Configurazione di Cisco Email Security and Security Management per gli aggiornamenti della gestione temporanea

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione di Cisco Email Security and Security Management per gli aggiornamenti della gestione temporanea
Accedere alla GUI
Accesso alla CLI
Verifica
Ripristina
Filtro URL
AsyncOS 13.0 e versioni precedenti
Ripristina
AsyncOS 13.5 e versioni successive (con Cisco Talos Services)
Impostazioni del firewall per accedere ai servizi Cisco Talos
Tracciamento interazione Web
Ripristina
Risoluzione dei problemi
Informazioni correlate

Introduzione

Questo documento descrive il processo per i clienti Beta e gli accessori con provisioning preliminare utilizzati per il test, che devono aggiornare le versioni AsyncOS e ottenere aggiornamenti per ESA e SMA che eseguono Beta e test preliminari. Questo documento si riferisce direttamente a Cisco Email Security Appliance (ESA) e Cisco Security Management Appliance (SMA). Tenere presente che i server di staging non devono essere utilizzati dai clienti di produzione standard per la produzione ESA o SMA. Le versioni del sistema operativo, le regole dei servizi e i motori dei servizi di gestione temporanea variano a seconda della produzione.

Prima di procedere, tenere presente che le licenze di produzione non possono essere aggiornate a Stage releases in quanto non superano la verifica e l'autenticazione della licenza. Una VLAN di produzione ha un valore di firma scritto quando la licenza viene generata, che corrisponde al servizio di licenza di produzione. Le licenze della fase hanno una firma separata scritta solo per il servizio di gestione temporanea delle licenze.

Prerequisiti

Requisiti

1. L'amministratore ha ricevuto in precedenza una comunicazione relativa all'installazione o agli aggiornamenti beta (versione non definitiva).
2. I clienti che partecipano ai test Beta e pre-release hanno completato un'applicazione beta e hanno letto e accettato un accordo di non divulgazione prima dell'inizio della versione beta.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione di Cisco Email Security and Security Management per gli aggiornamenti della gestione temporanea

> **Nota:** I clienti devono utilizzare gli URL del server di aggiornamento intermedio solo se hanno ottenuto l'accesso al pre-provisioning tramite Cisco solo per l'utilizzo Beta (sistema operativo precedente alla release). Se non si dispone di una licenza valida per l'utilizzo Beta, l'accessorio non riceverà aggiornamenti dai server di aggiornamento di gestione temporanea. Queste istruzioni devono essere utilizzate solo per i clienti Beta o dagli amministratori che partecipano ai test Beta.

Per ricevere aggiornamenti e aggiornamenti di gestione temporanea:

Accedere alla GUI

1. Scegliere **Servizi di sicurezza > Aggiornamenti servizi > Modifica impostazioni aggiornamento...**
2. Confermare che tutti i servizi sono configurati per l'utilizzo dei server di aggiornamento Cisco IronPort

Accesso alla CLI

1. Eseguire il comando **updateconfig**
2. Eseguire il sottocomando nascosto **dynamichost**
3. Immettere uno dei seguenti comandi: Per l'hardware ESA/SMA: **stage-update-manifests.ironport.com:443**Per ESA/SMA virtuale: **stage-stg-updates.ironport.com:443**
4. Premere Invio fino a tornare al prompt principale
5. Immettere **Commit** per salvare tutte le modifiche

Verifica

La verifica può essere verificata in *updater_logs* con la comunicazione riuscita per l'URL della fase appropriata. Dalla CLI dell'accessorio, immettere **grep stage updater_logs**:

```
esa.local> updatenow force

Success - Force update for all components requested
esa.local > grep stage updater_logs

Wed Mar 16 18:16:17 2016 Info: internal_cert beginning download of remote file "http://stage-
updates.ironport.com/internal_cert/1.0.0/internal_ca.pem/default/100101"
Wed Mar 16 18:16:17 2016 Info: content_scanner beginning download of remote file "http://stage-
updates.ironport.com/content_scanner/1.1/content_scanner/default/1132001"
Wed Mar 16 18:16:17 2016 Info: enrollment_client beginning download of remote file
"http://stage-updates.ironport.com/enrollment_client/1.0/enrollment_client/default/102057"
Wed Mar 16 18:16:18 2016 Info: support_request beginning download of remote file "http://stage-
updates.ironport.com/support_request/1.0/support_request/default/100002"
Wed Mar 16 18:16:18 2016 Info: timezones beginning download of remote file "http://stage-
updates.ironport.com/timezones/2.0/zoneinfo/default/2015100"
Wed Mar 16 18:26:19 2016 Info: repeng beginning download of remote file "http://stage-
updates.ironport.com/repeng/1.2/repeng_tools/default/1392120079"
```

In caso di errori di comunicazione imprevisti, immettere **dig <stage URL>** per verificare il DNS (Domain Name Server).

