Configure ThreatGrid Appliance for Cluster Operations

Contents

Introduction

This document describes how to configure the ThreatGrid Appliance for cluster operations.

Contributed to by TJ Busch, Cisco TAC Engineer.

Prerequisites

Requirements

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.

Background Information

ThreatGrid Appliance contains the functionality to cluster multiple TG Appliances together in order to increase the number of concurrent samples that can be processed at a single time. Note that TGA does not currently support any sort of High Availability with the current implementation of the clustering feature.

> **Warning**: Nodes must be free from any submitted samples. The command **destroy-data** from the TGSH console is recommended

Configuration

Initial Cluster Node

Step 1. Setup the Threat Grid node network interfaces as defined in the [Threat Grid Appliance Getting Started Guide](#) ensuring to enable/configure all required settings.

> **Warning**: All Cluster Interfaces must be connected to the same physical Layer 2 switch on the same VLAN. Layer 3 Routing or Layer 2 extension technologies are not supported.

EULA

Step 1. Point to the Admin interface DNS/IP address configured in step one using HTTPS

Step 2. Enter the initial Admin Password that you copied from the TGSH Dialog and Click **Login**. The Change Password page open

Step 3. Enter the password from the TGSH Dialog into the Old Password field.

Step 4. Enter and confirm a new password

Step 5. Click **Change Password**

Step 6. Review the End User License Agreement.

Step 7. Scroll down to the end, and Click **I HAVE READ AND AGREE**

License Installation

Step 1. Click on the **License** tab in the left column.

Step 2. Under Upload New License, Click **Choose File**, Select the provided license file from your file manager.

Step 3. Enter the license password you were given into the Passphrase field

Step 4. Click **Upload.** Updated License info appears in the previous blank fields.

Step 5. Click **Next** to continue

Configure NFS

Step 1. Configure the options as recommended:

- Host - The NFSv4 host server. Using the IP address is recommended over the hostname
- Path - The absolute path to the location on the NFS host server under which files are stored
- Opts - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4
- Status - Select Enabled from the dropdown (Pending Key)

Step 2. Select **Next**

Step 3. Under FS Encryption Password File, Click **Generate**

Step 4. After generating, Click **Download**

> **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

Step 5. Click **Activate**

Step 6. Click **Next**

Cluster Settings

Step 1. Under Clustering Status, Select **Start Cluster**

Step 2. The status changes from **Standalone (unsaved)** to **Clustered**

Step 3. Click **Next**

Review and Install

> **Warning**: Failure to allow the initial Cluster node to complete install before finish results in errors that require a restart of the process. Once the initial node is configured you can join multiple nodes at once to the primary node.

Step 1. Click **Start Install**

Step 2. After 20-30 minutes, the node prompts to reboot. Click **Reboot**

Step 3. After 20-30 minutes, the node becomes active. You can proceed with adding nodes

Add Node(s) to Existing Cluster

EULA

Step 1. Point to the Admin interface DNS/IP address configured in step one using HTTPS

Step 2. Enter the initial Admin Password that you copied from the TGSH Dialog and Click **Login**. The Change Password page open

Step 3. Enter the password from the TGSH Dialog into the Old Password field.

Step 4. Enter and confirm a new password

Step 5. Click **Change Password**

Step 6. Review the End User License Agreement.

Step 7. Scroll down to the end, and Click **I HAVE READ AND AGREE**

License Installation

Step 1. Click on the **License** tab in the left column.

Step 2. Under Upload New License, click **Choose File**, Select the provided license file from your file manager.

Step 3. Enter the license password you were given into the Passphrase field

Step 4. Click **Upload.** Updated License info appears in the previous blank fields.

Step 5. Click **Next** to continue

Configure NFS

Step 1. Configure the options as recommended:

- Host - The NFSv4 host server. Using the IP address is recommended over the hostname
- Path - The absolute path to the location on the NFS host server under which files are stored
- Opts - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4
- Status - Select Enabled from the dropdown (Pending Key)

Step 2. Select **Next**

Step 3. Under FS Encryption Password File, Click **Choose file** and navigate to your saved primary node key.

Step 4. Click **Upload**

Step 5. Click **Activate**

Step 6. Click **Next**

Cluster Settings

>   **Note**: The TGA initial node must be reachable and responsive over the cluster interface for additional nodes to join the cluster.

Step 1. Under Clustering Status, Select **Join Cluster**

Step 2. The status changes from **Standalone (unsaved)** to **Clustered**

Step 3. Click **Next**

Review and Install

Step 1. Click **Start Install**

Step 2. After 20-30 minutes, the node prompts to reboot. Click **Reboot**

Step 3. After 20-30 minutes, the node becomes active and shows joined to the cluster