ThreatGrid Appliance is advising a required reset needs to be completed before version 3.0 can be installed

Contents

Introduction

In preparation for the ThreatGrid Appliance 3.0 release, the specific appliance requires to be reset in order to perform low-level disk formatting required for the release resulting in all data on the device being destroyed.

Contributed by T.J. Busch, Cisco TAC Engineer.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco ThreatGrid Appliance

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Problem

You received the notice on your ThreatGrid Appliance:

```
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**: There is no production impact/ risk of data loss on the device until the destroy data command is issued on the device and the process begins

In preparation for the ThreatGrid Appliance 3.0 release, the specific appliance requires to be reset in order to perform low-level disk formatting required for the release resulting in all data on the device being destroyed. To prevent data loss to the device, you must configure the TGA to backup to an NFS share and then restore the data once the format is completed. In order to complete this, is vital to ensure that the backup successfully runs for at least 48 hours. Additionally, ensure the encryption key is backed up as this will need to be imported to the TGA in order to restore data.

> **Caution: if you do "destroy-data" all software configurations will be reset. CIMC Configuration would not be modified but the configuration on Admin, Clean, Dirty interface configuration will get removed. Therefore, with M5 ThreatGrid devices that have CIMC interface disabled, we should make sure that we have physical access to the appliance using a keyboard and a monitor to re-configure the Interface settings and IP Addresses before attempting this step.**

> **Caution**: Encryption Keys can not be retrieved once generated from the system. Ensure to back up the key to a safe location to prevent data loss