Upgrade-Prozess für sicheres E-Mail-Gateway

Inhalt

Einleitung

In diesem Dokument werden die Schritte im Zusammenhang mit dem AsyncOS-Upgrade-Prozess für das Cisco Secure Email Gateway (SEG) bzw. die Cisco Email Security Appliance (ESA) beschrieben.

Anforderungen

- Stellen Sie sicher, dass der RAID-Status der Einheit in der Ausgabe für den Systemstatus auf BEREIT oder OPTIMAL eingestellt ist. Initiieren Sie keine Aktualisierung für eine Appliance mit dem RAID-Status DEGRADED. Wenden Sie sich an Cisco TAC, um ein RMA-Ticket (Return Material Authorization) für Ihre Appliance zu erstellen.
- Überprüfen Sie, ob es sich bei der ESA um eine Standalone-Appliance oder um eine Cluster-Umgebung handelt. Überprüfen Sie bei Clusterumgebungen den Abschnitt *Clusteraktualisierung* dieses Dokuments.
- Stellen Sie sicher, dass die Ports 80 und 443 über eine Internetverbindung von der ESA ohne Paketprüfung verfügen.
- Ein funktionierender DNS-Server ist erforderlich.

Kompatibilität zwischen ESA/SMA

Überprüfen Sie die Kompatibilität der ESA- und SMA-Systeme, bevor Sie ein Upgrade durchführen. Ältere Versionen von AsyncOS für Email Security können mehrere Upgrades erfordern, um auf die neueste Version zugreifen zu können. Um den Upgrade-Pfad und die Appliance-Bereitstellung zu bestätigen, wenden Sie sich an Cisco TAC.

Upgrade vorbereiten

1. Speichern Sie die XML-Konfigurationsdatei offline. Wenn Sie aus irgendeinem Grund zu einer vorherigen Version zurückkehren müssen, können Sie diese Datei verwenden, um die

vorherige Konfiguration zu importieren.
2. Wenn Sie die Funktion für Listen sicherer Absender/Sperrlisten verwenden, exportieren Sie die Liste Off-Box.
3. Alle Listener anhalten. Wenn Sie das Upgrade über die CLI durchführen, verwenden Sie suspendlistener aus. Wenn Sie das Upgrade über die GUI durchführen, wird der Listener automatisch ausgesetzt.
4. Warten Sie, bis die Warteschlange leer ist. Sie können die workqueue -Befehl, um die Anzahl der Nachrichten in der Arbeitswarteschlange anzuzeigen, oder den Rate-Befehl in der CLI, um den Nachrichtendurchsatz auf Ihrer Appliance zu überwachen.

Upgrade herunterladen und installieren

Ab AsyncOS für Email Security Version 8.0 umfassen die Upgrade-Optionen nun zusätzlich zum **DOWNLOAD auch DOWNLOADINSTALL**. Dies gibt dem Administrator die Flexibilität, Dateien in einem einzigen Vorgang herunterzuladen und zu installieren, oder sie im Hintergrund herunterzuladen und später zu installieren.

```
(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]>
```

Weitere Informationen finden Sie im Benutzerhandbuch.

Upgrade über die CLI

1. Geben Sie status , und stellen Sie sicher, dass der Listener ausgesetzt ist. Sie können sehen "Systemstatus: **Empfang ausgesetzt**".
2. Geben Sie upgrade aus.
3. Wählen Sie eine Option für **DOWNLOADINSTALL** oder **DOWNLOAD**.
4. Wählen Sie die Nummer aus, die der gewünschten Upgrade-Version zugeordnet ist.
5. Beantworten Sie die erforderlichen Fragen, um die aktuelle Konfiguration zu speichern, und genehmigen Sie den Neustart, wenn das Upgrade angewendet wird.
6. Melden Sie sich nach dem Upgrade bei der CLI an, und geben Sie resume um die Listener wieder aufzunehmen und den Betrieb sicherzustellen. Geben Sie status und bestätigen Sie "Systemstatus: **Online**".

