Cómo Configurar el Cisco VPN 3000 Concentrator para Soportar la Autenticación TACACS+ para las Cuentas de Administración

Contenido

Introducción

Este documento proporciona instrucciones paso a paso para configurar los Cisco VPN 3000 Series Concentrators para soportar la Autenticación TACACS+ para las Cuentas de Administración.

Tan pronto como se configura un servidor TACACS+ en el VPN 3000 Concentrator, los nombres de cuentas y contraseñas configurados localmente como admin, config, isp, etc, ya no se utilizan. Todos los inicios de sesión del concentrador VPN 3000 se envían al servidor TACACS+ externo configurado para la verificación de usuario y contraseña.

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+. Luego, haga coincidir esto con el Nivel de Acceso AAA definido bajo el nombre de usuario configurado localmente en el concentrador VPN 3000. Este es un punto importante porque tan pronto como se define un servidor TACACS+, los nombres de usuario configurados localmente en el concentrador VPN 3000 ya no son válidos. Sin embargo, todavía se utilizan solamente para hacer coincidir el nivel de privilegio devuelto del servidor TACACS+ con el Nivel de acceso AAA bajo ese usuario local. A continuación, se asigna al nombre de usuario TACACS+ los privilegios que el usuario del concentrador VPN 3000 configurado localmente ha definido bajo su perfil.

Por ejemplo, descrito detalladamente en las secciones de configuración, se configura un usuario/grupo TACACS+ para devolver un Nivel de privilegio TACACS+ de 15. En la sección Administradores del VPN 3000 Concentrator, el usuario administrador tiene su nivel de acceso AAA también establecido en 15. Este usuario puede modificar la configuración en todas las secciones y leer/escribir archivos. Debido a que el nivel de privilegio TACACS+ y el nivel de acceso AAA coinciden, el usuario TACACS+ recibe esos permisos en el concentrador VPN 3000.

Por ejemplo, si decide que un usuario debe poder modificar la configuración, pero *no* los archivos de lectura/escritura, asígneles un nivel de privilegio de 12 en el servidor TACACS+. Puede seleccionar cualquier número entre uno y 15. Luego, en el VPN 3000 Concentrator, elija uno de los otros administradores configurados localmente. A continuación, establezca su nivel de acceso AAA en 12 y los permisos de este usuario para poder modificar la configuración, pero no para leer/escribir archivos. Debido al nivel de acceso/privilegio coincidente, el usuario obtiene esos permisos cuando inicia sesión.

Los nombres de usuario configurados localmente en el VPN 3000 Concentrator ya no se utilizan. Sin embargo, los derechos de acceso y los niveles de acceso AAA bajo cada uno de esos usuarios se utilizan para definir los privilegios que un usuario TACACS+ en particular obtiene al iniciar sesión.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Asegúrese de tener conectividad IP con el servidor TACACS+ desde el concentrador VPN 3000. Si su servidor TACACS+ se dirige a la interfaz pública, no olvide abrir el TACACS+ (puerto TCP 49) en el filtro público .
- Asegúrese de que el acceso a la copia de seguridad a través de la consola esté operativo. Es fácil bloquear accidentalmente a todos los usuarios fuera de la configuración cuando se configura por primera vez. La única manera de recuperar el acceso es a través de la consola, que todavía utiliza los nombres de usuario y las contraseñas configurados localmente.

Componentes Utilizados

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

- Cisco VPN 3000 Concentrator Software Release 4.7.2.B (Alternativamente, cualquier versión de 3.0 o posterior del software del sistema operativo funciona).
- Cisco Secure Access Control Server para Windows Servers Versión 4.0 (Alternativamente, cualquier versión de software 2.4 o posterior funciona).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

