Troubleshoot Secure Email "Update Failed" Alerts

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Identify

Resolution

- Network Connectivity
- Manifest Server Usage

Related Information

Introduction

This document describes identifying, troubleshooting, and resolving alerts pertaining to update failures.

Prerequisites

Requirements

Cisco recommends that you have a basic understanding of the Cisco Secure Email Gateway or Cisco Secure Email Cloud Gateway.

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

An alert is sent when an update has failed 3 or more times for one of the scanning engines. Failed alerts can occur to AMP, Case, Graymail, McAfee and Sophos. Here is an example for Graymail failing to successfully complete an update.

```
The graymail application tried and failed 3 times to successfully complete an update.
```

Identify

To identify this issue, you can first confirm that you are still receiving alerts concerning update failures. For this, you can run the **displayalerts** command from the CLI.

<#root>

```
(esa.example.local) (SERVICE)>
```

displayalerts

```
Date and Time Stamp Description
-------------------------------------------------------------------------------
22 Nov 2024 12:00:00 +0300 The graymail application tried and failed 3 times to successfully complete a
```

```
outage.
```

From there, you can then review the **updater_logs** from the CLI to confirm when the last failure occurred.

<#root>

```
esa.example.local (SERVICE)>
```

grep -i "update failed" updater_logs

```
Fri Nov 22 12:00:00 2024 Warning: graymail update failed
```

If the last failure was a while ago, then chances are it was due to some network latency, and the alert can safely be ignored.

You f can finally run the **enginestatus all** command from the CLI and confirm that the engines and rules are indeed updating successfully. Do note that the engines update less often than the rules. So, while you can see rules last updated within the last 5-10 minutes, it could be a few days or weeks since the last engine update.

<#root>

```
(Machine esa.example.local)>

enginestatus all



Component      Version      Last Updated      File      Version
CASE Core Files 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414068326236
CASE Utilities 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414072027229
Structural Rules 3.13.2-20241121_201008 21 Nov 2024 23:30 (GMT +00:00) 1732231660607257
Web Reputation DB 20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 1729091106299038
Web Reputation DB Update 20241016_150447-20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 172909110643616
Content Rules 20241122_021309 22 Nov 2024 02:15 (GMT +00:00) 1732241625451653
Content Rules Update 20241122_022837 22 Nov 2024 02:30 (GMT +00:00) 1732242536816053
Bayes DB 20241122_004336-20241122_013648 22 Nov 2024 01:40 (GMT +00:00) 1732239454073553

SOPHOS Status: UP CPU: 0.0% RAM: 396M
Component Version Last Updated File Version
Sophos Anti-Virus Engine 3.2.07.392.0_6.12 14 Nov 2024 04:06 (GMT +00:00) 1729232666
Sophos IDE Rules 2024112103 21 Nov 2024 22:55 (GMT +00:00) 1732228972

GRAYMAIL Status: UP CPU: 0.0% RAM: 280M
Component Version Last Updated File Version
Graymail Engine 01.430.00 Never updated 143000
Graymail Rules 01.431.37#45 22 Nov 2024 02:25 (GMT +00:00) 1709881322
Graymail Tools 8.0-006 Never updated 1110080006

MCAFEE Status: UP CPU: 0.0% RAM: 670M
Component Version Last Updated File Version
McAfee Engine 6700 Never updated 6700
McAfee DATs 11263 21 Nov 2024 11:29 (GMT +00:00) 1732187479

AMP Status: UP CPU: 0.0% RAM: 163M
Component Version Last Updated File Version
AMP Client Settings 15.0.0-006 14 Nov 2024 04:06 (GMT +00:00) 100110
AMP Client Engine 1.0 Never updated 10
```

Resolution

Network Connectivity

If the failures are still occurring, there are a few things that you can do to further troubleshoot.

1. Review the Firewall Index within the respective AsyncOS version matching your build and perform some basic network connectivity tests. Here you have some telnet tests showing successful **Connected** sessions, which is what you are looking for.
    1. Refer to the User Guide for AsyncOS 16.0 for Cisco Secure Email Gateway - GD (General Deployment) for one that you have available for AsyncOS 16.0.
2. If one or more of these tests are failing, then you must wish to make sure that your network has allowed this traffic outbound and retry.

<#root>

```
(Machine esa.example.local)>
telnet updates.ironport.com 80

Trying 23.62.46.116...
Connected
 to a23-62-46-116.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet downloads.ironport.com 80

Trying 96.16.55.20...
Connected
 to a96-16-55-20.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet update-manifests.ironport.com 443

Trying 208.90.58.5...
Connected
 to update-manifests.ironport.com.
(Machine esa.example.local)>
telnet update-manifests.sco.cisco.com 443

Trying 208.90.58.6...
Connected
 to update-manifests.sco.cisco.com.
```

Manifest Server Usage

Note: update-manifests.ironport.com is used for physical appliances while update-manifests.sco.cisco.com is used by virtuals. To make sure that the correct host is in use, you can run the updateconfig command followed by dynamichost. If it is incorrect then make sure to correct the hostname:port, and then commit and save your changes.

<#root>

```
(Cluster esa.lab)>

updateconfig



Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLUSTERSET - Set how updates are configured in a cluster
- CLUSTERSHOW - Display how updates are configured in a cluster
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>

dynamichost



This command is restricted to "machine" mode. Would you like to switch to "machine" mode? [Y]>

Choose a machine.
1. esa1.lab.local
2. esa2.lab.local
[1]>

Enter new manifest hostname:port
[

update-manifests.sco.cisco.com:443


]>
```

If you have gone through the steps and are still experiencing update failures, please proceed with opening a Cisco TAC case, contact Support.

Related Information

- Cisco Secure Email Cloud Gateway End-User Guides
- Cisco Secure Email Gateway End-User Guides
- Cisco Technical Support & Downloads