Upgrade über die Benutzeroberfläche

1. Wählen Sie **Systemverwaltung > Systemaktualisierung aus**.
2. Klicken Sie auf **Upgrade Options...**

3. Wählen Sie eine Option für *Download und Installation* oder *Download*.
4. Klicken Sie auf die gewünschte Upgrade-Version, und markieren Sie sie.
5. Wählen Sie die entsprechenden Optionen für die *Upgrade-Vorbereitung aus*.
6. **Fahren Sie fort**, um mit der Aktualisierung zu beginnen, und zeigen Sie die Statusleiste für die Überwachung an.
7. Melden Sie sich nach dem Upgrade bei der CLI an, und geben Sie resume um die Listener wieder aufzunehmen und den Betrieb sicherzustellen: Wählen Sie **Systemverwaltung > Herunterfahren/Aussetzen > Fortsetzen (Alle prüfen)**.
8. Wählen Sie im Abschnitt *Mail-Vorgänge* die Option **Übernehmen aus**.

Cluster-Upgrade

ESAs in einem Cluster würden den gleichen Upgrade-Prozess von der CLI oder der GUI wie in den vorherigen Abschnitten durchführen, mit der Ausnahme, dass eine Aufforderung zum Trennen von Geräten vom Cluster angezeigt wird.

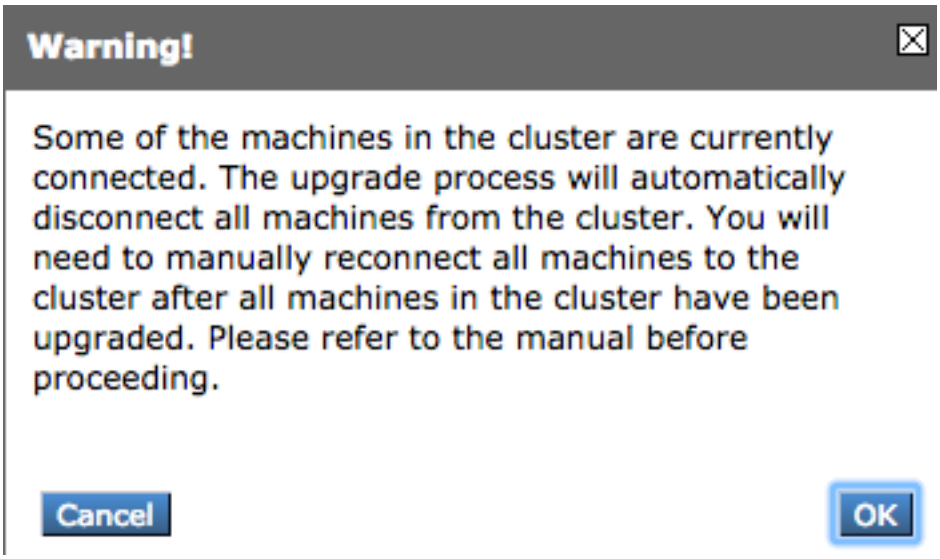
> **Anmerkung:** Sie können das Upgrade mit der CLI oder der GUI durchführen, aber die Verbindung clusterconfig Befehle sind nur über die CLI verfügbar. In diesem Dokument wird beschrieben, wie die Computer über die CLI aktualisiert werden.

Beispiel aus der Kommandozeile:

```
(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
```

Beispiel aus der GUI:



> **Anmerkung:** Dies ist nur eine administrative Trennung. Dadurch werden alle Synchronisierungsversuche der Konfiguration im Cluster von oder zu den getrennten Appliances gestoppt. Die Appliance-Konfiguration wird dadurch weder entfernt noch geändert.

Gehen Sie wie folgt vor, um ESAs zu aktualisieren, die in einem Cluster über die CLI ausgeführt

werden:

1. Geben Sie upgrade in die CLI ein, um AsyncOS auf eine neuere Version zu aktualisieren. Wenn Sie gefragt werden, ob Sie die Verbindung zum Cluster trennen möchten, antworten Sie mit dem Buchstaben Y fortfahren:

```
(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. Befolgen Sie alle Upgrade-Anweisungen (*Neustart*-Aufforderung eingeschlossen).

3. Nachdem alle Computer im Cluster aktualisiert und neu gestartet wurden, melden Sie sich über die CLI bei einem der Computer im Cluster an, und geben Sie die clusterconfig aus. Schließen Sie sie auf Cluster-Ebene wieder an, um die Konfigurations-Synchronisierung zu ermöglichen und den Cluster-Betrieb wieder aufzunehmen.
4. Antworten Yes wieder eine Verbindung herstellen. Es ist nicht notwendig, sich zu *verpflichten*.

```
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. Geben Sie den Befehl ein. connstatus um zu überprüfen, ob alle Geräte im Cluster vorhanden sind. Geben Sie außerdem den Befehl **clustercheck** um zu bestätigen, dass keine Inkonsistenz besteht.

