在安全工作负载(Tetration)上生成快照文件

目录

简介

本文档介绍如何在思科安全工作负载(Tetration)上为不同类型的日志收集生成快照捆绑包文件。

先决条件

使用的组件

思科建议您了解以下产品：

- 思科安全工作负载(Tetration)
- 思科集成管理控制器(CIMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

> **注意：** 您必须具有客户支持角色才能访问快照工具。

> **警告：**本文档中的说明适用于运行软件版本3.4.1.x或更高版本的Cisco安全工作负载(Tetration)。

用于确定Tetration Cluster硬件、软件和集成状态的快照捆绑包包括：

- 经典快照捆绑包：收集 集群相关数据的日志消息、配置数据、命令输出、警报、时序数据库(tsdb)等的集合。
- CIMC快照捆绑包：从统一计算系统(UCS)收集技术支持文件，适用于硬件设备(8RU、39RU)集

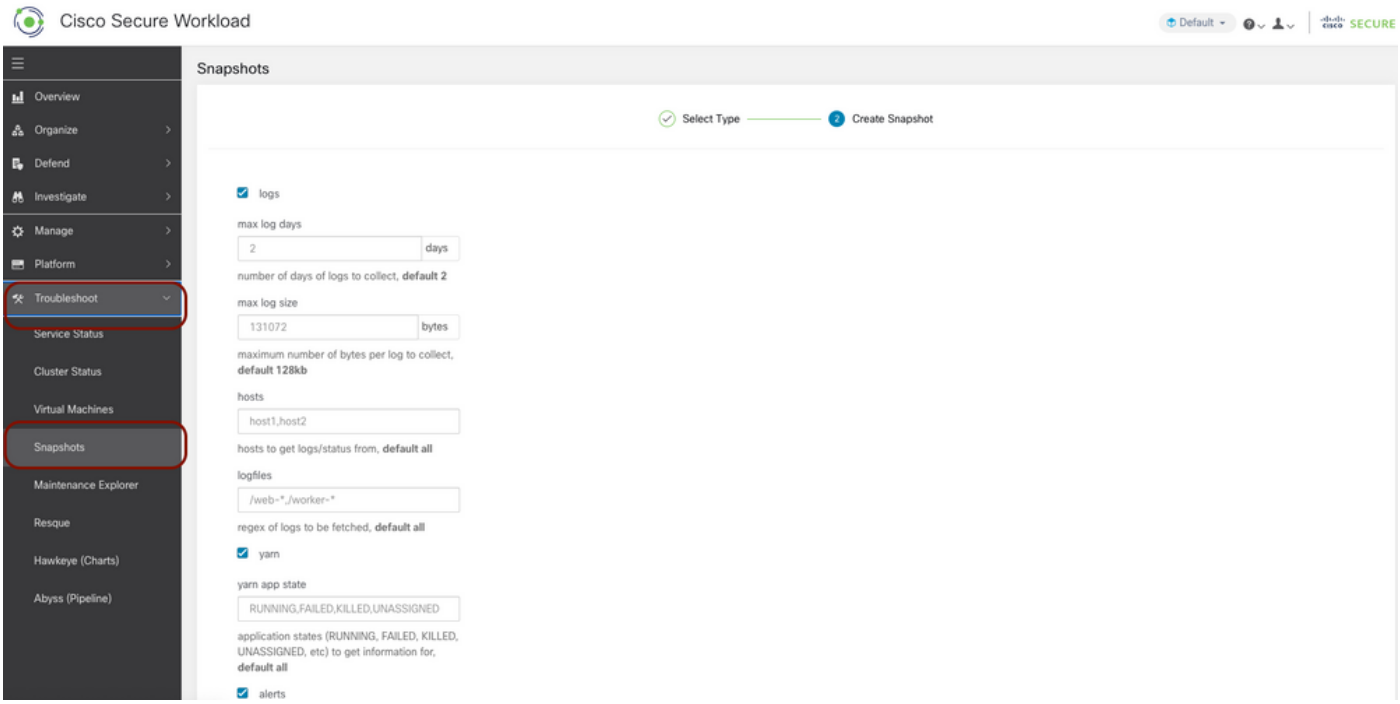
群。
- 软件代理捆绑包：包含安装在终端系统上用于遥测数据收集的Tetration代理日志。
- 虚拟设备连接器套件：包含来自Tetration Virtual设备的日志，该设备支持流接收、资产丰富和警报通知。

