ThreatGrid Appliance recomienda que se realice un reinicio necesario antes de poder instalar la versión 3.0

Contenido

Introducción

Como preparación para la versión 3.0 de ThreatGrid Appliance, el dispositivo específico debe restablecerse para realizar el formato de disco de bajo nivel necesario para la versión, lo que resulta en la destrucción de todos los datos del dispositivo.

Contribuido por T.J. Busch, ingeniero del TAC de Cisco.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo Cisco ThreatGrid

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Ha recibido el aviso en su dispositivo 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
```

Solución

> **Nota:** No hay impacto de producción/riesgo de pérdida de datos en el dispositivo hasta que se ejecuta el comando de destrucción de datos en el dispositivo y el proceso comienza

Como preparación para la versión 3.0 de ThreatGrid Appliance, el dispositivo específico debe restablecerse para realizar el formato de disco de bajo nivel necesario para la versión, lo que resulta en la destrucción de todos los datos del dispositivo. Para evitar la pérdida de datos en el dispositivo, debe configurar el TGA para realizar una copia de seguridad en un recurso compartido NFS y, a continuación, restaurar los datos una vez que se complete el formato. Para completar esto, es vital asegurarse de que la copia de seguridad se ejecute correctamente durante al menos 48 horas. Además, asegúrese de que se realice una copia de seguridad de la clave de cifrado, ya que será necesario importarla al TGA para restaurar los datos.

> **Precaución: si realiza "destrucción de datos", se restablecerán todas las configuraciones de software. La configuración de CIMC no se modificará pero se eliminará la configuración de la interfaz Admin, Clean y Dirty. Por lo tanto, con los dispositivos M5 ThreatGrid que tienen la interfaz CIMC desactivada, debemos asegurarnos de que tenemos acceso físico al dispositivo mediante un teclado y un monitor para volver a configurar la configuración de la interfaz y las direcciones IP antes de intentar este paso.**

> **Precaución**: las claves de cifrado no se pueden recuperar una vez generadas desde el sistema. Asegúrese de realizar una copia de seguridad de la clave en una ubicación segura para evitar la pérdida de datos