مجوم Cisco IOS: المصادقة المحلية و RADIUS لمثال تكوين اتصال TACACS+ و HTTP

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة محلية و TACACS+ و RADIUS لاتصال HTTP. يتم توفير بعض أوامر تصحيح الأخطاء ذات الصلة أيضا.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- برنامج Cisco IOS® الإصدار 11.2 أو إصدار أحدث
- الأجهزة التي تدعم مراجعات البرامج هذه

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.

النظرية الأساسية

في برنامج Cisco IOS® الإصدار 11.2، تمت إضافة ميزة لإدارة الموجه من خلال HTTP. يتضمن قسم "أوامر مستعرض الويب بنظام Cisco IOS" من مرجع أوامر أساسيات تكوين Cisco IOS المعلومات التالية حول هذه الميزة.

"يتيح لك أمر **مصادقة ip http** تحديد أسلوب مصادقة معين لمستخدمي خادم HTTP. يستخدم خادم HTTP أسلوب enable password لمصادقة مستخدم على مستوى الامتياز 15. يتيح لك أمر **مصادقة ip http** الآن تحديد مصادقة مستخدم خادم AAA) HTTP) على التمكين أو المحلي أو TACACS أو المصادقة والتخويل والمحاسبة (AAA).

التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

يستخدم هذا المستند التكوينات الموضحة أدناه.

- تكوين المصادقة المحلية لمستخدمي خادم HTTP
- تكوين مصادقة TACACS+ لمستخدمي خادم HTTP
- تكوين مصادقة RADIUS لمستخدمي خادم HTTP

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

تكوين المصادقة المحلية لمستخدمي خادم HTTP

- تكوينات الموجه
- نتائج المستخدم

تكوينات الموجه

المصادقة المحلية مع برنامج Cisco IOS الإصدار 11.2

```
This is the part of the configuration related to ---!
local authentication. ! aaa new-model aaa authentication
        login default local aaa authorization exec local
   username one privilege 15 password one username three
  password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
    of command moved from level 15 (enable) to level 7 !
                        privilege exec level 7 clear line
```

المصادقة المحلية مع برنامج Cisco IOS الإصدار T.11.3.3 أو الإصدارات الأحدث

```
This is the part of the configuration !--- related ---!
                to local authentication. ! aaa new-model aaa
     authentication login default local aaa authorization
    exec default local username one privilege 15 password
          one username three password three username four
        privilege 7 password four ip http server ip http
     authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
                                                  7 clear line
```

نتائج المستخدم

تنطبق هذه النتائج على المستخدمين في تكوينات الموجه السابقة.

- **المستخدم الأول**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/. #.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 15).إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.
- **المستخدم الثالث**سيفشل المستخدم في تخويل ويب بسبب عدم وجود مستوى امتياز.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع غير التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 1).إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.
- **المستخدم الرابع**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/level/7/exec.ستظهر أوامر المستوى 1 بالإضافة إلى أمر **مسح** المستوى **7**.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم على مستوى الامتياز 7 بعد تسجيل الدخول (**عرض الامتياز** سيكون 7)إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.

تكوين مصادقة TACACS+ لمستخدمي خادم HTTP

تكوينات الموجه

المصادقة مع البرنامج Cisco IOS Software، الإصدار 11.2

```
                                                aaa new-model
                                +aaa authentication login default tacacs
                                    +aaa authorization exec tacacs
                                                ip http server
                                    ip http authentication aaa
                                tacacs-server host 171.68.118.101
                                        tacacs-server key cisco
Example of command moved from level 15 (enable) to ---!
                                level 7 privilege exec level 7 clear line
```

المصادقة مع برنامج Cisco IOS الإصدارات T.11.3.3 إلى 12.0.5

```
aaa new-model
+aaa authentication login default tacacs
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
Example of command moved from level 15 (enable) to ---!
level 7 privilege exec level 7 clear line
```

المصادقة مع برنامج Cisco IOS الإصدار T.12.0.5 والإصدارات الأحدث

```
aaa new-model
+aaa authentication login default group tacacs
+aaa authorization exec default group tacacs
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
Example of command moved from level 15 (enable) to ---!
level 7 privilege exec level 7 clear line
```

نتائج المستخدم

تنطبق النتائج التالية على المستخدمين في تكوينات الخادم أدناه.

- **المستخدم الأول**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/. #.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 15).إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.
- **مستخدم إثنان**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/. #.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 15).إذا تمت إضافة تفويض الأوامر إلى الموجه، فسيفشل المستخدم في جميع الأوامر لأن تكوين الخادم لا يخولها.
- **المستخدم الثالث**سيفشل المستخدم في تخويل ويب بسبب عدم وجود مستوى امتياز.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع غير التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 1).إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.
- **المستخدم الرابع**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/level/7/exec.ستظهر أوامر المستوى 1 بالإضافة إلى أمر **مسح** المستوى **7**.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم على مستوى الامتياز 7 بعد تسجيل الدخول (**عرض الامتياز** سيكون 7)إذا تمت إضافة تفويض الأوامر إلى الموجه، سيظل المستخدم ناجحا في جميع الأوامر.

تكوين خادم برنامج Daemon المجاني

```
} user = one
default service = permit
"login = cleartext "one
} service = exec
priv-lvl = 15
{
```

```
{

} user = two
"login = cleartext "two
} service = exec
priv-lvl = 15
{
{

} user = three
default service = permit
"login = cleartext "three
{

} user = four
default service = permit
"login = cleartext "four
} service = exec
priv-lvl = 7
{
{
```

مصدر المحتوى الإضافي الآمن من Cisco لتكوين خادم UNIX

```
ViewProfile -p 9900 -u one/. #
User Profile Information
}user = one
profile_id = 27
profile_cycle = 1
"********" password = clear
default service=permit
} service=shell
set priv-lvl=15
{
{
ViewProfile -p 9900 -u two/. #
User Profile Information
}user = two
profile_id = 28
profile_cycle = 1
"********" password = clear
} service=shell
set priv-lvl=15
{
{
ViewProfile -p 9900 -u three/. #
User Profile Information
}user = three
profile_id = 29
profile_cycle = 1
"********" password = clear
default service=permit
{
ViewProfile -p 9900 -u four/. #
User Profile Information
}user = four
profile_id = 30
profile_cycle = 1
"********" password = clear
default service=permit
} service=shell
set priv-lvl=7
```

{
{

مصدر المحتوى الإضافي الآمن من Cisco لتكوين خادم Windows

المستخدم الأول في المجموعة الأولى

- إعدادات المجموعةتحقق من **shell (exec)**.فحصت **امتياز مستوى=15**.التحقق من **الخدمات الافتراضية (غير المحددة)**.**ملاحظة:** إذا لم يظهر هذا الخيار، فانتقل إلى **تكوين الواجهة** وحدد **TACACS+** ثم **خيارات التكوين المتقدمة**. أخترت **عرض enable تقصير خدمة** تشكيل.
- إعدادات المستخدمكلمة مرور من أي قاعدة بيانات، أدخل كلمة مرور وقم بتأكيدها في المنطقة العليا.

المستخدم الثاني في المجموعة الثانية

- إعدادات المجموعةتحقق من **shell (exec)**.فحصت **امتياز مستوى=15**.عدم التحقق من **الخدمات الافتراضية (غير المحددة)**.
- إعدادات المستخدمكلمة مرور من أي قاعدة بيانات، أدخل كلمة مرور وقم بتأكيدها في المنطقة العليا.

المستخدم الثالث في المجموعة الثالثة

- إعدادات المجموعةتحقق من **shell (exec)**.ترك **مستوى الامتياز** فارغا.التحقق من **الخدمات الافتراضية (غير المحددة)**.**ملاحظة:** إذا لم يظهر هذا الخيار، فانتقل إلى **تكوين الواجهة** وحدد **TACACS+** ثم **خيارات التكوين المتقدمة**. أخترت **عرض enable تقصير خدمة** تشكيل.
- إعدادات المستخدمكلمة مرور من أي قاعدة بيانات، أدخل كلمة مرور وقم بتأكيدها في المنطقة العليا.

المستخدم الرابع في المجموعة الرابعة

- إعدادات المجموعةتحقق من **shell (exec)**.فحصت **امتياز مستوى=7**.التحقق من **الخدمات الافتراضية (غير المحددة)**.**ملاحظة:** إذا لم يظهر هذا الخيار، فانتقل إلى **تكوين الواجهة** وحدد **TACACS+** ثم **خيارات التكوين المتقدمة**. أخترت **عرض enable تقصير خدمة** تشكيل.
- إعدادات المستخدمكلمة مرور من أي قاعدة بيانات، أدخل كلمة مرور وقم بتأكيدها في المنطقة العليا.

