تكوين فشل مصادقة NTP على ISE 3.4 بسبب معالجة بادئات HEX

المحتويات

مسألة

يفشل Cisco Identity Services Engine (ISE) 3.4.0.608 Patch 1 في المزامنة مع خوادم NTP عند إستخدام NTP المصدق عليه مع مفاتيح SHA1 التي يبلغ طولها 40 حرفا. يتم قبول أوامر مفتاح مصادقة NTP على CLI دون خطأ، ولكن لا تحدث مزامنة NTP عند تمكين المصادقة. بدون المصادقة، تعمل مزامنة NTP بشكل صحيح. نجحت أجهزة الشبكة الأخرى، بما في ذلك محولات Cisco، في المصادقة باستخدام خادم NTP نفسه باستخدام معرف مفتاح وقيم مفتاح متطابقة.

أثناء أستكشاف الأخطاء وإصلاحها، كشف تحليل التقاط الحزم عن أن ISE يرسل طلبات NTP التي تمت مصادقتها مع معرف المفتاح المناسب وحقول MAC/المصدق، ومع ذلك، تحتوي ردود الخادم على معرف مفتاح من جميع الأصفار والوجود MAC/المصدق، مما يؤدي إلى فشل المصادقة. إخراج تصحيح الأخطاء على محولات Cisco التي تعمل كخوادم NTP يشير إلى "SHA1-Match: 0" معروض.

البيئة

- Cisco Identity Services Engine (ISE)، الإصدار 3.4.0.608 مع Patch 1
- مصادقة NTP باستخدام خوارزمية SHA1
- مفاتيح مصادقة NTP ذات 40 حرفا بالطول
- cisco مادة حفازة 9500 مفاتيح (C9500-24Y4C) ذات صيغة برنامج 17.12.04
- أجهزة خادم NTP مع تكوين NTP المصدق

رارق

سبب هذا إصدار ل cisco ق id: CSCwq79772، والذي يؤثر على كيفية معالجة ISE لمفاتيح مصادقة NTP الطويلة عندما تكون بادئة HEX مطلوبة. تم إصلاح هذه الخطأ في ISE 3.4 Patch 3 و ISE 3.5 Patch 8.

فهم السبب الرئيسي

عند تكوين مفاتيح مصادقة NTP على أجهزة Cisco، يتم التعامل تلقائيا مع المفاتيح التي تحتوي على 20 حرفا أو أكثر كسلاسل سداسية عشرية بدلا من النص العادي. وهذا يقبل، أظرا للخطأ، نظرا لأن ISE يتطلب من إستخدام البادئة "hex:" عند تكوين المفاتيح. ومع ذلك، ظهرت مشكلة في معالجة البادئة "hex:" الإضافية، مما يؤدي إلى فشل المصادقة.

خيارات الحل الفوري

حتى يمكن ترقية برنامج ISE إلى إصدار يحتوي على الإصلاح، أستخدم أحد هذه الحلول البديلة:

الخيار 1: إستخدام مفتاح SHA1 مكون من 36 حرفا

قم بتكوين كل من خادم NTP و ISE باستخدام مفتاح SHA1 مكون من 36 حرفا بدلا من المفتاح المكون من 40 حرفا.

على ISE:

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

على خادم NTP (مثال لمحول Cisco):

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
ntp trusted-key 1
```

الخيار 2: إستخدام مصادقة MD5

قم بالتبديل من مصادقة MD5، والتي لا تعرض نفس حدود الطول إلى مصادقة SHA1.

على ISE:

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

على خادم NTP:

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

خطوات التحقق

بعد تنفيذ أي من الحل البديل، تحقق من مزامنة NTP:

على ISE:

```
show ntp
show clock
```

على المحول (إذا كنت تستخدم المحول كخادم NTP):

```
show ntp associations
show ntp status
```

ابحث عن مؤشرات المزامنة الناجحة وتحقق من عمل المصادقة من خلال تأكيد فشل مزامنة NTP عند تعطيل المصادقة على جانب ولكن تمكينها على الجانب الآخر.

قرار دائم

ترقية ISE إلى أحد هذه الإصدارات التي تحتوي على إصلاح معرف تصحيح الأخطاء من Cisco: CSCwq79772:

- ISE 3.4 Patch 8 (عند توفرها)
- ISE 3.5 Patch 3 أو إصدار أحدث

بعد الترقية، يعمل تكوين المفتاح SHA1 الأصلي الذي يتكون من 40 حرفا بشكل صحيح مع بادئة HEX.

السبب

سبب هذا الإصدار ل cisco بق id: CSCwq79772، في إصدارات ISE قبل 3.4 تصحيح 8 و 3.5 تصحيح 3. عندما تكون مفاتيح مصادقة NTP 20 حرف أو أكثر، تتعامل أجهزة Cisco مع هذه كسلاسل سداسية عشرية، تتطلب البادئة "hex:" في التكوين. ونظرا لهذا الخطأ، يعالج ISE حساب طول المفتاح بشكل غير صحيح عند إستخدام بادئة HEX، حيث تقبل 36 حرفا فقط من مفتاح مكون من 40 حرفا. وهذا يؤدي إلى عدم تطابق المفاتيح بين ISE وخادم NTP، مما يؤدي إلى فشل المصادقة أثناء محاولات مزامنة NTP.

المحتوى ذي الصلة

- Cisco Bug CSCwq79772
- مرجع أوامر وحدة التحكم اللاسلكية من Cisco - مصادقة NTP
- الدعم الفني والتنزيلات من Cisco

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).