IPS 5.x و إلى الإصدارات الأحدث: NTP على مثال تكوين IPS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
التكوين
تكوين موجه Cisco ليكون خادم NTP
تكوين المستشعر لاستخدام مصدر وقت NTP
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يقدم هذا المستند نموذجا لتكوين مزامنة ساعة نظام منع التسلل الآمن (IPS) من Cisco باستخدام خادم وقت الشبكة باستخدام بروتوكول وقت الشبكة (NTP). تم تكوين موجه Cisco كخادم NTP وتم تكوين مستشعر IPS لاستخدام خادم NTP (موجه Cisco) كمصدر الوقت.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يجب أن يكون خادم NTP قابلا للوصول إليه من مستشعر Cisco IPS قبل بدء تكوين NTP هذا.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز Cisco 4200 Series IPS الذي يشغل الإصدار 7.0 من البرنامج والإصدارات الأحدث
- IME (Cisco IPS Manager Express)، الإصدار 7.0.1 والإصدارات الأحدث**ملاحظة:** بينما يمكن إستخدام IME لمراقبة أجهزة الاستشعار التي تعمل بنظام Cisco IPS 5.0 والإصدارات الأحدث، فإن بعض الميزات والوظائف الجديدة التي يتم توفيرها في IME مدعومة فقط على أجهزة الاستشعار التي تعمل بنظام Cisco IPS 6.1 أو إصدار أحدث.

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.

المنتجات ذات الصلة

أنت يستطيع أيضا استعملت هذا وثيقة مع هذا جهاز وبرمجية صيغة:

- جهاز Cisco 4200 Series IPS الذي يشغل إصدارات البرنامج 6.0 وما قبله
- Cisco IPS Manager Express (IME)، الإصدار 6.1.1

الاصطلاحات

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

التكوين

تكوين موجه Cisco ليكون خادم NTP

يتطلب المستشعر اتصالا مصدقا بخادم NTP إذا كان سيستخدم خادم NTP كمصدر للوقت. يدعم المستشعر خوارزمية تجزئة MD5 فقط لتشفير المفاتيح. أستخدم الإجراء التالي لتشيط موجه Cisco للعمل كخادم NTP واستخدام ساعته الداخلية كمصدر للوقت.

أكمل الخطوات التالية لإعداد موجه Cisco للعمل كخادم NTP:

1. قم بتسجيل الدخول إلى الموجه.
2. دخلت التشكيل أسلوب.
```
router#configure terminal
```

3. قم بإنشاء معرف المفتاح وقيمة المفتاح.
```
router(config)#ntp authentication-key key_ID md5 key_value
```

يمكن أن يكون معرف المفتاح رقما بين 1 و 65535. قيمة المفتاح هي نص (رقمي أو حرف). يتم تشفيرها لاحقا. على سبيل المثال:
```
router(config)#ntp authentication-key 12345 md5 123
```

ملاحظة: يدعم المستشعر مفاتيح MD5 فقط. قد تكون المفاتيح موجودة بالفعل على الموجه. أستخدم أمر التكوين **show running** للتحقق من وجود مفاتيح أخرى. يمكنك إستخدام هذه القيم للمفتاح الموثوق به في الخطوة 4.

4. قم بتعيين المفتاح الذي قمت بإنشائه للتو في الخطوة 3 كمفتاح موثوق به (أو أستخدم مفتاح موجود).
```
router(config)#ntp trusted-key key_ID
```

معرف المفتاح الموثوق به هو نفس رقم معرف المفتاح في الخطوة 3. على سبيل المثال:
```
router(config)#ntp trusted-key 12345
```

5. حدد الواجهة على الموجه التي سيتصل بها المستشعر.
```
router(config)#ntp source interface_name
```

على سبيل المثال:
```
router(config)#ntp source FastEthernet 1/0
```

6. حدد رقم الطبقة الأساسية ل NTP الذي سيتم تعيينه للمستشعر كما هو موضح هنا:
```
router(config)#ntp master stratum_number
```

على سبيل المثال:
```
router(config)#ntp master 6
```

ملاحظة: يعرف رقم الطبقة الرئيسية ل NTP الموضع النسبي للخادم في التدرج الهرمي ل NTP. يمكنك إختيار رقم بين 1 و 15. ليس من المهم للمستشعر إختيار الرقم.

تكوين المستشعر لاستخدام مصدر وقت NTP

أتمت ال steps في هذا قسم in order to شكلت المستشعر أن يستعمل ال NTP وقت مصدر (cisco مسحاج تخديد ال NTP وقت مصدر في هذا مثال).