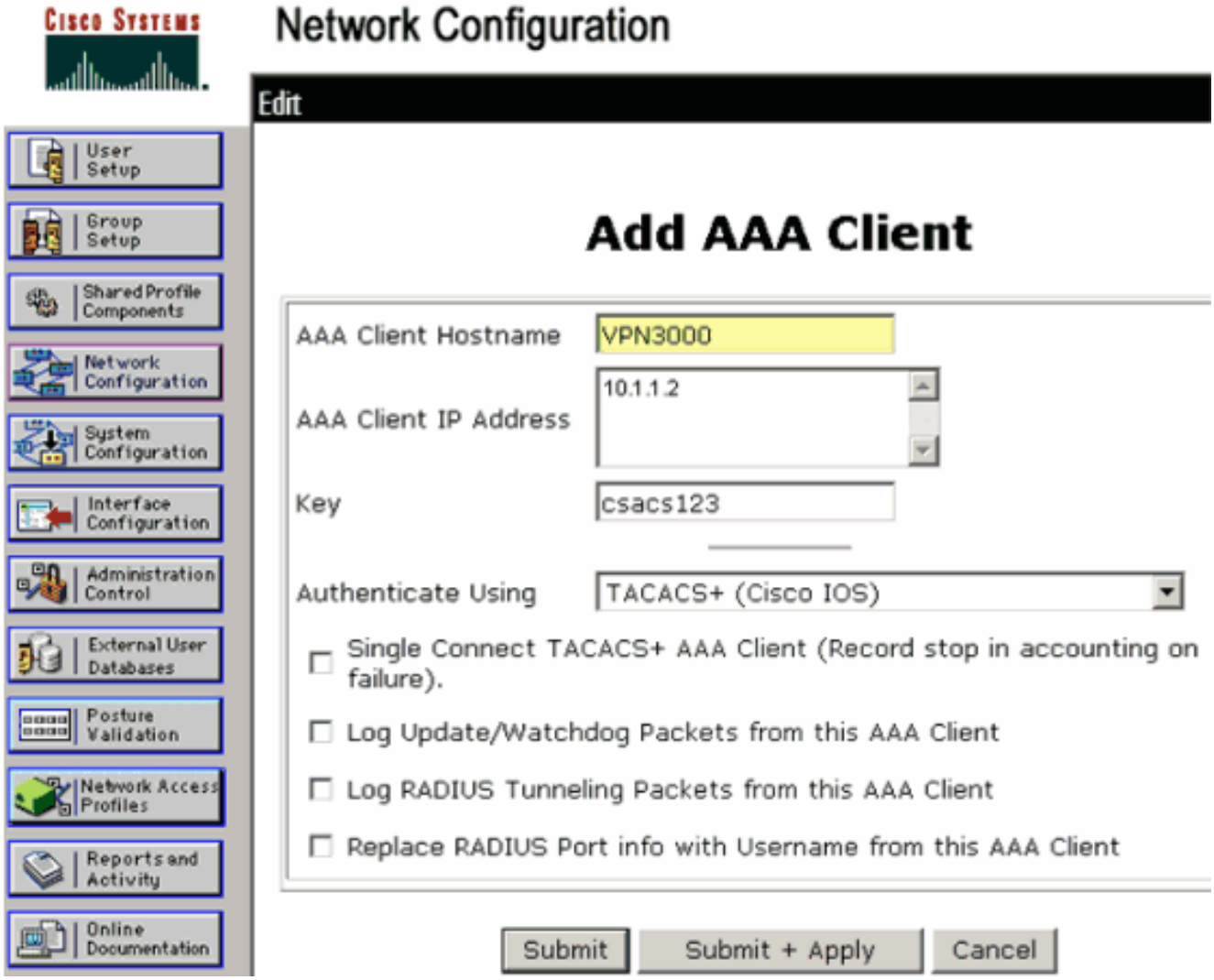
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración del servidor TACACS+

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

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

1. Haga clic en **Configuración de red** en el panel izquierdo. En los clientes AAA, haga clic en Add Entry (Agregar entrada).
2. En la siguiente ventana, rellene el formulario para agregar el concentrador VPN como cliente TACACS+. Este ejemplo utiliza:Nombre de host del cliente AAA = **VPN3000**AAA Client IP Address = **10.1.1.2**Clave = **csacs123**Autenticar mediante = **TACACS+ (Cisco IOS)**Haga clic en **Enviar +**
Reiniciar.