Empfehlungen für Cluster-Upgrades:

- Schließen Sie die ESAs erst wieder an den Cluster an, wenn ALLE Appliances auf eine übereinstimmende Version aktualisiert wurden.
- Sobald eine ESA ein Upgrade abgeschlossen hat, setzen Sie ggf. den Listener fort, falls dieser zuvor ausgesetzt wurde, und lassen Sie zu, dass er als eigenständige Appliance funktioniert.
- Nehmen Sie keine Konfigurationsänderungen oder -änderungen vor, wenn ESAs von einem Cluster getrennt werden, um Konfigurationsinkonsistenzen zu vermeiden, wenn die Verbindung nach dem Upgrade auf Cluster-Ebene wiederhergestellt wird.
- Sobald ALLE Appliances auf die gleiche Version aktualisiert wurden, verbinden Sie sie auf Cluster-Ebene erneut, um die Konfigurationssynchronisierung zu ermöglichen und den Cluster-Betrieb wieder aufzunehmen.

Nachprüfungen:

- Wenn die Appliances von der SMA verwaltet werden, gehen Sie wie folgt vor: Navigieren Sie zu **Management Appliance > Centralized Services > Security Appliances,** und stellen Sie sicher, dass alle Services verfügbar sind und die Verbindung als "**Established" (eingerichtet)**

angezeigt wird.Navigieren Sie zu **E-Mail > Message Tracking > Message Tracking Data Availability,** und prüfen Sie, ob der Status für alle ESAs **OK** anzeigt.Geben Sie auf jeder Appliance die status -Befehl ein, und suchen Sie nach diesem, um ihn als online anzuzeigen.Geben Sie displayalerts und überprüfen Sie, ob nach dem Upgrade neue Warnungen angezeigt werden.Wenn Sie sich in einem Cluster befinden, **clustercheck** -Befehl darf keine Inkonsistenzen aufweisen. **connstatus** muss Appliances fehlerfrei als verbunden anzeigen.Um den E-Mail-Fluss zu überprüfen, geben Sie **tail mail_logs** in die CLI ein.

Fehlerbehebung

1. **tail updater_logs** und **tail upgrade_logs** kann auch Informationen geben, wenn ein Problem mit dem Upgrade vorliegt.
2. Wenn beim Herunterladen des Images oder beim Aktualisieren des Antispam- oder Antivirus-Programms ein Problem auftritt, liegt dies wahrscheinlich daran, dass die Prozesse nicht in der Lage sind, die Service-Engine oder die Regelsätze zu aktualisieren. Befolgen Sie die Schritte unter vESA kann keine Updates für Antispam oder Antivirus herunterladen und anwenden.
3. Wenn das Upgrade aufgrund von Netzwerkunterbrechungen fehlschlägt, können während der Ausgabe des Upgrade-Prozesses ähnliche Fehler auftreten:

```
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.
```

Dies ist in der Regel auf eine Netzwerkunterbrechung zurückzuführen, die bei der Übertragung von Daten zwischen der ESA und den Update-Servern aufgetreten sein kann. Überprüfen Sie alle Netzwerk-Firewall-Protokolle, oder überwachen Sie den Paketverkehr von der ESA, um Server zu aktualisieren.

Verwenden Sie ggf. die ESA-Paketerfassungsverfahren, um die Paketerfassung auf der ESA zu aktivieren, und wiederholen Sie dann den Aktualisierungsvorgang.

> **Anmerkung:** Firewalls müssen insbesondere während des Upgrade-Prozesses dafür sorgen, dass inaktive Verbindungen erhalten bleiben.

Statische Netzwerk-Firewalls, die statische Upgrade-Server erfordern, finden Sie unter Content Security Appliance-Upgrades oder -Updates mit einem statischen Server, wie Sie statische Update- und Upgrade-Server konfigurieren.

Testen Sie bei Hardware-Appliances die Verbindungen mit den folgenden dynamischen Servern:

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

Für virtuelle Appliances müssen Sie folgende dynamische Server verwenden:

- telnet update-manifests.sco.cisco.com 443

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

Im Benutzerhandbuch finden Sie vollständige Informationen zur Firewall und zu den Port-Anforderungen.

Zugehörige Informationen

- Kompatibilitätsmatrix für Cisco Content Security Management Appliances
- ESA-Aktualisierungsverfahren
- ESA-Verfahren zur Paketerfassung
- Content Security Appliance-Upgrades oder -Updates mit einem statischen Server
- Technischer Support und Dokumentation für Cisco Systeme