Konfigurieren von Cisco Email Security und Security Management für Staging-Updates

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren von Cisco Email Security und Security Management für Staging-Updates
Anmeldung bei der GUI
Anmeldung bei der CLI
Überprüfen
Umkehren
URL-Filterung
AsyncOS 13.0 und älter
Umkehren
AsyncOS 13.5 und höher (mit Cisco Talos Services)
Firewall-Einstellungen für den Zugriff auf Cisco Talos-Services
Verfolgung von Webinteraktionen
Umkehren
Fehlerbehebung
Zugehörige Informationen

Einführung

Dieses Dokument beschreibt den Prozess für Beta-Kunden und vorab bereitgestellte Appliances, die zum Testen verwendet werden und ein Upgrade von AsyncOS-Versionen sowie Updates für ESA- und SMA-Anwendungen benötigen, die Beta- und Vorabtests ausführen. Dieses Dokument bezieht sich direkt auf die Cisco E-Mail Security Appliance (ESA) und die Cisco Security Management Appliance (SMA). Beachten Sie, dass die Staging-Server nicht von Standardproduktionskunden für Produktions-ESA oder SMA verwendet werden dürfen. Die Bereitstellung von Betriebssystemversionen, Servicestandards und Service-Engines unterscheidet sich von der Produktion.

Bitte beachten Sie, dass Produktionslizenzen nicht auf Stage-Versionen aktualisieren können, da sie die Überprüfung und Authentifizierung der Lizenz nicht bestehen können. Ein Produktions-VLN verfügt über einen Signaturwert, der bei der Generierung der Lizenz geschrieben wird und mit dem Produktionslizenzdienst übereinstimmt. Stage-Lizenzen verfügen über eine separate Signatur, die nur für den Staging-Lizenzdienst geschrieben wird.

Voraussetzungen

Anforderungen

1. Der Administrator wurde zuvor über die Installation oder Upgrades der Beta-Version (vorinstalliertes Betriebssystem) informiert.
2. Kunden, die an Beta- und Vorabtests teilnehmen, haben einen Beta-Antrag abgeschlossen und vor Beginn der Beta-Version eine Geheimhaltungsvereinbarung gelesen und diesen zugestimmt.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren von Cisco Email Security und Security Management für Staging-Updates

> **Hinweis**: Kunden sollten die Staging-Update-Server-URLs nur dann verwenden, wenn sie über Cisco Zugriff auf die Vorabbereitstellung nur für die Beta-Nutzung (Pre-Release OS) erhalten haben. Wenn Sie keine gültige Lizenz für die Verwendung von Beta beantragt haben, erhält Ihre Appliance keine Updates von den Staging-Update-Servern. Diese Anweisungen sollten nur für Beta-Kunden oder für Administratoren, die an Beta-Tests teilnehmen, verwendet werden.

So erhalten Sie Staging-Updates und -Upgrades:

Anmeldung bei der GUI

1. Wählen Sie **Sicherheitsdienste > Dienstaktualisierungen > Aktualisierungseinstellungen bearbeiten aus...**
2. Bestätigen Sie, dass alle Services für die Verwendung der Cisco IronPort Update-Server konfiguriert sind.

Anmeldung bei der CLI

1. Führen Sie den Befehl **updateconfig aus**
2. Ausführen des ausgeblendeten Unterbefehls **dynamichost**
3. Geben Sie einen der folgenden Befehle ein: Für Hardware ESA/SMA: **stage-update-manifests.ironport.com:443**Für virtuelle ESA/SMA: **stage-stg-updates.ironport.com:443**
4. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
5. Geben Sie "**Commit" ein**, um alle Änderungen zu speichern.

Überprüfen

Die Überprüfung kann im *updater_logs* angezeigt werden, wobei die Kommunikation für die

entsprechende Phase-URL erfolgreich war. Geben Sie in der CLI der Appliance **grep stage updater_logs ein**:

```
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"
```

Wenn unerwartete Kommunikationsfehler auftreten, geben Sie **dig <stage URL>** ein, um den Domain Name Server (DNS) zu überprüfen.

