كيفية تكوين مركز Cisco VPN 3000 لدعم مصادقة TACACS+ لحسابات الإدارة

المحتويات

المقدمة

يقدم هذا المستند إرشادات خطوة بخطوة لتكوين مركزات Cisco VPN 3000 Series لدعم مصادقة TACACS+ لحسابات الإدارة.

بمجرد تكوين خادم TACACS+ على مركز VPN 3000، لن يتم إستخدام أسماء الحسابات وكلمات المرور التي تم تكوينها محليا مثل admin و config و isp وما إلى ذلك. يتم إرسال جميع عمليات تسجيل الدخول إلى مركز VPN 3000 إلى خادم TACACS+ الخارجي الذي تم تكوينه للتحقق من المستخدم وكلمة المرور.

يحدد تعريف مستوى الامتياز لكل مستخدم على خادم TACACS+ الأذونات على مركز VPN 3000 لكل اسم مستخدم TACACS+. ثم، طابق ذلك مع مستوى الوصول AAA المحدد ضمن اسم المستخدم الذي تم تكوينه محليا على مركز VPN 3000. وهذه نقطة مهمة لأنه بمجرد تحديد خادم TACACS+، تصبح أسماء المستخدمين التي تم تكوينها محليا على مركز VPN 3000 غير صالحة. ولكن، لا تزال تستخدم فقط لمطابقة مستوى الامتياز الذي تم إرجاعه من خادم TACACS+، مع مستوى الوصول AAA أسفل ذلك المستخدم المحلي. وبعد ذلك، يتم تعيين اسم مستخدم TACACS+ للامتيازات التي قام مستخدم مركز VPN 3000 الذي تم تكوينه محليا بتعريفها أسفل ملف التعريف الخاص به.

على سبيل المثال، تم تكوين user/group +TACACS، الموضح بالتفصيل في أقسام التكوين، لإرجاع مستوى امتياز TACACS+ البالغ 15. تحت قسم Administrators (المسؤولون) من مركز الشبكة الخاصة الظاهرية (3000 VPN)، يكون لدى المستخدم المسؤول مستوى الوصول (AAA) الخاص به الذي تم تعيينه أيضا على 15. يسمح لهذا المستخدم بتعديل التكوين ضمن كافة المقاطع وقراءة/كتابة الملفات. نظرا لمطابقة مستوى امتياز TACACS+ ومستوى الوصول إلى AAA، يتم منح مستخدم TACACS+ هذه الأذونات على مركز VPN 3000.

على سبيل المثال، إذا قررت أن المستخدم يحتاج إلى أن يكون قادرا على تعديل التكوين، ولكن *ليس* ملفات قراءة/كتابة، فعليك تعيين مستوى امتياز له 12 على خادم TACACS+. يمكنك إختيار أي رقم بين واحد و 15. ثم، على مركز الشبكة الخاصة الظاهرية (VPN) 3000، أختر أحد المسؤولين الآخرين الذين تم تكوينهم محليا. بعد ذلك، قم بتعيين مستوى الوصول إلى AAA الخاص به إلى 12، ثم قم بتعيين الأذونات على هذا المستخدم ليكون قادرا على تعديل التكوين، ولكن ليس على قراءة/كتابة الملفات. بسبب مستوى الوصول/الامتياز المطابق، يحصل المستخدم على هذه الأذونات عند تسجيل الدخول.

لم تعد أسماء المستخدمين التي تم تكوينها محليا على مركز VPN 3000 مستخدمة. ولكن، يتم إستخدام حقوق الوصول ومستويات الوصول إلى المصادقة والتفويض والمحاسبة (AAA) أسفل كل من هؤلاء المستخدمين لتحديد الامتيازات التي يحصل عليها مستخدم TACACS+ معين عند تسجيل الدخول.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- تأكد من توفر اتصال IP بخادم TACACS+ من مركز VPN 3000. إذا كان خادم TACACS+ الخاص بك متجها نحو الواجهة العامة، فلا تنس فتح TACACS+ (منفذ TCP رقم 49) على التصفية العامة .
- تأكد من تشغيل الوصول إلى النسخة الاحتياطية عبر وحدة التحكم. من السهل قفل جميع المستخدمين بدون قصد من التكوين عند إعداد هذا الإعداد لأول مرة. الطريقة الوحيدة لاستعادة الوصول هي عبر وحدة التحكم، التي لا تزال تستخدم أسماء المستخدمين وكلمات المرور التي تم تكوينها محليا.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج مركز Cisco VPN 3000 الإصدار B.4.7.2 (بدلا من ذلك، يعمل أي إصدار من 3.0 أو برنامج نظام تشغيل أحدث.)
- خادم التحكم في الوصول الآمن من Cisco لخوادم Windows الإصدار 4.0 (يعمل أي إصدار من 2.4 أو إصدار أحدث من البرامج كبديل.)

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.

