ترقية الصورة ومعرفات التوقيع 4.1 إلى IPS 5.0 والإصدارات الأحدث (AIP-SSM، NM-IDs، IDSM-2) مثال التكوين

المحتويات

المقدمة

يوضح هذا المستند كيفية ترقية الصورة والتوقيع لبرنامج مستشعر اكتشاف الاقتحام (IDS) من الإصدار 4.1 إلى نظام منع الاقتحام (IPS) 5.0 من Cisco والإصدارات الأحدث.

ملاحظة: من الإصدار x.5 من البرنامج والإصدارات الأحدث، يستبدل Cisco IPS معرفات Cisco، والتي يتم تطبيقها حتى الإصدار 4.1.

ملاحظة: لا يمكن للمستشعر تنزيل تحديثات البرامج من Cisco.com. يجب تنزيل تحديثات البرامج من Cisco.com إلى خادم FTP، ثم تكوين المستشعر لتنزيلها من خادم FTP الخاص بك.

ارجع إلى قسم تثبيت صورة نظام AIP-SSM الخاص بالترقية والتخفيض وتثبيت صور النظام للإجراء.

ارجع إلى إجراء إسترداد كلمة المرور الخاصة بوحدات Cisco IDS Sensor and IDS Services Modules (IDSM-2، IDSM-1) لمعرفة المزيد حول كيفية إسترداد جهاز معرفات Cisco الآمنة (المعروف سابقا باسم NetRanger) والوحدات النمطية للإصدارات x.3 و x.4.

ملاحظة: لا تتأثر حركة مرور المستخدم أثناء الترقية في الإعداد **المضمن** والقابل **للفشل** على AIP-SSM - ASA.

ملاحظة: ارجع إلى قسم ترقية برنامج Cisco IPS من 5.1 إلى x.6 في تكوين مستشعر نظام منع التسلل من Cisco

باستخدام واجهة سطر الأوامر 6.0 للحصول على مزيد من المعلومات حول إجراء ترقية IPS 5.1 إلى الإصدار x.6.

ملاحظة: لا يدعم المستشعر الخوادم الوكيلة للتحديثات التلقائية. إعدادات الوكيل لميزة الارتباط العمومي فقط.

المتطلبات الأساسية

المتطلبات

الحد الأدنى لإصدار البرنامج المطلوب الذي تحتاج إليه للترقية إلى 5.0 هو 4.1(1).

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ال cisco 4200 sery IDS جهاز أن يركض برمجية صيغة 4،1 (أن يكون حسنت إلى صيغة 5،0).

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

تتوفر الترقية من Cisco 4.1 إلى 5.0 كتنزيل من Cisco.com. ارجع إلى الحصول على برنامج Cisco IPS للإجراء الذي تستخدمه للوصول إلى تنزيلات برامج IPS على Cisco.com.

يمكنك إستخدام أي من الطرق المدرجة هنا لإجراء الترقية:

- بعد تنزيل ملف ترقية 5.0، ارجع إلى الإجراء "قراءة" الخاص بكيفية تثبيت ملف ترقية 5.0 باستخدام الأمر **upgrade**. راجع قسم إستخدام الأمر upgrade في هذا المستند للحصول على مزيد من المعلومات.
- إذا قمت بتكوين التحديث التلقائي للمستشعر الخاص بك، فقم بنسخ ملف الترقية 5.0 إلى الدليل الموجود على الخادم الذي يقوم المستشعر بالبحث عن التحديثات. راجع قسم إستخدام أمر الترقية التلقائية في هذا المستند للحصول على مزيد من المعلومات.
- إذا قمت بتثبيت ترقية على جهاز الاستشعار الخاص بك وكان جهاز الاستشعار غير قابل للاستخدام بعد إعادة تمهيده، فيجب عليك إعادة تكوين جهاز الاستشعار الخاص بك. كما تتطلب ترقية مستشعر من أي إصدار من Cisco IDS أقدم من 4.1 إستخدام الأمر **recovery** أو القرص المضغوط الخاص بالاسترداد/الترقية. راجع قسم إعادة صورة المستشعر في هذا المستند للحصول على مزيد من المعلومات.

ترقية جهاز الاستشعار

توضح هذه الأقسام كيفية إستخدام الأمر **upgrade** لترقية البرنامج على المستشعر:

- نظرة عامة

نظرة عامة

يمكنك ترقية "أداة الاستشعار" باستخدام هذه الملفات، والتي تحتوي جميعها على الامتداد .pkg:

- تحديثات التوقيع، على سبيل المثال، IPS-SIG-S150-minreq-5.0-1.pkg
- تحديثات محرك التوقيع، على سبيل المثال، IPS-engine-E2-req-6.0-1.pkg
- التحديثات الرئيسية، على سبيل المثال، IPS-K9-MAJ-6. 0-1-PKG
- تحديثات بسيطة، على سبيل المثال، IPS-K9-min-5.1-1.pkg
- تحديثات حزمة الخدمة، على سبيل المثال، IPS-K9-SP-5.0-2.pkg
- تحديثات قسم الاسترداد، على سبيل المثال، IPS-K9-r-1.1-a-5.0-1.pkg
- إصدارات برامج التصحيح، على سبيل المثال، IPS-K9-patch-6.0-1p1-E1.pkg
- تحديثات قسم الاسترداد، على سبيل المثال، IPS-K9-r-1.1-a-6.0-1.pkg

تقوم ترقية المستشعر بتغيير إصدار البرنامج الخاص بالمستشعر.

أمر الترقية والخيارات

أستخدم الأمر **auto-upgrade-option enabled** في الوضع الفرعي لمضيف الخدمة لتكوين الترقيات التلقائية.

يتم تطبيق هذه الخيارات:

- **الافتراضي**—يعيد القيمة إلى الإعداد الافتراضي للنظام.
- **الدليل**—الدليل الذي توجد به ملفات الترقية على خادم الملفات.
- **بروتوكول نسخ الملفات**—بروتوكول نسخ الملفات المستخدم لتنزيل الملفات من خادم الملفات. القيم الصحيحة هي **ftp** أو **scp**.**ملاحظة:** إذا كنت تستخدم SCP، فيجب عليك إستخدام الأمر **ssh host-key** لإضافة الخادم إلى قائمة المضيفين المعروفة ل SSH حتى يمكن للمستشعر الاتصال به من خلال SSH. ارجع إلى إضافة مضيفين إلى قائمة المضيفين المعروفة للإجراء.
- **عنوان IP**—عنوان IP لخادم الملفات.
- **كلمة السر**—كلمة مرور المستخدم للمصادقة على خادم الملف.
- **خيار الجدول** الزمني - جداول عند حدوث ترقيات تلقائية. تبدأ جدولة التقويم الترقيات في أوقات محددة في أيام محددة. تبدأ الجدولة الدورية الترقيات على فترات دورية محددة.**جدول التقويم**—يقوم بتكوين أيام الأسبوع وأوقات اليوم التي يتم فيها إجراء الترقيات التلقائية.**أيام الأسبوع**—أيام الأسبوع التي يتم فيها إجراء عمليات الترقية التلقائية. يمكنك تحديد أيام متعددة. ومن الاحد إلى السبت هي القيم الصحيحة.**لا** — يزيل إعداد إدخال أو تحديد.**أوقات اليوم** - أوقات اليوم التي تبدأ فيها عمليات الترقية التلقائية. يمكنك تحديد عدة مرات. القيمة الصحيحة هي hh:mm[:ss].**جدولة دورية**—يقوم بتكوين الوقت الذي يجب أن تحدث فيه الترقية التلقائية الأولى ومدة الانتظار بين الترقيات التلقائية.**الفاصل الزمني**— عدد الساعات التي يجب الانتظار خلالها بين الترقيات التلقائية. القيم الصالحة هي من 0 إلى 8760.**وقت البدء** — الوقت من اليوم لبدء الترقية التلقائية الأولى. القيمة الصحيحة هي hh:mm[:ss].
- **اسم المستخدم**—اسم المستخدم للمصادقة على خادم الملف.

للحصول على إجراء IDM لترقية المستشعر، ارجع إلى تحديث المستشعر.

أستخدم الأمر upgrade

تتلقى أخطاء SNMP إذا لم يكن لديك معلمات **مجتمع للقراءة فقط** و**مجتمع للقراءة والكتابة** التي تم تكوينها قبل الترقية إلى IPS 6.0. إذا كنت تستخدم **مجموعة** SNMP و/أو **الحصول** على ميزات، فيجب تكوين معلمات **مجتمع للقراءة فقط** و**مجتمع للقراءة والكتابة** قبل الترقية إلى IPS 6.0. في IPS 5.x، تم تعيين **مجتمع للقراءة فقط** إلى

عام بشكل افتراضي، وتم تعيين **مجتمع للقراءة والكتابة** إلى خاص بشكل افتراضي. في IPS 6.0 لا يحتوي هذان الخياران على قيم افتراضية. إذا لم تكن تستخدم **حصول** SNMP على **مجموعات** باستخدام IPS 5.x، على سبيل المثال، تم تعيين enable-set-get على false، فلا توجد مشكلة في الترقية إلى IPS 6.0. إذا كنت تستخدم **الحصول** على SNMP و**تعيينه** باستخدام IPS 5.x، على سبيل المثال، تم تعيين enable-set-get على true، فيجب تكوين معلمات **مجتمع للقراءة فقط** و**مجتمع للقراءة والكتابة** إلى قيم معينة أو تفشل ترقية IPS 6.0.

تتلقى رسالة الخطأ هذه:

```
,Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true
 but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
.continue with null values in these fields
```

ملاحظة: ينكر IPS 6.0 الأحداث ذات المخاطر العالية بشكل افتراضي. هذا تغيير عن IPS 5.x. لتغيير الإعداد الافتراضي، قم بإنشاء تجاوز إجراء حدث للإجراء الوارد لرفض الحزمة وتكوينه ليتم تعطيله. إذا لم يكن المسؤول على علم بمجتمع القراءة والكتابة فيجب عليه محاولة تعطيل SNMP بالكامل قبل إجراء محاولة الترقية لإزالة رسالة الخطأ هذه.

أتمت هذا steps in order to حسنت المستشعر:

1. قم بتنزيل ملف التحديث الرئيسي (IPS-K9-maj-5.0-1-S149.rpm.pkg) إلى خادم FTP أو SCP أو HTTP أو HTTPS الذي يمكن الوصول إليه من جهاز الاستشعار الخاص بك.ارجع إلى الحصول على برنامج Cisco IPS للإجراء المتعلق بكيفية تحديد موقع البرامج على Cisco.com.**ملاحظة:** يجب عليك تسجيل الدخول إلى موقع Cisco.com باستخدام حساب ذي امتيازات تشفير لتنزيل الملف. لا تقم بتغيير اسم الملف. يجب الاحتفاظ باسم الملف الأصلي لكي يقبل "المستشعر" التحديث.**ملاحظة:** لا تغير اسم الملف. يجب الاحتفاظ باسم الملف الأصلي للمستشعر لقبول التحديث.
2. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
3. ادخل إلى وضع التكوين:
```
sensor#configure terminal
```

4. ترقية جهاز الاستشعار:
```
//:sensor(config)#upgrade scp
```

مثال:ملاحظة: يتم هذا الأمر في سطرين لأسباب مكانية.
```
/sensor(config)#upgrade scp://tester@10.1.1.1//upgrade
IPS-K9-maj-5.0-1-S149.rpm.pkg
```

ملاحظة: ارجع إلى الخوادم المدعومة على بروتوكول FTP و HTTP/HTTPS للحصول على قائمة بالخوادم التي تدعم بروتوكول FTP و HTTP/HTTPS. ارجع إلى إضافة مضيفين إلى قائمة مضيفات SSH المعروفة للحصول على مزيد من المعلومات حول كيفية إضافة خادم SCP إلى قائمة مضيفي SSH المعروفة.

5. أدخل كلمة المرور عند طلبها:
```
******** :Enter password
******** :Re-enter password
```
6. اكتب **نعم** لإكمال الترقية.**ملاحظة:** قد تؤدي التحديثات الرئيسية والتحديثات الثانوية وحزم الخدمات إلى فرض إعادة تشغيل عمليات نظام منع الاختراقات (IPS) أو حتى فرض إعادة تشغيل جهاز الاستشعار لإكمال التثبيت. يعني في انقطاع خدمة لمدة دقيقتين على الأقل. ومع ذلك، لا تتطلب تحديثات التوقيع إعادة التشغيل بعد إجراء التحديث. ارجع إلى تنزيل تحديثات التوقيع (العملاء المسجلون فقط) للحصول على آخر التحديثات.
7. التحقق من إصدار المستشعر الجديد:
```
sensor#show version
```

```
:Application Partition

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys

Platform: ASA-SSM-20

Serial Number: 021

No license present

.Sensor up-time is 5 days

(Using 490110976 out of 1984704512 bytes of available memory (24% usage

(system is using 17.3M out of 29.0M bytes of available disk space (59% usage

application-data is using 37.7M out of 166.6M bytes of
(available disk space (24 usage

(boot is using 40.5M out of 68.5M bytes of available disk space (62% usage

MainApp          2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

AnalysisEngine   2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

          CLI              2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600

:Upgrade History

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

#sensor
```

ملاحظة: بالنسبة ل IPS 5.x، تتلقى رسالة تفيد بأن الترقية من نوع غير معروف. يمكنك تجاهل هذه الرسالة.**ملاحظة:** يتم تعويض نظام التشغيل، كما تتم إزالة جميع الملفات التي تم وضعها على جهاز الاستشعار من خلال حساب الخدمة.

ارجع إلى تحديث المستشعر للحصول على مزيد من المعلومات حول إجراء IDM لترقية المستشعر.

تهيئة الترقيات التلقائية

الترقيات التلقائية

يمكنك تكوين أداة الاستشعار للبحث عن ملفات ترقية جديدة في دليل الترقية تلقائيا. على سبيل المثال، يمكن للعديد من أجهزة الاستشعار الإشارة إلى نفس دليل خادم FTP عن بعد مع جداول تحديث مختلفة، مثل كل 24 ساعة، أو يوم الاثنين والأربعاء والجمعة في الساعة 11:00 مساء.

يمكنك تحديد هذه المعلومات لجدولة الترقيات التلقائية:

- عنوان IP للخادم
- مسار الدليل على خادم الملفات حيث يقوم جهاز الاستشعار بالتحقق من ملفات الترقية
- بروتوكول نسخ الملفات (SCP أو FTP)
- اسم المستخدم وكلمة المرور
- جدول الترقية

يجب تنزيل ترقية البرامج من Cisco.com ونسخها إلى دليل الترقية قبل أن يتمكن المستشعر من إجراء الاستطلاع لإجراء عمليات الترقية التلقائية.

ملاحظة: إذا كنت تستخدم الترقية التلقائية باستخدام AIM-IPS وغيرها من أجهزة أو وحدات IPS، فتأكد من وضع كل من ملف ترقية 6.0(1) و IPS-K9-6.0-1-E1.pkg وملف ترقية IPS-AIM-K9-6.0-4-E1.pkg، AIM-IPS، على خادم التحديث التلقائي حتى يمكن ل AIM-IPS الكشف بشكل صحيح عن الملفات التي يلزم تنزيلها وتثبيتها تلقائيا. إذا وضعت ملف ترقية 6.0(1) فقط، IPS-K9-6.0-1-E1.pkg، على خادم التحديث التلقائي، يتم تنزيل AIM-IPS ويحاول تثبيته، وهو الملف غير الصحيح ل AIM-IPS.

ارجع إلى تحديث المستشعر تلقائيا للحصول على مزيد من المعلومات حول إجراء IDM للترقية التلقائية للمستشعر.

استعملت ال mise à niveau أمر

رأيت التحسين أمر وخيارات قسم من هذا وثيقة ل **ال mise à niveau** أمر.

أكمل الخطوات التالية لجدولة الترقيات التلقائية:

1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. قم بتكوين أداة الاستشعار للبحث تلقائيا عن ترقيات جديدة في دليل الترقية لديك.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#auto-upgrade-option enabled
```

3. تحديد الجدولة:لجدولة التقويم التي تبدأ الترقيات في أوقات محددة في أيام محددة:

```
sensor(config-hos-ena)#schedule-option calendar-schedule
sensor(config-hos-ena-cal#days-of-week sunday
sensor(config-hos-ena-cal#times-of-day 12:00:00
```

للجدولة الدورية التي تبدأ الترقيات على فترات دورية محددة:

```
sensor(config-hos-ena)#schedule-option periodic-schedule
sensor(config-hos-ena-per)#interval 24
sensor(config-hos-ena-per)#start-time 13:00:00
```

4. حدد عنوان IP الخاص بخادم الملفات:

```
sensor(config-hos-ena-per)#exit
sensor(config-hos-ena)#ip-address 10.1.1.1
```

5. حدد الدليل الذي توجد به ملفات الترقية على خادم الملفات:

```
sensor(config-hos-ena)#directory /tftpboot/update/5.0_dummy_updates
```

6. حدد اسم المستخدم للمصادقة على خادم الملفات:

```
sensor(config-hos-ena)#user-name tester
```

7. حدد كلمة مرور المستخدم:

```
sensor(config-hos-ena)#password

****** :[]Enter password
****** :Re-enter password
```

8. حدد بروتوكول خادم الملفات:

```
sensor(config-hos-ena)#file-copy-protocol ftp
```

ملاحظة: إذا كنت تستخدم SCP، فيجب عليك إستخدام الأمر **ssh host-key** لإضافة الخادم إلى قائمة المضيفين المعروفة ل SSH حتى يمكن للمستشعر الاتصال به من خلال SSH. ارجع إلى إضافة مضيفين إلى قائمة المضيفين المعروفة للإجراء.

9. دققت العملية إعداد:

```
sensor(config-hos-ena)#show settings

   enabled
   -----------------------------------------------
   schedule-option
   -----------------------------------------------
   periodic-schedule
   -----------------------------------------------
   start-time: 13:00:00
   interval: 24 hours
   -----------------------------------------------
   -----------------------------------------------
   ip-address: 10.1.1.1
   directory: /tftpboot/update/5.0_dummy_updates
   user-name: tester
   <password: <hidden
   file-copy-protocol: ftp default: scp
   -----------------------------------------------
#(sensor(config-hos-ena
```

10. خرجت mise à niveau submode:

```
sensor(config-hos-ena)#exit
sensor(config-hos)#exit

:[Apply Changes:?[yes
```

11. اضغط على **Enter** لتطبيق التغييرات أو اكتب **no** لتجاهلها.

إعادة تكوين صورة للمستشعر

يمكنك إعادة تصوير أداة الاستشعار الخاصة بك بهذه الطرق:

- بالنسبة لأجهزة IDS التي تحتوي على محرك أقراص مضغوطة، أستخدم القرص المضغوط الخاص بالاستعادة/الترقية.راجع قسم إستخدام القرص المضغوط للاسترداد/الترقية في ترقية صور النظام للإجراء

وتخفيضها وتثبيتها.
- بالنسبة لجميع أجهزة الاستشعار، أستخدم الأمر **recovery**.ارجع إلى قسم إسترداد قسم التطبيق في ترقية صور النظام وتخطيطها وتثبيتها للإجراء.
- بالنسبة لمعرف فئة المورد (IDS-4215 و IPS-4240 و IPS 4255)، أستخدم ROMMON لاستعادة صورة النظام.أحلت ال install ال IDS-4215 نظام صورة ويركب ال IPS-4240 و IPS-4255 نظام صورة قسم من يحسن، يخفض، ويثبت نظام صورة للإجراءات.
- بالنسبة ل NM-CIDS، أستخدم bootloader (أداة تحميل التمهيد).ارجع إلى قسم تثبيت صورة نظام NM-CIDS في ترقية صور النظام وترتيبها وتثبيتها للإجراء.
- بالنسبة ل IDSM-2، أعد تكوين قسم التطبيق من قسم الصيانة.راجع قسم تثبيت صورة نظام IDSM-2 من الترقية والتخفيض وتثبيت صور النظام الخاصة بالإجراء.
- ل AIP-SSM، reimage من ال ASA يستعمل ال **hw-module 1 إستعادة [يشكل | boot]** أمر.ارجع إلى قسم تثبيت صورة نظام AIP-SSM الخاص بالترقية والتخفيض وتثبيت صور النظام للإجراء.

معلومات ذات صلة

- صفحة دعم نظام منع الاقتحام من Cisco
- ترقية صور النظام ل IPS 6.0 وتخفيضها وتثبيتها
- صفحة دعم وحدة نظام اكتشاف الاقتحام من Cisco Catalyst 6500 Series الطراز (IDSM-2)
- إجراء إسترداد كلمة المرور الخاصة بوحدات IDSM-2، (Cisco IDS Sensor and IDS Services Modules 1
- أستكشاف أخطاء تحديثات التوقيع التلقائي وإصلاحها
- 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).