حل فشل الوصول المتقطع إلى SSH على أجهزة IOS XE الناتج عن الوضع الهادئ لكتلة تسجيل الدخول

المحتويات

مسألة

تعرض الأجهزة التي تشغل برنامج IOS XE حالات فشل في الوصول إلى SSH بشكل متقطع. يتم قبول إتصالات SSH في بعض الأحيان ويرفض في بعض الأحيان دون وجود نمط ثابت. ال يتأثر وصول وحدة التحكم إلى الأجهزة. بالنسبة لجلسة SSH فاشلة، تؤكد التقاط الحزم التي تم إجراؤها على الجهاز المتأثر أن الجهاز نفسه كان يرسل حزم TCP RST فورا عند تلقي نظام TCP للعميل، قبل أن تبدأ جلسة SSH حتى في التفاوض. مع تمكين حركات debug ip tcp للأمر، يوضح إخراج تصحيح الأخطاء التالي سلوك TCP RST:

```
Aug 21 19:46:04.697: Reserved port 0 in Transport Port Agent for TCP IP type 0
Aug 21 19:46:04.697: TCP: sending RST, seq 0, ack 1013312911
Aug 21 19:46:04.697: TCP: sent RST to 10.x.x.x:43266 from 10.x.x.x:22
Aug 21 19:46:04.698: Released port 0 in Transport Port Agent for TCP IP type 0 delay 0
Aug 21 19:46:04.698: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
Aug 21 19:46:04.698: TCB destroyed
```

تحقق من العناصر التالية لاستبعادها كأسباب مساهمة:

- أستخدم الأمر show ip ssh لتأكيد تمكين SSH على الجهاز.
- أستخدم الأمر show tcp brief لتأكيد أن منفذ TCP 22 يستمع داخل عملية IOSd.
- ال يوجد خطأ "no port" في إخراج الأمر show ip traffic أو debug ip error
- ال يتم إستهلاك خطوط vty بالكامل؛ ال يظهر إخراج الأمر من سطر العرض جميع الأسطر مشغولة.
- يبقى الإصدار بعد إزالة أي تكوين فئة الوصول على خطوط vty.

أظهر المخزن المؤقت لتسجيل الجهاز مستوى مرتفعا جدا من حالات فشل المصادقة المتكررة، بالإضافة إلى كون الوضع الهادئ نشطا:

```
Aug 21 12:24:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test_user] [Source: LOCAL] [localport: 
Aug 21 12:24:32: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs, [user: tes
```

يعرض إخراج show login في وقت الفشل الجهاز في الوضع الهادئ في وقت فشل SSH.

البيئة

- النظام الأساسي: المحولات Cisco Catalyst 9500 Series Switches (حزم المحولات المركزية والمحولات المدارة)
- تم تمكين SSH للوصول عن بعد إلى الجهاز
- تكوين كتلة تسجيل الدخول النشط على الجهاز: كتلة تسجيل الدخول - لـ 120 محاولة خلال 60 ثانية 3

رارق

تحدث هذه المشكلة بسبب تشغيل ميزة الوضع الهادئ لحظر تسجيل الدخول بشكل مستمر بواسطة عدد كبير من محاولات المصادقة الفاشلة. لحل المشكلة، أستخدم قائمة تحكم في الوصول (ACL) هادئة فئة الوصول لأجهزة الإدارة SSH الموثوق بها.

تكوين كتلة تسجيل الدخول باستخدام قائمة التحكم في الوصول (ACL) الموثوقة إلى IP في الوضع الهادئ

قم بتكوين ميزة كتلة تسجيل الدخول وتنفيذ قائمة تحكم في الوصول (ACL) من فئة التحكم في الوصول (قائمة التحكم في الوصول). تسمح قائمة التحكم في الوصول في الوضع الهادئ هذه للمضيفين الإداريين الموثوق بهم والشبكات الفرعية بتجاوز تنفيذ الوضع الهادئ لجميع المصادر الأخرى بينما تظل حماية كتلة تسجيل الدخول نشطة.

