Configuración de AAA básico en un servidor de acceso

Contenido

Introducción
Antes de comenzar
Convenciones
prerrequisitos
Componentes Utilizados
Diagrama de la red
Configuración de AAA general
Habilitación del AAA
Especificación del servidor AAA externo
Configuración del servidor AAA
Configuración de la Autenticación
Autenticación de inicio de sesión
Autenticación PPP
Configuración de la autorización
autorización de EXEC
Autorización de red
Configuración de la contabilidad
Ejemplos de configuración de contabilidad
Información Relacionada

Introducción

Este documento explica cómo configurar el autenticación, autorización y contabilidad (AAA) en un router Cisco mediante 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: Siga leyendo por favor la sección configuración AAA general antes de proceder con la configuración de Cisco IOS®. El error hacer tan puede dar lugar al misconfiguration y al bloqueo subsiguiente.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de

Consejos Técnicos de Cisco.

prerrequisitos

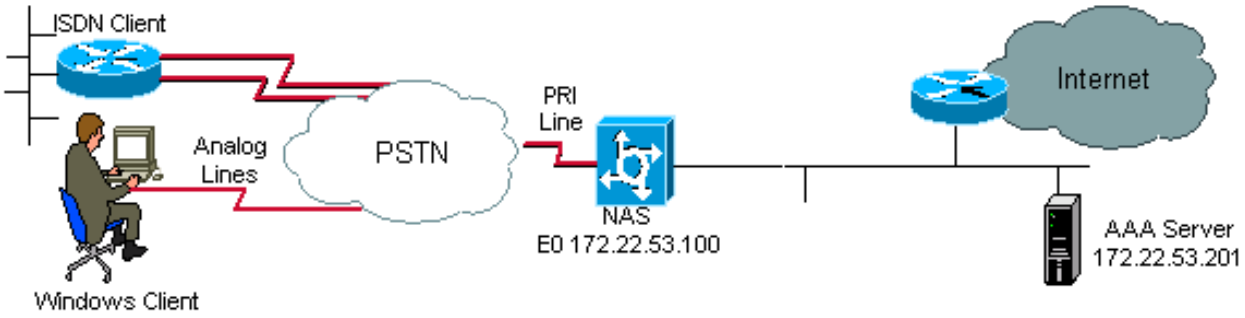
Para conseguir una descripción del AAA, y para los detalles completos sobre los comandos aaa y las opciones, refiera por favor a la guía de configuración de seguridad IOS 12.2: Autenticación, autorización y contabilidad.

Componentes Utilizados

La información en este documento se basa en la línea principal del Cisco IOS Software Release 12.1.

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.

Diagrama de la red



Configuración de AAA general

Habilitación del 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 y interfaces (excepto la **línea estafa 0 de la** línea de la consola). 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 usando la base de datos local del router. Para no ser bloqueado del router, recomendamos que defina un nombre de usuario y una contraseña en el servidor de acceso antes de comenzar la configuración AAA. Proceda como se muestra a continuación:

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

Consejo: Salve su configuración antes de configurar sus comandos aaa. Sólo debe volver a

guardar la configuración una vez que haya completado toda su configuración de AAA (y se haya asegurado de que funciona correctamente). Esto le permite recuperarse de cierres inesperados (antes de grabar la configuración), a través de la recarga de router.

Especificación del 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 usted está utilizando el TACACS+, utilice el **comando tacacs-server host <IP address of the AAA server> <key>**.

Si usted está utilizando el radio, utilice el **comando radius-server host <IP address of the AAA server> <key>**.

Configuración del servidor AAA

En el servidor de AAA, configure los parámetros siguientes:

- 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).
- El exacto la misma clave *<key>* configurada en el servidor de acceso.**Nota:** La clave es con diferenciación entre mayúsculas y minúsculas.
- El protocolo utilizado por el servidor de acceso (TACACS+ o Radius).

Refiera a su documentación del servidor de AAA para el procedimiento exacto usado para configurar los parámetros antedichos. 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 la Autenticación

La autenticación verifica a los usuarios antes de que les no prohiban el acceso a la red y a los servicios de red (que se verifican con la 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 la 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.