Agregar una cuenta de usuario en el servidor TACACS+

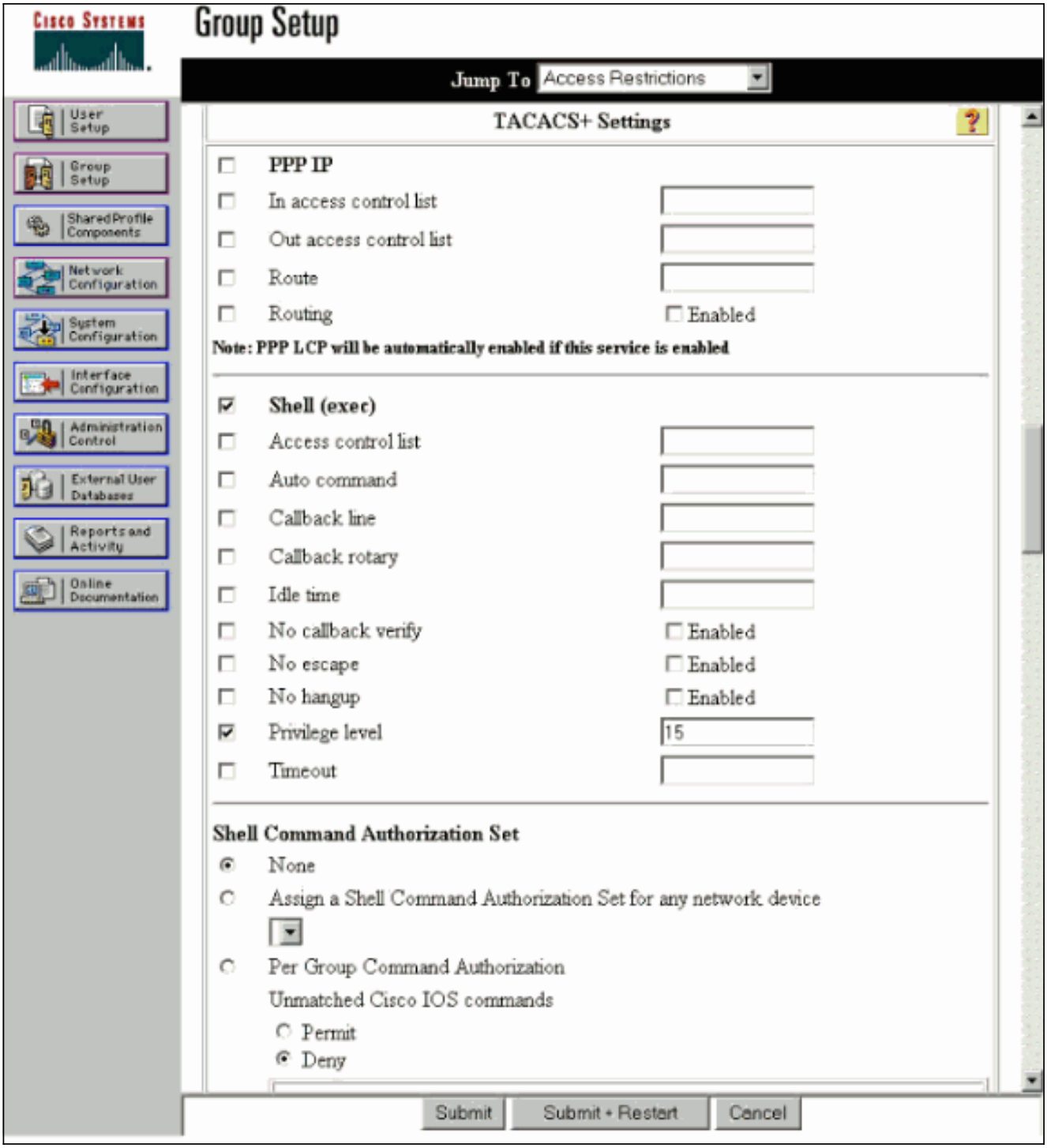
Complete estos pasos para agregar una cuenta de usuario en el servidor TACACS+.

1. Cree una cuenta de usuario en el servidor TACACS+ que pueda utilizarse posteriormente para la autenticación TACACS+. Haga clic en **User Setup** en el panel izquierdo, agregue el usuario "johnsmith" y haga clic en **Add/Edit** para hacerlo.
2. Agregue una contraseña para este usuario y asígnele un grupo ACS que contenga los otros administradores del concentrador VPN 3000.**Nota:** Este ejemplo define el nivel de privilegio bajo este perfil de grupo ACS de usuario en particular. Si esto se debe hacer por usuario, elija **Interface Configuration > TACACS+ (Cisco IOS)** y marque la casilla **User** para el servicio Shell (exec). Sólo entonces están disponibles las opciones TACACS+ descritas en este documento bajo cada perfil de usuario.

Editar el grupo en el servidor TACACS+

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

1. Haga clic en **Group Setup** en el panel izquierdo.
2. En el menú desplegable, elija el grupo al que se agregó el usuario en la sección Agregar una cuenta de usuario de TACACS+ Server, que es Grupo 1 en este ejemplo, y haga clic en **Editar configuración**.
3. En la siguiente ventana, asegúrese de que estos atributos estén seleccionados en Configuración TACACS+:**Shell (exec)Nivel de privilegio = 15**Una vez hecho, haga clic en **Enviar +**
   Reiniciar.



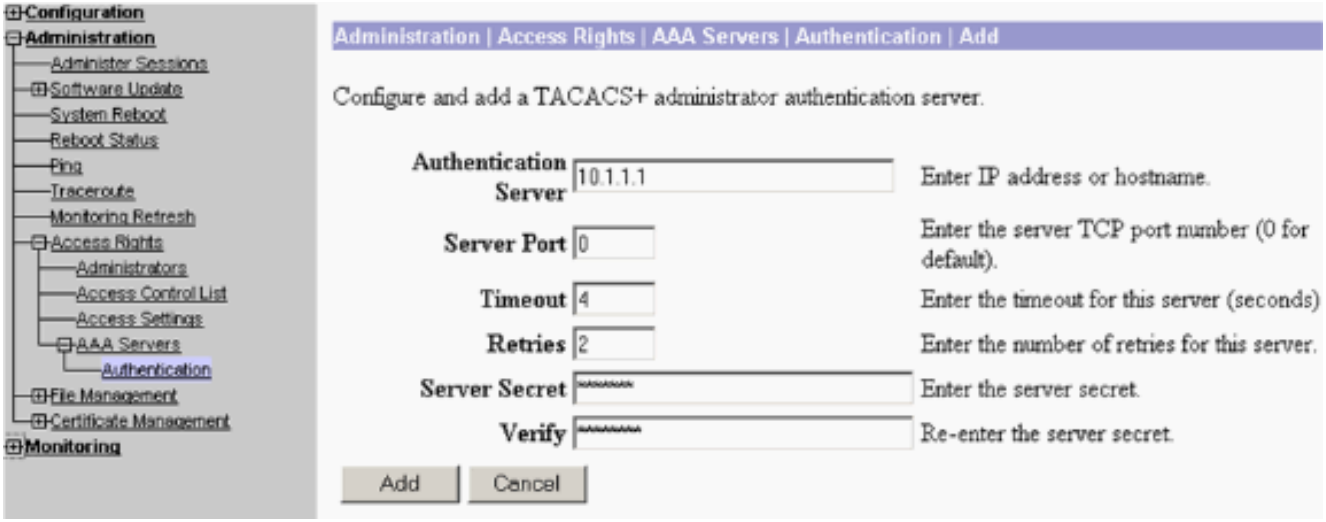
Configurar el concentrador VPN 3000

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

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

1. Elija **Administration > Access Rights > AAA Servers > Authentication** en el árbol de navegación en el panel izquierdo y luego haga clic en **Add** en el panel derecho.Tan pronto como haga clic en **Add** para agregar este servidor, ya no se utilizarán el nombre de usuario/las contraseñas configuradas localmente en el concentrador VPN 3000. Asegúrese de que el acceso de copia de seguridad a través de la consola funciona en caso de bloqueo.