如果思科工程师请求您从安全工作负载集群发送快照捆绑包，您可以使用本文档中提供的说明。

收集快照捆绑包

生成传统快照捆绑包

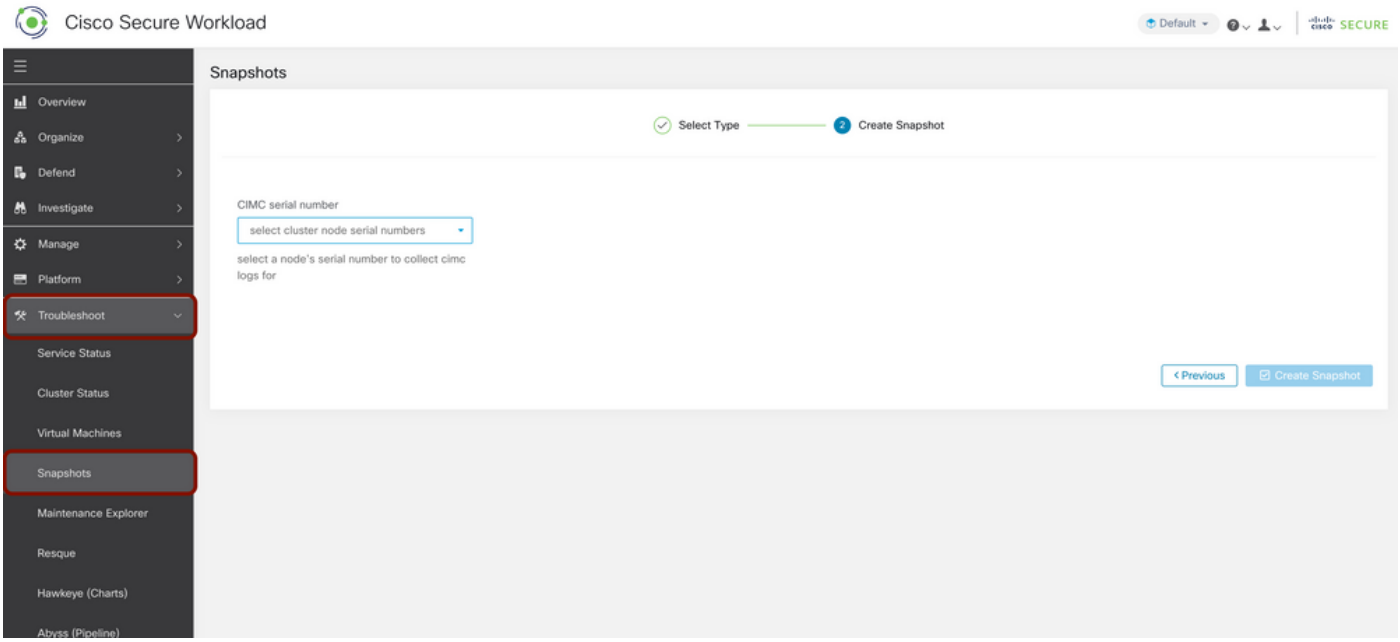
登录到安全工作负载用户界面(UI)，导航到左侧导航面板，然后选择**Troubleshoot > Snapshot** [**Maintenance > Snapshot**（3.4.x或3.5.x）]选项。单击“**创建快照**”，然后选**择“经典快照**”。系统将显示带有默认选项的快照页面。如果思科TAC工程师明确要求您，您可以覆盖默认选项。



向下滚动到页面底部，使用注释部分指定案例编号或问题说明，然后单击**创建快**照以启动生成传统快照捆绑包的过程。完成快照生成可能需要一段时间。快照生成达到100%后，单击**Download**下载经典快照捆绑包。向下滚动，获取将文件上传到案例编号的选项。

生成CIMC捆绑包

登录到安全工作负载UI，导航到左侧导航面板，然后选择**Troubleshoot > Snapshot** [**Maintenance > Snapshot**（3.4.x或3.5.x）]。单击**创建快**照，然后选择**CIMC快照**。系统将显示CIMC快照页面，其中包含用于选择节点序列号的下拉选项。搜索或选择节点，然后单击**创建快**照以启动生成CIMC快照捆绑包的过程。



完成快照生成可能需要一段时间。快照生成达到100%后，单击**Download**下载CIMC快照捆绑包。向下滚动，获取将文件上传到案例编号的选项。

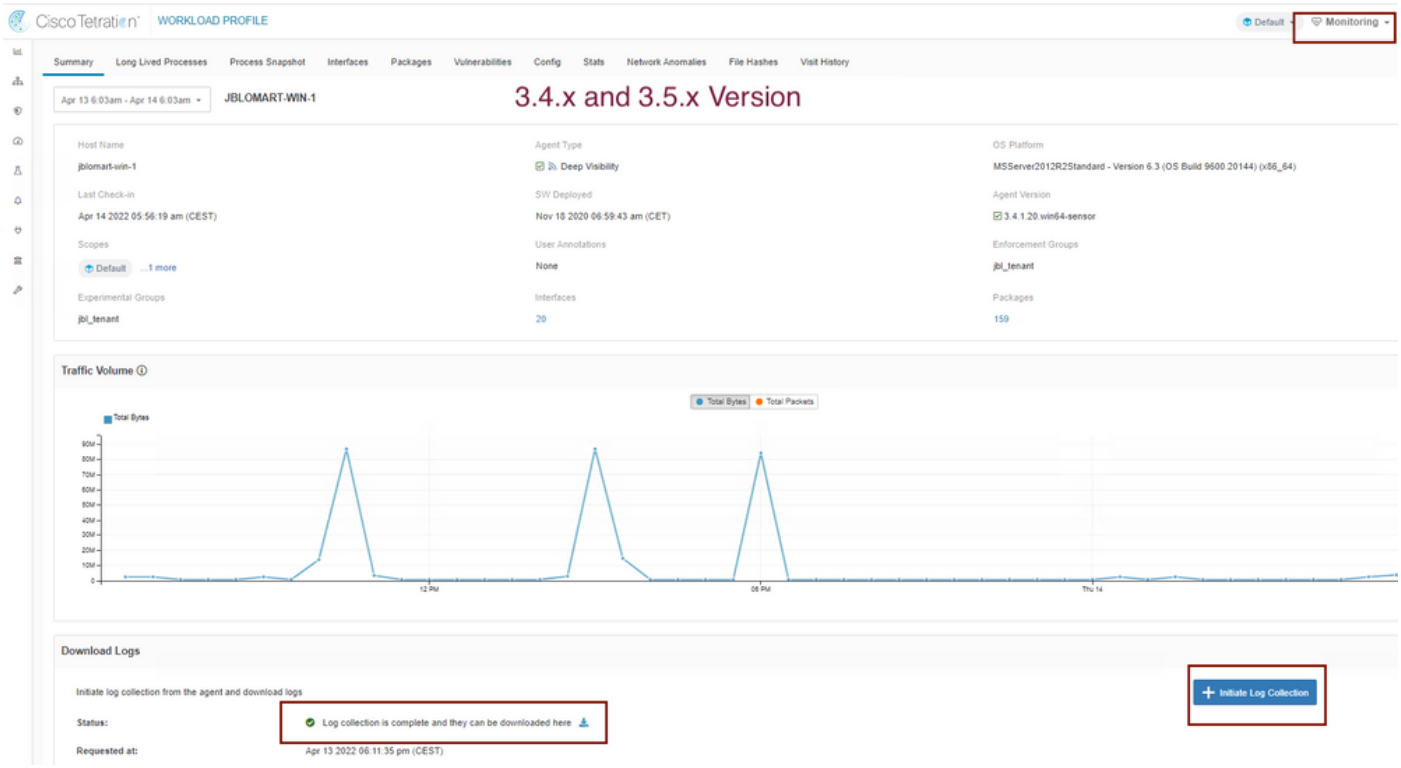
生成Tetration Agent日志捆绑包

要收集日志捆绑包，Tetration代理必须处于活动状态。

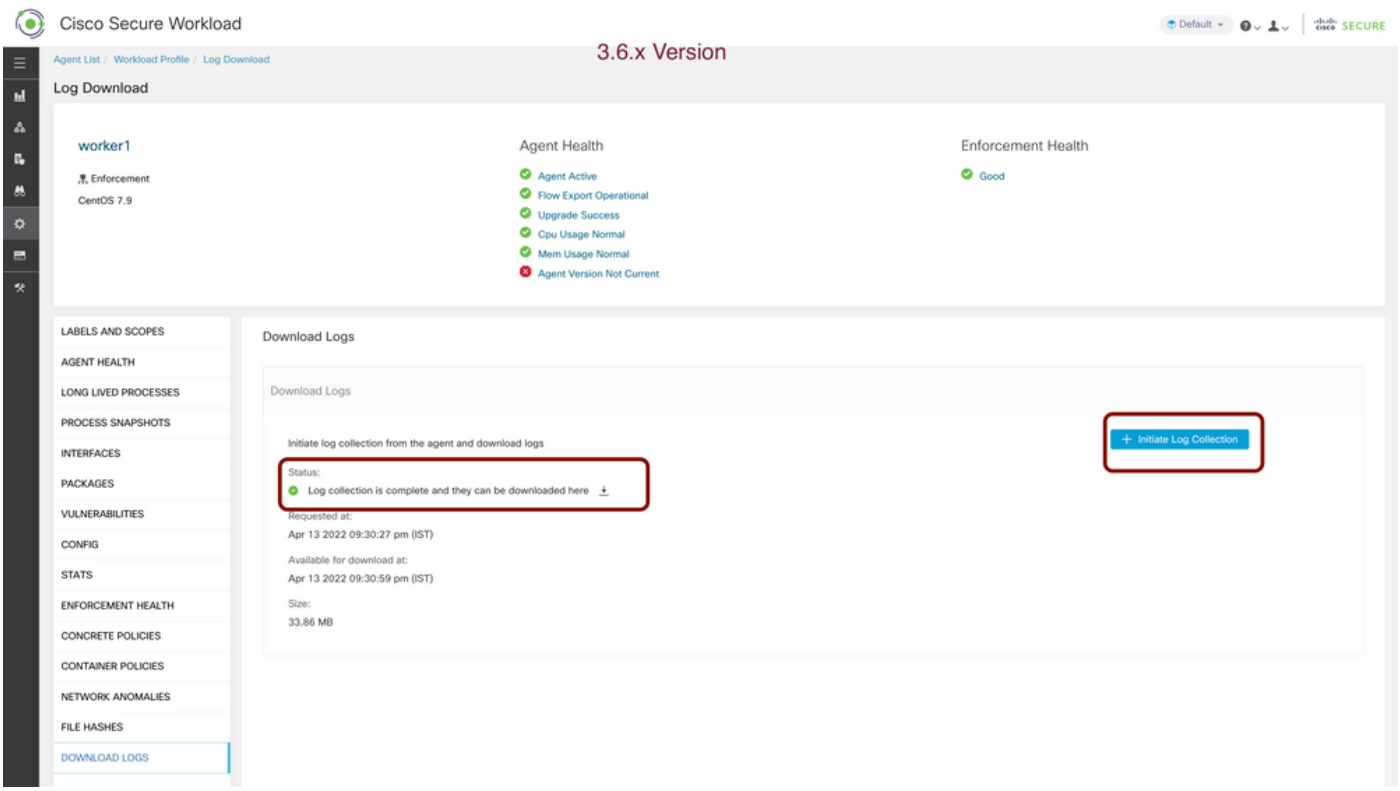
- 对于3.6.x版本，导航至左侧导航面板，选择“管理”**>“代理”**，然后单击“**代理列表**”。
- 对于3.4.x和3.5.x版本，从右上下拉菜**单导**航至“监控”，然后选择“代理**列表”**。

使用过滤器选项搜索代理，然后单击**Agent**。它会将您带到代理的工作量配置文件。您可以在此处找到有关代理配置、状态等的详细信息。

在工作负载配置文件页面(3.6.x)的左侧导航面板中，选择**Download Logs**（在3.4.x和3.5.x中，然后遵循摘要选项卡）。 单击**Initiate Log Collection(启动日**志收集)以从Tetration Agent启动日志收集。完成日志收集可能需要一段时间。完成日志收集后，单击“Download here”**选项**下载日志。向下滚动，获取将文件上传到案例编号的选项。