Los ejemplos de autenticación de más abajo utilizan Radius, identificación de entrada y autenticación de Point-to-Point Protocol (PPP) (el más comúnmente utilizado) 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 haya comunicación satisfactoria con un método de autenticación de la lista, o todos los métodos definidos en la lista de métodos se agotan.

Es importante observar que el Cisco IOS Software intenta la autenticación con el método de autenticación de la lista siguiente 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

Usted puede utilizar el **comando aaa authentication login** de autenticar a los usuarios que quieren el Acceso a Exec en el servidor de acceso (equipo teleescritor, vty, consola y aux.).

Ejemplo 1: Acceso Exec por medio de Radius y luego Local

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

En el comando mencionado arriba:

- 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 usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método). Para autenticación local, defina el nombre de usuario y la contraseña:

```
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 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: Con el ejemplo anterior, si no incluimos la palabra clave local, obtendremos:

```
Router(config)# aaa authentication login default group radius
```
Nota: Si el servidor AAA no responde a la petición de autenticación, la autenticación fallará (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. Para más información sobre esta función avanzada, refiera al Grupo de servidores AAA del documento.

Ejemplo 2: Acceso a la consola usando la contraseña de línea

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

La CONSOLA de la lista se define y después se aplica para alinear la estafa 0.

Configuramos:

```
Router(config)# aaa authentication login CONSOLE line
```
En el comando mencionado arriba:

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

Una vez creada una lista con un nombre asignado (en este ejemplo, CONSOLE), debe ser aplicada a una línea o interfaz para que surta efecto. Esto se hace usando el comando login authentication list_name:

```
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 de la CONSOLA reemplaza el valor por defecto de la lista del método predeterminado en la línea estafa 0. Usted necesita ingresar la contraseña “Cisco” (configurado en la línea con 0) para conseguir el acceso a la consola. La lista predeterminada todavía se utiliza en el equipo teleescritor, el vty y aux.

Nota: Para hacer el acceso a la consola autenticar por un nombre de usuario local y una contraseña, utilice:

```
Router(config)# aaa authentication login CONSOLE local
```
Nota: 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 ninguna autenticación, utilice

```
Router(config)# aaa authentication login CONSOLE none
```
Nota: 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 mediante un servidor externo AAA

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

Configuramos:

```
Router(config)# aaa authentication enable default group radius enable
```

Solamente la contraseña será pedida, el nombre de usuario es $enab15$. Por lo tanto el nombre de usuario $enab15$ se debe definir en el servidor de AAA.

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

Autenticación PPP

Utilizan al **comando aaa authentication ppp** de autenticar una conexión PPP. Se utiliza típicamente para autenticar el ISDN o a los usuarios remotos analogicos que quieren acceder Internet o 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 de ISDN que se configure para validar a los clientes de marcación de entrada PPP. Utilizamos un grupo rotativo de marcador 0, pero la configuración puede efectuarse en la interfaz principal o la interfaz de perfil de marcador.

Configuramos

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

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

Ejemplo 2: Autenticación PPP con una Lista específica.

Para utilizar una lista mencionada bastante que la lista predeterminada, configure los siguientes comandos:

```
Router(config)# aaa authentication ppp ISDN_USER group radius Router(config)# int dialer 0
Router(config-if)# pp 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 un indicador luminoso LED amarillo de la placa muestra gravedad menor del módem interno (mica, Microcom o puerto siguiente). Supongamos que ambos comandos aaa authentication login y aaa authentication ppp están configurados.

Si un usuario de módem primero accede al router utilizando una sesión exec en modo carácter (por ejemplo, utilizando 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. Puesto que la autenticación PPP se configura explícitamente (con la **autenticación PPP aaa**), autentican al usuario en el nivel PPP otra vez.

Para evitar esta segunda autenticación, podemos utilizar la palabra clave “if-needed”.

```
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.

Si desea obtener más información acerca de la autenticación AAA, consulte los documentos IOS 12.2 de la Guía de configuración de seguridad: Configuración de Autenticación e Implementación de Caso Práctico de Cisco AAA.

Configuración de la autorización

La autorización es el proceso mediante el cual puede controlar lo que un usuario puede o no hacer.

La autenticación AAA tiene las mismas reglas que la autenticación:

1. Primero, defina una lista que contenga métodos de autorización.
2. Entonces aplique esa lista a una o más interfaces (a excepción de la lista del método predeterminado).
3. Se utiliza el primer método mencionado. 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 del ejecutivo y de la Autorización de red.

Para más información sobre los otros tipos de autorización, consulte la Guía de configuración de seguridad de Cisco IOS, versión 12.2.

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 se realiza solamente sobre el vty y las líneas equipo teleescritor.

El siguiente ejemplo utiliza Radius.

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

Una vez que se autenticados con:

```
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 mediante Radius (primer método) o mediante la base de datos local (segundo método).

Configuramos:

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

Nota: En el servidor de AAA, Service-Type=1 (login) debe ser seleccionado.

Nota: Con este ejemplo, si la **palabra clave local** no es incluida y no responde el servidor de AAA, después la autorización nunca será posible y la conexión fallará.

Nota: En los ejemplos 2 y 3 abajo, no necesitamos agregar el comando any en el router pero configurar solamente el perfil en el servidor de acceso.

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

De acuerdo con el ejemplo 1, si se va un usuario que registra en el servidor de acceso a ser permitido ingresar el enable mode directamente, configure el cisco av-pair siguiente en el servidor de AAA:

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

Esto significa que el usuario irá directamente al modo activado.

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

Ejemplo 3: Asignación de 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: Ocioso-descanso bajo perfil de usuario.

Autorización de red

El comando aaa authorization network autoriza a todas las peticiones de servicios 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. Es más, el cliente puede solicitar las opciones PPP: servicio repetido, compresión, dirección IP, y así sucesivamente. 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.

La autorización de la demostración del siguiente ejemplo usando el radio:

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.

En primer lugar, se autentican los usuarios (tal como se configuró anteriormente) mediante:

```
Router(config)# aaa authentication ppp default group radius local
```
entonces se deben autorizar mediante:

```
Router(config)# aaa authorization network default group radius local
```
Nota: En el servidor de AAA, configure:

- Service-Type=7 (entramado)
- Protocolo entramado = PPP

Ejemplo 2: Aplicación de los 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, etc. 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, podemos configurar un nombre de lista en lugar de utilizar la predeterminada.

```
Router(config)# aaa authorization network ISDN_USER group radius local
```
Luego, se aplica la lista a la interfaz.

```
Router(config)# int dialer 0
Router(config-if)# ppp authorization ISDN_USER
```
Si desea obtener más información acerca de la autenticación AAA, consulte los documentos IOS 12.2 de la Guía de configuración de seguridad: Configuración de Autenticación e Implementación de Caso Práctico de Cisco AAA.

Configuración de la 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.

Las estadísticas AAA tienen las mismas reglas que la autenticación y 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.

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): la cuenta de paquetes, los octects cuenta, tiempo de la sesión, hora de inicio y de detención.
- 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 detención.

Para más información sobre los otros tipos de autorización, consulte la Guía de configuración de seguridad de Cisco IOS, versión 12.2.

Los siguientes ejemplos describen cómo se puede enviar información al servidor AAA.

Ejemplos de configuración de contabilidad

Ejemplo 1: Generación de registros contables de inicio y de detención

Para cada sesión PPP de marcado de entrada, la información de la cuenta se envía al servidor de AAA una vez que autentican al cliente y después de la desconexión usando la palabra clave **por marcha-parada**.

```
Router(config)# aaa accounting network default start-stop group radius local
```

Ejemplo 2: Generación de registros contables de detención únicamente

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

```
Router(config)# aaa accounting network default stop group radius local
```

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

Hasta esta punta, las estadísticas AAA proporcionan el soporte del registro de inicio y detención para las llamadas que han pasado la autenticación de usuario.

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

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

```
Router(config)# aaa accounting send stop-record authentication failure
```

Un registro de detención es enviado al servidor AAA.

Ejemplo 4: Habilitación de 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:

```
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 mediante una Id. de sesión exclusiva para la llamada.

Si desea obtener más información acerca de la autenticación AAA, consulte los documentos IOS 12.2 de la Guía de configuración de seguridad: Configuración de Autenticación e Implementación de Caso Práctico de Cisco AAA.

Información Relacionada

- Soporte Técnico - Cisco Systems