Cómo configurar el Cisco VPN 3000 Concentrator para soportar autenticación de TACACS+ para las Cuentas de administración

Contenido

Introducción

Este documento proporciona las instrucciones paso a paso para configurar el Concentradores Cisco VPN de la serie 3000 para soportar autenticación de TACACS+ para las Cuentas de administración.

Tan pronto como un servidor TACACS+ se configure en el concentrador VPN 3000, los nombres de la cuenta localmente configurados y las contraseñas tales como admin, los config, ISP, y así sucesivamente, son no se utilizan más. Todos los logines al concentrador VPN 3000 se envían al servidor para el usuario externo configurado y a la verificación de contraseña TACACS+.

La definición de un nivel de privilegio para cada usuario en el servidor TACACS+ determina los permisos en el concentrador VPN 3000 para cada nombre de usuario TACACS+. Entonces, coincidencia que encima con del nivel de acceso AAA definió bajo nombre de usuario localmente configurado en el concentrador VPN 3000. Esto es un punto importante porque tan pronto como se defina un servidor TACACS+, los nombres de usuario localmente configurados en el concentrador VPN 3000 son no más válidos. Pero, los todavía utilizan para hacer juego solamente encima del nivel de privilegio vuelto del servidor TACACS+, con el nivel de acceso AAA bajo ese usuario local. El nombre de usuario TACACS+ entonces se asigna los privilegios que el usuario concentrador VPN 3000 localmente configurado ha definido bajo su perfil.

Por ejemplo, descrito detalladamente en las secciones de configuración, configuran a un usuario TACACS+/al grupo para volver un nivel de privilegio TACACS+ de 15. Bajo sección de los administradores del concentrador VPN 3000, el Usuario administrador hace su nivel de acceso AAA también fijar a 15. Se permite a este usuario modificar la configuración bajo todas las secciones, y a los archivos de lectura/grabación. Porque el nivel de privilegio TACACS+ y el nivel de acceso AAA hacen juego, dan el usuario TACACS+ esos permisos en el concentrador VPN 3000.

Como un ejemplo, si usted decide que un usuario necesita poder modificar la configuración, pero los archivos no de lectura/grabación, les asignan un nivel de privilegio de 12 en el servidor TACACS+. Usted puede escoger cualquier número entre uno y 15. Entonces, en el concentrador VPN 3000, escoja a uno de los otros administradores localmente configurados. Después, fije su nivel de acceso AAA a 12, y fije los permisos en este usuario para poder modificar la configuración, pero no a los archivos de lectura/grabación. Debido al privilegio/el nivel de acceso que corresponden con, el usuario consigue esos permisos cuando inician sesión.

Los nombres de usuario localmente configurados en el concentrador VPN 3000 son no se utilizan más. Pero, los derechos de acceso y los niveles de acceso AAA bajo utilizan cada uno de esos usuarios para definir los privilegios que un usuario determinado TACACS+ consigue cuando usted inicia sesión.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Asegúrese de que usted tenga conectividad del IP al servidor TACACS+ del concentrador VPN 3000. Si su servidor TACACS+ está hacia la interfaz pública, no olvide abrir el TACACS+ (puerto TCP 49) en el Filtro público.
- Asegúrese que el acceso de reserva vía la consola sea operativo. Es fácil bloquear accidentalmente toda la configuración de los de los usuarios cuando usted primero configura esto. La única forma de recuperar el acceso está vía la consola, que todavía utiliza los nombres de usuario y contraseña localmente configurados.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 4.7.2.B del Cisco VPN 3000 Concentrator (alternativamente, cualquier version posterior a 3.0 o OS posterior más reciente del software de sistema operativo funciona.)
- Versión 4.0 de los servidores del Cisco Secure Access Control Server para Windows (alternativamente, cualquier versión de 2.4 o trabajos posteriores del software.)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

