ةقداصم مادختساب Cisco موجم نيوكت TACACS+

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين موجه Cisco للمصادقة باستخدام TACACS+ الذي يتم تشغيله على UNIX. لا يقدم TACACS+ عدد ميزات ACS الآمن من Cisco المتوفر تجاريا ل Windows أو Cisco Secure ACS UNIX.

تم إيقاف تشغيل برنامج TACACS+ الذي كان موفرا من قبل Cisco Systems ولم يعد مدعوما من قبل Cisco Systems.

اليوم، يمكنك العثور على العديد من إصدارات البرامج المجانية ل TACACS+ المتوفرة عند البحث عن "TACACS+ مجاني" على محرك البحث المفضل لديك عبر الإنترنت. لا توصي Cisco بشكل خاص بتنفيذ أي برنامج مجاني TACACS+ خاص.

يتوفر خادم التحكم في الوصول الآمن (ACS) من Cisco للشراء من خلال قنوات المبيعات والتوزيع العادية من Cisco في جميع أنحاء العالم. يتضمن مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows جميع المكونات اللازمة للتثبيت المستقل على محطة عمل تعمل بنظام التشغيل Microsoft Windows. يتم شحن محرك حلول ACS الآمن من Cisco باستخدام ترخيص برنامج Cisco Secure ACS المثبت مسبقا. قم بزيارة الصفحة الرئيسية لطلب الشراء من Cisco (العملاء المسجلون فقط) لتقديم طلب شراء.

ملاحظة: تحتاج إلى حساب CCO مع عقد خدمة مرتبط للحصول على إصدار تجريبي لمدة 90 يوما ل Cisco Secure ACS ل Windows.

تم تطوير تكوين الموجه في هذا المستند على موجه يعمل ببرنامج Cisco IOS® Software، الإصدار 11.3.3. يستخدم برنامج Cisco IOS الإصدار T.12.0.5 والإصدارات الأحدث **TACACS+** المجموعة بدلا من **TACACS+**، لذلك تظهر عبارات مثل **مصادقة AAA تسجيل الدخول الافتراضي ل TACACS+ enable** ك **AAA تسجيل الدخول الافتراضي للمجموعة TACACS+ enable**.

راجع وثائق برنامج Cisco IOS Software للحصول على مزيد من المعلومات الكاملة حول أوامر الموجه.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco IOS الإصدار 11.3.3 وبرنامج Cisco IOS الإصدار T.12.0.5 والإصدارات الأحدث.

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.

الاصطلاحات

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

المصادقة

أكمل الخطوات التالية:

1. تأكد من تحويل رمز TAC) +TACACS+) برمجيا على خادم UNIX.يفترض الخادم تشكيل هنا أن أنت تستخدم ال cisco+ TAC نادل رمز. يجب أن تعمل تكوينات الموجه سواء كان رمز الخادم هو رمز خادم Cisco أم لا. يجب تشغيل TAC+ كجذر، إذا لزم الأمر، إذا كان الجذر الجذر.
2. انسخ test_file في نهاية هذا المستند، ووضعه على خادم TAC+، واسمه **test_file**.تحقق للتأكد من أن البرنامج الخفي **TAC_PLUS_EXECUTABLE** يبدأ ب **test_file**. في هذا أمر، يتحقق خيار **-P** من أخطاء التحويل البرمجي ولكنه لا يبدأ الخيط:
```
tac_plus_executable -P -C test_file
```
قد ترى محتويات الاختبار_file التمرير لأسفل النافذة، ولكن لا يجب أن ترى رسائل مثل أو —تم العثور على نص واضح أو }. إذا كانت هناك أخطاء، تحقق من المسارات لاختبار_file، وأعد التحقق من كتابتك، وأعد الاختبار قبل المتابعة.
3. بدء تكوين TAC+ على الموجه.أدخل وضع **enable** واكتب **configure terminal** قبل مجموعة الأوامر. تضمن صياغة الأمر هذه عدم قفل حسابك من الموجه في البداية، مما يوفر عدم تشغيل **TAC_PLUS_EXECUTABLE**:

```
*Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of ---!
*authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are*
*names of lists, and the methods !--- listed on the same lines are the methods !--- in the*
*order to be tried. As used here, if !--- authentication fails due to the !---*
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
.is in each list

!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable
!
*Point the router to the server, where #.#.#.# !--- is the server IP address.* ! *---!*
tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being*
```

```
locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8
login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400
     flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being
          locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```

4. قم بإجراء إختبار للتأكد من إستمرار إمكانية الوصول إلى الموجه باستخدام برنامج Telnet ومن خلال منفذ وحدة التحكم قبل المتابعة. يجب قبول كلمة مرور **enable** لأن **tac_plus_executable** لا يعمل.**ملاحظة:** الحفاظ على تنشيط جلسة عمل منفذ وحدة التحكم والبقاء في وضع التمكين. يجب ألا تنتهي مدة هذه الجلسة. الوصول إلى الموجه محدود في هذه المرحلة، ويجب أن تكون قادرا على إجراء تغييرات التكوين دون قفل نفسك.أصدرت هذا أمر أن يرى نادل إلى مسحاج تخديد تفاعل في المسحاج تخديد:

