Configuración de AAA básico en un servidor de acceso

Contenido

Introducción

En este documento se describe cómo configurar la autenticación, la autorización y la auditoría (AAA) en un router Cisco con los protocolos Radius o TACACS+.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Convenciones

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

Componentes Utilizados

La información que contiene este documento se basa en la versión 12 del software Cisco IOS®.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En este documento se explica cómo configurar la autenticación, la autorización y la auditoría (AAA) en un router Cisco con los protocolos Radius o TACACS+. El objetivo de este documento no es cubrir todas las características AAA sino explicar los principales comandos y brindar algunos ejemplos y pautas.

Nota: Lea la sección sobre la configuración de AAA general antes de continuar con la configuración de Cisco IOS. De lo contrario, se puede producir un error de configuración y un bloqueo posterior.

Para obtener más información, consulte la Guía de configuración de autenticación, autorización y auditoría.

Diagrama de la red

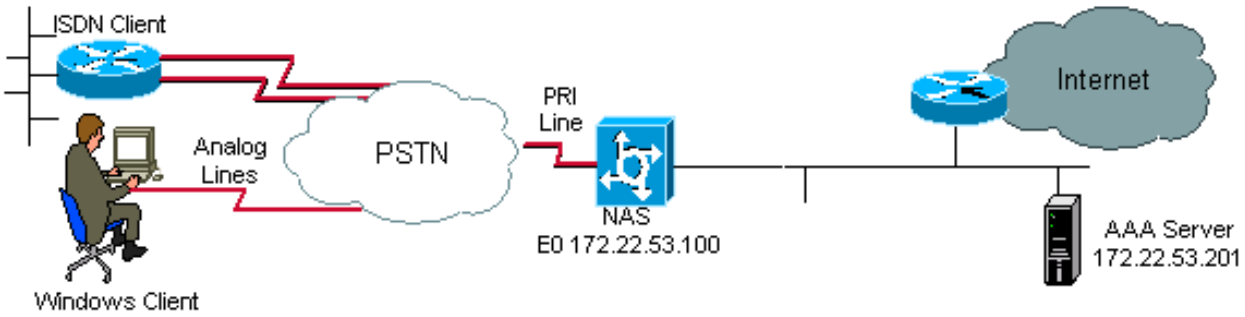

Diagrama de la red

Configuración de AAA general

Activar AAA

Para activar AAA, debe configurar el comando aaa new-model en configuración global.

Nota: Hasta que se active este comando, todos los otros comandos AAA están ocultos.

Advertencia: El comando aaa new-model aplica inmediatamente la autenticación local a todas las líneas e interfaces (excepto la línea de la consola línea con 0). Si se abre una sesión Telnet hacia el router después de habilitar este comando (o si una conexión caduca y debe volver a conectarse), entonces el usuario debe autenticarse con la base de datos local del router. Se recomienda definir un nombre de usuario y una contraseña en el servidor de acceso antes de iniciar la configuración AAA para que no quede bloqueado el acceso al router. Vea el siguiente ejemplo de código.

<#root>

```
Router(config)#
username xxx password yyy
```

Sugerencia: Antes de configurar los comandos AAA, save su configuración. Usted puede save la configuración de nuevo solo después de que haya completado su configuración AAA (y esté satisfecho de que funciona correctamente). Esto le permite recuperarse de bloqueos inesperados, ya que puede revertir cualquier cambio con una recarga del router.

Especificar el servidor AAA externo

En la configuración global, defina el protocolo de seguridad que usa con AAA (Radius, TACACS+). Si no desea utilizar alguno de estos dos protocolos, puede utilizar la base de datos

local en el router.

Si usa TACACS+, use el comando tacacs-server host<IP address of the AAA server> <key> .

Si usa Radius, use el comando radius-server host<IP address of the AAA server> <key> .

Configuración del servidor AAA

En el servidor AAA, configure los siguientes parámetros:

- El nombre del servidor de acceso.
- La dirección IP que el servidor de acceso utiliza para comunicarse con un servidor AAA.

> Nota: Si ambos dispositivos se encuentran en la misma red Ethernet, entonces, de forma predeterminada, el servidor de acceso utiliza la dirección IP definida en la interfaz Ethernet al momento de enviar el paquete AAA. Este aspecto es importante cuando el router posee interfaces múltiples (y, por lo tanto, múltiples direcciones).

- La misma clave <key> configurada en el servidor de acceso.

> Nota: La clave distingue entre mayúsculas y minúsculas.

- El protocolo utilizado por el servidor de acceso (TACACS+ o Radius).

Consulte la documentación del servidor AAA para conocer el procedimiento exacto utilizado para configurar los parámetros anteriores. Si el servidor de AAA no está correctamente configurado, entonces las solicitudes AAA del NAS serán ignoradas por el servidor de AAA y la conexión podría fallar.

El servidor de AAA debe ser alcanzable mediante IP desde el servidor de acceso (realice una prueba de ping para verificar la conectividad).

Configuración de autenticación

La autenticación verifica a los usuarios antes de que se les permita el acceso a la red y a los servicios de red (que se verifican con autorización).

Para configurar la autenticación AAA:

1. En primer lugar, defina una lista de métodos de autenticación que tenga nombre (en modo de configuración global).
2. Aplique esa lista a una o más interfaces (en el modo de configuración de interfaz).

La única excepción es la lista de método predeterminada (que se llama default). La lista de métodos predeterminados se aplica automáticamente a todas las interfaces excepto a las que

tienen una lista de método nombrada definida explícitamente. Una lista de métodos definida invalida la lista de métodos predeterminados.

Estos ejemplos de autenticación utilizan Radius, identificación de entrada y autenticación de Point-to-Point Protocol (PPP) para explicar conceptos tales como métodos y listas de nombres. En todos los ejemplos, TACACS+ puede sustituirse por Radius o por la autenticación local.

El software Cisco IOS utiliza el primer método enumerado para autenticar usuarios. Si ese método falla en responder (indicado por un ERROR), el software Cisco IOS detecta el siguiente método de autenticación que aparece en la lista de métodos. Este proceso continúa hasta que logra establecerse una comunicación con un método de autenticación de la lista o hasta que se agotan todos los métodos definidos en la lista de métodos.

Es importante tener en cuenta que el software Cisco IOS intenta la autenticación con el siguiente método de autenticación de la lista solamente cuando no hay respuesta del método anterior. Si falla la autenticación en cualquier instancia de este ciclo; es decir, el servidor AAA o la base de datos local de nombres de usuarios responde denegando el acceso al usuario (indicado por un FAIL [Falla]), el proceso de autenticación se detiene y no se realizan otros intentos para llevar a cabo métodos de autenticación.

Para permitir la autenticación de usuario, debe configurar el nombre de usuario y contraseña en el servidor AAA.

Autenticación de inicio de sesión

Puede usar el comando aaa authentication login para autenticar a los usuarios que deseen obtener acceso exec en el servidor de acceso (tty, vty, consola y aux).

Ejemplo 1: Acceso Exec con Radius y luego Local

<#root>

```
Router(config)#
```

aaa authentication login default group radius local

En el comando anterior:

- La lista que tiene nombre es la predeterminada (default).
- Existen dos métodos de autenticación (grupo radius y local).

La autenticación de todos los usuarios se hace con el servidor Radius (el primer método). Si el servidor Radius no responde, se usa la base de datos local del router (el segundo método). Para autenticación local, defina el nombre de usuario y la contraseña:

<#root>

```
Router(config)#
username xxx password yyy
```

Debido a que estamos utilizando la lista predeterminada en el comando aaa authentication login, se aplica automáticamente la autenticación de inicio de sesión en todas las conexiones de inicio de sesión (tales como tty, vty, console y aux).

Nota: El servidor (Radius o TACACS+) no responderá a una petición de autenticación aaa enviada por el servidor de acceso si no hay conectividad IP, si el servidor de acceso no está definido correctamente en el servidor AAA o si el servidor AAA no está correctamente definido en el servidor de acceso.

Nota: Si utiliza el ejemplo anterior, sin la palabra clave local, el resultado es:

```
<#root>
Router(config)#
aaa authentication login default group radius
```

Nota: Si el servidor AAA no responde a la petición de autenticación, la autenticación falla (ya que el router no puede intentar con un método alternativo).

Nota: La palabra clave group provee una forma de agrupar hosts servidores existentes. La función permite al usuario seleccionar un subconjunto de los hosts servidores configurados y los utiliza para un determinado servicio.

Ejemplo 2: Acceso a la consola con contraseña de línea

Expandamos la configuración del Ejemplo 1 de modo que el inicio de sesión de consola solo pueda ser autenticado por la contraseña establecida en línea con 0.

Se define la lista CONSOLA y luego, se aplica a line con 0.

Configuración:

```
<#root>
Router(config)#
aaa authentication login CONSOLE line
```

En el comando anterior:

- la lista que tiene nombre es CONSOLE.
- Existe un solo método de autenticación (línea).

Cuando se crea una lista con nombre (en este ejemplo, CONSOLE), se debe aplicar a una línea o interfaz antes de ejecutarse. Esto se hace con el login authentication

comando:

<#root>

```
Router(config)#
line con 0

Router(config-line)#
exec-timeout 0 0

Router(config-line)#
password cisco

Router(config-line)#
login authentication CONSOLE
```

La lista CONSOLA anula el valor predeterminado de la lista de métodos predeterminados en line con 0. Después de esta configuración en línea con 0, deberá ingresar la contraseña cisco para obtener acceso a la consola. La lista predeterminada aún se usa en tty, vty y aux.

Nota: Para la autenticación del acceso a la consola por un nombre de usuario y una contraseña locales, use el siguiente código de ejemplo:

<#root>

```
Router(config)#
aaa authentication login CONSOLE local
```

En este caso, se debe configurar un nombre de usuario y una contraseña en la base de datos local del router. También debe aplicarse la lista a la línea o interfaz.

Nota: Para no tener autenticación, utilice el siguiente ejemplo de código:

```
<#root>

Router(config)#

aaa authentication login CONSOLE none
```

En este caso, no hay autenticación para acceder a la consola. También debe aplicarse la lista a la línea o interfaz.

Ejemplo 3: Habilitar el acceso de modo con un servidor externo AAA

Puede ejecutar la autenticación para entrar al modo enable (privilegio 15).

Configuración:

```
<#root>

Router(config)#

aaa authentication enable default group radius enable
```

Solo se puede solicitar la contraseña; el nombre de usuario es $enab15$. Por lo tanto, se debe definir el nombre de usuario $enab15$ debe definirse en el servidor AAA.

Si el Servidor de radio no responde, tendrá que ser ingresada la contraseña habilitada configurada localmente en el router.

Autenticación PPP

El comando aaa authentication ppp se usa para autenticar una conexión PPP. En general, se usa para autenticar a los usuarios remotos de ISDN o analógicos que desean acceder a Internet o a una oficina central a través de un servidor de acceso.

Ejemplo 1: Método único de autenticación PPP para todos los usuarios

El servidor de acceso tiene una interfaz ISDN que está configurada para aceptar clientes de marcación PPP. Utilizamos un grupo rotativo de marcador 0, pero la configuración puede efectuarse en la interfaz principal o la interfaz de perfil de marcador.

Configuración:

```
<#root>

Router(config)#

aaa authentication ppp default group radius local
```

Este comando autentica a todos los usuarios PPP con Radius. Si el servidor Radius no responde, se utiliza la base de datos local.

Ejemplo 2: Autenticación PPP con una lista específica

Para usar una lista designada en lugar de la lista predeterminada, configure estos comandos:

```
<#root>

Router(config)#

aaa authentication ppp ISDN_USER group radius


Router(config)#

interface dialer 0


Router(config-if)#

ppp authentication chap ISDN_USER
```

En este ejemplo, la lista es ISDN_USER y el método es Radius.

Ejemplo 3: PPP iniciado desde sesión en modo carácter

El servidor de acceso tiene una tarjeta de módem interna (mica, Microcom o Next Port). Supongamos que ambos comandos aaa authentication login y aaa authentication ppp están configurados.

Si un usuario de módem primero accede al router con una sesión exec en modo carácter (por ejemplo, con la ventana de terminal después de marcar) el usuario es autenticado en una línea tty. Para iniciar una sesión en modo paquete, los usuarios deben escribir ppp default or ppp. Dado que la autenticación de PPP está configurada explícitamente (con aaa authentication ppp), el usuario se autentica nuevamente en el nivel de PPP.

Para evitar esta segunda autenticación, use la palabra clave if-needed.

```
<#root>

Router(config)#

aaa authentication login default group radius local

Router(config)#

aaa authentication ppp default group radius local if-needed
```

Nota: Si el cliente inicia directamente una sesión PPP, se realiza en forma directa la autenticación PPP ya que no hay acceso de inicio de sesión al servidor de acceso.

Configurar autorización

La autorización es el proceso mediante el cual puede controlar lo que un usuario puede hacer.

La autenticación AAA tiene las mismas reglas que la autenticación:

1. Primero, defina una lista que contenga métodos de autorización.
2. Luego aplique esa lista a una o más interfaces (excepto a la lista de métodos predeterminados).
3. Se utiliza el primer método indicado. Si falla en responder, se utiliza el segundo y así sucesivamente.

Las listas de métodos son específicas del tipo de autorización solicitada. Este documento se centra en los tipos de autorización de red y Exec.

Para más información sobre los otros tipos de autorización, consulte la Guía de configuración de seguridad de Cisco IOS.

autorización de EXEC

El comando aaa authorization exce determina si el usuario puede ejecutar EXEC shell. Este recurso debe devolver información del perfil de usuario como ser, información de comando automático, tiempo de espera inactivo, vencimiento de sesión, lista de acceso y privilegio y otros factores relacionados con cada usuario.

La autorización de exec solo se lleva a cabo a través de líneas vty y tty.

El siguiente ejemplo utiliza Radius.

Ejemplo 1: Los mismos métodos de autenticación exec para todos los usuarios

Cuando se autentica con:

<#root>

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

Todos los usuarios que quieran iniciar una sesión en el servidor de acceso deben estar autorizados con Radius (primer método) o con la base de datos local (segundo método).

Configuración:

<#root>

```
Router(config)#
aaa authorization exec default group radius local
```

Nota: En el servidor AAA, se debe seleccionar Service-Type=1 (inicio de sesión).

Nota: Con este ejemplo, si la palabra clave local no está incluida y el servidor AAA no responde, entonces no se podrá realizar la autorización y la conexión fallará.

Nota: En los siguientes ejemplos 2 y 3, no es necesario que agregue ningún comando en el router. Solo necesita configurar el perfil en el servidor de acceso.

Ejemplo 2: Asignar niveles de privilegios Exec desde el servidor AAA

Según el ejemplo 1, configure el siguiente par Cisco AV en el servidor AAA para que un usuario pueda iniciar sesión en el servidor de acceso e ingresar al modo de habilitación directamente:

```
shell:priv-lvl=15
```

El usuario ahora puede ir directamente al modo de activación.

Nota: Si el primer método falla en responder, entonces se utiliza la base de datos local. Sin embargo, el usuario no podrá ir directamente al modo de activación, sino que tendrá que ingresar el comando enable y suministrar la contraseña enable.

Ejemplo 3: Asignar tiempo de espera inactivo desde el Servidor AAA

Para configurar un tiempo de espera ocioso (de manera que la sesión se desconecte en caso de ausencia de tráfico luego del tiempo de espera ocioso), utilice el atributo IETF RADIUS 28:

Autorización de red

aaa authorization network ejecuta la autorización para todas las solicitudes de servicio relacionadas con la red como PPP, SLIP y ARAP. Esta sección se concentra en PPP, que es lo utilizado habitualmente.

El servidor AAA verifica si una sesión PPP del cliente está permitida. Además, el cliente puede solicitar las opciones de PPP: devolución de llamada, compresión, dirección IP, etc. Estas opciones deben configurarse en el perfil del usuario en el servidor AAA. Además, para un cliente específico, el perfil AAA puede contener tiempo de espera inactivo, lista de acceso y otros atributos por usuario que serán descargados por el software Cisco IOS y aplicados para este cliente.

Los siguientes ejemplos muestran la autorización con Radius.

Ejemplo 1: Los mismos métodos de autorización de red para todos los usuarios

El servidor de acceso se utiliza para aceptar conexiones de marcación PPP.

Se autentican los usuarios (tal como se configuró anteriormente) con:

```
<#root>

Router(config)#

aaa authentication ppp default group radius local
```

Utilice el siguiente comando para autorizar a los usuarios:

```
<#root>

Router(config)#

aaa authorization network default group radius local
```

Nota: En el servidor AAA, configure: Service-Type = 7 (framed) y Framed-Protocol = PPP.

Ejemplo 2: Aplicar atributos específicos del usuario

Puede utilizar el servidor AAA para asignar los atributos por usuario como dirección de IP, número de devolución de llamadas, valor de tiempo de espera inactiva del marcador o lista de acceso, entre otros. En este tipo de implementación, el NAS descarga los atributos adecuados desde el perfil de usuario del servidor AAA.

Ejemplo 3: Autorización PPP con una lista específica

Al igual que para autenticación, configure un nombre de lista en lugar de utilizar la predeterminada:

```
<#root>
```

```
Router(config)#
aaa authorization network ISDN_USER group radius local
```

Luego, se aplica la lista a la interfaz:

```
<#root>
  Router(config)#
interface dialer 0

  Router(config-if)#
ppp authorization ISDN_USER
```

Configuración de contabilidad

La función de contabilización AAA le permite efectuar un seguimiento de los servicios a los que tienen acceso los usuarios y la cantidad de recursos de red que consumen.

La auditoría AAA tiene las mismas reglas que la autenticación y la autorización:

1. Debe definir una lista que contenga métodos de contabilidad.
2. Luego aplique esa lista a una o más interfaces (excepto a la lista de métodos predeterminados).
3. Primero, se usa el primer método de la lista y, si éste no responde, se usa el segundo y así sucesivamente.

- La contabilidad de red proporciona información para todas las sesiones de PPP, Slip y Protocolo de acceso remoto AppleTalk (ARAP): conteo de paquetes, conteo de octetos, tiempo de sesión, tiempo de inicio y finalización.
- La contabilidad de Exec ofrece información acerca de las sesiones de terminal EXEC de usuario (una sesión telnet, por ejemplo) del servidor de acceso a la red: tiempo de sesión, tiempo de inicio y finalización.

En los siguientes ejemplos se describe cómo se puede enviar información al servidor AAA.

Ejemplos de configuración de contabilidad

Ejemplo 1: Generar registros contables de inicio y de detención

Para cada sesión PPP de marcación, se envía la información de auditoría al servidor AAA una vez que el cliente se autentica y después de la desconexión con la palabra clave start-stop.

<#root>

```
Router(config)#
```

aaa accounting network default start-stop group radius local

Ejemplo 2: Generar registros contables de detención únicamente

Si la información contable debe enviarse sólo luego de que un cliente se desconecte, utilice la palabra clave stop y configure la siguiente línea:

<#root>

```
Router(config)#
```

aaa accounting network default stop group radius local

Ejemplo 3: Generar registros de recurso para errores de autenticación y negociación

Hasta este punto, la auditoría AAA brinda soporte para registros de "inicio" y "detención" para llamadas que han superado la autenticación del usuario.

Si falla la autenticación o la negociación PPP, no hay registro de autenticación.

La solución es usar la contabilidad de detención por error del recurso AAA

<#root>

```
Router(config)#
```

aaa accounting send stop-record authentication failure

Un registro de detención es enviado al servidor AAA.

Ejemplo 4: Habilitar la contabilidad de recursos completos

Para habilitar la contabilidad de estado de todos los recursos, que genera un registro de inicio en la configuración de la llamada y un registro de detención en la terminación de la llamada, configure:

<#root>

```
Router(config)#
```

aaa accounting resource start-stop

Este comando fue introducido en la versión 12.1 (3)T del software Cisco IOS.

Con este comando, un registro de contabilidad de inicio-detención de configuración de llamada o desconexión de llamada hace un seguimiento del progreso de la conexión del recurso con el dispositivo. Otro registro de contabilidad iniciar-detener de la autenticación del usuario, realiza un seguimiento del progreso de administración del usuario. Estos dos conjuntos de registros contables están interrelacionados con una Id. de sesión exclusiva para la llamada.

Información Relacionada

- Soporte técnico y descargas de Cisco

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).