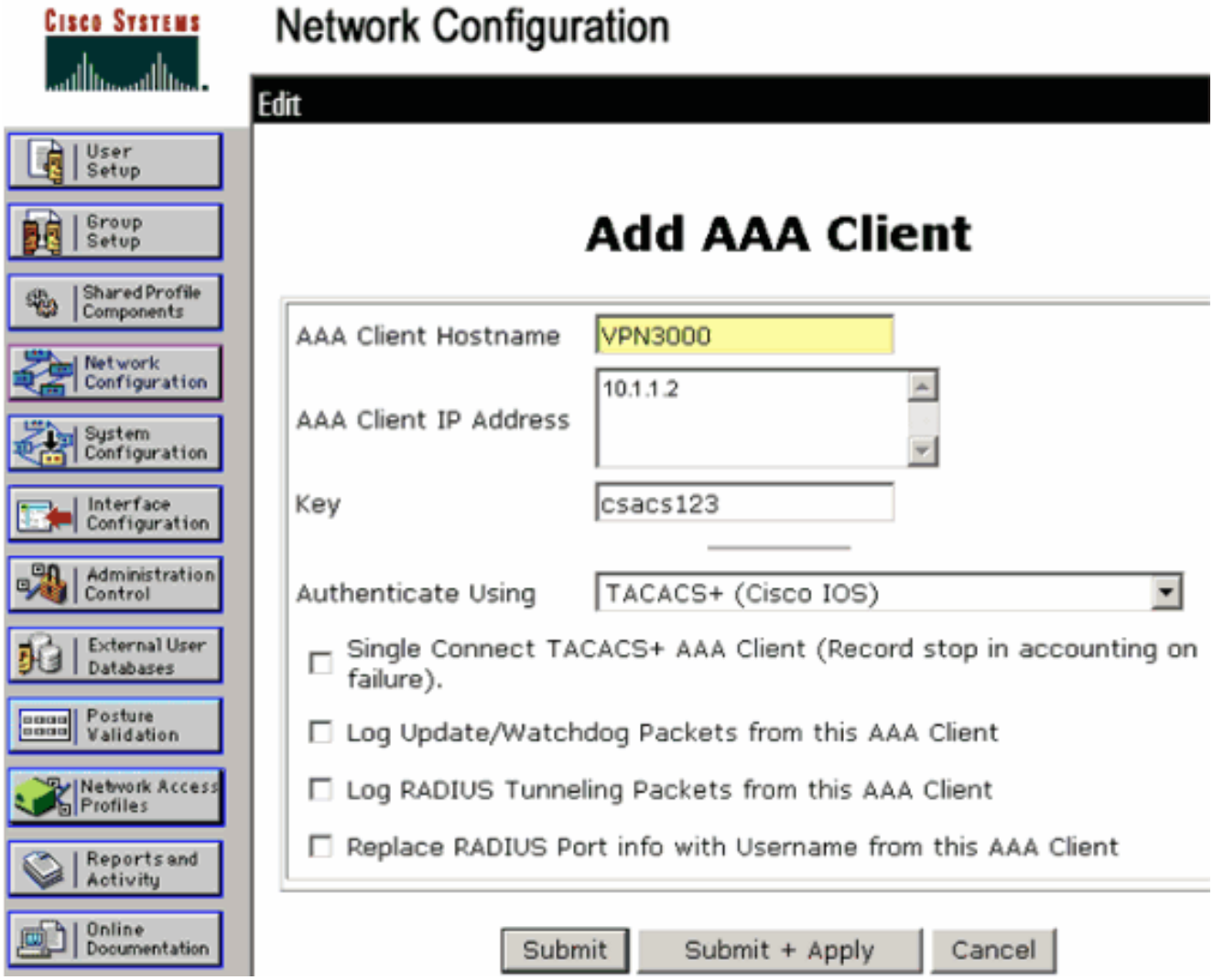
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configure el servidor TACACS+

Agregue una entrada para el concentrador VPN 3000 en el servidor TACACS+

Complete estos pasos para agregar una entrada para el concentrador VPN 3000 en el servidor TACACS+.

1. Haga clic la **configuración de red** en el panel izquierdo. En los clientes AAA, haga clic en Add Entry (Agregar entrada).
2. En la próxima ventana, rellene el impreso para agregar el concentrador VPN como el cliente TACACS+. Este ejemplo utiliza:Nombre del host del cliente AAA = **VPN3000**Dirección IP = **10.1.1.2 del** cliente AAAClave = **csacs123**Autentique usando = **TACACS+ (el Cisco IOS)**Tecleo **Submit +**
   Restart.



Agregue una cuenta de usuario en el servidor TACACS+

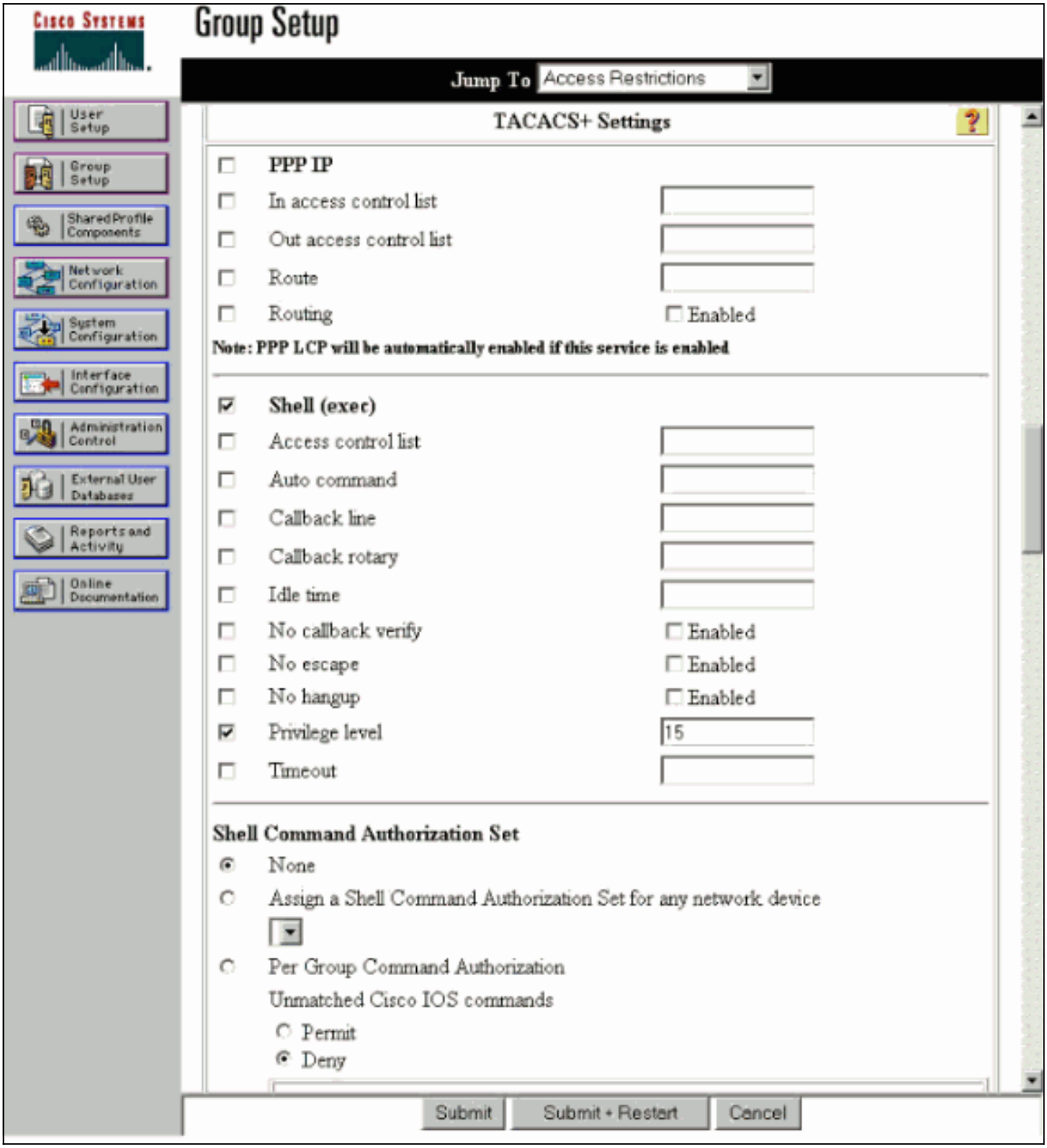
Complete estos pasos para agregar una cuenta de usuario en el servidor TACACS+.

1. Cree una cuenta de usuario en el servidor TACACS+ que se puede utilizar más adelante para autenticación de TACACS+. Haga clic la **configuración de usuario** en el panel izquierdo, agregue al usuario “johnsmith” y el tecleo **agrega/edita** para hacer esto.
2. Agregue una contraseña para este usuario, y asigne al usuario a un grupo ACS que contenga a los otros administradores concentradores VPN 3000.**Nota:** Este ejemplo define el nivel de privilegio bajo este perfil del grupo del usuario determinado ACS. Si se va éste a ser hecho sobre por usuario una base, elija **Interface Configuration > Tacacs+ (Cisco IOS)** y marque el cuadro del **usuario** para el servicio del shell (exec). Entonces están solamente las opciones TACACS+ descritas en este inferior disponible del documento cada perfil del usuario.

Edite al grupo en el servidor TACACS+

Complete estos pasos para editar al grupo en el servidor TACACS+.

1. Haga clic la **configuración de grupo** en el panel izquierdo.
2. Del menú desplegable, elija al grupo que agregaron al usuario en al agregar una cuenta de usuario en la sección del servidor TACACS+, que es group1 en este ejemplo, y el tecleo **edita las configuraciones**.
3. En la próxima ventana, aseegurese que estos atributos están seleccionados bajo configuraciones TACACS+:**Shell (exec)Privilege level=15**Una vez que está hecho, haga clic **Submit +**
   Restart.



Configurar el concentrador VPN 3000

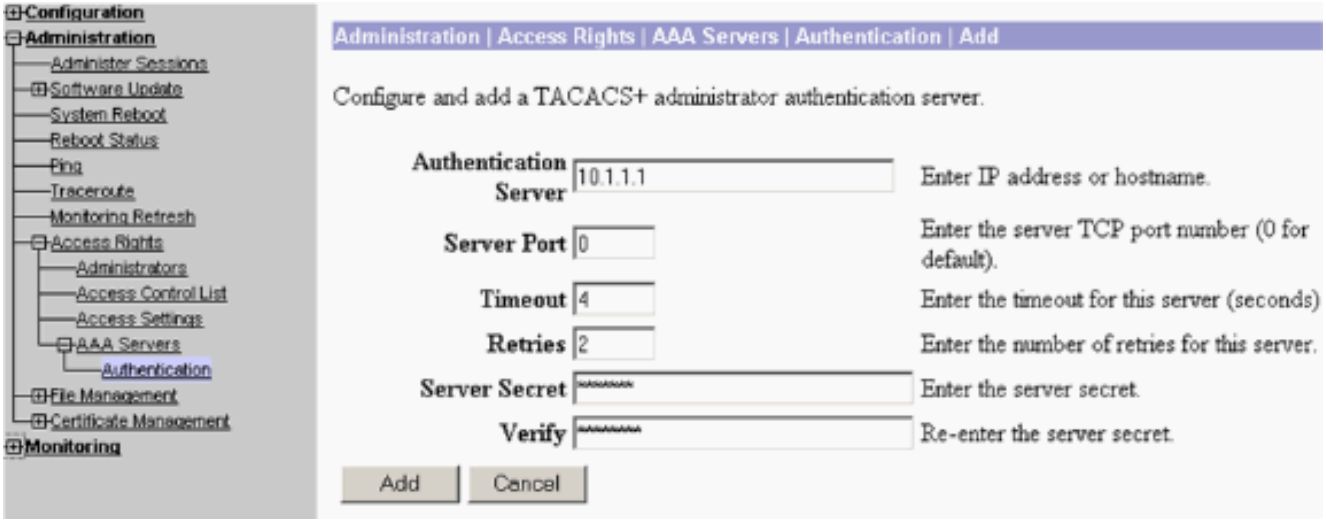
Agregue una entrada para el servidor TACACS+ en el concentrador VPN 3000

Complete estos pasos para agregar una entrada para el servidor TACACS+ en el concentrador VPN 3000.

1. Elija el **Administration (Administración) > Access Rights (Derechos de acceso) > AAA Servers (Servidores AAA) > Authentication (Autenticación)** en el árbol de navegación en el panel izquierdo, y después haga clic **agregan** en el panel derecho.Tan pronto como usted tecleo **agregue** para agregar este servidor, el nombre de usuario/las contraseñas localmente configurados en el concentrador VPN 3000 es no se utilizan más. Asegure el acceso de

reserva vía los trabajos de la consola en caso de un cierre.

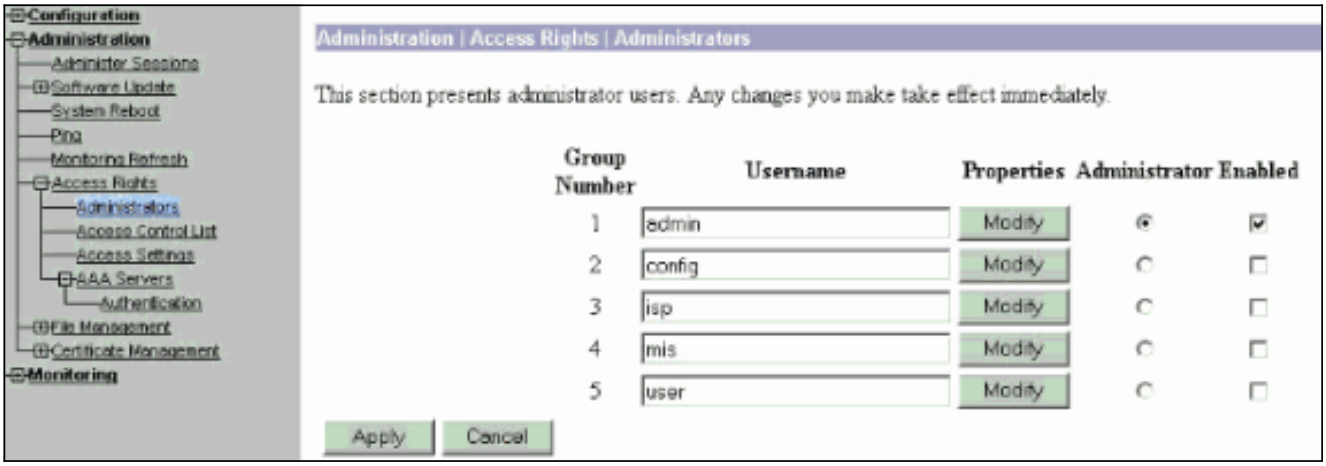
2. En la próxima ventana, rellene el impreso según lo visto aquí:Servidor de autenticación = **10.1.1.1** (dirección IP del servidor TACACS+)Puerto de servidor = **0** (valor por defecto)Descanso = **4**Retries = **2**Secreto de servidor = **csacs123**Verifique = **csacs123**



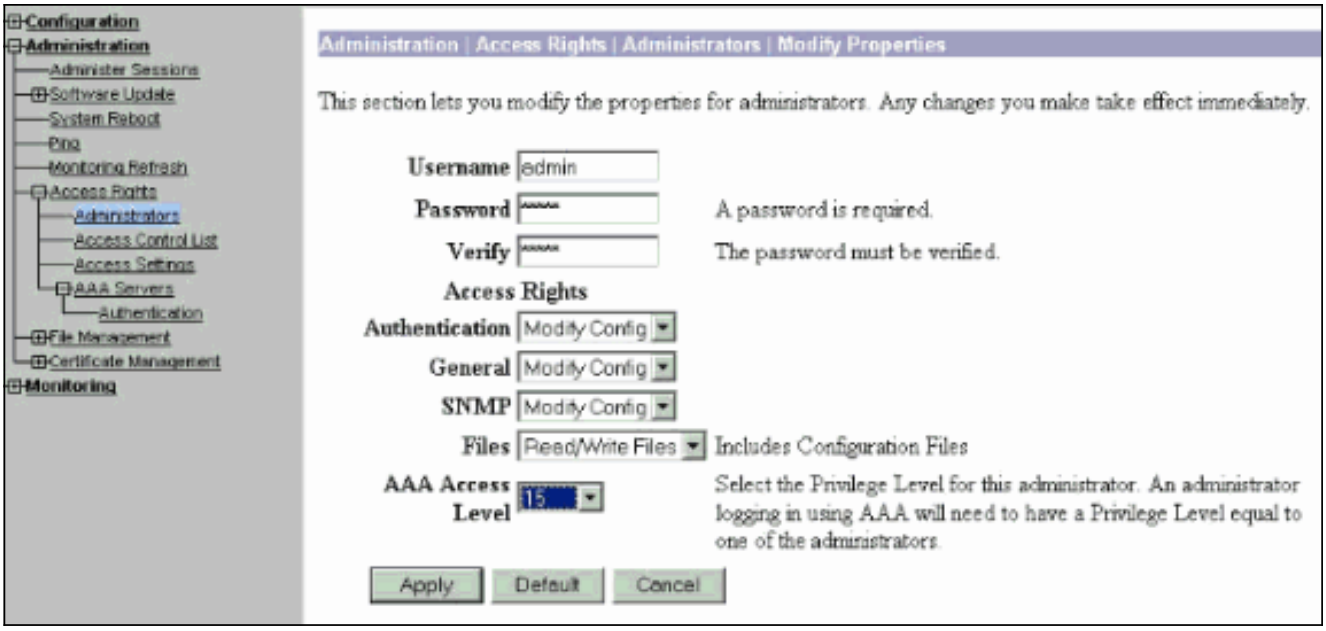
Modifique la cuenta de administración en el concentrador VPN para autenticación de TACACS+

Complete estos pasos para modificar la cuenta de administración en el concentrador VPN para autenticación de TACACS+.

1. El tecleo **se modifica** para el administrador de usuario para modificar las propiedades de este
usuario.



2. Elija el nivel de acceso AAA como **15**.Este valor puede ser cualquier número entre uno y 15. Observe que debe hacer juego el nivel de privilegio TACACS+ definido bajo el usuario/perfil del grupo en el servidor TACACS+. El usuario TACACS+ entonces coge los permisos definidos bajo este usuario concentrador VPN 3000 para la modificación de la configuración, los archivos de la lectura/de la escritura, y así
sucesivamente.



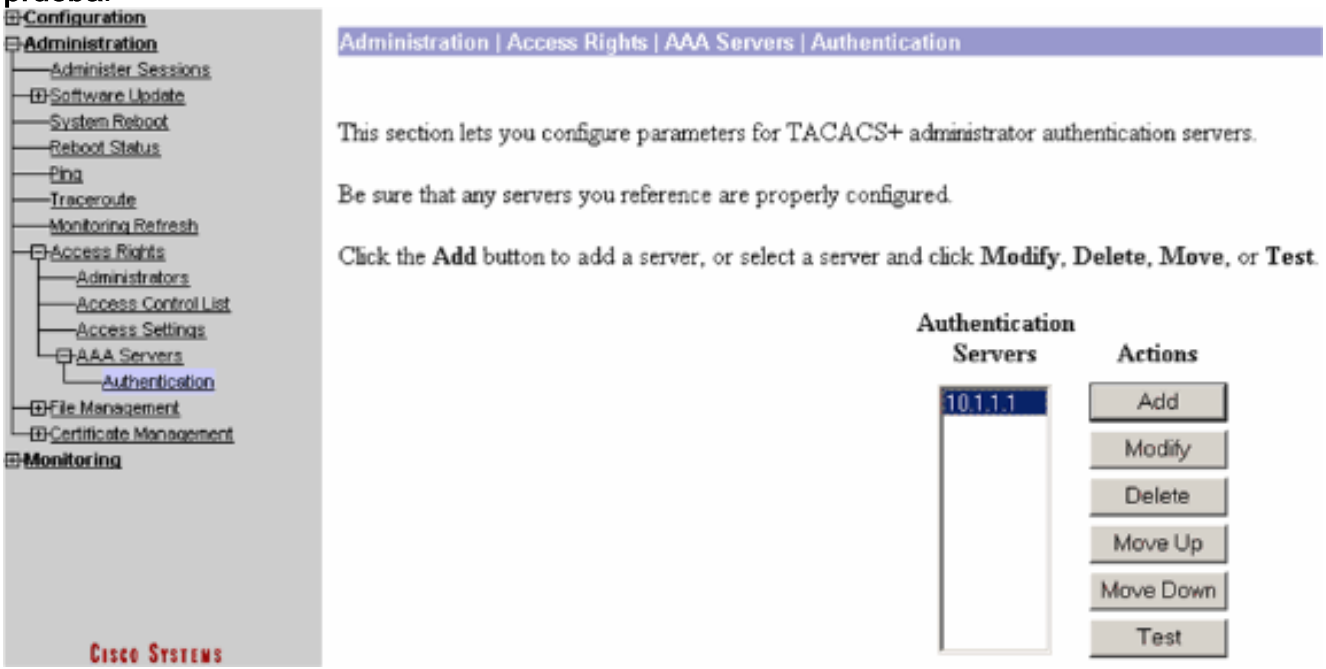
Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Complete los pasos en estas instrucciones para resolver problemas su configuración.

