Configure a un router Cisco con autenticación de TACACS+

Contenido

Introducción

Este documento describe cómo configurar un router Cisco para la autenticación con TACACS+ que se ejecuta en UNIX. TACACS+ no ofrece tantas funciones como la versión comercializada de Cisco Secure ACS for Windows o Cisco Secure ACS UNIX.

El software TACACS+ proporcionado previamente por Cisco Systems ha sido interrumpido y es soportado no más por Cisco Systems.

Hoy, usted puede encontrar muchas versiones de software libre disponibles TACACS+ cuando usted busca para el “freeware TACACS+” en su motor de búsqueda del Internet favorita. Cisco no recomienda específicamente ninguna implementación determinada del freeware TACACS+.

El Cisco Secure Access Control Server (ACS) está disponible para la compra a través de las ofertas de Cisco y de los canales de distribución regulares por todo el mundo. El Cisco Secure ACS for Windows incluye a todos los componentes necesarios necesarios para una instalación independiente en un puesto de trabajo de Microsoft Windows. El motor de solución del Cisco Secure ACS se envía con una licencia de software instalada previamente del Cisco Secure ACS. Visite Cisco que pide el Home Page (clientes registrados solamente) para poner una orden.

Nota: Usted necesita una cuenta CCO con un contrato de servicio asociado para conseguir la versión de prueba del 90-día para el Cisco Secure ACS for Windows.

La configuración del router en este documento fue desarrollada en un router que funciona con el Software Release 11.3.3 de Cisco IOS®. El Cisco IOS Software Release 12.0.5.T y Posterior utiliza el **TACACS+ de grupo** en vez de **tacacs+**, así que las declaraciones tales como **permiso del TACACS+ predeterminado de la conexión con el sistema de autenticación aaa** aparecen mientras que **permiso del grupo predeterminado tacacs+ de la conexión con el sistema de autenticación**

aaa.

Refiera a la documentación del Cisco IOS Software para información más completa sobre los comandos router.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco IOS Software Release 11.3.3 y el Cisco IOS Software Release 12.0.5.T y Posterior.

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.

Autenticación

Complete estos pasos:

1. Aseegurese le haber compilado el código TACACS+ (TAC+) en el servidor Unix.Las Configuraciones del servidor aquí asumen que usted utiliza el código de servidor de Cisco TAC+. Las configuraciones del router deben trabajar independientemente de si el código de servidor es código de servidor de Cisco. El TAC+ se debe ejecutar como raíz; su a arraigar en caso necesario.
2. Copie el test_file en el extremo de este documento, coloqúelo en el servidor TAC+, y nómbrelo **test_file**.Marque para estar seguro el comienzo **tac_plus_executable de la** daemon con **test_file**. En este comando, **-** Las comprobaciones para de la opción **P** compilan los errores pero no comienzan la daemon:
   ```
   tac_plus_executable -P -C test_file
   ```
   Usted puede ser que vea el contenido de test_file navegar hacia abajo la ventana, pero usted no debe ver que los mensajes tales como `no pueden encontrar el archivo`, `texto claro esperado--texto claro`, o `inesperado encontrado}`. Si hay errores, marque las trayectorias a test_file, vuelva a inspeccionar su teclear, y la contra-prueba antes de que usted continúe.
3. Comience a configurar el TAC+ en el router.Ingrese el **enable mode** y el tipo **configura terminal** antes del comando set. Esta sintaxis de los comandos se asegura de que usted no sea router bloqueado de los inicialmente, proporcionando al **tac_plus_executable** no se esté ejecutando:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.         !        aaa authentication login linmethod tacacs+ enable   aaa
authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+
enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```