3.4.x和3.5.x版本



3.6.x版本

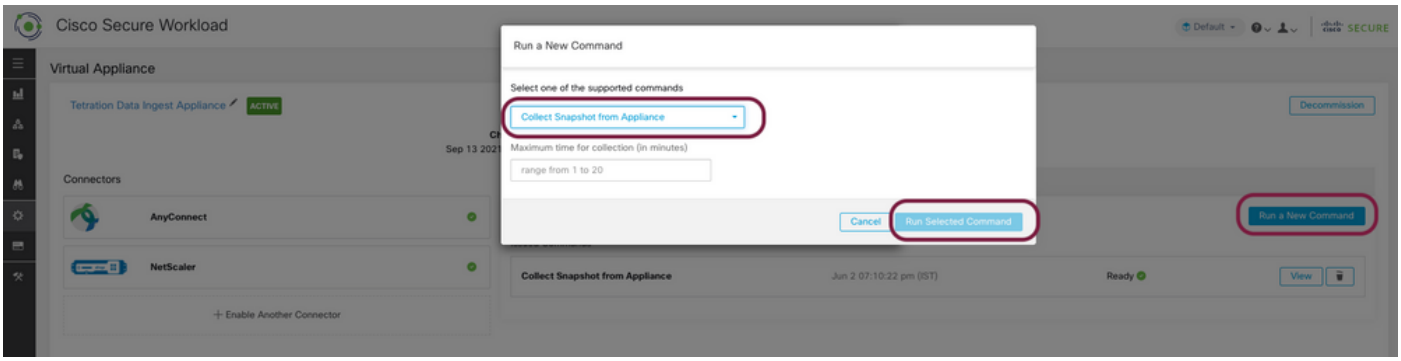
生成虚拟设备连接器快照捆绑包

要获取虚拟设备的快照捆绑包，您需要确保虚拟设备处于**活动**状态。

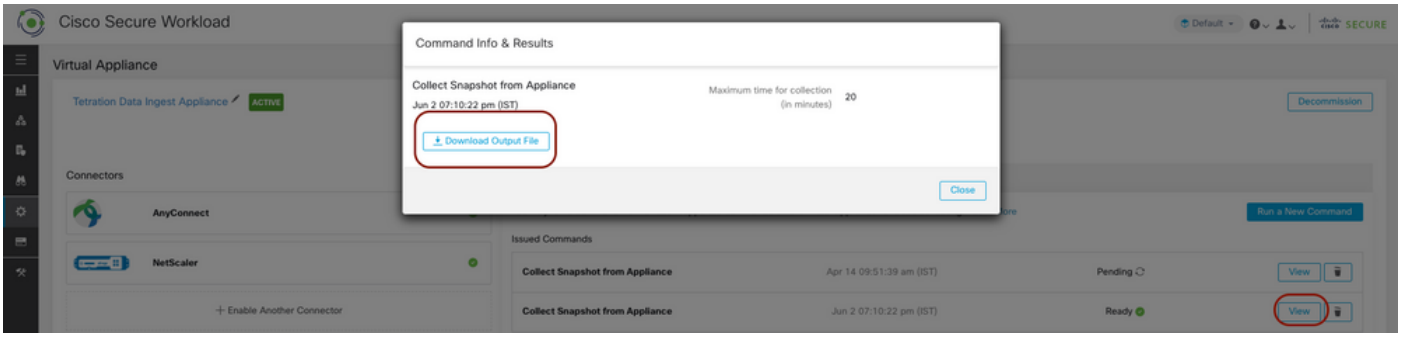
- 对于3.6.x版本，导航至左侧导航面板，然后选择**Manage > Virtual Appliance**。
- 对于3.4.x和3.5.x版本，导航至左侧导航面板，然后选择“连接器”>“虚拟设备”。

选择要为其生成快照捆绑包的虚拟设备。单击**Troubleshoot**，然后再次单击**Troubleshoot** 选项。单击**“运行新命令”**，将打开一个对话框。该对话框具有用于选择命令的下拉菜单。从下拉菜单中，选

择**从设备收集快照**并指定时间范围（以分钟为单位，例如20分钟），然后单击**运行选定命令**。它启动从虚拟设备收集快照捆绑包的过程。从虚拟设备收集日志捆绑包可能需要一段时间。



快照捆绑包的集合完成后，单击**View**下载快照捆绑包。向下滚动，获取将文件上传到案例编号的选项。



将捆绑包上传到思科服务请求(SR)

将快照捆绑包上传到案例(SR)有多种方法。 有关详细信息，请查看Cisco Technical Assistance Center页面的Customer File Uploads页面。

- 思科安全工作负载(Tetration)
- 思科安全工作负载(Tetration)产品概述
- **技术支持和文档 - Cisco Systems**