Beispiel:

```
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
```

Vergewissern Sie sich, dass die Appliance über Port 80 Telnet empfangen kann, und führen Sie den Befehl **telnet <stage URL> 80 aus**.

Beispiel:

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

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

Umkehren

Gehen Sie wie folgt vor, um wieder auf die Standard-Produktionsaktualisierungsserver zurückzusetzen:

1. Geben Sie den Befehl **updateconfig ein.**
2. Geben Sie den ausgeblendeten Unterbefehl **dynamichost ein.**
3. Geben Sie einen der folgenden Befehle ein: Für Hardware ESA/SMA: **update-manifests.ironport.com:443**Für virtuelle ESA/SMA: **update-manifests.sco.cisco.com:443**
4. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
5. Führen Sie den Befehl **Commit (Übernehmen)** aus, um alle Änderungen zu speichern.

Hinweis: Hardware-Appliances (C1x0, C3x0, C6x0 und X10x0) sollten NUR die dynamischen Host-URLs von *stage-update-manifests.ironport.com:443* oder *update-manifests.ironport.com:443* verwenden. Wenn eine Clusterkonfiguration mit ESA und vESA vorhanden ist, muss **updateconfig** auf Computerebene konfiguriert werden und sicherstellen, dass **dynamichost** entsprechend eingestellt wird.

URL-Filterung

AsyncOS 13.0 und älter

Wenn die URL-Filterung konfiguriert ist und auf der Appliance verwendet wird, muss die Appliance nach der Umleitung einer Appliance zur Verwendung der Stadium-URL für Updates auch so konfiguriert werden, dass sie den Staging-Server für die URL-Filterung verwendet:

1. Zugriff auf die Appliance über die CLI
2. Geben Sie den Befehl ein **websecurityadvanced config** Gehen Sie die Konfiguration durch, und ändern Sie den Wert für die Option *Geben Sie den Hostnamen des Websicherheitsdienstes* in **v2.beta.sds.cisco.com ein.**
3. Ändern Sie den Wert für die Option *Geben Sie den Schwellenwert für ausstehende Anfragen* vom Standardwert 50 bis **5** *ein.*
4. Standardwerte für alle anderen Optionen akzeptieren
5. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
6. Führen Sie den Befehl **Commit (Übernehmen) aus**, um alle Änderungen zu speichern.

Umkehren

Gehen Sie wie folgt vor, um zum Produktionswebsicherheitsdienst zurückzukehren:

1. Zugriff auf die Appliance über CLI
2. Geben Sie den Befehl **websecurityadvanced config ein.** Gehen Sie die Konfiguration durch, und ändern Sie den Wert für die Option *Geben Sie den Hostnamen des Websicherheitsdienstes* in **v2.sds.cisco.com ein.**
3. Standardwerte für alle anderen Optionen akzeptieren
4. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
5. Führen Sie den Befehl **Commit (Übernehmen)** aus, um alle Änderungen zu speichern.

AsyncOS 13.5 und höher (mit Cisco Talos Services)

Ab AsyncOS 13.5 für E-Mail-Sicherheit wurde die Cloud URL Analysis (CUA) eingeführt und die **websecurityadvanced config-**Optionen geändert. Da die URL-Analyse nun in der Talos-Cloud durchgeführt wird, ist der Hostname des Websicherheits-Services nicht mehr erforderlich. Diese wurde durch den Befehl **talosconfig** ersetzt. Diese Funktion steht nur in der Befehlszeile der ESA zur Verfügung.

```
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
```

Wenn Sie eine Stage-Lizenz verwenden, sollten Sie auf den Stage Server für Talos-Dienste verwiesen werden.

Sie können **Talosupdate** und **Talosstatus** ausführen, um eine Aktualisierung und den aktuellen Status aller Talos-basierten Services anzufordern.

Beispiel:

```
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
```

Weitere Informationen finden Sie im Benutzerhandbuch für AsyncOS 13.5 für Cisco Email Security Appliances.

Firewall-Einstellungen für den Zugriff auf Cisco Talos-Services

Sie müssen den HTTPS (Out) 443-Port der Firewall für die folgenden Hostnamen oder IP-Adressen öffnen (siehe Tabelle unten), um Ihr E-Mail-Gateway mit den Cisco Talos-Services zu verbinden.

Hostname	IPv4	IPv6
grpc.talos.cisco.com	112.62.0/24	2a04:e4c7:ffff:/48
email-sender-ip-rep-grpc.talos.cisco.com	112.63.0/24	2a04:e4c7:fffe:/48
serviceconfig.talos.cisco.com	112.255.0/24	-

Verfolgung von Webinteraktionen

Die Webinteraktionsüberwachungsfunktion liefert Informationen über die Endbenutzer, die auf neu geschriebene URLs geklickt haben, und über die Aktion (zugelassen, blockiert oder unbekannt), die jedem Benutzerklick zugeordnet ist.

Je nach Ihren Anforderungen können Sie die Verfolgung von Webinteraktionen auf einer der globalen Einstellungsseiten aktivieren:

1. Outbreak-Filter. Verfolgung von Endbenutzern, die durch Outbreak-Filter auf URLs umgeschrieben haben
2. URL-Filterung. Nachverfolgung von Endbenutzern, die auf URLs geklickt haben, die nach Richtlinien umgeschrieben wurden (mithilfe von Content- und Nachrichtenfiltern)

Wenn die Web-Interaktionsüberwachung konfiguriert und verwendet wird, muss nach der Umleitung einer Appliance zur Verwendung der Stadium-URL für Aktualisierungen die Appliance auch für die Verwendung des Staging-Aggregator-Servers konfiguriert werden:

1. Zugriff auf die Appliance über die CLI
2. Geben Sie den Befehl **aggregatorconfig ein.**
3. Geben Sie den folgenden Wert ein: **stage.aggregator.sco.cisco.com**
4. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
5. Führen Sie **Commit** aus, um alle Änderungen zu speichern.

Wenn der Aggregator nicht für die Bereitstellung konfiguriert ist, werden ähnliche Warnungen alle 30 Minuten über Admin-E-Mail-Warnungen angezeigt:

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

Oder durch Ausführen des Befehls **display alert** in der CLI:

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

Umkehren

Gehen Sie wie folgt vor, um zum Standard-Produktions-Aggregator-Server zurückzukehren:

1. Zugriff auf die Appliance über CLI
2. Geben Sie den Befehl **aggregatorconfig ein.**
3. Verwenden Sie den Befehl **EDIT**, und geben Sie den folgenden Wert ein: **aggregator.cisco.com**
4. Drücken Sie die Eingabetaste, bis Sie zur Hauptaufforderung zurückkehren.
5. Führen Sie den Befehl **Commit (Übernehmen)** aus, um alle Änderungen zu speichern.

Fehlerbehebung

Die Befehle zur Fehlerbehebung werden im Abschnitt "Überprüfen" dieses Dokuments aufgeführt.

Wenn beim Ausführen des Befehls **upgrade** Folgendes angezeigt wird:

```
Failure downloading upgrade list.
```

Überprüfen Sie, ob Sie den dynamischen Host geändert haben. Wenn dies so weitergeht, bitten und prüfen Sie, ob Ihre ESA oder SMA korrekt für Beta- oder Vorabtests bereitgestellt wurde.

Zugehörige Informationen

- vESA kann keine Updates für Antispam oder Antivirus herunterladen und anwenden.
- Technischer Support und Dokumentation - Cisco Systems