Cisco e-mail security en beveiligingsbeheer voor opslagupdates configureren

Inhoud

Inleiding

Dit document beschrijft het proces voor Beta-klanten en vooraf bevoorrade apparaten die voor het testen worden gebruikt, die moeten worden gemoderniseerd, AsyncOS-versies moeten verbeteren en updates moeten krijgen voor ESA en SMA die Beta en pre-release testen uitvoeren. Dit document heeft rechtstreeks betrekking op Cisco e-mail security applicatie (ESA) en Cisco Security Management-applicatie (SMA). Houd in gedachten dat de opslagservers niet door standaardproductieklanten voor ESA- of SMA-productie worden gebruikt. Het opslaan van OS releases, services regels en services motoren variëren van productie.

Houdt u er ook rekening mee dat de productievergunningen niet kunnen worden aangepast aan de Fase-introducties, aangezien zij niet in staat zijn de verificatie en de echtheidscontrole van de vergunning te behalen. Een productie-VLN heeft een waarde van een handtekening die is geschreven op het moment dat de licentie tijdens de productie wordt verleend, en die overeenkomt met de dienstverlening van de productievergunning. Niveau-licenties hebben een afzonderlijke handtekening die alleen voor de halveringsprestatie van de vergunning is geschreven.

Voorwaarden

Vereisten

1. De beheerder heeft voorafgaande communicatie ontvangen met betrekking tot de installatie of upgrades van het beta-systeem (pre-release OS).
2. Klanten die deelnemen aan Beta- en pre-release-testen hebben een bètaaanvraag voltooid en hebben vóór het begin van de bèta-test een non-openbaarmakingsovereenkomst gelezen en geaccepteerd.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Cisco e-mail security en beveiligingsbeheer voor opslagupdates configureren

> Opmerking: Klanten zouden alleen de URL's van de opslagserver moeten gebruiken als ze toegang hebben gekregen tot pre-provisioning via Cisco voor alleen Beta (pre-release OS) gebruik. Als u geen geldige licentie hebt voor Beta-gebruik, ontvangt uw apparaat geen updates van de geüploade update servers. Deze instructies mogen alleen worden gebruikt voor Beta-klanten of door beheerders die deelnemen aan Beta-tests.

Zo ontvangt u updates en upgrades:

Inloggen bij de GUI

1. Kies **Beveiligingsservices > Services updates > Instellingen voor bijwerken..**
2. Bevestig dat alle services zijn ingesteld om Cisco IronPort Update Server te gebruiken

Inloggen bij de CLI

1. Start de opdracht **update econfig**
2. Draai de verborgen **dynamiek** onder commando
3. Voer een van deze opdrachten in: Voor hardware ESA/SMA: **stadium-update-manifests.ironport.com:443**Voor Virtual ESA/SMA: **stage-stg-updates.ironport.com:443**
4. Druk op ENTER totdat u terugkeert naar de hoofdmelding
5. Voer **Commit in** om alle wijzigingen op te slaan

Verifiëren

Verificatie kan worden gezien in *update_logs* met communicatie die voor het juiste stadium URL slaagt. Voer in de CLI van het apparaat **grep stage update_logs in**:

```
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"
```

Als er onverwachte communicatiefouten zijn, voert u **<strong URL>**in om Domain Name Server (DNS) te controleren.

Voorbeeld:

```
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
```

Controleer dat het apparaat via poort 80 kan bellen en voer het **opdrachttelnet <stap URL> 80 uit**.

Voorbeeld:

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

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

omkeren

Voltooi de volgende stappen om terug te keren naar de standaard productieservers:

1. Voer de opdracht **update econfig in**
2. Geef de verborgen **dynamiek** onder opdracht op
3. Voer een van deze opdrachten in: Voor hardware ESA/SMA: **update-**

manifest.ironport.com:443 Voor Virtual ESA/SMA: **update-manifests.sco.cisco.com:443**
4. Druk op ENTER totdat u terugkeert naar de hoofdmelding
5. Start de opdracht **Commit** om alle wijzigingen op te slaan

Opmerking: Hardware toestellen (C1x0, C3x0, C6x0 en X10x0) mogen alleen de dynamische host-URL's van *stadium-update-manifest.ironport.com:443* of *update-manifsts.ironport.com:443* gebruiken. Indien er sprake is van een clusterconfiguratie met zowel ESA als vESA**, update econfig** moet op het niveau van de machine worden ingesteld en bevestigen dat de **dynamiek** vervolgens dienovereenkomstig wordt ingesteld.

URL-filtering

AsyncOS 13.0 en ouder

Als URL-filtering is ingesteld en in gebruik is op het apparaat, nadat een apparaat is omgeleid om stadium-URL te gebruiken voor updates, moet het apparaat ook worden geconfigureerd om de opslagserver te gebruiken voor URL-filtering:

1. Toegang tot het apparaat via de CLI
2. Typ de opdracht **websecurity geavanceerde configuratie** Stap door de configuratie en wijzig de waarde voor de optie *Voer de webbeveiligingsservice hostname* in op **v2.bèta.sds.cisco.com**
3. Wijzig de waarde voor de optie *Voer de drempelwaarde voor uitstaande aanvragen in* van de standaardinstelling van 50 tot **5**
4. Standaardwaarden voor alle andere opties accepteren
5. Druk op ENTER totdat u terugkeert naar de hoofdmelding
6. Start de opdracht **Commit** om alle wijzigingen op te slaan

omkeren

Voltooi de volgende stappen om terug te keren naar de beveiligingsservice van het productieweb:

1. Toegang tot het apparaat via CLI
2. Voer de opdracht **websecurity** in**, geavanceerde configuratie** Stap door de configuratie en wijzig de waarde voor de optie *Voer de webbeveiligingsservice hostname* in op **v2.sds.cisco.com**
3. Standaardwaarden voor alle andere opties accepteren
4. Druk op ENTER totdat u terugkeert naar de hoofdmelding
5. Start de opdracht **Commit** om alle wijzigingen op te slaan

AsyncOS 13.5 en nieuwer (met behulp van Cisco IOS-services)

Met ingang van AsyncOS 13.5 voor e-mail security is Cloud URL Analysis (CUA) geïntroduceerd en veranderd de opties **voor websecurity** bevorderde **configuratie**. Aangezien de URL analyse nu in de Talos cloud wordt uitgevoerd, is de Web security serviceshostname niet langer vereist. Dit is vervangen door het commando **talosfig**. Dit is alleen beschikbaar op de opdrachtregel van het 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
```

Als u een Niveau-licentie runt, dient u te worden verwezen naar de Niveau Server voor Talos services.

U kunt **talosupdate** en **talostatus** uitvoeren om een update en huidige status te vragen van alle door Talos geleide services.

Voorbeeld:

```
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
```

Zie de gebruikersgids voor AsyncOS 13.5 voor Cisco e-mail security applicaties.

Firewall-instellingen voor toegang tot Cisco-spraakservices

U moet HTTPS (Out) 443 poort op de firewall openen voor de volgende hostnamen of IP-adressen (raadpleeg de onderstaande tabel) om uw e-mailgateway te verbinden met Cisco Talos-services.

schuilnaam	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:fff:/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fff:/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

Web interactie-tracering

De webinteractie-tracking-functie biedt informatie over de eindgebruikers die op herschreven URL's hebben geklikt en de actie (toegestaan, geblokkeerd of onbekend) die met elke gebruikersklik is verbonden.

Afhankelijk van uw vereisten kunt u webinteractie volgen op een van de pagina's met mondiale instellingen inschakelen:

1. Afbraakfilters. Eindgebruikers aan het spoor die URLs herschreven door Ombraakfilters klikte
2. URL-filtering Eindgebruikers opsporen die URL's hebben geklikt die door beleid zijn herschreven (met behulp van content- en berichtfilters)

Als webinteractie-tracking wordt ingesteld en in gebruik is, nadat een apparaat is omgeleid naar het gebruik van URL in de fase voor updates, moet het apparaat ook worden geconfigureerd voor het gebruik van de opslagaggregator:

1. Toegang tot het apparaat via de CLI
2. Voer de opdrachtaggregatie in
3. Gebruik de opdracht EDIT en voer deze waarde in: **stage.aggregator.sco.cisco.com**
4. Druk op ENTER totdat u terugkeert naar de hoofdmelding
5. Start **Commit** om alle wijzigingen op te slaan

Als de Aggregator niet is ingesteld voor het opslaan, krijgt u elke 30 minuten dezelfde waarschuwingen te zien via Admin e-mailberichten:

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

Of door de opdracht **displays** op de CLI uit te voeren:

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

omkeren

Voltooi de volgende stappen om terug te keren naar de standaard productie-Aggregator-server:

1. Toegang tot het apparaat via CLI
2. Voer de opdrachtaggregatie in
3. Gebruik de opdracht **EDIT** en voer deze waarde in: **aggregator.cisco.com**
4. Druk op ENTER totdat u terugkeert naar de hoofdmelding
5. Start de opdracht **Commit** om alle wijzigingen op te slaan

Problemen oplossen

Opdrachten voor probleemoplossing worden in het gedeelte "Controleer" van dit document weergegeven.

Als u het volgende ziet tijdens het uitvoeren van de **upgrade-**opdracht:

```
Failure downloading upgrade list.
```

Controleer of u de dynamische host hebt gewijzigd. Als dit zo doorgaat, vraag en bevestig dan dat uw ESA of SMA correct is voorzien voor Bèta- of pre-release-testen.

Gerelateerde informatie

- vESA is niet in staat om updates voor Antispam of antivirus te downloaden en toe te passen
- Technische ondersteuning en documentatie – Cisco Systems