Configuración de RADIUS con el servidor Livingston

Contenido

Introducción

Este documento está diseñado para ayudar al usuario RADIUS por primera vez a configurar y depurar una configuración RADIUS en un servidor RADIUS Livingston. No es una descripción exhaustiva de las capacidades de Cisco IOS® RADIUS. La documentación de Livingston está disponible en el sitio web de Lucent Technologies.

La configuración del router es la misma independientemente del servidor que se utilice. Cisco ofrece código RADIUS disponible comercialmente en Couscouses NA, Couscouses UNIX o Cisco Access Registrar.

Esta configuración del router se desarrolló en un router que ejecuta Cisco IOS Software Release 11.3.3; La versión 12.0.5.T y posterior utiliza **group radius** en lugar de **radius**, por lo que las sentencias como **aaa authentication login default radius enable** aparecen como **aaa authentication default group radius enable**.

Consulte la información RADIUS en la documentación de Cisco IOS para obtener detalles sobre los comandos del router RADIUS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación

Complete estos pasos:

1. Asegúrese de que ha compilado el código RADIUS en el servidor UNIX. Las configuraciones del servidor suponen que utiliza el código del servidor Livingston RADIUS. Las configuraciones del router deben funcionar con otro código de servidor, pero las configuraciones del servidor difieren. El código, radiusd, debe ejecutarse como root.
2. El código Livingston RADIUS incluye tres archivos de ejemplo que se personalizarán para el sistema: clients.ejemplo, users.example y diccionario. Estos se encuentran generalmente en el directorio raddb. Puede modificar estos archivos o los archivos de usuarios y clientes al final de este documento. Los tres archivos deben colocarse en un directorio de trabajo. Asegúrese de que el servidor RADIUS comience con los tres archivos:
   ```
   radiusd -x -d (directory_containing_3_files)
   ```
   Los errores en el inicio deben imprimirse en la pantalla o en el archivo de registro_de_directorio_conteniendo_3_archivos_de_registro. Verifique para asegurarse de que se inició RADIUS, desde otra ventana de servidor:
   ```
   ps -aux | grep radiusd
   (or ps -ef | grep radiusd)
   ```
   Verá dos procesos radiusd.
3. Matar el proceso de radio:
   ```
   kill -9 highest_radiusd_pid
   ```
4. En el puerto de la consola del router, comience a configurar RADIUS. Ingrese enable mode y escriba **configure terminal** antes del comando set. Esta sintaxis garantiza que no esté bloqueado inicialmente del router, dado que RADIUS no se ejecuta en el servidor:

   ```
   !--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of
   authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" 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 radiusd !--- not being
   started, the enable password will be !--- accepted because it is in each list. aaa
   authentication login default radius enable aaa authentication login linmethod radius enable
   aaa authentication login vtymethod radius enable aaa authentication login conmethod radius
   enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address.
   radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server:
   radius-server key cisco 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
   password whatever 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
   ```
5. Permanezca conectado al router a través del puerto de la consola mientras se protege para asegurarse de que aún pueda acceder al router a través de Telnet antes de continuar. Debido a que radiusd no se está ejecutando, la contraseña de activación debe aceptarse con cualquier ID de usuario.**Precaución:** Mantenga activa la sesión del puerto de la consola y

manténgase en modo de activación. Asegúrese de que esta sesión no se agote. No se bloquee mientras realiza cambios en la configuración.Ejecute estos comandos para ver la interacción del servidor al router en el router:

```
terminal monitor
debug aaa authentication
```

6. Como root, inicie RADIUS en el servidor:

   ```
   radiusd -x -d (directory_containing_3_files)
   ```

   Los errores en el inicio se imprimen en la pantalla o en el archivo_de_registro_de_archivos_de_directorio_3_. Asegúrese de que RADIUS se inició desde otra ventana de servidor:

   ```
   Ps -aux | grep radiusd
   (or Ps -ef | grep radiusd)
   ```

   Debe ver dos procesos radiusd.
7. Los usuarios de Telnet (vty) ahora deben autenticarse a través de RADIUS. Con debug en el router y el servidor, pasos 5 y 6, conecte Telnet al router desde otra parte de la red. El router produce un mensaje de nombre de usuario y contraseña al que responde:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Vea el servidor y el router donde necesita ver la interacción RADIUS, por ejemplo, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.
8. Si también desea que los usuarios se autentiquen a través de RADIUS para entrar en el modo habilitar, asegúrese de que la sesión del puerto de la consola sigue activa y agregue este comando al router.

   ```
   !--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS
   not running. aaa authentication enable default radius enable
   ```

9. Los usuarios ahora deben **habilitar** a través de RADIUS. Con la depuración en el router y el servidor, pasos 5 y 6, conecte Telnet al router desde otra parte de la red. El router necesita producir un mensaje de nombre de usuario y contraseña al que usted responde:

   ```
   ciscousr (username from users file)
   ciscopas (password from users file)
   ```

   Cuando ingresa al modo enable, el router envía el nombre de usuario $enable15$ y solicita una contraseña, a la que responde:

   ```
   shared
   ```

   Vea el servidor y el router donde necesita ver la interacción RADIUS, por ejemplo, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.
10. Verifique la autenticación de los usuarios del puerto de la consola a través de RADIUS mediante el establecimiento de una sesión Telnet al router, que necesita autenticarse a través de RADIUS. Permanezca Telnet en el router y en el modo de activación hasta que esté seguro de que puede iniciar sesión en el router a través del puerto de la consola, cerrar la sesión de la conexión original al router a través del puerto de la consola y, a continuación, volver a conectarse al puerto de la consola. La autenticación del puerto de consola para iniciar sesión y habilitar mediante el uso de los identificadores de usuario y las contraseñas en el paso 9 debe realizarse ahora a través de RADIUS.
11. Mientras permanece conectado a través de una sesión Telnet o del puerto de la consola y con la depuración en el router y el servidor, los pasos 5 y 6, establecen una conexión de módem a la línea 1. Los usuarios de línea deben iniciar sesión y activarse a través de RADIUS. El router necesita producir un mensaje de nombre de usuario y contraseña al que usted responde:

    ```
    ciscousr (username from users file)
    ciscopas (password from users file)
    ```

Cuando ingresa al modo enable, el router envía el nombre de usuario $enable15$ y solicita una contraseña, a la que responde:

```
shared
```

Vea el servidor y el router donde necesita ver la interacción RADIUS, por ejemplo, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.

Incorporación de contabilidad

Agregar contabilidad es opcional.

1. La contabilidad no se realiza a menos que esté configurada en el router. Habilite la contabilización en el router como en este ejemplo:
   ```
   aaa accounting exec default start-stop radius
   aaa accounting connection default start-stop radius
   aaa accounting network default start-stop radius
   aaa accounting system default start-stop radius
   ```
2. Inicie RADIUS en el servidor con la opción de contabilización:
   ```
   Start RADIUS on the server with the accounting option:
   ```
3. Para ver la interacción de servidor a router en el router:
   ```
   terminal monitor
   debug aaa accounting
   ```
4. Acceda al router mientras observa la interacción del servidor y del router a través de la depuración y, a continuación, verifique el directorio de contabilidad para los archivos de registro.

Archivos de prueba

Este es el archivo de prueba de los usuarios:

```
ciscousr        Password = "ciscopas"
                User-Service-Type = Login-User,
                Login-Host = 1.2.3.4,
                Login-Service = Telnet

$enable15$      Password = "shared"
                User-Service-Type = Shell-User
```

Este es el archivo de prueba de clientes:

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4         cisco
```

Información Relacionada

- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems