Processo di aggiornamento per Secure Email Gateway

Sommario

Introduzione

In questo documento viene descritta la procedura associata al processo di aggiornamento di AsyncOS per Cisco Secure Email Gateway (SEG) o Cisco Email Security Appliance (ESA).

Requisiti

- Verificare che lo stato RAID dell'accessorio sia READY o OPTIMAL nell'output dello stato del sistema. Non avviare un aggiornamento su un accessorio con stato RAID DEGRADED. Contattare Cisco TAC per avviare una richiesta di autorizzazione alla restituzione del materiale (RMA) per l'appliance.
- Verificare se l'ESA è un dispositivo autonomo o in un ambiente cluster. Se si tratta di un cluster, verificare in modo appropriato la sezione *Aggiornamento cluster* di questo documento.
- Garantire la connettività Internet dell'ESA sui porti 80 e 443 senza ispezioni dei pacchetti.
- Sono necessari uno o più server DNS funzionanti.

Compatibilità tra ESA/SMA

Esaminare la compatibilità dei sistemi ESA e SMA prima di eseguire l'aggiornamento. Per ottenere la versione più recente, le versioni precedenti di AsyncOS for Email Security possono richiedere più di un aggiornamento. Per conferma del percorso di aggiornamento e del provisioning dell'appliance, contattare Cisco TAC.

Preparazione aggiornamento

1. Salvare il file di configurazione XML in modalità off-box. Se per qualsiasi motivo è necessario tornare alla release precedente all'aggiornamento, è possibile utilizzare questo file per importare la configurazione precedente.

2. Se si utilizza la funzione Safelist/Blocklist, esportare l'elenco fuori casella.
3. Sospendere tutti i listener. Se si esegue l'aggiornamento dalla CLI, usare il comando suspendlistener Se si esegue l'aggiornamento dalla GUI, il listener viene sospeso automaticamente.
4. Attendere che la coda si svuoti. È possibile utilizzare workqueue per visualizzare il numero di messaggi nella coda di lavoro o il comando rate nella CLI per monitorare il throughput dei messaggi sull'accessorio.

Scaricare e installare l'aggiornamento

a partire dalla versione 8.0 di AsyncOS for Email Security, le opzioni di aggiornamento sono state aggiornate per includere **DOWNLOADINSTALL** oltre a **DOWNLOAD**. In questo modo, l'amministratore può scaricare e installare i file con una sola operazione oppure scaricare i file in background e installarli in un secondo momento.

```
(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]>
```

Per ulteriori informazioni, consultare la Guida dell'utente.

Aggiornamento dalla CLI

1. Immettere il status e assicurarsi che il listener sia sospeso. È possibile visualizzare "Stato del sistema: **Ricezione sospesa**".
2. Immettere il upgrade
3. Selezionare un'opzione per **DOWNLOADINSTALL** o **DOWNLOAD**.
4. Scegliere il numero appropriato associato alla versione di aggiornamento desiderata.
5. Completare le domande necessarie per salvare la configurazione corrente e approvare il riavvio quando viene applicato l'aggiornamento.
6. Dopo l'aggiornamento, accedere alla CLI e immettere resume per riprendere i listener e garantire il funzionamento. Immettere il status e confermare "Stato del sistema: **Online**".

Aggiornamento tramite GUI

1. Scegliere **Amministrazione sistema > Aggiornamento sistema**.
2. Fare clic su **Opzioni di aggiornamento...**
3. Scegliere un'opzione per *Download e installazione* o *Download*.
4. Fare clic su ed evidenziare la versione di aggiornamento desiderata.
5. Scegliere le opzioni appropriate per *Preparazione aggiornamento*.

6. **Procedere** per iniziare l'aggiornamento e visualizzare l'indicatore di stato per il monitoraggio.
7. Dopo l'aggiornamento, accedere alla CLI e immettere resume per riprendere i listener e garantire il funzionamento: Scegliere **Amministrazione sistema > Arresto/Sospensione > Riprendi (selezionare Tutti)**.
8. Nella sezione *Operazioni posta*, scegliere **Conferma**.

Aggiornamento cluster

Le ESA in un cluster seguono lo stesso processo di aggiornamento dalla CLI o dalla GUI descritto nelle sezioni precedenti, con l'unica eccezione che viene richiesto di disconnettere i dispositivi dal cluster.

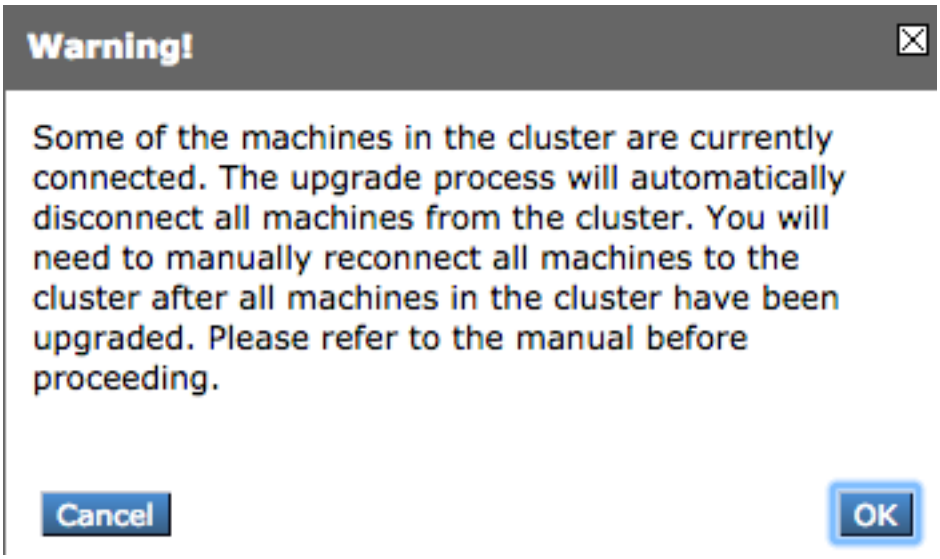
> **Nota:** È possibile eseguire l'aggiornamento dalla CLI o dalla GUI, ma la riconnessione clusterconfig i comandi sono disponibili solo tramite la CLI. Questo documento descrive come aggiornare i computer tramite la CLI.

