Resolución de problemas de CSS y TACACS+

Contenido

Introducción

El protocolo del Sistema de control de acceso del controlador de acceso a terminales (TACACS+) brinda control de acceso para routers, servidores de acceso a red (NAS) u otros dispositivos mediante uno o más servidores demonio. Cifra todo el tráfico entre el NAS y la daemon usando las comunicaciones TCP para la entrega confiable.

Este documento brinda información para la solución de problemas del switch de servicio de contenido (CSS) y TACACS+. Puede configurar el CSS como cliente de un servidor TACACS+, dándole un método de autenticación de usuarios, y autorización y contabilidad de comandos de configuración y de otro tipo. Esta característica está disponible en WebNS 5.03.

Nota: Refiera a configurar el CSS como cliente de un servidor TACACS+ para más información.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

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.

Problema

Cuando usted intenta iniciar sesión al CSS con un usuario TACACS+, el login no trabaja.

Solución y comandos debug

Generalmente, cuando autenticación de TACACS+ no trabaja con un CSS, el problema es generalmente un problema de configuración en el CSS o el servidor TACACS+. La primera cosa que usted necesita marcar es si usted ha configurado el CSS como cliente de un servidor TACACS+.

Cuando usted ha marcado esto, hay registración adicional esa usted puede utilizar en el CSS para determinar el problema. Complete estos pasos para dar vuelta encendido a la registración.

En el CSS, ingrese debug mode (modo de depuración).

```
CSS# llama
CSS(debug)# mask tac 0x3
CSS(debug)# exit
CSS# configure
CSS(config)# logging subsystem security level debug-7
CSS(config)# logging subsystem netman level info-6
CSS(config)# exit
CSS# logon
!--- This logs messages to the screen.
```

Para inhabilitar el registro, publique estos comandos:

```
CSS# llama
CSS(debug)# mask tac 0x0
CSS(debug)# exit
CSS# no logon
```

Estos mensajes pueden aparecer:

```
SEP 10 08:30:10 5/1 99 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0c
SEP 10 08:30:10 5/1 100 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:30:10 5/1 101 SECURITY-7: Security Manager sending error 7 reply to
ller 20201c00
```

Estos mensajes indican que el CSS intenta comunicar con el servidor TACACS+, pero el servidor TACACS+ rechaza el CSS. `el error 7` significa que la clave TACACS+ ingresada en el CSS no corresponde con la clave en el servidor TACACS+.

Una registración satisfactoria a través de un servidor TACACS+ muestra este mensaje (observe el `éxito de` envío `0` contestaciones):

```
SEP 10 08:31:46 5/1 107 SECURITY-7: SECMGR:SecurityAuth:Request from 0x20204b0d
```

```
SEP 10 08:31:46 5/1 108 SECURITY-7: SECMGR:SecurityMgrProc:Try Primary
SEP 10 08:31:47 5/1 109 SECURITY-7: Security Manager sending success 0 reply to
caller 20201c00

SEP 10 08:31:47 5/1 110 SECURITY-7: SECMGR:SecurityMgrProc:Try Done, Send 0x2020
4b0d
```

Errores comunes

La mayoría del error común cuando usted configura un CSS para trabajar con un servidor TACACS+ es realmente muy simple. Este comando dice a CSS qué clave a utilizar para comunicar con el servidor TACACS+:

CSS(config)# tacacs-server key system *enterkeyhere*

Esta clave puede ser texto claro o DES cifrada. La clave del texto claro es DES cifrada antes de que la clave se ponga en la configuración corriente. Para hacer un texto claro dominante, póngalo en las citas. Para hacerle el DES cifrado, no utilice las citas. El asunto importante es saber si la clave TACACS+ es DES cifrada o si la clave es texto claro. Después de que usted publique el comando, haga juego la clave del CSS a la clave que el servidor TACACS+ utiliza.

Información Relacionada

- Configuración de CSS como cliente para un servidor TACACS+
- Configuración de TACACS+ y de TACACS+ extendido.
- Soporte Técnico y Documentación - Cisco Systems