAP 用户凭证经过了加密，因此绝不会显示。或者，可以提供 LDAP 证书以安全地访问 LDAP 服务器。

Note AnyConnect 连接器会每 24 小时创建一个新的本地 LDAP 快照。此间隔可在连接器的 LDAP 配置中配置。

如何配置连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。连接器上允许以下配置。

- *LDAP*：LDAP 配置支持发现 LDAP 属性，并提供工作流程来选择与用户名对应的属性以及要为每位用户获取的最多 6 个属性的列表。有关更多信息，请参阅发现。
- 终端：有关详细信息，请参阅终端配置。
- 日志：有关详细信息，请参阅日志配置。

此外，可以使用允许的命令在Cisco Secure Workload注入设备中的Docker容器上更新连接器上IPFIX协议的侦听端口。通过提供连接器的连接器ID、要更新的端口类型和新端口信息，可在设备上发出此命令。连接器 ID 可在 Cisco Secure Workload UI 中的连接器页面上找到。有关详细信息，请参阅 update-listing-ports。

限制

指标	限制
一个 Cisco Secure Workload 注入设备上的最大 AnyConnect 连接器数	1
一个租户（根范围）上的最大 AnyConnect 连接器数	50
Cisco Secure Workload 上的最大 AnyConnect 连接器数	500

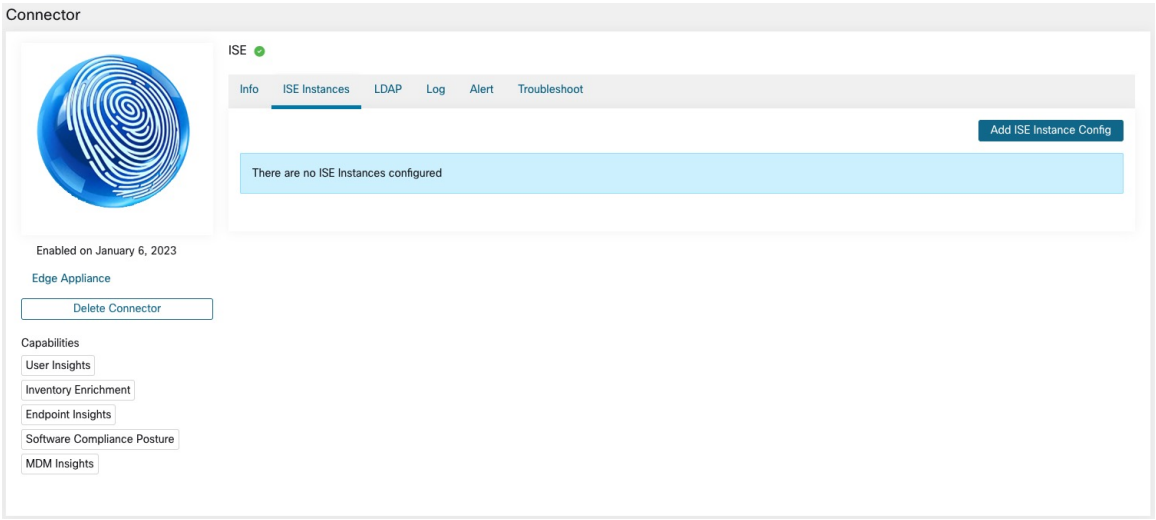
ISE 连接器

Cisco Secure Workload 中的 ISE 连接器使用思科平台交换网格 (pxGrid) 与 Cisco Identity Services Engine (ISE) 和 ISE 被动身份连接器 (ISE-PIC) 连接，以检索 ISE 报告的终端的情景信息，例如元数据。

ISE 连接器会执行以下功能：

1. 在 Cisco Secure Workload上注册标识为 ISE 终端的每个终端。
2. 更新 Cisco Secure Workload 上有关终端的元数据信息，例如 MDM 详细信息、身份验证、安全组标签、ISE 组名称和 ISE 组类型。
3. 定期拍摄快照并更新集群，使活动终端在 ISE 上可见。

Figure 12: ISE 连接器



Note 每个 ISE 连接器仅为一个 VRF 注册终端和接口。ISE 连接器报告的终端和接口会根据 Cisco Secure Workload 中的代理 VRF 配置与 VRF 相关联。

要为代理配置 VRF，请从导航窗格中选择**管理 (Manage)** > **工作负载 (Workloads)** > **代理 (Agents)**，然后点击**配置 (Configuration)** 选项卡。在此页面的**代理远程 VRF 配置 (Agent Remote VRF Configurations)** 部分下，点击**创建配置 (Create Config)** 并提供有关 ISE 连接器的详细信息 - VRF 的名称、安装代理的主机的 IP 子网以及在 Cisco Secure Workload上注册 ISE 终端和接口。

Note ISE 终端代理未在**代理列表 (Agents List)** 页面上列出；相反，可以在**资产 (Inventory)** 页面上查看具有属性的 ISE 终端。

如何配置连接器

Note 此集成需要使用 ISE 版本 2.4+ 和 ISE PIC 版本 3.1+。

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。对于 ISE 连接器，支持 IPv4 和 IPv6（双栈模式）地址。但请注意，双堆栈支持是一项测试功能。

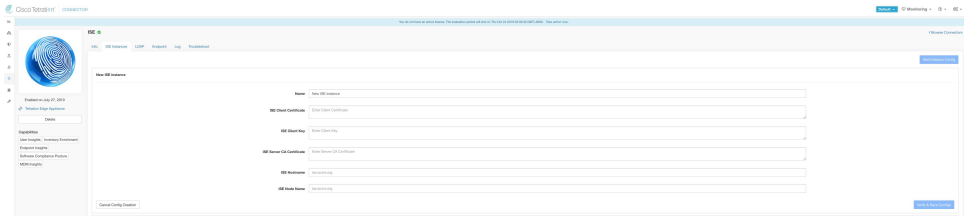
连接器上允许以下配置。

- *ISE 实例 (ISE Instance)*：ISE 连接器可以使用提供的配置连接到 ISE 的多个实例。每个实例都需要 ISE 证书凭证以及主机名和节点名才能连接到 ISE。有关详细信息，请参阅 ISE 实例配置。
- *LDAP*：LDAP 配置支持发现 LDAP 属性，并提供用于选择与用户名对应的属性的工作流程以及要为每位用户获取的最多六个属性的列表。有关更多信息，请参阅发现。
- 日志：有关详细信息，请参阅终端配置。

Note ISE 连接器会通过 getSessions API 调用连接，以获取该时间段内的所有活动终端。ISE 连接器还有一个侦听程序，用于订用 PxGrid 中提供所有新终端更新的会话主题。

ISE 实例配置

***Figure 13: ISE* 实例配置**



Note 从 Cisco Secure Workload 版本 3.7 开始，Cisco ISE pxGrid 节点的 SSL 证书需要此集成的主体备用名称 (SAN)。确保 ISE 节点的认证配置由 ISE 管理员完成，然后再执行与 Cisco Secure Workload 的集成。

要验证 pxGrid 节点的证书并确认是否已配置 SAN，您需要执行以下操作对来自 ISE 的证书进行验证。

Procedure

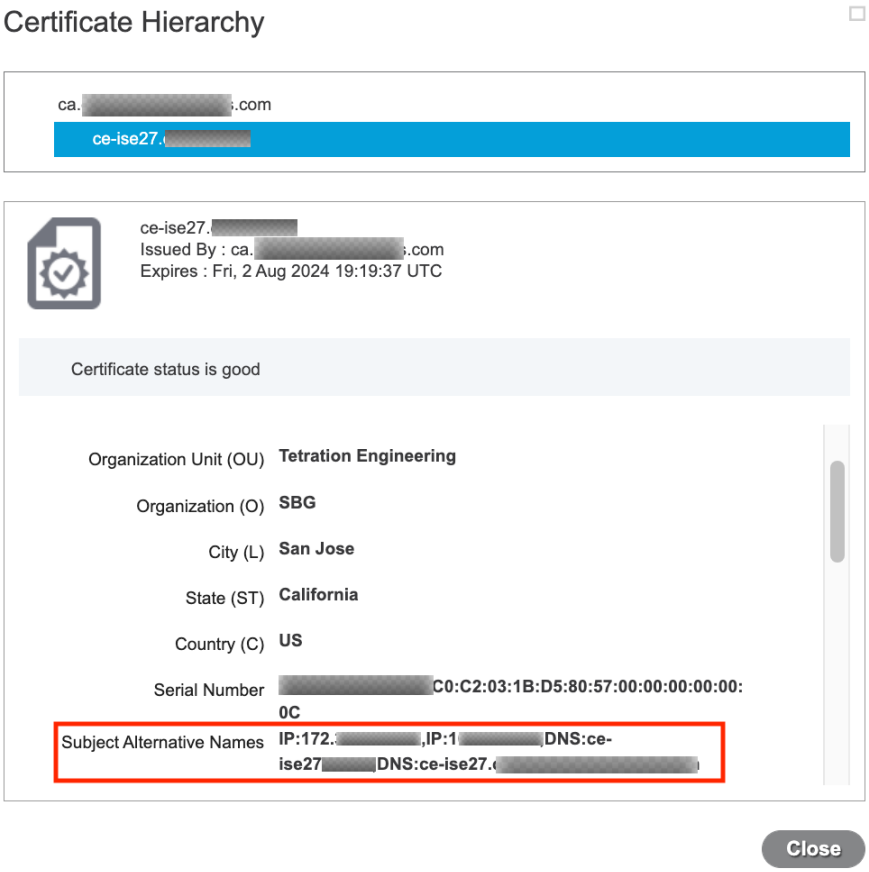
步骤 1 转至**管理 (Administration)** > **系统 (System)** 下的**证书 (Certificates)**。

步骤 2 在**证书管理 (Certificate Management)** 下，选择**系统证书 (System Certificates)**，选择“使用者”pxGrid 证书，然后选择**查看 (View)** 以查看 pxGrid 节点证书。

步骤 3 滚动证书，确保为该证书配置了主题备用名称。

步骤 4 该证书应由有效的证书颁发机构 (CA) 签署，该证书颁发机构还应签署用于 Cisco Secure Workload ISE 连接器的 pxGrid 客户端证书。

Figure 14: 有效 *ISE pxGrid* 节点证书的实例



步骤 5 现在，您可以在任何安装了 OpenSSL 的主机上使用以下模板生成 pxGrid 客户端证书签名请求。

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = YOUR_COUNTRY
ST = YOUR_STATE
L = YOUR_CITY
O = YOUR_ORGANIZATION
OU = YOUR_ORGANIZATION_UNIT
CN = ise-connector.example.com
[v3_req]
subjectKeyIdentifier = hash
basicConstraints = critical,CA:false
subjectAltName = @alt_names
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = serverAuth,clientAuth
[alt_names]
IP.1 = 10.x.x.x
DNS.1 = ise-connector.example.com
```

将文件另存为“example-connector.cfg”，并使用主机中的 OpenSSL 命令通过以下命令生成证书签名请求 (CSR) 和证书私钥。

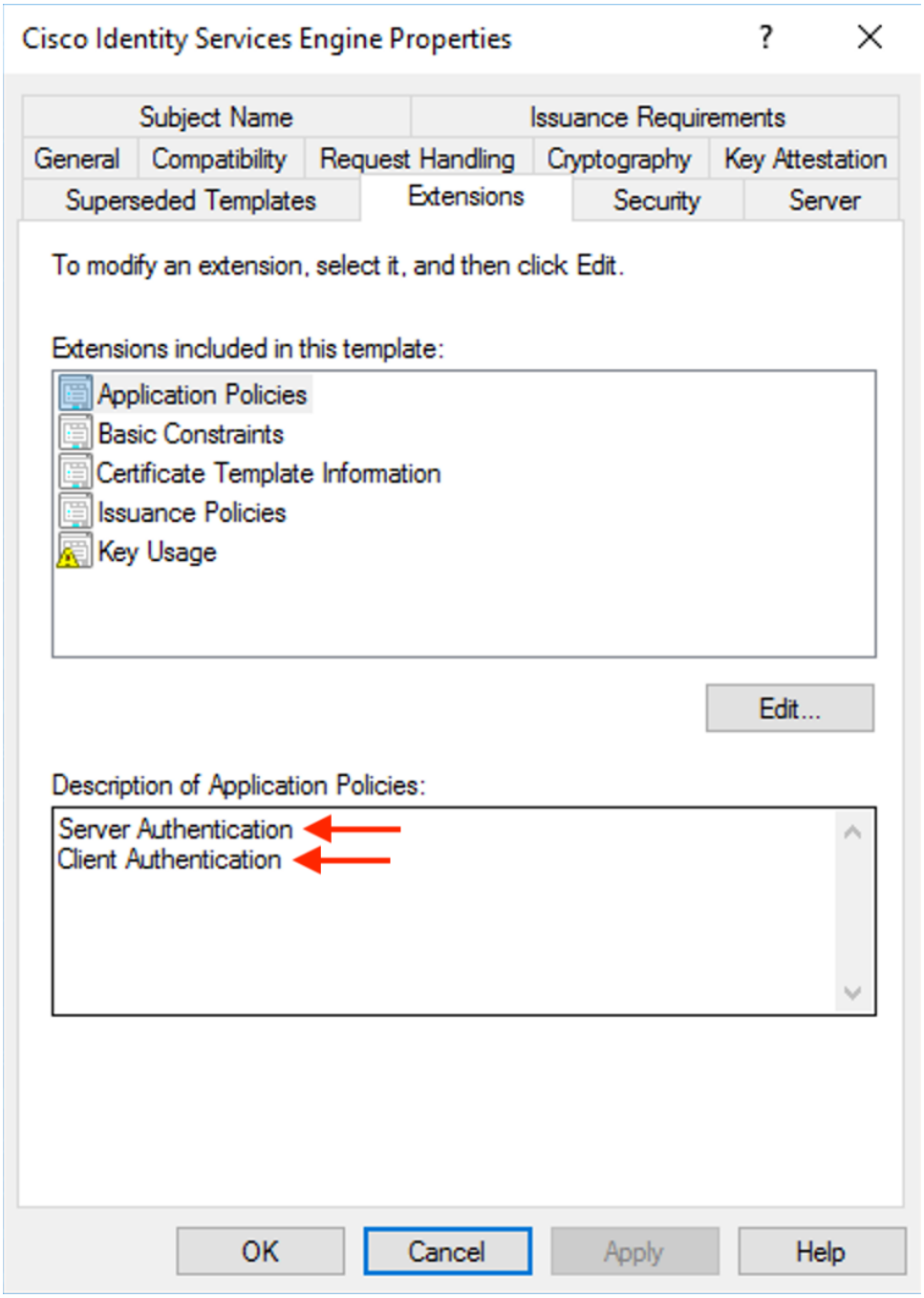
```
openssl req -newkey rsa:2048 -keyout example-connector.key -nodes -out example-connector.csr
 -config example-connector.cfg
```

步骤 6 由 CA 使用 Windows CA 服务器来签署证书签名请求 (CSR)。如果您还在使用 Windows CA 服务器，请运行以下命令来签署 pxGrid 客户端的 CSR。

```
certreq -submit -binary -attrib "CertificateTemplate:CiscoIdentityServicesEngine"
example-connector.csr example-connector.cer
```

Note Windows CA 需要使用证书模板。此模板应包含以下扩展。

Figure 15: 证书模板的应用策略扩展



步骤 7 将已签名的客户端证书和 PEM 格式的根 CA 复制到主机上。这与生成客户端 CSR 和私钥的主机相同。使用 OpenSSL 以确保客户端证书为 X.509 PEM 格式。使用 OpenSSL 运行以下命令，将经签名的客户端证书转换为 X.509 PEM 格式。

```
openssl x509 -inform der -in example-connector.cer -out example-connector.pem
```

步骤 8 您还可以使用以下命令确认由 CA 签名的 PEM。

```
openssl verify -CAfile root-ca.example.com.pem example-connector.pem
example-connector.pem: OK
```

Note 对于使用 pxGrid 的多节点 ISE 部署，所有 pxGrid 节点都必须信任用于 Cisco Secure Workload ISE 连接器的证书。

步骤 9 使用上述示例的文件名，将 ISE ISE client cert - example-connector.pem、client key - example-connector.key 和 CA – root-ca.example.com.pem 复制到 Secure ISE 配置页面上的相应字段工作负载，如下所示。

Note 在升级到 Cisco Secure Workload 的最新版本之前，请确保删除 ISE 连接器，以便删除任何现有配置数据。升级完成后，使用要应用的新过滤器来配置 ISE 连接器。

Figure 16: ISE 连接器配置

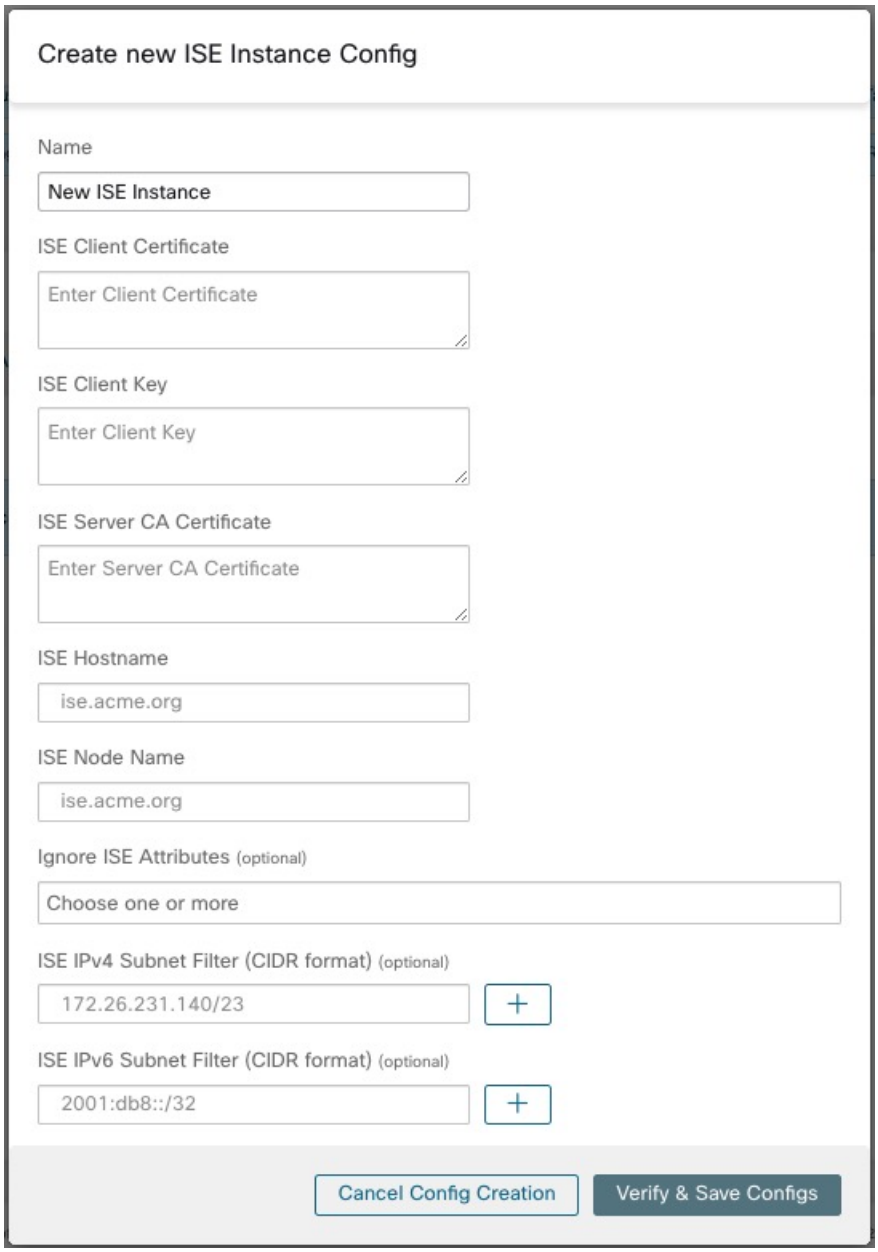


Table 2: ISE 连接器配置

字段	说明
名称 (Name)	输入 ISE 实例名称。
ISE 客户端证书 (ISE Client Certificate)	复制并粘贴 ISE 客户端证书。

字段	说明
ISE 客户端密钥 (ISE Client Key)	复制并粘贴 ISE 客户端密钥。客户端密钥必须是明文密钥，且未受密码保护。
ISE 服务器 CA 证书 (ISE Server CA Certificate)	复制并粘贴根 CA 证书。
ISE 主机名 (ISE Hostname)	输入 ISE 主机名 (FQDN)。
ISE 节点名称 (ISE Node Name)	输入 ISE 节点名称。
忽略 ISE 属性（可选）(Ignore ISE Attributes [Optional])	从列表中选择一个或多个 ISE 属性。 如果您不想注入通过 ISE 报告的终端的所有情景信息，则可以使用此选项。
ISE IPv4 子网过滤器（CIDR 格式）（可选）(ISE IPv4 Subnet Filter [CIDR Format] [Optional])	输入多个 IPv4 子网以过滤 ISE 终端。
ISE IPv6 子网过滤器（CIDR 格式）（可选）(ISE IPv6 Subnet Filter [CIDR Format] [Optional])	输入多个 IPv6 子网以过滤 ISE 终端。

Note

- 如果 ISE 主机名使用的是 IP 地址而不是 FQDN，则应使用 ISE CA 证书 SAN 中的 IP 地址，否则可能会出现连接失败。
- ISE 上的活动终端数量并非快照，它取决于 ISE 上的配置以及用于计算指标的汇聚持续时间。Cisco Secure Workload 上的代理计数始终是基于上次从 ISE 和 pxgrid 更新提取的快照，通常是过去一天的活动设备计数（完整快照的默认刷新频率为一天）。由于这些数字的描述方式不同，这两个数字有可能并不总是一致。

处理 ISE 记录

ISE 连接器将按如下所述处理记录。

终端记录

ISE 连接器连接到 ISE 实例，并通过 pxGrid 订用终端的任何更新。收到终端记录后，ISE 连接器会将该终端注册为 Cisco Secure Workload 上的 ISE 代理。ISE 连接器使用终端记录中的终端特定信息和 ISE 连接器证书来注册终端。注册终端后。ISE 连接器通过将终端对象作为 Cisco Secure Workload 上的用户标签发送，从而将终端对象用于资产扩充。ISE 连接器从 ISE 获取断开连接的终端时，会从 Cisco Secure Workload 中删除资产扩充。

安全组记录

ISE connect 还会通过 pxGrid 来订阅有关安全组标签更改的更新。在收到此记录后，ISE 连接器将维护本地数据库。它会使用此数据库将 SGT 名称与接收终端记录时的值进行映射。

定期任务

ISE 连接器会定期共享 ISE 终端资产中的用户标签。

1. **终端快照**：每 20 小时，ISE 连接器会从 ISE 实例获取终端和安全组标签的快照，并在检测到任何更改时更新集群。如果我们在 Cisco Secure Workload 上看不到来自 ISE 的终端，则不会为断开连接的终端计算此呼叫。
2. **用户标签**：ISE 连接器会每 2 分钟扫描一次本地维护的 LDAP 用户和 ISE 终端标签，并更新这些 IP 地址上的用户标签。

对于用户标签，ISE 连接器会创建组织中所有用户的 LDAP 属性的本地快照。启用 ISE 连接器后，可提供 LDAP 配置（服务器/端口信息、为用户获取的属性、包含用户名的属性）。此外，还可以提供用于访问 LDAP 服务器的 LDAP 用户凭证。LDAP 用户凭证已加密，绝不会在 ISE 连接器中显示。或者，可以提供 LDAP 证书以安全地访问 LDAP 服务器。

Note ISE 连接器会每 24 小时创建一次新的本地 LDAP 快照。此间隔可在连接器的 LDAP 配置中配置。

Note 在升级思科 ISE 设备时，ISE 连接器需要在升级后使用 ISE 生成的新证书重新配置。

限制

指标	限制
一个 ISE 连接器上可配置的最大 ISE 实例数	20
一个 Cisco Secure Workload 边缘设备上的最大 ISE 连接器数	1
一个租户（根范围）上的最大 ISE 连接器数	1
Cisco Secure Workload 上的最大 ISE 连接器数	150

Note 每个连接器支持的最大 ISE 代理数为 400000。

用于资产增强的连接器

用于资产扩充的连接器提供了有关 Cisco Secure Workload 监控的资产（IP 地址）的其他元数据和上下文。

连接器	说明	已在虚拟设备上部署
ServiceNow	从 ServiceNow 实例中收集终端信息，并利用 ServiceNow 属性扩充资产。	Cisco Secure Workload 边缘
另请参阅：	云连接器	–

有关所需虚拟设备的详细信息，请参阅连接器的虚拟设备。

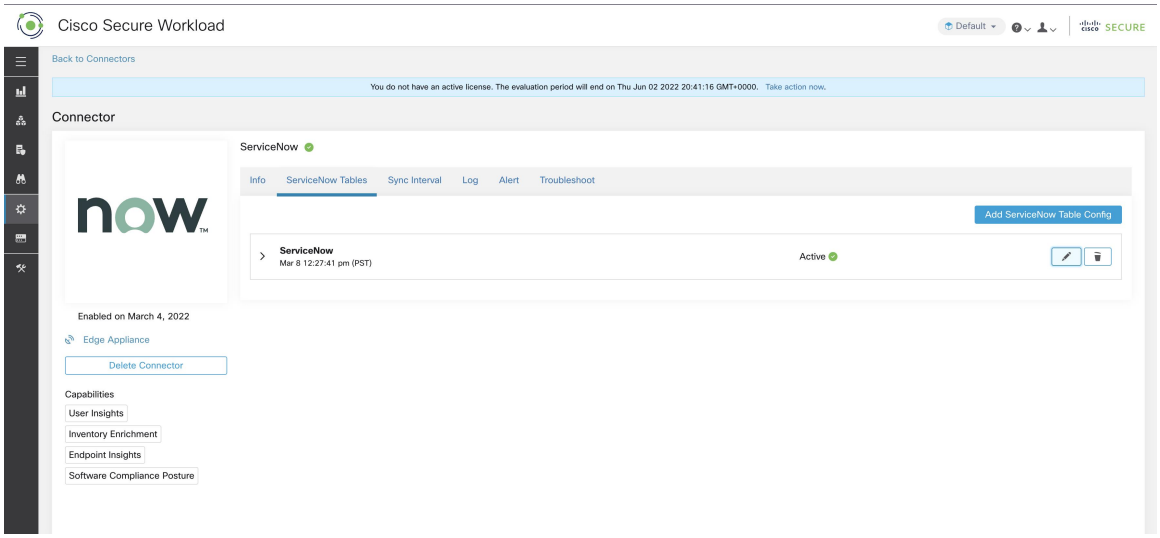
ServiceNow 连接器

ServiceNow 连接器与 ServiceNow 实例连接，以获取 ServiceNow 资产中终端的所有 ServiceNow CMDB 相关标签。使用此解决方案，我们可以为 Cisco Secure Workload 中的终端获取丰富的元数据。

ServiceNow 连接器执行以下高级功能。

1. 为这些终端更新 Cisco Secure Workload 资产中的 ServiceNow 元数据。
2. 定期拍摄快照并更新这些终端上的标签。

***Figure 17: ServiceNow* 连接器**



如何配置 ServiceNow 连接器

有关所需虚拟设备的信息，请参阅连接器的虚拟设备。连接器上允许以下配置。

- *ServiceNow* 表：ServiceNow 表配置 ServiceNow 实例的凭证以及要从中获取数据的 ServiceNow 表的相关信息。

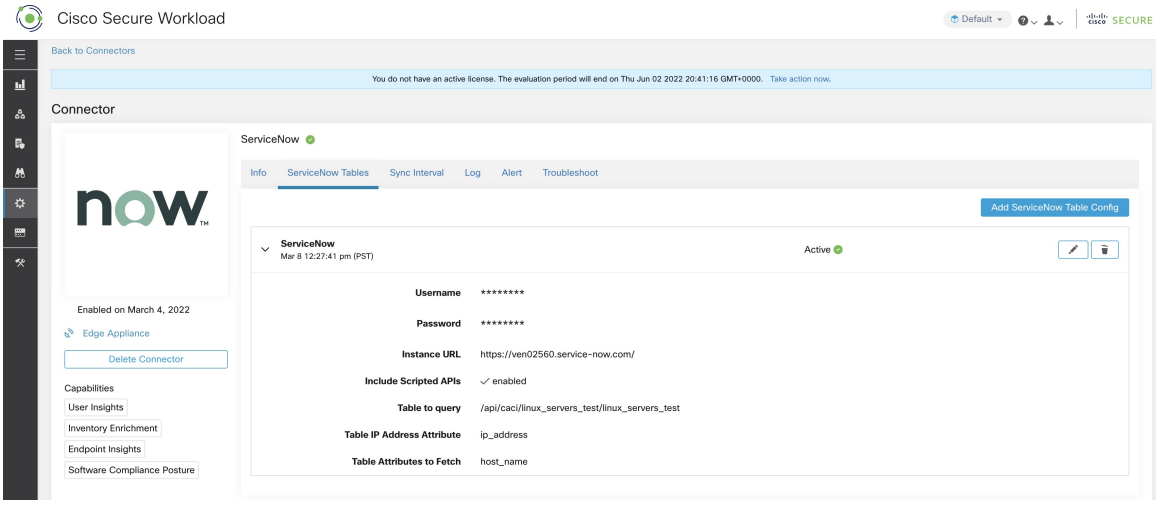
- 脚本化 *REST API*：ServiceNow 脚本化 REST API 表的配置类似于 ServiceNow 表。
- 同步间隔：同步间隔配置允许更改 Cisco Secure Workload 查询 ServiceNow 实例以获取更新数据的周期。默认同步时间间隔设置为 60 分钟。
- 日志：有关详细信息，请参阅日志配置。

ServiceNow 实例配置

您需要以下物品才能成功配置 ServiceNow 实例。

- ServiceNow 用户名
- ServiceNow 密码
- ServiceNow 实例 URL
- 脚本化 API
- （可选）其他 URL 参数（每个表）

***Figure 18: ServiceNow* 实例配置**



随后，Cisco Secure Workload 会发现来自 ServiceNow 实例和脚本化 REST API 的所有表（仅当启用了“包括脚本化 API”(Scripted APIs) 复选框时）。它向用户显示可供选择的表列表，一旦用户选择表，Cisco Secure Workload 会从该表中获取所有属性列表供用户选择。用户必须选择表中的 ip_address 属性作为键。随后，用户最多可以从表中选择 10 个唯一属性。有关每个步骤，请参阅下图。

Note ServiceNow 连接器只能支持与具有 **IP 地址 (IP Address)** 字段的表集成。

Note 要与 ServiceNow 脚本化 REST API 集成，您需要启用“脚本化 API”(Scripted APIs) 复选框，这将为您提供与其他表格类似的工作流程。

Note 要使脚本化 REST API 与 aServiceNow 连接器集成，脚本化 REST API 不能有路径参数。此外，脚本化 REST API 必须支持将 **sysparm_limit**、**sysparm_fields** 和 **sysparm_offset** 作为查询参数。

Note ServiceNow 用户角色必须包括用于表的 **cmdb_read** 和用于脚本化 REST API 的 **web_service_admin**，才能与思科 Cisco Secure Workload 集成。

Figure 19: 创建 ***ServiceNow*** 表配置

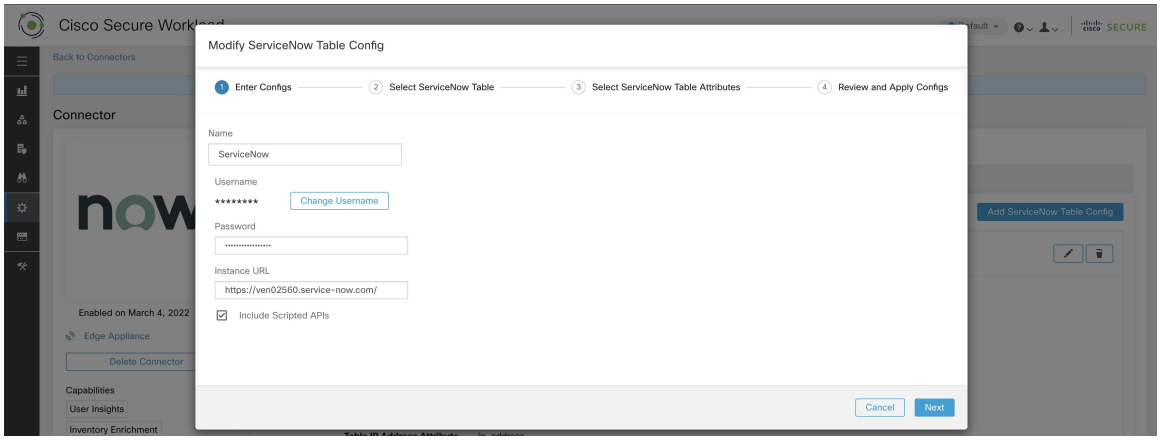


Figure 20: Cisco Secure Workload 从 ServiceNow 实例获取表信息

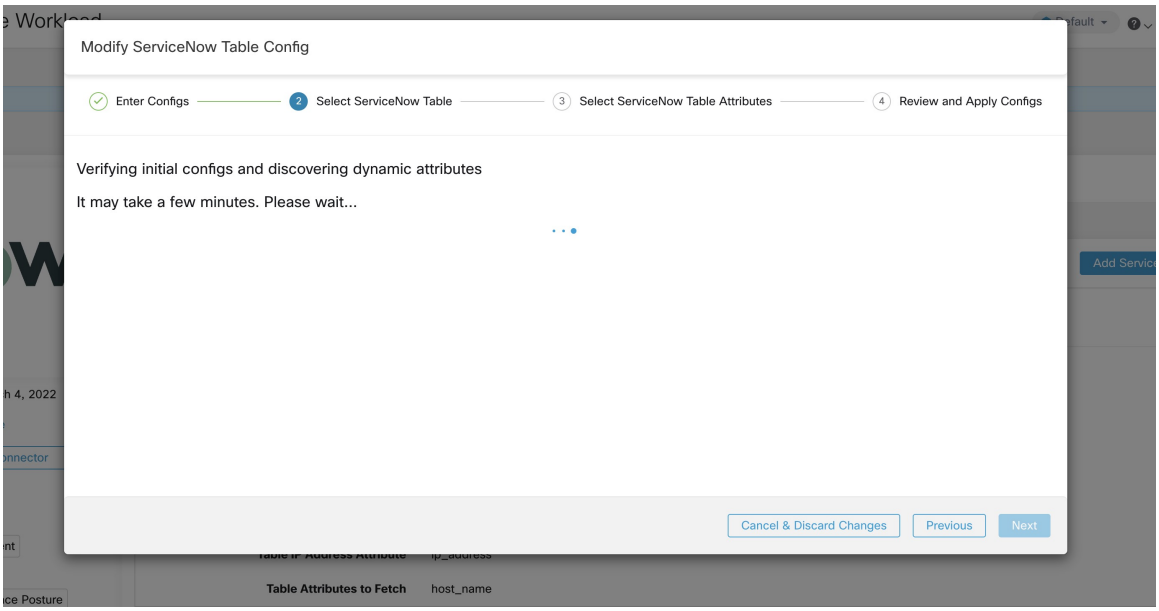


Figure 21: Cisco Secure Workload 显示表列表

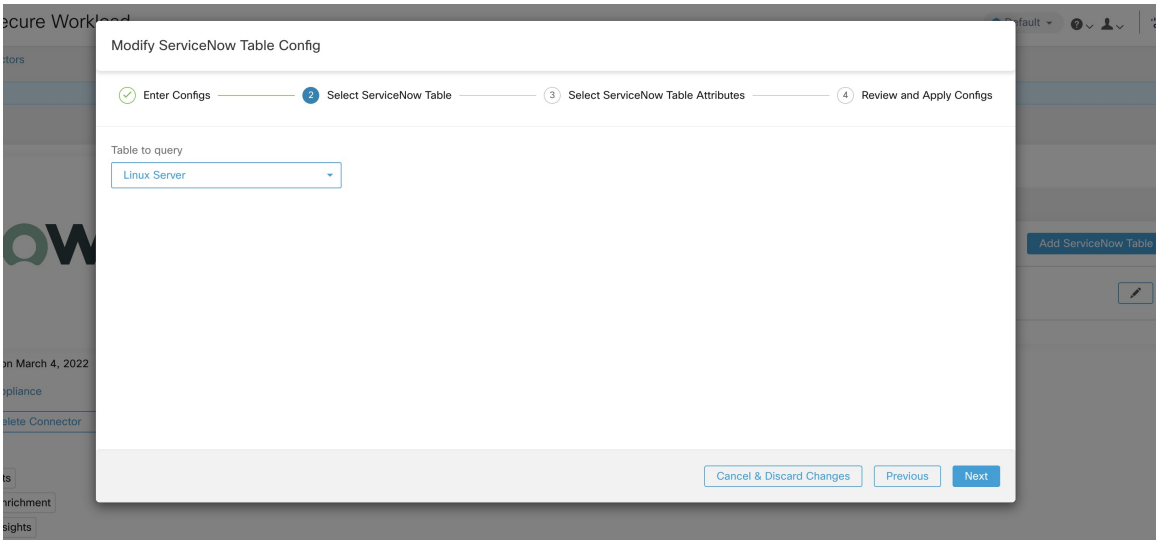


Figure 22: 选择 ***ServiceNow*** 表属性

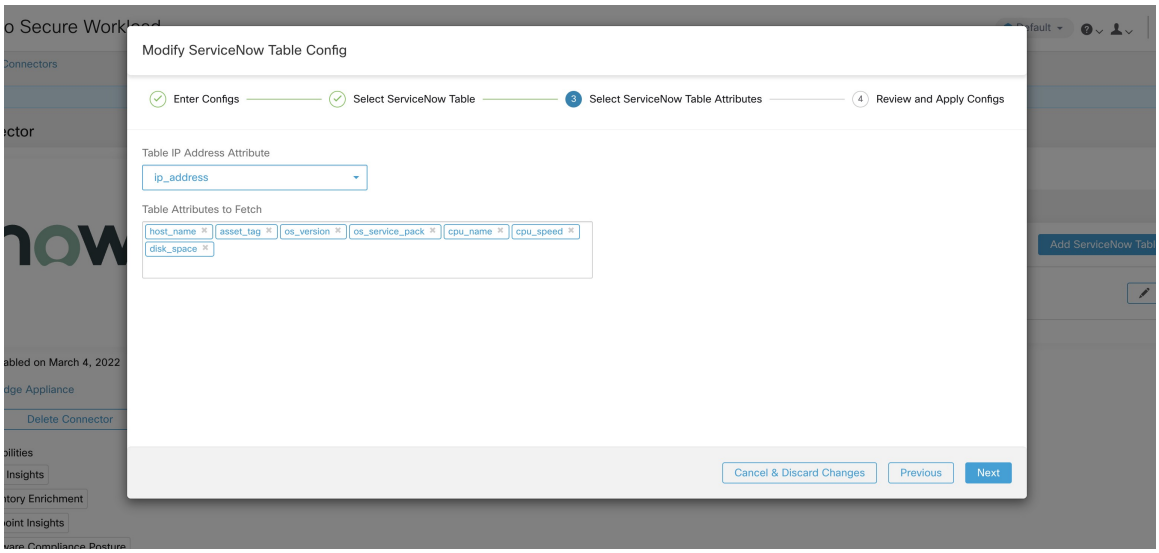
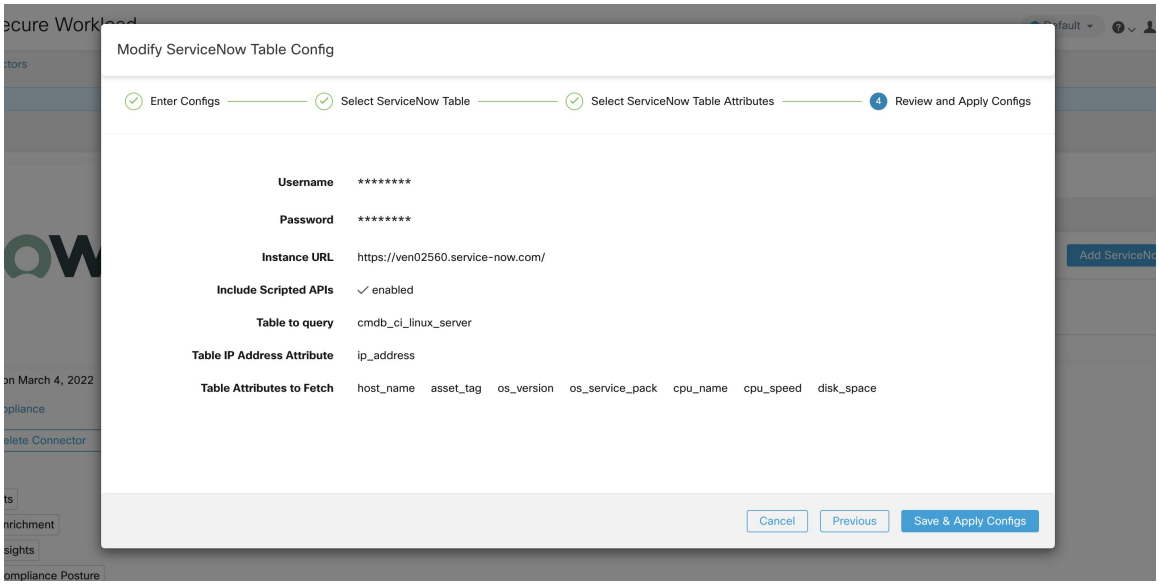


Figure 23: 查看并应用配置



处理 ServiceNow 记录

根据您在配置中提供的实例 URL，ServiceNow 连接器将连接到 ServiceNow 实例。ServiceNow 实例通过 `https://{Instance URL}/api/now/doc/table/schema` 来使用 HTTP 调用，以便从 ServiceNow 表 API 获取初始表架构。根据配置的表，它会查询这些表以获取 ServiceNow 标签/元数据。Cisco Secure Workload 会将 ServiceNow 标签注释到其资产中的 IP 地址。ServiceNow 连接器会定期获取新标签并更新 Cisco Secure Workload 资产。

Note Cisco Secure Workload 会定期从 ServiceNow 表获取记录。这可在 ServiceNow 连接器中的“同步间隔”(SyncInterval) 选项卡下进行配置。默认同步间隔为 60 分钟。如果与具有大量条目的 ServiceNow 表集成，同步间隔应设置为更高的值。

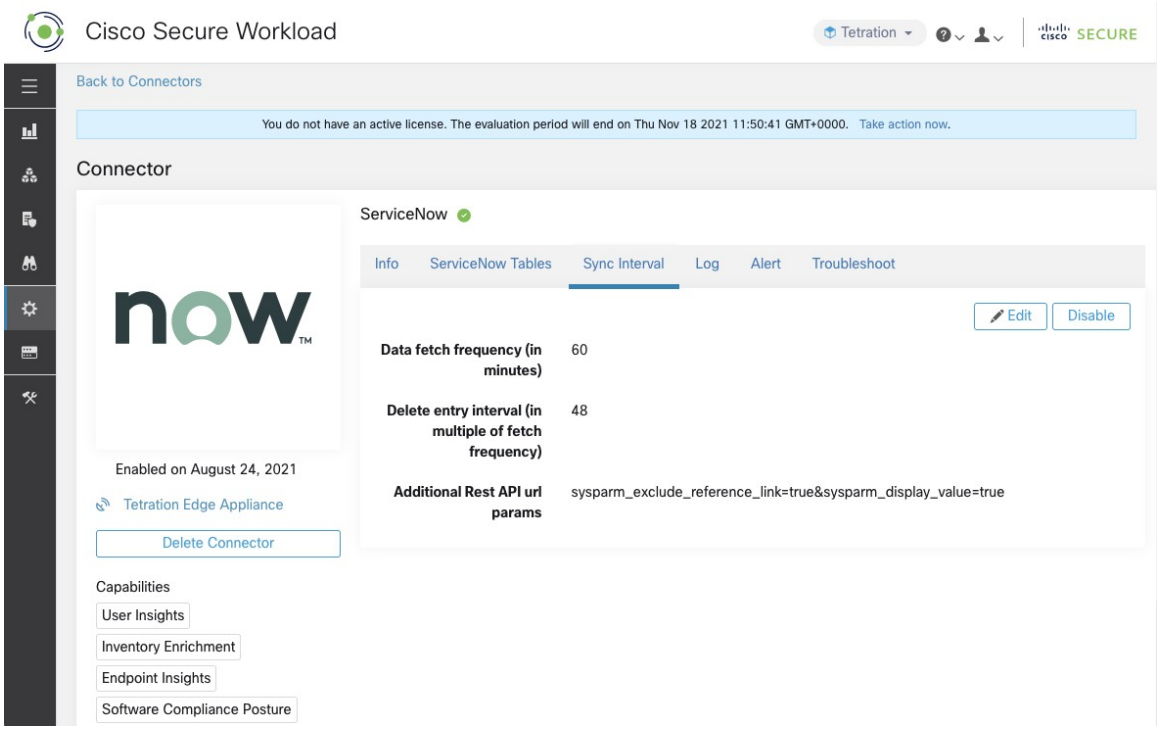
Note Cisco Secure Workload 将删除 10 个连续同步间隔内未见到的任何条目。如果与 ServiceNow 实例的连接长时间中断，则可能会导致该实例的所有标签被清理。

同步间隔配置

Cisco Secure Workload ServiceNow 连接器提供了一种配置 Cisco Secure Workload 与 ServiceNow 实例之间的同步频率的方法。默认情况下，同步间隔设置为 60 分钟，但可以在同步间隔配置下将其更改为**数据获取频率**。

- 为了检测记录的删除，Cisco Secure Workload ServiceNow 连接器依赖于来自 ServiceNow 实例的同步。如果在 48 个连续同步间隔内未看到某个条目，则我们会继续删除该条目。这可以在同步间隔配置下配置为**删除条目间隔**。
- 如果在调用 ServiceNow 表的 REST API 时需要传递任何其他参数，则可以将其配置为附加 Rest API url 参数的一部分。此配置为可选。例如，要从 ServiceNow 获取引用查找，请使用 **sysparm_exclude_reference_link=true&sysparm_display_value=true** URL 参数。

Figure 24: 同步间隔配置



与 Cisco Secure Workload 和 ServiceNow 的边缘设备通信流

在成功完成 Cisco Secure Workload ServiceNow 连接器集成和 ServiceNow 实例配置后，边缘虚拟机将通过如下所示的端口和 IP 地址与其通信：

- 边缘虚拟机通过从 Cisco Secure Workload 到 ServiceNow 的端口 443 与 ServiceNow 实例通信。使用的 IP 地址与 ServiceNow 实例上配置的相同。
- 边缘虚拟机通过端口 443 和 9092 与 Cisco Secure Workload 集群通信。使用的 Kafka 地址将与 Cisco Secure Workload 集群中为 Kafka-1、Kafka-2、Kafka-3、Kafka-1 FQDN 配置的地址相同。

注释 Cisco Secure Workload 集群不会发起与边缘虚拟机的连接。启动与集群连接的始终是边缘虚拟机。

用于删除标签的探索命令

如果用户想立即清理特定实例中某个 IP 的标签，而不等待删除间隔，则可以使用探索命令来完成。以下是运行命令的步骤。

1. 查找租户的 vrf ID
2. 开始探索命令 UI

3. 运行命令

查找租户的 VRF ID

站点管理员和**客户支持用户**可以访问窗口左侧导航栏中**平台 (Platform)** 菜单下的**租户 (Tenant)** 页面。此页面显示当前配置的所有租户和 VRF。有关详细信息，请参阅“租户”部分。

在租户页面上，租户表中的 ID 字段是租户的 vrf ID。

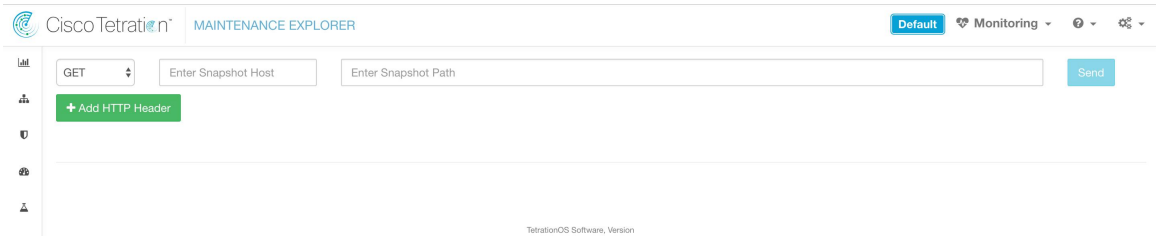
开始探索命令 UI

要访问维护资源管理器命令界面，请从 Cisco Secure Workload Web 界面的左侧导航栏中选择**故障排除 (Troubleshoot)** > **维护资源管理器 (Maintenance Explorer)**。

Note 需要具有客户支持权限才能访问探索菜单。如果未显示探索选项卡，则该帐户可能没有所需的权限。

点击下拉菜单中的探索选项卡，进入“维护资源管理器”(Maintenance Explorer) 页面。

Figure 25: *“维护资源管理器”(Maintenance Explorer)* 选项卡



运行命令

- 选择 `POST` 作为操作
- 输入 `orchestrator.service.consul` 作为快照主机
- 输入快照路径

  要珊瑚 `servicenow instance: servicenow_cleanup_annotations?args=<vrf-id> <ip_address> <instance_url> <table_name>` 的特定 IP 的标签
- 点击“发送”(Send)

注释 如果使用探索命令删除记录后，我们在 ServiceNow 实例中看到该记录显示，那么它将被重新填充

常见问题解答

- **如果 ServiceNow CMDB 表没有 IP 地址怎么办？**

  在这种情况下，建议在 ServiceNow 上创建一个视图，该视图将具有当前表中的所需字段以及 IP 地址（可能来自与另一个表的连接操作）。创建此类视图后，即可将其用于替代表名称。

- **如果 ServiceNow 实例需要 MFA，该怎么办？**

  目前，我们不支持与带有 MFA 的 ServiceNow 实例集成。

ServiceNow 连接器的限制

指标	限制
在一个 ServiceNow 连接器上配置的最大 ServiceNow 实例数	20
可以从一个 ServiceNow 实例获取的最大属性数	15
一个 Cisco Secure Workload 边缘设备上的最大 ServiceNow 连接器数	1
一个租户（根范围）上的最大 ServiceNow 连接器数	1
Cisco Secure Workload 上的最大 ServiceNow 连接器数	150

用于警报通知的连接器

警报通知连接器使 Cisco Secure Workload 能够在各种消息传递和日志记录平台上发布 Cisco Secure Workload 警报。这些连接器在 Cisco Secure Workload 边缘设备上的 TAN 服务上运行。

连接器	说明	已在虚拟设备上部署
系统日志	向系统日志服务器发送 Cisco Secure Workload 警报。	Cisco Secure Workload 边缘
邮件	通过邮件发送 Cisco Secure Workload 警报。	Cisco Secure Workload 边缘
Slack	在 Slack 上发送 Cisco Secure Workload 警报。	Cisco Secure Workload 边缘
Pager Duty	发送 Cisco Secure Workload 个有关 Pager Duty 的警报。	Cisco Secure Workload 边缘

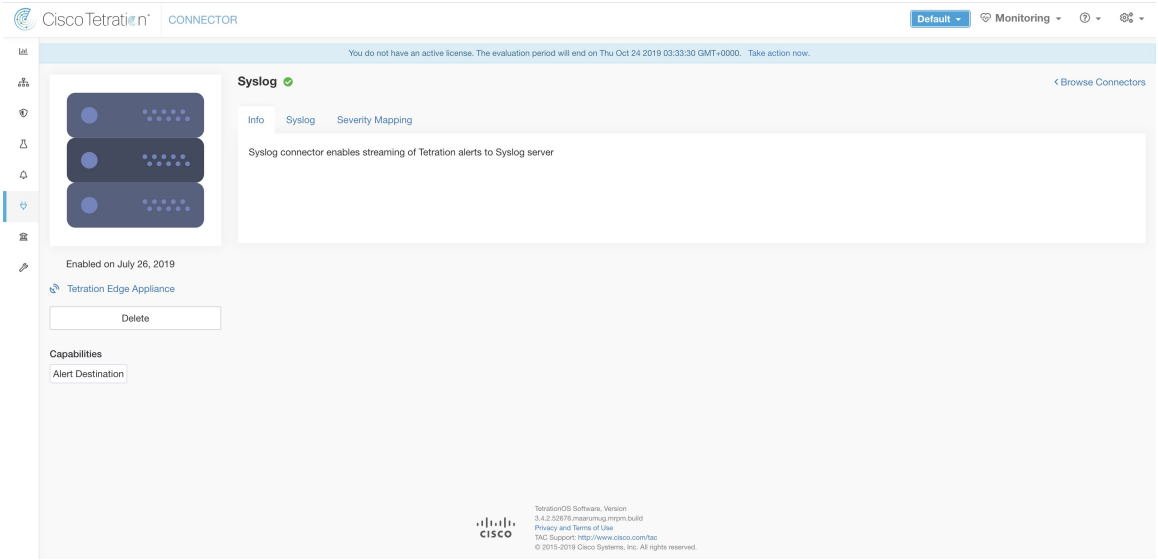
连接器	说明	已在虚拟设备上部署
Kinesis	在 Amazon Kinesis 上发送 Cisco Secure Workload 警报。	Cisco Secure Workload 边缘

有关所需虚拟设备的详细信息，请参阅连接器的虚拟设备。

系统日志连接器

启用后，Cisco Cisco Secure Workload 边缘设备上的 TAN 服务就可以使用配置向系统日志服务器发送警报。

Figure 26: 系统日志连接器



下表介绍了在系统日志服务器上发布 Cisco Secure Workload 警报的配置详细信息。有关详细信息，请参阅系统日志通知程序配置。

参数名称	类型	说明
协议	下拉菜单	用于连接到服务器的协议
	• *UDP*	
	• *TCP*	
服务器地址	字符串	系统日志服务器的 IP 地址或主机名
端口	数字	系统日志服务器的侦听端口。默认端口值为 514。

Figure 27: 系统日志连接器的配置示例

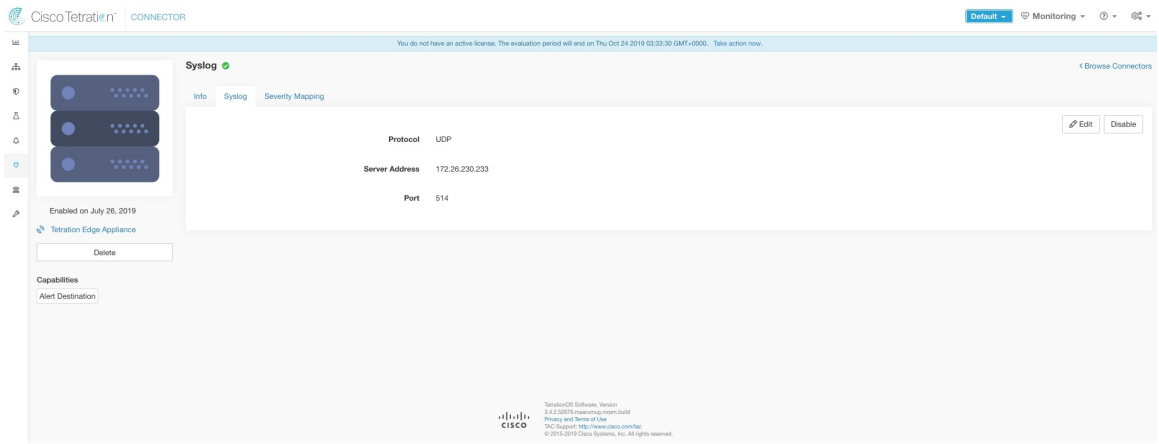


Figure 28: 示例警报

系统日志严重性映射

下表显示系统日志中 Cisco Secure Workload 警报的默认严重性映射。

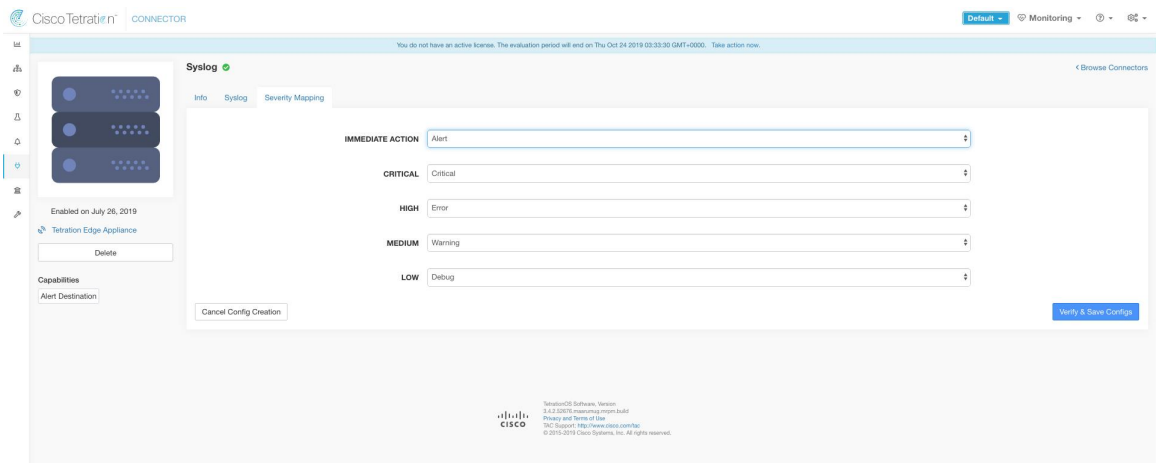
Cisco Secure Workload 警报严重性	系统日志严重性
LOW	LOG_DEBUG
中	LOG_WARNING
高	LOG_ERR
严重	LOG_CRIT

Cisco Secure Workload 警报严重性	系统日志严重性
IMMEDIATE ACTION	LOG_EMERG

可以使用“系统日志连接器”(Syslog Connector) 下的**严重性映射 (Severity Mapping)** 配置来修改此设置。您可以为每个 Cisco Secure Workload 警报严重性选择任何相应的系统日志优先级，并更改严重性映射。有关详细信息，请参阅系统日志严重性映射配置。

参数名称	映射下拉列表
IMMEDIATE_ACTION	• 紧急 • 警报 • 严重 • 错误 • 警告 • 通知 • 参考 • 调试
CRITICAL	
HIGH	
MEDIUM	
LOW	

Figure 29: 系统日志严重性映射配置示例。



限制

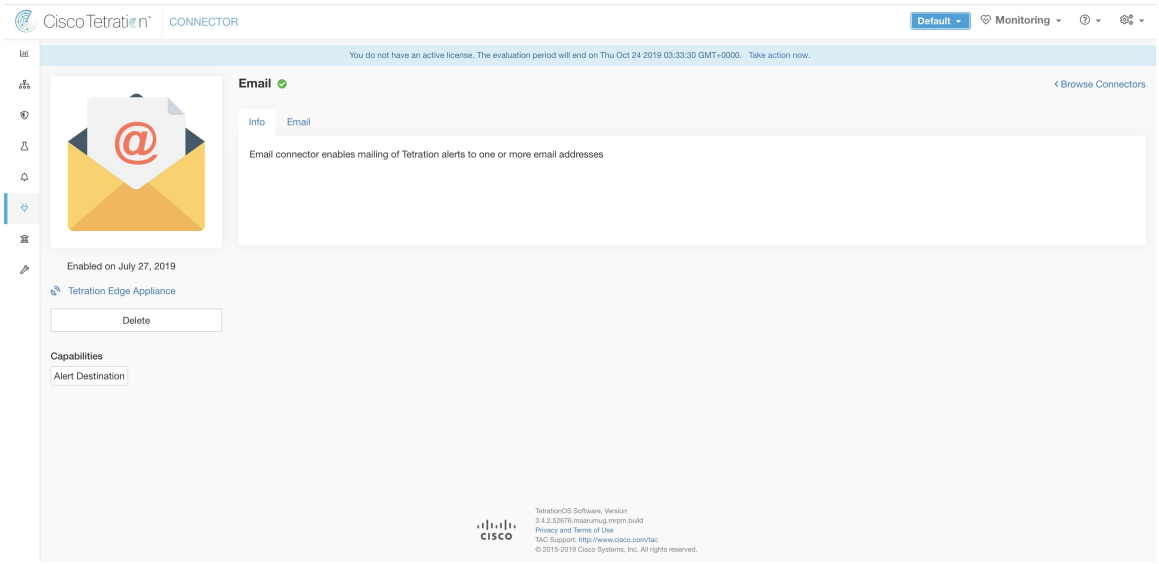
指标	限制
一个 Cisco Secure Workload 边缘设备上的最大系统日志连接器数	1
一个租户（根范围）上的最大系统日志连接器数	1

指标	限制
Cisco Secure Workload 上的最大系统日志连接器数	150

邮件连接器

启用后，Cisco Secure Workload 边缘设备上的 TAN 服务可以向给定配置发送警报。

Figure 30: 邮件连接器



下表介绍在邮件上发布 Cisco Secure Workload 警报的配置详细信息。有关详细信息，请参阅邮件通知程序配置。

Table 3: 邮件通知程序配置的更多详细信息

参数名称	类型	说明
SMTP Username	字符串	SMTP 服务器用户名。此参数可选。
SMTP Password	字符串	用户的 SMTP 服务器密码（如果已指定）。此参数可选。
SMTP Server	字符串	SMTP 服务器的 IP 地址或主机名
SMTP Port	数字	SMTP 服务器的侦听端口。默认值为 587。
Secure Connection	复选框	是否应将 SSL 用于 SMTP 服务器连接？

参数名称	类型	说明
From Email Address	字符串	用于发送警报的邮件地址
Default Recipients	字符串	以逗号分隔的收件人邮件地址列表

Figure 31: 邮件连接器的配置示例

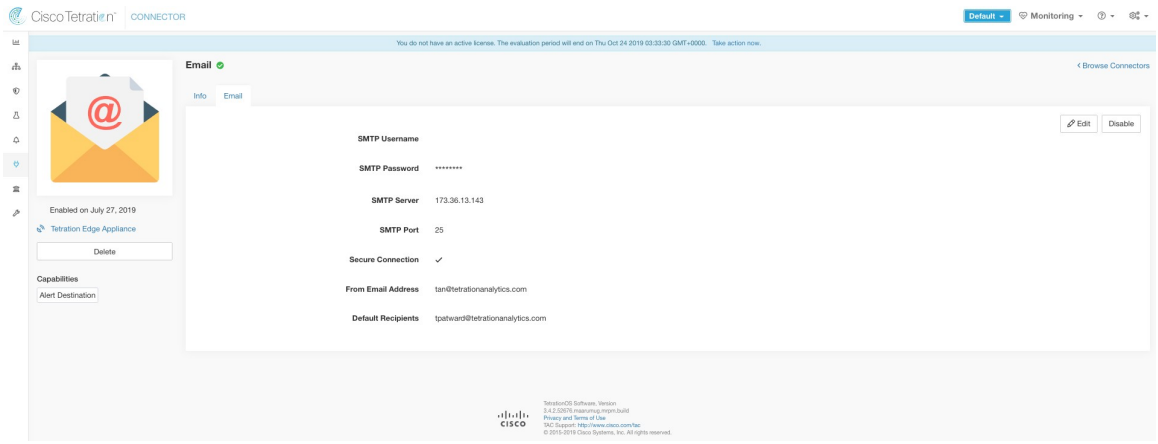
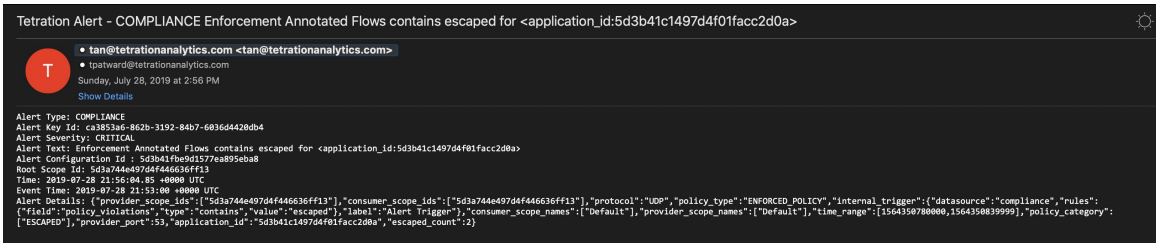


Figure 32: 示例警报



Note

- SMTP 用户名/密码为可选。如果未提供用户名，则会尝试在不进行任何身份验证的情况下连接到 SMTP 服务器。
- 如果未选中安全连接复选框，则会通过非安全连接发送警报通知。
- 默认收件人列表会被用于发送警报通知。如果警报配置中需要，可以根据警报覆盖此设置。

限制

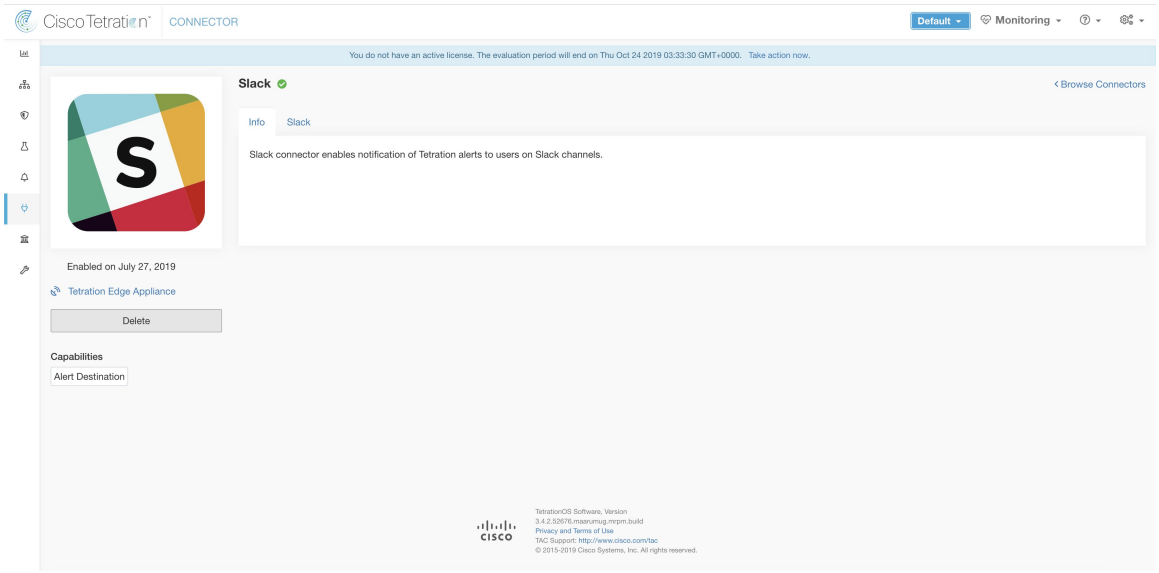
指标	限制
一个 Cisco Secure Workload 边缘设备上的最大邮件连接器数	1

指标	限制
一个租户（根范围）上的最大邮件连接器数	1
Cisco Secure Workload 上的最大邮件连接器数	150

Slack 连接器

启用后，Cisco Secure Workload 边缘设备上的 TAN 服务可以使用配置向 Slack 发送警报。

***Figure 33: Slack* 连接器**



下表介绍在 Slack 上发布 Cisco Secure Workload 警报的配置详细信息。有关详细信息，请参阅 Slack 通知程序配置。

参数名称	类型	说明
Slack Webhook URL	字符串	应在其上发布 Cisco Secure Workload 警报的 Slack Webhook

Note

- 要生成 Slack Webhook，请转到此处。

Figure 34: Slack 连接器的配置示例

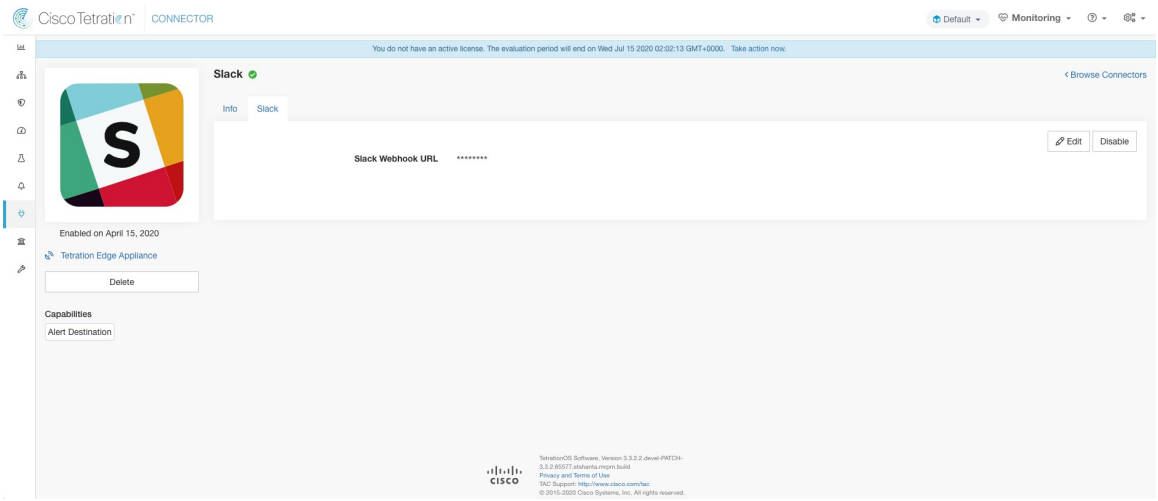
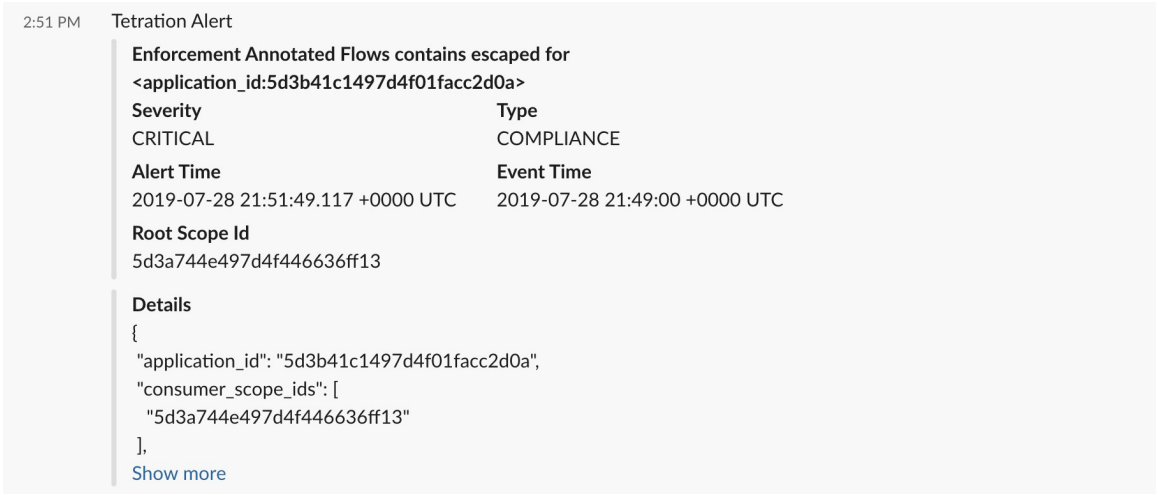


Figure 35: 示例警报



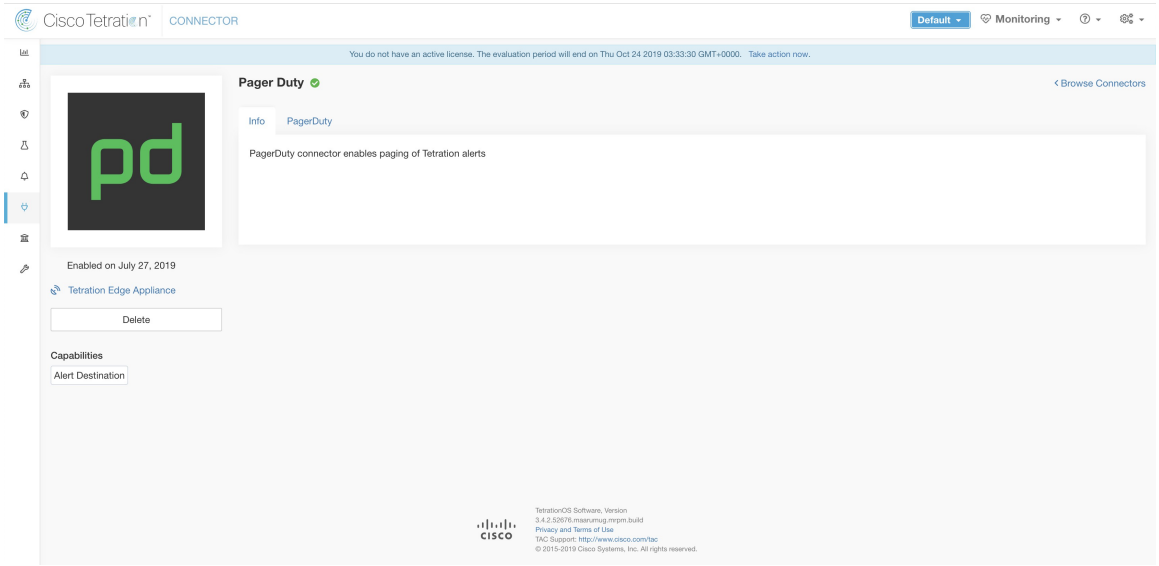
限制

指标	限制
一个 Cisco Secure Workload 边缘设备上的最大 Slack 连接器数	1
一个租户（根范围）上的最大 Slack 连接器数	1
Cisco Secure Workload 上的最大 Slack 连接器数	150

PagerDuty 连接器

启用后，Cisco Secure Workload 边缘设备上的 TAN 服务可以使用配置向 PagerDuty 发送警报。

***Figure 36: PagerDuty* 连接器**



下表介绍了在 PagerDuty 上发布 Cisco Secure Workload 警报的配置详细信息。有关详细信息，请参阅 PagerDuty 通知程序配置。

参数名称	类型	说明
PagerDuty 服务密钥	字符串	用于在 PagerDuty 上推送 Cisco Secure Workload 警报的 PagerDuty 服务密钥。

***Figure 37: PagerDuty* 连接器的配置示例**

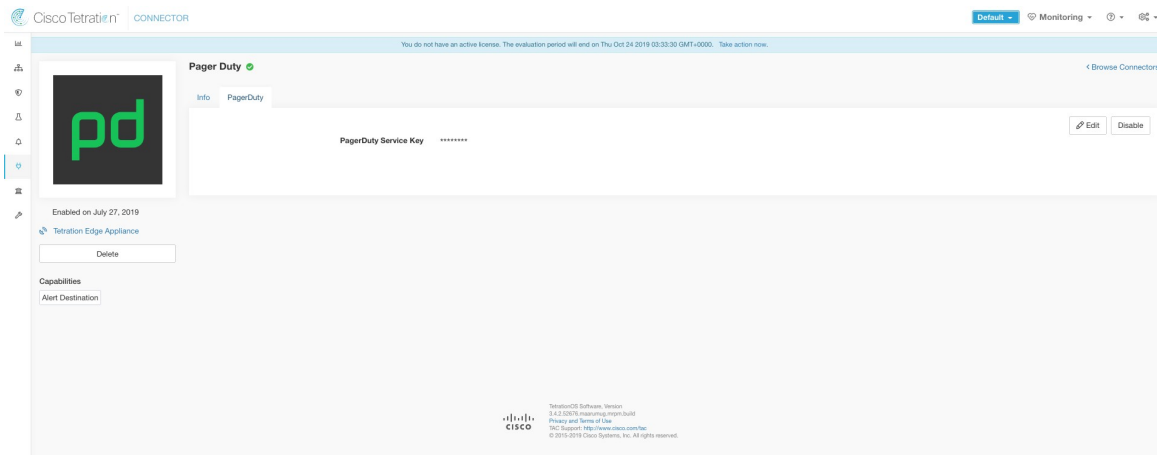
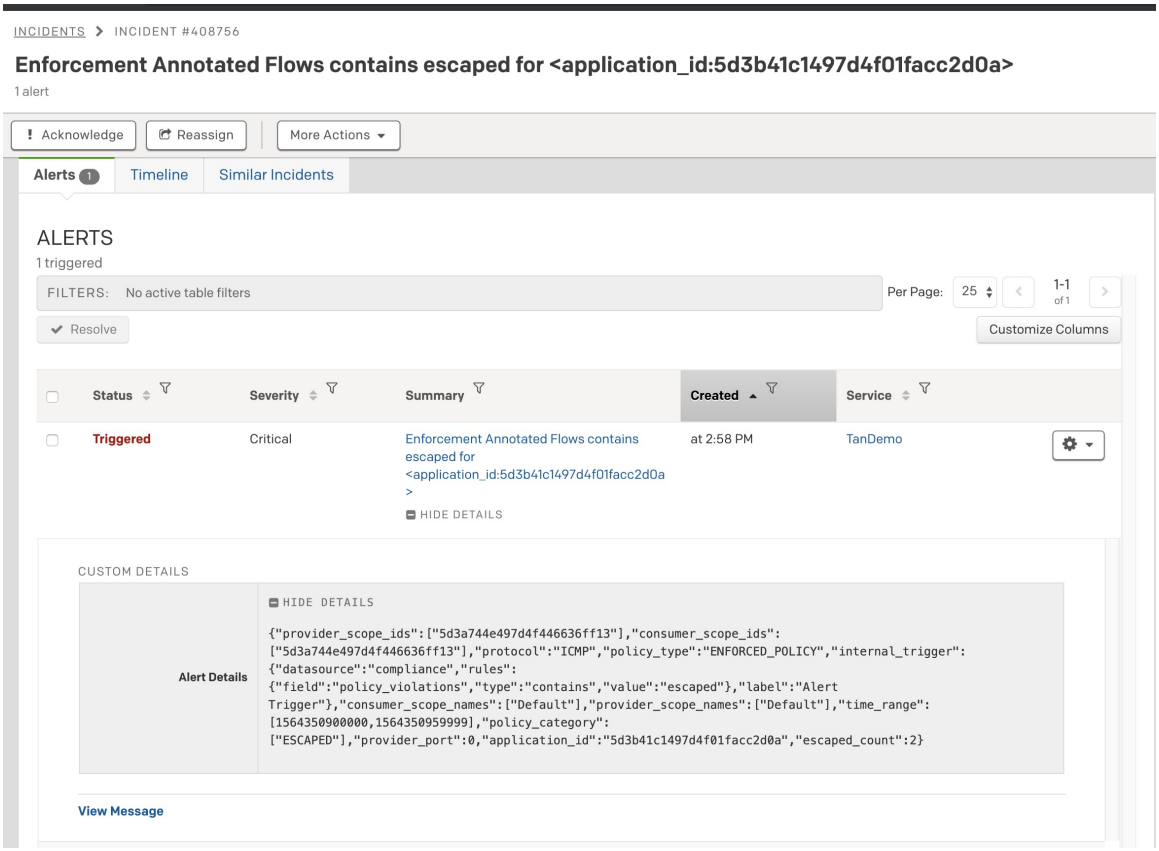


Figure 38: 示例警报



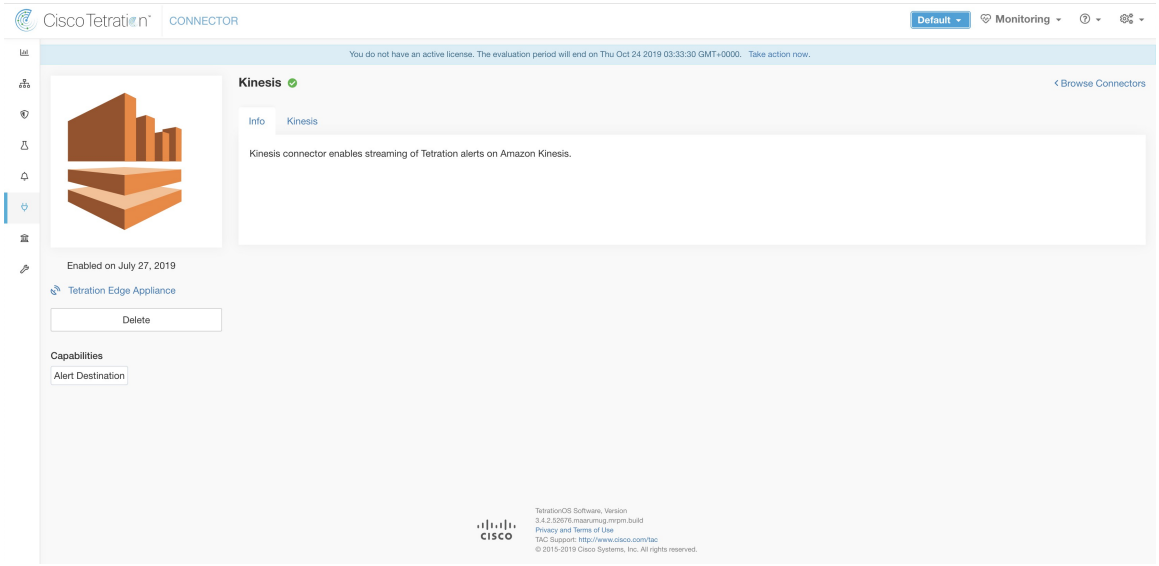
限制

指标	限制
一个 Cisco Secure Workload 边缘设备上的最大 PagerDuty 连接器数	1
一个租户（根范围）上的最大 PagerDuty 连接器数	1
Cisco Secure Workload 上的最大 PagerDuty 连接器数	150

Kinesis 连接器

启用后，Cisco Secure Workload 边缘设备上的 TAN 服务可以使用配置来发送警报。

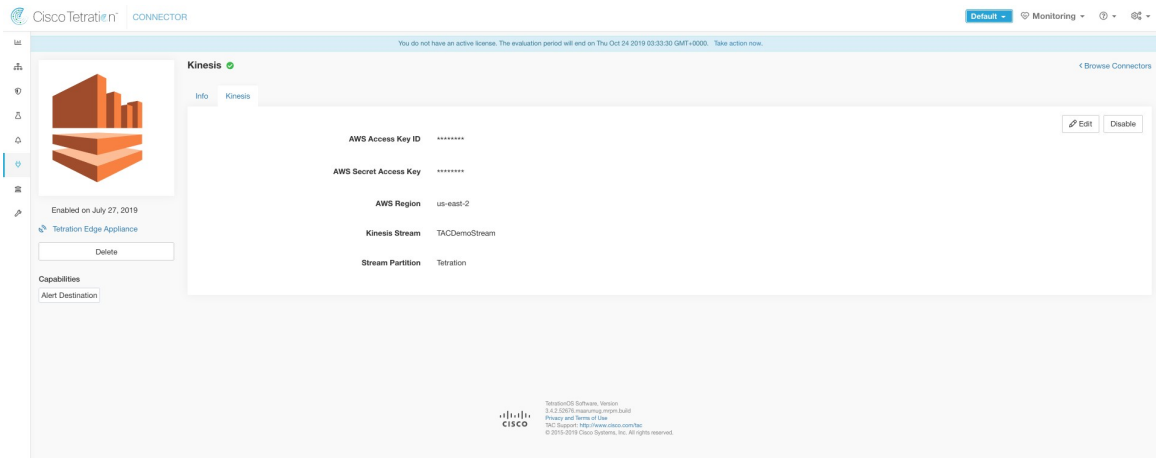
***Figure 39: Kinesis* 连接器**



下表介绍在 Amazon Kinesis 上发布 Cisco Secure Workload 警报的配置详细信息。有关详细信息，请参阅 Kinesis 通知程序配置。

参数名称	类型	说明
AWS 访问密钥 ID	字符串	用于与 AWS 通信的 AWS 访问密钥 ID
AWS 秘密访问密钥	字符串	用于与 AWS 通信的 AWS 访问密钥
AWS 区域	AWS 区域下拉列表	配置了 Kinesis 流的 AWS 区域的名称
Kinesis 流	字符串	Kinesis 流的名称
流分区	字符串	流的分区名称

Figure 40: Kinesis 连接器的配置示例。



限制

指标	限制
一个 Cisco Secure Workload 边缘设备上的最大 Kinesis 连接器数	1
一个租户（根范围）上的最大 Kinesis 连接器数	1
Cisco Secure Workload 上的最大 Kinesis 连接器数	150

云连接器

您可以在基于云的工作负载上使用用于 Cisco Secure Workload 功能的云连接器。

云连接器不需要使用虚拟设备。

连接器	支持的功能	已在虚拟设备上部署
AWS	对于 Amazon Web 服务 VPC： • 收集元数据（标签） • 收集流日志 • 执行分段策略 从弹性 Kubernetes 服务 (EKS) 集群： • 收集元数据	不适用

连接器	支持的功能	已在虚拟设备上部署
Azure	对于 Azure VNet： • 收集元数据（标签） • 收集流日志 • 执行分段策略 从 Azure Kubernetes 服务 (AKS) 集群： • 收集元数据	不适用
GCP	对于 Google Cloud 平台 VPC： • 收集元数据（标签） • 收集流日志 • 执行分段策略 从 Google Kubernetes Engine (GKE) 集群： • 收集元数据（标签）	不适用

AWS 连接器

Amazon Web 服务 (AWS) 连接器会与 AWS 连接，以执行以下高级功能：

- **从 AWS 虚拟私有云 (VPC) 自动注入资产及其标签** AWS 允许您以标签的形式将元数据分配给资源。Cisco Secure Workload 查询这些资源的标签，然后可将其用于资产和流数据可视化以及策略定义。此功能通过不断同步此数据来更新资源标签映射。

  注入来自 AWS VPC 的工作负载和网络接口的标签。如果同时配置工作负载和网络接口，则 Cisco Secure Workload 会合并并显示标记。有关详细信息，请参阅云连接器生成的标签。

- **注入 VPC 级别的流日志** 如果您已在 AWS 中设置 VPC 流日志用于监控目的，则 Cisco Secure Workload 可以通过读取相应的 S3 存储桶来注入流日志信息。您可以使用此遥测进行可视化和分段策略生成。

- **分段** 当分段选项启用时，Cisco Secure Workload 会使用 AWS 本地安全组来编程安全策略。为 VPC 启用执行后，相关策略会自动编程为安全组。

- **从 EKS 集群自动注入元数据** 在 AWS 上运行弹性 Kubernetes 服务 (EKS) 时，您可以选择收集与所有选定 Kubernetes 集群相关的所有节点、服务和 Pod 元数据。

您可以选择为每个 VPC 启用哪些功能。

Note 我们目前不支持中国地区。

AWS 的要求和前提条件

对于所有功能：在 AWS 中创建专用用户，或确定此连接器的现有 AWS 用户。连接器配置向导会生成一个 CloudFormation 模板 (CFT)，而您可以使用该模板向此用户分配所需的权限。确保您在 AWS 中具有上传此 CFT 的权限。

有关向专用用户授予跨 AWS 帐户访问权限，请参阅（可选）在 AWS 中配置跨 AWS 帐户访问, on page 67，包括所需的访问权限。

有关使用角色授予 AWS 帐户访问权限的信息，请参阅对 Cisco Secure Workload 集群的基于角色的访问。

每个 VPC 只能属于一个 AWS 连接器。一个 Cisco Secure Workload 集群可以有多个 AWS 连接器。收集配置新的 AWS 连接器 , on page 70 中的表中所述的信息。

此连接器不需要虚拟设备。

对于收集标签和资产：不需要其他前提条件。

对于注入流日志：需要 VPC 级别的流日志定义才能触发流日志收集。

只能注入 VPC 级别的流日志。

流日志必须发布到 Amazon Simple Storage Service (S3)；Cisco Secure Workload 无法从 Amazon CloudWatch 日志收集流数据。

如果创建连接器时提供的 AWS 用户帐户凭证可以访问 VPC 流量日志和 S3 存储桶，则 Cisco Secure Workload 可以从与任何帐户关联的 S3 存储桶中提取流日志。

流日志中需要包含以下属性：源地址、目标地址、源端口、目标端口、协议、数据包、字节、开始时间、结束时间、操作、TCP 标志、接口 ID、日志状态、流方向、数据包源地址和数据包目标地址。任何其他属性都将被忽略。

流日志必须同时捕获“允许”和“拒绝”的流量。

Note Cisco Secure Workload AWS 连接器支持每小时和每天对 VPC 流日志进行分区。

对于分段：启用分段需要启用收集标签。

在连接器中启用分段之前，请先备份现有的安全组，因为在为 VPC 启用分段时，所有现有规则都会被覆盖。

有关更多信息，请参阅对 AWS 资产执行分段策略时的最佳实践。

对于托管 Kubernetes 服务 (EKS)：如果启用 Kubernetes 选项，请参阅在 AWS 上运行的托管 Kubernetes 服务 (EKS) 部分中的EKS 的要求和前提条件，包括所需的访问权限。

（可选）在 AWS 中配置跨 AWS 帐户访问

如果给定用户凭证有权访问属于其他 AWS 帐户的 VPC，则这些凭证将可作为 AWS 连接器的一部分进行处理。

1. 指定的 Cisco Secure Workload 用户应具有以下 AWS 访问权限：

```
1. iam:GetPolicyVersion
2. iam:ListPolicyVersions
3. iam:ListAttachedUserPolicies
4. iam:GetUser
5. servicequotas:ListServiceQuotas
```

AWS 策略 JSON 示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:ListPolicyVersions",
        "iam:ListAttachedUserPolicies",
        "iam:GetUser",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 在指定的 Cisco Secure Workload 用户不是其一部分的所需 AWS 帐户中创建 AWS IAM 角色。
3. 允许由 Cisco Secure Workload 用户担任 AWS IAM 角色。这可以通过将 Cisco Secure Workload 用户 ARN 添加到 AWS IAM 角色信任策略来完成。

AWS IAM 角色信任策略 JSON 示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "AWS": <Secure Workload_user_arn>
            },
  "Action": "sts:AssumeRole",
  "Condition": {}
    }
  ]
}
```

4. 对 Cisco Secure Workload 用户不属于的所有所需 AWS 帐户执行步骤 2 和 3。
5. 创建具有权限的客户托管策略（不是内联策略），以从不同帐户代入所有已创建的 AWS 角色。

注释 在 AWS 连接器中，不支持客户内联策略。

托管策略 JSON 示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [<AWS_role_cross_account_1_arn>, <AWS_role_cross_account_2_arn>...]
    }
  ]
}
```

6. 将创建的客户托管策略附加到 Cisco Secure Workload 用户。
7. 连接器配置向导将提供一个 CloudFormation 模板。在将 CFT 按原样上传到指定的 Cisco Secure Workload 用户后，您将编辑模板并将编辑后的模板上传到 CloudFormation 门户，以便向 AWS IAM 角色授予所需的权限。有关详细信息，请参阅配置新的 AWS 连接器 ，第 70 页。

使用角色进行身份验证

基于用户的身份验证需要使用凭证密钥。如果未对凭证密钥进行适当管理，其敏感性可能会导致安全威胁。

使用基于角色的身份验证，您可以使用角色配置 AWS 帐户。连接器配置接受角色 ID (ARN) 并代入该角色，以便对客户的帐户执行特定操作。

基于角色的身份验证可降低未经授权访问的风险。

要访问基于角色的身份验证，请按照以下步骤操作：

过程

步骤 1 点击连接器配置页面中的**角色 (Role)** 选项卡。

步骤 2 注册集群。如果集群未注册，则显示消息“集群未注册，无法使用角色凭证”*(Cluster is not registered to use role credentials)*。下载提供的负载并联系客户服务代表。

步骤 3 在通知消息中，点击**下载**按钮并下载负载文件。

步骤 4 您可以使用通知消息中的链接联系 **TAC** 团队，然后提出请求并提供您已下载的文件。

步骤 5 注册集群后，系统会自动填充**外部 ID (External Id)** 和**用户 ARN (User ARN)**。

注释 刷新页面以查看外部 ID 和用户 ARN。

步骤 6 使用生成的**外部 ID** 和**用户 ARN** 更新角色信任关系。它允许承担角色。

JSON 文件的同一部分：

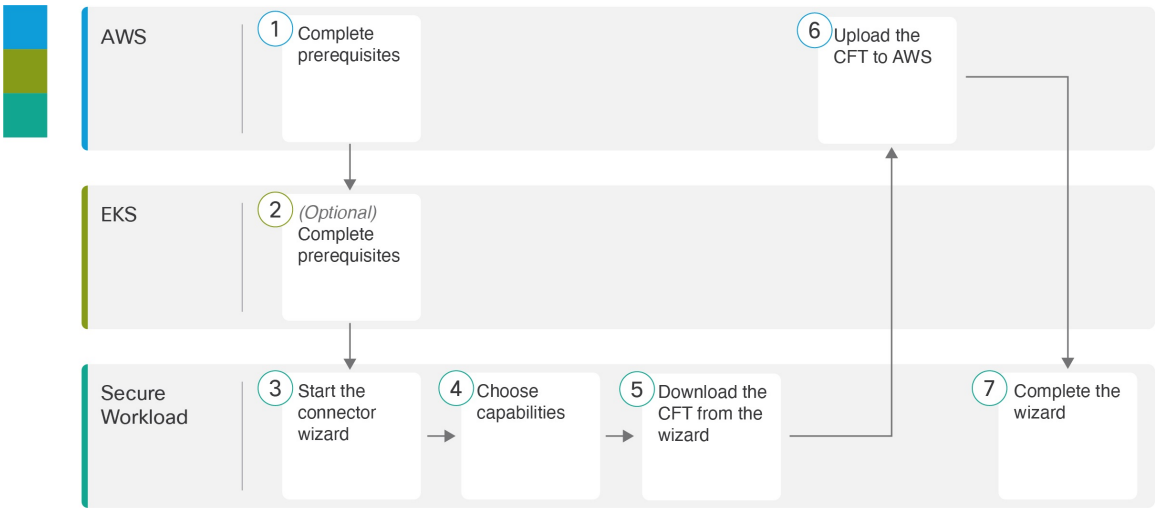
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "<User ARN>"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "<External Id>"
        }
      }
    }
  ]
}
```

步骤 7 完成上一步后，您可以从 AWS 帐户复制**角色 ARN**，并将其粘贴到 AWS 连接器配置页面中。

AWS 连接器配置概述

下图简要概述了连接器的配置过程。有关重要的详细信息，请参阅下一主题（配置新的 AWS 连接器 ，第 70 页。）

图 *41: AWS* 连接器配置概述



（请注意，图中的数字与详细程序中的步骤编号不对应。）

配置新的 AWS 连接器

过程

步骤 1 在导航窗格中，选择**管理 (Manage)** > **工作负载 (Workloads)** > **连接器 (Connectors)**。

步骤 2 点击 **AWS 连接器 (AWS Connector)**。

步骤 3 点击**生成模板 (Generate Template)**，然后选择所需的功能。

根据所选的功能，将生成 CloudFormation 模板 (CFT)。在 AWS CloudFormation 中使用生成的 CFT 模板为用户或角色创建策略。

要启用分段，还必须启用**收集标签**。

步骤 4 下载生成的 CloudFormation 模板 (CFT)。生成的 CFT 可同时用于用户和角色。

此模板具有上一步所选功能所需的 IAM 权限。

如果启用了 Kubernetes 选项，则必须单独为 EKS 配置权限。请参阅在 AWS (EKS) 上运行的托管 Kubernetes 服务，第 76 页。

步骤 5 将 CFT 上传到 AWS CloudFormation 门户，以便为用户分配此连接器的权限。确保 AWS 用户拥有所需的权限，然后才能继续 AWS 连接器的配置。

注释 无论您是否使用 AWS 跨帐户访问，我们都建议执行此任务。

您可以通过使用门户或 CLI 来应用 CFT。有关详情，请参阅：

- **门户**：AWS 管理控制台
- **CLI**：创建堆栈

上传 CFT 时，AWS 需要提供以下详细信息：

1. 策略的名称（可以是任何名称。例如，Cisco Secure Workload连接器）
2. 角色名：要向其应用 CFT 的 AWS IAM 角色的名称
3. 存储桶 ARN 和对象 ARN 列表（默认值：*）
4. 用户名：要向其应用 CFT 的 AWS 用户的名称
5. VPC ARN 列表（默认值：*）

   要输入特定的 VPC ARN 列表，请输入与特定 VPC 配对的安全组和网络接口资源，以便启用分段。

   1. `arn:aws:ec2:<region>:<account_id>:security-group/*`
   2. `arn:aws:ec2:<region>:<account_id>:network-interface/*`

   代码样本

   示例 1

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:us-east-1:123456789:security-group/*",
    "arn:aws:ec2:us-east-1:123456789:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

示例 2

```
{
   "Action": [
    "ec2:RevokeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateSecurityGroup",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:DeleteSecurityGroup",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateTags"
   ],
   "Resource": [
    "arn:aws:ec2:us-east-1:123456789:vpc/vpc-abcdef",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:network-interface/*"
   ],
   "Effect": "Allow"
  },
```

步骤 6 如果使用 AWS 基于角色的身份验证连接到 Cisco Secure Workload 连接器，请参阅 EKS 角色和访问权限部分。

步骤 7 如果使用 AWS 跨帐户访问，请执行以下附加步骤：

1. 您可以使用相同的上传 CFT 向角色/用户授予访问权限。如果您有多个帐户，请在每个帐户上使用相同的 CFT。
2. 将 CFT 上传到存在所需 IAM 角色的每个 AWS 帐户的 AWS CloudFormation 门户。

   您可以通过使用门户或 CLI 来应用 CFT，如上一步中所述。

   当您上传 CFT 时，AWS 会要求您提供以下信息：

   1. 策略的名称（可以是任何名称。例如，Cisco Secure Workload连接器）
   2. 存储桶 ARN 和对象 ARN 列表（默认值：*）
   3. 角色名：要向其应用 CFT 的 AWS IAM 角色的名称
   4. VPC ARN 列表（默认值：*）

步骤 8 点击**入门指南 (Getting started guide)**（推荐）或**在此处配置新连接器 (Configure your new connector here)** 按钮以配置连接器。

步骤 9 了解并满足 AWS、EKS 角色和访问权限以及对 AWS 资产执行分段策略时的最佳实践的AWS 的要求和前提条件，然后点击**开始 (Get Started)**。或者，如果您使用**在此处配置新连接器 (Configure your new connector here)** 按钮进行配置，则点击**是 (Yes)**。

步骤 10 为连接器命名并输入说明。

步骤 11 配置设置：

您可以使用其中一个选项连接到 AWS 帐户。

1. 凭证密钥
2. 角色

参数名称	属性	说明
凭证密钥	访问密钥	与具有上述 CFT 中所述权限的 AWS 用户关联的 ACCESS KEY ID。
	加密密钥	与上述 ACCESS KEY ID 关联的 SECRET KEY。
角色	外部 ID	它是自动生成的唯一标识符，用于授权访问 AWS 资源。用户使用它来为角色添加信任关系。
	用户 ARN	它是分配给 IAM 的自动生成的唯一标识符。用户使用它来为角色添加信任关系。
	ARN	分配给每个 AWS 资源的唯一标识符。
	HTTP 代理	（可选）Cisco Secure Workload 需要代理才能访问 AWS。
	全面扫描间隔	Cisco Secure Workload 刷新来自 AWS 的完整资产数据的频率。默认值及最小值为 3600 秒。
	Delta 扫描间隔	Cisco Secure Workload 从 AWS 获取资产数据的增量更改的频率。默认值及最小值为 600 秒。

步骤 12 点击“下一步”(Next)。

步骤 13 下一页显示**资源树**，用户可以在其中展开以查看各个区域，并且在该区域内，您可以选中或取消选中资源复选框，以从 AWS 获取 VPC 和 EKS 集群的列表。

步骤 14 从 VPC（虚拟网络）列表中，选择要为其启用所选功能的 VPC。

通常，您应尽快启用流注入，以便 Cisco Secure Workload 开始收集建议准确策略所需的足够数据。

请注意，由于 EKS 仅支持“收集标签”功能，因此没有提供明确的功能选择。选择 EKS 集群将隐式启用所支持的功能。对于启用此功能的每个集群，请输入**假设角色 ARN (Assume Role ARN)**（连接到 Cisco Secure Workload 时要代入的角色的 Amazon 资源编号。）

在 VPC 上**启用分段**将删除现有安全组，并提供对所有 VPC 的默认访问权限。

通常，在初始配置期间不应选择**启用分段 (Enable Segmentation)**。稍后，当您准备好对特定 VPC 执行分段策略时，可以编辑连接器并为这些 VPC 启用分段。请参阅“对 AWS 资产执行分段策略时的最佳实践”。

步骤 15 对于 EKS 集群，您可以通过提供 Assume Role ARN 访问 ID 来允许 AWS IAM 角色访问，从而连接到 AWS 连接器。

步骤 16 完成选择后，点击**创建 (Create)** 并等待几分钟以完成验证检查。

下一步做什么

如果您已启用收集标签、注入流数据和/或分段：

- 如果启用流注入，最多可能需要 25 分钟，流才会开始显示在**调查 (Investigate)** > **流量 (Traffic)** 页面上。
- （可选）要获得更丰富的流数据和其他优势，包括主机漏洞 (CVE) 的可视性，请在基于 VPC 的工作负载上为操作系统安装相应的代理。有关要求和详细信息，请参阅代理安装章节。
- 在成功配置 AWS 连接器以收集标签和注入流后，请按照标准流程构建分段策略。例如：允许 Cisco Secure Workload 收集足够的流数据以生成可靠的策略；定义或修改范围（通常每个 VPC 一个）；为每个范围创建工作空间；根据您的流数据自动发现策略，和/或手动创建策略；分析和优化您的策略；确保您的策略符合以下准则和最佳实践；准备就绪后，在工作空间中批准并执行这些策略。准备好为特定 VPC 执行分段策略后，返回连接器配置以便为 VPC 启用分段。有关详细信息，请参阅对 AWS 资产执行分段策略时的最佳实践，第 74 页。

如果您已启用 Kubernetes 托管服务 (EKS) 选项：

- 在基于容器的工作负载上安装 Kubernetes 代理。有关详细信息，请参阅代理部署一章中的 *Kubernetes/OpenShift* 代理 - 深度可视性和执行部分。

事件日志：

事件日志可用于通过不同的功能来了解每个连接器发生的重要事件。我们可以使用组件、命名空间、消息和时间戳等各种属性来对它们进行过滤。

编辑 AWS 连接器

您可以编辑 AWS 连接器，以便为特定 VPC 启用分段执行或进行其他更改。

在完成向导之前，更改不会被保存。

Procedure

步骤 1 从窗口左侧的导航栏中，选择**管理 (Manage)** > **工作负载 (Workloads)** > **连接器 (Connector)**。

步骤 2 点击 **AWS**。

步骤 3 如果有多个 AWS 连接器，请从窗口顶部选择要编辑的连接器。

步骤 4 点击**编辑连接器 (Edit Connector)**。

步骤 5 再次点击向导并进行更改。有关设置的详细说明，请参阅配置新的 AWS 连接器 , on page 70。

步骤 6 如果启用了不同的功能（收集标签、注入流、执行分段或收集 EKS 数据），则必须下载修订后的 CloudFormation 模板 (CFT) 并将其上传到 AWS，然后才能继续执行向导。

步骤 7 要启用分段策略的执行，请首先确保您已满足对 AWS 资产执行分段策略时的最佳实践中所述的建议前提条件。在列出 VPC 的页面上，为要启用执行的 VPC 选择**启用分段 (Enable Segmentation)**。

步骤 8 如果您已使用向导或手动为任何所选 VPC 创建范围，请点击**跳过此步骤 (Skip this step)** 以完成向导。

您可以使用**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 页面来手动编辑范围树。

步骤 9 如果您尚未为所选 VPC 创建任何范围，并且想要保留建议的层次结构，请从范围树上方选择父范围，然后点击**保存 (Save)**。

删除连接器和数据

如果删除连接器，该连接器已注入的数据不会被删除。

24 小时后，标签和库存会从活动库存中自动删除。

对 AWS 资产执行分段策略时的最佳实践

Warning 在任何 VPC 上启用分段执行之前，请在该 VPC 上创建安全组备份。为 VPC 启用分段会删除该 VPC 中的现有安全组。禁用分段不会恢复旧的安全组。

在创建策略时：

- 与所有被发现的策略一样，要确保有足够的流数据来生成准确的策略。
- 由于 AWS 在安全组中仅允许 ALLOW 规则，因此您的分段策略应仅包含 Allow 策略，但捕获全部策略除外，该策略应具有“拒绝”(Deny) 操作。

建议您在为关联的VPC启用分段之前，在工作空间中启用执行。如果您为未包含在已启用执行的工作空间中的 VPC 启用分段，则将允许该 VPC 上的所有流量。

当您准备好为 VPC 执行策略时，请编辑 AWS 连接器（请参阅编辑 AWS 连接器）并为该 VPC 启用分段。

查看 AWS 资产标签、详细信息和执行状态

要查看 AWS 连接器的摘要信息，请导航至连接器页面（管理 (Manage) > 连接器 (Connector)），然后从页面顶部选择连接器。有关更多详细信息，请点击 VPC 行。

要查看有关 AWS VPC 资产的信息，请点击“AWS 连接器”(AWS Connectors) 页面上的 IP 地址，以查看该工作负载的“资产配置文件”(Inventory Profile) 页面。有关资产配置文件的详细信息，请参阅资产配置文件。

有关标签的信息，请参阅：

- 云连接器生成的标签
- 与 Kubernetes 集群相关的标签

VPC 资产的具体策略会根据其 orchestrator_system/interface_id 标签值生成。您可以在“资产配置文件”(Inventory Profile) 页面上看到此信息。

要查看执行状态，请点击 Cisco Secure Workload 窗口左侧导航栏中的**防御 (Defend)** > **执行状态 (Enforcement Status)**。有关详细信息，请参阅“云连接器的执行状态”。

AWS 连接器问题故障排除

问题：“执行状态”(Enforcement Status) 页面显示已跳过某个具体策略。

解决方案：当安全组数量超过 AWS 连接器中配置的 AWS 限制时，就会发生这种情况。

当具体策略显示为“已跳过”(SKIPPED) 时，系统不会实施新的安全组，AWS 上以前存在的安全组仍然有效。

要解决此问题，请查看是否可以整合策略，例如在一个策略中使用较大的子网，而不是包含较小子网的多个策略。

如果您选择增加规则数量限制，必须先联系 Amazon，然后再更改 AWS 连接器配置中的限制。

背景：

启用分段时，系统会为每个 VPC 生成具体策略。这些具体策略用于在 AWS 中创建安全组。但是，AWS 和 Cisco Secure Workload 计数策略不同。将 Cisco Secure Workload 策略转换为 AWS 安全组时，AWS 会将每个唯一子网计为一个规则。

记帐示例：

请考虑以下示例 Cisco Secure Workload 策略：

出站：使用者地址集 -> 提供者地址集允许 TCP 端口 80、8080

AWS 将此策略计为 (提供者地址集中的唯一子网数) * (唯一端口数)。

因此，如果提供者地址集包含 20 个唯一子网，则此单个 Cisco Secure Workload 策略在 AWS 中计为 20（唯一子网数）* 2（唯一端口数）= 安全组中有 40 个规则。

请记住，由于 VPC 是动态的，规则计数也是动态的，因此计数为近似值。

问题：AWS 意外允许所有流量

解决方案：确保将 Cisco Secure Workload 中的捕获全部策略设置为“拒绝”(Deny)。

在 AWS (EKS) 上运行的托管 Kubernetes 服务

如果已在 AWS 云上部署 Amazon Elastic Kubernetes 服务 (EKS)，则可以使用 AWS 连接器从 Kubernetes 集群中提取资产和标签（EKS 标签）。

当 AWS 连接器配置为从托管 Kubernetes 服务提取元数据时，Cisco Secure Workload 会连接到集群的 API 服务器并跟踪该集群中节点、Pod 和服务的状态。有关使用此连接器收集和生成的 Kubernetes 标签，请参阅与 Kubernetes 集群相关的标签。

EKS 的要求和前提条件

- 验证您的 Kubernetes 版本是否支持。请参阅https://www.cisco.com/go/secure-workload/requirements/integrations。
- 在 EKS 中配置所需的访问权限，如下所述。

EKS 角色和访问权限

用户凭证和 AssumeRole（如适用）必须配置最低权限集。用户/角色必须在 aws-auth.yaml 配置映射中指定。可使用以下命令来编辑 aws-auth.yaml 配置映射。

```
$ kubectl edit configmap -n kube-system aws-auth
```

如果不使用 AssumeRole，则必须在 aws-auth.yaml 配置映射的“mapUsers”部分中添加用户和相应的组。如果指定了 AssumeRole ARN，则必须将角色添加到 aws-auth.yaml 配置映射的“mapRoles”部分中。下面提供了具有 AssumeRole 的 aws-auth.yaml 配置映射示例。

```
apiVersion: v1
data:
  mapAccounts: |
    []
  mapRoles: |
    - "groups":
      - "system:bootstrappers"
      - "system:nodes"
     "rolearn": "arn:aws:iam::938996165657:role/eks-cluster-20210114181445234700000000a"

      "username": "system:node:{{EC2PrivateDNSName}}"
    - "rolearn": arn:aws:iam::938996165657:role/BasicPrivilegesRole
      "username": secure.workload.read.only-user
      "groups":
        - secure.workload.read.only

  mapUsers: |
    []
kind: ConfigMap
metadata:
  creationTimestamp: "2021-01-14T18:14:47Z"
  managedFields:
  - apiVersion: v1
    fieldsType: FieldsV1
    fieldsV1:
      f:data:
        .: {}
        f:mapAccounts: {}
```

```
        f:mapRoles: {}
        f:mapUsers: {}
    manager: HashiCorp
    operation: Update
    time: "2021-01-14T18:14:47Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "829"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: 6c5a3ac7-58c7-4c57-a9c9-cad701110569
```

EKS 特定 RBAC 注意事项

创建集群角色与用户/服务帐户的集群角色绑定。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: csw-clusterrolebinging
subjects:
- kind: User
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: csw.read.only
  apiGroup: rbac.authorization.k8s.io
  kubectl create -f clusterrolebinding.yaml
clusterrolebinding.rbac.authorization.k8s.io/csw-clusterrolebinging created
```

有关 EKS 角色和访问权限的信息，请参阅“EKS 角色和访问权限”部分。

在 AWS 连接器向导中配置 EKS 设置

配置 AWS 连接器时，启用托管 Kubernetes 服务功能。请参阅配置新的 AWS 连接器 , on page 70。

每个 EKS 集群都需要“假设角色 ARN”。有关详细信息，请参阅：https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html

如果您使用 AWS 用户访问 EKS 集群，请允许该用户访问“假设角色”。

如果您使用的是跨帐户 IAM 角色，请允许 IAM 角色访问“假设角色”。

支持 EKS 负载均衡器

我们在 EKS 中添加了对负载均衡器服务的支持。CSW 代理在使用者主机和提供者主机/Pod 上执行规则。

EKS 负载均衡器有两个选项：

1. 保留客户端 IP。
2. 在提供者 Pod 上，生成
3. 目标类型。

在开始处理案例之前，对于以下策略意图：

对于各种情况，使用“允许”操作规则的使用者到提供者服务、服务协议和端口按如下方式生成：

支持案例	保留客户端	Target Type
1	打开	IP
2	打开	实例
3	熄灭	IP
4	熄灭	实例

案例 1：

在使用者节点上，我们使用使用者到负载均衡器服务 (lb ingress ip) 服务协议和端口允许来生成出口规则。

提供者节点上没有主机规则，但我们在提供者 Pod 上生成了一条输入规则，其中源为使用者，目标为提供者 Pod（任意），协议为目标协议，端口为目标端口，操作为允许。

案例 2：

在使用者节点上，我们使用使用者到负载均衡器服务 (lb ingress ip) 服务协议和端口允许来生成出口规则。

在提供者节点上，生成了一条预路由规则，其中源为使用者，目标为所有提供者节点，协议为服务协议，端口为服务的节点端口，操作为允许。

在提供者 Pod 上，我们生成一个入口规则，其中源为提供者节点，目标为提供者 Pod（任意），协议为目标协议，端口为目标端口，操作为允许。

案例 3：

在使用者节点上，我们使用使用者到负载均衡器服务 (lb ingress ip) 服务协议和端口允许来生成出口规则。

提供者节点上没有主机规则。在提供者 Pod 上，我们生成一个入口规则，其中源为 lb 入口 IP 的目标为提供者 Pod (any)，协议为目标协议，端口为目标端口，操作为允许。

案例 4：

在使用者节点上，我们使用使用者到负载均衡器服务 (lb ingress ip) 服务协议和端口允许来生成出口规则。

提供者节点生成预路由规则，将 lb 入口 IP 设置为源，并将所有提供者节点设置为目标。该规则将服务协议指定为协议，将服务的节点端口指定为端口，并将操作设置为允许。

在提供者 Pod 上，我们生成一个入口规则，其中源为提供者节点，目标为提供者 Pod（任意），协议为目标协议，端口为目标端口，操作为允许。

Azure 连接器

Azure 连接器与您的 Microsoft Azure 帐户连接，以执行以下高级功能：

- **从 Azure 虚拟网络 (VNet) 实时自动注入资产（及其标签）** Azure 允许您以标签的形式将元数据分配给资源。 Cisco Secure Workload 可以注入与虚拟机和网络接口关联的标签，然后可将其用

作 Cisco Secure Workload 中的标签，以实现资产和流数据可视化以及策略定义。此元数据会不断同步。

与连接器相关联的订用的工作负载和网络接口的标签会被注入。如果同时配置了工作负载和网络接口，则标记会合并并显示在 Cisco Secure Workload 中。有关详细信息，请参阅云连接器生成的标签。

- **注入流日志** 连接器可以注入您在 Azure 中为网络安全组 (NSG) 设置的流日志。然后，您可以使用 Cisco Secure Workload 中的此遥测数据来进行可视化和分段策略生成。
- **分段** 当为虚拟网络启用分段策略执行时，将使用 Azure 的本地网络安全组执行 Cisco Secure Workload 策略。
- **从 AKS 集群自动注入元数据** 在 Azure 上运行 Azure Kubernetes 服务 (AKS) 时，可以选择收集与所有选定 Kubernetes 集群相关的所有节点、服务和 pod 元数据。

您可以选择为每个 VNet 启用上述哪些功能。

Azure 连接器支持多个订用。

注释 目前不支持中国区域。

Azure 的要求和前提条件

对于所有功能：单个连接器可以处理多个订用。您需要一个订用 ID 来配置连接器。此订用 ID 可以是连接到连接器的许多订用 ID 之一。

在 Azure 中，使用 Azure Active Directory (AD) 创建/注册应用。您需要从此应用中获取以下信息：

- 应用（客户端）ID
- 目录（租户）ID
- 客户端凭证（可以使用证书或客户端密钥）
- 订用 ID

连接器配置向导将生成一个 Azure 资源管理器 (ARM) 模板，您可以使用该模板创建一个自定义角色，该角色应具有您选择启用的连接器功能所需的权限。这些权限将应用于您为连接器指定的订用中的所有资源。确保您在 Azure 中拥有上传此模板的权限。

如果需要连接，请确保有 HTTP 代理可用于此集成。

每个虚拟网络 (VNet) 只能属于一个 Azure 连接器。一个 Azure 帐户可以有多个 Azure 连接器。

此连接器不需要虚拟设备。

对于收集标签和资产：不需要其他前提条件。

对于注入流日志：每个虚拟网络 (VNet) 必须至少配置一个子网。

每个 VNet 下的每个子网都必须有一个与之关联的网络安全组 (NSG)。您可以将单个 NSG 与多个子网相关联。配置 NSG 时，您可以指定任何资源组。

只有符合 NSG 规则的流量才会包含在流日志中。因此，每个 NSG 应至少各有一条适用于任何源和任何目标的入站流量和出站流量规则，相当于Cisco Secure Workload 中的捕获全部规则。（默认情况下，NSG 将包括这些规则。）

每个 NSG 都必须启用流日志。

- Azure中需要一个存储帐户。在Azure中，需要启用存储帐户密钥访问才能成功集成。如果没有此配置，系统将无法连接，并会显示以下错误消息。

```
2024-05-01_01:30:39.10529 [ERROR] 2024-05-01T01:30:39.105 executor.go:225 (  16369)
6616eb5236f4590981ee2c0d error processing executo
rJobs: error fetching log

...
2024-05-01_01:30:39.10532 ===== RESPONSE ERROR
(ServiceCode=KeyBasedAuthenticationNotPermitted) =====
2024-05-01_01:30:39.10532 Description=Key based authentication is not permitted on this
 storage account.
2024-05-01_01:30:39.10532 RequestId:2cb0c2cb-b01e-006a-2c67-9bf9b8000000
2024-05-01_01:30:39.10532 Time:2024-05-01T01:30:39.0905677Z, Details:
2024-05-01_01:30:39.10532    Code: KeyBasedAuthenticationNotPermitted
```

- 流日志必须使用版本 2。
- 保留时间可以是 2 天（连接器每分钟都会提取一次新的流数据，两天的时间应该足够修复任何连接故障。）

对于分段：启用分段需要启用收集标签。

当您为虚拟网络 (VNet) 启用分段时，所有现有规则都将从与子网和属于这些子网的网络接口关联的 NSG 中删除。在连接器中启用分段之前，请备份子网和网络接口上现有的 NSG 规则。

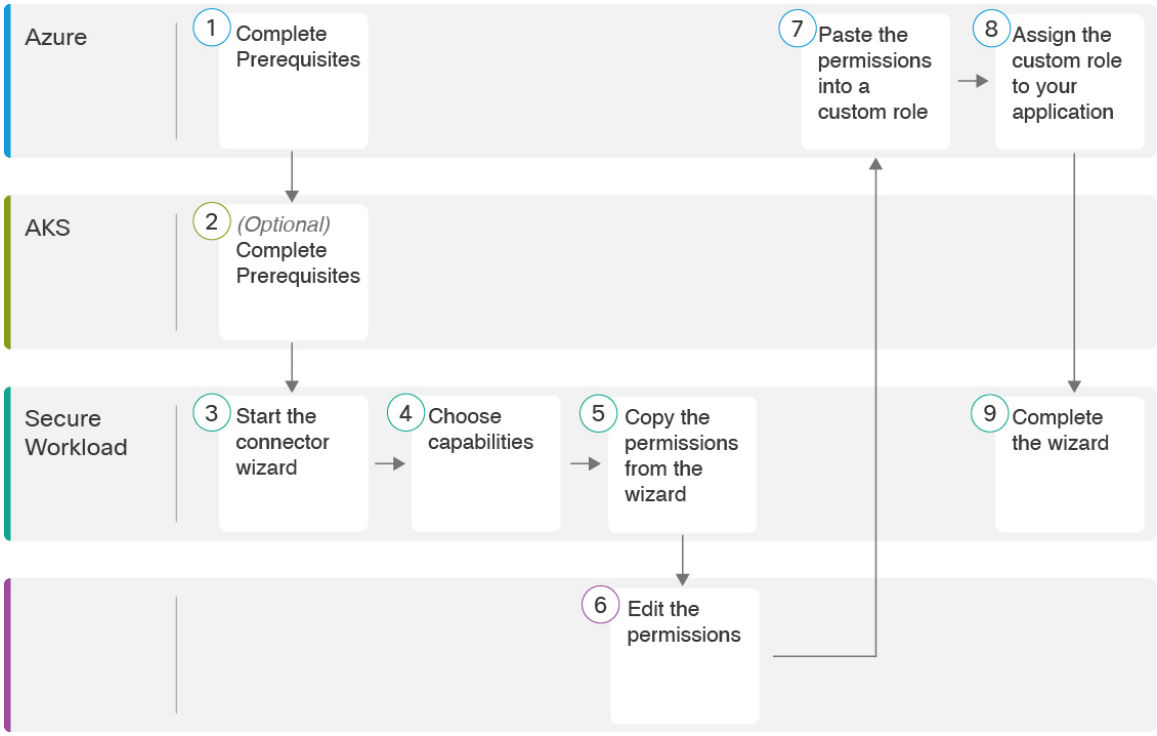
另请参阅下文的对 Azure 资产执行分段策略时的最佳实践，第 85 页。

对于托管 Kubernetes 服务 (AKS)：如果要启用 Kubernetes AKS 选项，请参阅下面“在 Azure 上运行的托管 Kubernetes 服务 (AKS)”部分中的要求和前提条件 。

Azure 连接器配置概述

下图简要概述了连接器的配置过程。有关基本详细信息，请参阅下一主题（配置 Azure 连接器）。

图 *42: Azure* 连接器配置概述



（请注意，图中的数字与详细程序中的步骤编号不对应。）

配置 Azure 连接器

过程

步骤 1 从窗口左侧的导航栏中，选择**管理 (Manage)** > **连接器 (Connectors)**。

步骤 2 点击 Azure 连接器。

步骤 3 点击第一个连接器（根范围内）的**启用 (Enable)**，或点击同一根范围内的其他连接器的**启用另一个 (Enable Another)**。

步骤 4 了解并满足要求和前提条件中的Azure 的要求和前提条件，然后点击“开始”(Get Started)。

步骤 5 为连接器命名并选择所需的功能：

您在此页面上所做的选择仅用于确定将在下一步中生成的 Azure 资源管理器 (ARM) 模板中包含的权限，并显示需要配置的设置。

要启用分段，还必须启用**收集标签 (Gather Labels)**。

在此页面上启用分段本身不会启用策略执行或影响现有网络安全组。仅当稍后在向导中为单个 VNet 启用分段时，才会执行策略执行和删除现有安全组。您可以稍后返回到此向导，为各个 VNet 启用分段策略执行。

步骤 6 点击**下一步 (Next)** 并阅读配置页面上的信息。

步骤 7 您的订用必须具有所需的权限，然后才能继续向导中的下一页。

要使用提供的 Azure 资源管理器 (ARM) 模板为连接器分配所需的权限，请执行以下操作：

1. 从向导下载 ARM 模板。
2. 编辑模板文本，以便将 **<subscription_ID>** 替换为您的 订用 ID。

   注释 对于连接器，您可以在 Azure 帐户中创建多个订用 ID。

   您可以输入多个订用 ID，其中凭证属于同一订用 ID。

3. 在 Azure 中，在适用的订用中创建自定义角色。
4. 在自定义角色表单中，对于基准权限，选择**从头开始 (Start from scratch)**。
5. 在自定义角色创建表单的 JSON 选项卡中，粘贴从连接器向导下载的已编辑文件中的文本。
6. 保存自定义角色。
7. 将自定义角色附加到您在此程序的前提条件中配置的应用。

此模板具有您在上一步中选择的功能所需的 IAM 权限。

如果启用了 Kubernetes 托管服务选项，则必须单独为 AKS 配置权限。请参阅在 Azure 上运行的托管 Kubernetes 服务 (AKS)，第 85 页。

步骤 8 配置设置：

属性	说明
订用 ID	与此连接器关联的 Azure 订用的 ID。
ClientID	您在 Azure 中为此连接器创建的应用的**应用（客户端）ID**。
TenantID	您在 Azure 中为此连接器创建的应用的**目录（租户）ID**。
客户端密钥或客户端证书	对于身份验证，可以使用客户端密钥或客户端证书和密钥。从您在 Azure 中为此连接器创建的应用中的**客户端凭证**链接获取。如果使用证书：证书应未加密。仅支持 RSA 证书。私钥可以是 PKCS1 或 PKCS8。
HTTP 代理	Cisco Secure Workload 需要使用代理才能访问 Azure。支持的代理端口：80、8080、443 和 3128。
全面扫描间隔	Cisco Secure Workload 会从 Azure 刷新完整资产数据的频率。默认值及最小值为 3600 秒。

属性	说明
Delta 扫描间隔	Cisco Secure Workload 从 Azure 获取资产数据增量变化的频率。默认值及最小值为 600 秒。

步骤 9 点击**下一步 (Next)**。系统可能需要几分钟才能从 Azure 获取 VNet 和 AKS 集群的列表。

步骤 10 从每个 VNet 的 VNet 和 AKS 集群列表中，选择要为其启用所选功能的 VNet 和 AKS 集群。

通常，您应尽快启用流注入，以便 Cisco Secure Workload 开始收集足够的数据来建议准确的策略。

请注意，由于 AKS 仅支持“收集标签”功能，因此没有提供明确的功能选择。选择 AKS 集群将隐式启用所支持的功能。为启用此功能的每个集群上传客户证书和密钥。

通常，在初始配置期间不应选择**启用分段 (Enable Segmentation)**。稍后，当您准备好对特定 VNet 执行分段策略时，可以编辑连接器并为这些 VNet 启用分段。请参阅对 Azure 资产执行分段策略时的最佳实践，第 85 页。

步骤 11 完成选择后，点击**创建 (Create)** 并等待几分钟以完成验证检查。

“查看组”(View Groups) 页面将显示您为上一页面上的任何功能启用的所有 VNet（按区域分组）。每个区域以及每个区域中的每个 VNet 都是一个新范围。

步骤 12 （可选）选择要在其下添加新范围集的父范围。如果尚未定义任何范围，则唯一的选择是默认范围。

步骤 13 （可选）要接受在向导中配置的所有设置（包括层次结构范围树），请点击**保存 (Save)**。

要接受层次结构范围树之外的所有设置，请点击**跳过 (Skip)** 以跳过此步骤。

您可以稍后在**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 下手动创建或编辑范围树。

下一步做什么

如果您已启用收集标签、注入流数据和/或分段：

- 如果启用了流注入，最多可能需要 25 分钟，流才会开始显示在**调查 (Investigate)** > **流量 (Traffic)** 页面上。
- （可选）要获得更丰富的流数据和其他优势，包括主机漏洞 (CVE) 的可视性，请在基于 VNet 的工作负载上为操作系统安装相应的代理。有关要求和详细信息，请参阅代理安装章节。
- 在成功配置 Azure 连接器以收集标签和注入流后，请按照标准流程构建分段策略。例如：允许 Cisco Secure Workload 收集足够的流数据以生成可靠的策略；定义或修改范围（通常每个 VNet 一个）；为每个范围创建工作空间；根据您的流数据自动发现策略，和/或手动创建策略；分析和优化您的策略；确保您的策略符合以下准则和最佳实践；准备就绪后，在工作空间中批准并执行这些策略。准备好为特定 VNet 执行分段策略后，返回连接器配置以便为 VNet 启用分段。有关详细信息，请参阅对 Azure 资产执行分段策略时的最佳实践，第 85 页。

如果您已启用 Kubernetes 托管服务 (AKS) 选项：

- 在基于容器的工作负载上安装 Kubernetes 代理。有关详细信息，请参阅代理部署一章中的安装 Kubernetes 或 OpenShift 代理以实现深度可视性和执行。

事件日志：

事件日志可用于通过不同的功能来了解每个连接器发生的重要事件。我们可以使用组件、命名空间、消息和时间戳等各种属性来对它们进行过滤。

编辑 Azure 连接器

您可以编辑 Azure 连接器，以便为特定 VNet 启用分段执行或进行其他更改。

在完成向导之前，更改不会被保存。

过程

步骤 1 从窗口左侧的导航栏中，选择**管理 (Manage)** > **连接器 (Connectors)**。

步骤 2 点击 **Azure**。

步骤 3 如果有多个 Azure 连接器，请从窗口顶部选择要编辑的连接器。

步骤 4 点击**编辑连接器 (Edit Connector)**。

步骤 5 再次点击向导并进行更改。有关设置的详细说明，请参阅配置 Azure 连接器，第 81 页。

步骤 6 如果启用了不同的功能（收集标签、注入流、执行分段或收集 AKS 数据），则必须下载修订后的 ARM 模板，编辑新模板文本以指定订用 ID，并将新模板上传到在 Azure 中创建的自定义角色，然后再继续向导操作。

步骤 7 要启用分段策略执行，请首先确保您已满足对 Azure 资产执行分段策略时的最佳实践，第 85 页中所述的建议前提条件。然后，在列出 VNet 的向导页面上，为要启用执行的 VNet 选择**启用分段 (Enable Segmentation)**。

步骤 8 如果您已使用向导或手动为任何所选 VNet 创建范围，请点击**跳过此步骤 (Skip this step)** 以完成向导。

您可以使用**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 页面来手动编辑范围树。

步骤 9 如果尚未为所选 VNet 创建任何范围，并且想要保留建议的层次结构，请从范围树上方选择父范围，然后点击**保存 (Save)**。

删除连接器和数据

如果删除连接器，该连接器已注入的数据不会被删除。

24 小时后，标签和库存会从活动库存中自动删除。

对 Azure 资产执行分段策略时的最佳实践

警告 在任何 VNet 上启用分段执行之前，请在该 VNet 上创建网络安全组的备份。为 VNet 启用分段功能会删除与该虚拟网络关联的网络安全组中的现有规则。禁用分段不会恢复旧的网络安全组。

创建策略时：与所有发现的策略一样，确保有足够的流数据来生成准确的策略。

建议您在为关联的VNet启用分段之前，在工作空间中启用执行。如果为已启用执行的工作空间中未包含的 VNet 启用分段，则该 VNet 上将允许所有流量。

当您准备好为 VNet 执行策略时，请编辑 Azure 连接器（请参阅编辑 Azure 连接器，第 84 页）并为该 VNet 启用分段。

请注意，如果子网没有与之关联的网络安全组，Cisco Secure Workload 不会在该子网上执行分段策略。在 VNet 上执行分段策略时，子网级别的 NSG 将更改为允许所有流量，Cisco Secure Workload 策略将覆盖接口级别 NSG。如果接口的 NSG 尚不存在，则会为该接口自动创建 NSG。

查看 Azure 资产标签、详细信息和执行状态

要查看 Azure 连接器的摘要信息，请导航至连接器页面（“管理”(Manage) > “连接器”(Connectors)），然后从页面顶部选择连接器。有关更多详细信息，请点击 VNet 行。

要查看有关 Azure VNet 资产的信息，请点击“Azure 连接器”(Azure Connectors) 页面上的 IP 地址，以查看该工作负载的“资产配置文件”(Inventory Profile) 页面。有关资产配置文件的详细信息，请参阅资产配置文件。

有关标签的信息，请参阅：

- 云连接器生成的标签
- 与 Kubernetes 集群相关的标签

VNet 资产的具体策略会根据其 orchestrator_system/interface_id 标签值生成。您可以在“资产配置文件”(Inventory Profile) 页面上看到此信息。

要查看执行状态，请点击 Cisco Secure Workload 窗口左侧导航栏中的**防御 (Defend)** > **执行状态 (Enforcement Status)**。有关详细信息，请参阅“云连接器的执行状态”。

Azure 连接器问题故障排除

问题：Azure 意外允许所有流量

解决方案：确保将 Cisco Secure Workload 中的捕获全部策略设置为“拒绝”(Deny)。

在 Azure 上运行的托管 Kubernetes 服务 (AKS)

如果已在 Azure 云上部署 Azure Kubernetes 服务 (AKS)，则可以使用 Azure 连接器从 Kubernetes 集群动态提取资产和标签（AKS 标签）。

当 Azure 连接器配置为从托管 Kubernetes 服务提取元数据时，Cisco Secure Workload 会跟踪该集群中节点、Pod 和服务的状态。

有关使用此连接器收集和生成的 Kubernetes 标签，请参阅与 Kubernetes 集群相关的标签。

AKS 的要求和前提条件

- 验证您的 Kubernetes 版本是否支持。请参阅适用于 Cisco Secure Workload 代理的操作系统、外部系统和连接器的兼容性矩阵。
- 配置 Azure 连接器时，启用并配置托管 Kubernetes 服务 (AKS) 功能。有关详细信息，请参阅配置 Azure 连接器。

支持 AKS 负载均衡器

AKS 支持保留客户端 IP。

对于以下策略意图：

对于各种情况，使用“允许”操作规则生成的使用者到提供者服务、服务协议和端口如下：

支持案例	保留客户端
1	打开
2	熄灭

案例 1：保留客户端 IP 为**开**。

在使用者节点上，我们使用使用者到负载均衡器服务 (lb 入口 IP) 服务协议和端口允许生成出口规则。

为提供者节点生成的预路由规则，将使用者指定为源节点，将所有提供者节点指定为目标节点。该规则包括作为协议的服务协议和作为端口的服务节点端口，并将操作设置为允许。

在提供者 Pod 上，我们生成一个入口规则，其中 src 为提供者节点，dest 为提供者 Pod（任意），协议为目标协议，端口为目标端口，操作为允许。

案例 2：保留客户端 IP **关**。

在使用者节点上，我们使用使用者到负载均衡器服务 (lb 入口 IP) 服务协议和端口允许生成出口规则。

提供者节点生成预路由规则，将 lb 入口 IP 设置为源，并将所有提供者节点设置为目标。该规则将服务协议指定为协议，将服务的节点端口指定为端口，并将操作设置为允许。

在提供者 Pod 上，我们生成一个入口规则，其中源为提供者节点，目标为提供者 Pod（任意），协议为目标协议，端口为目标端口，操作为允许。

GCP 连接器

Google Cloud 平台连接器可与 GCP 连接，以执行以下高级功能：

- **从 GCP 虚拟私有云 (VPC) 实时自动注入资产（及其标签）**

  GCP 允许您以标签的形式为资源分配元数据。Cisco Secure Workload 将查询这些资源的标签，然后将其用于资产和流数据可视化以及策略定义。此功能通过不断同步此数据来更新资源标签映射。

  注入来自GCP VPC的工作负载和网络接口的标签。如果同时配置了工作负载和网络接口，则标记会合并并显示在 Cisco Secure Workload 中。有关详细信息，请参阅云连接器生成的标签。

- **从 VPC 注入流日志** 如果您在 GCP 中设置了 VPC 流日志以进行监控，则 Cisco Secure Workload 可以通过读取相应的 Google Storage 存储桶来注入流日志信息。此遥测可用于可视化以及分段策略生成。

- **分段** 启用此选项可允许 Cisco Secure Workload 使用 GCP 本地 VPC 防火墙来编程安全策略。为 VPC 启用执行后，相关策略将自动编程到 VPC 防火墙。

- **自动从 GKE 集群注入元数据**（K8s 功能）在 GCP 上运行 Google Kubernetes Engine (GKE) 时，您可以选择收集与所有选定 Kubernetes 集群相关的所有节点、服务和 Pod 元数据。

您可以选择为每个 VPC 启用上述哪些功能。

GCP 连接器的要求和前提条件

对于所有功能：在 GCP 中创建专用服务帐户，或为此连接器标识现有 GCP 服务帐户。连接器配置向导会生成一个 IAM 策略列表，您可以使用该列表向此服务帐户分配所需的权限。确保您在 GCP 中具有上传此 IAM 策略列表的权限。

注释 将 IAM 策略列表中的权限应用于服务帐户的推荐方法是通过 CLI。

每个 VPC 只能属于一个 GCP 连接器。一个 Cisco Secure Workload 集群可以有多个 GCP 连接器。收集下文配置 GCP 连接器，第 90 页表格中所述的信息。

此连接器不需要虚拟设备。

- **对于收集标签和资产：**不需要其他前提条件。
- **对于注入流日志：**需要 VPC 级别的流日志定义才能触发流日志收集。

  要使用流日志注入，用户需要在所需 VPC 上启用流日志，并设置日志路由器接收器。

  日志路由器接收器的包含过滤器：

  1. `resource.type="gce-subnetwork"`
  2. `log_name="projects/<project_id>/logs/compute.googleapis.com%2Fvpc_flows"`

  选择接收器目标作为云存储桶，然后选择所需的存储桶。

  在使用入口流日志来配置 GCP 连接器时，必须输入存储桶名称。

  只能从 VPC 注入流日志。

流日志必须发布到 Google 存储桶；Cisco Secure Workload 无法从 Google Cloud 运营套件收集流数据。

如果在连接器创建期间提供的 GCP 用户帐户有权访问 VPC 流日志和 Google 存储桶，则 Cisco Secure Workload 可以从与任何帐户关联的 Google 存储桶中提取流日志。

流日志中需要以下流日志属性（按任意顺序）：源地址、目标地址、源端口、目标端口、协议、数据包、字节、开始时间、结束时间、操作、TCP 标志、接口 ID、日志状态和流方向。任何其他属性都将被忽略。

流日志必须同时捕获“允许”和“拒绝”的流量。

- **对于分段**：启用分段需要启用收集标签。

  在连接器中启用分段之前，请备份现有安全组，因为在为 VPC 启用分段策略执行时，所有现有规则都会被覆盖。

  另请参阅下文的对 GCP 资产执行分段策略时的最佳实践，第 93 页。

- **对于托管 Kubernetes 服务 (GKE)**：如果启用 Kubernetes 选项，请参阅下面在 GCP (GKE) 上运行的托管 Kubernetes 服务，第 94 页部分中的要求和前提条件，包括所需的访问权限。

在 GCP 中配置多个项目访问

要在 GCP 中配置跨多个项目访问，可以按照以下步骤进行操作：

过程

步骤 1 登录 GCP 控制台。

步骤 2 点击顶部导航栏中的项目下拉菜单，然后选择**新建项目 (New Project)**，也可以创建新项目或通过服务帐户使用现有项目。

步骤 3 输入新项目的名称。选择拥有新项目的组织，或者选择**无组织 (No organization)**（如果没有组织）。

步骤 4 点击**创建 (Create)** 按钮以创建新项目。

注释 您可以重复步骤 2 至 4，创建所需数量的项目。

步骤 5 要关联单个服务帐户中的多个项目，请导航至 **IAM 和管理 (IAM & Admin)** 页面，然后选择**服务帐户 (Service Account)**。

步骤 6 点击**创建服务帐户 (Create Service Account)** 按钮。按照提示创建服务帐户并授予其必要的权限。

注释 您可以使用现有的服务帐户或创建新的服务帐户。

步骤 7 在**密钥 (Keys)** 选项卡中，点击**添加密钥 (Add Key)** 以在 JSON 文件中生成私钥。

步骤 8 转到 GCP 控制台中的 **IAM 和管理 (IAM & Admin)** 页面，然后选择 **IAM**。

注释 您必须先更改项目，然后点击 IAM 和管理员，并尝试授予权限。

步骤 9 点击**授予访问权限 (Grant access)** 按钮以添加新项目。

步骤 10 在**新主体 (New principals)** 字段中，输入要链接到项目的服务帐户的邮件地址。

步骤 11 点击**保存 (Save)** 按钮，将服务帐户关联到您的项目。

注释 对要链接到原始项目的每个项目重复这些步骤。

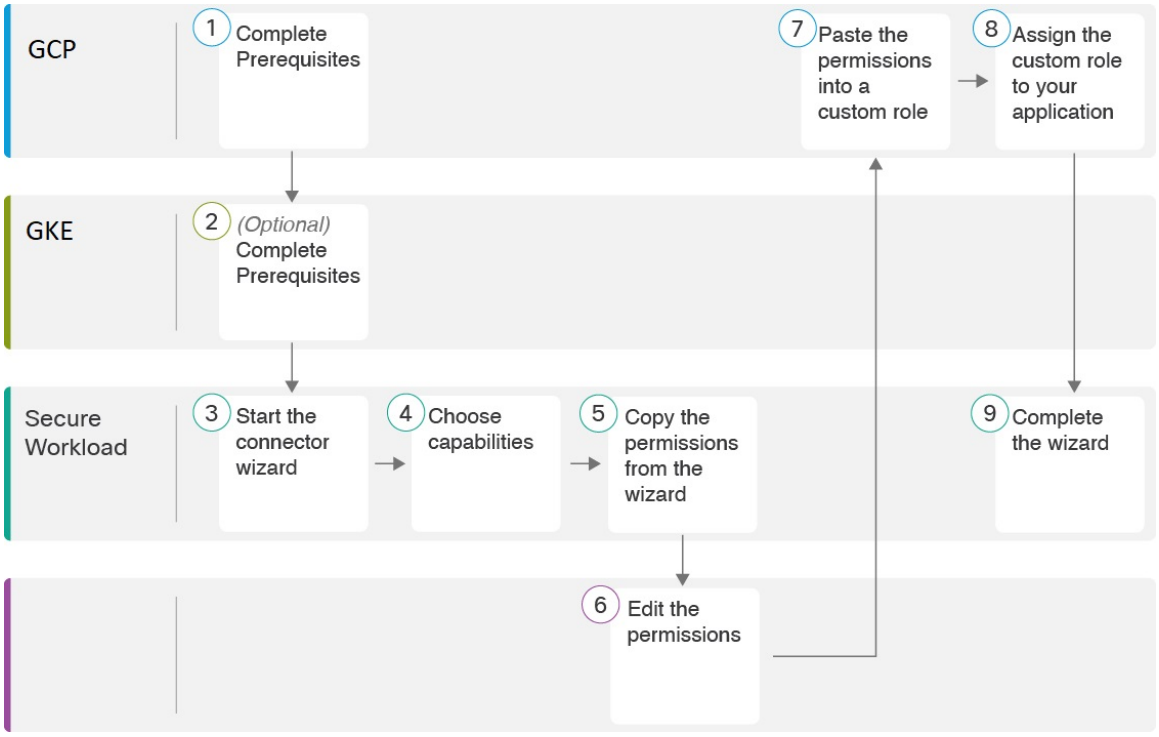
您可以通过以下方式来管理服务帐户权限：转到GCP控制台中的**IAM 和管理 (IAM & Admin)**页面，然后为每个项目选择 **IAM**。

步骤 12 确保服务帐户拥有对最小公共祖先（所有选定项目的共同祖先）资源级别的权限，例如文件夹或组织。

GCP 连接器配置概述

下图简要概述了连接器的配置过程。有关基本详细信息，请参阅下一个主题（配置GCP连接器，第 90 页）。

图 *43: GCP* 连接器配置概述



（请注意，图中的数字与详细程序中的步骤编号不对应。）

配置 GCP 连接器

过程

步骤 1 从窗口左侧的导航栏中，选择**管理 (Manage)** > **连接器 (Connectors)**。

步骤 2 点击 **GCP 连接器 (GCP connector)**。

步骤 3 点击第一个连接器（根范围内）的**启用 (Enable)**，或点击同一根范围内的其他连接器的**启用另一个 (Enable Another)**。

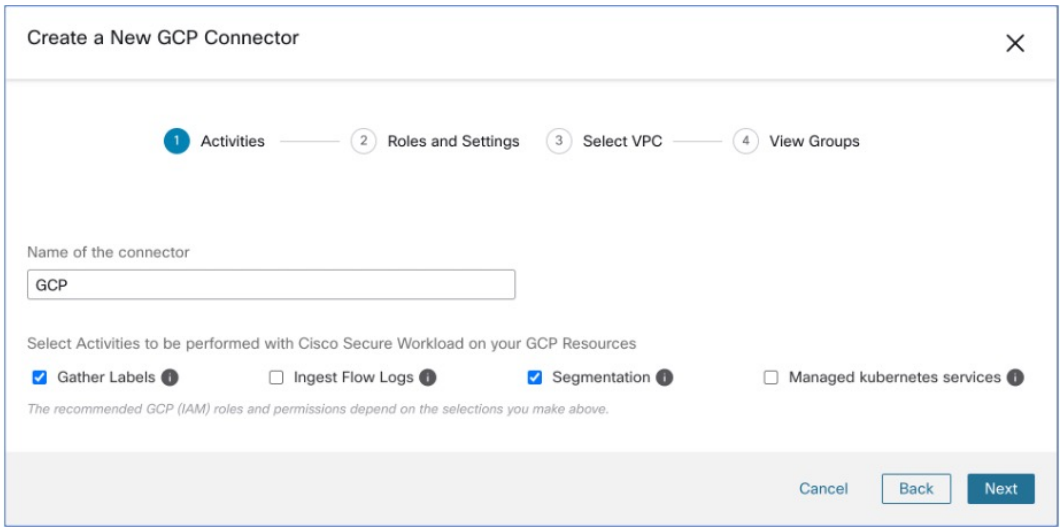
步骤 4 了解并满足GCP 连接器的要求和前提条件，第 87 页和在 GCP (GKE) 上运行的托管 Kubernetes 服务，第 94 页中的要求和前提条件，然后点击**开始 (Get Started)**。

步骤 5 输入连接器的名称并选择所需的功能，然后点击**下一步 (Next)**。

您在此页面上所做的选择仅用于确定将在下一步中生成的IAM策略列表中包含的权限，并显示您需要配置的设置。

如果选中**注入流日志**功能，则必须在下一步中输入**流日志存储桶名称**。

要启用**分段 (Segmentation)**，必须选中**收集标签 (Gather Labels)**。



步骤 6 下载生成的 IAM 自定义角色策略列表。

此 IAM 自定义角色策略列表包含上一步中选择的功能所需的 IAM 权限。

如果您已启用 Kubernetes 选项，则必须单独为 GKE 配置权限。

有关详细信息，请参阅在 GCP (GKE) 上运行的托管 Kubernetes 服务，第 94 页。

步骤 7 上传作为前提条件创建的具有所需功能的服务帐户 `json` 文件。

注释 在 GCP 中，单个连接器支持多个项目，并确保服务帐户直接关联到所有项目。

步骤 8 如果选中入口流日志功能，请输入**流日志存储桶名称**。

步骤 9 配置以下设置：

属性	说明
HTTP 代理	Cisco Secure Workload 需要代理才能访问 GCP。
全面扫描间隔	Cisco Secure Workload 从 GCP 刷新完整资产数据的频率。默认值及最小值为 3600 秒。
Delta 扫描间隔	Cisco Secure Workload 从 GCP 获取资产数据的增量更改的频率。默认值及最小值为 600 秒。

步骤 10 点击**下一步 (Next)**。系统可能需要几分钟才能从 GCP 项目中获取虚拟网络和 GKE 集群列表。

步骤 11 从 VPC（虚拟网络）和 GKE 集群列表中选择资源及其各自的功能。

通常，您应尽快启用流注入，以便 Cisco Secure Workload 开始收集建议准确策略所需的足够数据。

通常，在初始配置期间不应选择**启用分段 (Enable Segmentation)**。稍后，当您准备好对特定 VPC 执行分段策略时，可以编辑连接器并为这些 VPC 启用分段。请参阅“对 GCP 资产执行分段策略时的最佳实践”。

步骤 12 点击**创建 (Create)** 并等待几分钟以完成验证检查。

“查看组”(View Groups) 页面将显示您为上一个页面上的任何功能启用的所有 VPC，按逻辑组 ID (CSW) 分组，该 ID 也是 project_id (GCP)。每个逻辑组 ID 和每个逻辑组 ID 中的每个 VPC 都是一个新的范围。

步骤 13 选择要在其下添加新范围集的父范围。如果尚未定义任何范围，则唯一的选择是默认范围。

步骤 14 要接受在向导中配置的所有设置（包括层次结构范围树），请点击**保存 (Save)**。

要接受层次结构范围树之外的所有设置，请点击**跳过 (Skip)** 以跳过此步骤。

您可以稍后在**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 下手动创建或编辑范围树。

下一步做什么

如果您已启用收集标签、注入流数据和/或分段：

- 如果启用了流注入，最多可能需要 25 分钟，流才会开始显示在**调查 (Investigate)** > **流量 (Traffic)** 页面上。
- （可选）要获得更丰富的流数据和其他优势，包括主机漏洞 (CVE) 的可视性，请在基于 VPC 的工作负载上为操作系统安装相应的代理。有关要求和详细信息，请参阅代理安装章节。
- 在成功配置 GCP 连接器以收集标签和注入流后，请按照标准流程构建分段策略。例如：允许 Cisco Secure Workload 收集足够的流数据以生成可靠的策略；定义或修改范围（通常每个 VPC 一个）；为每个范围创建工作空间；根据您的流数据自动发现策略，和/或手动创建策略；分析和优化您的策略；确保您的策略符合以下准则和最佳实践；准备就绪后，在工作空间中批准并

执行这些策略。准备好为特定 VPC 执行分段策略后，返回连接器配置以便为 VPC 启用分段。有关详细信息，请参阅对 GCP 资产执行分段策略时的最佳实践，第 93 页。

如果您已启用 Kubernetes 托管服务 (GKE) 选项：

- 在基于容器的工作负载上安装 Kubernetes 代理。有关详细信息，请参阅代理部署一章中的 Kubernetes/OpenShift 代理 - 深度可视性和执行。

事件日志：

事件日志可用于通过不同的功能来了解每个连接器发生的重要事件。我们可以使用组件、命名空间、消息和时间戳等各种属性来对它们进行过滤。

编辑 GCP 连接器

如果要启用从不同或其他 VPC 或 GKE 集群收集数据的功能，您可能需要上传具有不同权限所需功能的服务帐户 json 文件，然后才能选择不同的 VPC 或 GKE。

在完成向导之前，更改不会被保存。

过程

步骤 1 从窗口左侧的导航栏中，选择**管理 (Manage)** > **工作负载 (Workloads)** > **连接器 (Connector)**。

步骤 2 点击 **GCP 连接器 (GCP Connector)**。

步骤 3 如果有多个 GCP 连接器，请从窗口顶部选择要编辑的连接器。

步骤 4 点击**编辑连接器 (Edit Connector)**。

步骤 5 再次点击向导并进行更改。有关设置的详细说明，请参阅配置 GCP 连接器，第 90 页。

步骤 6 如果您启用了不同的功能（收集标签、注入流、执行分段或收集GKE数据），则必须下载修订后的 IAM 模板并将其上传到 GKE，然后才能继续运行向导。

步骤 7 要启用分段策略执行，请首先确保您已满足对 GCP 资产执行分段策略时的最佳实践，第 93 页中所述的建议前提条件。在列出 VPC 的页面上，为要启用执行的 VPC 选择**启用分段 (Enable Segmentation)**。

步骤 8 如果您已使用向导或手动为任何所选 VPC 创建范围，请点击**跳过此步骤 (Skip this step)** 以完成向导。

您可以使用**整理 (Organize)** > **范围和资产 (Scopes and Inventory)** 页面来手动编辑范围树。

步骤 9 如果您尚未为所选 VPC 创建任何范围，并且想要保留建议的层次结构，请从范围树上方选择父范围，然后点击**保存 (Save)**。

删除连接器和数据 GCP

如果删除连接器，该连接器已注入的数据不会被删除。

24 小时后，标签和库存会从活动库存中自动删除。

对 GCP 资产执行分段策略时的最佳实践

警告 在任何 VPC 上启用分段执行之前，请在该 VPC 上创建安全组备份。为 VPC 启用分段会删除该 VPC 中的现有安全组。禁用分段不会恢复旧的安全组。

在创建策略时：

- 与所有被发现的策略一样，要确保有足够的流数据来生成准确的策略。
- 因为 GCP 允许在防火墙策略中同时使用 ALLOW/DENY 规则。由于 GCP 对规则数量有非常严格的限制，因此最好只有 ALLOW 列表。

建议您在为关联的VPC启用分段之前，在工作空间中启用执行。如果您为未包含在已启用执行的工作空间中的 VPC 启用分段，则将允许该 VPC 上的所有流量。

当您准备好为 VPC 执行策略时，请编辑 GCP 连接器（请参阅 编辑 GCP 连接器，第 92 页）并为该 VPC 启用分段。

GKE 资产标签、详细信息和执行状态

要查看 GCP 连接器的摘要信息，请导航至**连接器 (Connector)** >，然后在“连接器”(Connector) 页面上选择“GCP 连接器”(GCP Connector)。

要查看有关资产的信息，请从“范围和资产”(Scopes and Inventory) 页面中点击特定工作负载的 IP 地址。您还可以从VPC配置文件的界面选项卡访问资产配置文件。有关资产配置文件的详细信息，请参阅资产配置文件。

同样，要查看 VPC 配置文件下的所有具体策略，可从“资产配置文件具体策略”(Inventory Profile Concrete Policies) 选项卡导航至父 VPC 配置文件，以查看 VPC 下的所有具体策略。

可从“GCP配置”(GCP Configuration)或“执行状态”(Enforcement Status)页面（全局或在工作空间内）访问 VPC 配置文件。您可以在 VPC 配置文件中查看 VPC 级别的执行状态和具体策略。您还可以在“VPC 防火墙策略”(VPC Firewall Polices) 选项卡上查看所有接口的组合 VPC 防火墙策略。

有关标签的详细信息，请参阅：

- 云连接器生成的标签
- 与 *Kubernetes* 集群相关的标签

GCP 连接器问题故障排除

问题：“执行状态”(Enforcement Status) 页面显示已跳过某个具体策略。

解决方案：当防火墙策略中的规则数量超过GCP连接器中配置的GCP限制时，就会发生这种情况。

当具体策略显示为“已跳过”(SKIPPED) 时，系统不会实施新的安全组，GCP 上以前存在的安全组仍然有效。

要解决此问题，请查看是否可以整合策略，例如在一个策略中使用较大的子网，而不是包含较小子网的多个策略。

背景：

启用分段时，系统会为每个 VPC 生成具体策略。这些具体策略用于在 GCP 中创建防火墙策略。但是，GCP 和 Cisco Secure Workload 计数策略不同。在防火墙策略中将 Cisco Secure Workload 策略转换为 GCP 防火墙规则时，GCP 计数机制很复杂。有关详细信息，请参阅 GCP。

问题：GCP 意外允许所有流量

解决方案：确保将 Cisco Secure Workload 中的捕获全部策略设置为“拒绝”(Deny)。

在 GCP (GKE) 上运行的托管 Kubernetes 服务

您可以使用云连接器从在 Google Cloud 平台 (GCP) 上运行的 Google Kubernetes Engine (GKE) 集群中收集元数据。

连接器会收集与所有选定 Kubernetes 集群相关的所有节点、服务和 Pod 元数据。

要求和前提条件

Cisco Secure Workload 要求：此连接器不需要虚拟设备。

平台要求：

- 确保您在 GCP 中拥有为此连接器配置所需访问权限的权限。
- 每个 GKE 集群只能属于一个 GCP 连接器。
- 收集下面的配置 *GCP* 连接器中的表中所述的信息。

GKE 要求：

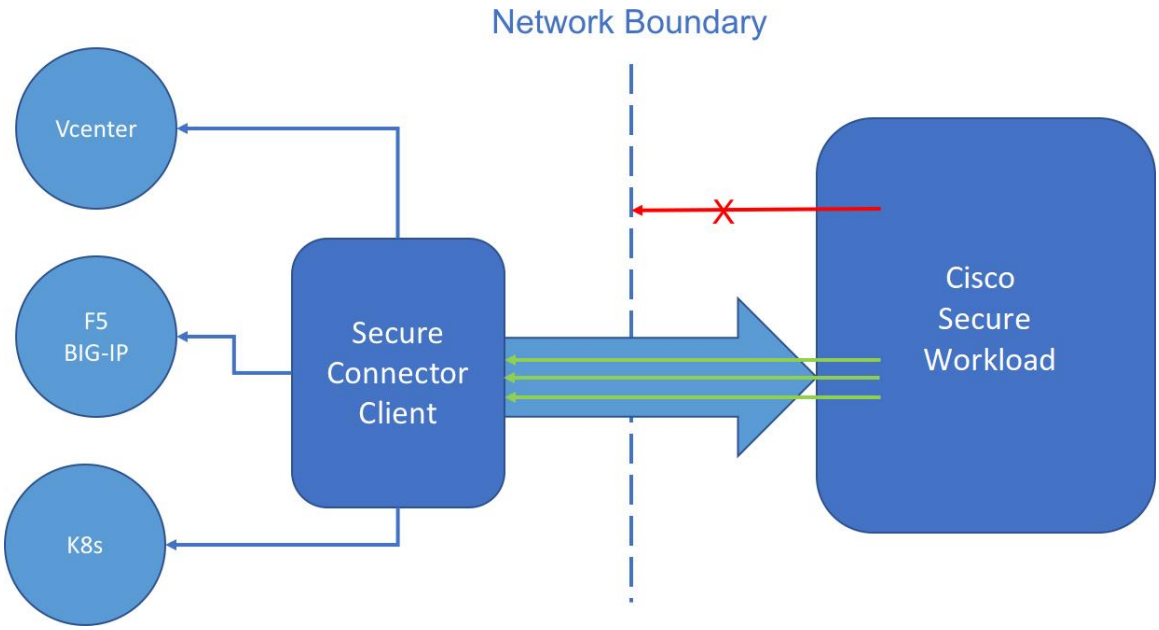
- 您必须在 GKE 中配置所需的访问权限。
- 要支持托管 K8s 功能，服务帐户所需的角色包括：
  - 计算网络查看器是一种 IAM 角色，可对 GCP 中的所有网络资源进行只读访问。 https://cloud.google.com/compute/docs/access/iam#compute.networkViewer
  - Kubernetes Engine Viewer 是一个 GKE 集群角色，可对 GKE 集群内的资源（如节点、pod 和 GKE API 对象）进行只读访问。 https://cloud.google.com/iam/docs/understanding-roles#kubernetes-engine-roles

安全连接器

为了使 Cisco Secure Workload 可以在外部协调器上导入用户标签或执行策略（请参阅外部协调器），Cisco Secure Workload 需要与协调器 API 服务器（vCenter、Kubernetes、F5 BIG-IP 等）建立传出连接。有时候不允许从 Cisco Secure Workload 集群到协调器的直接传入连接。安全连接器 通过与协调

器建立从同一网络到 Cisco Secure Workload 集群的传出连接来解决此问题。此连接用作反向隧道，将请求从集群传回协调器 API 服务器。

Figure 44: 安全连接器



对于每个根范围，任何时候都只能有一个隧道处于活动状态。尝试启动其他隧道将被拒绝，并显示一条错误消息，指明隧道已处于活动状态。活动隧道可用于连接多个协调器，这些协调器可从客户端运行的网络访问。每个协调器的配置用于指明与该协调器的连接是否应通过安全连接器隧道。

安全连接器客户端与 Cisco Secure Workload 集群之间的所有通信都使用 TLS 进行相互身份验证和加密。

为提高安全性，建议客户在经过适当保护的隔离计算机上安装安全连接器客户端。计算机应具有防火墙规则，以便只仅允许到 Cisco Secure Workload 集群的传出连接，并且还应允许任何外部协调器 API 服务器 Cisco Secure Workload 进行访问。

要将协调器配置为使用安全连接器隧道，请参阅有关为产品配置外部协调器的说明。

有关安全连接器的 OpenAPI 终端的详细信息，请参阅安全连接器 API 终端

技术详情

为了引导隧道，安全连接器客户端会创建一个公钥或私钥对，并由服务器远程签署其公钥证书。加密的单次使用限时令牌可用于确保远程签名过程的安全，并识别客户端所属的根范围。在服务器端，每个根范围都有一个唯一的证书，客户端将使用它来验证服务器。这些证书会定期轮换，从而确保通信的持续保密性。

安全连接器客户端内部由一个隧道客户端和一个 SOCKS5 服务器组成。隧道启动后，客户端会等待来自 Cisco Secure Workload 集群的传入隧道连接。传入连接由 SOCKS5 服务器处理并会被转发到目标主机。

安全连接器客户端的要求

以下是 安全连接器客户端的要求：

- RHEL 或 CentOS 7 (x86_64)
- 2 个 CPU 核心
- 4 GB RAM
- 有足够的网络带宽来处理来自使用安全连接器的本地协调器的数据。
- 在端口 443 上与 Cisco Secure Workload 集群的传出连接（直接或通过 HTTP(S) 代理）。
- 到内部协调器 API 服务器的传出连接（直接）。

安全连接器客户端部署

代理支持

安全连接器客户端支持通过 HTTP(S) 代理连接到 Cisco Secure Workload 集群。如有需要，必须通过为客户端设置 HTTPS_PROXY 环境变量来配置代理服务器。要设置此变量，请在位于 */etc/systemd/system/tetration-secure-connector.service* 的 systemd 服务文件的 *[Service]* 部分添加以下行。此设置在重新安装后不会保留。对于粘性配置，可以在 */etc/systemd/system/tetration-secure-connector.service.d/10-https-proxy.conf* 中的新文件中添加该行。要使任一配置生效，请运行 *systemctl daemon-reload* 以重新加载 systemd 配置。

```
[Service]
Environment="HTTPS_PROXY=<Proxy Server Address>"
```

部署概述

安全连接器会创建从 Cisco Secure Workload 集群到内部网络的反向隧道，以便访问协调器 API 服务器。

启动安全连接器客户端需要下载安全连接器 RPM 并生成一次性注册令牌。

1. 在支持的平台上下载最新的安全连接器客户端 RPM。
2. 生成注册令牌。
3. 在主机上复制令牌并启动客户端以启动客户端。

部署安全连接器客户端

下载最新的安全连接器客户端 RPM

过程

步骤 1 在导航窗格中，点击 **管理 (Manage)** > **工作负载 (Workloads)** > **安全连接器 (Secure Connector)**。

步骤 2 点击**下载最新 RPM (Download Latest RPM)**。

步骤 3 将 RPM 软件包复制到 Linux 主机进行部署，然后使用根权限执行以下命令：`rpm -ivh <rpm_filename>`

生成注册令牌

过程

步骤 1 点击**管理 (Manage)** > **工作负载 (Workloads)** > **安全连接器 (Secure Connector)**。

步骤 2 点击**生成注册令牌 (Generate Registration Token)**。

复制令牌并启动客户端

在**安全连接器 (Secure Connector)** 页面上生成注册令牌后，您将获得一个 *registration.token* 文件，其中包含用于引导客户端的一次性限时令牌。停止主机上的安全连接器客户端，并复制已安装安全连接器客户端软件包的令牌文件。

1. 要停止客户端，请运行以下命令：`systemctl stop tetration-secure-connector`
2. 将 *registration.token* 文件复制到 `/etc/tetration/cert/` 文件夹。
3. 要重启客户端，请运行以下命令：`systemctl start tetration-secure-connector`

[可选] 部署特定版本的安全连接器客户端

过程

步骤 1 下载安全连接器客户端 RPM 的特定版本。

a) 在导航窗格中，点击**管理 (Manage)** > **工作负载 (Workloads)** > **代理 (Agents)**。

b) 点击**安装程序 (Installer)** 选项卡。

c) 点击 **使用经典打包安装程序手动安装 (Manual Install using classic packaged installers)**，然后点击**下一步 (Next)**。

安全连接器客户端软件包的代理类型为安全连接器 *(Secure Connector)*。

d) 找到适当的版本（如果集群上有多个可用），然后点击**下载 (Download)**。

e) 将 RPM 软件包复制到 Linux 主机进行部署，然后使用根权限执行以下命令：`rpm -ivh <rpm_filename>`。

步骤 2 使用 API 检索新令牌。

安全连接器令牌也可以通过 OpenAPI (Get Tokenendpoint) 进行检索。以下 Python 和 Bash 代码片段可用于检索新令牌。请注意，使用的 API 密钥必须具有 *external_integration* 功能，并且必须对指定的根范围具有写入访问权限。有关安装适用于 python 的 Cisco Secure Workload OpenAPI 客户端和创建新 API 密钥的信息，请参阅 OpenAPI 身份验证。

- **用于令牌检索的 Python 片段**

```
from tetpyclient import RestClient
from urllib import quote

API_ENDPOINT = "https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
ROOT_SCOPE_NAME = r"""<ROOT_SCOPE_NAME>"""
API_CREDENTIALS_FILE = "<API_CREDENTIALS_JSON_FILE>"
OUTPUT_TOKEN_FILE = "registration.token"

if __name__ == "__main__":
  client = RestClient(API_ENDPOINT,
                      credentials_file=API_CREDENTIALS_FILE)  # Add (verify=False) to
skip certificate verification
  escaped_root_scope_name = quote(ROOT_SCOPE_NAME, safe='')
  resp = client.get('/secureconnector/name/{}/token'.format(escaped_root_scope_name))
  if resp.status_code != 200:
    print 'Error ({}): {}'.format(resp.status_code, resp.content)
    exit(1)
  else:
    with open(OUTPUT_TOKEN_FILE, 'w') as f:
      f.write(resp.content)
```

- **用于令牌检索的 BASH 片段**

```
#!/bin/bash
HOST="https://<UI_VIP_OR_DNS_FOR_TETRATION_DASHBOARD>"
API_KEY="<API_KEY>"
API_SECRET="<API_SECRET>"
ROOTSCOPE_NAME="<ROOT_SCOPE_NAME>" # if the name contains spaces or special characters,
 it should be url-encoded
TOKEN_FILE="registration.token"
INSECURE=1 # Set to 0 if you want curl to verify the identity of the cluster

METHOD="GET"
URI="/openapi/v1/secureconnector/name/$ROOTSCOPE_NAME/token"
CHK_SUM=""
CONTENT_TYPE=""
TS=$(date -u "+%Y-%m-%dT%H:%M:%S+0000")
CURL_ARGS="-v"
if [ $INSECURE -eq 1 ]; then
    CURL_ARGS=$CURL_ARGS" -k"
fi

MSG=$(echo -n -e "$METHOD\n$URI\n$CHK_SUM\n$CONTENT_TYPE\n$TS\n")
SIG=$(echo "$MSG"| openssl dgst -sha256 -hmac $API_SECRET -binary | openssl enc -base64)

REQ=$(echo -n "curl $CURL_ARGS $HOST$URI -w '%{http_code}' -H 'Timestamp: $TS' -H 'Id:
```

```
$API_KEY' -H 'Authorization: $SIG' -o $TOKEN_FILE")
   status_code=$(sh -c "$REQ")
   if [ $status_code -ne 200 ]; then
       echo "Failed to get token. Status: " $status_code
   else
       echo "Token retrieved successfully"
   fi
```

步骤 3 复制令牌并启动客户端。有关详细说明，请参阅复制令牌并启动客户端 ， 第 97 页。

验证安全连接器客户端状态

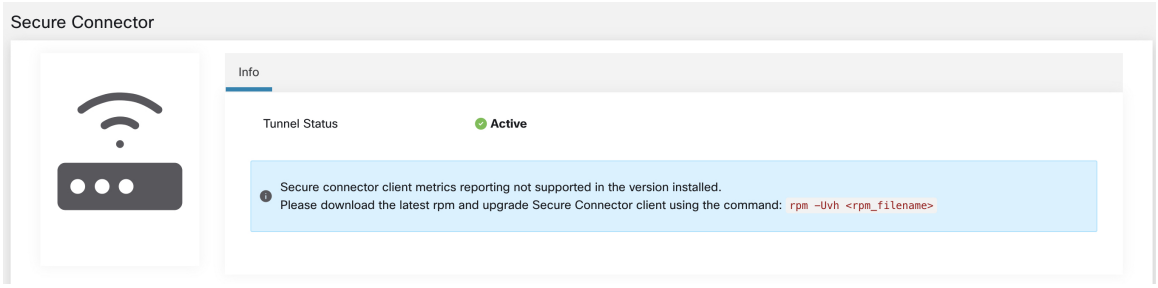
- 要检查是否已安装安全连接器客户端，请运行以下命令，在 RPM 数据库中查询 *tet-secureconnector-client-site* 软件包：`rpm -q tet-secureconnector-client-site`
- 要检查已安装客户端的状态，您可以通过运行以下命令来检查 *tetration-secure- connector* systemd 服务的状态：`systemctl status tetration-secure-connector`

安全连接器客户端状态

外部协调器 (External Orchestrators) 页面上会显示已配置的外部协调器和安全连接器隧道的状态。如果在配置外部协调器时启用了 安全连接器，您可以在**安全连接器 (Secure Connector)** 页面上查看安全连接器客户端指标。

但是，如果安全连接器隧道状态为**活动 (Active)**，但客户端指标不可见，则表示已安装较旧版本的安全连接器。系统将显示一条升级安全连接器客户端版本的消息，如下所示：

Figure 45: 安全连接器客户端升级消息



Note 有关安装最新安全连接器 RPM 的说明，请参阅下载最新的安全连接器客户端 RPM

查看客户端指标的步骤：

Procedure

步骤 1 在**配置详细信息 (Configure Details)** 下，点击**状态 (Status)** 行。系统将显示**安全连接器 (Secure Connector)** 页面。

Note 要访问安全连接器隧道的状态，请在左侧窗格中选择**管理 (Manage)** > **工作负载 (Workloads)** > **安全连接器 (Secure Connector)**。

步骤 2 选择**常规 (General)**、**接口 (Interface)** 或**路由 (Routes)** 选项卡，以访问有关客户端和 Cisco Secure Workload 集群之间连接状态的更多详细信息。

选项卡	描述
常规	列出以下信息： • 隧道状态 • 主机名 • IP 地址 • HTTP/HTTPS 代理 • 版本 - 列出内部版本。 • vCPU 数量 • 总内存 (GB) • 正常运行时间 - 列出运行安全连接器客户端的虚拟机的正常运行时间。 • 上次接收的心跳 - 列出上次从客户端收到心跳的日期和时间戳。 • 心跳失败次数（最近 1 天）- 列出一天内与安全连接器客户端的连接失败的次数。如果客户端保持非活动状态，则计数不会递增。计数在一天结束时重置。 • 往返延迟 (ms)
接口	列出运行安全连接器客户端的虚拟机的接口详细信息。
路由	路由表列出目标 IP 地址、网关、掩码和接口。

安全连接器警报

当安全连接器停止运行或在过去一分钟内没有心跳时，会生成警报。

步骤 1：要启用警报，请依次点击**管理 (Manage)** > **工作负载 (Workloads)** > **安全连接器 (Secure Connector)**。

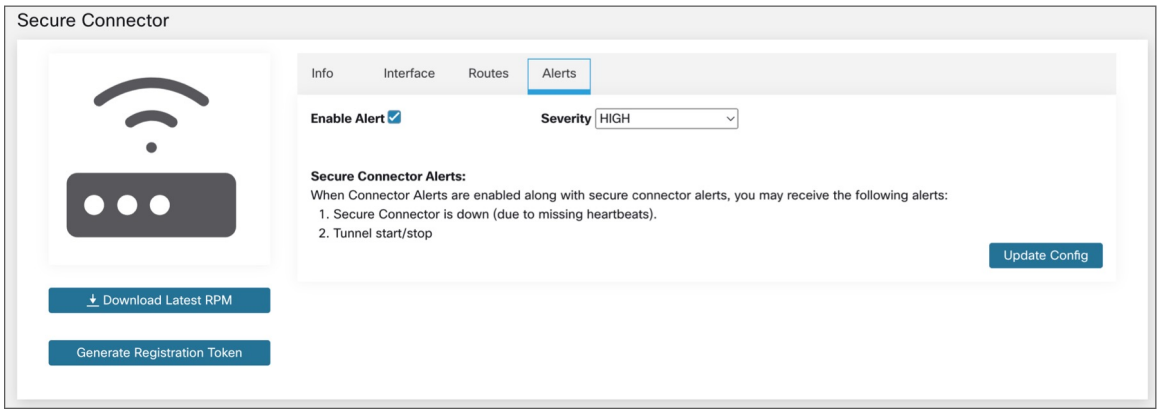
步骤 2：点击**警报 (Alerts)** 选项卡。

步骤 3：选中**启用警报 (Enable Alert)** 复选框。

步骤 4：从下拉列表中选择**严重性 (Severity)** 值。

步骤 5：点击**更新配置 (Update Config)**。

图 *46:* 启用安全连接器警报



注释 确保在**管理 (Manage)** > **警报 - 配置 (Alerts - Configuration)** 页面中启用了连接器警报。

导航至**调查 (Investigate)** > **警报 (Alerts)**，然后点击警报以查看更多详细信息 。

警报文本：安全连接器：<reason for connection failure>

图 *47:* 安全连接器警报

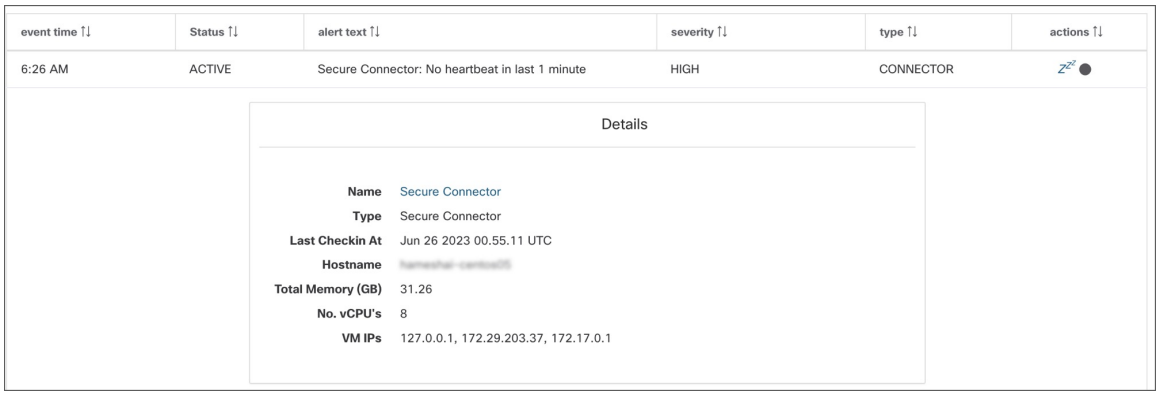


表 4: 警报详细信息

字段	类型	说明
名称 (Name)	字符串	安全连接器名称
类型 (Type)	字符串	安全连接器类型
上次签入时间 (Last CheckIn At)	字符串	上次发生心跳的已知时间
主机名 (Hostname)	字符串	托管此安全连接器的计算机的名称
总内存 (GB) (Total Memory [GB])	字符串	以 GB 为单位的 RAM
vCPU 数量 (No. vCPU's)	字符串	CPU 数量
VM IP	字符串	安全连接器客户端主机上的网络接口列表

升级安全连接器客户端

安全连接器客户端不支持自动更新。要部署新版本，请执行以下操作：

1. 运行以下命令以卸载当前版本：`rpm -e tet-secureconnector-client-site`
2. 部署新版本。有关详细说明，请参阅部署安全连接器客户端, on page 97。

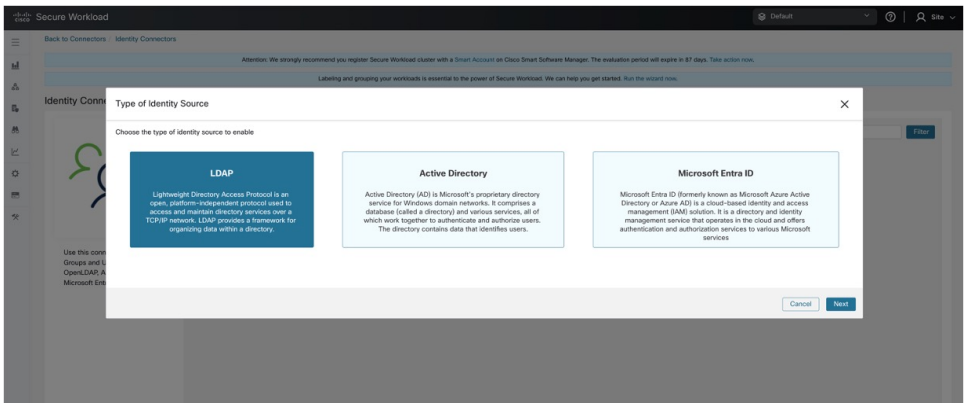
卸载安全连接器客户端

可以使用以下命令卸载安全连接器客户端：`rpm -e tet-secureconnector-client-site`

身份连接器

身份连接器充当 Cisco Secure Workload 与各种身份存储库（例如 OpenLDAP、Active Directory 和 Microsoft Entra ID）之间的桥梁。通过该连接器，无需人工干预即可同步身份存储库中存储的信息。现在可以配置身份连接器，从 LDAP、Active Directory 和 Microsoft Entra ID 中导入用户数据和用户组数据。

Figure 48: 身份源类型



OpenLDAP 连接器

轻量级目录访问协议 (LDAP) 是一种用于检索用户、用户组、组织和其他属性信息的协议。其主要目标是将数据存储在 LDAP 目录中，从而简化用户管理。

Note OpenLDAP 数据注入支持的版本是 OpenLDAP 2.6。

使用 OpenLDAP 配置身份连接器

在 Cisco Secure Workload 中创建用于 LDAP 的身份连接器，以建立与 OpenLDAP 的通信。

过程

步骤 1 从导航窗格中，依次选择**管理 (Manage)** > **工作负载 (Workloads)** > **连接器 (Connectors)**。

步骤 2 点击**身份连接器 (Identity Connector)**，然后选择**在此处配置新连接器 (Configure your new connector here)**。

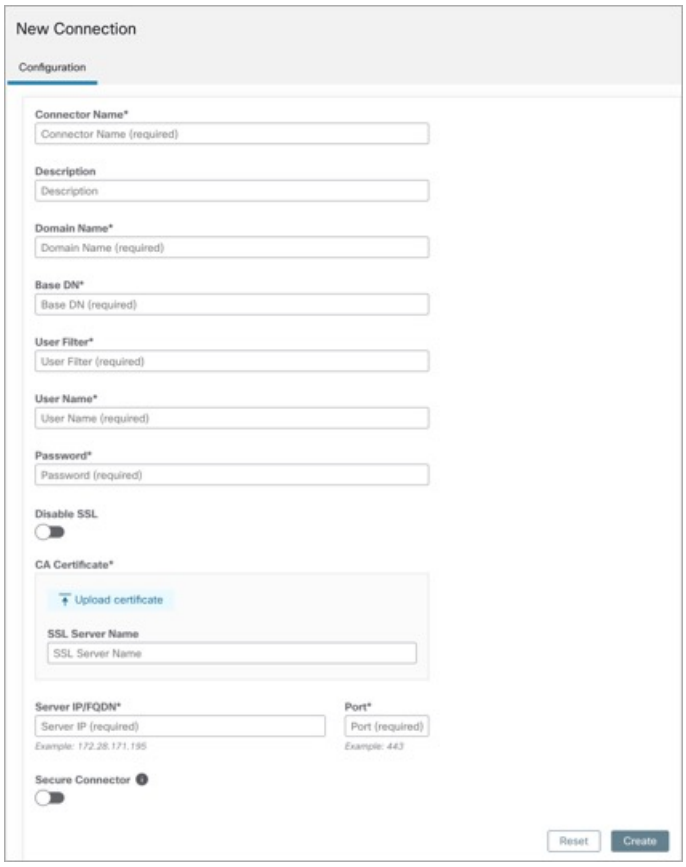
步骤 3 在**新建连接 (New Connection)** 页面中，输入以下详细信息：

字段	说明
连接器名称 (Connector Name)	输入连接器的名称。
说明 (Description)	输入说明。
域名 (Domain Name)	输入域名。域名在所选范围内必须是唯一的，例如 csw.com。

字段	说明
基本 DN (Base DN)	输入在目录树中用作搜索起点的基本 DN 或可分辨名称。例如，dc=csw、dc=com。
用户过滤器 (User Filter)	输入过滤器以定义识别包含特定类型信息的条目的标准。 示例 1：要识别用户，可以通过设置两个 objectClass 属性来区分用户，一个设置为“person”，另一个设置为“user”。匹配条件可以是 `(&(objectClass=person)(objectClass=user))` 示例 2：要检索 objectClass=user 且 cn 属性包含单词 Marketing 的所有条目，搜索过滤器可以是 `(&(objectClass=user)(cn=*Marketing*))`
用户名 (Username) 和密码 **(Password)**	输入用于连接到 OpenLDAP 服务器的凭证。
CA 证书	上传 CA 证书并输入 Cisco Secure Workload 用于进行身份验证的 SSL 服务器名称。如果没有，请**禁用 SSL**。
服务器 IP/FQDN 和端口	输入服务器 IP 地址和端口号。
安全连接器	在安全连接器用于通过隧道连接从 Cisco Secure Workload 到 OpenLDAP 时启用。 在启用此选项之前，您应已部署安全连接器。 有关详细信息，请参阅安全连接器。

步骤 4 点击**创建 (Create)**。

图 *49:* 配置新连接器



系统将创建新的身份连接器，并在 Cisco Secure Workload 和 OpenLDAP 之间建立通信。

资产

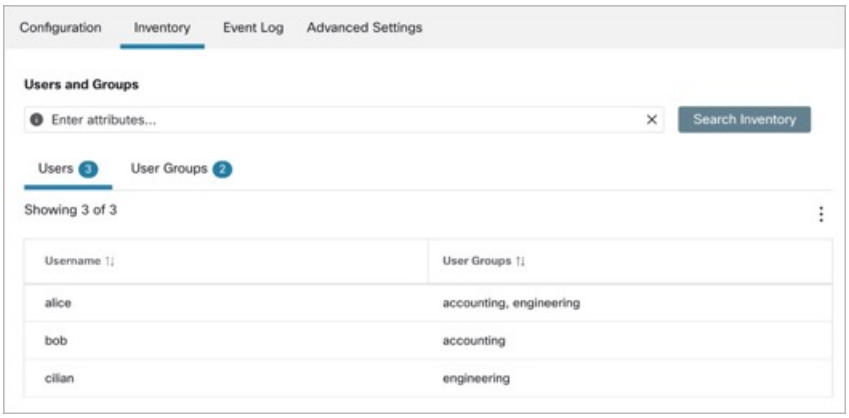
在 Cisco Secure Workload 和 OpenLDAP 之间建立连接后，您可以在**资产 (Inventory)** 选项卡中查看**用户 (Users)** 和 **用户组 (User Groups)**的列表。用户所属的所有用户组都显示在**用户 (Users)** 选项卡中。**用户组 (User Groups)** 选项卡中仅显示唯一用户组。

过程

步骤 1 输入要过滤的属性。将光标悬停在信息图标上可查看要过滤的属性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 *50:* 用户和用户组



注释　显示的用户数的建议限制为 300,000，而用户组为 30,000。

事件日志

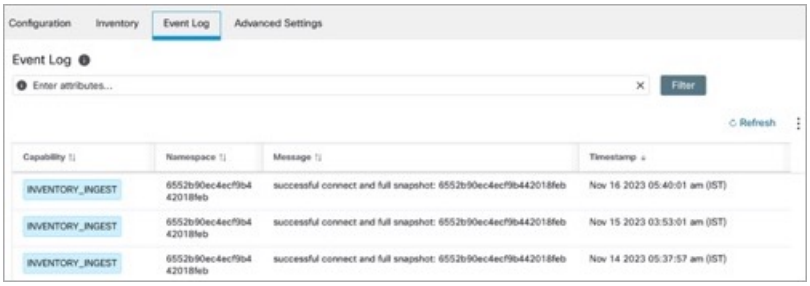
事件日志 (Event Log) 选项卡显示在与 OpenLDAP 建立连接时发生的信息、警告和错误。

过程

步骤 1 输入要过滤的属性。将光标悬停在信息图标上可查看要过滤的属性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 *51:* 事件日志



注释　日志的颜色代码为信息（蓝色）、警告（橙色）和错误（红色）。

高级设置

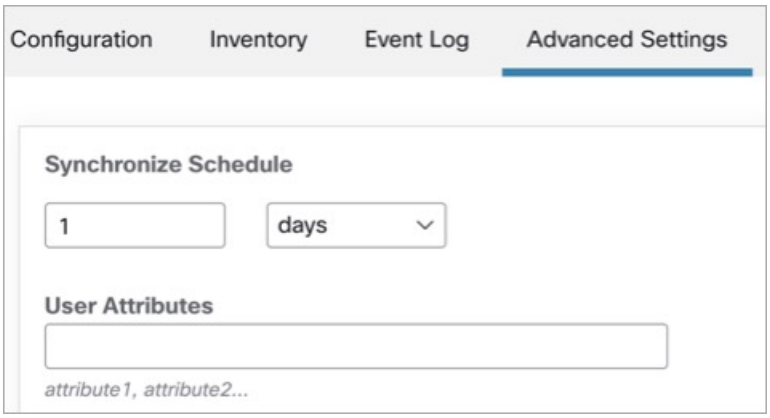
高级设置 (Advanced Settings) 选项卡显示同步用户数据和用户属性的计划。

过程

步骤 1 在同步计划 **(Synchronize Schedule)** 下，您可以选择 Cisco Secure Workload 从 LDAP 服务器同步用户数据的时间频率。

步骤 2 在用户属性 **(User Attributes)** 字段中，输入最多六个要显示的用户属性。

图 *52:* 高级设置



Active Directory

Active Directory (AD) 是 Microsoft 的目录服务，用于管理用户帐户、权限和对网络的网络资源的访问。AD 提供了多项重要功能，以促进联网元素的管理和安全。

使用身份连接器配置 Active Directory

在 Cisco Secure Workload 中，通过将身份连接器用作身份管理源来支持 Active Directory (AD)。身份连接器旨在与 AD 集成，以验证用户身份并管理他们对 Cisco Secure Workload 环境中资源的访问。

在 Cisco Secure Workload 中创建用于 **Active Directory** (AD) 的身份连接器，以建立与 AD 的通信。

过程

步骤 1 从导航窗格中，依次选择管理 **(Manage)** > 工作负载 **(Workloads)** > 连接器 **(Connectors)**。

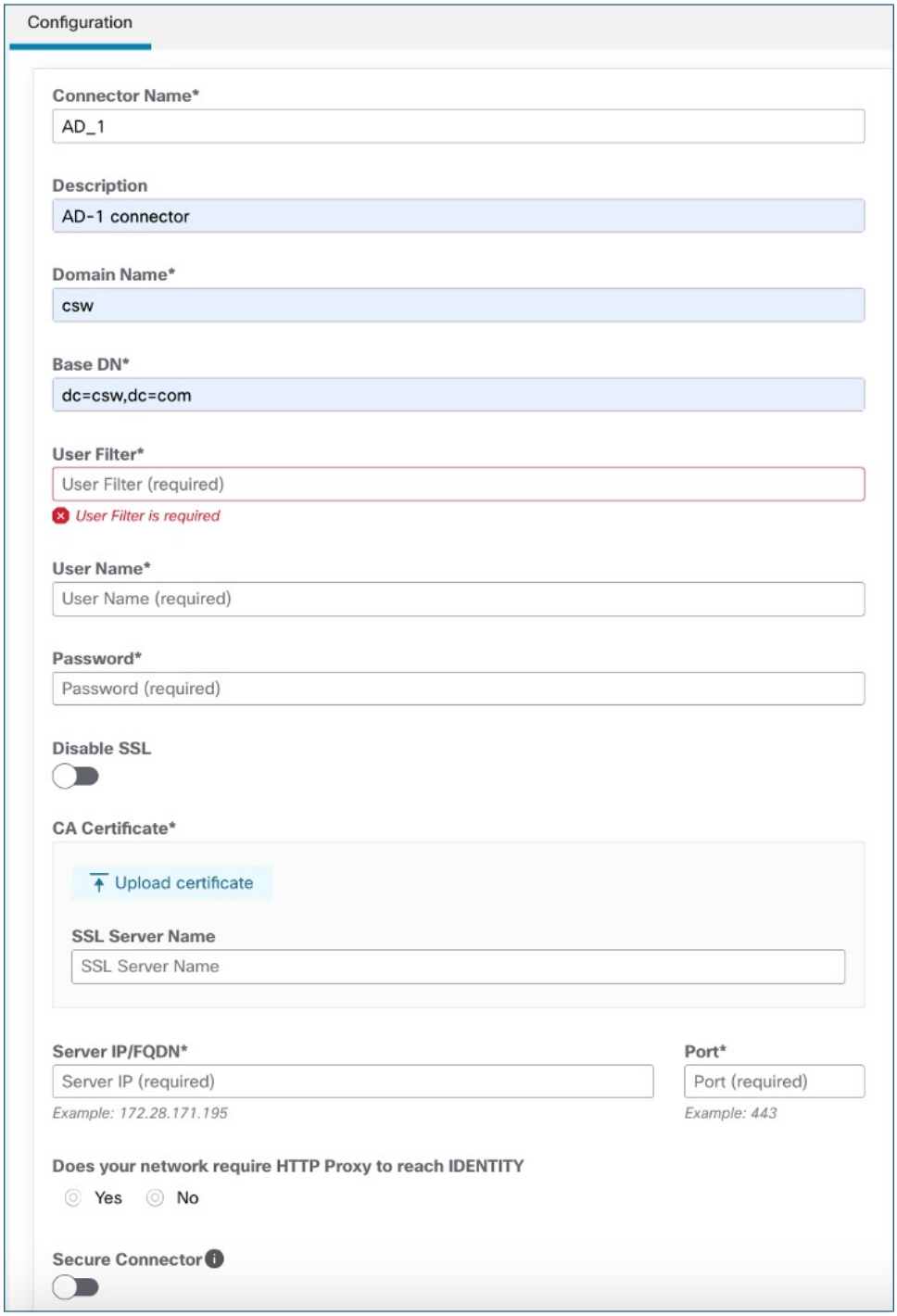
步骤 2 选择身份连接器 **(Identity Connector)**，然后点击在此处配置新连接器 **(Configure your new connector here)**。

步骤 3 在新建 AD 连接 **(New AD Connection)** 页面中，输入以下详细信息：

字段	说明
连接器名称 (Connector Name)	输入连接器的名称。
说明 (Description)	输入说明。
域名 (Domain Name)	输入域名。域名在所选范围内必须是唯一的，例如 csw.com。
基本 DN (Base DN)	输入在目录树中用作搜索起点的基本 DN 或可分辨名称。例如，dc=csw、dc=com。
用户过滤器 (User Filter)	输入过滤器以定义识别包含特定类型信息的条目的标准。 示例 1：要识别用户，可以通过设置两个 objectClass 属性来区分用户，一个设置为“person”，另一个设置为“user”。匹配条件可以是 `(&(objectClass=person)(objectClass=user))` 示例 2：要检索 objectClass=user 且 cn 属性包含单词 Marketing 的所有条目，搜索过滤器可以是 `(&(objectClass=user)(cn=*Marketing*))`
用户名 (Username) 和密码 (Password)	输入用于连接到 OpenLDAP 服务器的凭证。
CA 证书	上传 CA 证书并输入 Cisco Secure Workload 用于进行身份验证的 SSL 服务器名称。如果没有，请禁用 SSL。
服务器 IP/FQDN 和端口	输入服务器 IP 地址和端口号。
您的网络是否需要 HTTP 代理才能访问 IDENTITY？	（可选）Cisco Secure Workload 需要代理才能访问身份连接器。 如果是，请输入代理 URL 和端口号。
安全连接器	如果使用安全连接器从 Cisco Secure Workload 建立隧道连接，请启用此选项。在启用此选项之前，您应已部署安全连接器。 有关详细信息，请参阅安全连接器。

步骤 4 点击创建 (Create)。

图 *53:* 配置 *Active Directory* 连接器



系统将创建新的身份连接器，并在 Cisco Secure Workload 和 **Active Directory** 之间建立通信。

Active Directory 资产

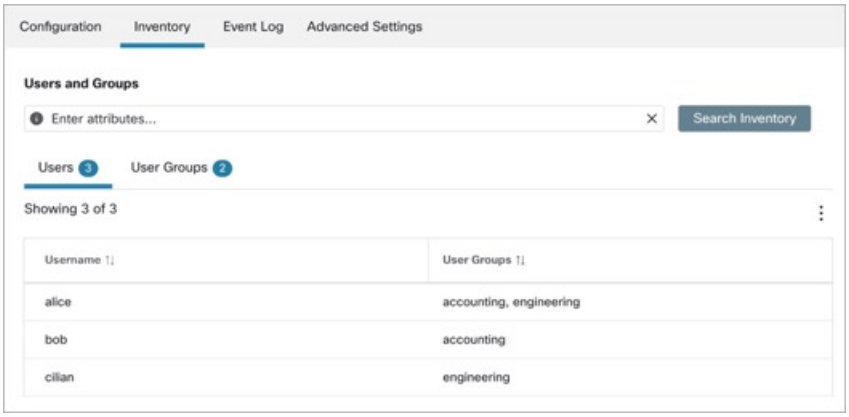
在 Cisco Secure Workload 和 Active Directory (AD) 之间建立连接后，您可以在**资产 (Inventory)** 选项卡中查看**用户 (Users)** 和 **用户组 (User Groups)** 的列表。用户所属的所有用户组都显示在**用户 (Users)** 选项卡中。**用户组 (User Groups)** 选项卡中仅显示唯一用户组。

过程

步骤 1 在**用户和组 (Users and Groups)** 下，输入要按其过滤的属性，然后点击“搜索资产”(Search Inventory)。将光标悬停在信息图标上，以查看要过滤的属性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 *54:* 用户和用户组



注释　显示的用户数限制为 300,000，而用户组为 30,000。

事件日志

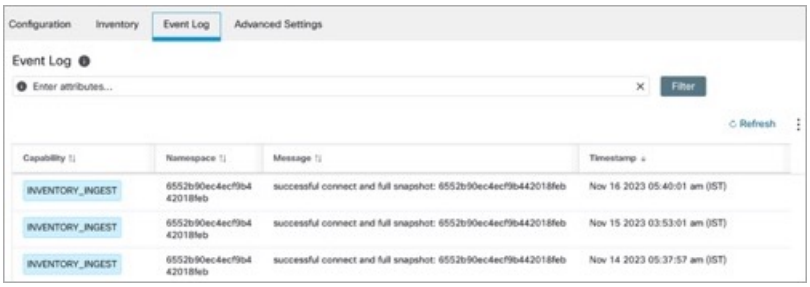
事件日志 (Event Log) 选项卡显示在与 OpenLDAP 建立连接时发生的信息、警告和错误。

过程

步骤 1 输入要过滤的属性。将光标悬停在信息图标上可查看要过滤的属性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 *55:* 事件日志



注释　日志的颜色代码为信息（蓝色）、警告（橙色）和错误（红色）。

高级设置

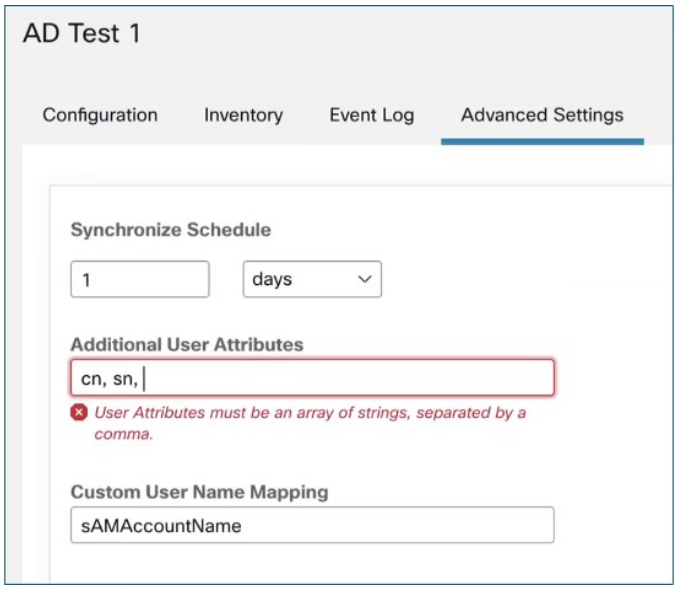
过程

步骤 1 在同步计划 **(Synchronize Schedule)** 下，您可以选择 Cisco Secure Workload 从 Active Directory 服务器同步用户数据的频率。

步骤 2 在用户属性 **(User Attributes)** 字段中，输入最多十五个要显示的用户属性。

步骤 3 在自定义用户名映射 **(User Name Mapping)** 字段中，将用户名映射到 **sAMAccountName**。

图 *56:* 高级设置



Microsoft Entra ID 连接器

Microsoft Entra ID（以前称为 Azure Active Directory）是一种基于云的身份和访问管理服务，可为用户、应用和服务提供身份验证和授权功能。通过使用 Active Directory 作为身份管理源，Cisco Secure Workload 中的身份连接器支持 Microsoft Entra ID。

配置 Microsoft Entra ID

在 Cisco Secure Workload 中为 Microsoft Entra ID 创建身份连接器，以便与 Microsoft Entra ID 建立通信。

过程

步骤 1 从导航窗格中，依次选择**管理 (Manage)** > **工作负载 (Workloads)** > **连接器 (Connectors)**。

步骤 2 点击**身份连接器 (Identity Connector)**，然后选择**在此处配置新连接器 (Configure your new connector here)**。

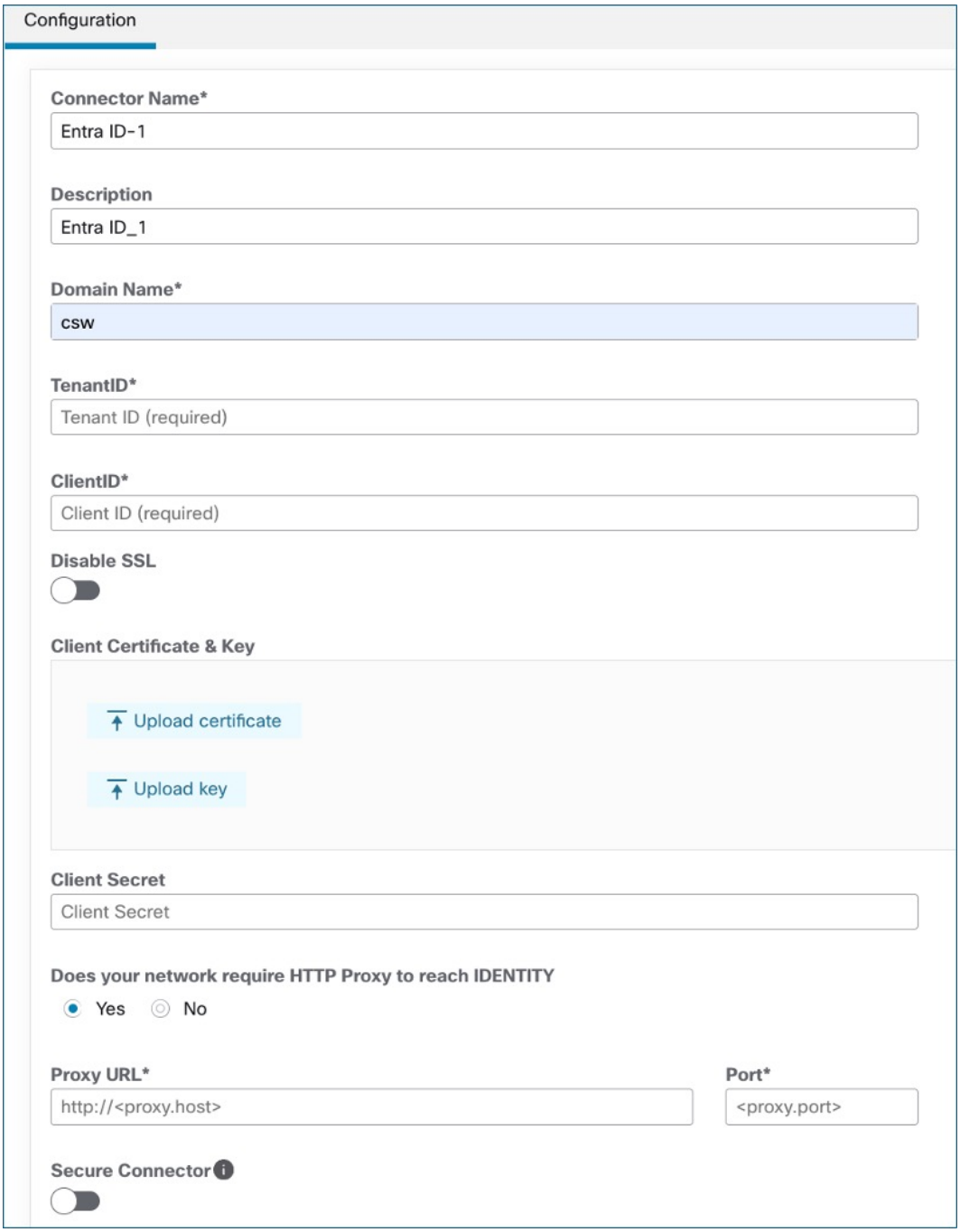
步骤 3 在**新建 Entra ID 连接 (New Entra ID Connection)** 页面中，输入以下详细信息：

字段	说明
连接器名称 (Connector Name)	输入连接器的名称。
说明 (Description)	输入说明。
域名 (Domain Name)	输入域名。域名在所选范围内必须是唯一的，例如 csw.com。
TenantID	您在此连接器的 Entra ID 中创建的**应用 TenantID**。
ClientID	您以此连接器的 Entra ID 创建的应用中的 **Director ClientID** 。
客户端密钥或客户端证书和密钥	对于身份验证，可以使用客户端密钥或客户端证书和密钥。从您以 Entra ID 为此连接器创建的应用中的**客户端凭证 (Client credentials)** 链接获取。如果使用证书：证书应未加密。仅支持 RSA 证书。私钥可以是 PKCS1 或 PKCS8。
CA 证书	上传 CA 证书并输入 Cisco Secure Workload 用于进行身份验证的 SSL 服务器名称。如果没有，请**禁用 SSL**。
您的网络是否需要 HTTP 代理才能访问 IDENTITY？	根据您的网络是否需要 HTTP 代理，选中**是 (Yes)** 或**否 (No)**。

字段	说明
安全连接器 (Secure Connector)	在安全连接器用于通过隧道连接从 Cisco Secure Workload 到 OpenLDAP 时启用。 在启用此选项之前，您应已部署安全连接器。 有关详细信息，请参阅安全连接器。

步骤 4 点击**创建 (Create)**。

图 *57:* 配置新的 ***Entra ID*** 连接器



系统将创建新的身份连接器，并在 Cisco Secure Workload 和 Entra ID 之间建立通信。

Microsoft Entra ID 资产

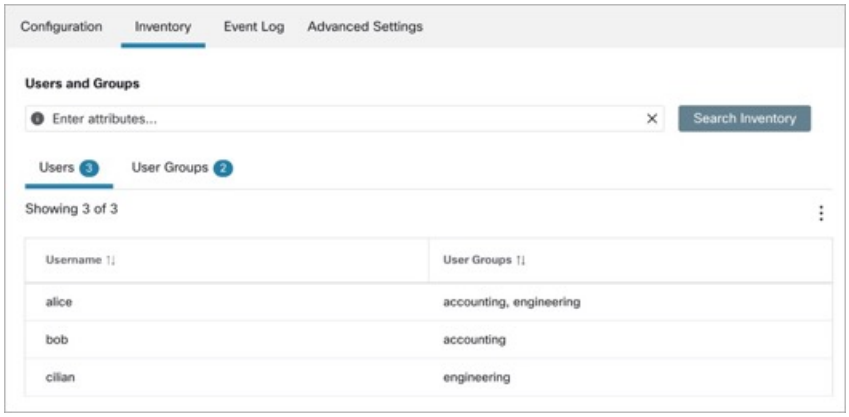
在 Cisco Secure Workload 和 Microsoft Entra ID 之间建立连接后，您可以在**资产 (Inventory)** 选项卡中查看用户和用户组的列表。用户所属的所有用户组都显示在**用户 (Users)** 选项卡中。**用户组 (User Groups)** 选项卡中仅显示唯一用户组。

过程

步骤 1 输入要过滤的属性。将光标悬停在信息图标上可查看要过滤的属性特性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 ***58:*** 用户和用户组



注释　显示的用户数限制为 300,000，而用户组为 30,000。

Microsoft Entra ID 事件日志

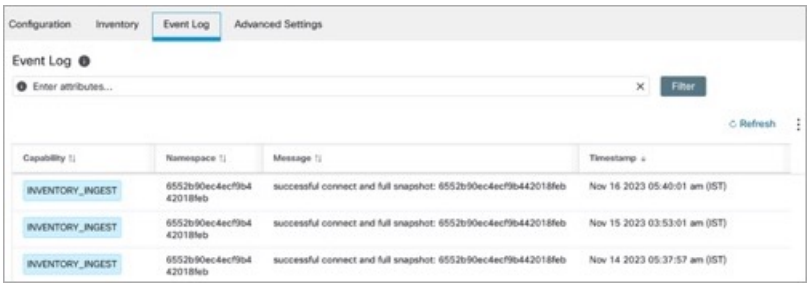
事件日志 (Event Log) 选项卡显示在与 Microsoft Entra ID 建立连接时发生的信息、警告和错误。

过程

步骤 1 输入要过滤的属性。将光标悬停在信息图标上可查看要过滤的属性。

步骤 2 点击菜单图标以下载 JSON 或 CSV 格式的数据。

图 *59:* 事件日志



注释　日志的颜色代码为信息（蓝色）、警告（橙色）和错误（红色）。

高级设置

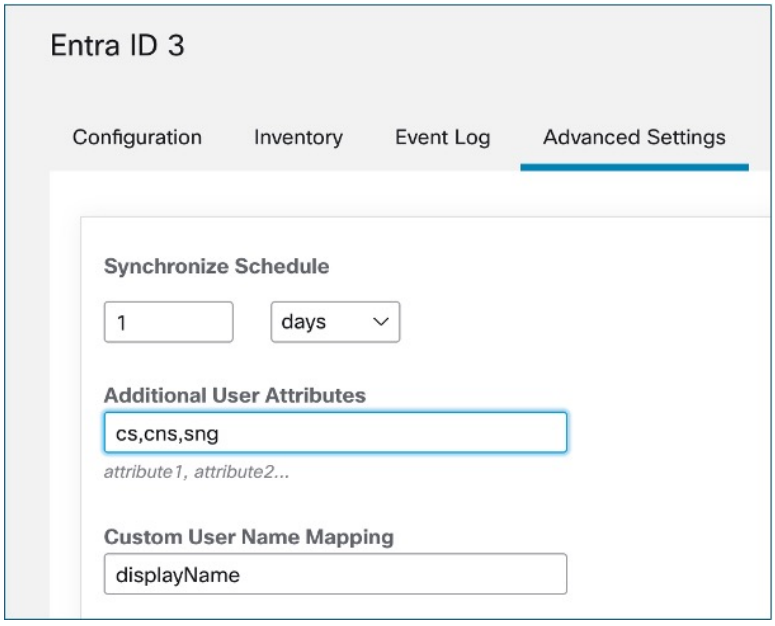
过程

步骤 1 在同步计划 **(Synchronize Schedule)** 下，选择 Cisco Secure Workload 同步 Active Directory 中的用户数据的频率。

步骤 2 在用户属性 **(User Attributes)** 字段中，输入最多六个要显示的用户属性。

步骤 3 在自定义用户名映射 **(User Name Mapping)** 字段中，将用户名映射到 **displayName**。

图 *60:* 高级设置



连接器警报

设备或服务在遇到异常行为时会创建连接器警报。

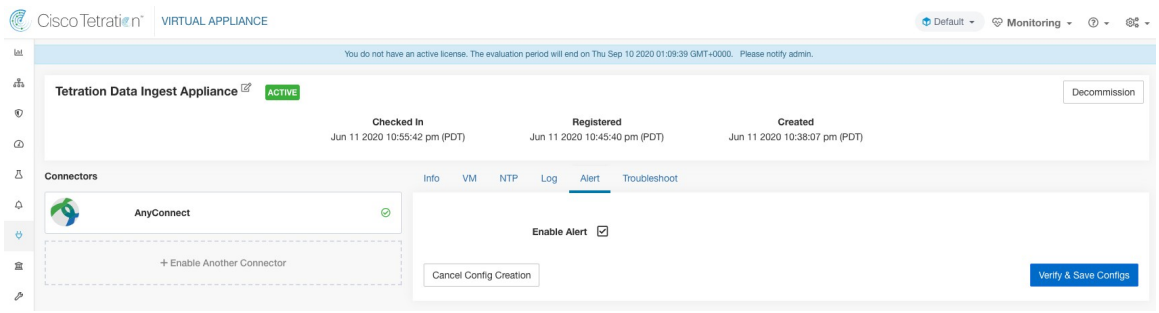
警报配置

设备和连接器的警报配置可让您针对各种事件生成警报。在 3.4 版本中，此配置可启用已配置设备/连接器可能发出的所有类型警报。

参数名称	类型	说明
启用警报	复选框	是否应启用警报？

Note 启用警报 *(Enable Alert)* 的默认值为 *true*。

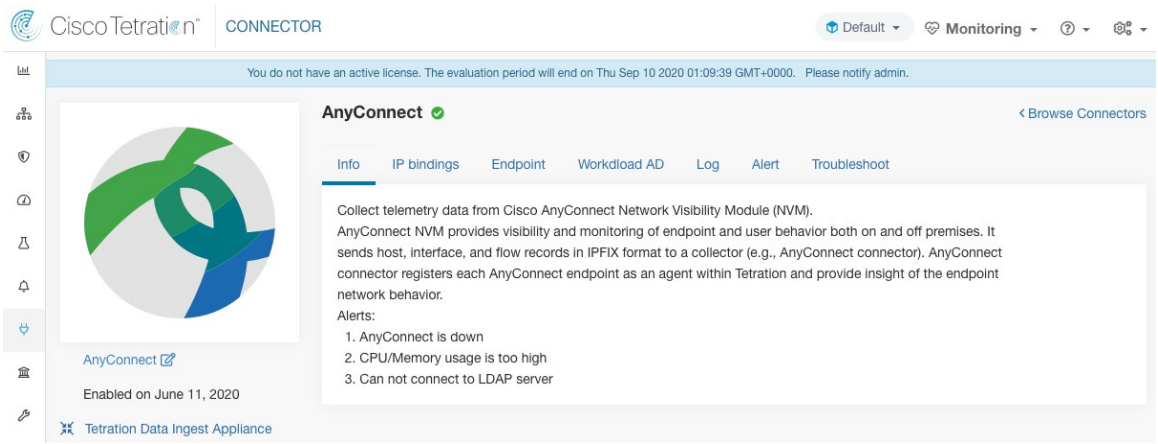
Figure 61: 显示 ***Cisco Secure Workload*** 数据注入设备上的警报配置



警报类型

设备和连接器页面上的“信息”(Info) 选项卡包含特定于每台设备和连接器的各种警报类型。

Figure 62: 警报列表信息



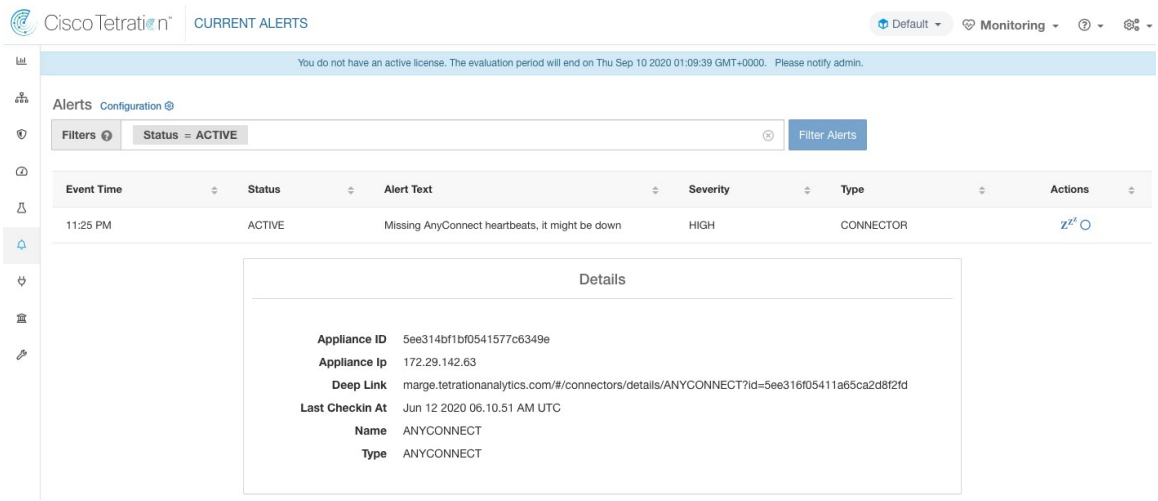
设备/连接器关闭

如果设备（或连接器）由于缺少来自设备/连接器的心跳而可能关闭，则会生成警报。

警报文本：缺失 <Appliance/Connector> 心跳，它可能已关闭。

严重性：高

Figure 63: 连接器关闭的警报



允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备

允许的连接器：全部

设备/连接器系统使用情况

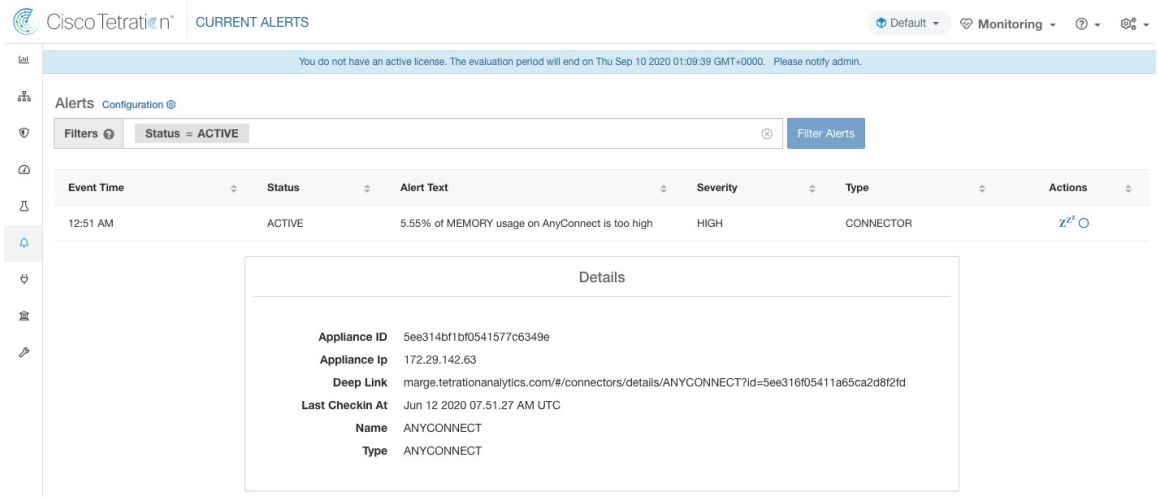
当设备（和连接器）上的系统使用率（CPU、内存和磁盘）超过 90% 时。设备（和/或连接器）会生成一个信息警报，提示当前正在处理增加的系统负载。

在繁重的处理活动中，设备和连接器消耗 90% 以上的系统资源是正常的。

警报文本：<Appliance/Connector> 上的 <Number> 个 CPU/内存磁盘使用率太高。

严重性：高

Figure 64: 连接器系统使用率过高的警报



允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备

允许的连接器：全部

连接器配置错误

当您尝试将已配置的连接器连接到已配置的服务器并且配置失败时，系统会生成警报，以指明在接受并部署配置后可能存在问题。

例如，AnyConnect 连接器可以采用 LDAP 配置，验证和接受配置。但在正常操作期间，配置可能不再有效。

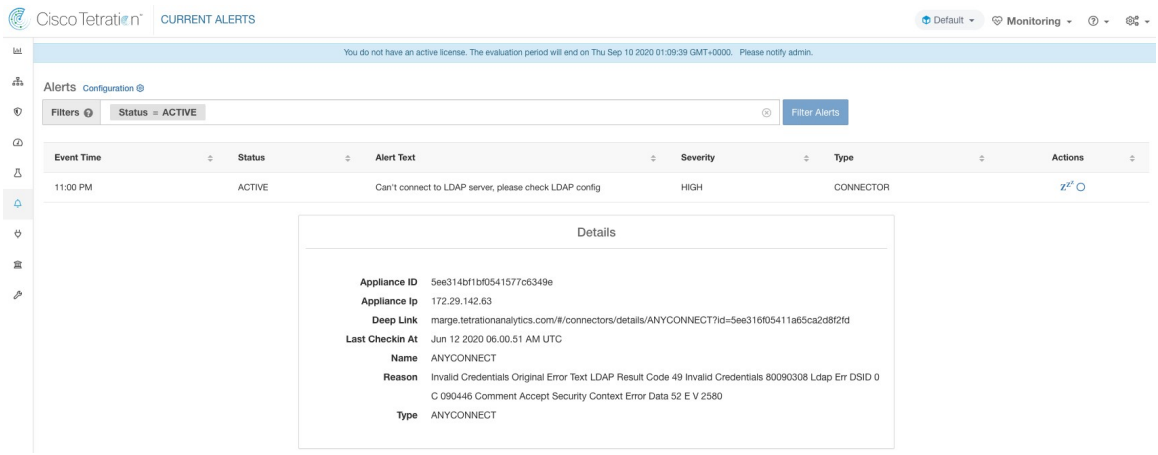
警报会捕捉到这种情况，并指出您必须采取纠正措施来更新配置。

警报文本：无法连接到 <Appliance/Connector> 服务器，检查 <Appliance/Connector> 配置。

严重性：高、低

服务器	连接器
LDAP 服务器	AnyConnect、F5、ISE、WDC
ISE 服务器	ISE
ServiceNow 服务器	ServiceNow

Figure 65: 配置状态错误警报

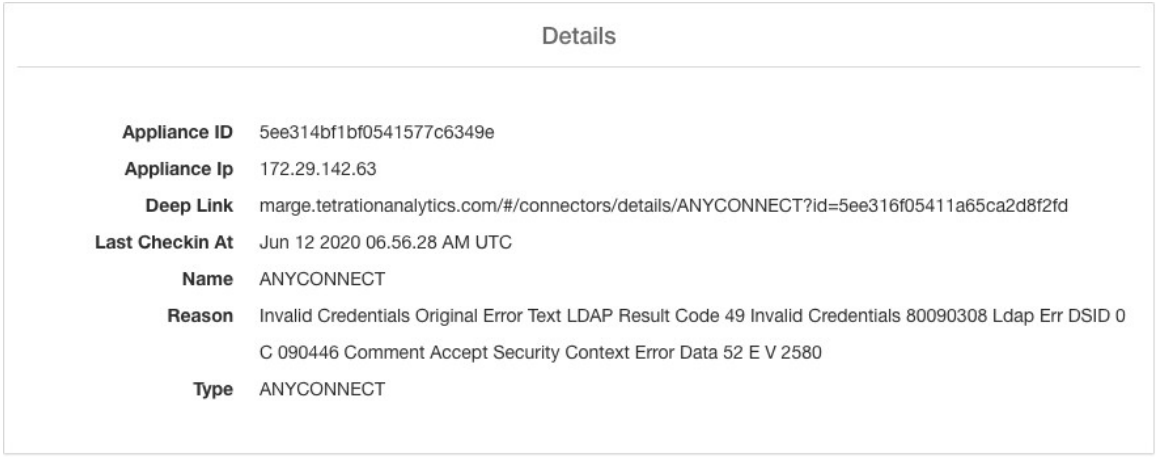


允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备。

允许的连接器：AnyConnect、F5、ISE、WDC 和 ServiceNow。

连接器 UI 警报详细信息

Figure 66: 连接器 *UI* 警报详细信息



警报详细信息

有关一般警报结构和有关字段的信息，请参阅通用警报结构 。*alert_details* 字段结构包含连接器警报的以下子字段。

字段	类型	说明
设备 ID (Appliance ID)	字符串	设备 ID

字段	类型	说明
设备 IP (Appliance IP)	字符串	设备 IP
连接器 ID (Connector ID)	字符串	连接器 ID
连接器 IP (Connector IP)	字符串	连接器 IP
深度链接 (Deep Link)	超链接	重定向到“设备/连接器”页面
上次签入时间 (Last CheckIn At)	字符串	上次签入时间
名称 (Name)	字符串	设备/连接器名称
原因 (Reason)	字符串	设备/连接器无法连接到 Cisco Secure Workload 的原因
类型 (Type)	字符串	设备/连接器类型

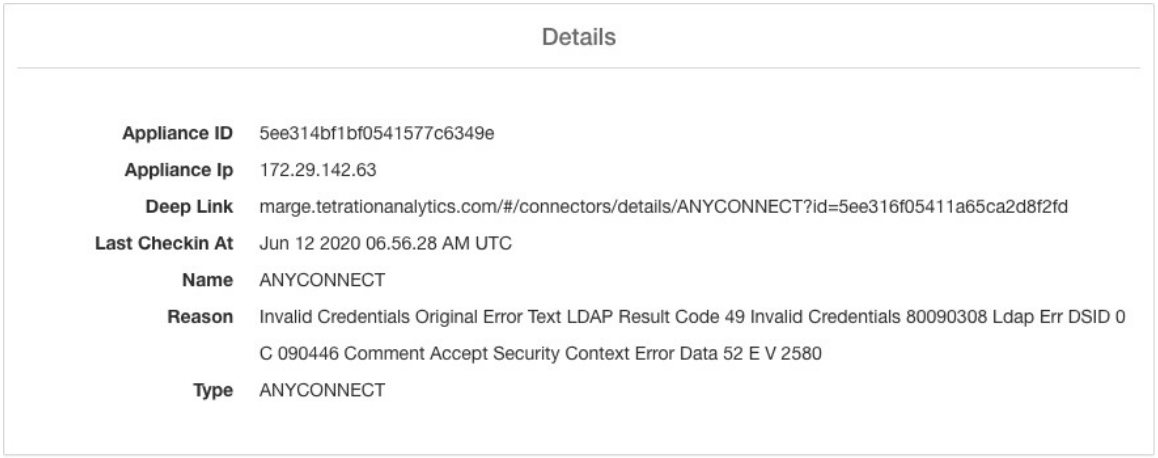
警报详细信息示例

在将 alert_details 解析为 JSON（未字符串化）后，它将显示如下。

