Router del Cisco IOS: Local, TACACS+ y autenticación de RADIUS del ejemplo de configuración de la conexión HTTP

Contenido

Introducción

Este documento muestra cómo configurar el local, el TACACS+, y la autenticación de RADIUS de la conexión HTTP. Proporcionan algunos comandos de debugging relevantes también.

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

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

indicadas a continuación.

- El Cisco IOS ® Software libera 11.2 o más adelante
- Hardware compatible con estas revisiones del software

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Teoría Precedente

En el Software Release 11.2 de Cisco IOS®, una característica para manejar al router con el HTTP fue agregada. La sección "Comandos del buscador Web del Cisco IOS" de la referencia de comandos de los fundamentales de la configuración del Cisco IOS incluye la siguiente información sobre esta característica.

“El **comando ip http authentication** le permite para especificar un método de autenticación determinado para los usuarios de servidor HTTP. El servidor HTTP utiliza el método de la contraseña habilitada para autenticar a un usuario en el nivel de privilegio 15. **El comando ip http authentication** ahora deja le especificar el permiso, el local, el TACACS, o la autenticación de usuario de servidor HTTP del Authentication, Authorization, and Accounting (AAA).”

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Este documento usa las configuraciones detalladas a continuación.

- Configuración de autenticación local para usuarios de servidores HTTP
- Configuración de autenticación TACACS+ para usuarios de servidores HTTP
- Configuración de autenticación de RADIUS para usuarios de servidores HTTP

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Configuración de autenticación local para usuarios de servidores HTTP

- Configuración del router
- Resultados del usuario

Configuración del router

Autenticación local con el Cisco IOS Software Release 11.2
`!--- This is the part of the configuration related to local authentication. ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three`

```
password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

Autenticación local con los Cisco IOS Software Release 11.3.3.T o Posterior

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Resultados del usuario

Estos resultados se aplican a los usuarios en las configuraciones del router anteriores.

- **Usuario uno**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de autenticarse, el usuario estará en modo habilitado (el comando show privilege será 15).Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.
- **Usuario tres**El usuario fallará el autorización de la Web debido al no tener un nivel de privilegio.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de registrarse, el usuario estará en modo sin permisos (el comando show privilege será 1).Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.
- **Usuario cuatro**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#/level/7/exec.Aparecerán los comandos de nivel 1 y el comando clear line de nivel 7.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.El usuario estará en el nivel de privilegio 7 después de login (el **privilegio de la demostración** será 7)Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.

Configuración de autenticación TACACS+ para usuarios de servidores HTTP

Configuración del router

Autenticación con el Cisco IOS Software Release 11.2

```
aaa new-model
aaa authentication login default tacacs+
```

```
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticación con los Cisco IOS Software Release 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticación con los Cisco IOS Software Release 12.0.5.T y Posterior

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Resultados del usuario

Los resultados siguientes se aplican a los usuarios en las Configuraciones del servidor abajo.

- **Usuario uno**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de autenticarse, el usuario estará en modo habilitado (el comando show privilege será 15).Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.
- **Usuario dos**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de autenticarse, el usuario estará en modo habilitado (el comando show privilege será 15).Si agregan al comando authorization al router, el usuario fallará los comandos all pues la Configuración del servidor no los autoriza.
- **Usuario tres**El usuario fallará el autorización de la Web debido al no tener un nivel de privilegio.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de registrarse, el usuario estará en modo sin permisos (el comando show privilege será 1).Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.
- **Usuario cuatro**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#/level/7/exec.Aparecerán los comandos de nivel 1 y el comando clear line de nivel 7.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.El usuario estará en el nivel de privilegio 7 después de login

(el **privilegio de la demostración** será 7)Si agregan al comando authorization al router, el usuario todavía tendrá éxito en los comandos all.

Configuración del servidor Freeware Daemon

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS para la configuración de servidor Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
```

```
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

Configuración del servidor del Cisco Secure ACS for Windows

Usuario uno en grupo uno

- Configuraciones de grupoMarque la casilla shell (exec).Verifique privilege level=15.Seleccione Default Undefined Services (Servicios predeterminados (no definidos))**Nota:** Si esta opción no aparece, vaya a Interface Configuration (Configuración de interfaz) y seleccione TACACS+ y luego Advanced Configuration Options (Opciones de configuración avanzadas). Elija la configuración del servicio Display enable default (undefined) (Mostrar habilitar de forma predeterminada [no definido]).
- Ajustes de usuarioContraseña de cualquier base de datos; ingrese la contraseña y confírmela en la área superior.

