تكوين TACACS+ و RADIUS و Kerberos على محولات Catalyst

المحتويات

المقدمة

ساندت عائلة Cisco Catalyst من المحولات (Catalyst 5000، Catalyst 4000، و Catalyst 6000 التي تعمل بنظام التشغيل CatOS) شكلا ما من أشكال المصادقة، والتي تبدأ في الرمز 2.2. تمت إضافة تحسينات مع الإصدارات الأحدث. يكون منفذ TACACS+ TCP رقم 49، وليس منفذ XTACACS لمخطط بيانات المستخدم (UDP) رقم 49)، أو RADIUS، أو إعداد مستخدم خادم Kerberos للمصادقة والتخويل والمحاسبة (AAA) هو نفسه لمستخدمي الموجه. يحتوي هذا المستند على أمثلة للأوامر الدنيا اللازمة لتمكين هذه الوظائف. تتوفر خيارات إضافية في وثائق المحول الخاصة بالإصدار المعني.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

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

معلومات أساسية

بما أن الإصدارات الأحدث من الرمز تدعم الخيارات الإضافية، فأنت تحتاج إلى إصدار الأمر **show version** لتحديد إصدار الرمز على المحول. بمجرد تحديد إصدار الرمز الذي يتم إستخدامه على المحول، أستخدم هذا الجدول لتحديد الخيارات المتوفرة على الجهاز الخاص بك، والخيارات التي ترغب في تكوينها.

ابق دائما في المحول عند إضافة المصادقة والتفويض. اختبر التكوين في نافذة أخرى لتجنب التأمين دون قصد.

الأسلوب (الحد الأدنى)	CAT الإصدار 2.2 إلى 5.1	Cat الإصدار 5.1 إلى 5.4.1	CAT الإصدار 5.4.1 إلى 7.5.1	Cat الإصدار 7.5.1 والإصدارات الأحدث
مصادقة TACACS+ أو	الخطوة A	الخطوة A	الخطوة A	الخطوة A
مصادقة RADIUS	غير متوفر	الخطوة ب	الخطوة ب	الخطوة ب
مصادقة Kerberos أو	غير متوفر	غير متوفر	الخطوة K	الخطوة K
مصادقة/تفويض اسم المستخدم المحلي	غير متوفر	غير متوفر	غير متوفر	الخطوة ج
زائد (خيارات)				
تفويض أوامر TACACS+	غير متوفر	غير متوفر	الخطوة D	الخطوة D
تفويض TACACS+ EXEC	غير متوفر	غير متوفر	الخطوة E	الخطوة E
تفويض RADIUS EXEC	غير متوفر	غير متوفر	الخطوة F	الخطوة F
المحاسبة - TACACS+ أو RADIUS	غير متوفر	غير متوفر	الخطوة G	الخطوة G
تمكين التفويض ل	الخطوة H	الخطوة H	الخطوة H	الخطوة H

TACACS+				
تمكين تفويض RADIUS	غير متوفر	الخطوة ا	الخطوة ا	الخطوة ا
تمكين التفويض ل TACACS+	غير متوفر	غير متوفر	الخطوة ياء	الخطوة ياء

خطوات التكوين

الخطوة أ - مصادقة TACACS+

مع إصدارات سابقة من الرمز، لا تكون الأوامر معقدة كما هو الحال مع بعض الإصدارات الأحدث. يمكن أن تتوفر خيارات إضافية في الإصدارات الأحدث على المحول لديك.

1. قم بإصدار الأمر **set authentication login local enable** للتأكد من وجود باب خلفي في المحول إذا كان الخادم معطلا.
2. قم بإصدار الأمر **set authentication login tacacs enable** لتمكين مصادقة TACACS+.
3. قم بإصدار الأمر **set tacacs server #.#.#. لتحديد الخادم.**
4. قم بإصدار الأمر **set tacacs key *your_key*** لتحديد مفتاح الخادم، والذي يكون إختياريا مع TACACS+، لأنه يتسبب في تشفير البيانات من محول إلى خادم. في حالة إستخدامه، يجب أن يتوافق مع الخادم.**ملاحظة: لا** يقبل برنامج Cisco Catalyst OS علامة الاستفهام (؟) أن يكون جزءا من أي مفاتيح أو كلمات مرور. يتم إستخدام علامة الاستفهام بشكل صريح للمساعدة في صياغة الأمر.