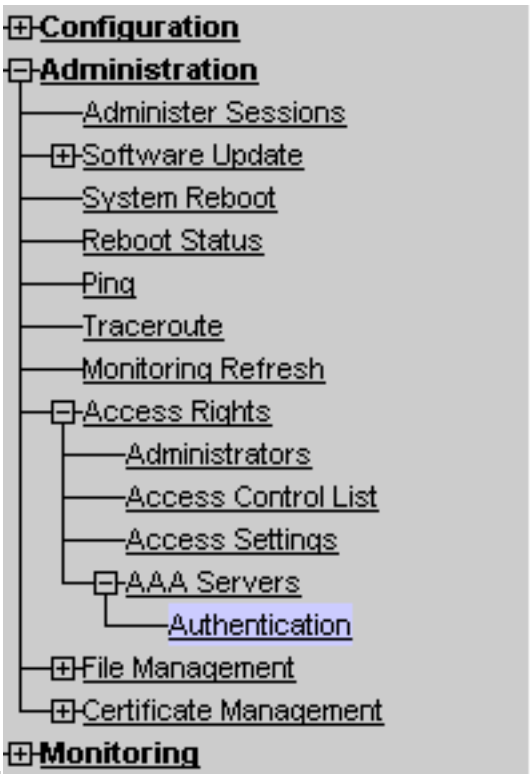
1. Para probar la autenticación:Para los servidores TACACS+Elija el **Administration (Administración) > Access Rights (Derechos de acceso) > AAA Servers (Servidores AAA) > Authentication (Autenticación)**.Seleccione su servidor, y después haga clic la **prueba**.

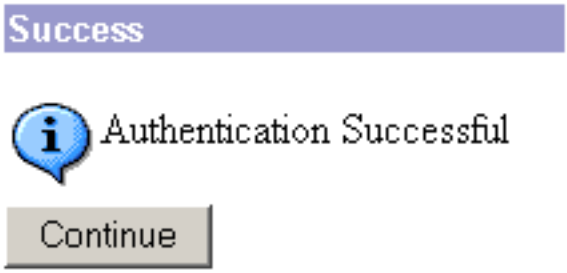


Nota: Cuando el servidor TACACS+ se configura en la lengueta de la administración, no hay manera de configurar al usuario para autenticar en la base de datos local VPN 3000. Usted puede solamente retraso usando otra base de datos externa o servidor TACACS.Ingrese el nombre de usuario y contraseña TACACS+ y haga clic la

AUTORIZACIÓN.

Una autenticación satisfactoria





aparece.

2. Si falla, hay un problema de configuración o un problema de conectividad IP. Marque el inicio de los intentos fallidos el servidor ACS para los mensajes relacionados con el error.Si ningunos mensajes aparecen en este registro entonces hay probablemente un problema de conectividad IP. La petición TACACS+ no alcanza el servidor TACACS+. Verifique los filtros aplicados a la interfaz concentradora VPN 3000 apropiada permite los paquetes TACACS+ (puerto TCP 49) adentro y hacia fuera.Si las visualizaciones del error como servicio negaron en el registro, después el servicio del shell (exec) no se ha habilitado correctamente bajo el usuario o perfil del grupo en el servidor TACACS+.
3. Si la prueba de la autentificación es acertada, pero los logines al concentrador VPN 3000 continúan fallando, marque el registro de eventos filtrables vía el puerto de la consola.Si usted ve un mensaje similar:
   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 Este mensaje indica que el nivel de privilegio asignado en el servidor TACACS+ no tiene ningún nivel de acceso AAA que corresponde con bajo los usuarios concentradores VPN 3000 uces de los. Por ejemplo, el johnsmith del usuario tiene un nivel de privilegio TACACS+ de 7 en el servidor TACACS+, pero ningunos de los cinco administradores concentradores VPN 3000 tienen un nivel de acceso AAA de 7.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- Soporte Técnico y Documentación - Cisco Systems