Appliance ThreatGrid: si avvisa che è necessario completare un ripristino prima di poter installare la versione 3.0

Sommario

Introduzione

In preparazione della release 3.0 di ThreatGrid, è necessario reimpostare l'accessorio specifico per eseguire la formattazione del disco di basso livello richiesta per la release, in modo da distruggere tutti i dati del dispositivo.

Contributo di T.J. Busch, Cisco TAC Engineer.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Appliance Cisco ThreatGrid

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

L'avviso è stato inviato all'utente sull'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
```

Soluzione

> **Nota:** Non vi è alcun impatto sulla produzione/rischio di perdita di dati sul dispositivo finché il comando di eliminazione dei dati non viene emesso sul dispositivo e il processo non inizia

In preparazione della release 3.0 di ThreatGrid, è necessario reimpostare l'accessorio specifico per eseguire la formattazione del disco di basso livello richiesta per la release, in modo da distruggere tutti i dati del dispositivo. Per evitare la perdita di dati nel dispositivo, è necessario configurare la TGA per il backup in una condivisione NFS e quindi ripristinare i dati una volta completato il formato. A tale scopo, è fondamentale garantire che il backup venga eseguito correttamente per almeno 48 ore. Inoltre, assicurarsi di eseguire il backup della chiave di crittografia, in quanto sarà necessario importarla nella TGA per ripristinare i dati.

> **Attenzione: se si esegue la "distruzione dei dati", tutte le configurazioni software verranno ripristinate. La configurazione CIMC non verrà modificata, ma quella dell'interfaccia Admin, Clean, Dirty verrà rimossa. Pertanto, se i dispositivi M5 ThreatGrid hanno l'interfaccia CIMC disabilitata, prima di provare a eseguire questa operazione è necessario verificare di disporre di accesso fisico all'accessorio tramite tastiera e monitor per riconfigurare le impostazioni dell'interfaccia e gli indirizzi IP.**

> **Attenzione**: le chiavi di crittografia non possono essere recuperate dopo essere state generate dal sistema. Eseguire il backup della chiave in un percorso sicuro per evitare la perdita di dati