يتطلب المستشعر مصدر وقت متناسق. يوصى باستخدام خادم NTP. أستخدم الإجراء التالي لتكوين المستشعر لاستخدام خادم NTP كمصدر للوقت الخاص به. يمكنك إستخدام بروتوكول وقت الشبكة (NTP) المصدق عليه أو غير المصدق عليه.

ملاحظة: بالنسبة ل NTP المصدق عليه، يجب الحصول على عنوان IP لخادم NTP ومعرف مفتاح خادم NTP وقيمة المفتاح من خادم NTP.

أتمت هذا steps in order to شكلت المستشعر أن يستعمل NTP نادل كمصدر الوقت:

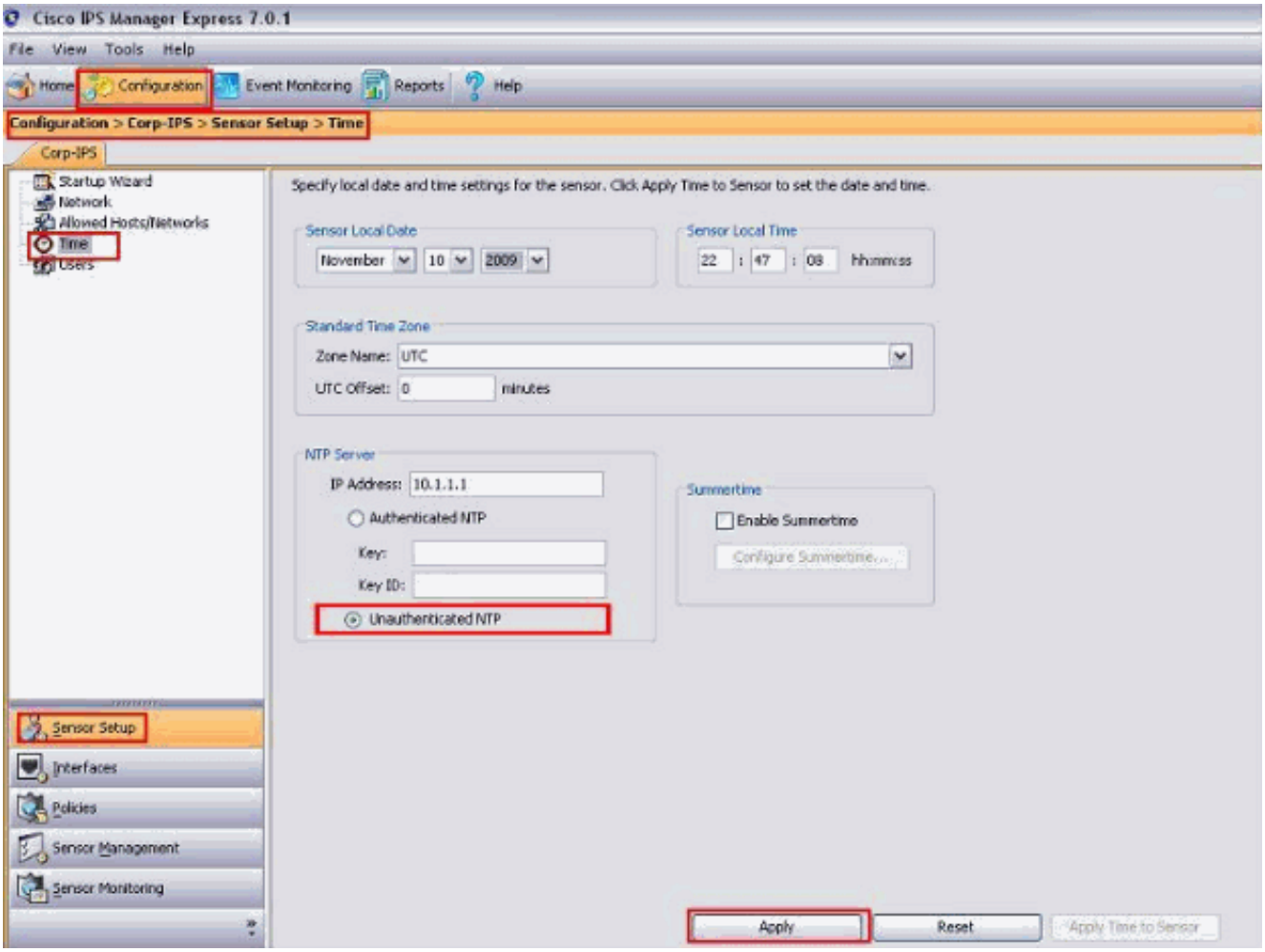
1. قم بتسجيل الدخول إلى CLI باستخدام حساب له امتيازات المسؤول.
2. دخلت التشكيل أسلوب كما هو موضح هنا:
```
sensor#configure terminal
```

