Understand Best Practices to Migrate Hardware ESA/SMA to Virtual ESA/SMA

Contents

Introduction

This document describes the best practices regarding deployment, migration, and configuration from hardware ESA/SMA to Virtual ESA/SMA.

Essential Steps

Step 1. Download the Virtual ESA Image and Deploy the VM

It is recommended to have a virtual Secure Email Gateway (ESA)/Security Management Appliance (SMA) running on the same AsyncOS version as the hardware before you can migrate the configuration. You can choose the AsyncOS release closest to the version running on your appliance and upgrade it after that, if required, or download the latest version of AsyncOS.

Deployments on these platforms are supported – Microsoft Hyper-V, Keyboard/Video/Mouse (KVM), and VMWare ESXi. Check the installation guide for more details: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_V

You can download the virtual image from the link: https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0.

Step 2. Obtain Licenses for the Virtual ESA/SMA

In order to be able to upgrade the virtual ESA/SMA, first you must install its licenses – you can share the existing licenses from your hardware with the new virtual ESA (both ESAs can run together).

For Traditional licenses, once the physical license has been successfully shared for the vESA/vSMA, and you received your license, open up the .XML file you received with NotePad++ or WordPad. Select all, and then copy/paste via the vESA/vSMA CLI using the loadlicense command. Refer to the link for more details: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html.

For Smart licenses, add the new vESA/vSMA in the smart account, once the token is generated, register the devices as per the process mentioned in the article: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-overview-and-best-practi.html.

Step 3. Upgrade the Virtual ESA/SMA to the Exact AsyncOS Version of the Hardware ESA/SMA (If Required)

The hardware and virtual appliance must be on the same version prior to the migration. You can check the compatibility matrix for the SMA and ESA on the link mentioned in order to upgrade the ESA to the proper version: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html.

Step 4. Migrate the Existing Configuration from the Hardware ESA/SMA to the Virtual ESA/SMA

The virtual ESA/SMA can be configured in these ways:

- Configure the devices from scratch if the existing hardware is reaching End-Of-Life (EOL)/End-Of-Support (EOS) or Upgraded vESA/SMA image is installed or if multiple devices must be configured.
- If the hardware device is already in the cluster, add the new vESA/vSMA to the cluster. The new devices obtain a copy of your existing configuration from the cluster.
- If the hardware device is a standalone device, enable cluster configuration and add the new virtual ESA/SMA to the cluster in order to obtain a copy of the existing configuration.

Note: Once the virtual ESA/SMA obtains the current configuration, you can choose to disconnect the devices from the cluster or keep them as-is based on requirement. The hardware device can be removed from the cluster configuration and decommissioned.

Step 5. Correct the Updated Server on the Virtual ESA/SMA

The virtual and hardware ESA/SMA use different upgrade servers and after migrating the configuration, the server changes. In order to be able to further upgrade your vESA/vSMA, you can correct the server via the vESA/vSMA CLI with these steps:

- Run the command `updateconfig`, and then the subcommand `dynamichost`.
- Change server to `update-manifests.sco.cisco.com:443`.
- Commit the changes.

For additional FAQs regarding migration, refer to the link: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdf.