Hoe u de Cisco VPN 3000 Concentrator configureren voor ondersteuning van TACACS+ verificatie voor beheerrekeningen

Inhoud

Inleiding

Dit document bevat stap-voor-stap instructies om Cisco VPN 3000 Series Concentrators te configureren om de TACACS+ verificatie voor beheerrekeningen te ondersteunen.

Zodra een TACACS+ server op de VPN 3000 Concentrator is geconfigureerd worden de lokaal ingestelde accountnamen en wachtwoorden zoals admin, configuratie, isp, enzovoort niet langer gebruikt. Alle logins naar de VPN 3000 Concentrator worden naar de geconfigureerde externe TACACS+-server verzonden voor gebruikers- en wachtwoordverificatie.

De definitie van een voorkeursniveau voor elke gebruiker op de TACACS+ server bepaalt de permissies op de VPN 3000 Concentrator voor elke TACACS+ gebruikersnaam. Pak dat vervolgens op met het AAA-toegangsniveau dat onder de lokaal ingestelde gebruikersnaam in de VPN-centrator 3000 is gedefinieerd. Dit is een belangrijk punt omdat zodra een TACACS+ server is gedefinieerd, de lokaal ingestelde gebruikersnamen op de VPN 3000 Concentrator niet langer geldig zijn. Maar ze worden nog steeds uitsluitend gebruikt om het retourniveau van voorrechten op te halen van de TACACS+ server, met het AAA Access Level onder die lokale gebruiker. De gebruikersnaam voor TACACS+ wordt dan de rechten toegewezen die de lokaal geconfigureerde VPN 3000 Concentrator-gebruiker onder hun profiel heeft gedefinieerd.

Bijvoorbeeld, in de configuratiesecties uitvoerig beschreven, wordt een TACACS+ gebruiker/groep geconfigureerd om een TACACS+ bevoorrecht niveau van 15 terug te geven. Onder het gedeelte Administrators van de VPN 3000 Concentrator is de beheerder zijn AAA Toegangsniveau ook ingesteld op 15. Deze gebruiker mag de configuratie onder alle secties wijzigen en bestanden lezen/schrijven. Omdat het niveau van TACACS+ bevoorrechte toegang en het niveau van AAA toegang worden aangepast, krijgt de gebruiker TACACS+ die permissies op de VPN 3000 Concentrator.

Als u bijvoorbeeld beslist dat een gebruiker de configuratie moet kunnen wijzigen maar bestanden *niet* lezen/schrijven moet lezen/schrijven, dan moet u een bevoorrecht niveau van 12 op de TACACS+ server toewijzen. U kunt een willekeurig aantal tussen één en 15 kiezen. Kies vervolgens op de VPN 3000-centrator een van de andere lokaal geconfigureerde beheerders. Stel vervolgens het AAA Access Level op 12 in en stel de toegangsrechten op deze gebruiker in om de configuratie te kunnen wijzigen, maar niet om bestanden te lezen/schrijven. Vanwege het overeenkomende privilege/toegangsniveau krijgt de gebruiker die rechten wanneer hij inlogt.

De lokaal ingestelde gebruikersnamen in de VPN 3000 Concentrator worden niet langer gebruikt. Maar de toegangsrechten en AAA-toegangsniveaus onder elk van deze gebruikers worden gebruikt om de privileges te definiëren die een bepaalde TACACS+-gebruiker krijgt wanneer u inlogt.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Zorg ervoor dat u IP-connectiviteit hebt naar de TACACS+ server vanaf de VPN 3000-centrator. Als uw TACACS+ server naar de openbare interface is gericht, vergeet dan niet de TACACS+ (TCP poort 49) op het openbare filter te openen.
- Zorg ervoor dat back-uptoegang via de console beschikbaar is. Het is gemakkelijk om per ongeluk alle gebruikers uit de configuratie te halen wanneer u dit voor het eerst instelt. De enige manier om toegang te herstellen is via de console, die nog steeds de lokaal ingestelde gebruikersnaam en wachtwoorden gebruikt.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 3000 Concentrator-softwarerelease 4.7.2.B (Alternatief: elke release van 3.0 of hoger OS-software werkt.)
- Cisco Secure Access Control Server voor Windows Server release 4.0 (Alternatief voor elke release van 2.4 of hoger software werkt.)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