تكوين مصادقة RADIUS لمستخدمي خادم HTTP

تكوينات الموجه

المصادقة مع البرنامج Cisco IOS Software، الإصدار 11.2
aaa new-model aaa authentication login default radius aaa authorization exec radius ip http server ip http authentication aaa ! *Example of command moved from level 15 (enable) to ---!* *level 7* ! privilege exec level 7 clear line radius- server host 171.68.118.101 radius-server key cisco

المصادقة مع برنامج Cisco IOS الإصدارات T.11.3.3 إلى 12.0.5
aaa new-model aaa authentication login default radius aaa authorization exec default radius ip http server ip http authentication aaa radius-server host 171.68.118.101 auth-port 1645 acct-port 1646 radius-server key cisco privilege exec level 7 clear line
المصادقة مع برنامج Cisco IOS الإصدار T.12.0.5 والإصدارات الأحدث
aaa new-model aaa authentication login default group radius aaa authorization exec default group radius ip http server ip http authentication aaa radius-server host 171.68.118.101 auth-port 1645 acct-port 1646 radius-server key cisco privilege exec level 7 clear line

نتائج المستخدم

تنطبق النتائج التالية على المستخدمين في تكوينات الخادم أدناه.

- **المستخدم الأول**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#. #.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 15).
- **المستخدم الثالث**سيفشل المستخدم في تخويل ويب بسبب عدم وجود مستوى امتياز.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم في وضع غير التمكين بعد تسجيل الدخول (سيكون **عرض الامتياز** 1).
- **المستخدم الرابع**سيمرر المستخدم تفويض الويب إذا تم إدخال عنوان URL ك http://#.#.#.#/level/7/exec.ستظهر أوامر المستوى 1 بالإضافة إلى أمر **مسح** المستوى **7**.بعد Telnet إلى الموجه، يمكن للمستخدم تنفيذ جميع الأوامر بعد مصادقة تسجيل الدخول.سيكون المستخدم على مستوى الامتياز 7 بعد تسجيل الدخول (**عرض الامتياز** سيكون 7)

تكوين RADIUS على الخادم الذي يدعم أزواج Cisco AV

```
"one Password= "one
Service-Type = Shell-User
"cisco-avpair = "shell:priv-lvl=15

"three Password = "three
Service-Type = Login-User

"four Password= "four
Service-Type = Login-User
"cisco-avpair = "shell:priv-lvl=7
```

مصدر المحتوى الإضافي الآمن من Cisco لتكوين خادم UNIX

```
ViewProfile -p 9900 -u one/. #
      User Profile Information
                  }user = one
            profile_id = 31
set server current-failed-logins = 0
          profile_cycle = 3
             } radius=Cisco
             } =check_items
                   "one"=2
                         {
       } =reply_attributes
                       6=6
                         {
                         {
                         {
ViewProfile -p 9900 -u three/. #
      User Profile Information
                   }user = three
            profile_id = 32
set server current-failed-logins = 0
          profile_cycle = 3
             } radius=Cisco
             } =check_items
                  "three"=2
                         {
       } =reply_attributes
                       1=6
                         {
                         {
                         {
ViewProfile -p 9900 -u four/. #
      User Profile Information
                    }user = four
            profile_id = 33
          profile_cycle = 1
             } radius=Cisco
             } =check_items
                   "four"=2
                         {
       } =reply_attributes
                       1=6
  "shell:priv-lvl=7"=9,1
                         {
                         {
                         {
```

[مصدر المحتوى الإضافي الآمن من Cisco لتكوين خادم Windows]

- المستخدم = واحد، نوع الخدمة (السمة 6) = إداري
- المستخدم = ثلاثة، نوع الخدمة (السمة 6) = تسجيل الدخول
- المستخدم = أربعة، نوع الخدمة (السمة 6) = تسجيل الدخول، تحقق من مربع أزواج Cisco AV وأدخل shell:priv-lvl=7

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

تفيد الأوامر التالية في تصحيح أخطاء مصادقة HTTP. يتم إصدارها على الموجه.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- **terminal monitor** - يعرض إخراج الأمر **debug** ورسائل خطأ النظام للمحطة الطرفية والجلسة الحالية.
- **مصادقة debug aaa** - يعرض معلومات حول مصادقة AAA/TACACS+.
- **تفويض تصحيح الأخطاء AAA** - يعرض معلومات حول تفويض AAA/TACACS+.
- **debug radius** - يعرض معلومات تصحيح الأخطاء التفصيلية المرتبطة ب RADIUS.
- **debug tacacs** - يعرض المعلومات المرتبطة ب tacacs.
- **debug ip http authentication** - أستخدم هذا الأمر لاستكشاف أخطاء مصادقة HTTP وإصلاحها. يعرض طريقة المصادقة التي حاول الموجه إستخدامها ورسائل الحالة الخاصة بالمصادقة.

معلومات ذات صلة

- صفحة دعم برنامج الوصول إلى Cisco TACACS+
- صفحة دعم RADIUS
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX
- 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).