Esempio tratto dalla 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
```

Esempio tratto dalla GUI:



> **Nota:** Si tratta solo di una disconnessione amministrativa. In questo modo, qualsiasi tentativo di sincronizzazione della configurazione nel cluster da o verso gli accessori disconnessi verrà interrotto. La configurazione dell'accessorio non viene rimossa né modificata.

Completare questi passaggi per aggiornare le ESA eseguite in un cluster tramite la CLI:

1. Immettere il upgrade nella CLI per aggiornare AsyncOS a una versione successiva. Quando viene richiesto se si desidera disconnettere il cluster, rispondere con la lettera Y per procedere:

```
(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. Seguire tutte le istruzioni di aggiornamento (prompt di *riavvio* incluso).

3. Dopo aver aggiornato e riavviato tutti i computer nel cluster, accedere a uno dei computer nel cluster tramite la CLI e immettere il comando clusterconfig Riconnetterli a livello di cluster per consentire la sincronizzazione della configurazione e la ripresa delle operazioni del cluster.
4. Rispondi Yes per riconnettersi. Non è necessario eseguire il *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. Eseguire il comando connstatus per verificare che tutti i dispositivi siano nel cluster. Inoltre, usare il comando **clustercheck** per confermare che non vi sono incoerenze.

Consigli per l'aggiornamento del cluster:

- Non riconnettere le ESA al cluster finché TUTTI gli accessori non vengono aggiornati a una versione corrispondente.
- Se necessario, una volta completato l'aggiornamento di un'ESA, riprendere il listener, se precedentemente sospeso, e consentirne il funzionamento come accessorio autonomo.
- Non apportare modifiche o modifiche alla configurazione quando le ESA vengono disconnesse da un cluster per evitare incoerenze nella configurazione quando vengono riconnesse al livello di cluster dopo l'aggiornamento.
- Dopo aver aggiornato TUTTI gli accessori alla stessa versione, riconnetterli a livello di cluster per consentire la sincronizzazione della configurazione e la ripresa del funzionamento del cluster.

Controlli postali:

- Se gli accessori sono gestiti dallo SMA: Passare a **Management Appliance > Centralized Services > Security Appliance (Appliance di gestione > Servizi centralizzati > Appliance di sicurezza)** e accertarsi che tutti i servizi siano attivi e che la connessione mostri "**Stabilito**".Selezionare **Email > Message Tracking > Message Tracking Data Availability** (Disponibilità dati verifica messaggi) e verificare se lo stato indica **OK** per tutte le ESA.Su ciascun accessorio, immettere il status e cercarlo per visualizzarlo in linea.Immettere il displayalerts e verificare la presenza di eventuali nuovi avvisi rilevati dopo l'aggiornamento.Se in un cluster, **clustercheck** non devono essere visualizzate incoerenze e il comando **connstatus** deve visualizzare gli accessori come connessi senza errori.Per verificare il flusso di posta, immettere il **tail mail_logs** nella CLI.

Risoluzione dei problemi

1. **tail updater_logs** e **tail upgrade_logs** può inoltre fornire informazioni in caso di problemi con l'aggiornamento.
2. Se si verifica un problema durante il download dell'immagine o l'aggiornamento dell'antispam o dell'antivirus, è probabile che i processi non siano in grado di raggiungere e aggiornare il motore del servizio o i set di regole. Seguire le istruzioni fornite in vESA Is Not Can to Download and Apply Updates for Antispam or Antivirus (vESA non è in grado di scaricare e applicare aggiornamenti per Antispam o Antivirus).
3. Se l'aggiornamento non riesce a causa di interruzioni della rete, si possono verificare errori simili durante l'output del processo di aggiornamento:

```
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.
```

Ciò è in genere dovuto a un'interruzione della rete che può essersi verificata durante la trasmissione dei dati tra l'ESA e i server di aggiornamento. Esaminare i registri del firewall di rete o monitorare il traffico dei pacchetti dall'ESA per aggiornare i server.

Se necessario, consultare il documento ESA Packet Capture Procedures (Procedure di acquisizione pacchetti ESA) per abilitare l'acquisizione dei pacchetti sull'ESA, quindi riprovare il processo di aggiornamento.

> **Nota:** I firewall devono consentire le connessioni inattive per rimanere attive, soprattutto per il processo di aggiornamento.

Per informazioni sui firewall di rete rigidi che richiedono server di aggiornamento statici, vedere Aggiornamenti di Content Security Appliance o Aggiornamenti con un server statico per informazioni su come configurare i server di aggiornamento statici.

Per i dispositivi hardware, verificare le connessioni ai seguenti server dinamici:

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

Per le appliance virtuali è necessario utilizzare i seguenti server dinamici:

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

Fare riferimento al Manuale dell'utente per informazioni complete sul firewall e i requisiti delle porte.

Informazioni correlate

- Matrice di compatibilità per le appliance Cisco Content Security Management

- Procedure di aggiornamento ESA
- Procedure di acquisizione dei pacchetti ESA
- Aggiornamento di Content Security Appliance con un server statico
- Documentazione e supporto tecnico – Cisco Systems