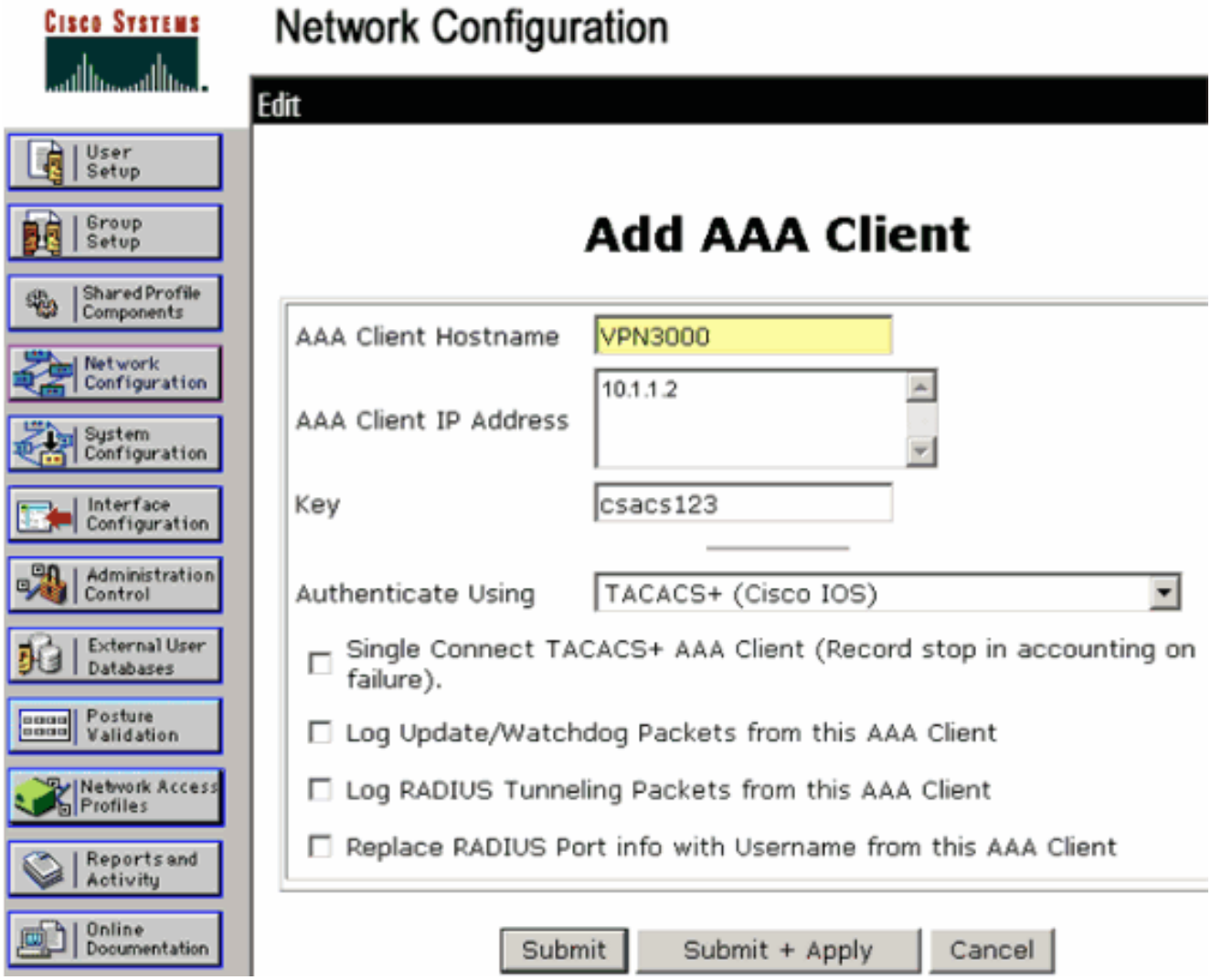
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

De TACACS+ server configureren

Voeg een Ingang voor de VPN 3000 Concentrator in de TACACS+ server toe

Voltooi deze stappen om een ingang voor de VPN 3000 Concentrator in de TACACS+ server toe te voegen.

1. Klik in het linkerpaneel op **Network Configuration**. Klik onder AAA-clients op **Toevoegen**.
2. Vul in het volgende venster het formulier in om de VPN-Concentrator aan de TACACS+ client toe te voegen. In dit voorbeeld wordt gebruik gemaakt van:AAA-clientnaam = **VPN3000**AAA client-IP-adres = **10.1.1.2**Sleutel = **cas123**Verifiëren met behulp van = **TACACS+ (Cisco IOS)**Klik op **Inzenden + opnieuw starten**.



Een gebruikersaccount in de TACACS+ server toevoegen

Voltooi deze stappen om een gebruikersaccount aan de TACACS+ server toe te voegen.

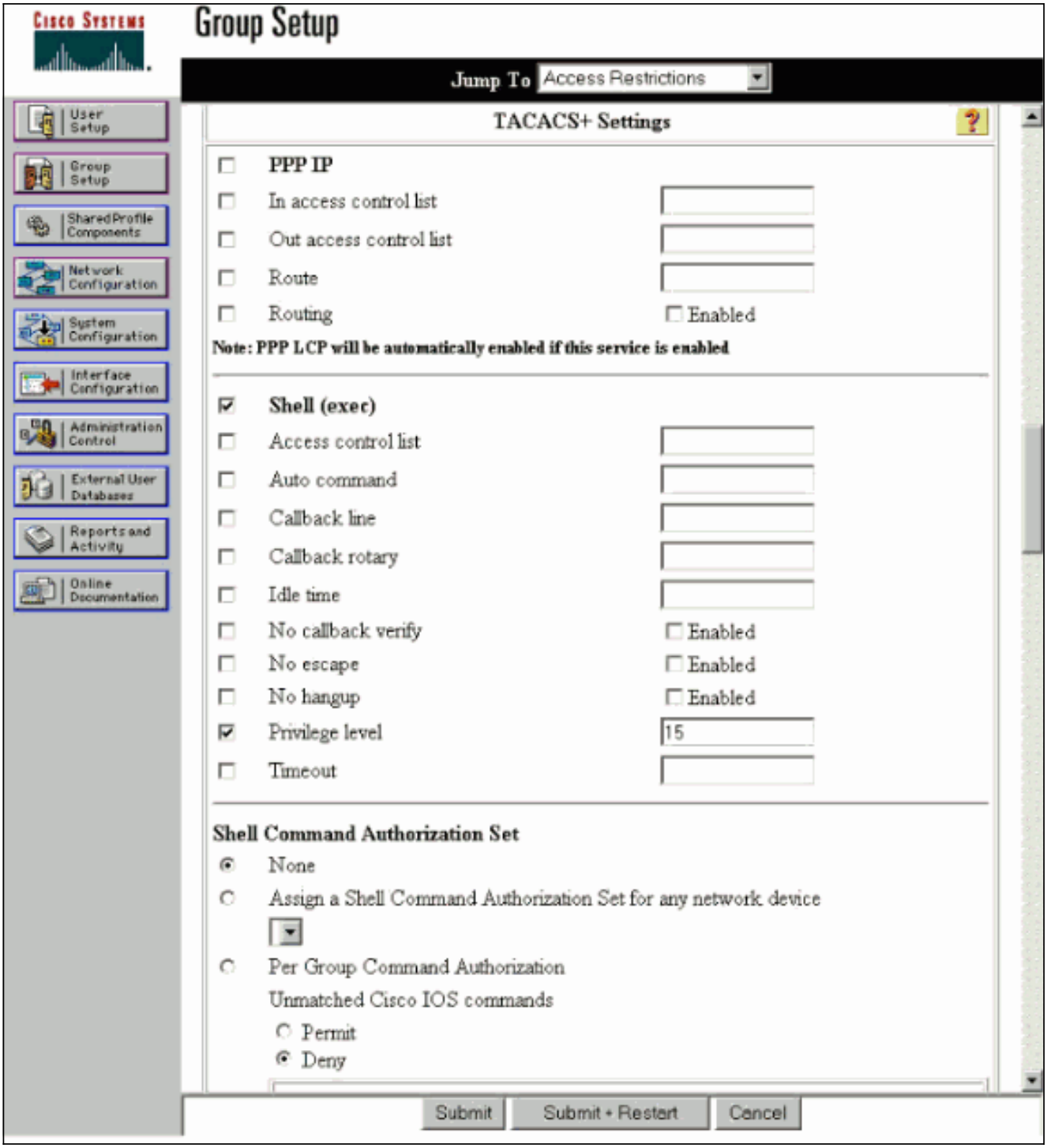
1. Maak een gebruikersaccount in de TACACS+ server die later kan worden gebruikt voor

TACACS+ verificatie. Klik op **Gebruikersinstelling** in het linker paneel, voeg gebruiker "johnsmith" toe en klik op **Add/Edith** om dit te doen.
2. Voeg een wachtwoord voor deze gebruiker toe, en wijs de gebruiker aan een ACS groep toe die de andere VPN 3000 Concentrator beheerders bevat.**Opmerking:** Dit voorbeeld definieert het voorkeursniveau onder dit specifieke ACS-groepsprofiel van gebruikers. Als dit op een gebruikersbasis moet worden gedaan, kiest u **Interfaceconconfiguratie > TACACS+ (Cisco IOS)** en controleert u het **gebruikersvenster** voor de Shell (exec) service. Alleen dan zijn de opties TACACS+ die in dit document zijn beschreven, beschikbaar onder elk gebruikersprofiel.

Bewerk de groep op de TACACS+ server

Voltooi deze stappen om de groep op de TACACS+ server te bewerken.

1. Klik op **Groepsinstallatie** in het linker paneel.
2. Kies in het vervolgkeuzemenu de groep waaraan de gebruiker is toegevoegd in het gedeelte Een gebruikersaccount toevoegen in het gedeelte TACACS+ server, dat in dit voorbeeld groep 1 is, en klik op **Instellingen bewerken**.
3. Zorg ervoor dat deze eigenschappen in het volgende venster zijn geselecteerd onder TACACS+ Instellingen:**Shell (exec)Privigiteitsniveau = 15**Klik na voltooiing op **Inzenden + opnieuw starten**.



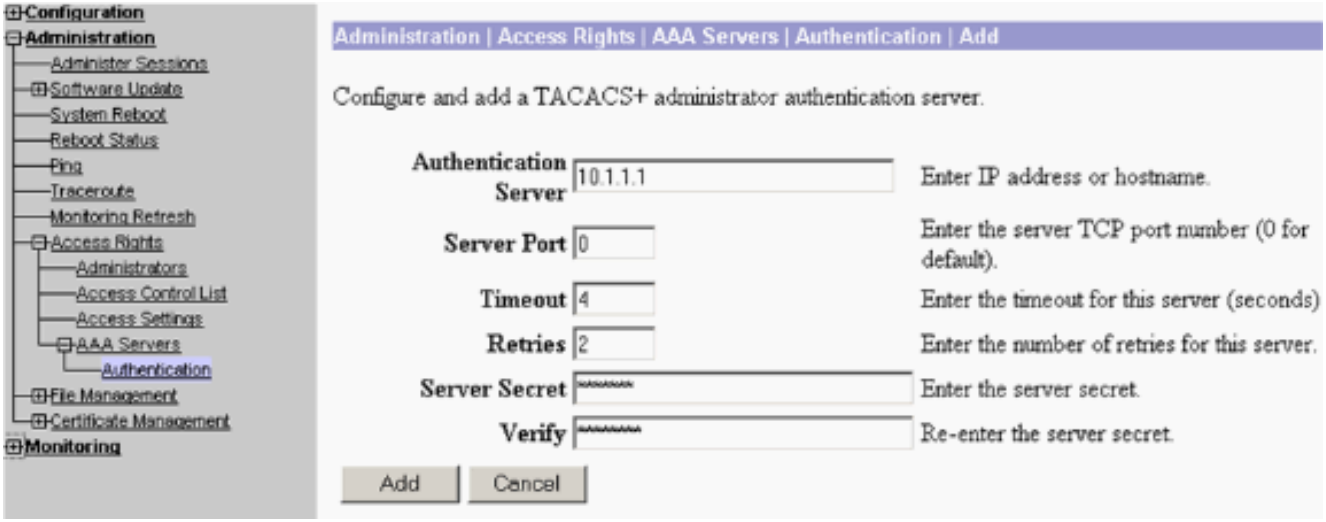
De VPN 3000-concentratie configureren

Voeg een ingang voor de TACACS+ server in de VPN 3000 Concentrator toe

Voltooi deze stappen om een ingang voor de TACACS+ server in de VPN 3000 Concentrator toe te voegen.

1. Kies **Beheer > Toegangsrechten > AAA-servers > Verificatie** in de navigatieboom in het linker paneel en klik vervolgens op **Toevoegen** in het rechterpaneel.Zodra u op **Add** klikt om deze server toe te voegen, worden de lokaal ingestelde gebruikersnaam/wachtwoorden in de VPN 3000 Concentrator niet langer gebruikt. Zorg ervoor dat back-uptoegang via de console werkt in het geval van een uitsluiting.

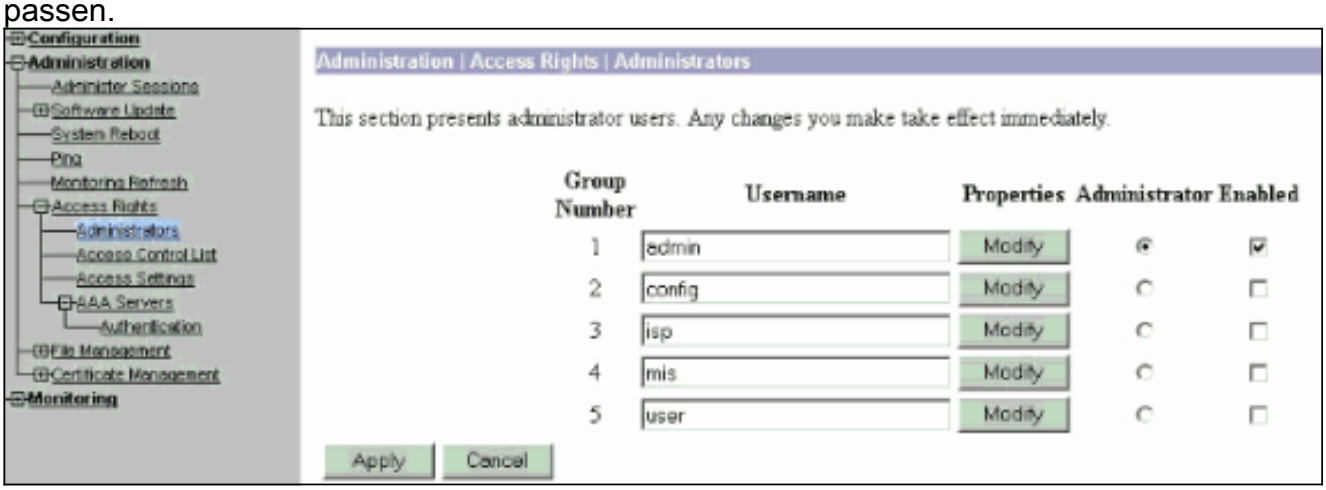
2. Vul in het volgende venster het formulier in zoals hieronder wordt getoond:Verificatieserver = **10.1.1.1** (IP-adres van TACACS+ server)Server poort = **0** (standaard)Time-out = **4**Retries = **2**Servergeheim = **SCS123**Verifiëren = **blokkeren123**



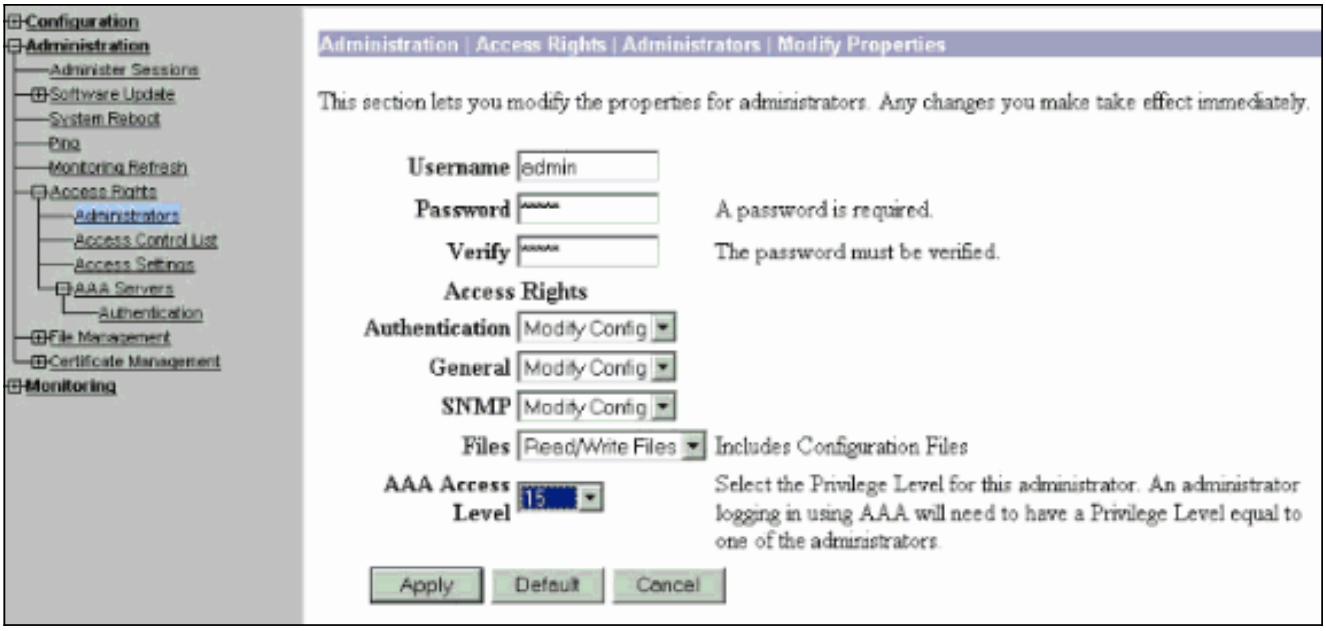
Admin-account wijzigen op VPN Concentrator voor TACACS+ verificatie

Voltooi deze stappen om de admin-account op de VPN-Concentrator aan te passen voor TACACS+-verificatie.

1. Klik op **Wijzigen** voor de gebruikersbeheerder om de eigenschappen van deze gebruiker aan te passen.



2. Kies het AAA-toegangsniveau als **15**.Deze waarde kan een getal tussen één en 15 zijn. Merk op dat de waarde moet overeenkomen met het niveau TACACS+ bevoorrecht dat is gedefinieerd onder het gebruiker/groepsprofiel op de TACACS+ server. De TACACS+ gebruiker pakt dan de permissies op die onder deze VPN 3000 Concentrator-gebruiker zijn gedefinieerd voor de wijziging van de configuratie-, lees-/schrijfbestanden, enzovoort.



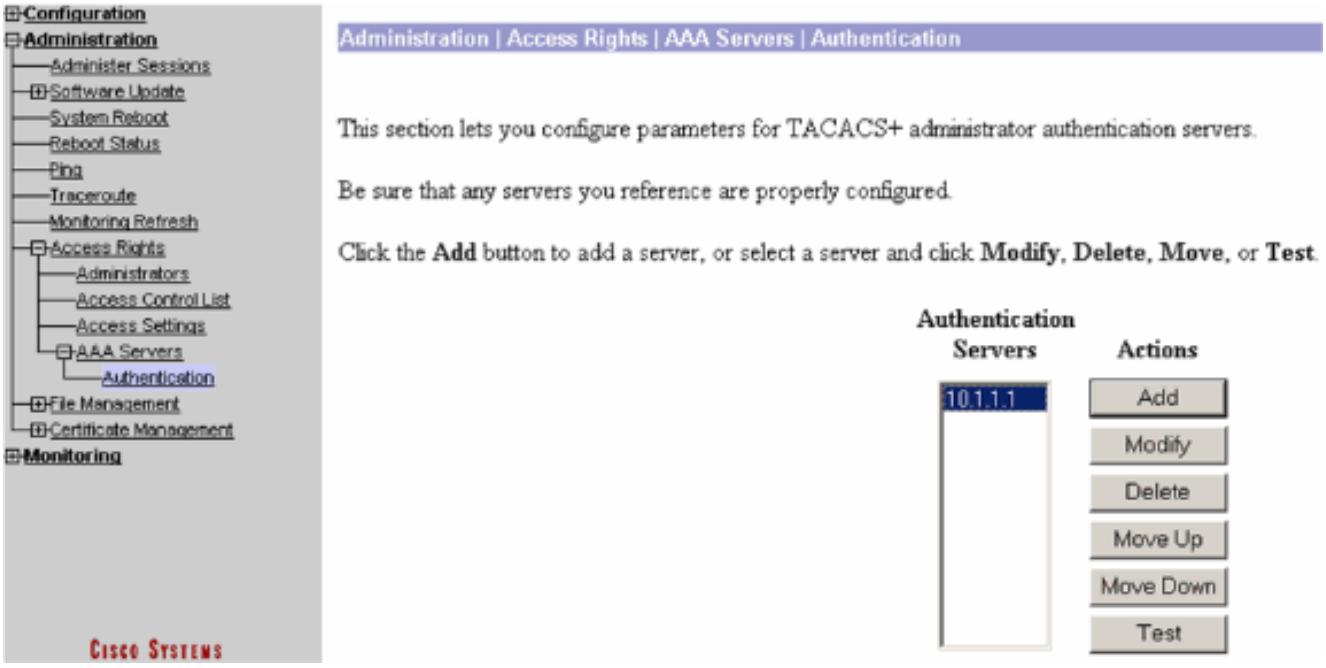
Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

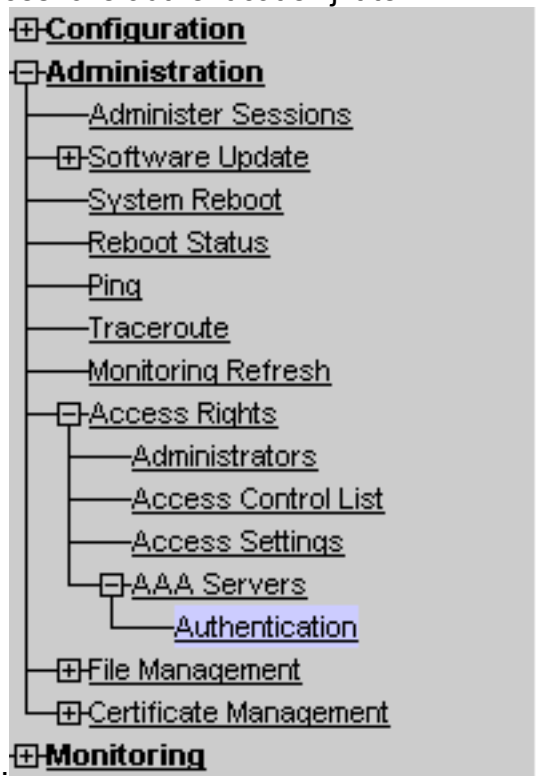
Volg de stappen in deze instructies om uw configuratie problemen op te lossen.

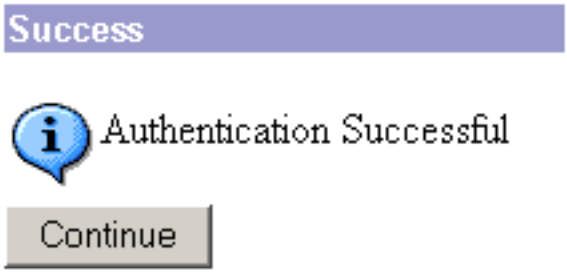
1. Om de echtheidscontrole te testen:Voor TACACS+ serversKies **Beheer > Toegangsrechten > AAA-servers > Verificatie**.Selecteer uw server en klik vervolgens op **Test**.



Opmerking: Wanneer de TACACS+ server is ingesteld op het tabblad Beheer, is er geen manier om de gebruiker in te stellen om de lokale VPN-database van 3000 voor echt te maken. U kunt alleen een back-up uitvoeren met een andere externe database of een TACACS-server.Voer de gebruikersnaam en het wachtwoord voor TACACS+ in en klik op **OK**.

Een succesvolle authenticatie lijkt te





bestaan.

2. Als het mislukt, is er een configuratieprobleem of een IP-connectiviteit-probleem. Controleer de mislukte pogingen om op de ACS-server in te loggen op berichten met betrekking tot de fout.Als er geen berichten in dit logbestand verschijnen is er waarschijnlijk een probleem met IP-connectiviteit. Het TACACS+ verzoek bereikt de TACACS+ server niet. Controleer de filters die op de juiste VPN 3000 Concentrator-interface worden toegepast en stelt TACACS+ (TCP poort 49) pakketten in en uit in.Als de mislukkingen worden weergegeven zoals de service in het logbestand wordt ontkend, is de Shell (exec)-service niet correct ingeschakeld onder het gebruikers- of groepsprofiel op de TACACS+ server.
3. Als de testverificatie geslaagd is, maar de logins bij de VPN 3000 Concentrator blijven mislukken, controleert u het logbestand van gebeurtenis voor filtering via de console-poort.Als je een vergelijkbaar bericht ziet:

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

Dit bericht geeft aan dat het voorkeursniveau dat op de TACACS+ server is toegewezen, niet gelijk is aan het AAA-toegangsniveau onder een van de VPN 3000 Concentrator-gebruikers. De gebruiker johnsmith heeft bijvoorbeeld een TACACS+ voorkeursniveau van 7 op de TACACS+ server, maar geen van de vijf VPN 3000 Concentrator-beheerders heeft een AAA-toegangsniveau van 7.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Cisco VPN 3000 Series clientondersteuningspagina
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Ondersteuningspagina voor TACACS/TACACS+
- TACACS+ in IOS-documentatie
- Technische ondersteuning en documentatie – Cisco Systems