4. Prueba a estar segura que usted puede todavía acceder al router con Telnet y a través del puerto de la consola antes de que usted continúe. Porque el **tac_plus_executable** no se está ejecutando, la **contraseña habilitada** debe ser validada.**Nota:** Mantenga a la sesión de puerto de la consola activa y permanezca en el enable mode. Esta sesión no debe medir el tiempo hacia fuera. El acceso al router se limita en este momento, y usted necesita poder realizar los cambios de configuración sin bloquearse hacia fuera.Publique estos comandos de ver la interacción entre el servidor y el router en el router:
   ```
   terminal monitor  debug aaa authentication
   ```
5. Como raíz, comience el TAC+ en el servidor:
   ```
   tac_plus_executable -C test_file -d 16
   ```
6. Marque para ser el TAC+ seguro comenzado:
   ```
   ps -aux | grep tac_plus_executable
   ```
   o
   ```
   ps -ef | grep tac_plus_executable
   ```
   Si el TAC+ no comienza, es generalmente un problema con el sintaxis en el test_file. Vuelva al paso 1 para corregir esto.
7. Teclee el **tail -f /var/tmp/tac_plus.log** para ver la interacción del router-a-servidor en el servidor.**Nota:** - La opción `d 16` en el paso 5 envía la salida de todas las transacciones a /var/tmp/tac_plus.log.
8. Los usuarios de Telnet (VTY) deben ahora tener que autenticar con el TAC+.Con el debug yendo en el router y el servidor (pasos 4 y 7), Telnet en el router de otra parte de la red.El router produce un prompt del nombre de usuario y contraseña, al cual usted contesta:
   ```
   'authenuser'   (username from test_file)'admin'   (password from test_file)
   ```
   El `authenuser del` usuario está en el grupo `admin`, que tiene la contraseña admin.¿Mire el servidor y al router donde usted puede ver la interacción TAC+? se envía qué donde, las respuestas, las peticiones, y así sucesivamente. Corrija cualquier problema antes de que usted continúe.
9. Si usted también quisiera que sus usuarios autenticaran con el TAC+ para conseguir en el enable mode, aseegurese a su sesión de puerto de la consola sigue siendo active y agrega este comando al router:
   ```
   !--- For enable mode, list 'default' looks to TAC+ !--- then enable password if TAC+ does
   not run. aaa authentication enable default tacacs+ enable
   ```
   Los usuarios ahora tienen que habilitar con el TAC+.
10. Con el debug yendo en el router y el servidor (pasos 4 y 7), Telnet en el router de otra parte de la red. El router produce un prompt del nombre de usuario y contraseña, al cual usted contesta:
    ```
    'authenuser'   (username from test_file)'admin'   (password from test_file)
    ```
    Cuando usted ingresa el enable mode, los pedidos de router una contraseña, a la cual usted contesta:

```
'cisco'  ($enable$ password from test_file)
```
¿Mire el servidor y al router donde usted debe ver la interacción TAC+? se envía qué donde, las respuestas, las peticiones, y así sucesivamente. Corrija cualquier problema antes de que usted continúe.

11. Derribe el proceso TAC+ en el servidor mientras que todavía está conectado con el puerto de la consola para estar seguro que sus usuarios pueden todavía acceder al router si el TAC+ está abajo:
```
ps -aux | grep tac_plus_executable
```
o
```
ps -ef | grep tac_plus_executable)  kill -9 pid_of_tac_plus_executable
```
Relance Telnet y el permiso del paso anterior. El router después realiza que no está respondiendo el proceso TAC+ y permite que los usuarios inicien sesión y que habiliten con las contraseñas predeterminadas.
12. Marque para saber si hay autenticación de sus usuarios del puerto de la consola con el TAC+. Para hacer esto, traiga para arriba el servidor TAC+ otra vez (los pasos 5 y 6), y establecen a una sesión telnet al router (que debe autenticar con el TAC+).Remain conectó con Telnet en el router en el enable mode hasta que usted esté seguro que usted puede iniciar sesión al router a través del puerto de la consola.El logout de su conexión original al router a través del puerto de la consola, entonces vuelve a conectar al puerto de la consola. Autenticación de puerto de consola a iniciar sesión y a habilitar usando las identificaciones del usuario y las contraseñas (mostradas en el paso 10) debe ahora estar con el TAC+.
13. Mientras que usted sigue conectado a través de una sesión telnet o del puerto de la consola y con el debug que va en el router y el servidor (los pasos 4 y 7), establecen una conexión del módem para alinear 1.La línea usuarios ahora tiene que iniciar sesión y habilitar con el TAC+.El router produce un prompt del nombre de usuario y contraseña, al cual usted contesta:
```
'authenuser'   (username from test_file)'admin'   (password from test_file)
```
Cuando usted ingresa el enable mode, los pedidos de router una contraseña.Contestación:
```
'cisco'   ($enable$ password from test_file)
```
¿Mire el servidor y al router donde usted ve la interacción TAC+? se envía qué donde, las respuestas, las peticiones, y así sucesivamente. Corrija cualquier problema antes de que usted continúe.Los usuarios ahora tienen que habilitar con el TAC+.

