ThreatGrid裝置建議在安裝3.0版之前完成所需的重置

目錄

[簡介](#)
[必要條件](#)
[採用元件](#)
[問題](#)
[解決方案](#)

簡介

在準備ThreatGrid裝置3.0版本時，需要重置特定裝置，以便執行版本所需的低級磁碟格式設定，從而銷毀裝置上的所有資料。

作者：T.J. Busch，思科TAC工程師。

必要條件

思科建議您瞭解以下主題：

- Cisco ThreatGrid裝置

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

您在ThreatGrid裝置上收到通知：

```
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
```

解決方案

附註：在裝置上發出destroy data命令並開始處理之前，不會產生裝置上的生產影響/資料丟失風險

在準備ThreatGrid裝置3.0版本時，需要重置特定裝置，以便執行版本所需的低級磁碟格式設定，從而銷毀裝置上的所有資料。為防止資料丟失裝置，您必須將TGA配置為備份到NFS共用，然後在完成格式化後恢複資料。要完成此操作，必須確保備份成功運行至少48小時。此外，請確保備份加密金鑰，因為需要將此金鑰匯入到TGA才能還原資料。

注意：如果執行「destroy-data」，則所有軟體配置都將重置。將不會修改CIMC配置，但將刪除Admin、Clean、Dirty介面配置上的配置。因此，在禁用了CIMC介面的M5 ThreatGrid裝置的情況下，在嘗試此步驟之前，我們應確保使用鍵盤和顯示器對裝置進行物理訪問，以重新配置介面設定和IP地址。

注意：從系統生成加密金鑰後，將無法檢索加密金鑰。確保將金鑰備份到安全位置，以防止資料丟失