Secure Malware Analytics (Formerly Threat Grid) Appliance is advising a required reset needs to be completed before version 3.0 can be installed

Contents

Introduction

In preparation for the Secure Malware Analytics (SMA) Appliance 3.0 release, the SMA appliances shipped with software version 2.7 must be reset (destroy-data) to perform the low-level disk formatting required for the release.

SMA appliances shipped with a version newer than 2.7, or those that have undergone a reset (destroy-data) at least once since the upgrade from 2.7, do not require another reset (destroy-data) to install the 3.0 release.

Prerequisites

Cisco recommends that you know these topics:

- Cisco Secure Malware Analytics Appliance

Components Used

The information in this document is based on these software and conditions:

- Cisco Secure Malware Analytics Appliance shipped with version 2.7 (2019.02.20190601T155353.srchash.b67f91c65917.rel)
- Cisco Secure Malware Analytics Appliance has not been reset (destroy-data) since 2.7

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.

Background information

The 3.0 software release will make incompatible changes to how content is stored on-disk, to avoid data loss in appliances that were initially installed with version 2.7 and have not been reset (destroy-data), content must be backed up and restored after reset (destroy-data) is done.

Appliances shipped with later versions than 2.7 are not affected.

Problem

You received the notice on your SMA Appliance:

```
This appliance was initially installed with a software release prior to 2.7.0, and has not had its data
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 inst
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 is mandatory before installing the appliance 3.0 release.
To prevent data loss, verify the backup system has run successfully for 48 hours without any failure re
and ensure you have downloaded the backup encryption key before proceeding.

Contact customer support for any questions.
```

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 SMA 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, follow the instructions below:

1. Configure the SMA appliance to **backup** to an NFS share. It is vital to ensure that the backup successfully runs for at least 48 hours prior to destroy-data process is run. Useful links - Secure Malware Analytics (Formerly Threat Grid) Appliance Backup FAQ v2.2.4
2. Ensure the encryption key is backed up as this will need to be imported to the SMA appliance in order to restore data.
3. Once the backup is confirmed, run `destroy-data` command to reset the appliance. See SMA Appliance Data Reset
4. Once data has been reset and initial configurations (Network, SSL certificates etc) is complete **Restore** the data from NFS .

Caution: if you do "destroy-data" all software configurations will be reset. CIMC Configuration will remain unchanged, but the configurations on Admin, Clean, Dirty interface will be removed. For M5 SMA devices with a disabled CIMC interface, ensure physical access to the appliance with a keyboard and monitor is available before performing the destroy-data operation to reconfigure interface settings and IP addresses.

Caution:Encryption keys are irretrievable after generation. Failure to back up the key will result in permanent data loss. Ensure the key is securely stored in a safe location.