```
    {
      "Appliance ID": "5f1f3d26d674b01832c6792a",
      "Connector ID": "5f1f3e47baba512a70abee43",
      "Connector IP": "172.29.142.22",
      "Deep Link":
"bingo.tetrationanalytics.com/#/connectors/details/F5?id=5f1f3e47baba512a70abee43",
      "Last checkin at": "Aug 04 2020 20.37.33 PM UTC",
      "Name": "F5",
      "Reason": "Invalid Credentials (Original error text: LDAP Result Code 49 \"Invalid
Credentials\": )",
      "Type": "F5"
    }
```

连接器 UI 警报详细信息

Figure 67: 连接器 *UI* 警报详细信息



连接器的生命周期管理

连接器可以直接从 Cisco Secure Workload 进行启用、部署、配置、故障排除和删除。

启用连接器

在“连接器”(Connectors) 页面（**管理 (Manage)** > **连接器 (Connectors)** ）中，可以选择并启用连接器。连接器可以部署在新的虚拟设备（必须先调配并变为活动状态，然后才能在其上启用连接器）或现有虚拟设备上。选择虚拟设备后，Cisco Secure Workload 会将连接器的 rpm 软件包发送到设备。

当所选设备上的设备控制器收到 rpm 时，它会执行以下操作：

1. 使用从 Cisco Secure Workload 收到的 rpm 软件包构建 Docker 映像。此 Docker 映像包括与发送设备管理消息的 Kafka 主题通信所需的配置。这使得从该映像实例化的服务能够发送和接收用于管理相应连接器的消息。
2. 从 Docker 映像创建 Docker 容器。
3. 在 Cisco Secure Workload 注入设备上，将执行以下附加任务。
   - 识别空闲插槽并确定相应的 IP 地址。
   - 连接器侦听端口（例如，NetFlow 连接器上的 4729 和 4739 端口，用于接收来自 NetFlow V9 或启用 IPFIX 的交换机和路由器的流记录），通过与所选插槽相对应的 IP 向主机公开。
   - 系统将创建 Docker 卷并将其添加到容器中。
4. Docker 容器已启动，并将连接器作为监督托管服务来执行。服务会将服务控制器作为 *tet-controller* 启动，该控制器会向 Cisco Secure Workload 注册并生成实际的连接器服务。

***Figure 68: Docker* 映像**

```
[root@beretta-ingest-1 tetter]# docker images
REPOSITORY                                              TAG                 IMAGE ID            CREATED              SIZE
netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow  5d379fac6e37d85f2bdeff45  2635145b44c8        About a minute ago   650MB
tet-service-base                                        latest              6be171bbe648        4 days ago           519MB
artifacts.tet.wtf:6555/centos                           7.3.1611            c5d48e81b986        4 months ago         192MB
[root@beretta-ingest-1 tetter]#
```

***Figure 69: Docker* 卷**

```
[root@beretta-ingest-1 tetter]# docker volume ls
DRIVER              VOLUME NAME
local               373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439
[root@beretta-ingest-1 tetter]#
```

***Figure 70: Docker* 容器**

```
[root@beretta-ingest-1 tetter]# docker ps
CONTAINER ID        IMAGE                                                                                COMMAND                  CREATE
D              STATUS              PORTS                                                  NAMES
2c7a7ed4f853        netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45   "/usr/bin/supervisor…"   About
a minute ago   Up About a minute   172.29.142.26:4729->4729/udp, 172.29.142.26:4739->4739/udp   nf-5d379fac6e37d85f2bdeff45
[root@beretta-ingest-1 tetter]#
```

Figure 71: Docker 容器使用的插槽和公开端口列表


```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


Figure 72: Docker 容器公开的端口列表


```
[root@beretta-ingest-1 tetter]# docker port 2c7a7ed4f853
4729/udp -> 172.29.142.26:4729
4739/udp -> 172.29.142.26:4739
[root@beretta-ingest-1 tetter]#
```


Figure 73: 装载到容器的 ***Docker*** 卷


```
[root@beretta-ingest-1 tetter]# docker inspect --format='{{json .Mounts}}' 2c7a7ed4f853
[{"Type":"volume","Name":"373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439","Source":"/var/lib/docker/volumes/373b5b6
82a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439/_data","Destination":"/local/tetration","Driver":"local","Mode":"z","RW":tr
ue,"Propagation":""}]
[root@beretta-ingest-1 tetter]#
```


服务控制器负责以下功能：

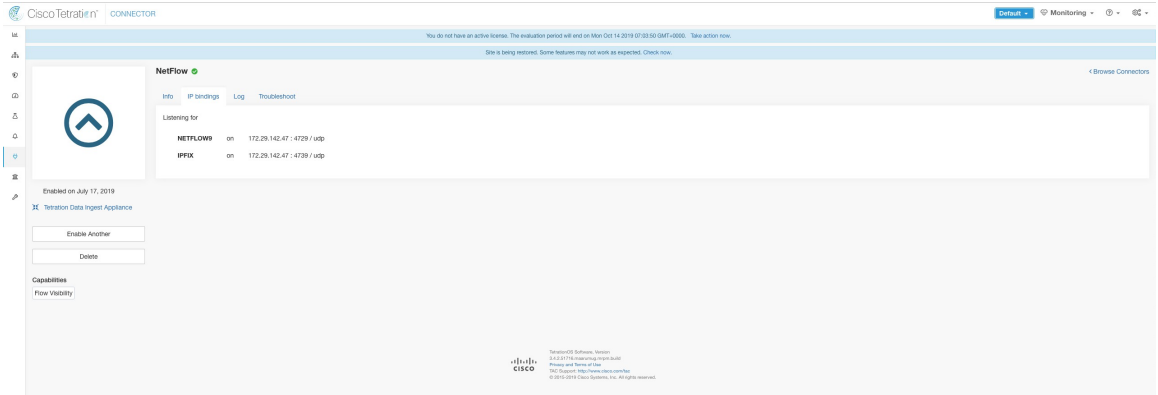
1. **注册**：向 Cisco Secure Workload 注册连接器。在连接器注册并标记为已启用 *(Enabled)* 之前，无法将任何配置更新推送到连接器。当 Cisco Secure Workload 收到连接器的注册请求时，它会将连接器的状态更新为已启用 *(Enabled)*。
2. **连接器上的配置更新**：测试并应用连接器上的配置更新。有关详细信息，请参阅连接器和虚拟设备上的配置管理。
3. 连接器上的**故障排除命令**：在连接器服务上执行允许的命令，以便对连接器服务上的问题进行故障排除和调试。有关更多信息，请参阅故障排除。
4. **心跳**：定期向 Cisco Secure Workload 发送心跳和统计信息，以报告连接器的运行状况。有关详细信息，请参阅监控虚拟设备。

查看连接器相关信息

已启用的连接器：点击窗口左侧导航栏中的**管理 (Manage)** > **连接器 (Connectors)**，可以找到所有已启用连接器的列表。

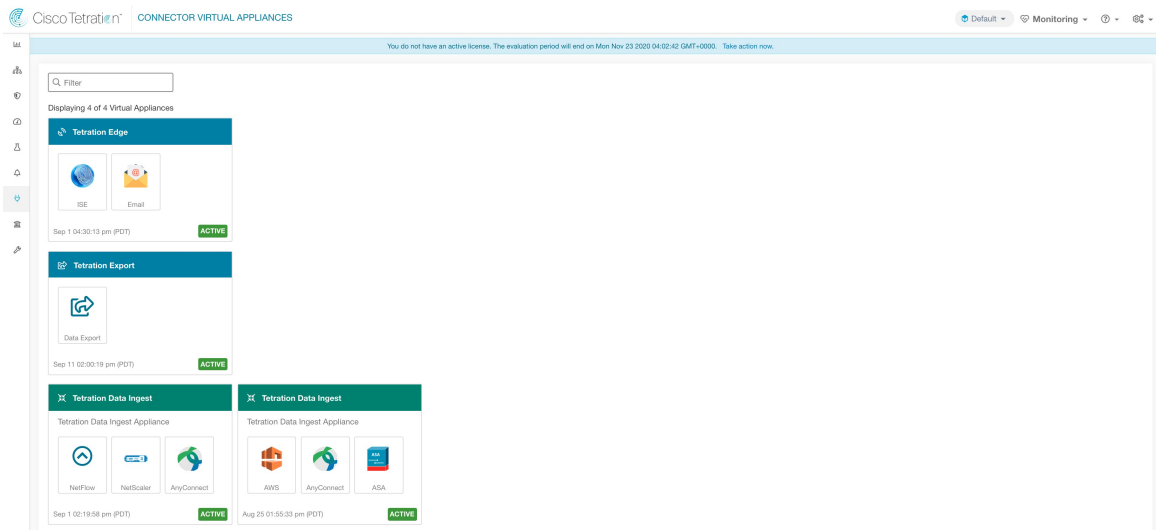
连接器详细信息：可以通过点击连接器获取有关连接器的详细信息。此页面显示端口绑定（如有），可用于配置上游网络元素将遥测数据发送到正确的 IP 和端口。

Figure 74: 连接器详细信息



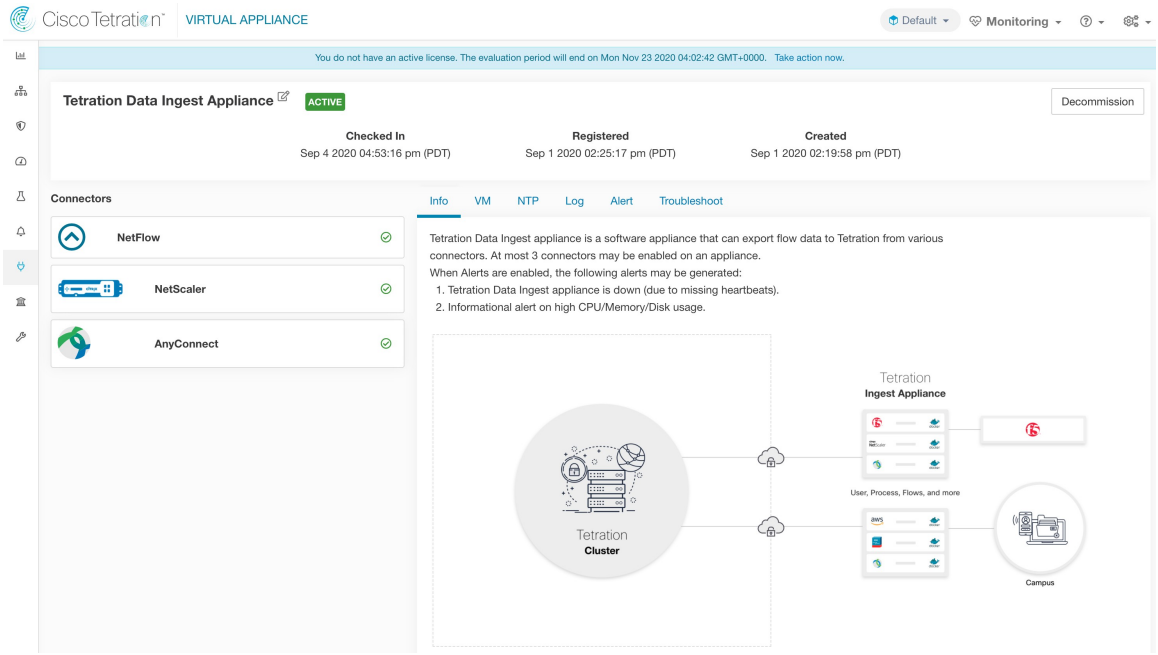
已部署的虚拟设备：可在以下位置找到已部署虚拟设备的列表：**管理 (Manage)** > **虚拟设备 (Virtual Appliances)**。

Figure 75: 已部署的虚拟设备列表



虚拟设备详细信息可以通过直接从已部署的虚拟设备列表中点击设备来获取设备的详细视图。

Figure 76: 设备详细信息和连接器



删除连接器

删除连接器时，启用连接器的设备上的设备控制器会收到一条信息，要求删除为连接器创建的服务。设备控制器执行以下操作：

1. 停止与连接器对应的 Docker 容器。

2. 删除 Docker 容器。
3. 如果连接器部署在 Cisco Secure Workload 注入设备上并且它会暴露端口，则删除装载到容器的 Docker 卷。
4. 删除为连接器创建的 Docker 映像。
5. 最后，将消息发送回 Cisco Secure Workload，指明删除请求的状态。

监控连接器

连接器服务会定期向 Cisco Secure Workload 发送心跳和统计信息。心跳间隔为 5 分钟。心跳消息包括有关服务运行状况的统计信息，其中包括系统统计信息、进程统计信息，以及通过用于设备管理的 Kafka 主题发送/接收/出错的信息数量统计信息。此外，它还包括连接器服务本身导出的统计信息。

所有指标均在 *Digger* (OpenTSDB) 中可用，并标注了设备 ID、连接器 ID 和根范围名称。此外，连接器服务的 Grafana 控制面板还可显示服务的重要指标。

连接器的虚拟设备

大多数连接器都部署在 Cisco Secure Workload 虚拟设备上。您将使用 OVA 模板在 VMware vCenter 的 ESXi 主机上部署所需的虚拟设备，或使用 QCOW2 映像在其他基于 KVM 的管理程序上部署所需的虚拟设备。部署虚拟设备中介绍了部署虚拟设备的程序。

虚拟设备类型

每个需要虚拟设备的连接器都可以部署在两种类型的虚拟设备中的任意一种上。

Cisco Secure Workload 注入

Cisco Secure Workload 注入设备是一种软件设备，可将流观察结果从各种连接器导出到 Cisco Secure Workload。

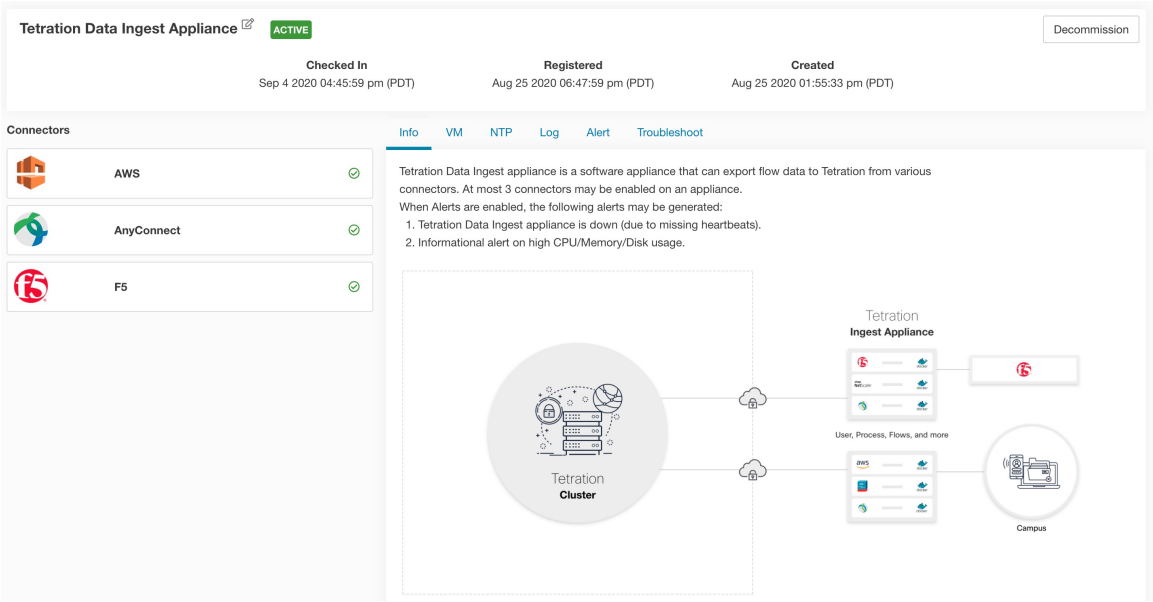
规格

- CPU 核心数量：8
- 内存：8 GB
- 存储：250 GB
- 网络接口数：3
- 一台设备上的连接器数量：3
- 操作系统：CentOS 7.9（Cisco Secure Workload 3.8.1.19 及更低版本）、AlmaLinux 9.2（Cisco Secure Workload 3.8.1.36 及更高版本）

请参阅适用于连接器的 Cisco Secure Workload 虚拟设备中的重要限制。

Note Cisco Secure Workload 上的每个根范围最多可以部署 100 台 Cisco Secure Workload 注入设备。

***Figure 77: Cisco Secure Workload* 注入设备**



Cisco Secure Workload 注入设备最多允许在一台设备上启用 3 个连接器。在同一设备上可以启用多个相同连接器的实例。对于 ERSPAN 注入设备，总是会自动配置三个 ERSPAN 连接器。注入设备上部署的许多连接器都从网络中的不同点收集遥测数据，这些连接器需要侦听设备上的特定端口。因此，每个连接器都与其中一个 IP 地址和默认端口绑定，连接器应在这些地址和端口上侦听，以收集遥测数据。因此，每个 IP 地址实质上就是设备上连接器占用的一个插槽。启用一个连接器后，就会占用一个插槽（从而占用该插槽对应的 IP）。而且，当某个连接器被禁用时，该连接器所占用的插槽也会被释放（从而释放与该插槽相对应的 IP）。有关如何在设备注入 维护插槽状态的信息，请参阅 *Cisco Secure Workload* 注入设备插槽。

Figure 78: Cisco Secure Workload 注入设备插槽


```
[root@beretta-ingest-1 tetter]# cat /local/tetration/appliance/appliance.conf
{
  "type": "TETRATION_DATA_INGEST",
  "slots": [
    {
      "available": false,
      "index": 0,
      "mapped_ip": "172.29.142.26",
      "share_volume": true,
      "count": 1,
      "service_containers": {
        "5d379fac6e37d85f2bdeff45": {
          "connector_id": "5d379fac6e37d85f2bdeff44",
          "service_id": "5d379fac6e37d85f2bdeff45",
          "container_id": "2c7a7ed4f853e85f3d620c663f1c7f5395b53b9dd6696276ac439d34fe142bf1",
          "image_name": "netflow_sensor-3.4.2.52222.maarumug.mrpm.build-netflow:5d379fac6e37d85f2bdeff45",
          "container_name": "nf-5d379fac6e37d85f2bdeff45",
          "service_type": "NETFLOW_SENSOR",
          "ip_bindings": [
            {
              "ip": "172.29.142.26",
              "port": "4729",
              "protocol": "udp"
            },
            {
              "ip": "172.29.142.26",
              "port": "4739",
              "label": 1,
              "protocol": "udp"
            }
          ],
          "volume_id": "373b5b682a96547bf2526784a5943c2f110593b88485b996e7259fa4e314c439"
        }
      }
    },
    {
      "available": true,
      "index": 1,
      "mapped_ip": "172.29.142.27",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    },
    {
      "available": true,
      "index": 2,
      "mapped_ip": "172.29.142.28",
      "share_volume": true,
      "count": 0,
      "service_containers": null
    }
  ]
}[root@beretta-ingest-1 tetter]#
```


允许的配置

- *NTP*：在设备上配置 NTP。有关详细信息，请参阅 NTP 配置。
- 日志：在设备上配置日志记录。有关详细信息，请参阅日志配置。

Cisco Secure Workload 边缘

Cisco Secure Workload 边缘是一种控制设备，可将警报流传输到各种通知程序，并从网络访问控制器（例如 Cisco ISE）收集资产元数据。在 Cisco Secure Workload 边缘设备中，可以部署所有警报通知程序连接器（例如 Syslog、Email、Slack、PagerDuty 和 Kinesis）、ServiceNow 连接器、Workload AD 连接器和 ISE 连接器。

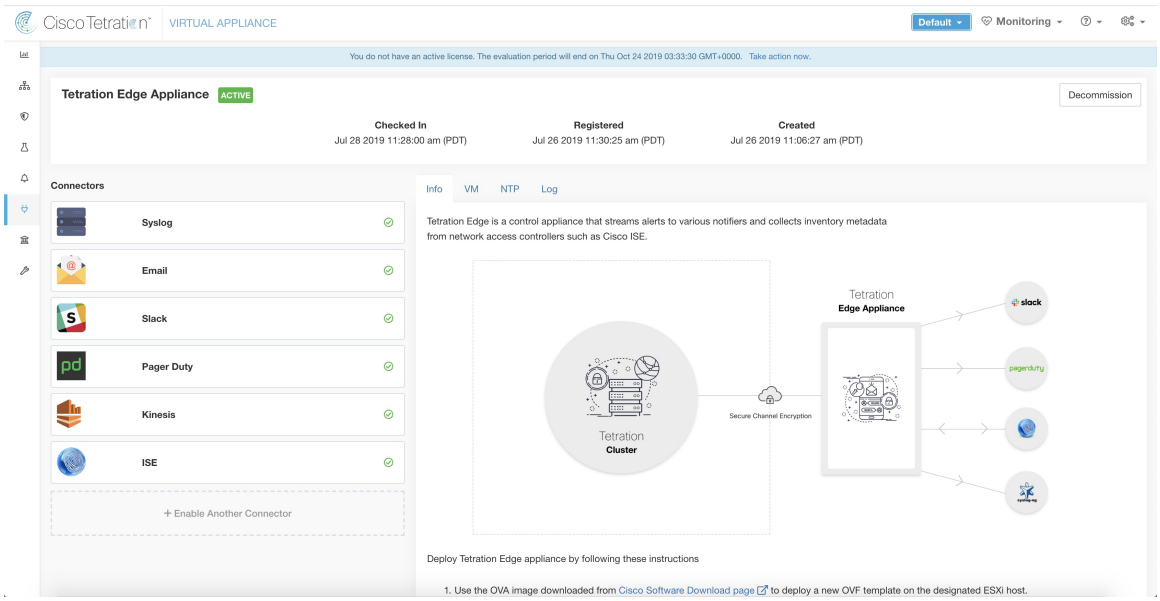
规格

- CPU 核心数量：8
- 内存：8 GB
- 存储：250 GB
- 网络接口数：1
- 一台设备上的连接器数量：8
- 操作系统：CentOS 7.9（Cisco Secure Workload 3.8.1.19 及更低版本）、AlmaLinux 9.2（Cisco Secure Workload 3.8.1.36 及更高版本）

请参阅适用于连接器的 Cisco Secure Workload 虚拟设备中的重要限制。

Note Cisco Secure Workload 上的每个根范围最多可以部署一个 Cisco Secure Workload 边缘设备。

***Figure 79: Cisco Secure Workload* 边缘设备**



Cisco Secure Workload 边缘设备上部署的连接器不会在端口上侦听。因此，为 Cisco Secure Workload 边缘设备上的连接器实例化的 Docker 容器不会向主机公开任何端口。

允许的配置

- *NTP*：在设备上配置 NTP。有关详细信息，请参阅 NTP 配置。
- 日志：在设备上配置日志记录。有关详细信息，请参阅日志配置。

部署虚拟设备

在 VMware vCenter 的 ESXi 主机或其他基于 KVM 的管理程序（如 Red Hat Virtualization）上部署虚拟设备。此程序会提示您从思科软件下载页面下载虚拟设备 OVA 模板或 QCOW2 映像。

Attention 要部署 Cisco Secure Workload 外部设备，在其中创建设备的 ESXi 主机应符合以下规格：

- **vSphere**：5.5 或更高版本。
- **CPU**：每个核心至少 2.2 GHz，并且有足够的可预留容量供设备使用。
- **内存**：至少有适合设备的足够空间。

要部署虚拟设备以从收集器收集数据，请执行以下操作：

Procedure

步骤 1 在 Cisco Secure Workload Web 门户中，从左侧导航栏中选择管理虚拟设备（**管理器 (Manage)** > **虚拟设备 (Virtual Appliances)**）。

步骤 2 点击**启用连接器 (Enable a Connector)**。您必须部署的虚拟设备类型取决于您要启用的连接器类型。

步骤 3 点击您必须为其创建虚拟设备的连接器类型。例如，点击 NetFlow 连接器。

步骤 4 在连接器页面上，点击**启用 (Enable)**。

步骤 5 如果看到通知您必须部署虚拟设备的通知，请点击**是 (Yes)**。如果未看到此通知，则可能已经有了该连接器可以使用的虚拟设备，在这种情况下无需执行此步骤。

步骤 6 点击链接下载虚拟设备的 OVA 模板或 QCOW2 映像。让向导在屏幕上保持打开，不要点击其他任何内容。

步骤 7 使用下载的：

- OVA 在指定的 ESXi 主机上部署新的 OVF 模板。
  - 要在 vSphere Web 客户端上部署 OVA，请按照有关如何部署 OVF 模板的说明进行操作。
  - 确保部署的虚拟机设置与虚拟设备类型的建议配置相匹配。
  - **不启动已部署的 VM**
- QCOW2 映像，以便在 KVM 虚拟机监控程序（例如 Red Hat Virtualization）上创建新 VM。