الخطوة B - مصادقة RADIUS

مع إصدارات سابقة من الرمز، لا تكون الأوامر معقدة كما هو الحال مع بعض الإصدارات الأحدث. يمكن أن تتوفر خيارات إضافية في الإصدارات الأحدث على المحول لديك.

1. قم بإصدار الأمر **set authentication login local enable** للتأكد من وجود باب خلفي في المحول إذا كان الخادم معطلا.
2. قم بإصدار الأمر **set authentication login radius enable** لتمكين مصادقة RADIUS.
3. قم بتعريف الخادم. في جميع أجهزة Cisco الأخرى، تكون منافذ RADIUS الافتراضية هي 1646/1645 (المصادقة/المحاسبة).على المادة حفازة، التقصير ميناء 1813/1812. إذا كنت تستخدم Cisco Secure أو خادم يتصل بمعدات Cisco الأخرى، فاستخدم منفذ 1646/1645. قم بإصدار الأمر **set radius server #.#.#.# auth-port 1645 acct-port 1646 basic** لتحديد الخادم والأمر المماثل في Cisco IOS **كمنافذ مصدر-server 1645-1646**.
4. قم بتحديد مفتاح الخادم.وهذا إلزامي، نظرا لأنه يتسبب في تشفير كلمة مرور المحول إلى الخادم كما هو الحال في مصادقة/تفويض RADIUS RFC 2865 وRADIUS Accounting RFC 2866 . في حالة إستخدامه، يجب أن يتوافق مع الخادم. قم بإصدار الأمر **set radius key *your_key***.

الخطوة C - مصادقة/تفويض اسم المستخدم المحلي

ابتداء من الإصدار 7.5.1 من CatOS، يمكن أن تكون مصادقة المستخدم المحلي. مثلا، أنت يستطيع حققت صحة هوية/تخويل مع الإستعمالمن username وكلمة يخزن على المادة حفازة، instead of صحة هوية مع كلمة محلي.

هناك فقط إثنان امتياز مستوى لمصادقة مستعمل محلي، 0 أو 15. المستوى 0 هو مستوى EXEC غير ذي الامتيازات. المستوى 15 هو مستوى التمكين ذي الامتيازات.

إذا قمت بإضافة هذه الأوامر في هذا المثال، فإن المستخدم powerUser يصل إلى وضع التمكين على برنامج Telnet أو وحدة تحكم إلى المحول enable إلى وضع EXEC على برنامج Telnet أو وحدة تحكم إلى المحول.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

ملاحظة: إذا كان المستخدم قادر يعرف كلمة مرور **set enable**، فيمكن لذلك المستخدم الاستمرار في تمكين الوضع.

بعد التكوين، يتم تخزين كلمات المرور مشفرة.

يمكن إستخدام مصادقة اسم المستخدم المحلي بالاقتران مع محاسبة TACACS+ EXEC عن بعد أو محاسبة الأوامر أو محاسبة EXEC عن بعد ل RADIUS. كما يمكن إستخدامها أيضا بالاقتران مع TACACS+ EXEC البعيد أو تفويض الأوامر، ولكن من غير المنطقي إستخدامه بهذه الطريقة لأن اسم المستخدم يحتاج إلى التخزين على كل من خادم TACACS+ وكذلك محليا على المحول.

الخطوة D - تفويض أوامر TACACS+

في هذا المثال، يقال للمحول إنه يتطلب التفويض لأوامر التكوين فقط مع TACACS+. في حالة تعطل خادم TACACS+، تكون المصادقة بلا. ينطبق هذا على كل من منفذ وحدة التحكم وجلسة عمل Telnet. قم بإصدار هذا الأمر:

تعيين أوامر التخويل enable config tacacs none كلتيهما

في هذا المثال، يمكنك تكوين خادم TACACS+ للسماح عند تعيين هذه المعلمات:

```
command=set
arguments (permit)=port 2/12
```

يتم إرسال الأمر **set port enable 2/12** إلى خادم TACACS+ للتحقق.

ملاحظة: مع تمكين تفويض الأوامر، على عكس ما يحدث في الموجه حيث لا يعتبر التمكين أمرا، يرسل المحول الأمر **enable** إلى الخادم عند محاولة إجراء تمكين. تأكد من تكوين الخادم أيضا للسماح بالأمر **enable**.