Esempio:

```
esa.local > dig stage-updates.ironport.com


; <<>> DiG 9.8.4-P2 <<>> stage-updates.ironport.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52577
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;stage-updates.ironport.com. IN A

;; ANSWER SECTION:
stage-updates.ironport.com. 275 IN A 208.90.58.21

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 22 14:31:10 2016
;; MSG SIZE rcvd: 60
```

Verificare che l'accessorio sia in grado di comunicare via telnet sulla porta 80, eseguire il comando **telnet <URL stadio> 80**.

Esempio:

```
esa.local > telnet stage-updates.ironport.com 80

Trying 208.90.58.21...
Connected to origin-stage-updates.ironport.com.
Escape character is '^]'.
```

Ripristina

Per ripristinare i server di aggiornamento della produzione standard, attenersi alla seguente procedura:

1. Immettere il comando **updateconfig**
2. Immettere il sottocomando nascosto **dynamichost**
3. Immettere uno dei seguenti comandi: Per l'hardware ESA/SMA: **update-manifests.ironport.com:443**Per ESA/SMA virtuale: **update-manifests.sco.cisco.com:443**
4. Premere Invio fino a tornare al prompt principale
5. Eseguire il comando **Commit** per salvare tutte le modifiche

Nota: Gli accessori hardware (C1x0, C3x0, C6x0 e X10x0) devono utilizzare SOLO gli URL host dinamici *stage-update-manifests.ironport.com:443* o *update-manifests.ironport.com:443*. Se è presente una configurazione cluster con ESA e vESA, è necessario configurare updateconfig a livello di computer e verificare che **dynamichost** sia impostato di conseguenza.

Filtro URL

AsyncOS 13.0 e versioni precedenti

Se il filtro URL è configurato e in uso sull'accessorio e un accessorio è stato reindirizzato per l'utilizzo dell'URL della fase di aggiornamento, sarà necessario configurare l'accessorio in modo che utilizzi il server di gestione temporanea per il filtro URL:

1. Accesso all'accessorio dalla CLI
2. Immettere il comando **configurazione avanzata websecurityadvancedconfig** Eseguire la configurazione e modificare il valore dell'opzione *Immettere il nome host del servizio di sicurezza Web* in **v2.beta.sds.cisco.com**
3. Modificare il valore dell'opzione *Immettere il valore di soglia per le richieste in sospeso* dal valore predefinito 50 a **5**
4. Accetta valori predefiniti per tutte le altre opzioni
5. Premere Invio fino a tornare al prompt principale
6. Eseguire il comando **Commit** per salvare tutte le modifiche

Ripristina

Per tornare al servizio di protezione Web di produzione, attenersi alla seguente procedura:

1. Accesso all'accessorio tramite CLI
2. Immettere il comando **websecurityadvancedconfig** Eseguire la configurazione e modificare il valore dell'opzione *Immettere il nome host del servizio di sicurezza Web* in **v2.sds.cisco.com**
3. Accetta valori predefiniti per tutte le altre opzioni
4. Premere Invio fino a tornare al prompt principale
5. Eseguire il comando **Commit** per salvare tutte le modifiche

AsyncOS 13.5 e versioni successive (con Cisco Talos Services)

A partire da AsyncOS 13.5 for Email Security, è stata introdotta l'analisi degli URL del cloud (CUA)

che ha modificato le opzioni **websecurityadvancedconfig**. Poiché l'analisi dell'URL viene ora eseguita nel cloud Talos, il nome host dei servizi di sicurezza Web non è più necessario. Questa configurazione è stata sostituita dal comando **talosconfig**. Questa funzione è disponibile solo sulla riga di comando dell'ESA.

```
esa.local> talosconfig


Choose the operation you want to perform:
- SETUP - Configure beaker streamline configuration settings
[]> setup

Configured server is: stage_server

Choose the server for streamline service configuration:
1. Stage Server
2. Production Server
[]> 1
```

Se si esegue una licenza Stage, è necessario puntare a Stage Server per i servizi Talos.