```
terminal monitor
debug aaa authentication
```

5. كجذر، ابدأ TAC+ على الخادم:

```
tac_plus_executable -C test_file -d 16
```

6. تحقق للتأكد من بدء TAC+:

```
ps -aux | grep tac_plus_executable
```

أو

```
ps -ef | grep tac_plus_executable
```

إذا لم يبدأ TAC+، فإنه عادة ما يكون مشكلة في الصيغة في test_file. ارجع إلى الخطوة 1 لتصحيح هذا الأمر.

7. اكتب **tail -f /var/tmp/tac_plus.log** للاطلاع على تفاعل الموجه مع الخادم في الخادم.**ملاحظة:** يرسل خيار - D 16 في الخطوة 5 ناتج جميع الحركات إلى /var/tmp/tac_plus.log.
8. يجب أن يكون على مستخدمي VTY) Telnet) الآن المصادقة من خلال TAC+.مع إستمرار تصحيح الأخطاء على الموجه والخادم (الخطوات 4 و 7)، يدخل Telnet إلى الموجه من جزء آخر من الشبكة.ينتج الموجه اسم مستخدم وكلمة مرور، والذي ترد عليه:

```
(authenuser'   (username from test_file'
    (admin'   (password from test_file'
```

المستخدم `authenuser` موجود في المجموعة، والذي يحتوي على كلمة المرور `admin`.راقب الخادم والموجه حيث يمكنك رؤية تفاعل TAC+-ما يتم إرساله حيث والاستجابة والطلبات وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.

9. إن يريد أنت أيضا مستعملك أن يصدق من خلال TAC+ in order to دخلت إلى enable أسلوب، تأكدت أن وحدة طرفية للتحكم ميناء جلسة ما تزال نشط وأضفت هذا أمر إلى المسحاج تخديد:

```
For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does ---!
not run. aaa authentication enable default tacacs+ enable
```

يجب على المستخدمين الآن التمكين من خلال TAC+.

10. مع إستمرار تصحيح الأخطاء على الموجه والخادم (الخطوات 4 و 7)، يدخل Telnet إلى الموجه من جزء آخر من الشبكة. ينتج الموجه اسم مستخدم وكلمة مرور، والذي ترد عليه:

```
(authenuser'   (username from test_file'
    (admin'   (password from test_file'
```

عندما تدخل وضع التمكين، يطلب الموجه كلمة مرور، ترد عليها:

```
(cisco'  ($enable$ password from test_file'
```

راقب الخادم والموجه حيث يجب أن ترى تفاعل TAC+ - ما يتم إرساله حيث تتم الاستجابات والطلبات وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.

11. قم بتنزيل عملية TAC+ على الخادم أثناء إتصالك بمنفذ وحدة التحكم للتأكد من إستمرار قدرة المستخدمين على الوصول إلى الموجه إذا كان TAC+ معطلا:

```
ps -aux | grep tac_plus_executable
```

أو

```
(ps -ef | grep tac_plus_executable
kill -9 pid_of_tac_plus_executable
```

كرر Telnet وتمكين الخطوة السابقة. يدرك الموجه بعد ذلك أن عملية TAC+ لا تستجيب وتسمح للمستخدمين بتسجيل الدخول والتمكين باستخدام كلمات المرور الافتراضية.

12. تحقق من مصادقة مستخدمي منفذ وحدة التحكم الخاصة بك من خلال TAC+. للقيام بهذا الإجراء، قم بإحضار خادم TAC+ مرة أخرى (الخطوات 5 و 6)، وإنشاء جلسة عمل برنامج Telnet للموجه (الذي يجب أن

يصدق من خلال TAC+).ابق متصلا من خلال Telnet في الموجه في وضع التمكين حتى تتأكد من أنك تستطيع تسجيل الدخول إلى الموجه من خلال منفذ وحدة التحكم.قم بتسجيل الخروج من الاتصال الأصلي بالموجه من خلال منفذ وحدة التحكم، ثم قم بإعادة الاتصال بمنفذ وحدة التحكم. يجب أن تكون مصادقة منفذ وحدة التحكم لتسجيل الدخول والتمكين باستخدام معرفات المستخدم وكلمات المرور (الموضحة في الخطوة 10) الآن من خلال TAC+.

13. بينما تظل متصلا إما من خلال جلسة عمل على برنامج Telnet أو منفذ وحدة التحكم ومع إستمرار تصحيح الأخطاء على الموجه والخادم (الخطوات 4 و 7)، قم بإنشاء اتصال مودم بالسطر 1.يجب على مستخدمي الخط الآن تسجيل الدخول والتمكين من خلال TAC+.ينتج الموجه اسم مستخدم وكلمة مرور، والذي ترد عليه:

```
(authenuser'   (username from test_file'
     (admin'   (password from test_file'
```

عندما تدخل وضع التمكين، يطلب الموجه كلمة مرور.رد:

```
(cisco'   ($enable$ password from test_file'
```

راقب الخادم والموجه حيث ترى تفاعل TAC+ - ما يتم إرساله حيث والاستجابة والطلبات وما إلى ذلك. قم بتصحيح أي مشاكل قبل المتابعة.يجب على المستخدمين الآن التمكين من خلال TAC+.

إضافة تخويل

تعد إضافة التخويل أمرا إختياريا.

بشكل افتراضي، هناك ثلاثة مستويات أوامر على الموجه:

- مستوى الامتياز 0 الذي يتضمن تعطيل، تمكين، إنهاء، تعليمات، وتسجيل الخروج
- امتياز مستوى 1 - عادي مستوى على telnet - رسالة حث يقول >
- امتياز مستوى 15 - enable مستوى - رسالة حث يقول #

بما أن الأوامر المتاحة تعتمد على مجموعة ميزات IOS، إصدار من Cisco IOS، طراز الموجه، وما إلى ذلك، فلا توجد قائمة شاملة لجميع الأوامر على المستويين 1 و 15. على سبيل المثال، **لا يكون show ipx route** موجودا في مجموعة ميزات IP فقط، و**show ip nat trans** ليس في برنامج Cisco IOS الإصدار x.10.2 لأن NAT لم يتم تقديمه في ذلك الوقت، و**show environment** غير موجودة في نماذج الموجهات دون مصدر الطاقة ومراقبة درجة الحرارة. يمكن العثور على الأوامر المتوفرة في موجه معين على مستوى معين عند إدخال ؟ في موجه الأمر في الموجه عندما تكون على مستوى الامتياز هذا.

لم تتم إضافة تفويض منفذ وحدة التحكم كميزة حتى يتم تنفيذ معرف تصحيح الأخطاء من Cisco CSCdi82030 (العملاء المسجلون فقط). يكون تفويض منفذ وحدة التحكم قيد الإيقاف بشكل افتراضي لتقليل أحتمالية أنك تصبح مؤمنا عن طريق الخطأ خارج الموجه. إذا كان للمستخدم وصول فعلي إلى الموجه من خلال وحدة التحكم، فإن تفويض منفذ وحدة التحكم ليس فعالا للغاية. مهما، وحدة طرفية للتحكم ميناء يستطيع كنت شغلت تحت خط `con 0` في صورة أن cisco بق CSCdi82030 id (يسجل زبون فقط) طبقت في مع الأمر:

```
authorization exec default|WORD
```

1. يمكن تكوين الموجه لتخويل الأوامر من خلال TAC+ على جميع المستويات أو بعض المستويات.يتيح تكوين الموجه هذا لجميع المستخدمين إعداد التفويض لكل أمر على الخادم. هنا نقوم بتخويل جميع الأوامر من خلال TAC+، ولكن إذا كان الخادم معطلا، فلا يلزم أي تفويض.

```
aaa authorization commands 1 default tacacs+ none
aaa authorization commands 15 default tacacs+ none
```

2. أثناء تشغيل خادم TAC+، يعمل برنامج Telnet في الموجه باستخدام **authenuser** لمعرف المستخدم.نظرا لأن AuthUser لديه الخدمة الافتراضية = السماح في test_file، يجب أن يكون هذا المستخدم قادرا على تنفيذ جميع الوظائف.دخلت بينما في المسحاج تخديد، **enable** أسلوب، وشغل تخويل تصحيح:

