ThreatGrid Appliance indique qu'une réinitialisation requise doit être effectuée avant l'installation de la version 3.0

Contenu

Introduction

En préparation de la version 3.0 de ThreatGrid Appliance, l'appliance spécifique doit être réinitialisée afin d'effectuer le formatage de disque de bas niveau requis pour la version, ce qui entraîne la destruction de toutes les données du périphérique.

Contribution de T.J. Occupé, ingénieur TAC Cisco.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance Cisco ThreatGrid

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Vous avez reçu la notification sur votre appliance ThreatGrid :

```
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
```

Solution

> **Note**: Il n'y a aucun impact sur la production/risque de perte de données sur le périphérique tant que la commande de destruction des données n'est pas exécutée sur le périphérique et que le processus n'est pas lancé

En préparation de la version 3.0 de ThreatGrid Appliance, l'appliance spécifique doit être réinitialisée afin d'effectuer le formatage de disque de bas niveau requis pour la version, ce qui entraîne la destruction de toutes les données du périphérique. Pour empêcher la perte de données sur le périphérique, vous devez configurer le TGA pour effectuer une sauvegarde sur un partage NFS, puis restaurer les données une fois le format terminé. Pour y parvenir, il est essentiel de s'assurer que la sauvegarde fonctionne correctement pendant au moins 48 heures. En outre, assurez-vous que la clé de chiffrement est sauvegardée car elle devra être importée dans le TGA afin de restaurer les données.

> **Attention : si vous détruisez les données, toutes les configurations logicielles seront réinitialisées. La configuration CIMC ne sera pas modifiée, mais la configuration de l'interface Admin, Clean et Dirty sera supprimée. Par conséquent, avec les périphériques M5 ThreatGrid dont l'interface CIMC est désactivée, nous devons nous assurer que nous avons un accès physique à l'appliance à l'aide d'un clavier et d'un moniteur pour reconfigurer les paramètres d'interface et les adresses IP avant de tenter cette étape.**

> **Attention** : les clés de chiffrement ne peuvent pas être récupérées une fois générées à partir du système. Veiller à sauvegarder la clé dans un emplacement sûr pour éviter la perte de données