تكوين إدارة أمان البريد الإلكتروني وأمان البريد الإلكتروني من Cisco لتحديثات التشغيل المرحلي

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
تكوين إدارة أمان البريد الإلكتروني وأمان البريد الإلكتروني من Cisco لتحديثات التشغيل المرحلي
تسجيل الدخول إلى واجهة المستخدم الرسومية
تسجيل الدخول إلى واجهة سطر الأوامر
التحقق من الصحة
إرتداد
تصفية URL
AsyncOS 13.0 وما فوق
إرتداد
AsyncOS 13.5 والإصدارات الأحدث (باستخدام خدمات Cisco Talos)
إعدادات جدار الحماية للوصول إلى خدمات Cisco Telos
تعقب التفاعل عبر الويب
إرتداد
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا المستند العملية لعملاء الإصدار بيتا والأجهزة المزودة مسبقا المستخدمة للاختبار والتي تحتاج إلى ترقية إصدارات نظام التشغيل AsyncOS والحصول على تحديثات ل ESA و SMA التي تقوم بتشغيل الإصدار بيتا واختبار الإصدار الأولي. يتعلق هذا المستند مباشرة بأجهزة أمان البريد الإلكتروني من Cisco (ESA) وأجهزة إدارة الأمان من Cisco (SMA). تذكر دائما أنه لا يجب إستخدام خوادم التشغيل المرحلي من قبل عملاء الإنتاج القياسي ESA أو SMA للإنتاج. تختلف إصدارات نظام التشغيل المرحلي وقواعد الخدمات ومحركات الخدمات عن الإنتاج.

قبل أن تصبح كذلك، يرجى مراعاة أن تراخيص الإنتاج لن تتمكن من الترقية إلى إصدارات Stage لأنها غير قادرة على تمرير التحقق من الترخيص ومصادقته. تحتوي شبكة VLAN للإنتاج على قيمة توقيع مكتوبة عند الترخيص أثناء الإنشاء، والتي ستطابق خدمة ترخيص الإنتاج. تحتوي تراخيص المرحلة على توقيع منفصل مكتوب فقط لخدمة ترخيص التشغيل المرحلي.

المتطلبات الأساسية

المتطلبات

1. تلقى المسؤول اتصالا مسبقا فيما يتعلق بتثبيت أو ترقيات بيتا (نظام تشغيل ما قبل الإصدار).

2. وأكمل العملاء المشاركون في الاختبار التجريبي والتجريبي السابق للإصدار التجريبي تطبيق بيتا وقرأوا إتفاقا على عدم الإفصاح قبل بدء الإصدار التجريبي.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تكوين إدارة أمان البريد الإلكتروني وأمان البريد الإلكتروني من Cisco لتحديثات التشغيل المرحلي

ملاحظة: يجب على العملاء إستخدام عناوين URL الخاصة بخادم تحديث التشغيل المرحلي فقط في حالة تمكنهم من الوصول إلى الإعداد المسبق من خلال Cisco لاستخدام الإصدار بيتا (قبل إصدار نظام التشغيل) فقط. إذا لم يكن لديك ترخيص صالح مطبق لاستخدام الإصدار بيتا، فلن يتلقى الجهاز تحديثات من خوادم تحديث التشغيل المرحلي. يجب إستخدام هذه التعليمات فقط لعملاء الإصدار بيتا أو من قبل المسؤولين الذين يشاركون في إختبار الإصدار بيتا.

لتلقي تحديثات وترقيات التشغيل المرحلي:

تسجيل الدخول إلى واجهة المستخدم الرسومية

1. أختر **خدمات التأمين > تحديثات الخدمات > تحرير إعدادات التحديث..**
2. تأكيد تكوين جميع الخدمات لاستخدام خوادم تحديث Cisco IronPort

تسجيل الدخول إلى واجهة سطر الأوامر

1. تشغيل الأمر **updateConfig**
2. تشغيل الأمر الفرعي المخفي **dynamic ichost**
3. دخلت واحد من هذا أمر: بالنسبة للأجهزة ESA/SMA: **stage-update-**
manifests.ironport.com:443للحصول على بنية Virtual ESA/SMA: **stage-stg-**
updates.ironport.com:443
4. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
5. أدخل **الالتزام** لحفظ كافة التغييرات

التحقق من الصحة

يمكن ملاحظة التحقق في *updater_log* مع نجاح الاتصال لعنوان URL للمرحلة المناسبة. من واجهة سطر الأوامر (CLI) الموجودة على الجهاز، أدخل الأمر **grep stage updater_log**:

```
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
```

إذا كانت هناك أي أخطاء إتصالات غير متوقعة، فأدخل **بحث <stage url>**للتحقق من خادم اسم المجال (DNS).

مثال:

```
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
```

دققت أن الجهاز يستطيع أن يراقب عبر ميناء 80، يركض الأمر **telnet <stage url> 80**.

مثال:

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

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

إرتداد

للعودة إلى خوادم تحديث الإنتاج القياسية، أكمل الخطوات التالية:

1. دخلت الأمر **تحديث config**
2. إدخال الأمر الفرعي المخفي **dynamic ichost**
3. دخلت واحد من هذا أمر: بالنسبة للأجهزة **update-manifests.ironport.com:443** :ESA/SMAللحصول على بنية Virtual ESA/SMA: **update-manifests.sco.cisco.com:443**
4. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
5. قم بتشغيل الأمر **Commit** لحفظ جميع التغييرات

ملاحظة: يجب أن تستخدم أجهزة الأجهزة (C1x0 و C3x0 و C6x0 و X10x0) عناوين URL الخاصة بالمضيف الديناميكي *stage-update-manifests.ironport.com:443* أو *update-manifests.ironport.com:443*. في حالة وجود تكوين نظام مجموعة باستخدام الإيسا و vESA على حد سواء، يجب تكوين **updateConfig** على مستوى الجهاز والتأكيد من تعيين **dynamicHost** وفقا لذلك.

تصفية URL

AsyncOS 13.0 وما فوق

إذا تم تكوين تصفية URL وكانت قيد الاستخدام على الجهاز، بمجرد إعادة توجيه أحد الأجهزة لاستخدام URL المرحلة للتحديثات، فسيحتاج الجهاز أيضا إلى تكوين لاستخدام خادم التشغيل المرحلي لتصفية URL:

1. الوصول إلى الجهاز عبر واجهة سطر الأوامر (CLI)
2. دخلت الأمر **webSecurityAdvancedConfig** انتقل عبر التكوين وقم بتغيير قيمة الخيار *أدخل اسم مضيف خدمة أمان الويب* إلى **v2.beta.sds.cisco.com**
3. قم بتغيير قيمة الخيار *أدخل قيمة الحد للطلبات المعلقة* من القيمة الافتراضية 50 إلى **5**
4. قبول الافتراضيات لكل الخيارات الأخرى
5. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
6. قم بتشغيل الأمر **Commit** لحفظ جميع التغييرات

إرتداد

للعودة إلى خدمة أمان الويب للإنتاج، أكمل الخطوات التالية:

1. الوصول إلى الجهاز عبر CLI (واجهة سطر الأوامر)
2. أدخل الأمر **webSecurityAdvancedConfig** انتقل عبر التكوين وقم بتغيير قيمة الخيار *أدخل اسم مضيف خدمة أمان الويب* إلى **v2.sds.cisco.com**
3. قبول الافتراضيات لكل الخيارات الأخرى
4. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
5. قم بتشغيل الأمر **Commit** لحفظ جميع التغييرات

AsyncOS 13.5 والإصدارات الأحدث (باستخدام خدمات Cisco Talos)

بدءا من AsyncOS 13.5 لأمان البريد الإلكتروني، تم تقديم تحليل عنوان URL للسحابة (CUA) وتغيير خيارات **WebSecurityAdvancedConfig**. نظرا لأنه يتم الآن إجراء تحليل عنوان URL في سحابة Talos، لم يعد اسم المضيف لخدمات أمان الويب مطلوبا. تم إستبدال هذا الأمر **talosconfig**. وهذا متاح فقط على سطر أوامر 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
Stage Server .1
Production Server .2
1 <[]
```

إذا كنت تقوم بتشغيل ترخيص Stage، فيجب توجيهك إلى خادم Stage الخاص بخدمات Talos.

يمكنك تشغيل **Talosupdate** و**Talosstatus** لطلب تحديث والحالة الحالية لكافة الخدمات التي تم الاستناد إليها من Talos.

مثال:

```
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
```

لمزيد من المعلومات، راجع دليل المستخدم ل AsyncOS 13.5 لأجهزة أمان البريد الإلكتروني من Cisco.

إعدادات جدار الحماية للوصول إلى خدمات Cisco Telos

تحتاج إلى فتح منفذ 443 (Out) HTTPS على جدار الحماية لأسماء المضيف أو عناوين IP التالية (ارجع إلى الجدول أدناه) لتوصيل بوابة البريد الإلكتروني لديك بخدمات Cisco Telos.

اسم المضيف	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:/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

تعقب التفاعل عبر الويب

توفر ميزة تعقب التفاعل عبر الويب معلومات حول المستخدمين النهائيين الذين قاموا بالنقر فوق عناوين URL المعاد كتابتها والإجراء (مسموح به أو محظور أو غير معروف) المرتبط بكل نقرة للمستخدم.

حسب متطلباتك، يمكنك تمكين تتبع تفاعل الويب على أحد صفحات الإعدادات العامة:

1. عوامل تصفية التفشي. تعقب المستخدمين النهائيين الذين قاموا بالنقر فوق عناوين URL التي تمت إعادة كتابتها بواسطة عوامل تصفية التفشي
2. تصفية URL. تعقب المستخدمين النهائيين الذين قاموا بالنقر فوق عناوين URL المعاد كتابتها بواسطة النهج (باستخدام عوامل تصفية المحتوى والرسائل)

إذا تم تكوين تعقب تفاعل الويب وكان قيد الاستخدام، بمجرد إعادة توجيه جهاز لاستخدام عنوان URL للمرحلة للتحديثات، سيحتاج الجهاز أيضا إلى تكوين لاستخدام خادم "مجمع التشغيل المرحلي":

1. الوصول إلى الجهاز عبر واجهة سطر الأوامر (CLI)
2. دخلت الأمر **aggregationOrconfig**
3. أستخدم أمر تحرير وأدخل هذه القيمة: **stage.aggregator.sco.cisco.com**

4. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
5. قم بتشغيل **الالتزام** لحفظ جميع التغييرات

إذا لم يتم تكوين "المجمع" للتشغيل المرحلي، فسترى تنبيهات مماثلة كل 30 دقيقة من خلال تنبيهات البريد الإلكتروني للمسؤول:

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

أو، من خلال تشغيل الأمر **displayalerts** على واجهة سطر الأوامر:

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

إرتداد

للعودة إلى خادم مجمع الإنتاج القياسي، أكمل الخطوات التالية:

1. الوصول إلى الجهاز عبر CLI (واجهة سطر الأوامر)
2. دخلت الأمر **aggregationOrconfig**
3. أستخدم الأمر **edit** (تحرير) وأدخل هذه القيمة: **aggregator.cisco.com**
4. اضغط على المفتاح Enter حتى يتم إرجاعك إلى موجه الأمر الرئيسي
5. قم بتشغيل الأمر **Commit** لحفظ جميع التغييرات

استكشاف الأخطاء وإصلاحها

يتم سرد أوامر أستكشاف الأخطاء وإصلاحها في قسم "التحقق" في هذا المستند.

إذا كنت ترى ما يلي عند تشغيل الأمر **upgrade**:

```
.Failure downloading upgrade list
```

الرجاء التحقق من أنك قمت بتغيير المضيف الديناميكي. إذا استمر هذا، فيرجى الاستفسار والتحقق من أن ESA أو SMA لديك قد تم تزويده بشكل صحيح للحصول على بيتا أو إختبار ما قبل الإصدار.

معلومات ذات صلة

- [يتعذر على vESA تنزيل تحديثات مكافحة البريد العشوائي أو الفيروسات وتطبيقها]
- [الدعم التقني والمستندات - Cisco Systems]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).