أستكشاف أخطاء مصادقة TACACS وإصلاحها

المحتويات

المقدمة

يصف هذا المستند الخطوات الرامية إلى أستكشاف أخطاء مصادقة TACACS وإصلاحها على الموجهات والمحولات Cisco IOS®/Cisco IOS® XE.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- تكوين المصادقة والتفويض والمحاسبة (AAA) على أجهزة Cisco
- تكوين TACACS

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 المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

كيفية عمل TACACS

يستخدم بروتوكول TACACS+ بروتوكول التحكم في الإرسال (TCP) كبروتوكول النقل مع منفذ الوجهة رقم 49. عندما يستقبل الموجه طلب تسجيل الدخول، فإنه يقوم بإنشاء اتصال TCP بخادم TACACS، ويقوم بنشر مطالبة اسم المستخدم التي يتم عرضها على المستخدم. عندما يدخل المستخدم اسم المستخدم، يتصل الموجه مرة أخرى بخادم TACACS لمطالبة كلمة المرور. بمجرد إدخال المستخدم لكلمة المرور، يرسل الموجه هذه المعلومات إلى خادم TACACS مرة أخرى. يتحقق خادم TACACS من بيانات اعتماد المستخدم ويرسل إستجابة مرة أخرى إلى الموجه. يمكن أن تكون نتيجة جلسة AAA أي مما يلي:

PASS: عند مصادقتك، تبدأ الخدمة فقط في حالة تكوين تفويض AAA على الموجه. تبدأ مرحلة التخويل في هذا الوقت.

فشل: عند فشل المصادقة، يمكن رفض مزيد من الوصول أو يمكنك إعادة محاولة تسجيل الدخول في التسلسل. يعتمد ذلك على برنامج TACACS+. وفي هذه الحالة، يمكن التحقق من السياسات التي تم تكوينها للمستخدم في خادم TACACS، إذا تم تلقي فشل من الخادم.

خطأ: يشير إلى حدوث خطأ أثناء المصادقة. يمكن أن يكون هذا إما في البرنامج الخفي أو في اتصال الشبكة بين البرنامج الخدمي والموجه. إذا تم تلقي إستجابة خطأ، يحاول الموجه عادة إستخدام طريقة بديلة لمصادقة المستخدم.

هذه هي التكوينات الأساسية من AAA و TACACS على موجه Cisco.

```
aaa new-model

aaa authentication log in default group tacacs+ local

aaa authorization exec default group tacacs+ local

!

tacacs server prod

address ipv4 10.106.60.182

key cisco123

!

ip tacacs source-interface Gig 0/0
```

أستكشاف أخطاء TACACS وإصلاحها

الخطوة 1.

تحقق من الاتصال بخادم TACACS باستخدام برنامج Telnet على المنفذ 49 من الموجه باستخدام واجهة المصدر المناسبة. في حالة عدم قدرة الموجه على الاتصال بخادم TACACS على المنفذ 49، يمكن أن يكون هناك بعض جدار الحماية أو قوائم الوصول التي تمنع حركة المرور.

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

الخطوة 2.

تحقق من تكوين عميل AAA بشكل صحيح على خادم TACACS باستخدام عنوان IP الصحيح والمفاتيح السري المشترك. إذا كان الموجه يحتوي على واجهات صادرة متعددة، فيوصى بتكوين واجهة مصدر TACACS باستخدام هذا الأمر. يمكنك تكوين الواجهة، التي تم تكوين عنوان IP الخاص بها كعنوان IP للعميل على خادم TACACS، كواجهة مصدر TACACS على الموجه

```
Router(config)#ip tacacs source-interface Gig 0/0
```

الخطوة 3.

تحقق مما إذا كانت واجهة مصدر TACACS على توجيه وإعادة توجيه ظاهريين (VRF). في حالة إذا كانت الواجهة على VRF، فيمكنك تكوين معلومات VRF ضمن مجموعة خوادم AAA. ارجع إلى دليل تكوين TACACS لتكوين TACACS المدركة لبروتوكول VRF.

الخطوة 4.

قم بإجراء إختبار المصادقة والتفويض والمحاسبة (AAA) وتحقق من تلقي الاستجابة الصحيحة من الخادم.

```
Router#test aaa  group tacacs+ cisco cisco legacy
Sending password
User successfully authenticated
```

الخطوة 5.

إذا فشل Test AAA، قم بتمكين عمليات تصحيح الأخطاء هذه مع التحليل الرحلات بين الموجه وخادم TACACS لتحديد السبب الجذري.

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

هذا نموذج إخراج تصحيح الأخطاء في سيناريو عمل:

```
*Apr  6 13:32:50.462: AAA/BIND(00000054): Bind i/f
*Apr  6 13:32:50.462: AAA/AUTHEN/LOGIN (00000054): Pick method list 'default'
*Apr  6 13:32:50.462: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:50.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:50.462: TPLUS: processing authentication start request id 84
```

```
*Apr  6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr  6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr  6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
*Apr  6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr  6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:53.242: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:53.242: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr  6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr  6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr  6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:54.454: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr  6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr  6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr  6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr  6 13:32:54.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr  6 13:32:54.462: TPLUS: Protocol set to None .....Skipping
*Apr  6 13:32:54.462: TPLUS: Sending AV service=shell
*Apr  6 13:32:54.462: TPLUS: Sending AV cmd*
*Apr  6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr  6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr  6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr  6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful
```

هذا نموذج إخراج تصحيح أخطاء من الموجه عند تكوين خادم TACACS باستخدام مفتاح مشترك مسبقا غير صحيح.

```
*Apr  6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr  6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr  6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr  6 13:35:07.826: TPLUS(00000055) log in timer started 1020 sec timeout
*Apr  6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr  6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr  6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr  6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr  6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr  6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr  6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

معلومات ذات صلة

- تكوين TACACS على Cisco IOS
- 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).