Usuario dos en el grupo dos

- Configuraciones de grupoMarque la casilla shell (exec).Verifique privilege level=15.No marque los **servicios (indefinidos) del valor por defecto**.
- Ajustes de usuarioContraseña de cualquier base de datos; ingrese la contraseña y confírmela en la área superior.

Usuario tres en el grupo tres

- Configuraciones de grupoMarque la casilla shell (exec).Deje el nivel de privilegio en blanco.Seleccione Default Undefined Services (Servicios predeterminados (no definidos))**Nota:** Si esta opción no aparece, vaya a Interface Configuration (Configuración de interfaz) y seleccione TACACS+ y luego Advanced Configuration Options (Opciones de configuración avanzadas). Elija la configuración del servicio Display enable default (undefined) (Mostrar habilitar de forma predeterminada [no definido]).
- Ajustes de usuarioContraseña de cualquier base de datos; ingrese la contraseña y confírmela en la área superior.

Usuario cuatro en el grupo cuatro

- Configuraciones de grupoMarque la casilla shell (exec).Compruebe que el nivel de privilegios=7.Seleccione Default Undefined Services (Servicios predeterminados (no definidos))**Nota:** Si esta opción no aparece, vaya a Interface Configuration (Configuración de interfaz) y seleccione TACACS+ y luego Advanced Configuration Options (Opciones de configuración avanzadas). Elija la configuración del servicio Display enable default (undefined) (Mostrar habilitar de forma predeterminada [no definido]).
- Ajustes de usuarioContraseña de cualquier base de datos; ingrese la contraseña y confírmela en la área superior.

Configuración de autenticación de RADIUS para usuarios de servidores HTTP

Configuración del router

Autenticación con el Cisco IOS Software Release 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Autenticación con los Cisco IOS Software Release 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Autenticación con los Cisco IOS Software Release 12.0.5.T y Posterior

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Resultados del usuario

Los resultados siguientes se aplican a los usuarios en las Configuraciones del servidor abajo.

- **Usuario uno**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.Luego de autenticarse, el usuario estará en modo habilitado (el comando show privilege será 15).
- **Usuario tres**El usuario fallará el autorización de la Web debido al no tener un nivel de privilegio.Después de Telnet al router, el usuario puede realizar los comandos all después de

la autenticación de inicio de sesión.Luego de registrarse, el usuario estará en modo sin permisos (el comando show privilege será 1).

- **Usuario cuatro**El usuario pasará el autorización de la Web si el URL se ingresa como http://#.#.#.#/level/7/exec.Aparecerán los comandos de nivel 1 y el comando clear line de nivel 7.Después de Telnet al router, el usuario puede realizar los comandos all después de la autenticación de inicio de sesión.El usuario estará en el nivel de privilegio 7 después de login (el **privilegio de la demostración** será 7)

Configuración de RADIUS en el servidor que soporta los cisco av-pair

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS para la configuración de servidor Unix

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
```

```
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Configuración del servidor del Cisco Secure ACS for Windows

- User = uno, tipo de servicio (atributo 6) = administrativo
- Usuario = tres, tipo de servicio (atributo 6) = inicio de sesión
- User = four, service type (attribute 6) = login, verifique la casilla Cisco AV-pairs (pares AV Cisco) e ingrese shell:priv-lvl=7

Verificación

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

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Los siguientes comandos son útiles para la autenticación de HTTP de debugging. Les publican en el router.

Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

- **monitor terminal** - Visualizaciones **resultado del comando de debug** y mensajes de error del sistema para el terminal actual y la sesión.
- **autenticación aaa del debug** - Visualiza la información sobre la autenticación AAA/TACACS+.
- **debug aaa authorization** - Visualiza la información sobre la autorización AAA/TACACS+.
- **radio del debug** - Visualiza la información de debugging detallada asociada al RADIUS.
- **tacacs del debug** - Visualiza la información asociada al TACACS.
- **debug ip http authentication** - Utilice este comando de resolver problemas los problemas de la autenticación HTTP. Visualiza el método de autentificación los mensajes de estado frustrados y autenticación-específicos del router.

Información Relacionada

- Página de soporte del Software Cisco TACACS+ Access
- Página de soporte de RADIUS
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de Cisco Secure ACS para Windows

- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems