Die ThreatGrid-Appliance empfiehlt, eine erforderliche Zurücksetzung durchzuführen, bevor Version 3.0 installiert werden kann.

Inhalt

Einführung

In Vorbereitung auf die ThreatGrid Appliance 3.0-Version muss die jeweilige Appliance zurückgesetzt werden, um eine für die Veröffentlichung erforderliche Low-Level-Festplattenformatierung durchzuführen, die zur Zerstörung aller Daten auf dem Gerät führt.

Verfasst von T.J. Busch, Cisco TAC-Engineer

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ThreatGrid-Appliance

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Sie haben die Benachrichtigung über Ihre ThreatGrid-Appliance erhalten:

```
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
```

Lösung

> **Hinweis:** Es bestehen keine Produktionsauswirkungen bzw. kein Risiko von Datenverlusten auf dem Gerät, bis der Befehl zur Löschung der Daten auf dem Gerät ausgegeben wird und der Prozess beginnt

In Vorbereitung auf die ThreatGrid Appliance 3.0-Version muss die jeweilige Appliance zurückgesetzt werden, um eine für die Veröffentlichung erforderliche Low-Level-Festplattenformatierung durchzuführen, die zur Zerstörung aller Daten auf dem Gerät führt. Um Datenverluste auf dem Gerät zu vermeiden, müssen Sie die TGA so konfigurieren, dass sie eine Sicherung auf einer NFS-Freigabe durchführen und die Daten nach Abschluss des Formats wiederherstellen. Um dies abzuschließen, muss unbedingt sichergestellt werden, dass die Sicherung erfolgreich für mindestens 48 Stunden ausgeführt wird. Stellen Sie außerdem sicher, dass der Verschlüsselungsschlüssel gesichert ist, da dieser in die TGA importiert werden muss, um Daten wiederherzustellen.

> **Vorsicht: Wenn Sie "zerstören-data" verwenden, werden alle Softwarekonfigurationen zurückgesetzt. Die CIMC-Konfiguration wird nicht geändert, aber die Konfiguration für die "Admin"-, "Clean"- und "Dirty"-Schnittstellenkonfiguration wird entfernt. Daher sollten wir bei M5 ThreatGrid-Geräten, bei denen die CIMC-Schnittstelle deaktiviert ist, sicherstellen, dass der physische Zugriff auf die Appliance über eine Tastatur und einen Monitor möglich ist, um die Schnittstelleneinstellungen und IP-Adressen neu zu konfigurieren, bevor wir diesen Schritt durchführen.**

> **Vorsicht**: Verschlüsselungsschlüssel können nicht abgerufen werden, nachdem sie vom System generiert wurden. Sichern Sie den Schlüssel an einem sicheren Ort, um Datenverluste zu vermeiden.