Agregue la autorización

Agregar la autorización es opcional.

Por abandono, hay tres niveles del comando en el router:

- nivel de privilegio 0 que incluye la neutralización, el permiso, la salida, la ayuda, y el logout
- el prompt del nivel de privilegio 1 - nivel normal en Telnet - dice el `router>`
- el prompt del nivel de privilegio 15 - permiso llano - dice el `router-`

Puesto que los comandos disponibles dependen del conjunto de características IOS, versión del Cisco IOS, modelo del router, y así sucesivamente, no hay una lista amplia de comandos all en los niveles 1 y 15. Por ejemplo, la **ruta de IPX de la demostración** no está presente en un conjunto de características IP solamente, el **transporte nacional del IP de la demostración** no está en el Cisco IOS Software Release 10.2.x porque el NAT no fue introducido en ese entonces, y el **entorno de la demostración** no está presente en los modelos de router sin la fuente de alimentación y el control de temperatura. ¿Los comandos disponibles en un router determinado

en un nivel determinado pueden ser encontrados cuando usted ingresa a**?** en el prompt en el router cuando en ese nivel de privilegio.

La autorización de puerto de la consola no fue agregada como característica hasta que el Id. de bug Cisco CSCdi82030 (clientes registrados solamente) fuera implementado. La autorización de puerto de la consola es apagado por abandono aminorar la probabilidad que usted hace router accidentalmente bloqueado de los. Si un usuario tiene acceso físico al router a través de la consola, la autorización de puerto de la consola no es extremadamente eficaz. Sin embargo, la autorización de puerto de la consola se puede girar bajo línea `con 0` en una imagen que el Id. de bug Cisco CSCdi82030 (clientes registrados solamente) fue implementado adentro con el comando:

```
authorization exec default|WORD
```

1. El router puede ser configurado para autorizar los comandos con el TAC+ en absoluto o algunos niveles.Esta configuración del router permite que todos los usuarios tengan autorización del por-comando configurada en el servidor. Aquí autorizamos los comandos all con el TAC+, pero si el servidor está abajo, no hay autorización necesaria.
   ```
   aaa authorization commands 1 default tacacs+ none  aaa authorization commands 15 default tacacs+ none
   ```
2. Mientras que el servidor TAC+ se ejecuta, Telnet en el router con userid authenuser (Autenticar usuario con el ID de usuario).Porque el authenuser tiene el servicio predeterminado = permiso en test_file, este usuario debe poder realizar todas las funciones.Mientras que en el router, ingrese el **enable mode**, y gire el debugging de la autorización:
   ```
   terminal monitor  debug aaa authorization
   ```
3. Telnet en el router con la userid authoruser y el operador de contraseña.Este usuario no puede hacer el **traceroute de** dos comandos show y **terminar sesión** (véase el test_file).Mire el servidor y al router donde usted debe ver la interacción TAC+ (se envía qué donde, las respuestas, las peticiones, y así sucesivamente). Corrija cualquier problema antes de que usted continúe.
4. Si usted quiere configurar a un usuario para un autocommand, elimine el transitorio del usuario comentado-hacia fuera en el test_file, y ponga un destino del IP Address válido en lugar del #.#.#.#.Pare y encienda el servidor TAC+.En el router:
   ```
   aaa authorization exec default tacacs+
   ```
   Telnet al router con la userid transitorio y la contraseña transitoria. **El telnet #.#.#.#** ejecuta y el transitorio del usuario se envía a la otra ubicación.

