Validate and Troubleshoot an AsyncOS Upgrade on ESA

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Compatibility Between ESA and SMA

Preparing and Completing an AsyncOS Upgrade

Perform Post-Upgrade Checks

Troubleshoot Upgrade Issues

Related Information

Introduction

This document describes post-upgrade steps to validate a successful AsyncOS upgrade and troubleshoot common issues on the Cisco Secure Email Gateway (SEG).

Prerequisites

Note: Cisco Secure Email Gateway was formerly know as Email Security Appliance.

Requirements

- The appliance RAID status must be READY or OPTIMAL in the System Status output; do not initiate an upgrade if the status is DEGRADED and contact Cisco TAC for a Return Material Authorization (RMA).
- Confirm no significant errors exist, specifically network connectivity or DNS issues, by reviewing system alerts in the GUI under **System Administration > Alerts** or by running the **displayalerts** command in the CLI.
- Identify if the ESA operates as a stand-alone appliance or in a cluster and review the Cluster Upgrade section of this document for clustered environments.
- Verify a functional DNS server configuration and ensure internet connectivity on **ports 80 and 443** without packet inspection.

Note: When firewall access is based on Fully Qualified Domain Names (FQDNs), ensure both Email Security Appliance (ESA) and firewall use the same DNS server for correct hostname-to-IP mapping. The upgrade and update URLs including downloads.ironport.com, upgrades.ironport.com, updates.ironport.com, and manifest URLs are hosted on the Akamai CDN network.

Caution: Cisco Smart Software Licensing usage is mandatory starting with AsyncOS 15.5.x and all future versions for Cisco Secure Email Gateway.

Components Used

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.

Compatibility Between ESA and SMA

You must review the compatibility matrix between ESA and SMA before starting the upgrade. Some versions require multiple upgrades to reach the latest release. For upgrade path confirmation and appliance provisioning, contact Cisco TAC.

Preparing and Completing an AsyncOS Upgrade

For AsyncOS upgrade requirements and steps, please refer to the User Guide. Please familiarize yourself with these steps before proceeding.

Perform Post-Upgrade Checks

- If appliances are managed by SMA:
  - Navigate to **Management Appliance > Centralized Services > Security Appliances** to ensure all services are up.
  - Check **Email > Message Tracking > Message Tracking Data Availability** for **OK** status on all ESAs.
- On each appliance, run **status** and confirm **Online** status.
- Run **displayalerts** to view any new alerts after the upgrade.
- In a cluster, **clustercheck** must show no inconsistencies and **connstatus** must show all appliances connected.
- To verify mail flow, use the CLI command **tail mail_logs** to watch real-time processing.

Troubleshoot Upgrade Issues

1. Run **tail updater_logs** and **tail upgrade_logs** from the CLI for upgrade issue details.
2. If the image download or antispam/antivirus update fails, check network connectivity to update servers.
3. If the upgrade fails due to network interruptions, errors can appear:

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

1. This typically results from network interruptions during data transmission between ESA and update servers.
2. Check firewall logs or monitor packet traffic for issues.
3. To capture network packets on the ESA, use the packet capture tool in the GUI or CLI.



Note: Firewalls must allow idle connections to remain active during the upgrade process.

For hardware appliances, test connectivity to dynamic servers using these commands:

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

For virtual appliances, test connectivity to these servers using these commands:

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

Refer to the User Guide for firewall and port requirements.

Related Information

- Compatibility Matrix for Cisco Content Security Management Appliances
- ESA Packet Capture Procedures
- Content Security Appliance Upgrades or Updates with a Static Server
- Understand Smart Licensing Overview and Best Practices for Email and Web Security