Upgrade Process for Secure Email Gateway

Contents

Introduction

This document describes steps associated with the AsyncOS upgrade process for the Cisco Secure Email Gateway (SEG) aka Cisco Email Security Appliance.

Requirements

- Ensure the appliance RAID status is READY or OPTIMAL in the System Status output. Do not initiate an upgrade on an appliance with a RAID status of DEGRADED. Contact Cisco TAC to initiate a Return Material Authorization (RMA) case for your appliance.
- Verify if the Email Security appliance (ESA) is a stand-alone appliance or in a clustered environment. If clustered, be sure to properly review the *Cluster Upgrade* section of this document.
- Ensure there is Internet connectivity from the ESA on ports 80 and 443 with no packet inspections.
- A functional DNS server(s) is required.

Compatibility Between ESA/SMA

Review the compatibility of the ESA and SMA systems before you upgrade. Older versions of AsyncOS for Email Security can require more than one upgrade to get to the latest version. For confirmation of the upgrade path and appliance provisioning, contact Cisco TAC.

Prepare to Upgrade

1. Save the XML configuration file off-box. If you need to revert to the pre-upgrade release for any reason, you can use this file to import the previous configuration.
2. If you use the Safelist/Blocklist feature, export the list off-box.
3. Suspend all listeners. If you perform the upgrade from the CLI, use the suspendlistener command. If you perform the upgrade from the GUI, listener suspension occurs automatically.
4. Wait for the queue to empty. You can use the workqueue command to view the number of messages in the work queue or the rate command in the CLI to monitor the message throughput on your appliance.

Download and Install the Upgrade

As of AsyncOS for Email Security version 8.0, the upgrade options are updated to now include

DOWNLOADINSTALL in addition to **DOWNLOAD**. This gives the administrator flexibility to download and install in a single operation, or download in the background and install later.

```
(Machine host1.example.com)> upgrade


Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> download

Upgrades available.
1. AsyncOS 14.2.0 build 616 upgrade For Email, 2022-05-27,release available as General Deployment
2. AsyncOS 14.2.0 build 620 upgrade For Email, 2022-07-05,release available as General Deployment
[2]>
```

Refer to the [User Guide](#) for complete information.

Upgrade on the CLI

1. Enter the status command and make sure the listener is suspended. You can see "System status: Receiving suspended".
2. Enter the upgrade command.
3. Choose an option for **DOWNLOADINSTALL** or **DOWNLOAD**.
4. Choose the appropriate number associated with the upgrade version desired.
5. Complete the needed questions to save the current configuration and approve the reboot when the upgrade is applied.
6. Post-upgrade, log in to the CLI, and enter resume to resume the listeners and ensure operation. Enter the status command and confirm "System status: Online".

Upgrade via the GUI

1. Choose **System Administration > System Upgrade**.
2. Click **Upgrade Options...**
3. Choose an option for Download and install or Download.
4. Click and highlight the upgrade version desired.
5. Choose the appropriate options for Upgrade Preparation.
6. **Proceed**, to begin the upgrade and display the progress bar for your monitoring.
7. Post-upgrade, log in to the CLI and enter resume to resume the listeners and ensure operation: Choose **System Administration > Shutdown/Suspend > Resume (Check All)**.
8. In the Mail Operations section, choose **Commit**.

Cluster Upgrade

ESAs in a cluster would use the same upgrade process from the CLI or the GUI as in the previous sections, with the one exception that there would be a prompt to disconnect devices off the cluster.