步骤 8 在部署 VM 之后、打开电源之前，请返回 Cisco Secure Workload Web 门户中的虚拟设备部署向导。

步骤 9 在虚拟设备部署向导中点击**下一步 (Next)**。

步骤 10 通过提供 IP 地址、网关、主机名、DNS、代理服务器设置和 Docker 桥子网配置来配置虚拟设备。请参阅使用网络参数配置 *VM* 的屏幕截图。

- 如果设备必须使用代理服务器访问 Cisco Secure Workload，请选中使用代理服务器连接到 *Cisco Secure Workload (Use proxy server to connect to Secure Workload)*复选框。如果此设置不正确，连

接器可能无法与 Cisco Secure Workload 通信，因此无法获取控制消息、注册连接器以及将流数据发送到 Cisco Secure Workload 收集器。

- 如果设备的 IP 地址和网关与默认 Docker 桥接子网 (*172.17.0.1/16*) 冲突，则可以使用 *Docker* 桥接（*CIDR* 格式）*(Docker Bridge [CIDR format])* 字段中指定的自定义 Docker 桥接子网来配置设备。这需要使用设备 OVA 3.3.2.16 或更高版本。

步骤 11 点击**下一步 (Next)**。

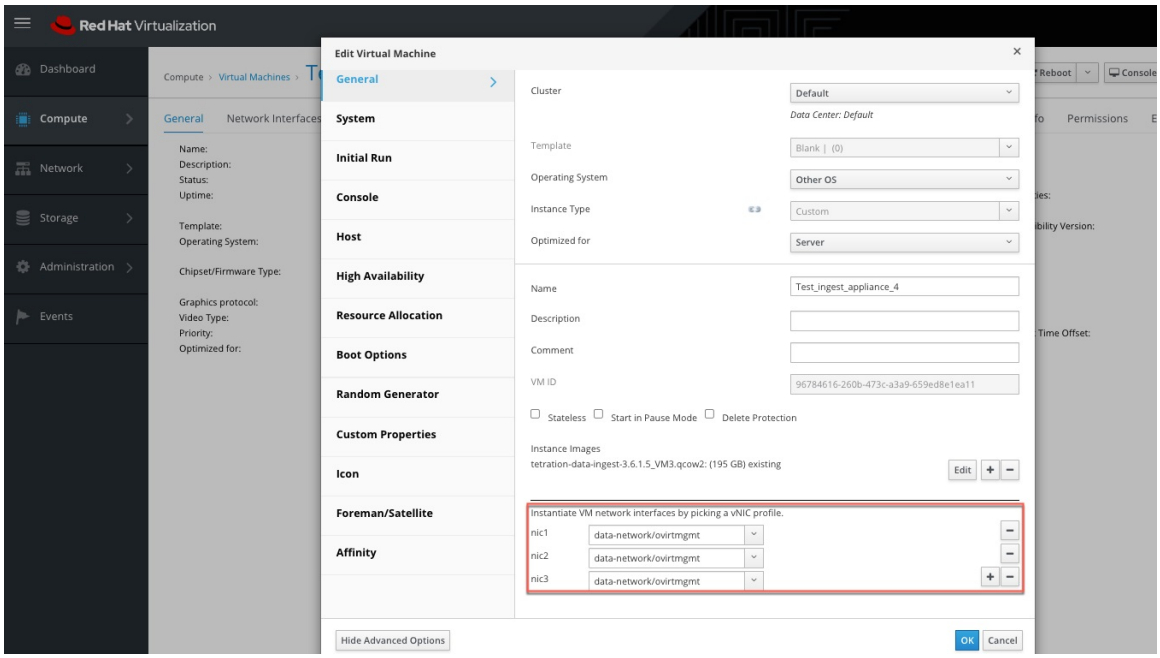
步骤 12 在下一步中将生成 VM 配置捆绑包，并且可供下载。下载 VM 配置捆绑包。请参阅下载 *VM* 配置捆绑包的屏幕截图。

步骤 13 将 VM 配置捆绑包上传到与目标 ESXi 主机或其他虚拟化主机对应的数据存储区。

步骤 14 [**仅当使用 QCOW2 映像时适用**] 在已上传 VM 配置捆绑包的其他虚拟化主机上完成以下配置：

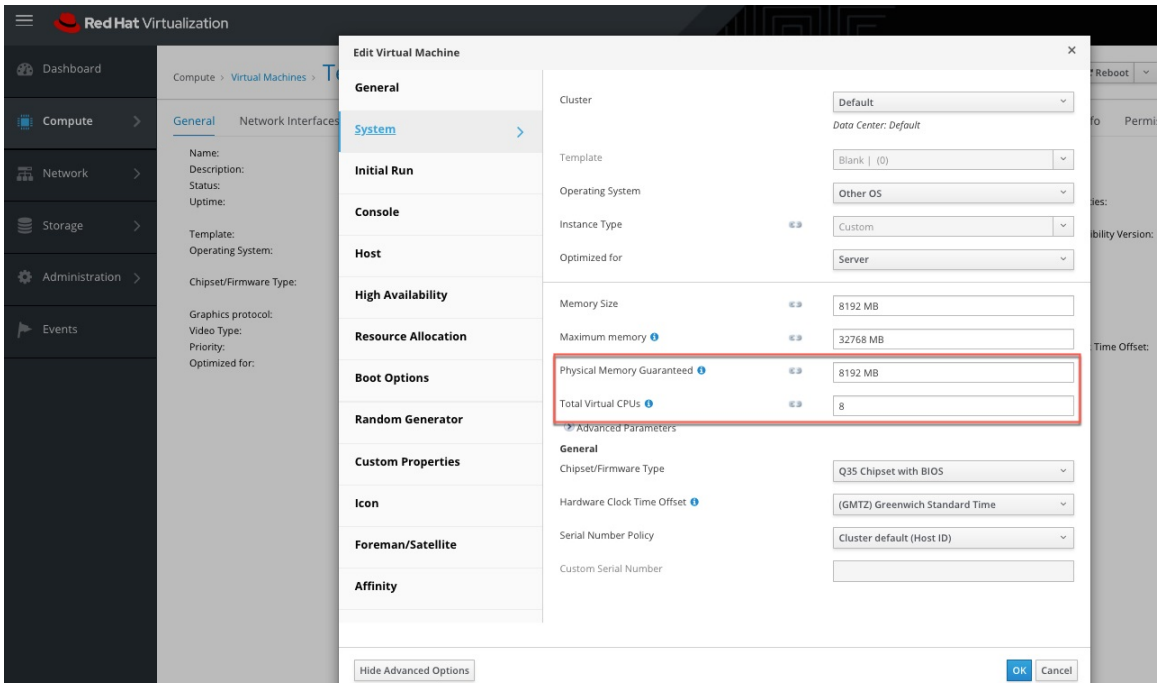
- 对于注入设备，请配置三个网络接口。

Figure 80: **在基于 *KVM* 的环境中配置网络接口的示例**



- 在内存分配中，指定 8192 MB RAM 的最低要求。
- 将虚拟 CPU 的总数指定为 8。

Figure 81: 在基于 ***KVM*** 的环境中配置系统资源的示例



步骤 15 编辑 VM 设置，并将 VM 配置捆绑包从 Datastore 装载到 CD/DVD 驱动器。确保选中**启动时连接 (Connect at Power On)** 复选框。

步骤 16 打开已部署虚拟机的电源。

步骤 17 当 VM 启动并自行配置时，它会连接回 Cisco Secure Workload。此过程可能需要几分钟。Cisco Secure Workload 上的设备状态应从待注册 *(Pending Registration)* 转换为活动 *(Active)*。请参阅 处于待注册状态的 *Cisco Secure Workload* 注入设备的屏幕截图。

Note 我们不建议为 Cisco Secure Workload 外部设备启用 vMotion。

Note 我们建议按原样使用 Cisco Secure Workload 外部设备 OVA，并为 QCOW2 映像预留 8 个 vCPU 核心和 8192 MB 内存，用以部署虚拟机。如果没有足够的资源，VM 设置脚本将在启动后失败。

当设备处于活动状态时，即可在设备上启用和部署连接器。

Figure 82: 部署 ***Cisco Secure Workload*** 注入设备

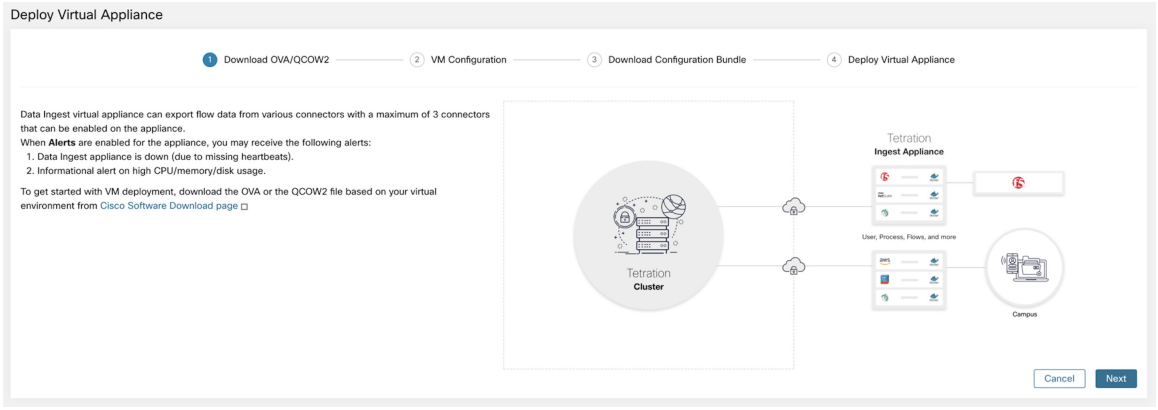


Figure 83: 使用网络参数配置 ***VM***

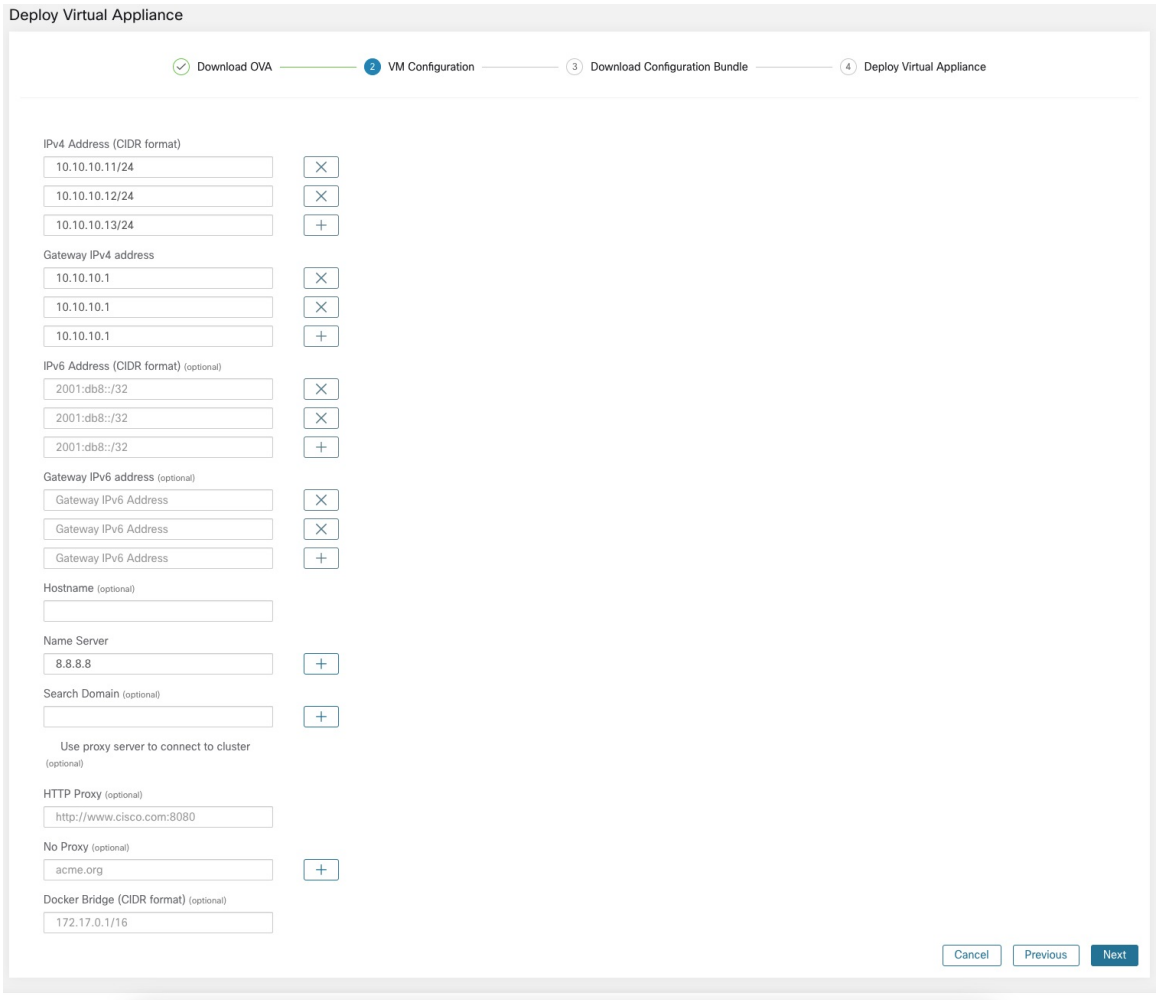


Figure 84: 下载 ***VM*** 配置捆绑包

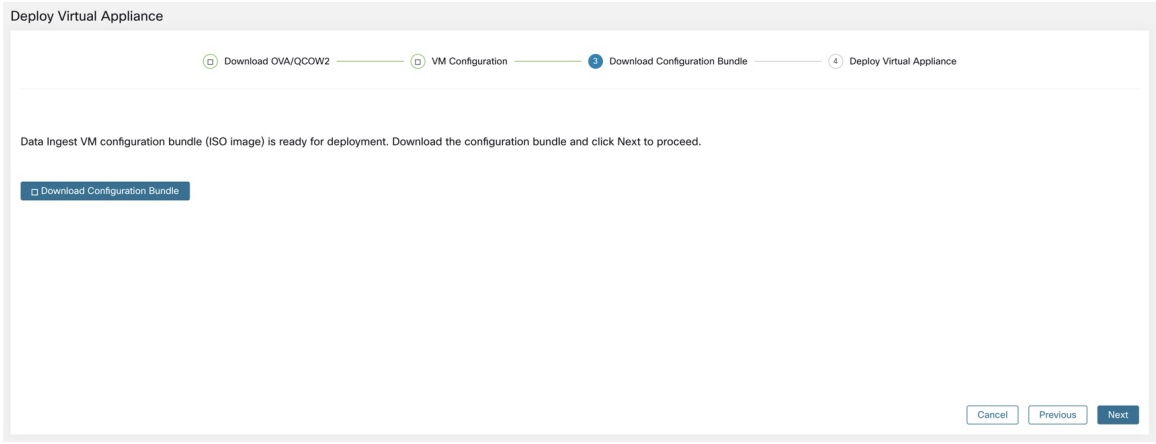


Figure 85: 部署 ***VM***

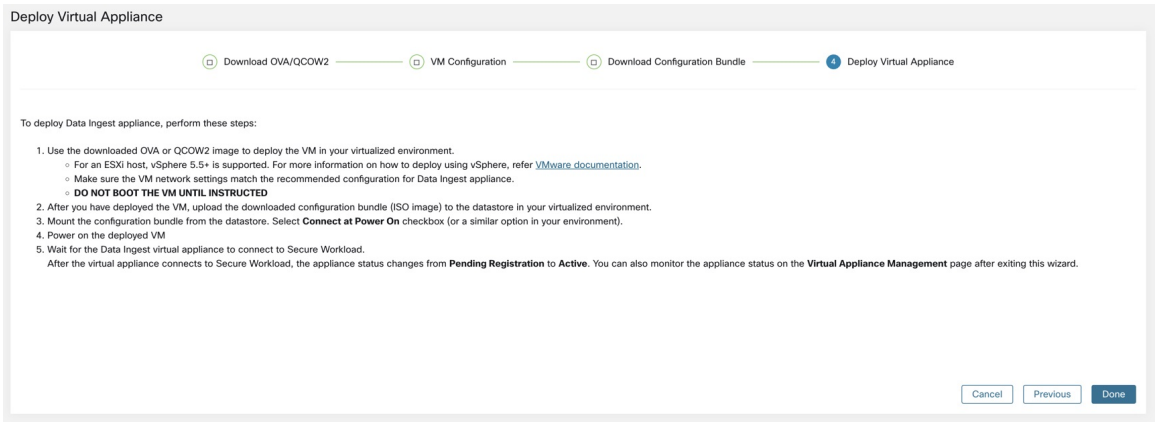
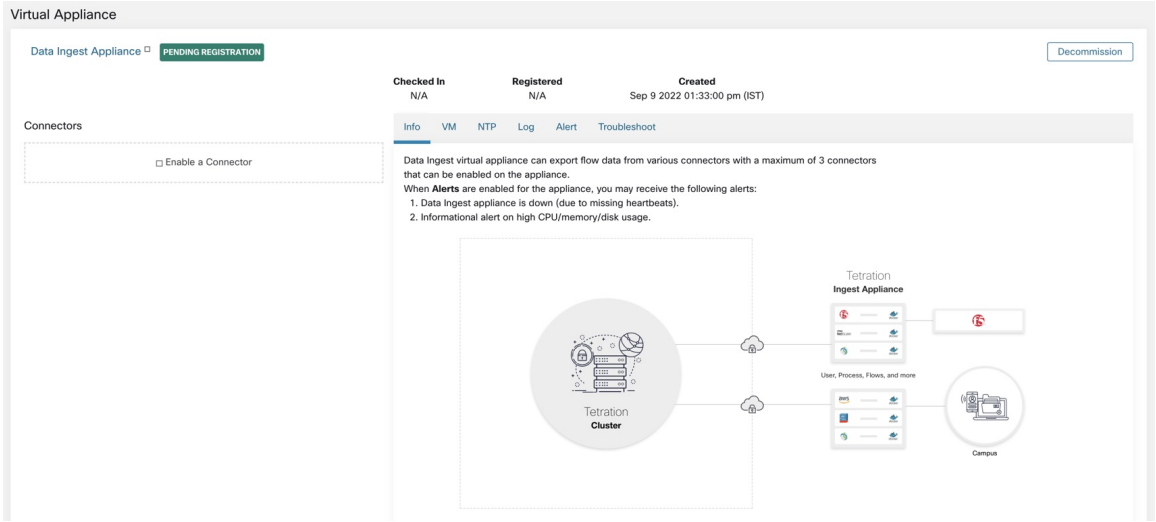


Figure 86: Cisco Secure Workload 注入设备处于待注册状态



首次部署和启动虚拟设备时，*tet-vm-setup* 服务会执行并设置设备。此服务负责执行以下任务：

a. **验证设备**：验证设备是否符合所部署虚拟设备类型的强制性资源要求。

b. **IP 地址分配**：为设备上调配的所有网络接口分配 IP 地址。

c. **主机名分配**：为设备分配主机名（如果已配置主机名）。

d. **DNS 配置**：更新 DNS resolv.conf 文件（如果已配置名称服务器和/或搜索域参数）。

e. **代理服务器配置**：更新设备（如已提供）上的 HTTPS_PROXY 和 NO_PROXY 设置。

f. **准备设备**：复制用于发送和接收设备管理消息的 Kafka 主题的证书捆绑包。

g. **安装设备控制器**：安装并启动由 SuperVision 作为 *tet-controller* 服务托管的设备控制器。

当 *tet-controller* 实例化时，它将接管设备的管理。此服务负责以下功能：

a. **注册**：向 Cisco Secure Workload 注册设备。在注册设备之前，无法在设备上启用任何连接器。当 Cisco Secure Workload 收到设备的注册请求时，它会将设备的状态更新为活动。

b. **部署连接器**：将连接器部署为设备上的 Docker 服务。有关详细信息，请参阅启用连接器。

c. **删除连接器**：停止并从设备中删除 Docker 服务和相应的 Docker 映像。有关详细信息，请参阅删除连接器。

d. **设备上的配置更新**：测试并应用设备上的配置更新。有关详细信息，请参阅连接器和虚拟设备上的配置管理。

e. **设备上的故障排除命令**：在设备上执行允许的命令集，以便对设备上的问题进行故障排除和调试。有关更多信息，请参阅故障排除。

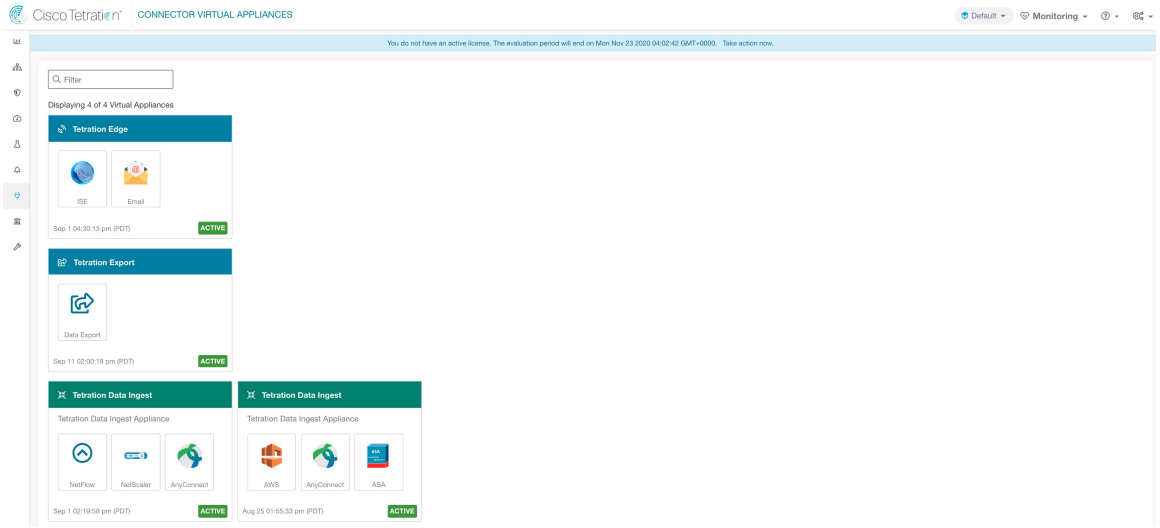
f. **心跳**：定期向 Cisco Secure Workload 发送心跳和统计信息，以报告设备的运行状况。有关详细信息，请参阅监控虚拟设备。

g. **修剪**：定期修剪所有未使用或悬空的 Docker 资源，以恢复存储空间。此任务每 24 小时执行一次。

h. **下线设备**：下线并删除设备中的所有 Docker 实例。有关详细信息，请参阅下线虚拟设备。

可在以下位置找到已部署虚拟设备的列表：**管理 (Manage)** > **虚拟设备 (Virtual Appliances)**

Figure 87: 已部署的虚拟设备列表



下线虚拟设备

可以从 Cisco Secure Workload 下线虚拟设备。当设备下线时，会触发以下操作。

1. 设备上的所有配置和设备上启用的连接器都将被删除。
2. 设备上所有启用的连接器都将被删除。
3. 设备标记为待删除 *(Pending Delete)*。
4. 当设备回复成功的删除响应时，系统会删除设备 Kafka 主题和证书。

Note 设备下线无法撤消。要恢复设备和连接器，应部署新设备并在新设备上启用连接器。

监控虚拟设备

Cisco Secure Workload 虚拟设备会定期向 Cisco Secure Workload 发送心跳和统计信息。心跳间隔为 5 分钟。心跳消息包括有关设备运行状况的统计信息，其中包括系统统计信息、进程统计信息，以及通过用于设备管理的 Kafka 主题发送/接收/出错的信息数量统计信息。

所有指标均在 *Digger* (OpenTSDB) 中可用，并标注了设备 ID 和根范围名称。此外，设备控制器的 Grafana 控制面板也可用于设备中的重要指标。

安全注意事项

注入/边缘虚拟机的访客操作系统是 CentOS 7.9，其中的 OpenSSL 服务器/客户端软件包已被移除。因此，访问设备的唯一途径是通过其控制台。

Note CentOS 7.9 是 Cisco Secure Workload 3.8.1.19 及更早版本中注入和边缘虚拟设备的访客操作系统。从 Cisco Secure Workload 3.8.1.36 开始，操作系统为 AlmaLinux 9.2。

容器运行基于 centos:7.9.2009 的 Docker 映像。除了 ERSPAN 容器具有 NET_ADMIN 功能外，大多数容器都以基本权限（无 –privileged 选项）运行。

Note 从 Cisco Secure Workload 3.8.1.36 开始，容器运行 almalinux/9-base:9.2。

万一容器被入侵，虚拟机客户操作系统也无法从容器内部入侵。

连接器和虚拟设备上的配置管理

配置更新可以从 Cisco Secure Workload 推送到设备和连接器。设备应已成功向 Cisco Secure Workload 注册并处于活动状态，然后才能启动配置更新。同样，连接器应先向 Cisco Secure Workload 注册，然后才能在连接器服务上启动配置更新。

设备和连接器有三种配置更新模式。

1. **测试并应用**：测试配置，并在测试成功后提交配置。
2. **发现**：测试配置，并在测试成功后发现可以为配置启用的其他属性。
3. **删除**：删除配置。

Note ERSPAN 设备和连接器不支持配置更新。

测试并应用

支持测试并应用模式的配置会先验证配置，然后再在所需设备和/或连接器上应用（提交）配置。

NTP 配置

NTP 配置允许设备与指定的 NTP 服务器同步时钟。

参数名称	类型	说明
启用 NTP (Enable NTP)	复选框	是否应启用 NTP 同步？
NTP 服务器 (NTP Servers)	listof 字符串	NTP 服务器的列表。应至少提供一台服务器，最多可提供 5 台服务器。

测试：测试是否可以在端口 123 上与给定 NTP 服务器建立 UDP 连接。如果任何 NTP 服务器发生错误，请不要接受配置。

应用：更新 `/etc/ntp.conf` 并使用 systemctl restart ntpd.service 重启 ntpd 服务。以下是用于生成 *ntp.conf* 的模板

```
# --- GENERAL CONFIGURATION ---
server <ntp-server>
...
server 127.127.1.0
fudge 127.127.1.0 stratum 10
# Drift file
driftfile /etc/ntp/drift
```

Note 适用于 Cisco Secure Workload 3.8.1.19 及更低版本。

对于 Cisco Secure Workload 3.8.1.36 及更高版本，请更新 `/etc/chrony.conf` 并使用 systemctl restart chronyd.service 重启 chronyd 服务。以下是用于生成 *chrony.conf* 的模板

```
# Secure Workload appliance chrony.conf.
server <ntp-server> iburst
...
driftfile /var/lin/chrony/drift
makestep 1.0 3
rtcsync
```

允许的思科 Cisco Secure Workload 虚拟设备：全部

允许的连接器：无

Figure 88: 测试 *NTP* 配置时出错

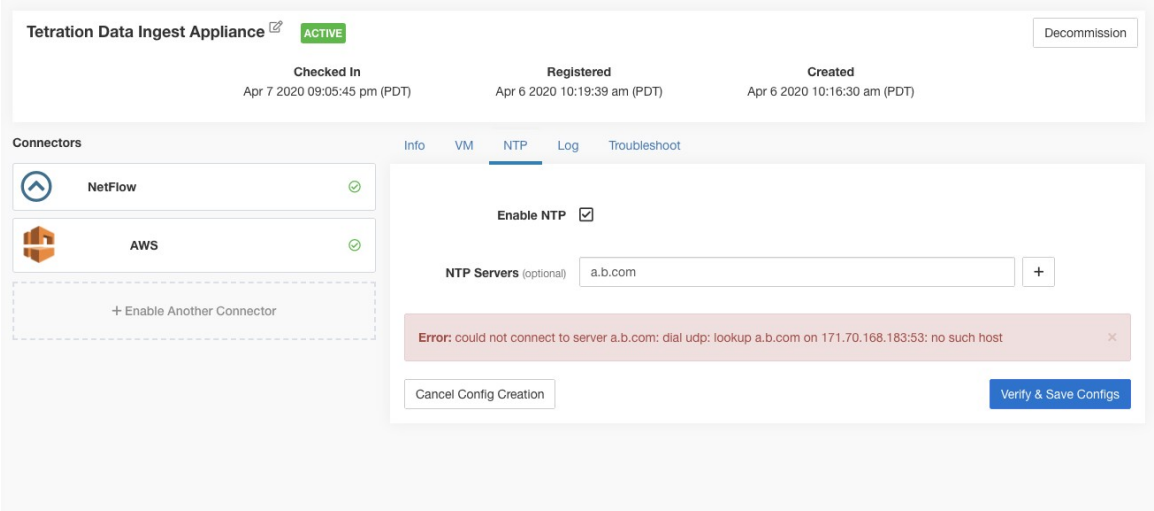


Figure 89: 具有有效 *NTP* 服务器的 *NTP* 配置

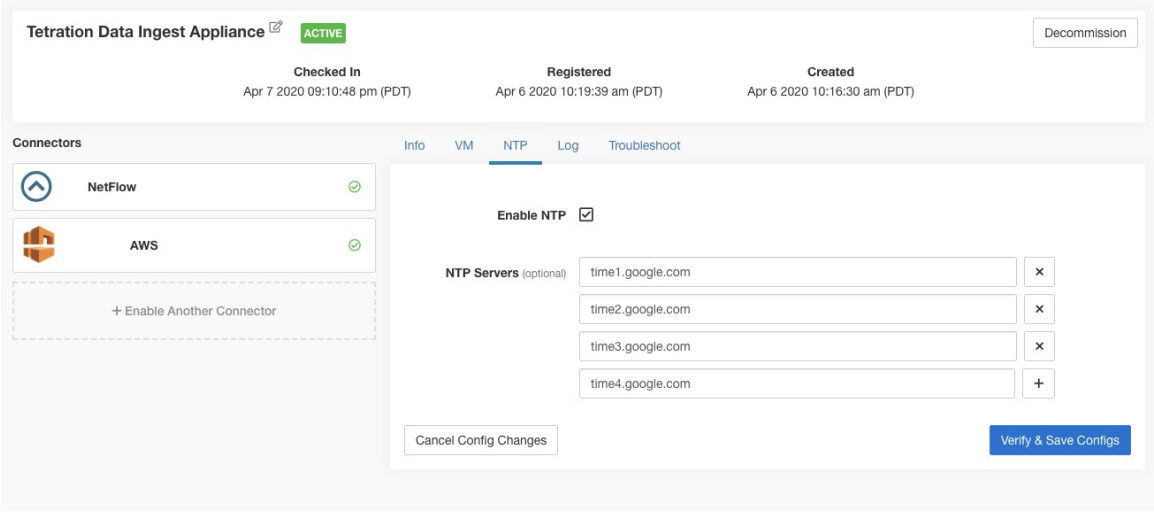
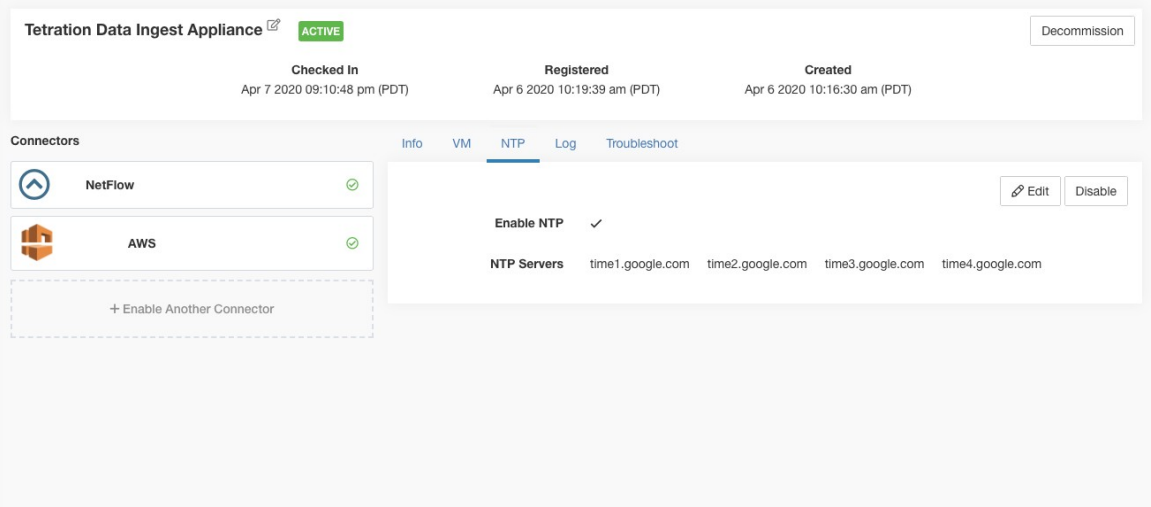


Figure 90: NTP 配置已验证并已应用



日志配置

日志配置可更新设备和/或连接器上的日志级别、日志文件最大大小和日志轮换参数。如果在设备上触发了配置更新，则会更新设备控制器日志设置。另一方面，如果在连接器上触发配置更新，则服务控制器和服务日志设置也会更新。

参数名称	类型	说明
日志记录级别 (Logging level)	下拉菜单	要设置的日志记录级别
	• 调试 *(debug)*	调试日志级别
	• 信息 *(info)*	信息日志级别
	• 警告 *(warn)*	警告日志级别
	• 错误 *(error)*	错误日志级别
最大日志文件大小 (MB) (Max log file size [in MB])	数字	开始日志轮换之前日志文件的最大大小
日志轮换（天）(Log rotation [in days])	数字	开始日志轮换之前日志文件的最长期限
日志轮换（以实例为单位）(Log rotation [in instances])	数字	保留的最大日志文件实例数

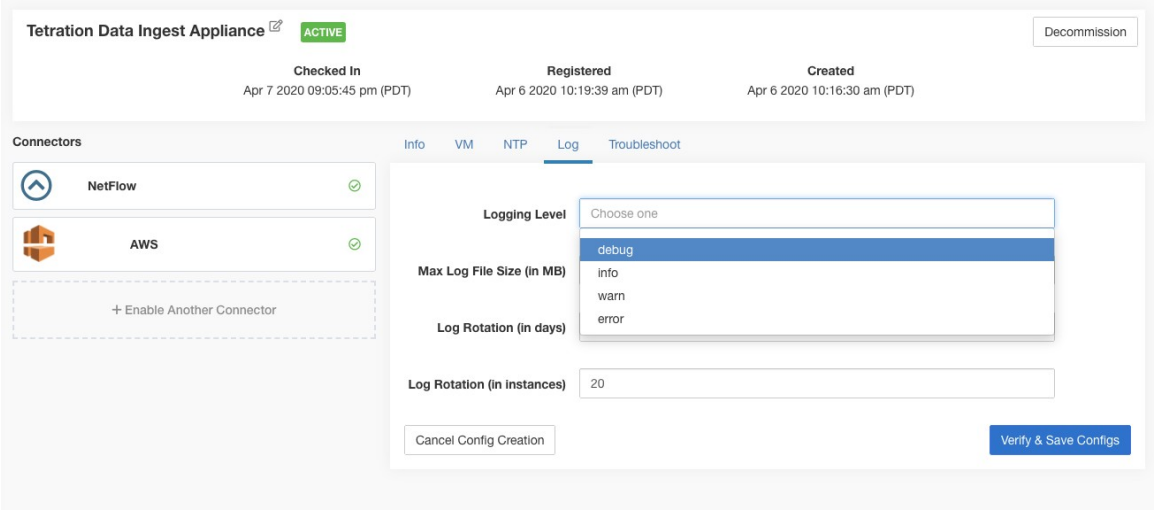
测试：无操作

应用：如果在设备上触发配置，请更新设备上 *tet-controller* 的配置文件。如果在连接器上触发了配置，请更新由负责连接器的 Docker 容器上的控制器管理的 *tet-controller* 和服务的配置文件。

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、ISE、ASA 和 Meraki。

Figure 91: 设备上的日志配置



Note 由于所有警报通知程序连接器（Syslog、Email、Slack、PagerDuty 和 Kinesis）在 Cisco Secure Workload 边缘上的单个 Docker 服务（Cisco Secure Workload 警报通知程序）上运行，因此无法在不影响配置的情况下更新连接器的日志配置。可以使用允许的命令更新 Cisco Secure Workload 边缘设备上的 Cisco Secure Workload 警报通知程序 (TAN) Docker 服务的日志配置。

有关详细信息，请参阅更新警报通知程序连接器日志配置。

终端配置

终端配置指定 AnyConnect 和 ISE 连接器上终端的非活动超时。当终端超时时，连接器会停止签入 Cisco Secure Workload，并清除连接器上终端的本地状态。

参数名称	类型	说明
终端的 InactivityTimeout（以分钟为单位）	数字	AnyConnect / ISE 连接器发布的终端的非活动超时。如果超时，终端将不再签入 Cisco Secure Workload。默认值为 30 分钟。

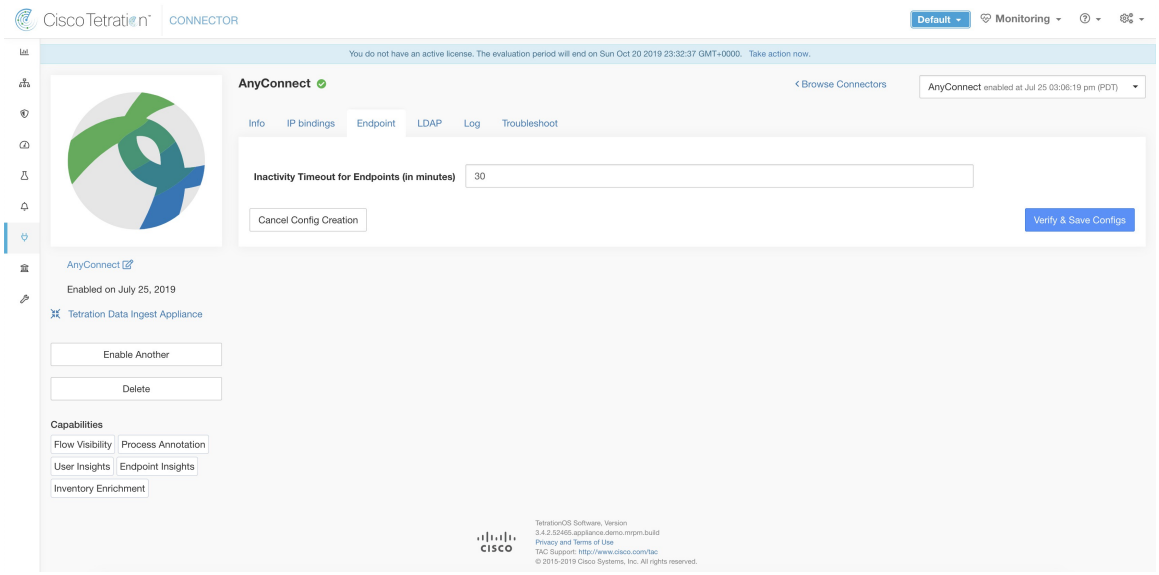
测试：无操作

应用：使用新值更新连接器的配置文件

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器： AnyConnect 和 ISE

***Figure 92: AnyConnect* 连接器上的终端非活动超时配置**



Slack 通知程序配置

用于在 Slack 上发布 Cisco Secure Workload 警报的默认配置。

参数名称	类型	说明
Slack Webhook URL	字符串	应在其上发布 Cisco Secure Workload 警报的 Slack Webhook

测试： 使用 Webhook 将测试警报发送到 Slack。如果警报发布成功，则测试通过。

应用： 使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备： 无

允许的连接器： Slack

PagerDuty 通知程序配置

用于在 PagerDuty 上发布 Cisco Secure Workload 警报的默认配置。

参数名称	类型	说明
PagerDuty 服务密钥	字符串	用于在 PagerDuty 上推送 Cisco Secure Workload 警报的 PagerDuty 服务密钥

测试： 使用服务密钥向 PagerDuty 发送测试警报。如果警报发布成功，则测试通过。

应用： 使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：PagerDuty

Kinesis 通知程序配置

用于在 Amazon Kinesis 上发布 Cisco Secure Workload 警报的默认配置。

参数名称	类型	说明
AWS 访问密钥 ID	字符串	用于与 AWS 通信的 AWS 访问密钥 ID
AWS 秘密访问密钥	字符串	用于与 AWS 通信的 AWS 访问密钥
AWS 区域	AWS 区域下拉列表	配置了 Kinesis 流的 AWS 区域的名称
Kinesis 流	字符串	Kinesis 流的名称
流分区	字符串	流的分区名称

测试：使用给定配置将测试警报发送到 Kinesis 流。如果警报发布成功，则测试通过。

应用：使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：Kinesis

邮件通知程序配置

在邮件上发布 Cisco Secure Workload 警报的默认配置。

参数名称	类型	说明
SMTP Username	字符串	SMTP 服务器用户名。此参数可选。
SMTP Password	字符串	用户的 SMTP 服务器密码（如果已指定）。此参数可选。
SMTP Server	字符串	SMTP 服务器的 IP 地址或主机名
SMTP Port	数字	SMTP 服务器的侦听端口。默认值为 587。
Secure Connection	复选框	是否应将 SSL 用于 SMTP 服务器连接？
From Email Address	字符串	用于发送警报的邮件地址

参数名称	类型	说明
Default Recipients	字符串	以逗号分隔的收件人邮件地址列表

测试：使用给定配置发送测试邮件。如果警报发布成功，则测试通过。

应用：使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：邮件

系统日志通知程序配置

用于在系统日志上发布 Cisco Secure Workload 警报的默认配置。

参数名称	类型	说明
协议	下拉菜单	用于连接到服务器的协议
	•*UDP*	
	• *TCP*	
服务器地址	字符串	系统日志服务器的 IP 地址或主机名
端口	数字	系统日志服务器的侦听端口。默认端口值为 514。

测试：使用给定配置将测试警报发送到系统日志服务器。如果警报发布成功，则测试通过。

应用：使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：系统日志

系统日志严重性映射配置

下表显示系统日志中 Cisco Secure Workload 警报的默认严重性映射

Cisco Secure Workload 警报严重性	系统日志严重性
LOW	LOG_DEBUG
MEDIUM	LOG_WARNING
HIGH	LOG_ERR
CRITICAL	LOG_CRIT
IMMEDIATE ACTION	LOG_EMERG

您可以使用此配置来修改此设置。

参数名称	映射下拉列表
IMMEDIATE_ACTION	• 紧急 • 警报 • 严重 • 错误 • 警告 • 通知 • 参考 • 调试
CRITICAL	
HIGH	
MEDIUM	
LOW	

测试：无操作

应用：使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：系统日志

ISE 实例配置

此配置提供连接到 Cisco Identity Services Engine (ISE) 所需的参数。通过提供该配置的多个实例，ISE 连接器可从多个 ISE 设备连接并提取有关终端的元数据。最多可以提供 20 个 ISE 配置实例。

参数名称	类型	说明
ISE 客户端证书	字符串	用于使用 pxGrid 连接 ISE 的 ISE 客户端证书
ISE 客户端密钥	字符串	用于连接到 ISE 的 ISE 客户端密钥
ISE 服务器 CA 证书	字符串	ISE 的 CA 证书
ISE 主机名	字符串	ISE pxGrid 的 FQDN
ISE 节点名称	字符串	ISE pxGrid 的节点名称

测试：使用给定参数连接到 ISE。连接成功后，接受配置。

应用：使用指定参数更新连接器的配置文件。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：ISE

发现

支持发现模式的配置会执行以下操作。

1. 从用户收集基本配置。
2. 验证基本配置。
3. 发现配置的其他属性，并将其呈现给用户。
4. 让用户使用发现的属性来增强配置。
5. 验证并应用增强的配置。

在 3.3.1.x 版本中，LDAP 配置支持发现模式。

LDAP 配置

LDAP 配置指定如何连接到 LDAP，要使用的基本可分辨名称 (DN) 是什么，与用户名对应的属性是什么，以及要为每位用户名获取哪些属性。LDAP 属性是 LDAP 在特定环境下的属性。

只要配置好连接 LDAP 的方式和基本 DN，就可以在 LDAP 中发现用户的属性。然后，这些被发现的属性就可以在UI中向用户显示。从这些发现的属性中，用户选择与用户名和最多六个属性的列表对应的属性，以便为每位用户名从 LDAP 收集。因此，这消除了 LDAP 属性的手动配置，减少了错误。

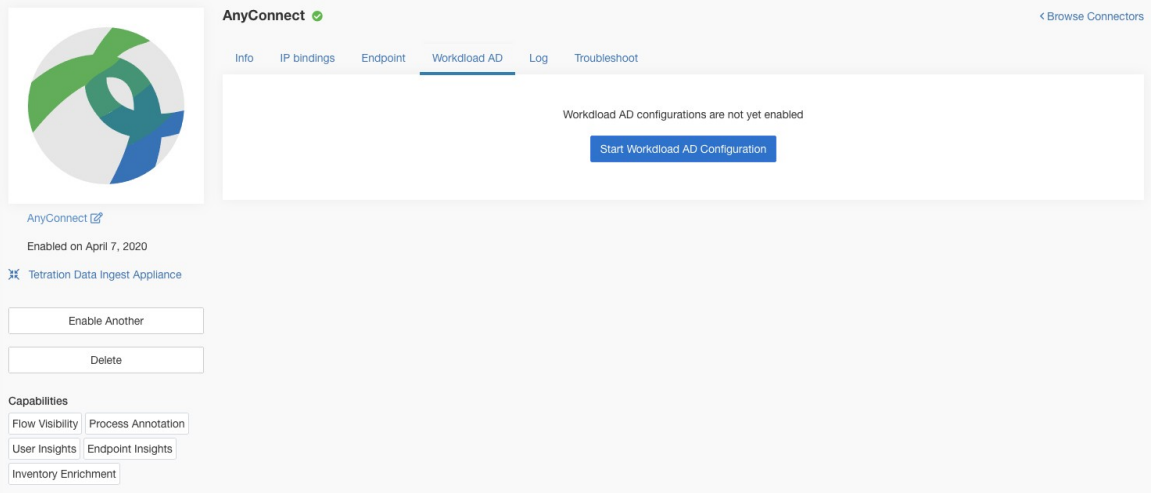
以下是通过发现来创建 LDAP 配置的详细步骤。

Procedure

步骤 1 启动 LDAP 配置

为连接器启动 LDAP 配置。

Figure 93: 启动 ***LDAP*** 配置发现



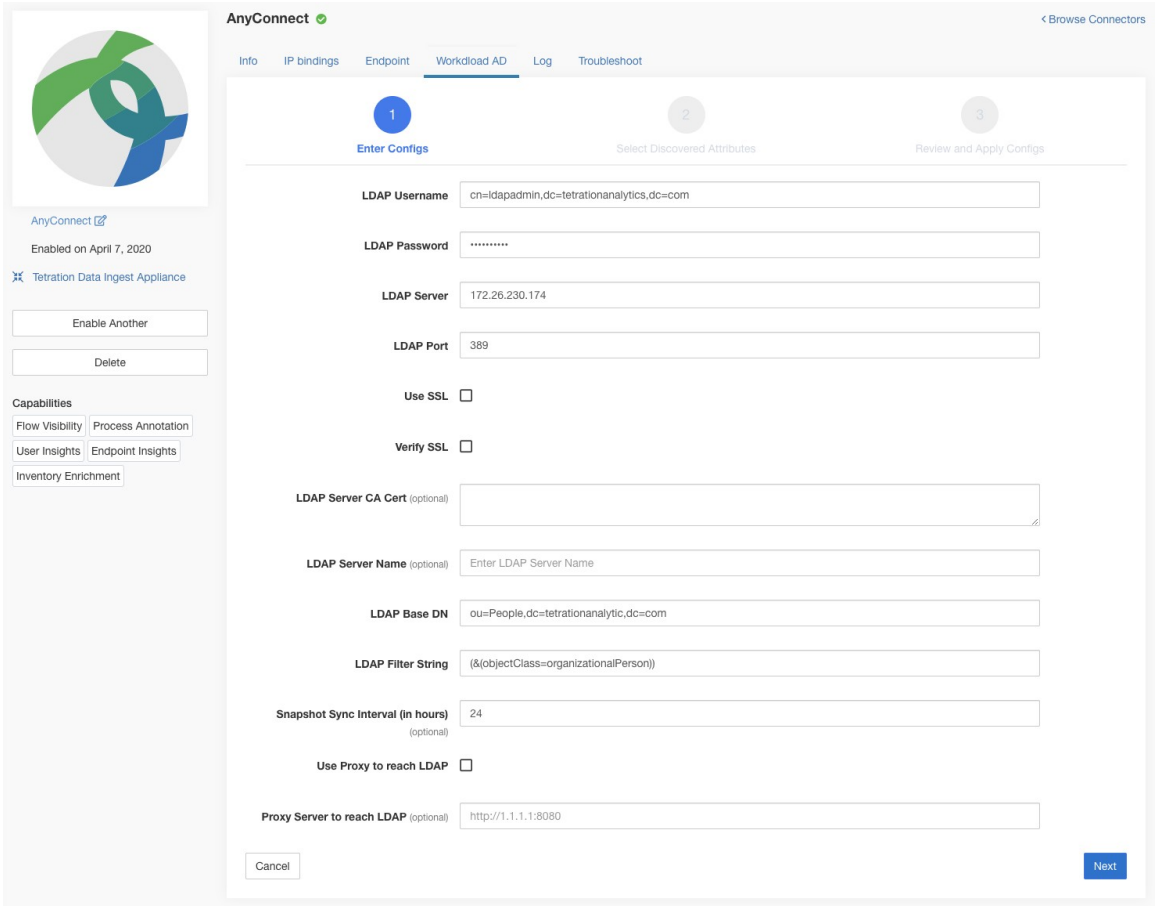
步骤 2 提供基本 LDAP 配置

指定用于连接到 LDAP 的基本配置。在此配置中，用户提供用于连接 LDAP 服务器的 LDAP 绑定 DN 或用户名、用于连接 LDAP 服务器的 LDAP 密码、LDAP 服务器地址、LDAP 服务器端口、用于连接的基本 DN，以及用于获取与此过滤器匹配的用户的过滤器字符串。

