ThreatGridアプライアンスは、バージョン3.0をインストールする前に、必要なリセットを完了する必要があることを推奨しています

内容

概要

ThreatGridアプライアンス3.0リリースの準備として、リリースに必要な低レベルのディスクフォーマットを実行するために、特定のアプライアンスをリセットする必要があります。その結果、デバイス上のすべてのデータが破棄されます。

著者：Cisco TACエンジニア、T.J. Busch

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ThreatGridアプライアンス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

ThreatGridアプライアンスで次の通知を受信しました。

```
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
```

解決方法

> **注**：デバイスでdestroy dataコマンドが発行されてプロセスが開始されるまで、デバイスに対する実稼働への影響やデータ損失のリスクはありません

ThreatGridアプライアンス3.0リリースの準備として、リリースに必要な低レベルのディスクフォーマットを実行するために、特定のアプライアンスをリセットする必要があります。その結果、デバイス上のすべてのデータが破棄されます。デバイスへのデータ損失を防ぐために、NFS共有にバックアップし、フォーマットが完了したらデータを復元するようにTGAを設定する必要があります。これを完了するには、バックアップが少なくとも48時間正常に実行されるようにすることが重要です。また、データを復元するには、TGAにインポートする必要があるため、暗号化キーがバックアップされていることを確認します。

> **注意：「destroy-data」を実行すると、すべてのソフトウェア設定がリセットされます。CIMC設定は変更されませんが、Admin、Clean、Dirtyインターフェイス設定の設定は削除されます。したがって、CIMCインターフェイスが無効になっているM5 ThreatGridデバイスでは、キーボードとモニタを使用してアプライアンスに物理的にアクセスし、インターフェイス設定とIPアドレスを再設定してから、この手順を実行します。**

> **注意**：システムから一度生成された暗号キーは取得できません。データ損失を防ぐために、キーを安全な場所にバックアップしてください