

Ejemplo de Configuración de FreeRADIUS Utilizado para el Acceso Administrativo en Cisco IOS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de un switch para autenticación y autorización](#)

[Configuración de FreeRADIUS](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la autenticación RADIUS en switches Cisco IOS[®] con un servidor RADIUS de terceros (FreeRADIUS). En este ejemplo se trata la ubicación de un usuario directamente en el modo de privilegio 15 tras la autenticación.

Prerequisites

Requirements

Asegúrese de que su switch de Cisco está definido como un cliente en FreeRADIUS con la dirección IP y la misma clave secreta compartida definidas en FreeRADIUS y el switch.

Componentes Utilizados

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

- FreeRADIUS
- Cisco IOS versión 12.2

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Configuración de un switch para autenticación y autorización

1. Para crear un usuario local en el switch con privilegios completos para el acceso de reserva, ingrese:

```
Switch(config)#username admin privilege 15 password 0 cisco123!
```

2. Para habilitar AAA, ingrese:

```
switch(config)# aaa new-model
```

3. Para proporcionar la dirección IP del servidor RADIUS así como la clave, ingrese:

```
switch# configure terminal
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
switch(config)#radius-server key hello123
```

Nota: La clave debe coincidir con el secreto compartido configurado en el servidor RADIUS para el switch.

4. Para probar la disponibilidad del servidor RADIUS, ingrese el comando **test aaa**:

```
switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
```

La autenticación de prueba falla con un Rechazo del servidor porque aún no está configurado, pero confirmará que el servidor en sí es accesible.

5. Para configurar las autenticaciones de inicio de sesión para que recurran a los usuarios locales si RADIUS es inalcanzable, ingrese:

```
switch(config)#aaa authentication login default group radius local
```

6. Para configurar la autorización para un nivel de privilegio de 15, siempre que se autentique a un usuario, ingrese:

```
switch(config)#aaa authorization exec default group radius if-authenticated
```

Configuración de FreeRADIUS

Defina el cliente en el servidor FreeRADIUS

1. Para navegar al directorio de configuración, ingrese:

```
# cd /etc/freeradius
```

2. Para editar el archivo **clients.conf**, ingrese:

```
# sudo nano clients.conf
```

3. Para agregar cada dispositivo (router/switch) identificado por el nombre de host e incluir el secreto compartido correcto, ingrese:

```
client 192.168.1.1 {
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. Para editar el archivo de usuarios, ingrese:

```
# sudo nano users
```

5. Agregue cada usuario con permiso para acceder al dispositivo. En este ejemplo se muestra cómo establecer un nivel de privilegio de Cisco IOS de 15 para el usuario "cisco".

```
cisco Cleartext-Password := "password"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=15"
```

6. Para reiniciar FreeRADIUS, ingrese:

```
# sudo /etc/init.d/freeradius restart
```

7. Para cambiar el grupo de usuarios PREDETERMINADO en el archivo del usuario para dar a todos los usuarios que son miembros de cisco-rw un nivel de privilegio de 15, ingrese:

```
DEFAULT Group == cisco-rw, Auth-Type = System
Service-Type = NAS-Prompt-User,
cisco-avpair := "shell:priv-lvl=15"
```

8. Puede agregar otros usuarios en diferentes niveles de privilegio según sea necesario en el archivo de usuarios de FreeRADIUS. Por ejemplo, a este usuario (life) se le da un nivel de 3 (mantenimiento del sistema):

```
sudo nano/etc/freeradius/users

life Cleartext-Password := "testing"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=3"

Restart the FreeRADIUS service:
sudo /etc/init.d/freeradius restart
```

Nota: La configuración en este documento se basa en FreeRADIUS ejecutado en Ubuntu 12.04 LTE y 13.04.

Verificación

Para verificar la configuración en el switch, utilice estos comandos:

```
switch# show run | in radius      (Show the radius configuration)
switch# show run | in aaa        (Show the running AAA configuration)
switch# show startup-config Radius (Show the startup AAA configuration in
start-up configuration)
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [FreeRADIUS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).