1. تحديد قائمة تحكم في الوصول (ACL) موسعة مسماة تتيح لمضيفي الإدارة الموثوق بهم والشبكات الفرعية. يسمح المثال التالي بنقطتي IP مضيف محددتين وشبكة فرعية واحدة /22 للإدارة. قم بضبط الإدخالات لتطابق مصادر الإدارة الموثوقة في البيئة:

```
device# configure terminal
device(config)# ip access-list extended quietmode_trusted_ip
device(config-ext-nacl)# 10 permit ip host <trusted_host_1_ip> any
device(config-ext-nacl)# 20 permit ip host <trusted_host_2_ip> any
device(config-ext-nacl)# 30 permit ip <subnet_address> <wildcard_mask> any
device(config-ext-nacl)# exit
```

بالنسبة لإنشاء قائمة التحكم في الوصول (ACL):

- أستخدم الكلمة الأساسية المضيف التي يتبعها عنوان IP واحد للسماح بمضيف إدارة محدد (على سبيل المثال، خادم انتقال).
- للسماح بشبكة فرعية بأكملها، حدد عنوان الشبكة متبوعا بقناع حرف البدل المناسب.

2. تطبيق قائمة التحكم في الوصول (ACL) على فئة الوصول في الوضع الهادئ حتى يسمح للمصادر التي تطابق قائمة التحكم في الوصول (ACL) بالاتصال حتى عندما يكون الوضع الهادئ نشطا:

```
device(config)# login quiet-mode access-class quietmode_trusted_ip
device(config)# end
```

3. إعادة تمكين أمر التكوين block-for لتسجيل الدخول في حالة إزالته:

```
device# configure terminal
device(config)# login block-for 120 attempts 3 within 60
device(config)# end
```

4. حفظ التكوين:

```
device# write memory
```

5. مراقبة سجل النظام لمعرفة ما إذا كان يستمر تشغيل الوضع الهادئ ووضع تسجيل الدخول الحالي:

```
device# show logging
device# show login
```

معالجة السبب الرئيسي لفشل المصادقة المتواصل

يتم) المعروف أعلاه الأعراض يعالج الحل المستند إلى قائمة التحكم في الوصول (ACL) ولكنه لا يعالج السبب الأساسي، وهو الحجم الكبير من حظر SSH من خلال الوضع الهادئ) حالات فشل المصادقة المتكررة. هذه الإخفاقات هي ما يؤدي باستمرار إلى تشغيل الوضع الهادئ. لحل هذه المشكلة بشكل كامل، يجب التحقق من مشكلة المصادقة المتكررة وحلها.

السبب

تتسبب ميزة حظر تسجيل الدخول إلى IOS-XE التي تدخل الوضع الهادئ في حالات فشل الوصول إلى SSH المتقطعة بسبب كثرة محاولات المصادقة الفاشلة المتكررة. مثال كتلة تسجيل الدخول للتكوين:

```
login block-for 120 attempts 3 within 60
```

يرشد هذا التكوين جهاز IOS XE لإدخال الوضع الهادئ وحظر جميع إتصالات تسجيل الدخول الجديدة لمدة 120 ثانية كلما تم اكتشاف 3 محاولات تسجيل دخول فاشلة أو أكثر داخل نافذة مدة 60 ثانية. يؤدي الحجم الكبير من محاولات المصادقة الفاشلة بشكل مستمر إلى تشغيل الوضع الهادئ لتسجيل الدخول. يعد فرض الوضع الهادئ عموميا ويطبق على جميع خطوط VTY وجميع منافذ TCP التي تم تكوينها ل SSH. عندما يكون الوضع الصامت نشطا، يرسل الجهاز حزمة TCP RST فورا عند تلقي حزمة TCP SYN جديدة من أي مصدر غير مسموح به بشكل صريح بواسطة قائمة التحكم في الوصول (ACL) من النوع Quiet-Mode access-class، مما يمنع إنشاء جلسة SSH.

المحتوى ذي الصلة

- [دليل تكوين أمان IOS-XE من Cisco: تحسينات تسجيل الدخول (فئة حظر تسجيل الدخول والوصول في الوضع الهادئ)]
- [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).