الخطوة E - تفويض TACACS+ EXEC

في هذا المثال، يقال للمحول إنه يتطلب تفويضا لجلسة عمل EXEC باستخدام TACACS+. في حالة تعطل خادم TACACS+، يكون التخويل بلا. يطبق هذا إلى على حد سواء الوحدة طرفية للتحكم ميناء وال telnet جلسة. قم بإصدار الأمر **set authorization exec enable tacacs+ none كلا**

بالإضافة إلى طلب المصادقة، يرسل هذا طلب تفويض منفصل إلى خادم TACACS+ من المحول. إذا تم تكوين ملف تعريف المستخدم ل shell/exec على خادم TACACS+، فإن ذلك المستخدم يكون قادرا على الوصول إلى المحول.

وهذا يؤدي إلى منع المستخدمين الذين لا تتوفر لهم خدمة shell/exec التي تم تكوينها على الخادم، مثل مستخدمي PPP، من تسجيل الدخول إلى المحول. تتلقى رسالة تفيد EXEC. بالإضافة إلى السماح بوضع EXEC للمستخدمين/رفضه، يمكن إجبارك على وضع التمكين عند الدخول باستخدام مستوى الامتياز 15 المعين على الخادم. هو ينبغي ركضت رمز في أي cisco بق CSCdr51314 id (يسجل زبون فقط) ثابت.

الخطوة F - تفويض RADIUS EXEC

لا يوجد أمر لتمكين تفويض RADIUS EXEC. والحل البديل هو تعيين نوع الخدمة (سمة RADIUS 6) على إداري

(قيمة 6) في خادم RADIUS لتشغيل المستخدم في وضع التمكين في خادم RADIUS. إذا تم تعيين نوع الخدمة على أي شيء غير administrative-6، على سبيل المثال، login-1، أو shell-7، أو framed-2، يصل المستخدم إلى موجه أمر EXEC للمحول، ولكن ليس موجه الأمر enable.

أضفت هذا أمر في المفتاح للمصادقة والتخويل:

```
aaa authorization exec TEST group radius
                                line vty 0 4
                  authorization exec TEST
                 login authentication TEST
```

الخطوة G - المحاسبة - TACACS+ أو RADIUS

لتمكين محاسبة TACACS+ ل:

1. إذا قمت بالحصول على موجه أمر المحول، فعليك إصدار الأمر **set accounting exec enable start-stop tacacs+**.
2. المستخدمون الذين يصدر Telnet خارج المحول أمر **set accounting connect enable start-stop tacacs+**.
3. إذا قمت بإعادة تمهيد المحول، فعليك إصدار الأمر **set accounting system enable start-stop tacacs+**.
4. المستخدمون الذين يقومون بتنفيذ الأوامر، **قم** بإصدار **مجموعة أوامر المحاسبة لتمكين** أمر **بدء-إيقاف tacacs+**.
5. قم بإصدار تذكيرات للخادم، على سبيل المثال، لتحديث السجلات مرة واحدة في الدقيقة لإظهار أن المستخدم لا يزال مسجلا للدخول، الأمر **set accounting update periodic 1** .

لتمكين عملية محاسبة RADIUS ل:

1. المستخدمون الذين يحصلون على موجه أمر المحول، قم بإصدار الأمر **set accounting exec enable start-stop radius**.
2. المستخدمون الذين يصدر برنامج Telnet من المحول، قم بإصدار أمر **set accounting connect enable start-stop radius**.
3. عندما تقوم بإعادة تمهيد المحول، قم بإصدار الأمر **set accounting system enable start-stop radius**.
4. قم بإصدار تذكيرات للخادم، على سبيل المثال، لتحديث السجلات مرة واحدة في الدقيقة لإظهار أن المستخدم لا يزال مسجل الدخول، قم بإصدار الأمر **set accounting update periodic 1**.

سجلات TACACS+ للبرامج المجانية

هذا الإخراج هو مثال على كيفية ظهور السجلات على الخادم:

```
                Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
  stop task_id=5 start_time=953936729 timezone=UTC 171.68.118.100
                          service=shell disc-cause=2 elapsed_time=236
                Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
 stop task_id=15 start_time=953936975 timezone=UTC 171.68.118.100
                                service=shell priv-lvl=0 cmd=enable
                Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
 stop task_id=16 start_time=953936979 timezone=UTC 171.68.118.100
                       service=shell priv-lvl=15 cmd=write terminal
                Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
 stop task_id=17 start_time=953936984 timezone=UTC 171.68.118.100
                         service=shell priv-lvl=15 cmd=show version
                Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
update task_id=14 start_time=953936974 timezone=UTC 171.68.118.100
```

```
service=shell
```