Note: You can perform the upgrade with the CLI or the GUI, but the reconnect clusterconfig commands are only available via the CLI. This document describes how to upgrade the machines via the CLI.
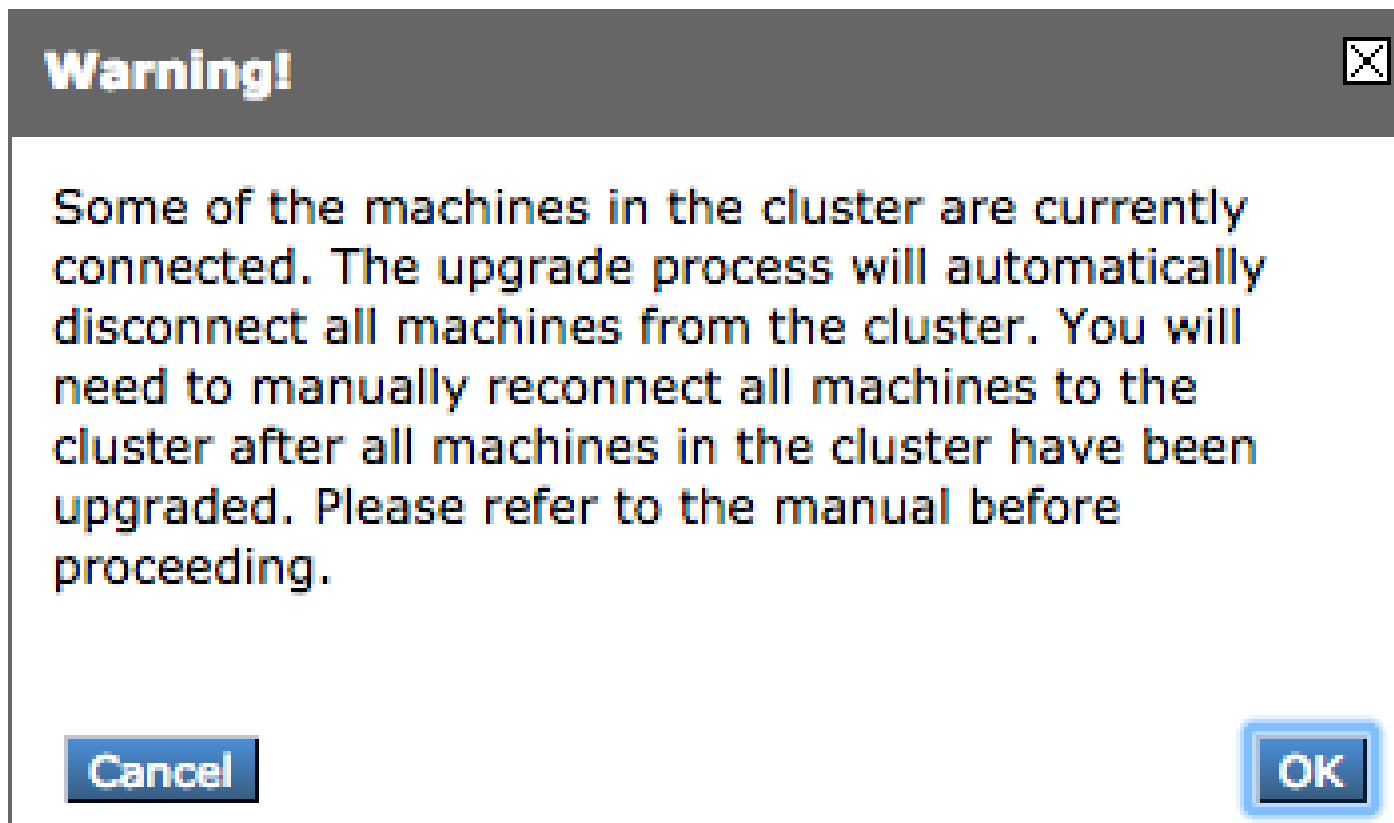

Example as seen from CLI:

```
(Cluster my_cluster)> upgrade

This command is restricted to run in machine mode of the machine you are logged in to.
 Do you want to switch to "Machine applianceA.local" mode? [Y]> y
```

Example as seen from GUI:

Warning! ⊠

Some of the machines in the cluster are currently connected. The upgrade process will automatically disconnect all machines from the cluster. You will need to manually reconnect all machines to the cluster after all machines in the cluster have been upgraded. Please refer to the manual before proceeding.

Cancel   OK

Note: This is an administrative disconnect only. This would stop any sync attempts of the configuration across the cluster from or to the disconnected appliances. This does not remove or alter the appliance configuration.