3. أدخل وضع مضيف الخدمة.
```
sensor(config)# service host
```
4. يمكن تكوين NTP على أنه NTP مصدق وغير مصدق عليه.أتمت هذا steps in order to شكلت NTP غير مصدق:دخلت ال NTP تشكيل أسلوب.
```
sensor(config-hos)#ntp-option enabled-ntp-unauthenticated
```

حدد عنوان IP لخادم NTP.
```
sensor(config-hos-ena)#ntp-server ip_address
```

في هذا المثال، عنوان IP لخادم NTP هو 10.1.1.1.
```
sensor(config-hos-ena)#ntp-server 10.1.1.1
```

هذا هو الإجراء لتكوين NTP غير المصدق عليه باستخدام Cisco IPS Manager Express:أختر **تكوين > Corp-IPS > إعداد المستشعر > الوقت**. بعد ذلك، انقر فوق زر الراديو المجاور ل **NTP غير المصدق عليه** بعد توفير عنوان IP الخاص بخادم NTP كما هو موضح في لقطة الشاشة.طقطقة **يطبق**.



يؤدي هذا إلى اكتمال تكوين NTP غير المصدق عليه.أتمت هذا steps in order to شكلت NTP يصدق:دخلت ال NTP تشكيل أسلوب.

```
sensor(config-hos)#ntp-option enable
```

حدد عنوان IP الخاص بخادم NTP ومعرف المفتاح. معرف المفتاح هو رقم بين 1 و 65535. هذا هو معرف المفتاح الذي قمت بإعداده بالفعل على خادم NTP.

```
sensor(config-hos-ena)#ntp-servers ip_address key-id key_ID
```

في هذا المثال، عنوان IP لخادم NTP هو 10.1.1.1.

```
sensor(config-hos-ena)#ntp-server 10.1.1.1 key-id 12345
```

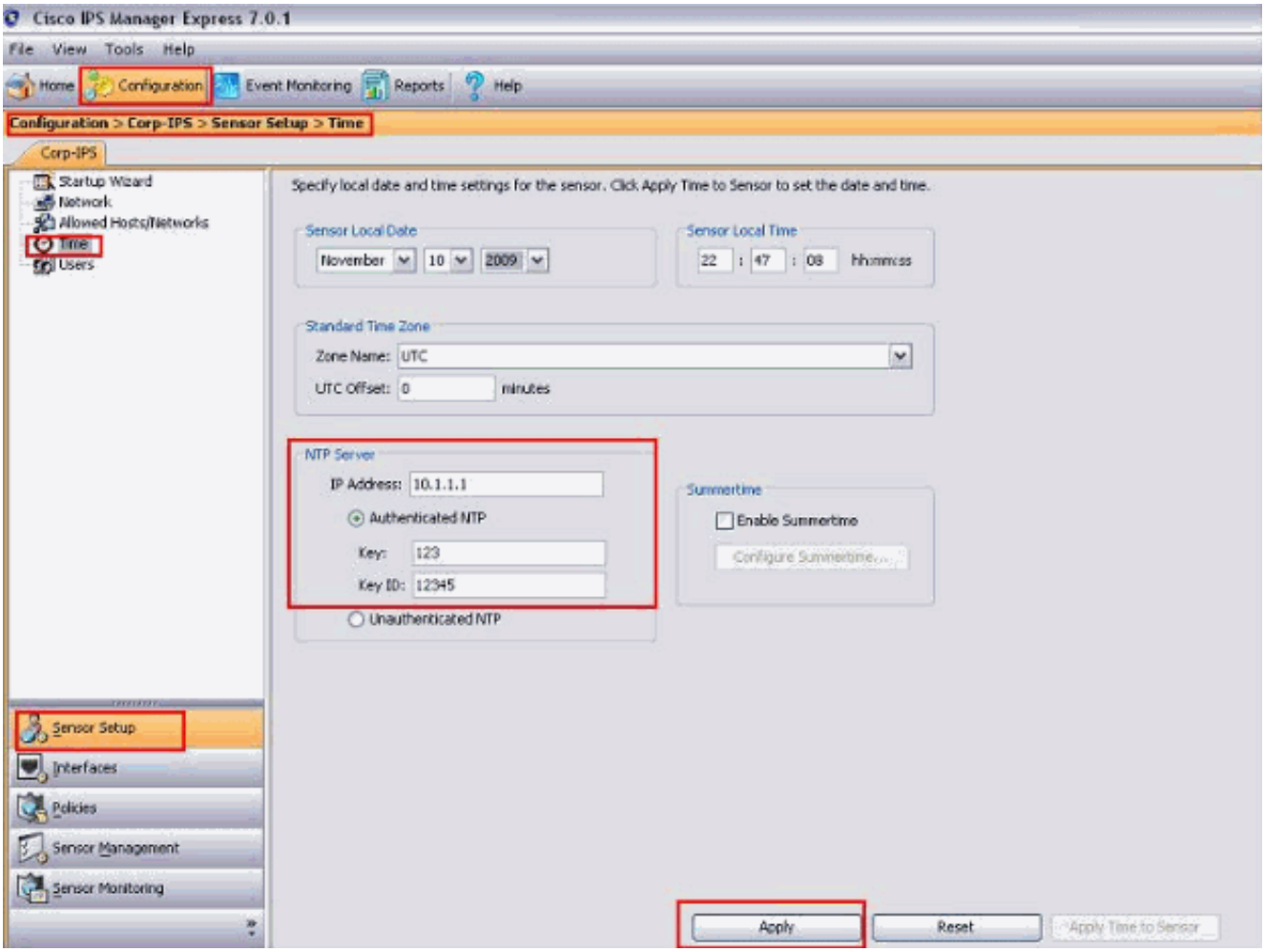
حدد خادم NTP الخاص بقيمة المفتاح.

```
sensor(config-hos-ena)#ntp-keys key_ID md5-key key_value
```

قيمة المفتاح هي نص (رقمي أو حرف). هذه هي القيمة الأساسية التي قمت بإعدادها بالفعل على خادم NTP. على سبيل المثال:

```
sensor(config-hos-ena)#ntp-keys 12345 md5-key 123
```

هذا هو الإجراء لتكوين NTP الذي تمت مصادقته باستخدام Cisco IPS Manager Express:أختر **تكوين > Corp-IPS > إعداد المستشعر > الوقت**. بعد ذلك، انقر فوق زر الراديو المجاور ل **NTP المصدق عليه** بعد أن تقوم بتوفير عنوان IP الخاص بخادم NTP كما هو موضح في لقطة الشاشة.قم بتوفير المفتاح ومعرف المفتاح اللذين يجب أن يكونا نفس الشيء المذكور في خادم NTP.في هذا المثال، يكون المفتاح 123 ومعرف المفتاح 12345.طقطقة **يطبق**.



يؤدي هذا إلى اكتمال تكوين NTP الذي تمت مصادقته.

5. خرجت NTP تشكيل أسلوب.

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

sensor(config-hos)# exit

[Apply Changes:?[yes
```

6. اضغط على **Enter** لتطبيق التغييرات أو أدخل **لا** لتجاهلها.يؤدي هذا إلى اكتمال مهمة التكوين.

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

دققت ال يصدق NTP عملية إعداد. وهذا يضمن تنفيذ تكوين NTP المصدق عليه بشكل صحيح.

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

                                                enabled

                ----------------------------------------------

                    (ntp-keys (min: 1, max: 1, current: 1

            ----------------------------------------------

                                                key-id: 12345

        ----------------------------------------------
```

```
                                        md5-key: 123

                    ----------------------------------------------

                    ----------------------------------------------

                           (ntp-servers (min: 1, max: 1, current: 1

                    ----------------------------------------------

                                    ip-address: 10.1.1.1

                                       key-id: 12345

                    ----------------------------------------------

                    ----------------------------------------------

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

لعرض محتويات التكوين الموجود في الوضع الفرعي الحالي، أستخدم الأمر show settings في وضع أمر الخدمة أي. وهذا يتحقق من تنفيذ تكوين NTP غير المصدق عليه بشكل صحيح.

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

                    enabled-ntp-unauthenticated

                  ----------------------------------------------

                                  ntp-server: 10.1.1.1

                  ----------------------------------------------

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

لعرض ساعة النظام، أستخدم الأمر show clock في وضع EXEC كما هو موضح. يوضح هذا المثال بروتوكول NTP الذي تم تكوينه ومزامنته:

```
sensor#show clock detail

CST Tues Jul 20 2011 11:45:02

Time source is NTP

#sensor
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- صفحة دعم نظام منع الاقتحام من Cisco
- صفحة الدعم السريع ل Cisco IPS Manager
- بروتوكول وقت الشبكة (NTP)

- طلبات التعليقات (RFCs)
- 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).