ThreatGrid-applicatie adviseert dat een vereiste reset moet zijn voltooid voordat versie 3.0 kan worden geïnstalleerd

Inhoud

Inleiding

Ter voorbereiding van de release van ThreatGrid-applicatie 3.0 dient het specifieke apparaat opnieuw ingesteld te worden om een lage diskopmaak te kunnen uitvoeren die nodig is voor de release, resulterend in alle gegevens over het apparaat die vernietigd worden.

Bijgedragen door T.J. Busch, Cisco TAC Engineer.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Threat Grid-applicatie

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

U hebt het bericht op uw ThreatGrid-applicatie ontvangen:

```
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
```

Oplossing

> **Opmerking:** Er is geen effect/risico van gegevensverlies op het apparaat totdat de opdracht van de vernietigingsgegevens op het apparaat is afgegeven en het proces begint

Ter voorbereiding van de release van ThreatGrid-applicatie 3.0 dient het specifieke apparaat opnieuw ingesteld te worden om een lage diskopmaak te kunnen uitvoeren die nodig is voor de release, resulterend in alle gegevens over het apparaat die vernietigd worden. Om gegevensverlies op het apparaat te voorkomen, dient u de TGA te configureren om back-up te maken op een NFS-aandeel en vervolgens de gegevens te herstellen zodra de indeling is voltooid. Om dit te voltooien is het van cruciaal belang om ervoor te zorgen dat de back-up gedurende ten minste 48 uur succesvol loopt. Zorg er bovendien voor dat er een back-up is gemaakt van de encryptiesleutel, aangezien deze naar de TGA moet worden geïmporteerd om de gegevens te herstellen.

> **Voorzichtig: als u 'vernietigende gegevens' doet, worden alle software configuraties hersteld. CIMC-configuratie kan niet worden aangepast, maar de configuratie van de Admin-, Schone of vieze interface-configuratie wordt verwijderd. Daarom moeten we, met M5 ThreatGrid-apparaten met een CIMC-interface uitgeschakeld, ervoor zorgen dat we fysieke toegang tot het apparaat hebben via een toetsenbord en een monitor om de interfaceinstellingen en IP-adressen opnieuw te configureren voordat we deze stap proberen.**

> **Waarschuwing**: encryptietoetsen kunnen niet worden opgeroepen zodra ze uit het systeem zijn gegenereerd. Zorg ervoor dat u een back-up maakt van de toets naar een veilige locatie om gegevensverlies te voorkomen