Agregar contabilidad

La Incorporación de contabilidad es opcional.

¿La referencia al archivo de contabilidad está en test_file? archivo de contabilidad = /var/log/tac.log. Pero las estadísticas no ocurren a menos que estén configuradas en el router (proporcionado el router funciona con una versión del Cisco IOS Software más adelante de 11.0).

1. Estadísticas del permiso en el router:
   ```
   aaa accounting exec default start-stop tacacs+  aaa accounting connection default start-stop tacacs+  aaa accounting network default start-stop tacacs+  aaa accounting system default start-stop tacacs+
   ```
   Nota: Las estadísticas AAA no hacen las estadísticas del por-comando en algunas

versiones. Una solución alternativa es utilizar la autorización del por-comando y registrar el acontecimiento en el archivo de contabilidad. (Refiera al Id. de bug Cisco CSCdi44140.) Si usted utiliza una imagen en la cual esto reparada se utiliza [los Cisco IOS Software Release 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA en septiembre 24, 1997] usted puede también habilitar las comando-estadísticas.

2. Mientras que el TAC+ se ejecuta en el servidor, ingrese este comando en el servidor de ver las entradas que entran el archivo de contabilidad:
   ```
   tail -f /var/log/tac.log
   ```
   Entonces registre en y router de los, router de los de Telnet, y así sucesivamente. En caso necesario, en el router ingrese:
   ```
   terminal monitor  debug aaa accounting
   ```

Archivos de prueba

```
- - - - - - - (cut here) - - - - - - - -# Set up accounting file if enabling accounting on
NASaccounting file = /var/log/tac.log# Enable password setup for everyone:user = $enable$ {
login = cleartext "cisco"        }# Group listings must be first:group = admin {# Users in group
'admin' have cleartext password        login = cleartext "admin"        expires = "Dec 31
1999"}group = operators {# Users in group 'operators' have cleartext password        login =
cleartext "operator"        expires = "Dec 31 1999"}group = transients {# Users in group
'transient' have cleartext password        login = cleartext "transient"        expires = "Dec
31 1999"}# This user is a member of group 'admin' & uses that group's password to log in.#  The
$enable$ password is used to enter enable mode.  The user can perform all commands. user =
authenuser {        default service = permit        member = admin        }# This user is
limitted in allowed commands when aaa authorization is enabled: user = telnet {        login =
cleartext "telnet"        cmd = telnet {        permit .*        }        cmd = logout {
permit .*        }        }# user = transient {#       member = transients#       service = exec
{        # When transient logs on to the NAS, he's immediately        # zipped to another site#
autocmd = "telnet #.#.#.#"#       }#       }# This user is a member of group 'operators' # &
uses that group's password to log in  user = authenuser {        member = operators# Since this
user does not have 'default service = permit' when command # authorization through TACACS+ is on
at the router, this user's commands# are limited to:        cmd = show {         permit ver
permit ip        }        cmd = traceroute {        permit .*        }        cmd = logout {
permit .*        }}- - - - (end cut here) - - - -
```

Nota: Se genera este mensaje de error si su servidor TACACS no es accesible: `%AAAA-3-DROPACCTSNDFAIL: el registro de contabilidad caído, envía al servidor fallado: sistema-principio.` Verifique que el servidor TACACS+ sea operativo.

Información Relacionada

- Seguridad de acceso a la red de usuario único TACACS+
- Terminal Access Controller Access Control System (TACACS+)
- Cisco Secure Access Control Server para Windows
- Soporte Técnico y Documentación - Cisco Systems