Complete these steps to upgrade ESAs that run in a cluster via the CLI:

1. Enter the upgrade command into the CLI to upgrade AsyncOS to a later version. When you are asked whether you wish to disconnect the cluster, respond with the letter Y to proceed:

   <#root>

   ```
   (Machine host1.example.com)>
   ```

   upgrade

   ```
   You must disconnect all machines in the cluster in order to upgrade them. Do you wish
   to disconnect all machines in the cluster now? [Y]>
   ```

   Y

2. Use all of the upgrade prompts (*reboot* prompt included).

3. After all of the machines in the cluster are upgraded and rebooted, log onto one of the machines in the cluster via the CLI and enter the `clusterconfig` command. Reconnect them at the cluster level to allow configuration sync and resume cluster operation.
4. Respond `Yes` to reconnect. It is not necessary to *commit*.

```
Choose the machine to reattach to the cluster. Separate multiple machines with commas
or specify a range with a dash.

1. host2.example.com (group Main)
2. host3.example.com (group Main)
3. host4.example.com (group Main)

[1]> 1-3
```

5. Issue the command `connstatus` to confirm all devices are in the cluster. Also, issue the command **clustercheck** to confirm there is no inconsistency.

Cluster upgrade recommendations are:

- Do not reconnect ESAs to the cluster until ALL appliances are upgraded to a matched version.
- If needed, once one ESA has completed an upgrade, resume the listener, if previously suspended, and allow it to function as a stand-alone appliance.
- Do not make configuration changes or modifications when ESAs are disconnected from a cluster to help avoid configuration inconsistencies when reconnected to cluster-level post-upgrade.
- Once ALL appliances are upgraded to the same version, reconnect them at the cluster level to allow configuration sync and resume cluster operation.

Post Checks:

- If the appliances are managed by the SMA then:
  ◦ Navigate to **Management Appliance > Centralized Services > Security Appliances** and make sure all services are up and the connection shows "**Established**".
  ◦ Navigate to **Email > Message Tracking > Message Tracking Data Availability** and check if the status shows **OK** for all ESAs.
  ◦ On each appliance, enter the `status` command and look for it to show as online.
  ◦ Enter the `displayalerts` command and check for any new alerts seen after the upgrade.
  ◦ If in a cluster, then the **clustercheck** command must not show any inconsistencies, and the **connstatus** command must show appliances as connected without errors.
  ◦ To verify the mail flow, enter the **tail mail_logs** command into the CLI.

Troubleshoot

1. **tail updater_logs** and **tail upgrade_logs** can also give information if there is an issue with the upgrade.
2. If there is an issue when you download the image or when you update the antispam or antivirus it is probably because the processes are not able to reach out and update the service engine or rulesets. Use the steps provided in [vESA Is Not Able to Download and Apply Updates for Antispam or Antivirus](#).
3. If the upgrade fails due to network interruptions, similar errors can be seen during the upgrade process

output:

```
Reinstalling AsyncOS... 66% 01:05ETA.
/usr/local/share/doc/jpeg/libjpeg.doc: Premature end of gzip compressed data&colon;
 Input/output error
tar: Error exit delayed from previous errors.
Upgrade failure.
```

This is typically due to a network interruption that can have occurred during the transmission of data between the ESA and the update servers. Investigate any network firewall logs or monitor packet traffic from the ESA to update servers.

If needed, refer to ESA Packet Capture Procedures to enable packet capture on the ESA, and then re-attempt the upgrade process.

>   **Note**: Firewalls need to allow idle connections to stay active, especially for the upgrade process.

For strict network firewalls that require static upgrade servers, refer to Content Security Appliance Upgrades or Updates with a Static Server for how to configure static update and upgrade servers.

For hardware appliances, test connections to these dynamic servers:

- telnet updates.ironport.com 80
- telnet downloads.ironport.com 80

For virtual appliances you must use these dynamic servers:

- telnet update-manifests.sco.cisco.com 443
- telnet updates.ironport.com 80
- telnet downloads.ironport.com 80

Refer to the User Guide for complete firewall information and port requirements.

Related Information

- **Compatibility Matrix for Cisco Content Security Management Appliances**
- **ESA Upgrade Procedures**
- **ESA Packet Capture Procedures**
- **Content Security Appliance Upgrades or Updates with a Static Server**
- **Technical Support & Documentation - Cisco Systems**