Configuración de TACACS+ en el Catalyst 1900 y 2820

Contenido

Introducción

El versión Catalyst 1900/2820 8.x Enterprise Edition soporta TACACS+ (no XTACACS). El TACACS+ o la configuración de usuario del servidor CiscoSecure para la autenticación es lo mismo que para los usuarios del router. Este consejo técnico describe la configuración en el Catalyst 1900 y los 2820.

Nota: La Conmutación por falla en el 1900 y los 2820 se implementa diferentemente que en el otro equipo de Cisco. Si el servidor TACACS+ es inalcanzable, las contraseñas locales pueden ser utilizadas o ninguna autenticación ser requeridas (dependiendo de cómo se configura el Switch). Aunque, si el servidor TACACS+ es accesible pero la daemon TACACS+ está abajo, las contraseñas locales y la Conmutación por falla a ninguna autenticación no sean utilizadas (es decir usted será Switch bloqueado de los).

Nota: Las conexiones Web HTTP se autentican siempre usando la contraseña local (no tacacs+). El uso de las opciones de menú es inválido cuando se habilita el TACACS+. El TACACS+ se utiliza para la autenticación de la interfaz de la línea de comandos.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Pasos de configuración

1. Del comando line interface(cli), habilite autenticación de TACACS+ para el login usando el comando abajo.**inicio de sesión en TACACS**
2. Utilice el comando abajo de decir al Switch donde está el servidor.**host 1.1.1.1 del TACACS-servidor**
3. Utilice el comando abajo de decir al Switch cuáles es la clave compartida.**tacacs-server key cisco**
4. Elija una de las dos opciones abajo.Utilice el comando abajo de decir al Switch la contraseña utilizar si el servidor TACACS+ llega a ser inalcanzable.**nivel 1 Cisco de la contraseña habilitada**Utilice el comando abajo de decir el Switch utilizar la contraseña local si el servidor TACACS+ llega a ser inalcanzable.**contraseña del último-centro turístico del TACACS-servidor**Utilice el comando abajo de decir el Switch dejar a los usuarios adentro sin una contraseña si el servidor TACACS+ llega a ser inalcanzable.**el último-centro turístico del TACACS-servidor tiene éxito**Antes de salir el Switch, Telnet al Switch de otra sesión para estar seguro que usted puede conseguir al usar el TACACS+. Antes de salir el Switch, haga el servidor inalcanzable para estar seguro que usted puede entrar sin usar el TACACS+. Los pasos restantes son opcionales.
5. Utilice el comando abajo de habilitar autenticación de TACACS+ para el enable mode.**habilite el uso-TACACSNota:** Este paso es necesario solamente si se van los usuarios del permiso a ser autenticados a través del servidor TACACS+; también necesita ser una entrada del permiso en el servidor para que esto trabaje.
6. Utilice el comando abajo de habilitar la autenticación local para el enable mode si el servidor TACACS+ llega a ser inalcanzable.**nivel 15 Cisco de la contraseña habilitada**Esta contraseña es válida solamente si la contraseña del último-centro turístico del TACACS-servidor también se configura.
7. Utilice el comando abajo de configurar el número de intentos de inicio de sesión permitidos en el servidor TACACS+.**el TACACS-servidor intenta el *número***
8. Utilice el comando abajo de fijar el intervalo de tiempo de espera en el cual la daemon del servidor debe responder (ésta es opcional, pero podría ser necesaria en una red lenta.**descanso *N del TACACS*-servidor**

Información Relacionada

- Soporte Técnico - Cisco Systems