ThreatGrid设备建议在安装3.0版之前完成所需的重置

目录

简介

为准备ThreatGrid设备3.0版，需要重置特定设备，以便执行版本所需的低级磁盘格式设置，导致设备上的所有数据被销毁。

作者：T.J. Busch，思科TAC工程师。

先决条件

Cisco 建议您了解以下主题：

- 思科ThreatGrid设备

使用的组件

本文档不限于特定的软件和硬件版本。

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。

问题

您在ThreatGrid设备上收到通知：

```
This appliance was initially installed with a software release prior to 2.7.0, and has not had
its datastore reset
after 2.7.0 or later was installed.

The 3.0 software release only supports the new storage format introduced with 2.7.0, and cannot
be installed without first
performing a data reset (which will delete all content and recreate the datastore in the new
format).

This can be done at any time before the appliance 3.0 release is installed.

A data reset will be required before the appliance 3.0 release can be installed.
```

```
Be sure the backup system has been running for 48 hours without any failure reports before
performing this reset,
and that you have downloaded your backup encryption key.

Contact customer support for any question
```

解决方案

> **注意**：在设备上发出destroy data命令并且流程开始之前，设备上不会产生生产影响/数据丢失风险

为准备ThreatGrid设备3.0版，需要重置特定设备，以便执行版本所需的低级磁盘格式设置，导致设备上的所有数据被销毁。为防止设备丢失数据，必须将TGA配置为备份到NFS共享，然后在格式完成后恢复数据。为了完成此操作，确保备份成功运行至少48小时至关重要。此外，请确保备份加密密钥，因为需要将此密钥导入TGA以恢复数据。

> **警告：如果执行“destroy-data”，所有软件配置都将重置。不会修改CIMC配置，但管理员、干净、脏接口配置上的配置将被删除。因此，在禁用CIMC接口的M5 ThreatGrid设备的情况下，我们应确保在尝试此步骤之前，能够使用键盘和显示器对设备进行物理访问，以重新配置接口设置和IP地址。**

> **注意**：一旦从系统生成加密密钥，便无法检索加密密钥。确保将密钥备份到安全位置以防止数据丢失