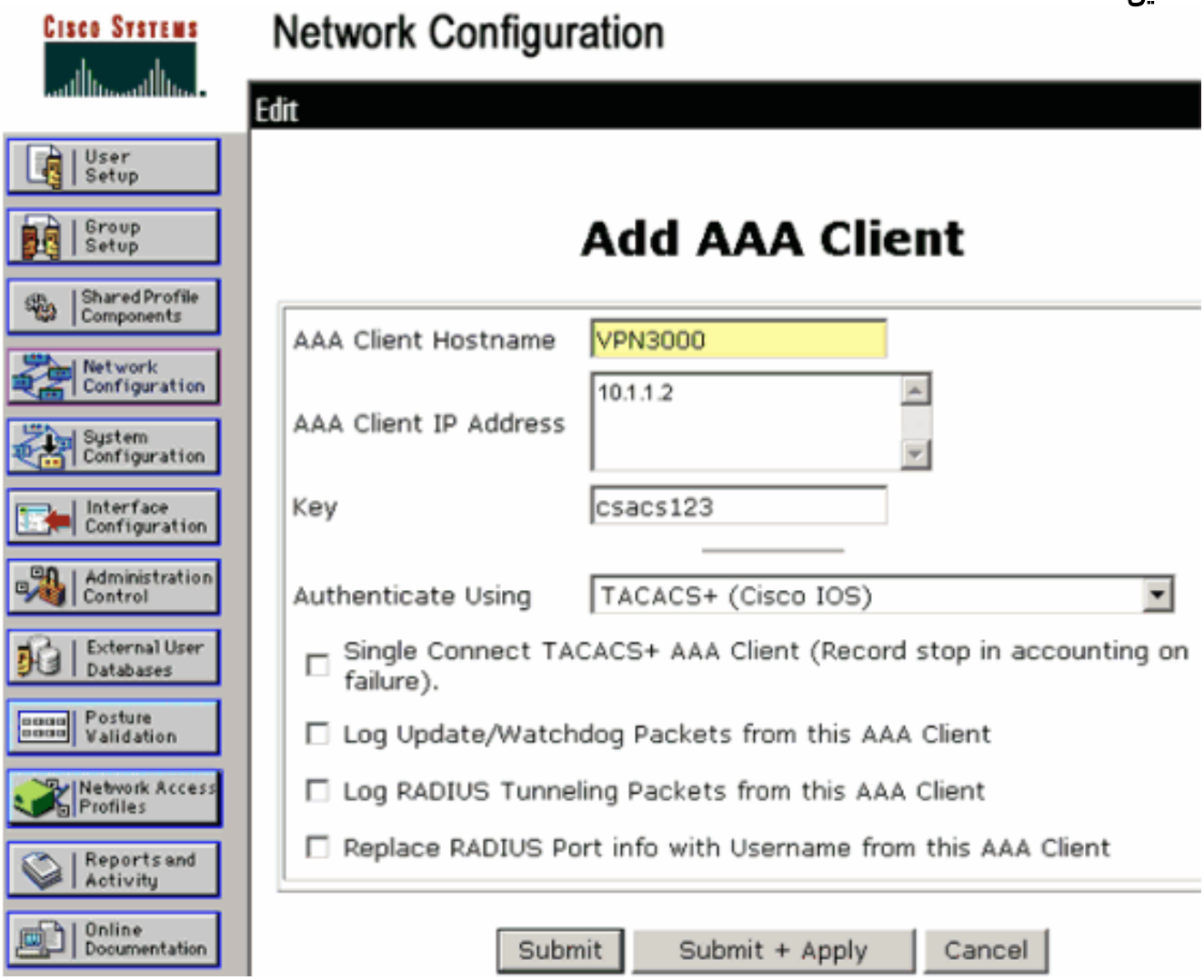
تكوين خادم TACACS+

قم بإضافة إدخال لمركز تركيز VPN 3000 في خادم TACACS+

أتمت هذا steps in order to أضفت مدخل ل VPN 3000 مركز في ال TACACS+ نادل.

1. انقر على **تكوين الشبكة** في اللوحة اليسرى. تحت عملاء AAA، انقر فوق **إضافة إدخال**.
2. في الإطار التالي، املأ النموذج لإضافة مركز الشبكة الخاصة الظاهرية (VPN) كعميل TACACS+. يستخدم هذا المثال:اسم مضيف عميل **VPN3000** = AAAعنوان IP لعميل **10.1.1.2** = AAAالمفتاح =

CSACS123المصادقة باستخدام = TACACS+ (Cisco IOS)انقر فوق **إرسال + إعادة تشغيل**.



إضافة حساب مستخدم في خادم TACACS+

أكمل هذه الخطوات لإضافة حساب مستخدم في خادم TACACS+.

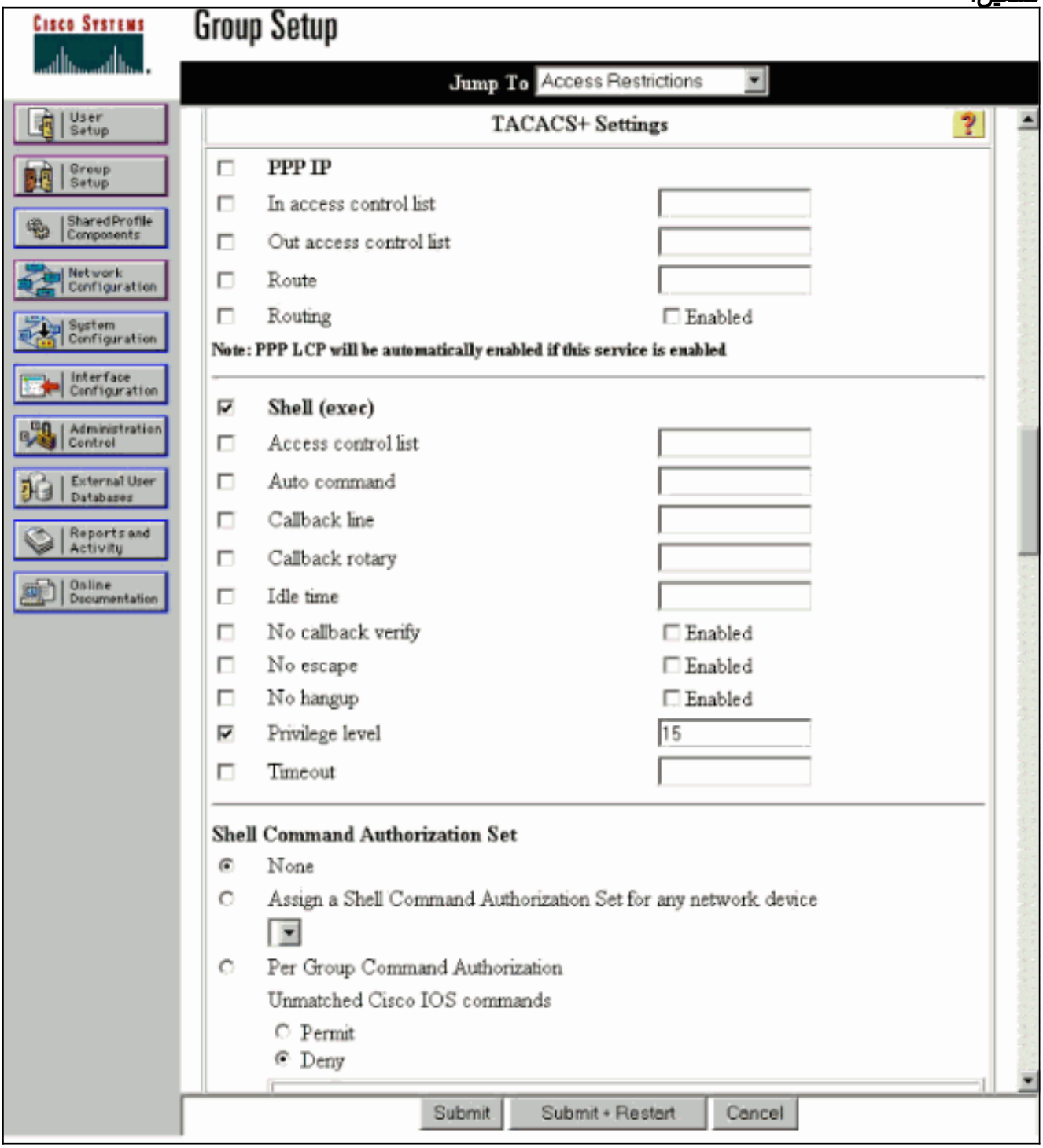
1. قم بإنشاء حساب مستخدم في خادم TACACS+ الذي يمكن إستخدامه لاحقا لمصادقة TACACS+. انقر فوق **إعداد المستخدم** في اللوحة اليسرى، ثم أضف المستخدم "johnsmith" وانقر فوق **إضافة/تحرير** للقيام بذلك.
2. قم بإضافة كلمة مرور لهذا المستخدم، وعينت المستخدم إلى مجموعة ACS التي تحتوي على مسئولي مركز VPN 3000 الآخرين.**ملاحظة:** يحدد هذا المثال مستوى الامتيازات ضمن ملف تعريف مجموعة ACS الخاصة بهذا المستخدم. إذا كان يجب القيام بذلك على أساس كل مستخدم، أختر **تكوين الواجهة > TACACS+ (Cisco IOS)** وحدد مربع **المستخدم** لخدمة Shell (EXEC). في هذه الحالة فقط تتوفر خيارات TACACS+ الموضحة في هذا المستند ضمن كل ملف تعريف مستخدم.

تحرير المجموعة على خادم TACACS+

أكمل الخطوات التالية لتحرير المجموعة على خادم TACACS+.

1. انقر فوق **إعداد المجموعة** في اللوحة اليسرى.
2. من القائمة المنسدلة، أختر المجموعة التي تمت إضافة المستخدم إليها في قسم إضافة حساب مستخدم في خادم TACACS+، وهي المجموعة 1 في هذا المثال، وانقر فوق **تحرير الإعدادات**.

3. في الإطار التالي، تأكد من تحديد هذه السمات ضمن إعدادات TACACS+:**طبقة (exec)مستوى الامتياز = 15**بمجرد الانتهاء، انقر فوق **إرسال + إعادة تشغيل**.



تكوين مركز VPN 3000

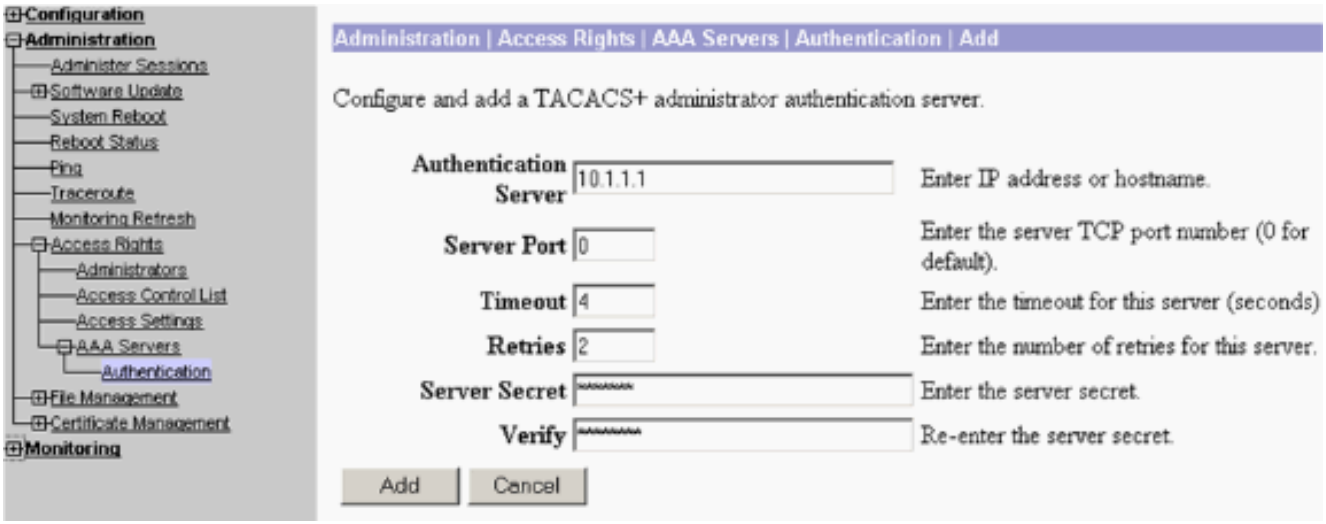
قم بإضافة إدخال لخادم TACACS+ في مركز VPN 3000

أكمل هذه الخطوات لإضافة إدخال لخادم TACACS+ في مركز VPN 3000.

1. أختر **إدارة > حقوق الوصول > خوادم AAA > المصادقة** في شجرة التصفح في اللوحة اليسرى، ثم انقر **إضافة** في اللوحة اليمنى.ما إن ينقر أنت **يضيف** in order to أضفت هذا نادل، يشكل محلي username/كلمة على ال VPN 3000 مركز لم يعد استعملت. تأكد من أن الوصول إلى النسخة الاحتياطية عبر وحدة التحكم يعمل في

حالة منع الوصول.

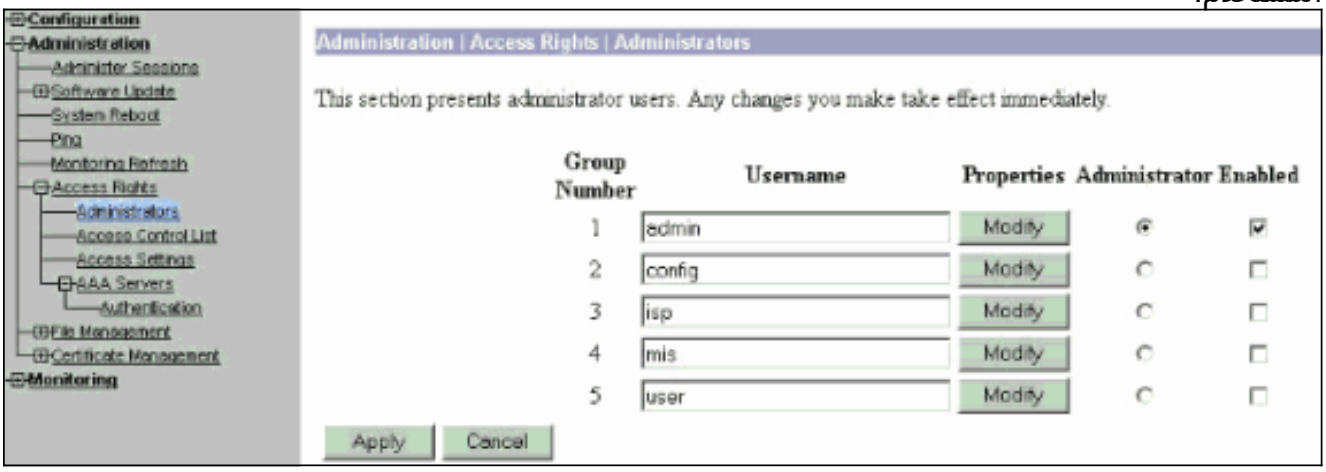
2. في الإطار التالي، املأ النموذج كما يظهر هنا:خادم المصادقة = **10.1.1.1** (عنوان IP لخادم TACACS+)منفذ الخادم = **0** (الافتراضي)المهلة = **4**عمليات إعادة المحاولة = **2**سر الخادم = **csacs123**التحقق من الصحة = **csacs123**



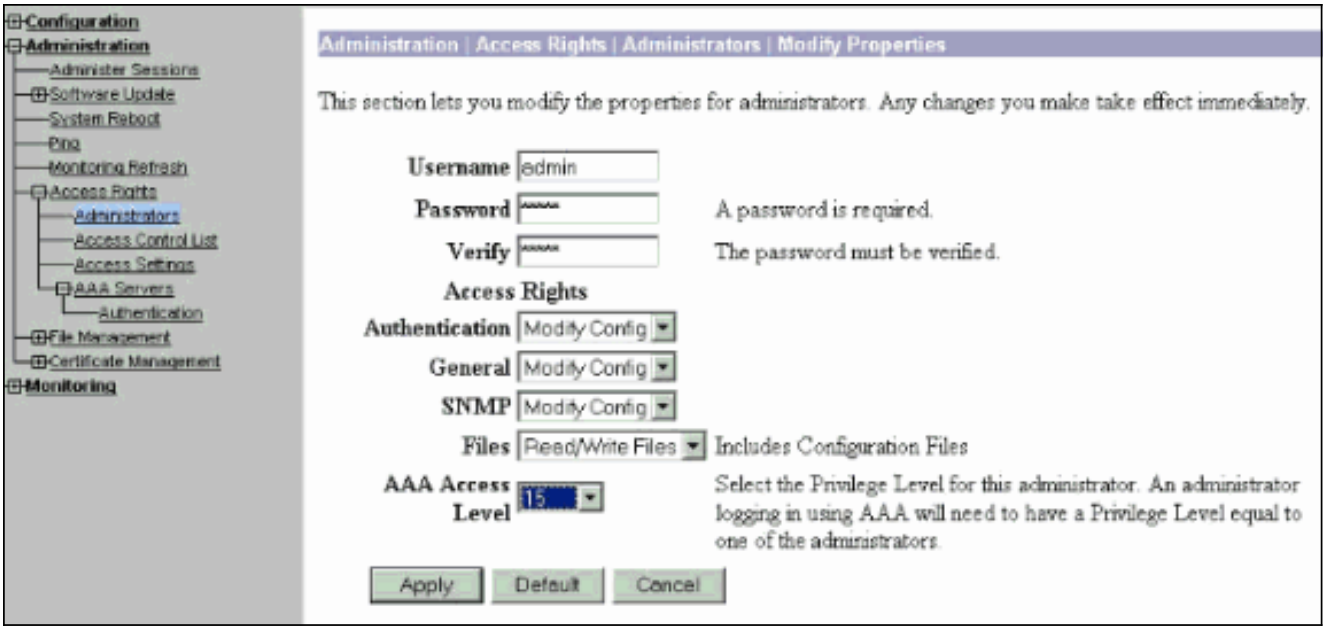
تعديل حساب Admin على مركز VPN لمصادقة TACACS+

أكمل هذه الخطوات لتعديل حساب المسؤول على مركز VPN لمصادقة TACACS+.

1. انقر فوق **تعديل** لمسؤول المستخدم لتعديل خصائص هذا المستخدم.



2. أختر مستوى الوصول إلى AAA ك **15**.يمكن أن تتراوح هذه القيمة بين واحد و 15. لاحظ أنه يجب أن يطابق مستوى امتياز TACACS+ المحدد ضمن ملف تعريف المستخدم/المجموعة على خادم TACACS+. ثم يقوم مستخدم TACACS+ بتجميع الأذونات المعرفة ضمن مستخدم مركز VPN 3000 لتعديل التكوين وقراءة/كتابة الملفات وما إلى ذلك.



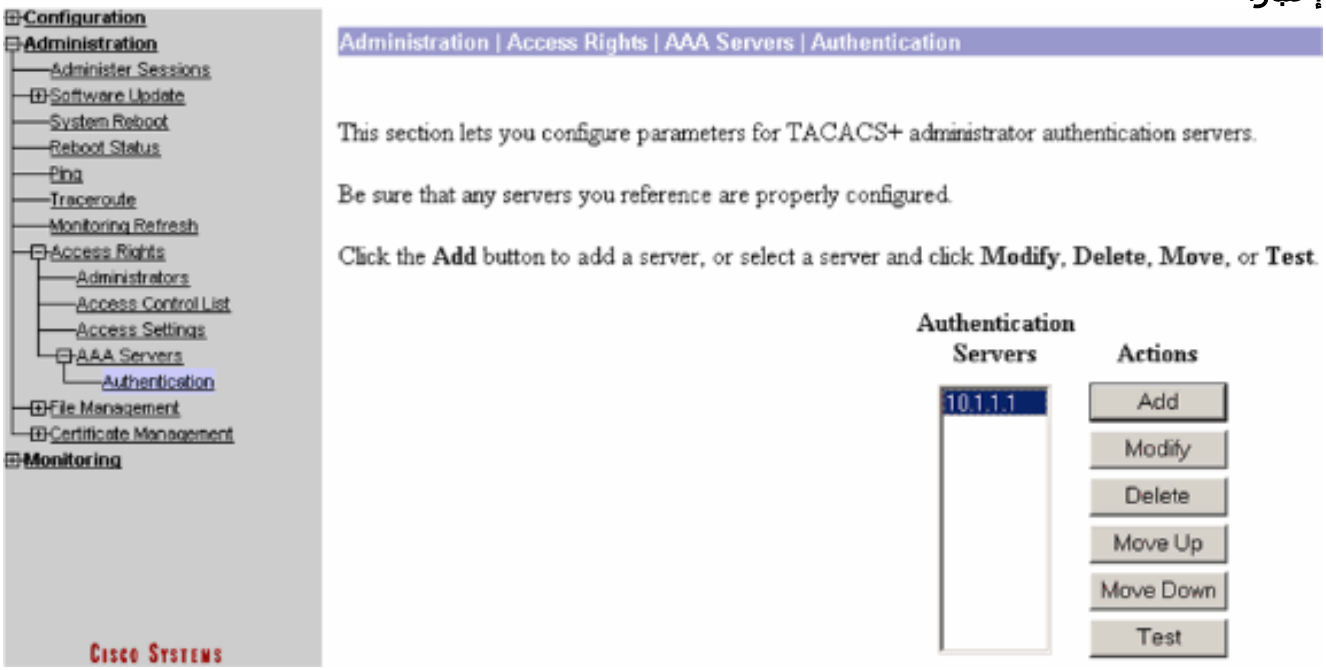
التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

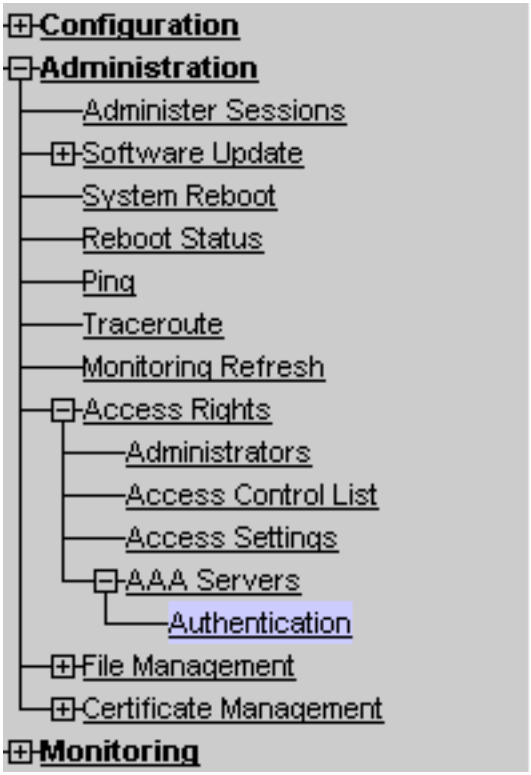
أتمت ال steps في هذا تعليم in order to تحريت تشكيلك.

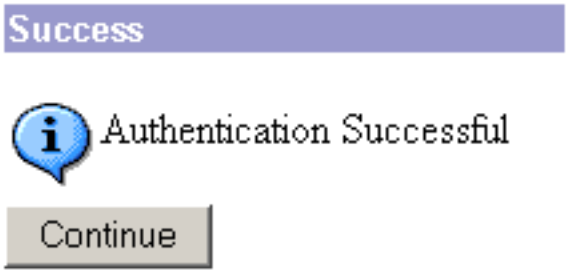
1. لاختبار المصادقة:لخوادم TACACS+أختر **إدارة > حقوق الوصول > خوادم AAA > المصادقة**.حدد الخادم، ثم انقر فوق
إختبار.



ملاحظة: عند تكوين خادم TACACS+ على علامة التبويب "الإدارة"، فلا توجد طريقة لإعداد المستخدم للمصادقة على قاعدة البيانات المحلية ل VPN 3000. لا يمكنك إجراء النسخ الاحتياطي إلا باستخدام قاعدة بيانات خارجية أخرى أو خادم TACACS+.أدخل اسم مستخدم وكلمة مرور TACACS+ وانقر على **موافق**.

تظهر مصادقة





ناجحة.

2. إن يفشل هو، هناك إما مشكلة تشكيل أو ip موصولية إصدار. تحقق من "سجل المحاولات الفاشلة" الموجود على خادم ACS بحثا عن الرسائل المتعلقة بهذا الفشل.إذا لم تظهر أي رسائل في هذا السجل، فمن المحتمل أن تكون هناك مشكلة في اتصال IP. لا يصل طلب TACACS+ إلى خادم TACACS+. تحقق من المرشحات المطبقة على واجهة مركز VPN 3000 المناسبة التي تسمح لحزم TACACS+ (منفذ TCP رقم 49) بالدخول والخروج.إذا عرض الفشل كخدمة مرفوضة في السجل، فلن يتم تمكين خدمة (EXEC Shell) بشكل صحيح ضمن ملف تعريف المستخدم أو المجموعة على خادم TACACS+.
3. إذا كانت مصادقة الاختبار ناجحة، وتستمر عمليات التسجيل في الدخول إلى مركز VPN 3000 في الفشل، فتحقق من سجل الأحداث القابل للتصفية عبر منفذ وحدة التحكم.إذا رأيت رسالة مماثلة:

```
SEV=5 AUTH/32 RPT=2 13:14:40.150 02/09/2005 65
.User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon
Status: <REFUSED> authorization failure. NO Admin Rights
```

يشير هذا الرسالة إلى أن مستوى الامتياز المعين على خادم TACACS+ لا يحتوي على مستوى وصول AAA مطابق تحت أي من مستخدمي مركز VPN 3000. على سبيل المثال، يتمتع المستخدم jsmith بمستوى امتياز TACACS+ على خادم TACACS+، ولكن لا يتمتع أي من مسؤولي مركز VPN 3000 الخمسة بمستوى وصول AAA يبلغ 7.

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series

- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم مفاوضة IPSec/بروتوكولات IKE
- صفحة دعم TACACS/TACACS+
- TACACS+ في وثائق 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).