参数名称	类型	说明
LDAP 用户名 (LDAP Username)	字符串	用于访问 LDAP 服务器的 LDAP 用户名或绑定 DN*
LDAP 密码 (LDAP Password)	字符串	用于访问 LDAP 服务器的用户名的 LDAP 密码*
LDAP 服务器 (LDAP Server)	字符串	LDAP 服务器地址
LDAP 端口 (LDAP Port)	数字	LDAP 服务器端口
使用 SSL (Use SSL)	复选框	连接器是否应安全连接到 LDAP？（可选）默认值为 false。
验证 SSL (Verify SSL)	复选框	连接器是否应验证 LDAP 证书？（可选）默认值为 false。
LDAP 服务器 CA 证书 (LDAP Server CA Cert)	字符串	服务器 CA 证书。（可选）
LDAP 服务器名称 (LDAP Server Name)	字符串	为其颁发 LDAP 证书的服务器名称（如果选中验证 *SSL (Verify SSL)*，则为必填项。
LDAP 基本 DN (LDAP Base DN)	字符串	LDAP 基本 DN，LDAP 中目录搜索的起点
LDAP 过滤器字符串 (LDAP Filter String)	字符串	LDAP 过滤器前缀字符串。过滤仅匹配此条件的搜索结果。
快照同步间隔（以小时为单位）(Snapshot Sync Interval [in hours])	数字	指定（重新）创建 LDAP 快照的时间间隔（以小时为单位）。（可选）默认值为 24 小时。
使用代理访问 LDAP (Use Proxy to reach LDAP)	复选框	连接器是否应使用代理服务器访问 LDAP 服务器？
代理服务器访问 LDAP (Proxy Server to reach LDAP)	字符串	用于访问 LDAP 的代理服务器

在连接器上配置 LDAP 所需的最低用户权限是**标准域用户**。

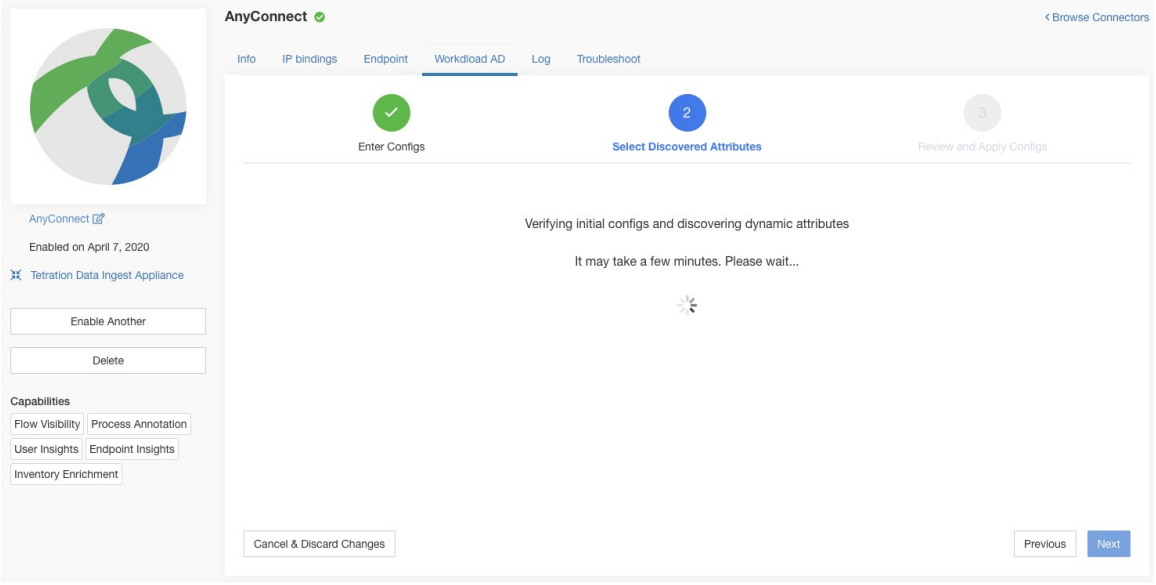
Figure 94: 初始 *LDAP* 配置



步骤 3 正在发现中

用户点击下一步 *(Next)* 后，此配置将发送到连接器。连接器会使用给定的配置与 LDAP 服务器建立连接。它可从LDAP服务器获取多达1000个用户，并识别所有属性。此外，它还能计算出所有1000个用户共有的所有单值属性列表。连接器将此结果返回给 Cisco Secure Workload。

Figure 95: 正在发现中



步骤 4 使用已发现的属性增强配置

用户必须选择与用户名对应的属性，并选择连接器必须为组织中的每位用户（即，匹配过滤器字符串的用户）获取和快照的最多六个属性。此操作使用已发现属性列表的下拉菜单来执行。因此，消除了手动错误和配置错误。

参数名称	类型	说明
LDAP 用户名属性 (LDAP Username Attribute)	字符串	包含用户名的 LDAP 属性
要获取的 LDAP 属性 (LDAP Attributes to Fetch)	字符串列表	应为用户获取的LDAP属性列表

Figure 96: 发现 *LDAP* 属性

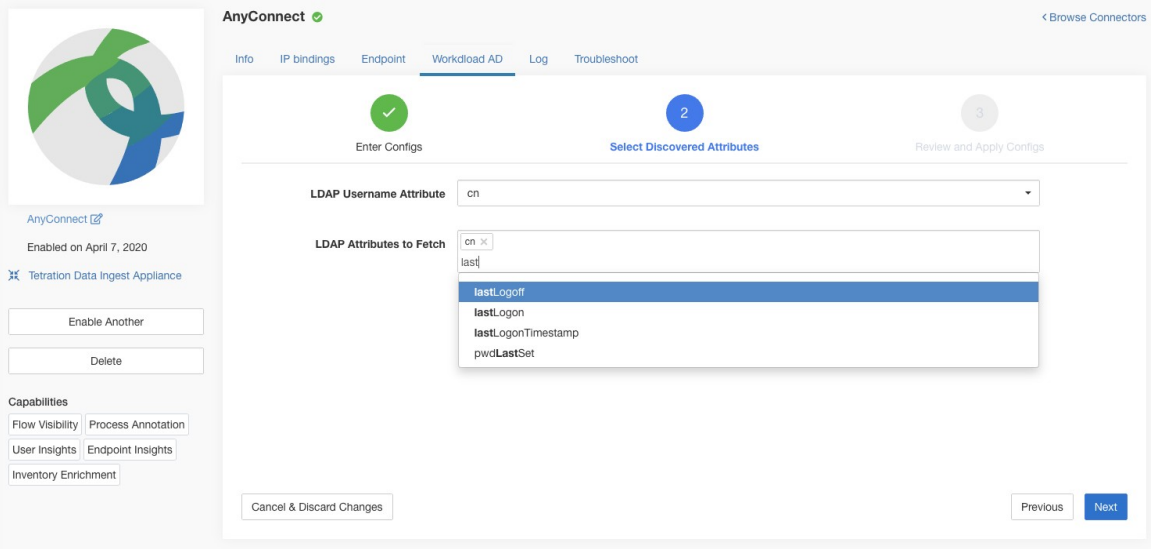
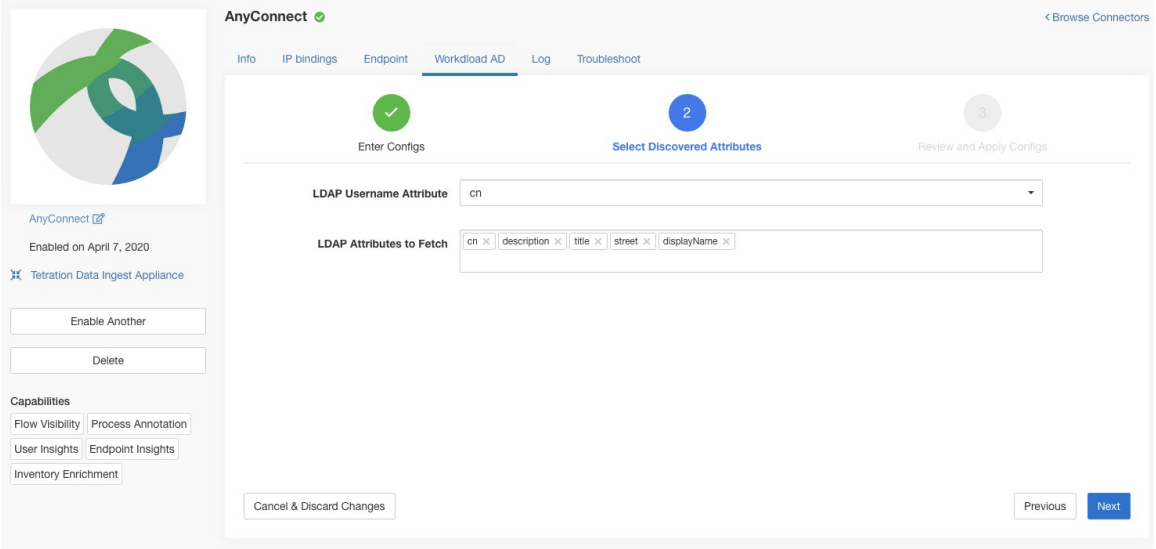


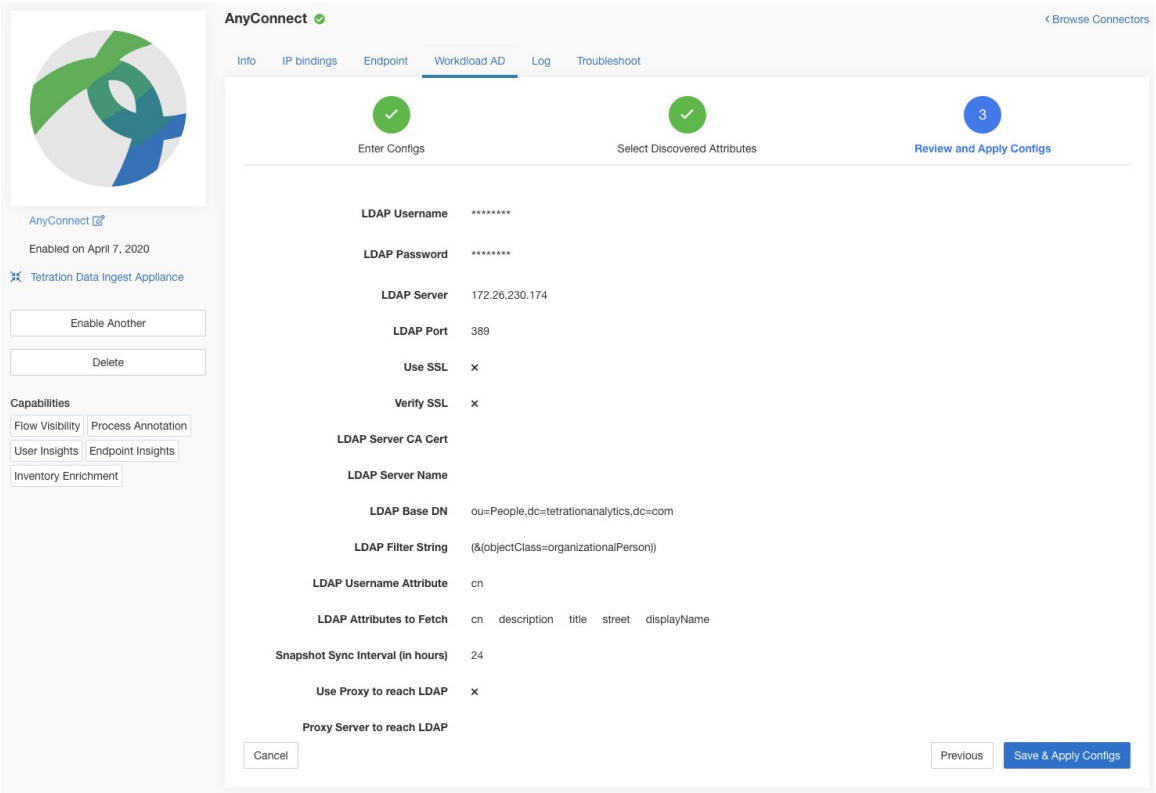
Figure 97: 确定用户名属性以及要为每位用户名收集的属性

步骤 5 完成、保存和应用配置

最后，点击保存并应用更改 *(Save and Apply Changes)* 完成配置。

Figure 98: 完成 ***LDAP*** 配置发现和提交





连接器接收完成的配置。它会创建与过滤字符串匹配的所有用户的本地快照，并只获取所选属性。快照完成后，连接器服务就可以开始使用快照在资产中注释用户及其 LDAP 属性。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：AnyConnect、ISE 和 F5。

删除

您可以使用适用于每个配置的删除 *(Delete)* 按钮，从连接器和/或设备中删除已添加的所有配置。

故障排除

连接器和虚拟设备支持各种故障排除机制来调试可能出现的问题。

Note 本部分不适用于以下情况：

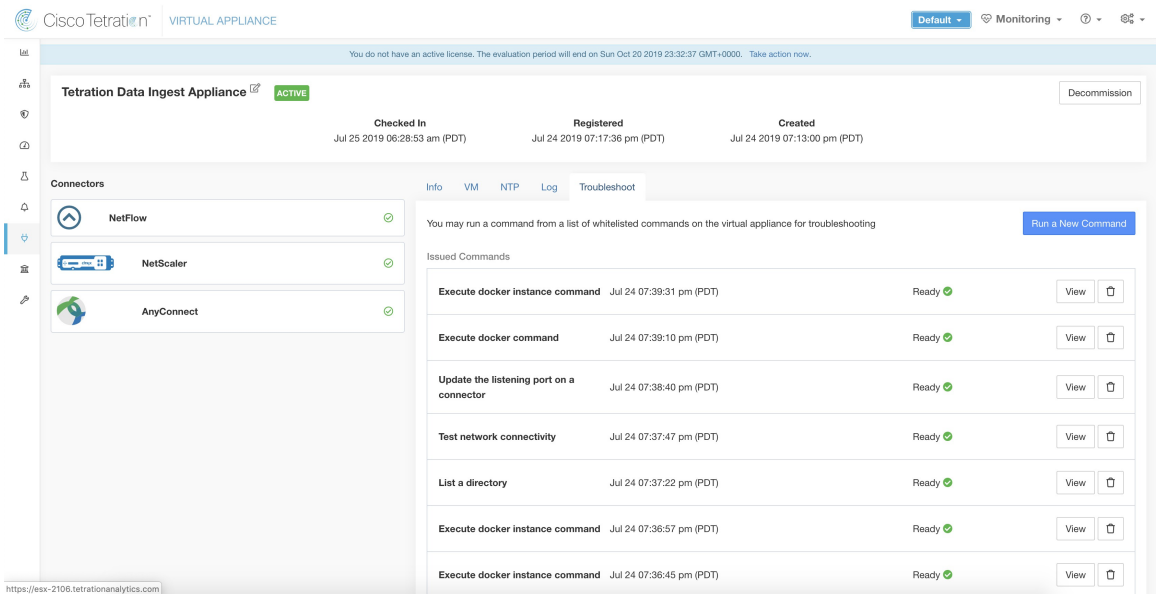
ERSPAN 虚拟设备：有关故障排除的详细信息，请参阅 ERSPAN 设备页面。

云连接器：要对云连接器进行故障排除，请参阅云连接器对应的部分，例如AWS 连接器问题故障排除。

允许的命令集

允许的命令集让您能够在设备和Docker容器（用于连接器）上运行某些调试命令。允许使用的命令包括检索日志和当前运行配置、测试网络连接以及捕获与指定端口匹配的数据包。

***Figure 99: Cisco Secure Workload* 虚拟设备上的“故障排除” *(Troubleshoot)* 页面**



Note 只有具有客户支持角色的用户才能在设备和连接器上使用允许的命令集进行故障排除。

显示日志

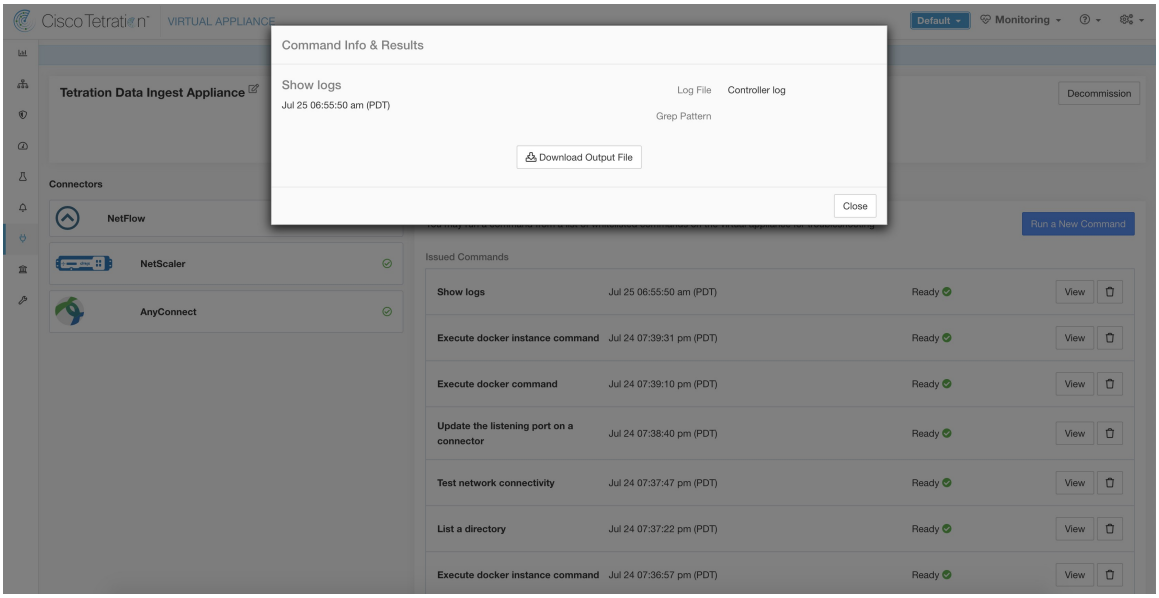
显示控制器日志文件的内容，也可以选择对文件进行 grep 查找以查找指定的模式。Cisco Secure Workload 会将命令发送到发出命令的设备/连接器。设备/连接器服务上的控制器会返回结果（最后 5000 行的结果尾部截短）。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮以下载文件。

参数名称	类型	说明
Grep 模式	字符串	要从日志文件 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 100: 从 ***Cisco Secure Workload*** 注入设备下载显示日志输出



显示服务日志

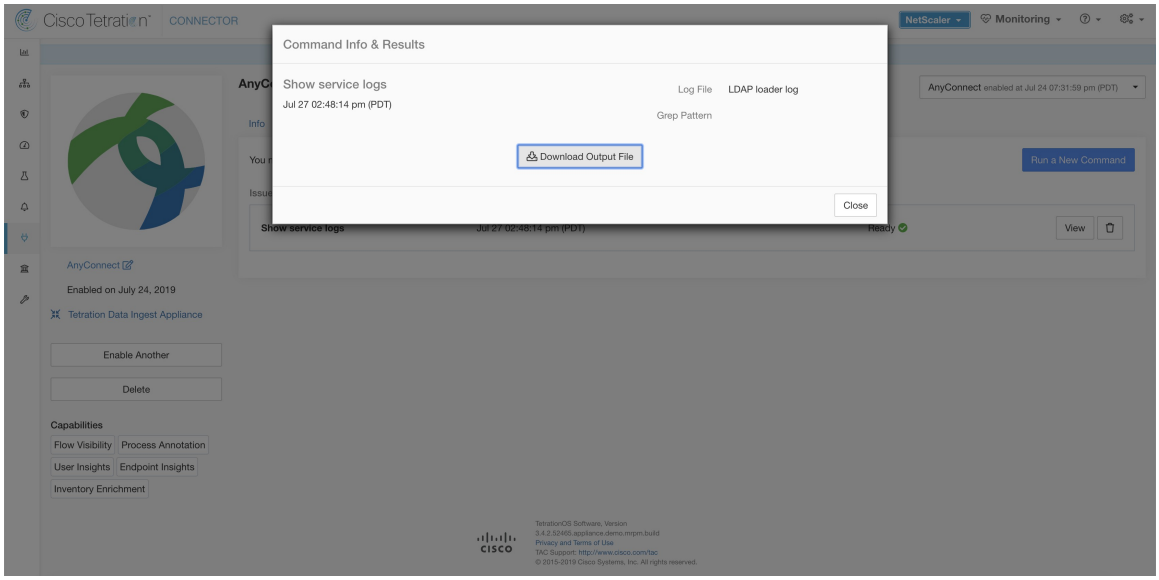
显示服务日志文件的内容，并选择性地对指定模式的文件进行 grep。Cisco Secure Workload 会将命令发送到发出命令的设备/连接器。设备/连接器服务上的控制器会返回结果（最后 5000 行的结果尾部截短）。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮以下载文件。

参数名称	类型	说明
日志文件	下拉菜单	要收集的日志文件的名称
	• 服务日志	连接器服务的日志
	• 升级日志	服务的升级日志
	• *LDAP* 加载程序日志	已启用 LDAP 的连接器的 LDAP 快照日志
Grep 模式	字符串	要从日志文件 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备： 无（仅在有效的连接器服务上可用）

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 101: 从用于 ***LDAP*** 加载程序的 ***AnyConnect*** 连接器日志文件下载显示服务日志输出



显示运行配置

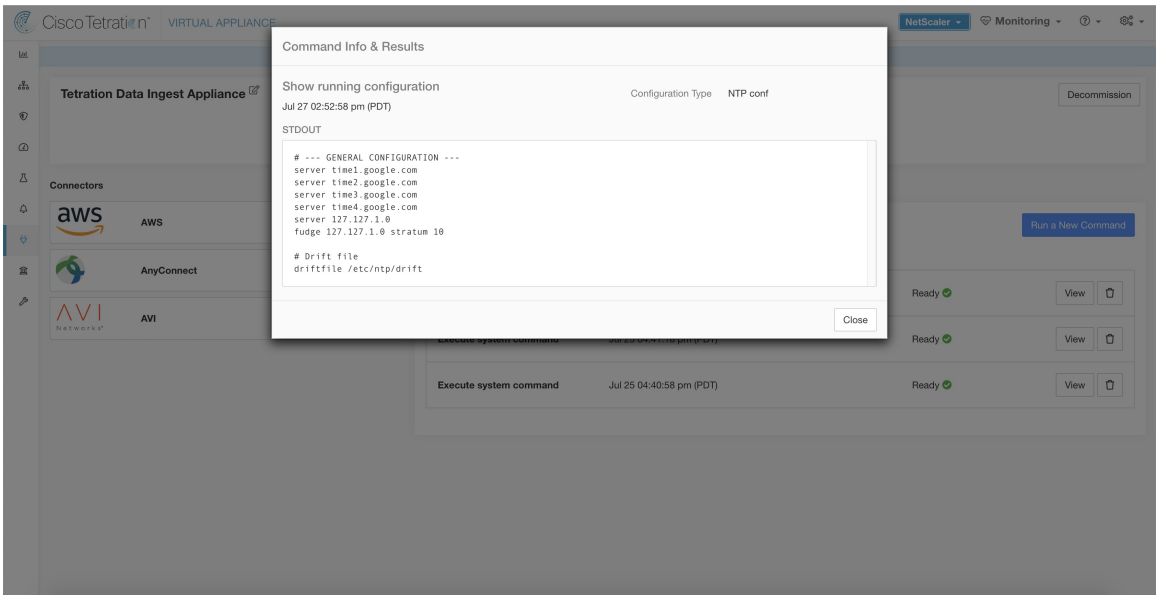
显示设备/连接器控制器的运行配置。设备/连接器上的控制器会检索与请求参数相对应的配置，并返回结果。当结果在 Cisco Secure Workload 中可用时，配置的内容会显示在文本框中。

参数名称	类型	说明
配置类型	下拉菜单	要收集的配置文件
	• *Controller conf*	设备控制器的配置文件
	• *Supervisor conf*	运行控制器的管理引擎的配置文件
	• *NTP conf*	NTP 配置文件
	• *Chrony conf*	/etc/chrony.conf

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 102: 在 ***Cisco Secure Workload*** 注入设备上显示 ***NTP conf*** 的运行配置



显示服务运行配置

显示为设备上的连接器实例化的服务的运行配置。服务上的控制器会检索与请求参数相对应的配置并返回结果。当结果在 Cisco Secure Workload 中可用时，配置的内容会显示在文本框中。

参数名称	类型	说明
Configuration Type	下拉菜单	要收集的配置文件。
	• *Controller conf*	服务控制器的配置文件。
	• *Supervisor conf*	运行控制器的管理引擎的配置文件。
	• *Service conf*	服务配置文件。
	• *LDAP conf*	已启用 LDAP 的连接器的 LDAP 配置。

允许的 Cisco Secure Workload 虚拟设备： 无（仅在有效的连接器服务上可用）

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

显示系统命令

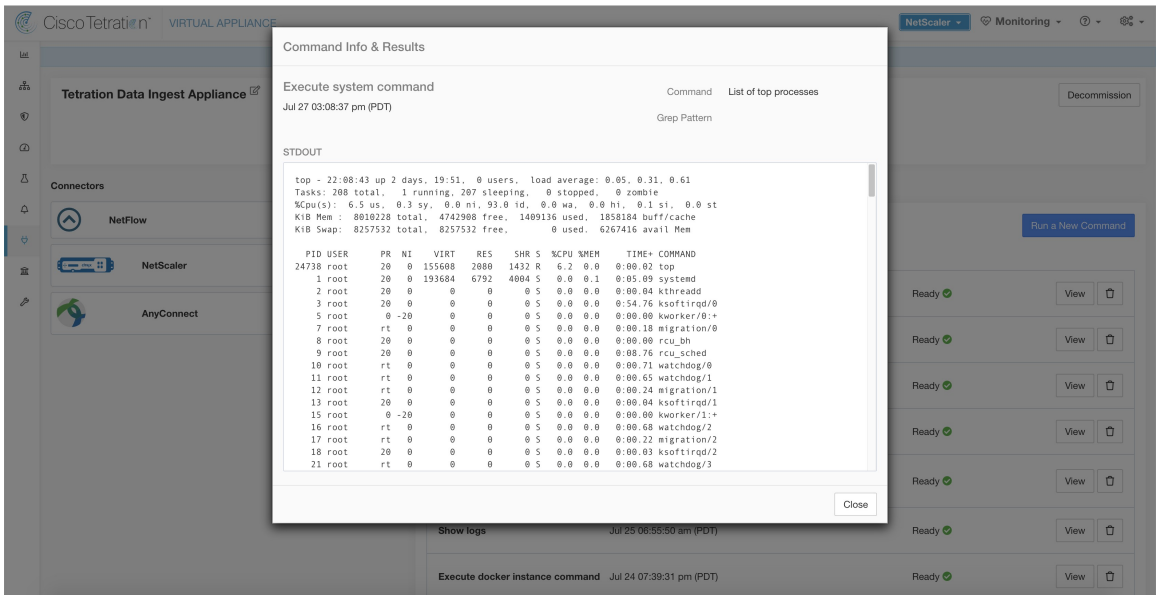
对指定的模式执行系统命令和 grep（可选）。设备/连接器服务上的控制器会返回结果（最后 5000 行的结果尾部截短）。也可选择提供一个 grep 模式作为参数，并对输出进行相应过滤。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
系统命令	下拉菜单	要执行的系统命令
	• *IP* 配置	**ifconfig**
	• *IP* 路由配置	**ip route**
	• *IP* 数据包过滤规则	**iptables -L**
	• 网络状态	**netstat**
	• 网络状态 *(EL9)*	**ss**
	• 进程状态	**ps -aux**
	• 排名靠前的进程列表	**top -b -n 1**
	• *NTP* 状态	**ntpstat**
	• *NTP* 查询	**ntpq -pn**
	• 时间状态 (EL9)	**chronyc tracking**
	• Chrony 查询 (EL9)	**chronyc sources**
	• *CPU* 信息	**lscpu**
	• 内存信息	**lsmem**
	• 可用磁盘	**df -H**
Grep 模式	字符串	要从输出中 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 103: 在 *Cisco Secure Workload* 注入设备上使用 *show system* 命令检索排名靠前的进程列表



显示 Docker 命令

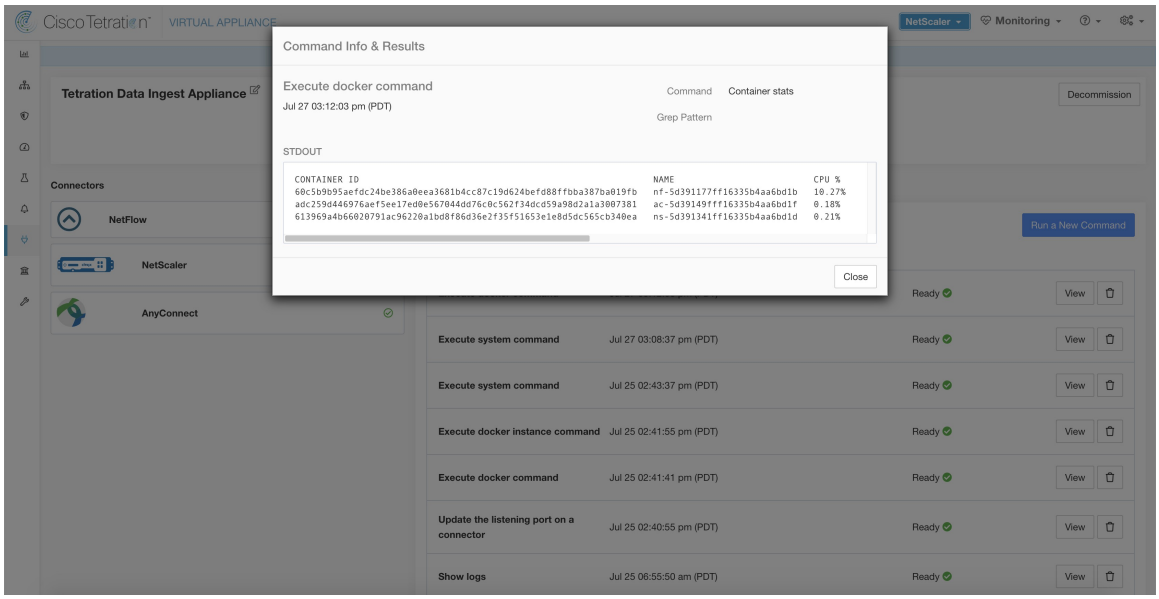
对指定的模式执行 Docker 命令和 grep（可选）。命令由设备控制器在设备上执行。最后 5000 行的结果尾部截短。也可选择提供一个 grep 模式作为参数，并对输出进行相应过滤。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
Docker 命令	下拉菜单	要执行的 Docker 命令
	• *Docker* 信息	**docker info**
	• 列出映像	**docker images --no-trunc**
	• 列出容器	**docker ps --no-trunc**
	• 列出网络	**docker network ls --no-trunc**
	• 列出卷	**docker volume ls**
	• 容器统计信息	**docker stats --no-trunc--no-stream**
	• *Docker* 磁盘使用率	`docker system df -v`
	• *Docker* 系统事件	**docker system events --since '10m'**
	• 版本	**docker version**
Grep 模式	字符串	要从输出中 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：无

Figure 104: 在 *Cisco Secure Workload* 注入设备上执行 *Docker* 命令以显示容器统计信息



显示 Docker 实例命令

在 Docker 资源的特定实例上执行 docker 命令。可以使用 显示 Docker 命令 来获取实例 ID。命令由设备控制器在设备上执行。最后 5000 行的结果尾部截短。也可选择提供一个 grep 模式作为参数，并对输出进行相应过滤。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

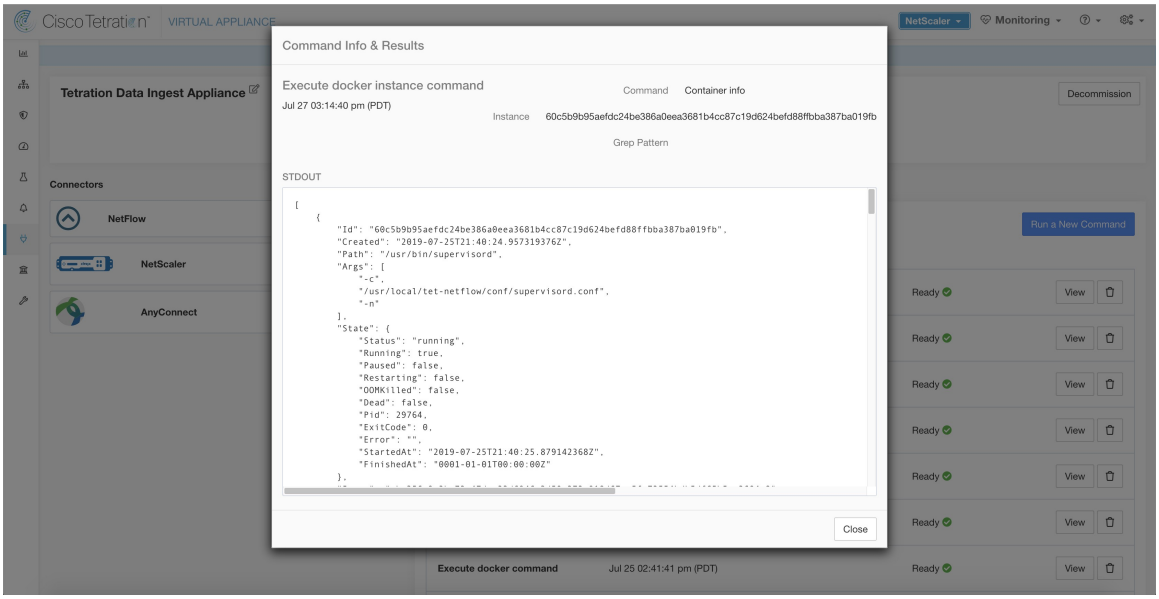
参数名称	类型	说明
Docker 命令	下拉菜单	要执行的 Docker 命令
	• 映像信息	**docker images --no-trunc <instance>**
	• 网络信息	**docker network inspect <instance>**
	• 卷信息	**docker volume inspect <instance>**
	• 容器信息	**docker container inspect--size <instance>**
	• 容器日志	**docker logs --tail 5000 <instance>**
	• 容器端口映射	**docker port <instance>**
	• 容器资源使用情况统计信息	**docker stats --no-trunc--no-stream <instance>**
	• 正在运行进程的容器	**docker top <instance>**

参数名称	类型	说明
实例	字符串	Docker 资源（映像、网络、卷、容器）ID（请参阅显示 Docker 命令）
Grep 模式	字符串	要从输出中 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：无

Figure 105: *在 **Cisco Secure Workload** 注入设备上执行 **Docker** 实例命令以检索容器信息*



显示管理引擎命令

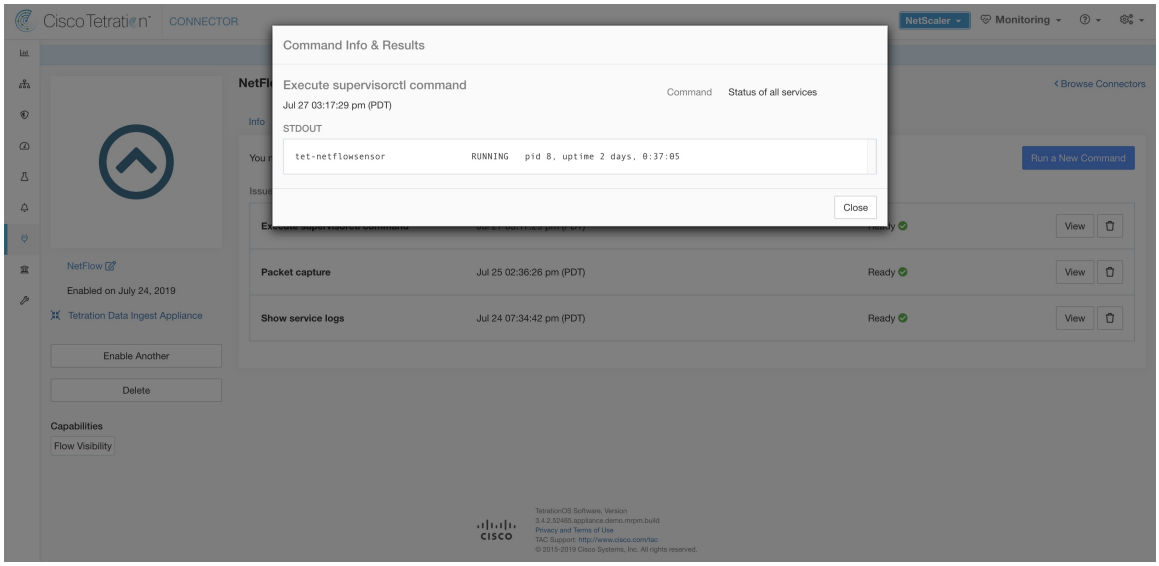
执行 supervisorctl 命令并返回结果。Cisco Secure Workload 将命令发送到发出命令的设备/连接器。设备/连接器服务上的控制器返回结果 当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
SupervisorCtl 命令	下拉菜单	要执行的*supervisorctl* 命令
	• 所有状态的服务	**supervisorctl 状态**
	• 管理引擎的 *PID*	**supervisorctl pid**
	• 所有服务的 *PID*	**supervisorctl pid all**

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 106: 在 ***NetFlow*** 连接器上执行 ***supervisorctl*** 命令，以获取所有服务的状态

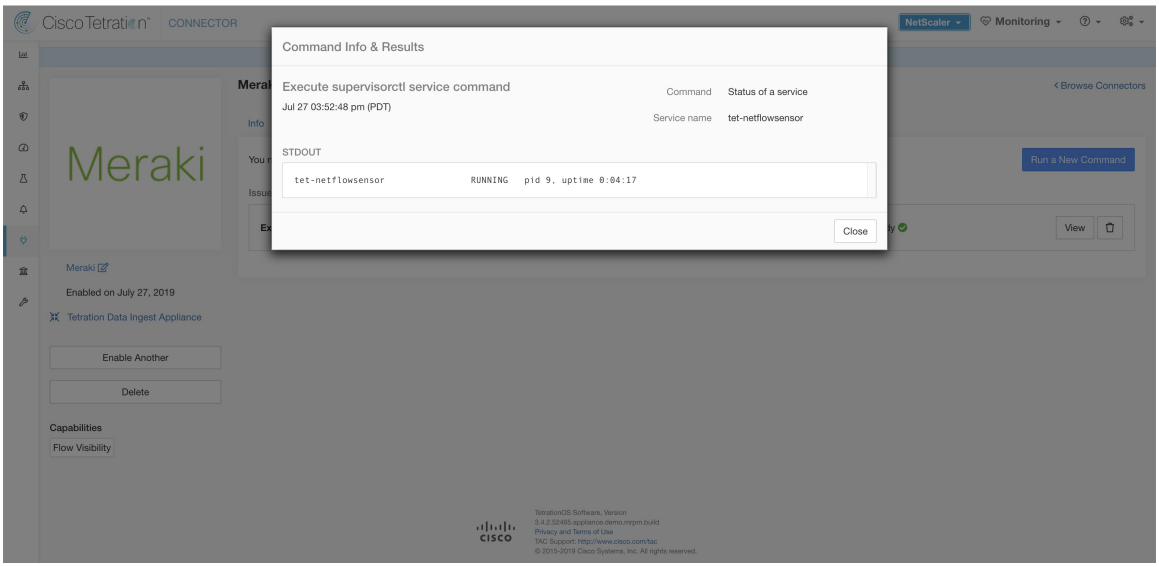


显示管理引擎服务命令

对特定服务执行 supervisorctl 命令。可以使用 显示管理引擎命令 来获取服务名称。Cisco Secure Workload 会将命令发送到发出命令的设备/连接器。设备/连接器服务上的控制器会返回结果。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称**Secure Workload Ingest**	类型	说明
SupervisorCtl 命令	下拉菜单	要执行的 *supervisorctl* 命令
	• 服务状态	**supervisorctl status <服务名称>**
	• 服务的 *PID*	**supervisorctl pid <服务名称>**
服务名称	字符串	管理引擎控制服务的名称（请参阅显示管理引擎命令）

Figure 107: 在 ***NetFlow*** 连接器上执行 ***supervisorctl*** 命令，以获取指定服务名称的状态



允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

网络连接命令

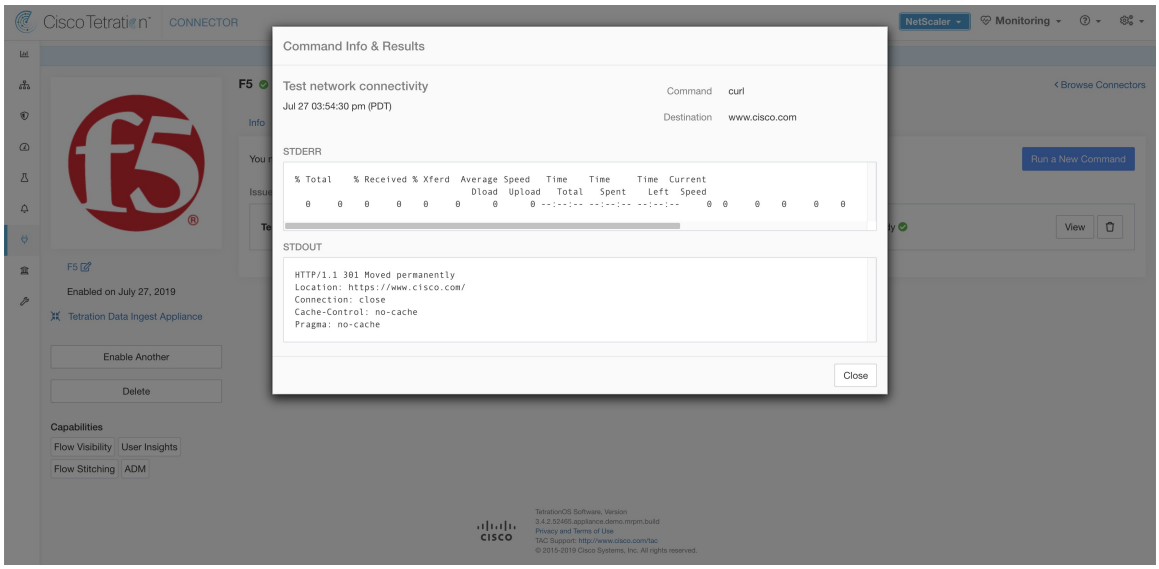
从设备/连接器测试网络连接。命令由设备控制器在设备上执行。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
网络命令 (Network Command)	下拉菜单	要执行的网络连接命令
	• *ping*	**ping -c 5 <destination>**
	• *curl*	**curl -I <destination>**
目标 (Destination)	字符串	用于测试的目标

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 108: 通过运行 ***curl*** 在 ***F5*** 连接器上测试网络连接



列出文件

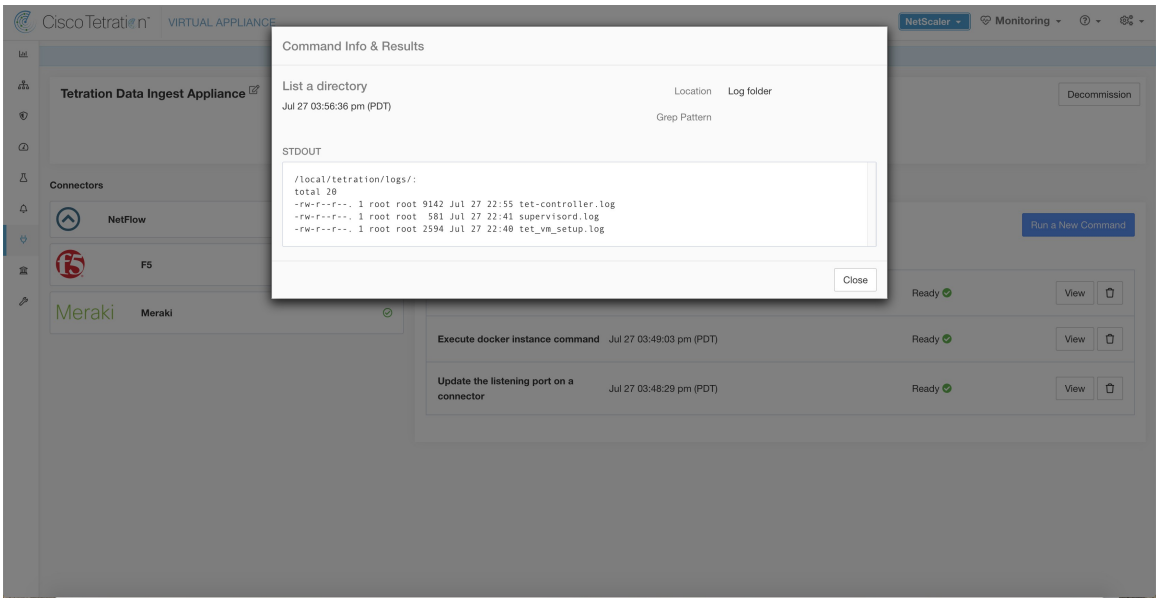
列出设备已知位置中的文件。（可选）grep 指定的模式。Cisco Secure Workload 会将命令发送到发出命令的设备。设备上的控制器会返回结果。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
位置	下拉菜单	列出目标位置中的文件
	• 控制器配置文件夹	列出保存控制器配置文件的文件夹中的内容。
	• 控制器证书文件夹	列出保存控制器证书的文件夹中的内容。
	• 日志文件夹	列出存在日志文件的文件夹中的内容。
Grep 模式	字符串	要从输出中 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：无

Figure 109: 列出 *Cisco Secure Workload* 注入设备中的日志文件夹中的文件



列出服务文件

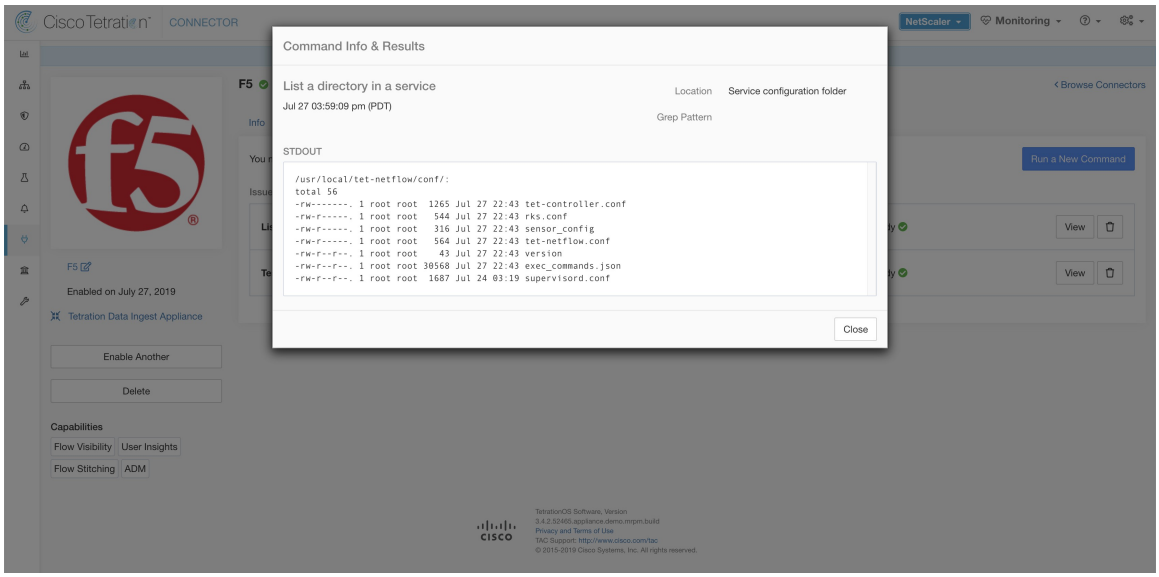
列出连接器服务的已知位置中的文件。（可选）对指定的模式进行 grep。Cisco Secure Workload 会向发出命令的连接器发送命令。连接器服务上的控制器会返回结果。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
位置	下拉菜单	列出目标位置中的文件。
	• 服务配置文件夹	列出保存服务配置文件的文件夹中的内容。
	• 服务证书文件夹	列出保留服务证书的文件夹中的内容。
	• 日志文件夹	列出存在日志文件的文件夹中的内容。
	• 数据库文件夹	列出保存终端（尤其是 AnyConnect 和 ISE 连接器）状态的文件夹中的内容。
Grep 模式	字符串	要从输出中 grep 的模式字符串

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 110: 列出 ***Cisco Secure Workload*** 注入设备中 ***F5*** 连接器的配置文件夹中的文件



数据包捕获

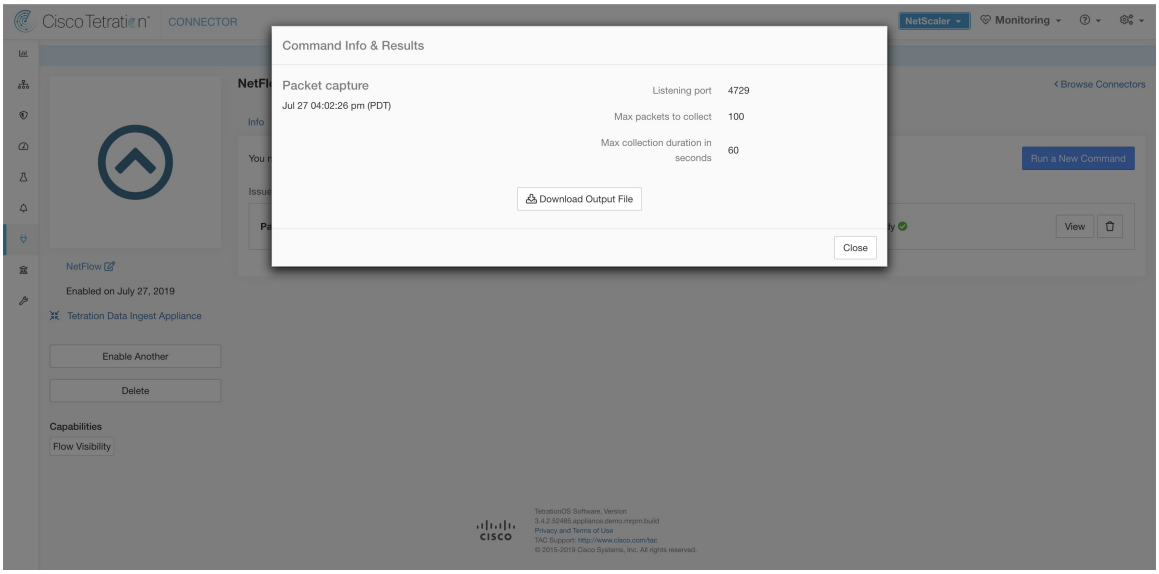
捕获设备/连接器上的传入数据包。Cisco Secure Workload 会将命令发送到发出命令的设备/连接器。设备/连接器服务上的控制器会捕获数据包，对其进行编码，并将结果返回给 Cisco Secure Workload。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮，用于下载 `.pcap` 格式的文件。

参数名称	类型	说明
侦听端口	数字	捕获在此端口上发送/接收的数据包
要收集的最大数据包数	数字	在返回结果前要收集的最大数据包数。应小于 1000
以秒为单位的最大收集持续时间	数字	返回结果之前收集的最大持续时间。应小于 600 秒。

允许的 Cisco Secure Workload 虚拟设备：全部

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA 和 Meraki。

Figure 111: 捕获 ***NetFlow*** 连接器上给定端口上的数据包



更新连接器的侦听端口

更新 Cisco Secure Workload 注入设备中连接器上的侦听端口。Cisco Secure Workload 将命令发送到发出命令的设备上的设备控制器。控制器执行以下操作：

- 停止与连接器对应的 Docker 服务。
- 收集服务的当前运行配置。
- 删除 Docker 服务。
- 更新服务的运行配置以使用新端口。
- 从被删除容器中使用的相同Docker映像启动一个新容器，并使用新的暴露端口。此外，如果之前有一个 Docker 卷被挂载到移除的容器上，那么新容器也会挂载相同的卷。
- 将连接器的新 IP 绑定返回到 Cisco Secure Workload。
- Cisco Secure Workload 将在文本框中显示结果。

参数名称	类型	说明
Connector ID	字符串	需要更新其侦听端口的连接器的连接器 ID
Listening port label	下拉菜单	更新的端口的类型。
	NET-FLOW9	NetFlow v9 侦听端口
	IPFIX	IPFIX 侦听端口
侦听端口	字符串	连接器的新端口

允许的 Cisco Secure Workload 虚拟设备： Cisco Secure Workload 注入

允许的连接器 无

Figure 112: 将 ***Cisco Secure Workload*** 注入设备中的 ***Meraki*** 连接器上的侦听端口更新为 ***2055***

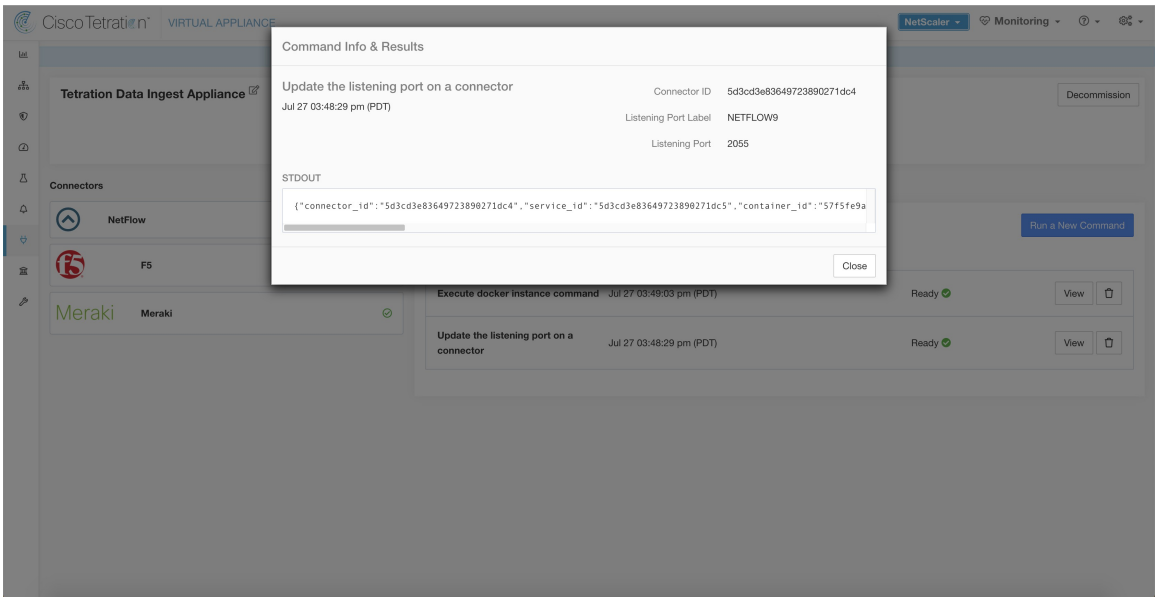
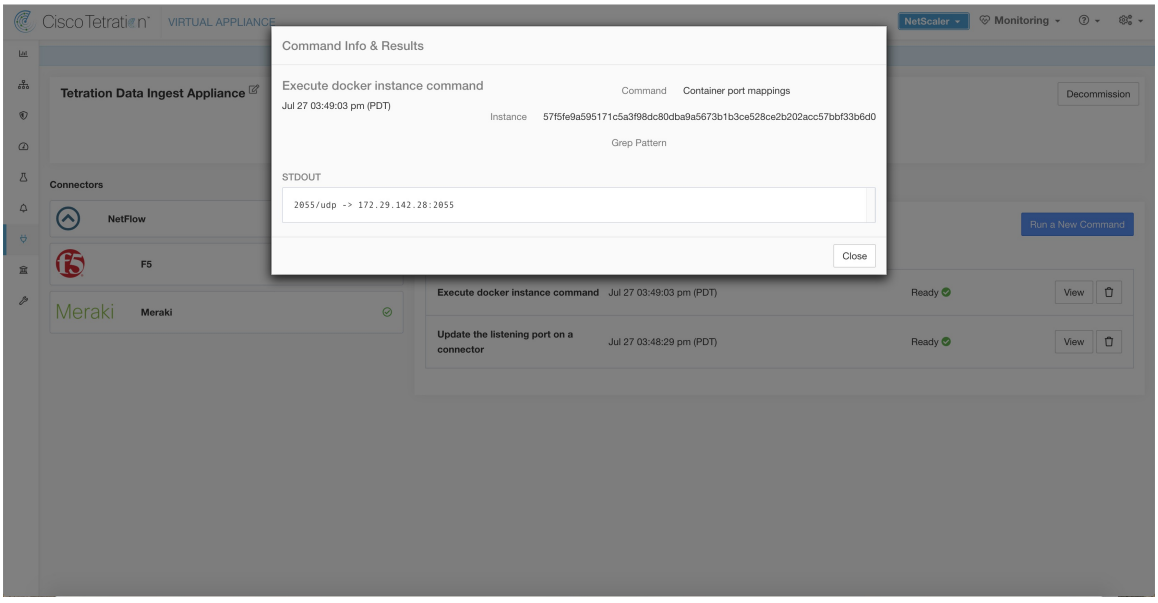


Figure 113: 检索 ***Cisco Secure Workload*** 注入设备中 ***Meraki*** 连接器上的端口映射



更新警报通知程序连接器日志配置

更新托管系统日志、邮件、Slack、PagerDuty 和 Kinesis 警报通知程序连接器的 Cisco Secure Workload 警报通知程序 (TAN) 服务的日志配置。由于 TAN 会托管多个连接器，因此无法直接从连接器页面更新日志配置。此允许的命令允许用户更新日志配置。

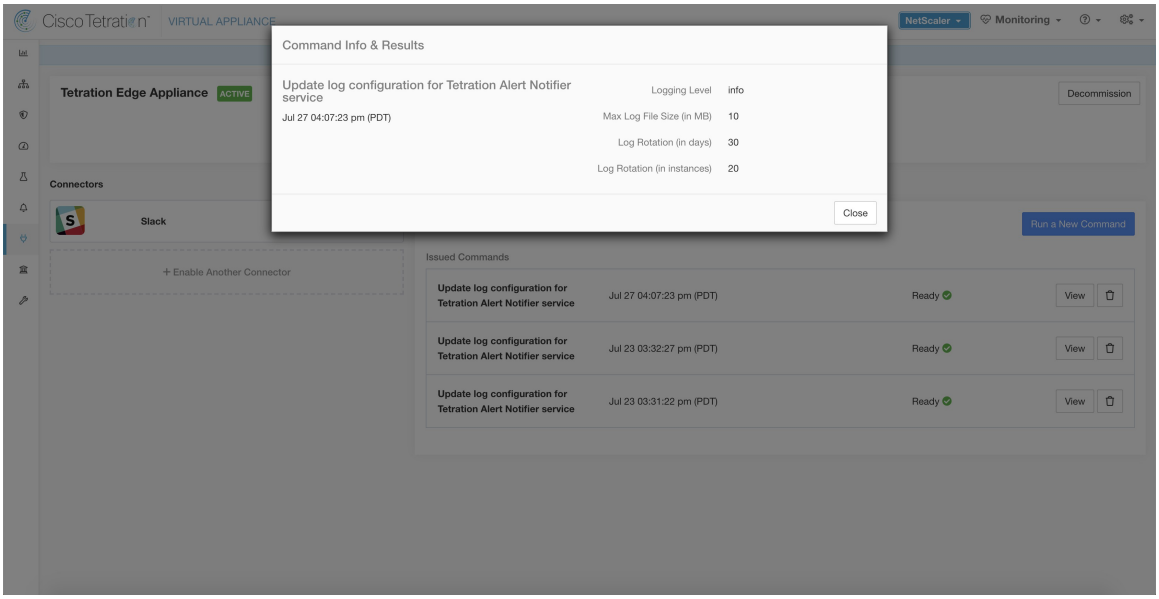
Cisco Secure Workload 会将命令发送到 Cisco Secure Workload 边缘设备的 TAN Docker 服务上的服务控制器。控制器会在服务上应用配置，并返回配置更新的状态。

参数名称	类型	说明
日志记录级别 **(Logging level)**	下拉菜单	服务使用的日志记录级别
	• 调试	调试日志级别
	• 信息	信息日志级别
	• 警告	警告日志级别
	• 错误	错误日志级别
最大日志文件大小 **(MB) (Max log file size [in MB])**	数字	开始日志轮换之前日志文件的最大大小
日志轮换（天）**(Log rotation [in days])**	数字	开始日志轮换之前日志文件的最长期限
日志轮换（以实例为单位）**(Log rotation [in instances])**	数字	保留的最大日志文件实例数

允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 边缘

允许的连接器：无

Figure 114: 更新 ***Cisco Secure Workload*** 边缘设备中的 ***Cisco Secure Workload*** 警报通知程序 ***Docker*** 服务上的日志配置



从设备收集快照

Cisco Secure Workload 将命令发送到发出命令的设备。当设备上的控制器收到来自 Cisco Secure Workload 的此命令时，它会收集设备快照，对其进行编码并将结果返回给 Cisco Secure Workload。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮，用于下载 `.tar.gz` 格式的文件。

快照中包含的文件：

- /local/tetration/appliance/appliance.conf
- /local/tetration/{logs, sqlite, user.cfg}
- /opt/tetration/tet_vm_setup/conf/tet-vm-setup.conf
- /opt/tetration/tet_vm_setup/docker/Dockerfile
- /opt/tetration/ova/version
- /usr/local/tet-controller/conf
- /usr/local/tet-controller/cert/{topic.txt, kafkaBrokerIps.txt}
- /var/run/supervisord.pid
- /etc/resolv.conf

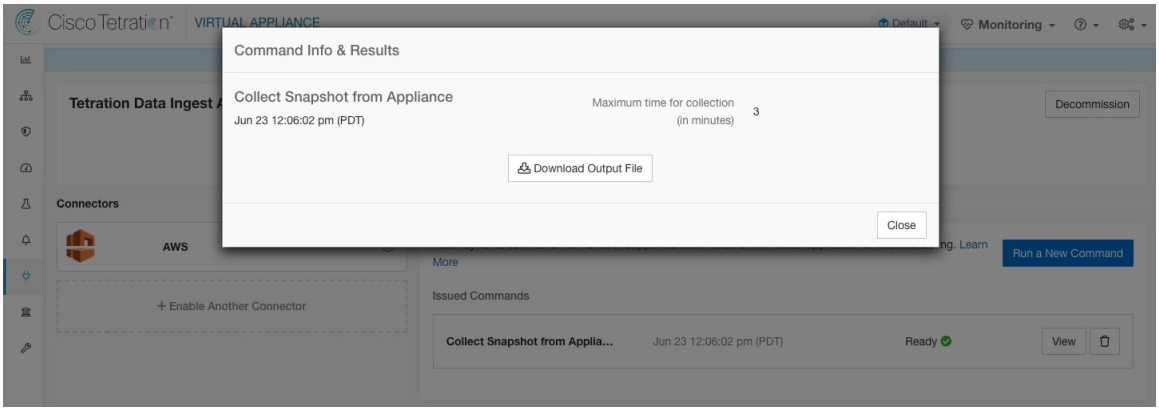
快照中包含的命令输出：

- ps aux
- iptables -L
- netstat {-nat, -rn, -suna, -stna, -tunlp}
- ss {-nat, -rn, -suna, -stna, -tunlp}
- /usr/local/tet-controller/tet-controller -version
- supervisorctl status
- rpm -qi tet-nic-driver tet-controller
- du -shc /local/tetration/logs
- ls {/usr/local/tet-controller/cert/, -l /local/tetration/sqlite/, -l /opt/tetration/tet_vm_setup/.tet_vm.done, -l/opt/tetration/tet_vm_setup/templates/}
- docker {images, ps -a}
- blkid/ifconfig/lscpu/uptime
- free -m
- df -h

参数名称	类型	说明
最长收集时间（分钟）	数字	返回结果之前收集的最长持续时间。应 < 20 分钟。

允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备

Figure 115: 从 ***Cisco Secure Workload*** 设备收集快照



从连接器收集快照

Cisco Secure Workload 将命令发送到部署了连接器的设备。根据连接器 ID，控制器收集连接器快照，对其进行编码并将结果返回到 Cisco Secure Workload。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮，用于下载 .tar.gz 格式的文件。

快照中包含的文件：

- /usr/local/tet-netflow/conf
- /local/tetration/{logs, sqlite}
- /var/run/{supervisord.pid, tet-netflow.pid}

快照中包含的命令输出：

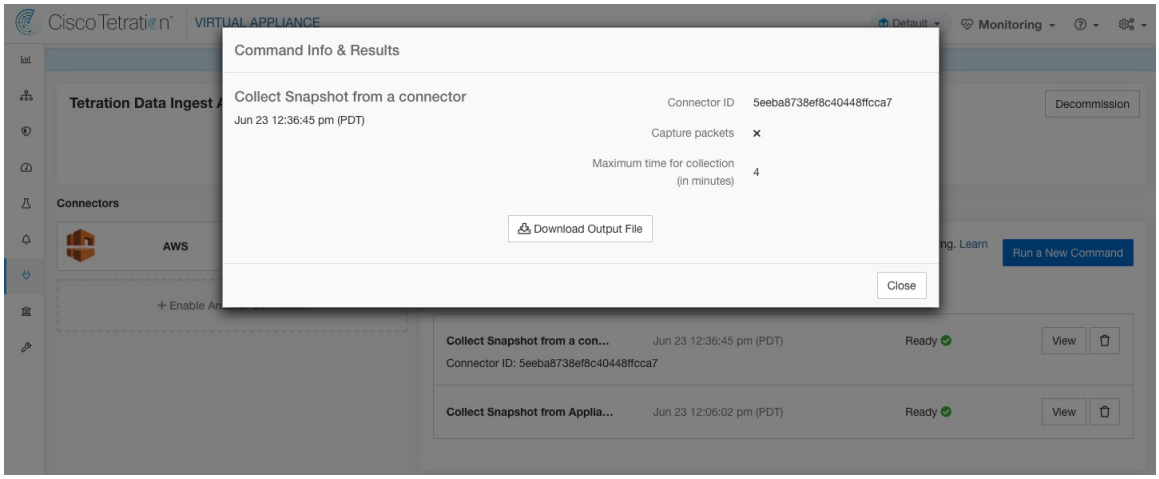
- ps aux
- netstat {-nat, -rn, -suna, -stna, -tunlp}
- ss {-nat, -rn, -suna, -stna, -tunlp}

参数名称	类型	说明
Connector ID	字符串	运行快照命令的连接器的连接器 ID。
Capture packets	复选框	是否应捕获数据包？

参数名称	类型	说明
Max time for collection in minutes	数字	返回结果之前收集的最长持续时间。应 < 20 分钟。

允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备

Figure 116: 从指定连接器 ***ID*** 上的 ***Cisco Secure Workload*** 连接器收集快照



收集控制器配置文件

收集设备或连接器上的控制器进程分析结果。Cisco Secure Workload 会将命令发送到发出命令的连接器。服务控制器会在指定的分析模式下重启连接器服务。收集分析结果后，服务控制器会在正常模式下重启服务，并将结果发送到 Cisco Secure Workload。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮，用于下载 `.tar.gz` 格式的文件。

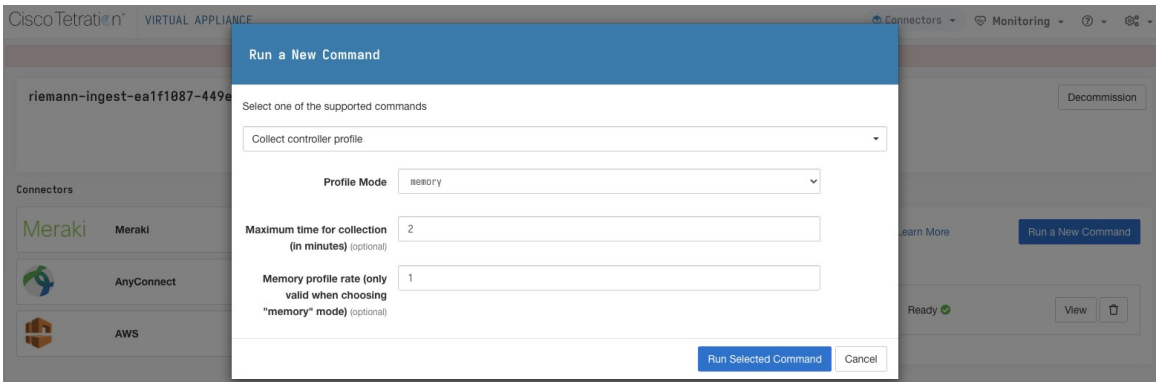
参数名称	类型	说明
配置文件模式	下拉菜单	分析模式。
	• *memory*	内存分析模式。
	• *cpu*	CPU 分析模式。
	• *block*	块分析模式。
	• *mutex*	Mutex 分析模式。
	• *goroutine*	Goroutine 分析模式。

参数名称	类型	说明
最长收集时间（分钟）	数字	返回结果之前收集的最长持续时间。
内存配置文件速率（仅在选择“内存”模式时有效）	数字	内存分析速率。此字段为选填字段。如果未提供，则会使用 Golang 中的默认值。

允许的 Cisco Secure Workload 虚拟设备：Cisco Secure Workload 注入和 Cisco Secure Workload 边缘设备

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE 和 Meraki。

Figure 117: 从 ***Cisco Secure Workload*** 设备收集控制器配置文件



收集连接器配置文件

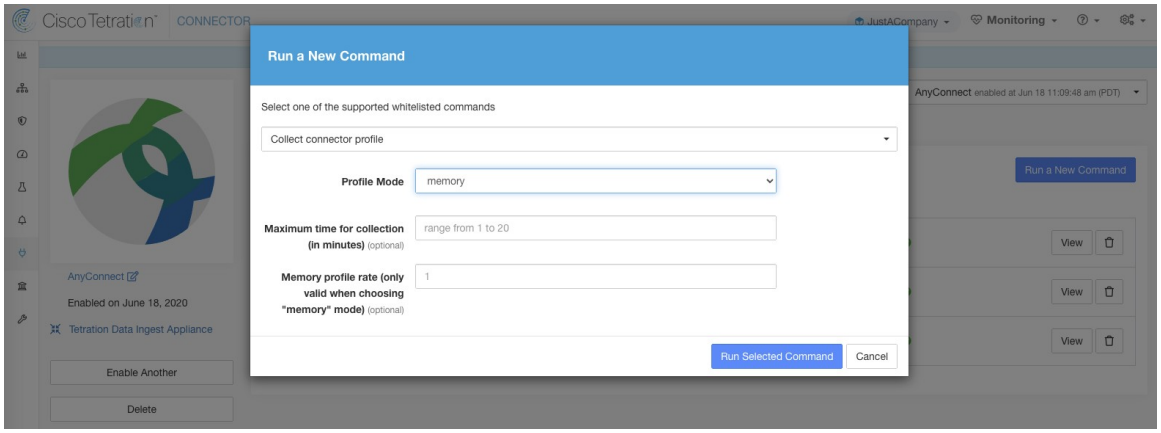
收集连接器上的连接器进程分析结果。Cisco Secure Workload 会将命令发送到发出命令的连接器。服务控制器会以指定的分析模式来重启连接器服务。收集分析结果后，服务控制器会在正常模式下重启服务，并将结果发送到 Cisco Secure Workload。当 Cisco Secure Workload 中提供结果时，系统会显示下载按钮，用于下载 `.tar.gz` 格式的文件。

参数名称	类型	说明
配置文件模式	下拉菜单	分析模式。
	• *memory*	内存分析模式。
	• *cpu*	CPU 分析模式。
	• *block*	块分析模式。
	• *mutex*	Mutex 分析模式。
	• *goroutine*	Goroutine 分析模式。
最长收集时间（分钟）	数字	返回结果之前收集的最长持续时间。
内存配置文件速率（仅在选择“内存”模式时有效）	数字	内存分析速率。此字段为选填字段。如果未提供，则会使用 Golang 中的默认值。

允许的 Cisco Secure Workload 虚拟设备： Cisco Secure Workload 注入和 Cisco Secure Workload 边缘

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE 和 Meraki。

Figure 118: 从 ***Cisco Secure Workload*** 连接器收集连接器配置文件



覆盖设备的连接器警报间隔

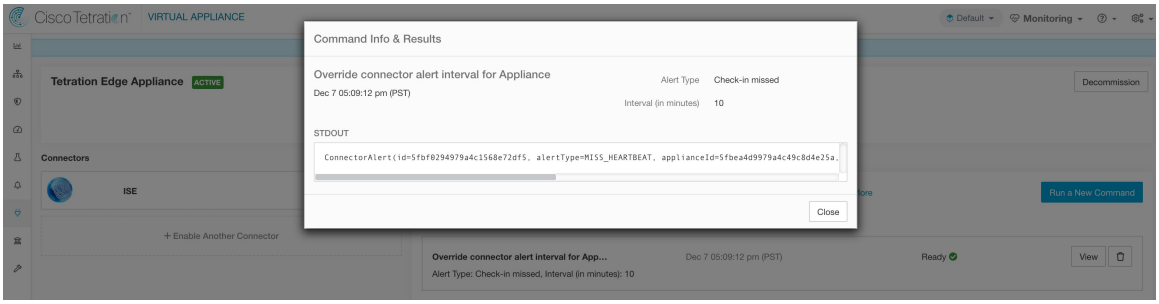
覆盖设备的默认连接器警报间隔。Cisco Secure Workload 将同一连接器警报限制默认每天仅发送一次。当管理员认为一天一次的间隔时间太长时，可以使用此命令来覆盖间隔时间。当 Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
警报类型	下拉菜单	要覆盖的连接器警报类型。
	• 已错过签入	错过设备签入。
	• *CPU* 使用率	CPU 使用率
	• 内存使用率	高内存使用率。
	• 磁盘使用率	高磁盘使用率
间隔（以分钟为单位）	数字	覆盖间隔的持续时间（以分钟为单位）。

允许的 Cisco Secure Workload 虚拟设备： Cisco Secure Workload 注入和 Cisco Secure Workload 边缘

允许的连接器：无

Figure 119: 覆盖 ***Cisco Secure Workload*** 设备的连接器警报间隔



覆盖连接器的连接器警报间隔

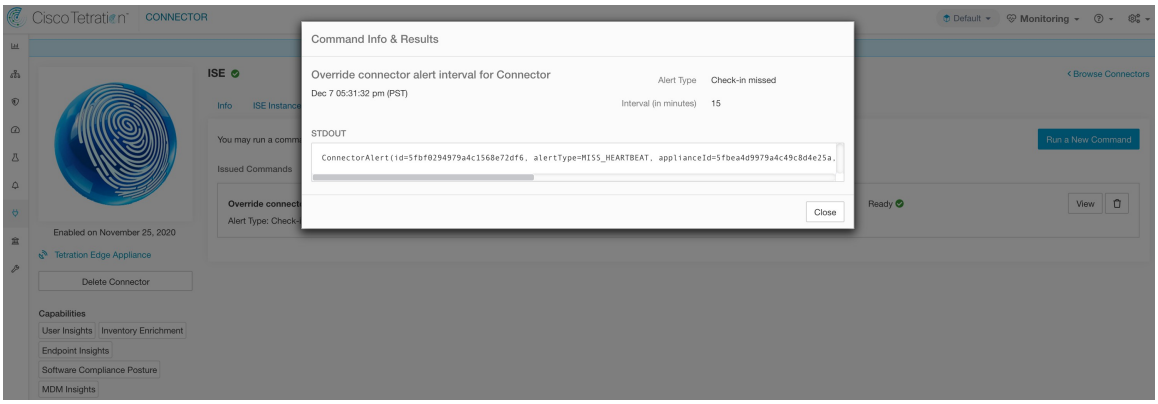
覆盖连接器的默认连接器警报间隔。Cisco Secure Workload 将同一连接器警报限制默认每天仅发送一次。当管理员认为一天一次的间隔时间太长时，可以使用此命令来覆盖间隔时间。当Cisco Secure Workload 中提供结果时，结果会显示在文本框中。

参数名称	类型	说明
警报类型	下拉菜单	要覆盖的连接器警报类型。
	• 已错过签入	未完成连接器的签入。
间隔（以分钟为单位）	数字	覆盖间隔的持续时间（以分钟为单位）。

允许的 Cisco Secure Workload 虚拟设备：无

允许的连接器：NetFlow、NetScaler、F5、AnyConnect、Syslog、Email、Slack、PagerDuty、Kinesis、ISE、ASA、Meraki、ServiceNow、WAD。

Figure 120: 覆盖 ***Cisco Secure Workload*** 连接器的连接器警报间隔



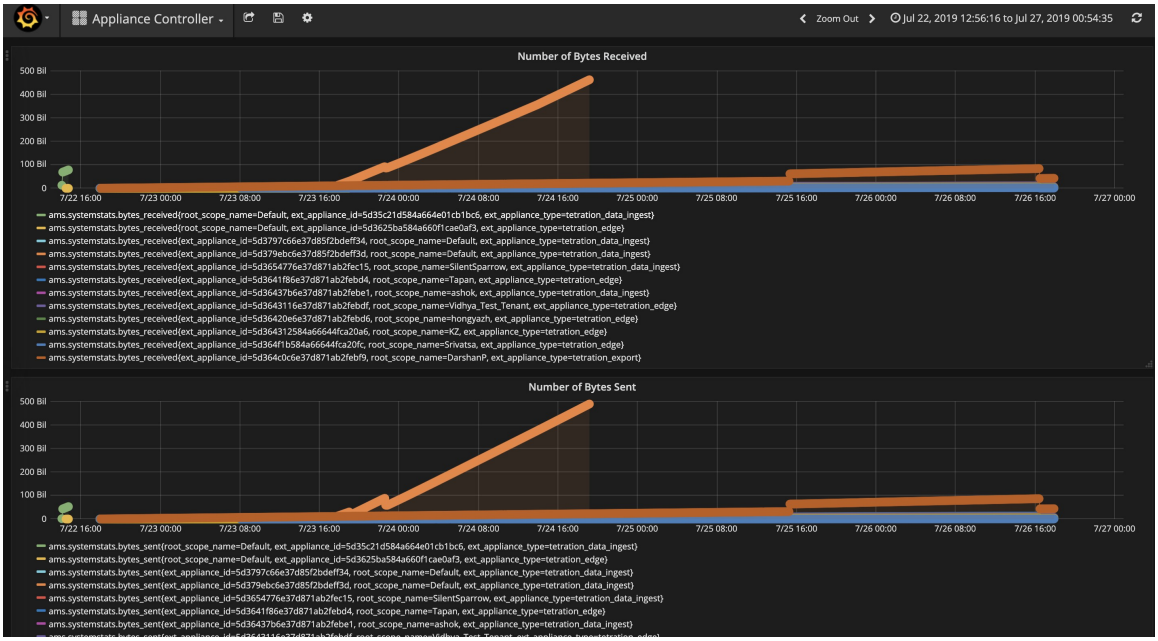
Hawkeye 控制面板

“Hawkeye”控制面板提供有关连接器和启用了连接器的虚拟设备运行状况的见解。

设备控制器控制面板

设备控制器控制面板提供有关网络统计信息、系统指标（例如CPU使用百分比、内存使用率、磁盘使用率和打开文件描述符数）的信息。

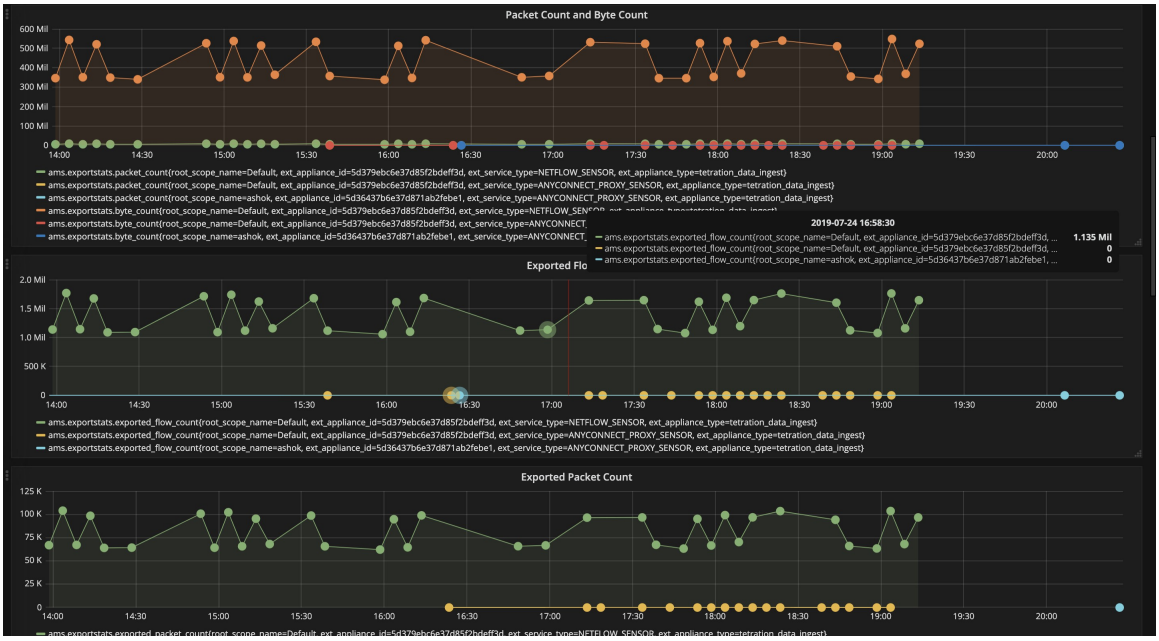
Figure 121: 设备控制器控制面板



服务控制面板

服务控制面板提供有关导出指标的信息（如果适用），包括导出到 Cisco Secure Workload 的流观察结果的数量、导出到 Cisco Secure Workload 的数据包数以及导出到 Cisco Secure Workload 的字节数。此外，此控制面板还提供有关协议处理和解码的信息（例如，处理 NetFlow v9 和 IPFIX 的服务）。此控制面板中提供解码计数、解码错误计数、流计数、数据包计数和字节计数等指标。此外，此控制面板中还包括运行服务的 Docker 容器的系统指标。CPU 使用率、内存使用率、磁盘使用率和打开的文件描述符数等指标是此控制面板的一部分。

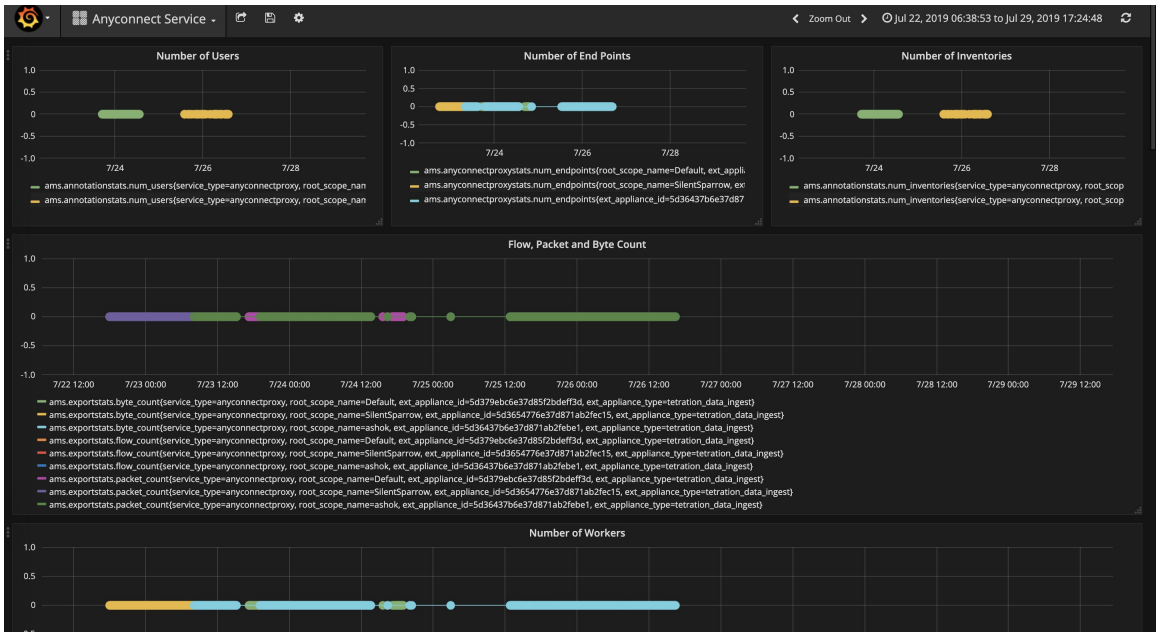
Figure 122: 服务控制面板



AnyConnect 服务控制面板

AnyConnect 服务控制面板提供有关 AnyConnect 特定服务信息的信息。此控制面板中提供 AnyConnect 连接器向 Cisco Secure Workload 报告的终端数量、资产数量、用户数量等指标。此外，此控制面板还提供有关 IPFIX 协议处理和解码的信息。此控制面板中提供解码计数、解码错误计数、流计数、数据包计数和字节计数等指标。

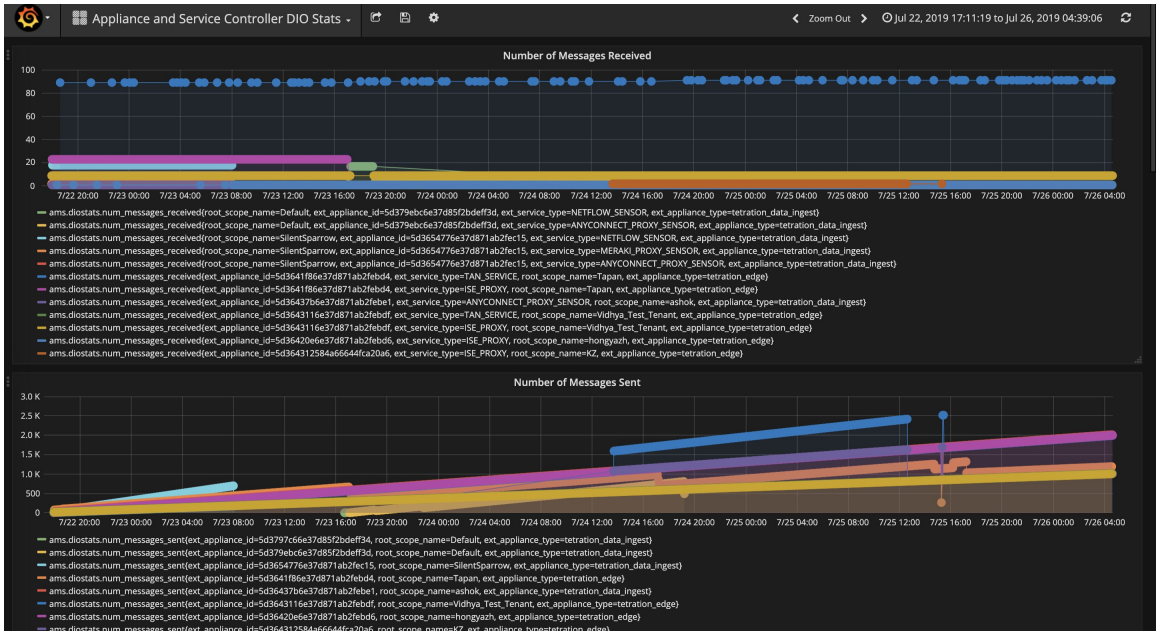
Figure 123: AnyConnect 控制面板



设备和服务 DIO 控制面板

设备和服务 DIO 面板提供有关在设备管理器和设备/服务控制器通信的 Kafka 主题中交换的消息数量的消息。此控制面板包括收到的消息数量、发送的消息数量、失败的消息数量等指标。此外，还提供控制器读取的最后偏移量，以了解控制器在处理来自管理器的控制信息时是否滞后。

Figure 124: 设备和服务 ***DIO*** 控制面板



常规故障排除指南

一旦连接器在 Cisco Secure Workload 的连接器页面中显示为活动状态，则无需在启用了该连接器的设备上执行任何操作；用户无需登录。如果没有出现这种情况，以下信息将有助于对此类问题进行故障排除。

正常情况下，在设备上：

- `systemctl status tet_vm_setup.service` 报告具有 *SUCCESS* 退出状态的非活动服务；
- `systemctl status tet-nic-driver` 报告活动服务。
- `supervisorctl status tet-controller` 报告 *RUNNING* 服务。这表示设备控制器已启动并正在运行。
- `docker network ls` 报告三个网络：`bridge`、`host` 和 `none`。
- `docker ps` 报告正在设备上运行的容器。通常情况下，在设备上成功启用连接器后，设备上会实例化一个 Docker 容器。对于系统日志、邮件、Slack、PagerDuty 和 Kinesis 连接器，Cisco Secure Workload 警报通知程序服务会在 Cisco Secure Workload 边缘设备上实例化为 Docker 容器。
- 每个容器的 `docker logs <cid>` 应报告 tet-netflowsensor 已进入 RUNNING 状态。
- `docker exec <cid> ifconfig` 只报告一个接口（环回除外）。
- `docker exec <cid> netstat -rn` 报告默认网关。
- 设备上的 `cat /local/tetration/appliance/appliance.conf`，以查看设备上运行的 Docker 服务列表。它包括有关服务 ID、连接器 ID、容器、映像 ID 和端口映射（如适用）的详细信息。在 Cisco Secure Workload 注入设备上，最多可在设备上运行三项服务。端口映射和容器上装载的 Docker 卷可在此文件中找到。

***Figure 125: Cisco Secure Workload* 设备部署服务和状态**

```
[root@esx-2106-ingest tetter]# systemctl status tet_vm_setup.service
• tet_vm_setup.service - Tetration Appliance Setup
   Loaded: loaded (/etc/systemd/system/tet_vm_setup.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Sat 2019-07-27 23:51:29 UTC; 21h ago
 Main PID: 1249 (code=exited, status=0/SUCCESS)

Jul 27 23:51:12 localhost.localdomain python[1249]: mount: /dev/sr0 is write-protected, mounting read-only
Jul 27 23:51:29 esx-2106-ingest python[1249]: Docker version 18.09.8, build 0dd43dd87f
Jul 27 23:51:29 esx-2106-ingest python[1249]: REPOSITORY          TAG                 IMAGE ID            CREATE... SIZE
Jul 27 23:51:29 esx-2106-ingest python[1249]: userPrivateKey.key
Jul 27 23:51:29 esx-2106-ingest python[1249]: intermediateCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaBrokerIps.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: userCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: kafkaCA.cert
Jul 27 23:51:29 esx-2106-ingest python[1249]: topic.txt
Jul 27 23:51:29 esx-2106-ingest python[1249]: Created symlink from /etc/systemd/system/multi-user.target.wants/s...vice.
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 126: Cisco Secure Workload 网络驱动程序服务状态

```
[root@esx-2106-ingest tetter]# systemctl status tet-nic-driver.service
● tet-nic-driver.service - NIC network driver plugin for Docker
   Loaded: loaded (/etc/systemd/system/tet-nic-driver.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2019-07-27 23:51:12 UTC; 21h ago
 Main PID: 733 (nic)
   Memory: 4.4M
   CGroup: /system.slice/tet-nic-driver.service
           └─733 /usr/local/tet/nic-driver/nic -log-level debug

Jul 27 23:51:12 localhost.localdomain systemd[1]: Started NIC network driver plugin for Docker.
Jul 27 23:51:12 localhost.localdomain systemd[1]: Starting NIC network driver plugin for Docker...
Jul 27 23:51:12 localhost.localdomain nic[733]: time="2019-07-27T23:51:12Z" level=info msg="NIC network driver started"
Hint: Some lines were ellipsized, use -l to show in full.
[root@esx-2106-ingest tetter]#
```

Figure 127: 设备控制器状态

```
[root@esx-2106-ingest tetter]# supervisorctl status tet-controller
tet-controller                   RUNNING   pid 1971, uptime 21:43:29
[root@esx-2106-ingest tetter]#
```

如果上述任何一项不成立，请检查 /local/tetration/logs 中的部署脚本日志，查找设备和/或连接器部署失败的原因。

您可以按如下所述对任何其他连接器注册/连接问题进行故障排除。

`docker exec <cid> ps -ef` 会报告 tet-netflowsensor-engine、`/usr/local/tet/ tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf` 实例，以及进程管理器 `/usr/bin/supervisord -c /usr/local/tet-netflow/ conf/supervisord.conf -n` 实例。

Figure 128: 在 *Cisco Secure Workload* 注入设备中的 *Cisco Secure Firewall ASA* 连接器上运行进程

```
[root@esx-2106-ingest tetter]# docker ps
CONTAINER ID        IMAGE                                                                                                COMMAND
     CREATED             STATUS              PORTS                                    NAMES
c82decfaa877        asa_sensor-3.4.2.52465.appliance.demo.mrpm.build-asa:5d3ce5e43649723890271dd3   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours         172.29.142.27:4729->4729/udp    asa-5d3ce5e43649723890271dd3
eddd5cd59839        aws_sensor-3.4.2.52465.appliance.demo.mrpm.build-aws:5d3ce3b73649723890271dce   "/usr/bin/supervisor
…"   22 hours ago        Up 22 hours                                          aws-5d3ce3b73649723890271dce
[root@esx-2106-ingest tetter]# docker exec c8 ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 00:01 ?        00:00:15 /usr/bin/python /usr/bin/supervisord -c /usr/local/tet-netflow/conf/supe
rvisord.conf -n
root         8     1  0 00:01 ?        00:02:24 /usr/local/tet-netflow/tet-netflowsensor-engine -ctrl-config /usr/local/
tet-netflow/conf/tet-controller.conf -upgrade-script /usr/local/tet-netflow/scripts/check_config_update.sh -service /usr
/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/conf/tet-netflow.conf
root     27002     8  0 21:31 ?        00:00:00 /usr/local/tet-netflow/tet-netflowsensor -config /usr/local/tet-netflow/
conf/tet-netflow.conf
root     27024     0  0 21:32 ?        00:00:00 ps -ef
[root@esx-2106-ingest tetter]#
```

日志文件

以下命令可用于查看设备上各种服务的日志。

- **/local/tetration/logs/tet-controller.log** 可显示设备控制器的日志。
- **docker exec <cid> cat /local/tetration/logs/tet-controller.log**可显示连接器上服务控制器的日志。
- **docker exec <cid> cat /local/tetration/logs/tet-netflow.log**可显示连接器服务的日志。

- **docker exec <cid> cat /local/tetration/logs/tet-ldap-loader.log** 可显示 LDAP 快照创建的日志（如果 LDAP 配置适用于连接器）。
- **docker exec <cid> cat /local/tetration/logs/check_conf_update.log** 可显示配置更新轮询日志（适用于注入设备上的连接器）。

Note Cisco Secure Workload 上有允许的命令集，可直接从设备和/或连接器提取这些日志。有关详细信息，请参阅允许的命令集。

调试模式

设备/服务控制器和连接器服务的默认日志记录级别会被设置为 *info* 级别。为了解决问题，我们可能需要将代理设置为调试模式。为此，请直接在 Cisco Secure Workload 上为所需设备/连接器更新设备/连接器上的日志配置。如果更新连接器上的配置，控制器和服务的日志级别都会更新。有关详细信息，请参阅日志配置。

Cisco Secure Firewall Management Center

将 Cisco Secure Workload 的强大功能与 Cisco Secure Firewall（以前称为 Cisco Firepower）的强大功能相结合，可实现利用以下功能的安全解决方案：

- 分段

  基于防火墙的分段适用于未安装软件代理的工作负载。但是，您也可以将此方法用于基于代理的工作负载。您可以针对进入网络的流量、离开网络的流量以及网络内工作负载之间的流量，轻松、广泛地应用不同的策略集。

- 虚拟修补

  虚拟修补可为安装了软件代理的工作负载添加思科入侵防御系统 (IPS) 保护。您可以使用此方法来保护应用免受恶意流量的攻击。当您在 Cisco Secure Workload 上配置虚拟修补时，它会向 Cisco Secure Firewall 发布常见漏洞和风险 (CVE)，以供创建 IPS 策略时考虑。

通过此集成，Cisco Secure Workload 会自动在由 Cisco Secure Firewall Management Center 实例管理的 Cisco Secure Firewall Threat Defense（以前称为 Firepower Threat Defense）防火墙上执行和管理分段策略。策略会动态更新，并且随着应用环境的变化不断刷新应用策略的工作负载集。

网络资产由分段策略所基于的 Cisco Secure Workload 资产过滤器动态更新；当从网络中添加、更改或删除工作负载时，Cisco Secure Workload 会自动更新相应访问控制规则所基于的 Cisco Secure Firewall Management Center 中的动态对象。所有已执行的策略更改都会自动部署到托管 Cisco Secure Firewall Threat Defense（以前称为 Firepower Threat Defense 或 FTD）设备；您无需在 Cisco Secure Firewall Management Center 中重新部署更改。

有关此集成的完整信息，包括有关其工作原理、支持的平台、限制、两种产品的设置说明以及故障排除信息的更多详细信息，请参阅《Cisco Secure Workload 和 Cisco Secure Firewall Management Center 集成指南》。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。