```
terminal monitor
debug aaa authorization
```

3. يدخل Telnet في المسحاج تخديد مع **مستعمل** وكلمة **مشغل**.لا يمكن لهذا المستخدم تنفيذ أمري show **traceroute** و**logout** (راجع test_file).راقب الخادم والموجه حيث يجب أن ترى تفاعل TAC+ (ما يتم إرساله

حيث، والاستجابات، والطلبات، وما إلى ذلك). قم بتصحيح أي مشاكل قبل المتابعة.
4. إذا كنت ترغب في تكوين مستخدم لأمر تلقائي، فقم بإزالة عبارات المستخدم التي تم التعليق عليها في test_file، وقم بوضع وجهة عنوان IP صالحة بدلا من #.#.#.#.قم بإيقاف تشغيل خادم TAC+.على الموجه:
```
+aaa authorization exec default tacacs
```
Telnet إلى الموجه مع معرف المستخدم **المؤقت** وكلمة المرور **العابرة**. يتم إرسال برنامج **telnet #.#.#.** **عمليات التنفيذ** وفترة انتقال المستخدم إلى الموقع الآخر.

إضافة محاسبة

إضافة المحاسبة أمر إختياري.

المرجع إلى ملف المحاسبة في test_file - ملف المحاسبة = /var/log/tac.log. ولكن لا تتم المحاسبة ما لم يتم تكوينها في الموجه (شريطة أن يقوم الموجه بتشغيل إصدار من برنامج Cisco IOS Software بعد الإصدار 11.0).

1. تمكين المحاسبة في الموجه:
```
+aaa accounting exec default start-stop tacacs
+aaa accounting connection default start-stop tacacs
+aaa accounting network default start-stop tacacs
+aaa accounting system default start-stop tacacs
```
ملاحظة: لا تقوم محاسبة AAA بالمحاسبة لكل أمر في بعض الإصدارات. الحل البديل هو إستخدام التفويض لكل أمر وتسجيل التكرار في ملف المحاسبة. (راجع معرف تصحيح الأخطاء من CSCdi44140 Cisco.) إذا كنت تستخدم صورة يتم فيها إستخدام هذا المحول الثابت [برنامج Cisco IOS الإصدار 11.2(1.3)F و 11.2(1.2) و 11.1(6.3) و 11.1(6.3)AA01 و 11.1(6.3)CA اعتبارا من 24 سبتمبر 1997] فيمكنك أيضا تمكين محاسبة الأوامر.
2. أثناء تشغيل TAC+ على الخادم، أدخل هذا الأمر على الخادم لترى الإدخالات التي تنتقل إلى ملف المحاسبة:
```
tail -f /var/log/tac.log
```
ثم قم بتسجيل الدخول إلى الموجه والخروج منه، وإدخال Telnet من الموجه، وما إلى ذلك. إذا لزم الأمر، فأدخل على الموجه:
```
terminal monitor
debug aaa accounting
```

ملف الاختبار

```
- - - - - - - (cut here) - - - - - - -

Set up accounting file if enabling accounting on NAS #
accounting file = /var/log/tac.log

:Enable password setup for everyone #
} $user = $enable
"login = cleartext "cisco
{

:Group listings must be first #
} group = admin
Users in group 'admin' have cleartext password #
"login = cleartext "admin
"expires = "Dec 31 1999
{

} group = operators
Users in group 'operators' have cleartext password #
"login = cleartext "operator
"expires = "Dec 31 1999
```

```
{

                                                    } group = transients
                                    Users in group 'transient' have cleartext password #
                                                "login = cleartext "transient
                                                     "expires = "Dec 31 1999
                                                    {

                                .This user is a member of group 'admin' & uses that group's password to log in #
.The $enable$ password is used to enter enable mode.  The user can perform all commands  #
                                                    } user = authenuser
                                              default service = permit
                                                        member = admin
                                                               {

                                    :This user is limitted in allowed commands when aaa authorization is enabled #
                                                                 } user = telnet
                                                "login = cleartext "telnet
                                                        } cmd = telnet
                                                             *. permit
                                                                    {
                                                        } cmd = logout
                                                             *. permit
                                                                    {
                                                                    {

                                                                 } user = transient #
                                                          member = transients       #
                                                            } service = exec        #
                                          When transient logs on to the NAS, he's immediately #
                                                            zipped to another site #
                                                "#.#.#.# autocmd = "telnet        #
                                                                    {       #
                                                                    {       #

                                                'This user is a member of group 'operators #
                                                    uses that group's password to log in & #
                                                                 } user = authenuser
                                                          member = operators
                                    Since this user does not have 'default service = permit' when command #
                                authorization through TACACS+ is on at the router, this user's commands #
                                                                     :are limited to #
                                                        } cmd = show
                                                          permit ver
                                                           permit ip
                                                                  {
                                                      } cmd = traceroute
                                                               *. permit
                                                                      {
                                                          } cmd = logout
                                                               *. permit
                                                                      {
                                                                    {
                                                - - - - (end cut here) - - - -
```

ملاحظة: يتم إنشاء رسالة الخطأ هذه إذا لم يكن خادم TACACS الخاص بك قابلا للوصول: AAA-3-DROPACCTSNDFAIL: . تحقق من تشغيل خادم TACACS+.

معلومات ذات صلة

- بروتوكول TACACS+ لأمان الوصول إلى الشبكة لمستخدم واحد
- نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+)

- خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows
- 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).