Revert ESA and SMA to Original Configuration

Contents

Introduction

Key Considerations

- Reversion is Destructive
- Preparation for Possible Reversion

Solution

Hardware Appliances (ESA / SMA)

Virtual Appliances (ESA / SMA)

- VMware ESXi
- Microsoft Hyper-V
- KVM
- Nutanix

Public Cloud Deployment

- Azure
- AWS
- GCP

Introduction

This document describes the procedure to revert and redeploy an Email Security Appliance (ESA) or Security Management Appliance (SMA).



Caution: A reversion should only be performed when absolutely necessary, as it will erase all data from the device(s). Please confirm that this action is required before proceeding.

Key Considerations

Reversion is Destructive

Reverting the device will result in significant data loss:

- All messages in the work queue and delivery queue will be deleted.
- All reporting data and log files will be permanently removed.
- All configurations, except for feature key data, will be lost.
- All databases and message tracking data will be erased.
- All Spam Quarantine messages and end-user safelist/blocklist data will be deleted.
- Only network settings will be preserved.

Preparation for Possible Reversion

To ensure you can recover essential information, if possible, Cisco recommends the following best practices prior to executing a revert:

1. Save the XML configuration file to an external location (ensure passwords are unmasked).
2. If you use the Safelist/Blocklist feature, export these lists to an external location.
3. Suspend all listeners.
4. Drain both the mail and delivery queues.
5. Export the Spam Quarantine safelist/blocklist database to another machine, if applicable.

Solution

Hardware Appliances (ESA / SMA)

Steps to clean and revert a physical appliance.

1. SSH to the appliance and run **version** and make note of the active version running on the appliance.

2. Run **Revert**, select a version of code that is older than **From #1** and type **Y**.

```
sma.example.com> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine messages
  and end-user safelist/blocklist data

Only the network settings (except the 'allow_arp_multicast' configuration variable)
will be retained. If you need to establish connectivity to a Microsoft Network Load Balancer,
you must configure the 'allow_arp_multicast' configuration variable after the revert process
is complete.

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.

    Available versions
    ==================
 1. 16.0.1-010
 2. 16.0.2-088
 3. 16.0.3-016
Please select an AsyncOS version [2]: 1
Do you want to continue? [N]> y
Are you sure you want to continue? [N]> y
```

Warning: This procedure will wipe the configuration, data and history of upgrades on the appliance

4. Allow the machine to complete revert and it is expected to take approximately 30 minutes to complete.

3. Once revert is complete and appliance is up, access the command line again and execute **Reload** via **Diagnostic**.

```
esa.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[]> reload

This command will remove all user settings and reset the entire device.

If this is a Virtual Appliance, all feature keys will be removed, and the license must be reapplied. Th
Are you sure you want to continue? [N]> y
Are you *really* sure you want to continue? [N]> y
Do you want to wipe also? Warning: This action is recommended if the device is being sanitized before s
Sometimes, it may take several minutes to complete the process because it follows the NIST Purge standa
Reverting to "virtualimage" preconfigure install mode.
```

Virtual Appliances (ESA / SMA)

For information on hardware requirements, supported hypervisor platform please refer https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Secur

VMware ESXi

1. Download the virtual appliance image and MD5 hash from Cisco.
2. Unzip the .zip file for the virtual appliance in its own directory; for example, C:\vESA\C100V.
3. Open the VMware vSphere Client on your local machine.
4. Select the ESXi host or cluster to which you want to deploy the virtual appliance.
5. Choose **File > Deploy OVF template**.
6. Enter the path to the OVF file in the directory you created and click **Next**. Complete the wizard.
7. If DHCP is disabled, set up the appliance on your network. Install the license file.
8. Log in to the web UI of your appliance and configure the appliance software.

Microsoft Hyper-V

1. Download the virtual appliance image and MD5 hash from Cisco.

2. Open Hyper-V Manager, use the "New Virtual Machine Wizard" to create a new virtual machine.

3. Assign the recommended hardware resources. (refer to virtual installation guide)

4. Attach the downloaded virtual appliance image as the virtual hard disk. Complete the wizard and start the virtual machine.

5. If DHCP is disabled, set up the appliance on your network. Install the license file.

6. Log in to the web UI of your appliance and configure the appliance software.

KVM

Deploy virtual machine using Virtual Machine Manager. Download the virtual appliance image and MD5 hash from Cisco,

1. Launch the virt-manager application. Select **New**.

2. Enter a unique name for your virtual appliance. Select **Import existing image**.

3. Select **Forward**, enter options OS Type: **UNIX**, version: **FreeBSD 13**.

4. Browse and select the virtual appliance image that was downloaded and select **Forward**.

5. Enter RAM and CPU values for the virtual appliance model that needs to be deployed. (refer to virtual installation guide)

6. Select **Forward**, select the **Customize** check box and select **Finish**.

7. Configure the disk drive. In the left pane, select the drive and under **Advanced Options**, Disk bus: **Virtio**, Storage format: **qcow2** and select **Apply**.

8. Configure the network device for the management interface. In the left pane, select a NIC and selection options Source Device: Your management Vlan, Device Model: virtIO, Source mode: VEPA, select **Apply**.

9. Configure network devices for additional interfaces, repeat step 8 for each interface added to the virtual machine.

10. Select **Begin Installation**.

Nutanix

1. Download the virtual appliance image and MD5 hash from Cisco.

2. Access Nutanix Prism, untar the virtual appliance **qcow2** image and upload it to your storage pool.

3. Click the Hamburger icon in the top left corner of the Nutanix Prism dashboard, select Compute and Storage > VM from the left navigation pane.

4. Click the Create VM button, enter the details to configure the VM and click Next.

5. Configure hardware resources based on the model (refer to virtual installation guide)

6. Click the **Attach Disk** button under **Disks** and select, **Clone from Image** from the **Operation** drop-down list and uploaded **qcow2** image from the **Image** drop-down list.

7. Click the **Attach to Subnet** button under **Networks** and configure the network interface settings.

8. Complete the wizard to deploy the Virtual Appliance on Nutanix Prism.

Public Cloud Deployment

For information and procedure to deployment ESA & SMA on public cloud please refer https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtual_A

Azure

1. Create the requirement components.

2. Obtain the VM image.

3. Configiure Access Control - Identity and Access Management (IAM)

4. Log in and create the VM.

Refer pages 4 to 18 from the deployment guide for public clouds for detailed procdeure to deploy the virtual machine on Azure.

AWS

1. Contact Cisco TAC to obtain the AMI ID.

2. Open the Amazon EC2 console.

3. Choose AMIs in the navigation pane.

4. Choose **Public Images** in the first filter.

5. In the search bar, enter the "build number" and "model" according to the virtual appliance model required.

Refer pages 19 to 29 from the deployment guide for public clouds for detailed procdeure to deploy the virtual machine on AWS.

GCP

1. Prepare the environment and configure the virtual machine.

2. Choose OS and Storage.

3. Configure the network, firewall, and network interface.

4. Configure Virtual Machine.

Refer pages 30 to 34 from the deployment guide for public clouds for detailed procdeure to deploy the virtual machine on GCP.