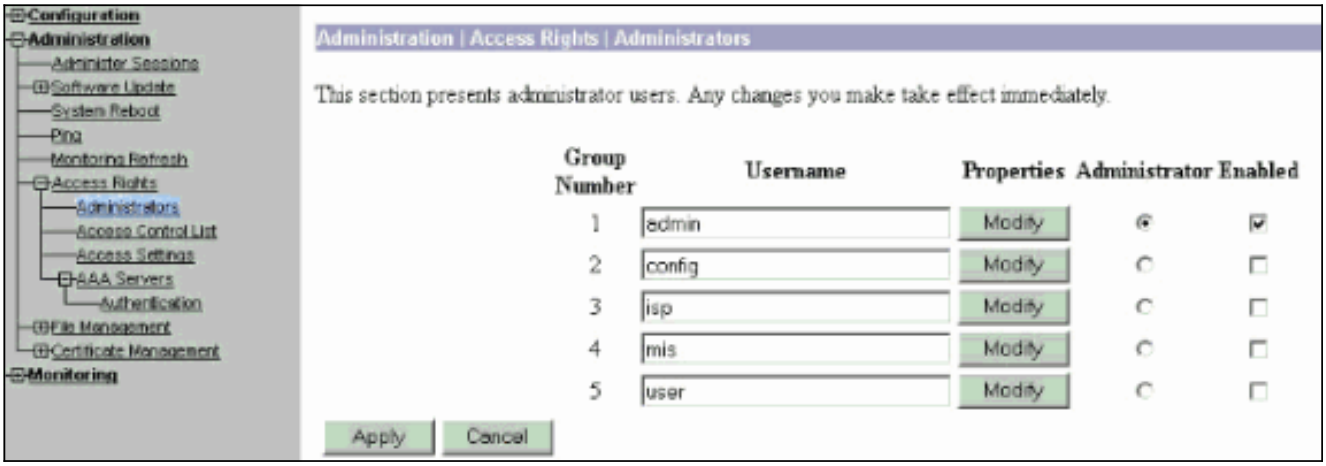
2. En la siguiente ventana, rellene el formulario como se muestra aquí:Servidor de autenticación = **10.1.1.1** (dirección IP del servidor TACACS+)Puerto del servidor = **0** (valor predeterminado)Tiempo de espera = **4**Reintentos = **2**Secreto de servidor = **csacs123**Verificar = **csacs123**



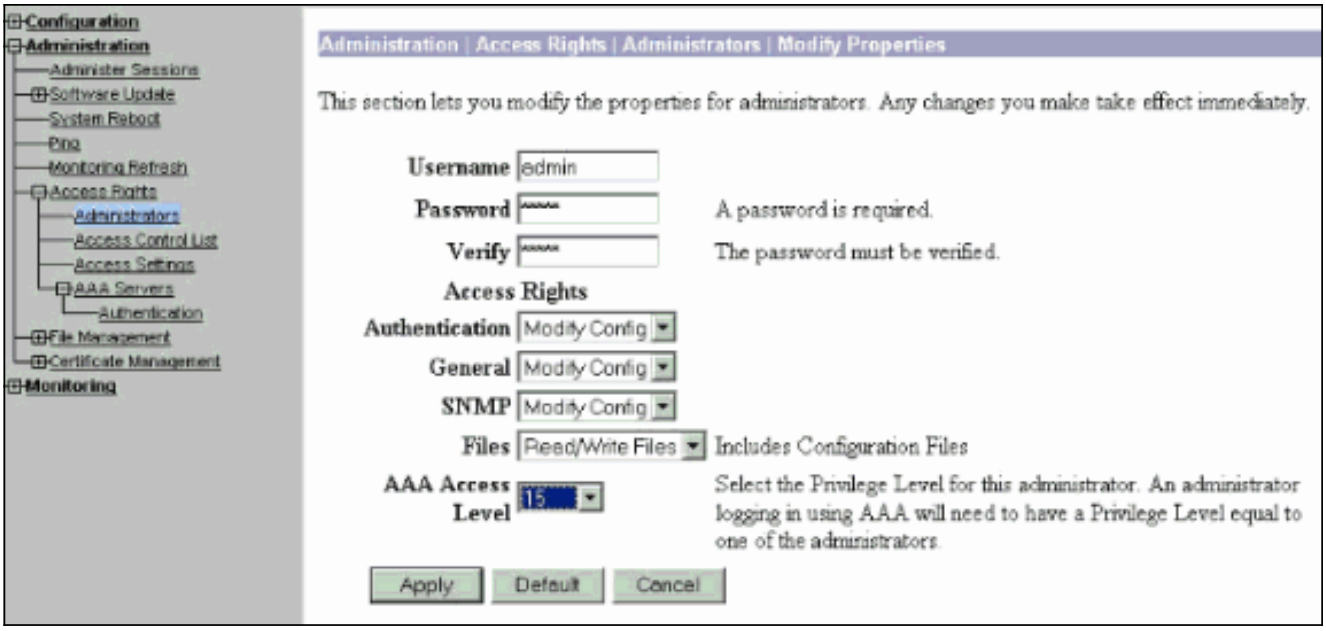
Modifique la cuenta de administrador en el concentrador VPN para la autenticación TACACS+

Complete estos pasos para modificar la cuenta de administrador en el VPN Concentrator para la autenticación TACACS+.

1. Haga clic en **Modificar** 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. Tenga en cuenta que debe coincidir con el nivel de privilegio TACACS+ definido en el perfil de usuario/grupo en el servidor TACACS+. El usuario TACACS+ luego recoge los permisos definidos en este usuario del concentrador VPN 3000 para la modificación de la configuración, la lectura/escritura de archivos, etc.



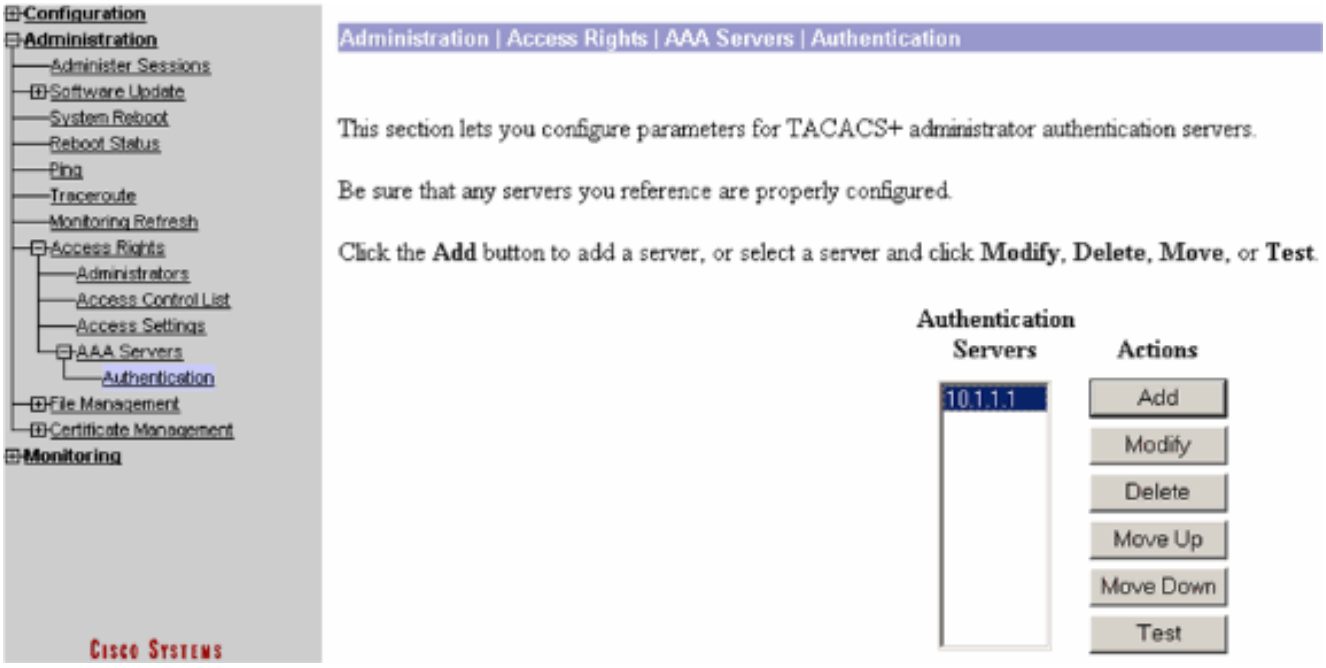
Verificación

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

Troubleshoot

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

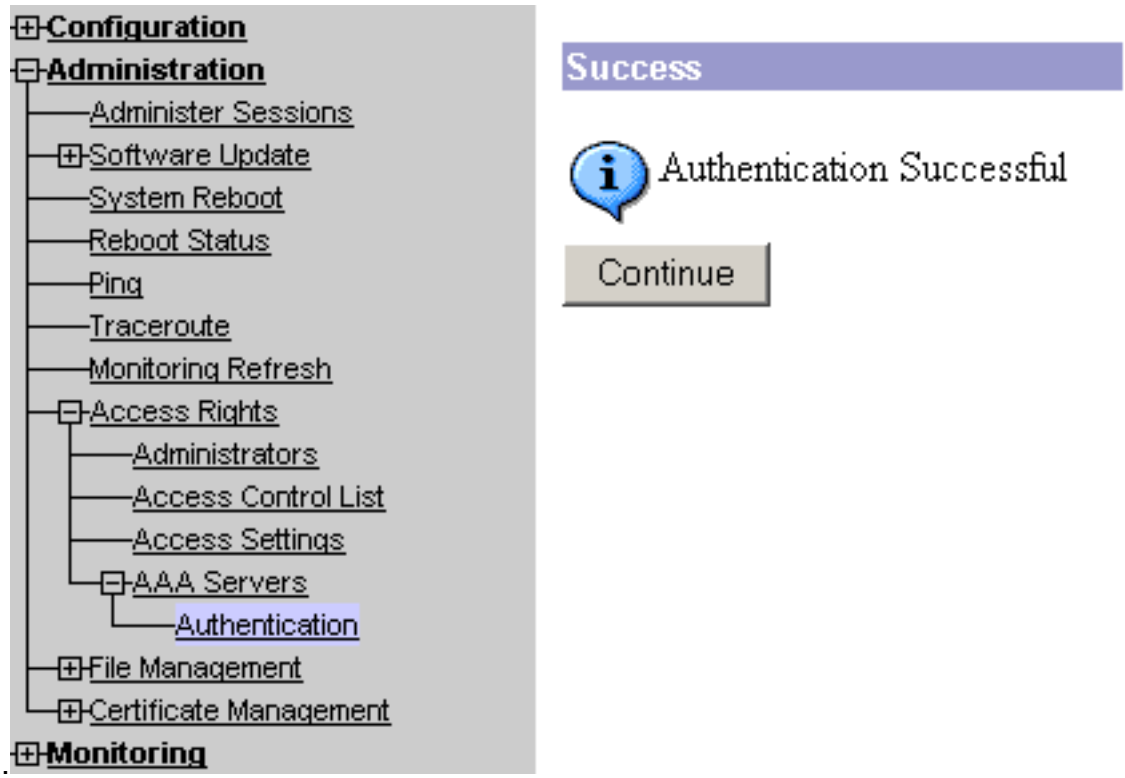
1. Para probar la autenticación:Para servidores TACACS+Elija **Administration > Access Rights > AAA Servers > Authentication**.Seleccione su servidor y, a continuación, haga clic en **Prueba**.



Nota: Cuando el servidor TACACS+ está configurado en la ficha Administration (Administración), no hay forma de configurar el usuario para autenticarse en la base de datos local VPN 3000. Sólo puede realizar una reserva utilizando otra base de datos externa o servidor TACACS.Introduzca el nombre de usuario y la contraseña de TACACS+ y haga clic en

Aceptar.

Aparece una autenticación



correcta.

2. Si falla, hay un problema de configuración o de conectividad IP. Verifique el registro de intentos fallidos en el servidor ACS para los mensajes relacionados con el error.Si no aparece ningún mensaje en este registro, es probable que haya un problema de conectividad IP. La solicitud TACACS+ no llega al servidor TACACS+. Verifique que los filtros aplicados a la interfaz del concentrador VPN 3000 apropiada permitan el ingreso y la salida de paquetes TACACS+ (puerto TCP 49).Si la falla se muestra como servicio denegado en el registro, el servicio Shell (exec) no se ha habilitado correctamente en el perfil de usuario o grupo del servidor TACACS+.
3. Si la autenticación de prueba es exitosa, pero los inicios de sesión en el VPN 3000 Concentrator continúan fallando, verifique el Registro de Eventos Filtrable a través del puerto de la consola.Si 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 un nivel de acceso AAA coincidente en ninguno de los usuarios del concentrador VPN 3000. Por ejemplo, el usuario johnsmith tiene un nivel de privilegio TACACS+ de 7 en el servidor TACACS+, pero ninguno de los cinco administradores del concentrador VPN 3000 tiene 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