خرج سجل RADIUS على UNIX

هذا الإخراج هو مثال على كيفية ظهور السجلات على الخادم:

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
"User-Name = "login
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
"Acct-Session-Id = "0000002b
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
"User-Name = "login
"Calling-Station-Id = "171.68.118.100
Acct-Status-Type = Start
User-Service-Type = Login-User
"Acct-Session-Id = "0000002c
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
"User-Name = "login
"Calling-Station-Id = "171.68.118.100
Acct-Status-Type = Stop
User-Service-Type = Login-User
"Acct-Session-Id = "0000002c
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
"User-Name = "login
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
"Acct-Session-Id = "0000002b
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

الخطوة TACACS - H+ تمكين المصادقة

أكمل الخطوات التالية:

1. قم بإصدار الأمر **set authentication enable local enable** وذلك للتأكد من وجود باب خلفي في في حالة تعطل الخادم.
2. قم بإصدار الأمر **set authentication enable tacacs enable** لإعلام المحول بإرسال طلبات التمكين إلى الخادم.

الخطوة I - تمكين مصادقة RADIUS

قم بإضافة هذه الأوامر للحصول على المحول لإرسال اسم المستخدم enab15$$ إلى خادم RADIUS. لا تدعم جميع خوادم RADIUS هذا النوع من اسم المستخدم. راجع الخطوة E للحصول على بديل آخر، على سبيل المثال، إذا قمت بضبط نوع خدمة [سمة RADIUS 6 - على إداري]، والذي يقوم بتشغيل المستخدمين الأفراد في وضع التمكين.

1. قم بإصدار الأمر **set authentication enable local enable** وذلك للتأكد من وجود باب خلفي في حالة تعطل الخادم.
2. قم بإصدار الأمر **set authentication enable radius enable** لإعلام المحول بإرسال طلبات التمكين إلى الخادم إذا كان خادم RADIUS يدعم اسم المستخدم enab15$$.

الخطوة ل - تمكين التفويض ل TACACS+

تؤدي إضافة هذا الأمر إلى إرسال المحول للتمكين إلى الخادم عندما يحاول المستخدم التمكين. يجب أن يكون الأمر **enable** مسموحا به للخادم. في هذا المثال، يتم تجاوز الفشل إلى لا شيء في حالة تعطل الخادم:

set author enable enable tacacs+ none كلا

الخطوة K - مصادقة Kerberos

راجع التحكم في الوصول ومراقبته للمحول باستخدام المصادقة والتفويض والحساب للحصول على مزيد من المعلومات حول كيفية إعداد Kerberos إلى المحول.

إسترداد كلمة المرور

ارجع إلى إجراءات إسترداد كلمة المرور للحصول على مزيد من المعلومات حول إجراءات إسترداد كلمة المرور.

هذه الصفحة هي فهرس إجراءات إسترداد كلمة المرور لمنتجات Cisco.

أوامر تصريح بروتوكول الإنترنت لتوفير أمان إضافي

للحصول على أمان إضافي، يمكن تكوين المادة حفازة للتحكم في الوصول إلى Telnet من خلال أوامر **ip permit**:

set ip permit enable telnet

تعيين *قناع نطاق* تصريح ip|*المضيف*

وهذا يسمح فقط بالنطاق أو الأجهزة المضيفة المحددة ل Telnet في المحول.

تصحيح الأخطاء على المادة حفازة

قبل تمكين تصحيح الأخطاء على المادة حفازة، تحقق من سجلات الخادم لأسباب الفشل. يكون هذا أسهل وأقل إزعاجا للمحول. في إصدارات المحولات السابقة، تم تنفيذ **تصحيح الأخطاء** في الوضع الهندسي. ليس من الضروري الوصول إلى الوضع الهندسي لتنفيذ أوامر **تصحيح الأخطاء** في الإصدارات الأحدث من الرمز:

تعيين 4 Tacacs|radius|kerberos

ملاحظة: يقوم الأمر **set trace tacacs|radius|kerberos 0** بإرجاع Catalyst إلى وضع عدم التتبع.

راجع صفحة دعم منتجات المحولات للحصول على مزيد من المعلومات حول محولات LAN متعددة الطبقات

.(Multilayer LAN Switches)

معلومات ذات صلة

- مقارنة TACACS+ و RADIUS
- RADIUS و TACACS+ و Kerberos في وثائق Cisco IOS
- صفحة دعم RADIUS
- صفحة دعم TACACS/TACACS+
- صفحة دعم Kerberos
- 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).