كيفية تخصيص مستويات الامتيازات باستخدام RADIUS و TACACS+

المحتويات

المقدمة

يشرح هذا المستند كيفية تغيير مستوى الامتياز لأوامر معينة، ويقدم مثالا بأجزاء من تكوينات نموذجية للموجه وخوادم TACACS+ و RADIUS.

المتطلبات الأساسية

المتطلبات

يجب أن يكون لقارئ هذا المستند معرفة مستويات الامتيازات على الموجه.

افتراضيا، هناك ثلاثة مستوى امتياز على المسحاج تخديد.

- مستوى الامتياز 1 = غير ذي امتياز (موجه الأمر هو `Router>`)، المستوى الافتراضي لتسجيل الدخول
- مستوى الامتياز 15 = ذو امتياز (موجه الأمر هو `Router#`)، المستوى بعد الانتقال إلى وضع التمكين
- مستوى الامتياز 0 = نادرا ما يتم إستخدامه، ولكنه يتضمن 5 أوامر: **help**، **exit**، **enable**، **disable**، و**logout**

لا يتم إستخدام المستويات 2-14 في تكوين افتراضي، ولكن يمكن نقل الأوامر التي تكون عادة في المستوى 15 إلى أحد هذه المستويات ويمكن نقل الأوامر التي تكون عادة في المستوى 1 إلى أحد هذه المستويات. من الواضح أن نموذج الأمان هذا يتضمن بعض الإدارة على الموجه.

لتحديد مستوى الامتياز كمستخدم سجل الدخول، اكتب الأمر **show privilege**. لتحديد الأوامر المتوفرة على مستوى امتياز محدد لإصدار برنامج Cisco IOS® الذي تستخدمه، اكتب **a؟** في سطر الأوامر عند تسجيل الدخول على مستوى الامتياز هذا.

ملاحظة: بدلا من تعيين مستويات الامتيازات، يمكنك القيام بتفويض الأوامر إذا كان خادم المصادقة يدعم TACACS+. لا يدعم بروتوكول RADIUS تفويض الأوامر.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco IOS Software، الإصدار 11.2 والإصدارات الأحدث.

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

مثال

في هذا المثال، يتم نقل أوامر **snmp خادم** إلى أسفل من مستوى الامتياز 15 (الافتراضي) إلى مستوى الامتياز 7. **العملية أزيز** نقلت أمر up من امتياز مستوى 1 إلى امتياز مستوى 7. عندما تتم مصادقة المستخدم 7، يتم تعيين مستوى الامتياز 7 لذلك المستخدم بواسطة الخادم ويعرض أمر **show privilege** "مستوى الامتياز الحالي هو 7." يمكن للمستخدم إختبار الاتصال وإجراء تكوين خادم snmp في وضع التكوين. لا تتوفر أوامر التكوين الأخرى.

التكوينات - الموجه

الموجه - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

الموجه - T.11.3.3 والإصدارات الأحدث (حتى T.12.0.5)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
```

```
privilege exec level 7 configure
```

الموجه - T.12.0.5 والإصدارات الأحدث

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

التكوينات - الخادم

بروتوكول TACACS+ الآمن من Cisco

اتبع هذه الخطوات لتكوين الخادم.

1. قم بملء اسم المستخدم وكلمة المرور.
2. في "إعدادات المجموعة"، تأكد من تحديد shell/exec، ومن إدخال 7 في مربع مستوى الامتياز.

TACACS+ - Stanza في خادم البرامج المجانية

```
:Stanza in TACACS+ freeware
} user = seven
login = cleartext seven
} service = exec
priv-lvl = 7
{
{
```

بروتوكول UNIX TACACS+ الآمن من Cisco

```
} user = seven
"password = clear "seven
} service = shell
set priv-lvl = 7
{
{
```

Cisco Secure NT RADIUS

اتبع هذه الخطوات لتكوين الخادم.

1. أدخل اسم المستخدم وكلمة المرور.
2. في إعدادات المجموعة ل IETF، نوع الخدمة (السمة 6) = NAS-Prompt
3. في منطقة CiscoRADIUS، حدد **زوج AV**، وفي المربع المستطيل الموجود أسفله، أدخل **shell:priv-lvl=7**.

```
}user = seven
} radius=Cisco
} =check_items
"seven"=2
{
} =reply_attributes
7=6
"shell:priv-lvl=7"=9,1
{
{
{
```

هذا هو ملف المستخدم لاسم المستخدم "سبعة."

ملاحظة: يجب أن يدعم الخادم أزواج Cisco AV.

- سبعة كلمة مرور = **passwdxyz**
- نوع الخدمة = **مستخدم Shell**
- Cisco-avpair =**shell:priv-lvl=7**

معلومات ذات صلة

- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- TACACS+ في وثائق IOS
- صفحة دعم TACACS+
- صفحة دعم UNIX الآمن من Cisco
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- الدعم الفني - 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).