Èpossibile eseguire **talosupdate** e **talosstatus** per richiedere un aggiornamento e lo stato corrente di tutti i servizi basati su Talos.

Esempio:

```
esa.local> talosstatus

Component                          Version           Last Updated
Sender IP Reputation Client        1.0               Never updated
URL Reputation Client              1.0               Never updated
Service Log Client                 1.0               Never updated
Talos Engine                       1.95.0.269        Never updated
Talos Intelligence Services Module 1.95.0.808        Never updated
Talos-HTTP2 Component              0.9.330           Never updated
Libraries                          1.0               Never updated
Protofiles                         1.0               Never updated
```

Per ulteriori informazioni, vedere la guida per l'utente di AsyncOS 13.5 for Cisco Email Security Appliance.

Impostazioni del firewall per accedere ai servizi Cisco Talos

Per connettere il gateway e-mail ai servizi Cisco Talos, è necessario aprire la porta HTTPS (Out) 443 sul firewall per i seguenti nomi host o indirizzi IP (fare riferimento alla tabella seguente).

Nome host	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff:/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe: 1000/48
serviceconfig.talos.cisco.com	146.112.255.0/24 146.112.59.0/24	- -

Tracciamento interazione Web

La funzionalità di monitoraggio delle interazioni Web fornisce informazioni sugli utenti finali che hanno fatto clic sugli URL riscritti e sull'azione (consentita, bloccata o sconosciuta) associata a ciascun clic dell'utente.

A seconda dei requisiti, è possibile attivare la registrazione dell'interazione Web in una delle pagine delle impostazioni globali:

1. Filtri epidemie. Tracciare gli utenti finali che hanno fatto clic sugli URL riscritti dai filtri epidemie
2. Filtro URL. Tenere traccia degli utenti finali che hanno fatto clic sugli URL riscritti tramite policy (utilizzando i filtri contenuti e messaggi)

Se il rilevamento dell'interazione Web è configurato e in uso, dopo che un accessorio è stato reindirizzato per l'utilizzo dell'URL della fase per gli aggiornamenti, sarà necessario configurare l'accessorio per l'utilizzo del server Aggregator della fase di gestione temporanea:

1. Accesso all'accessorio dalla CLI
2. Immettere il comando **aggregatorconfig**
3. Utilizzare il comando EDIT e immettere il seguente valore: **stage.aggregator.sco.cisco.com**
4. Premere Invio fino a tornare al prompt principale
5. Esegui **commit** per salvare tutte le modifiche

Se Aggregator non è configurato per la gestione temporanea, verranno visualizzati avvisi simili ogni 30 minuti tramite avvisi e-mail di amministrazione:

```
Unable to retrieve Web Interaction Tracking information from the Cisco Aggregator Server.
Details: Internal Server Error.
```

Oppure, eseguendo il comando **displayalert** sulla CLI:

```
20 Apr 2020 08:52:52 -0600 Unable to connect to the Cisco Aggregator Server.
Details: No valid SSL certificate was sent.
```

Ripristina

Per ripristinare il server Aggregator di produzione standard, attenersi alla seguente procedura:

1. Accesso all'accessorio tramite CLI
2. Immettere il comando **aggregatorconfig**
3. Utilizzare il comando **EDIT** e immettere il seguente valore: **aggregator.cisco.com**
4. Premere Invio fino a tornare al prompt principale
5. Eseguire il comando **Commit** per salvare tutte le modifiche

Risoluzione dei problemi

I comandi per la risoluzione dei problemi sono elencati nella sezione "Verifica" di questo documento.

Se durante l'esecuzione del comando **upgrade** si verificano le condizioni seguenti:

```
Failure downloading upgrade list.
```

Verificare di aver modificato l'host dinamico. Se il problema persiste, verificare che l'ESA o l'SMA siano stati predisposti correttamente per il test Beta o pre-release.

Informazioni correlate

- vESA non è in grado di scaricare e applicare aggiornamenti per Antispam o Antivirus
- Documentazione e supporto tecnico – Cisco Systems