Cómo asignar niveles de privilegio con TACACS+ y RADIUS

Contenido

Introducción

Este documento explica cómo cambiar el nivel de privilegio de ciertos comandos y brinda un ejemplo con partes de ejemplos de configuraciones para un router y servidores TACACS+ y RADIUS.

prerrequisitos

Requisitos

Los Quien lea este documento deben tener conocimiento de los niveles de privilegio en un router.

Por abandono, hay tres niveles de privilegio en el router.

- nivel de privilegio 1 = sin privilegios (el prompt es `router>`), el nivel predeterminado para abrir una sesión
- nivel de privilegio 15 = privilegiado (la solicitud es router#), el nivel luego de pasar al modo de activación
- el nivel de privilegio 0 = utilizado raramente, pero incluye 5 comandos: **neutralización**, **permiso**, **salida**, **ayuda**, y **logout**

Los niveles 2 a 14 no se usan en una configuración predeterminada, pero los comandos normalmente ubicados en el nivel 15 pueden desplazarse hacia abajo a uno de esos niveles, y comandos que normalmente están en el nivel 1 puede desplazarse hacia arriba a uno de esos niveles. Obviamente, este modelo de seguridad implica un cierto grado de administración desde el router.

Para determinar el nivel de privilegio como usuario conectado al sistema, teclee el **comando show**

privilege. ¿Para determinar qué comandos están disponibles en un nivel de privilegio determinado para la versión del software de Cisco IOS® que usted está utilizando, teclee a**?** en la línea de comandos cuando se encuentra registrado con ese nivel de privilegio.

Nota: En vez de asignar los niveles de privilegio, usted puede hacer el comando authorization si el servidor de autenticación soporta el TACACS+. El protocolo RADIUS no admite la autorización de comandos.

Componentes Utilizados

La información en este documento se basa en los Cisco IOS Software Release 11.2 y Posterior.

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.

Convenciones

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

Ejemplo:

En este ejemplo, bajan a los **comandos snmp-server** desde el nivel de privilegio 15 (el valor por defecto) al nivel de privilegio 7. **El comando ping** es levantado el nivel de privilegio 1 al nivel de privilegio 7. Cuando autentican al usuario siete, el servidor asigna ese usuario el nivel de privilegio 7 y el nivel de privilegio actual de las visualizaciones de un **comando show privilege** “es el 7." que el usuario puede hacer ping y hacer la configuración del SNMP-servidor en el modo de configuración. Otros comandos configuration no están disponibles.

Configuraciones - Router

Router - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router - 11.3.3.T y posterior (hasta 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router: 12.0.5.T y posteriores

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Configuraciones - Servidor

Cisco Secure NT TACACS+

Siga estos pasos para configurar el servidor.

1. Complete el nombre de usuario y la contraseña.
2. En configuraciones de grupo, asegúrese de verificar shell/exec y de ingresar 7 en la casilla de nivel de privilegio.

TACACS+ - Estrofa en el servidor Freeware

```
Stanza in TACACS+ freeware:
user = seven {
login = cleartext seven
service = exec {
priv-lvl = 7
}
}
```

Cisco UNIX seguro TACACS+

```
user = seven {
password = clear "seven"
```

```
service = shell {
set priv-lvl = 7
}
}
```

Cisco Secure NT RADIUS

Siga estos pasos para configurar el servidor.

1. Ingrese el nombre de usuario y la contraseña.
2. En las configuraciones de grupo para IETF, Tipo de servicio (atributo 6) = Mensaje de Nas
3. En el área RADIUS de Cisco, verifique el par AV y en la caja rectangular inferior, ingrese shell:priv-lvl=7.

Cisco Secure UNIX RADIUS

```
user = seven{
radius=Cisco {
check_items= {
2="seven"
}
reply_attributes= {
6=7
9,1="shell:priv-lvl=7"
}
}
}
```

Éste es el archivo de usuario para el "seven." del nombre de usuario

Nota: El servidor debe soportar los pares AV de Cisco.

- seven Password = passwdxyz
- Tipo de servicio = Usuario de Shell
- Cisco-avpair =shell:priv-lvl=7

Información Relacionada

- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- TACACS+ en documentación de IOS
- Página de soporte TACACS/TACACS+
- Página de soporte de Secure para UNIX de Cisco
- Página de soporte de Cisco Secure ACS para Windows
- Soporte Técnico - Cisco Systems