Configuración básica del cambio de autorización en el switch Catalyst 1300 mediante CLI

Objetivo

El objetivo de este artículo es mostrarle cómo realizar una configuración básica de la función de cambio de autorización (CoA) en switches Catalyst 1300 mediante la interfaz de línea de comandos (CLI).

Dispositivos y versiones de software aplicables

- switches Catalyst 1300 | 4.1.3.36

Introducción

Change of Authorization (CoA) es una extensión del protocolo RADIUS que permite cambiar las propiedades de una sesión de usuario de autenticación, autorización y administración de cuentas (AAA) o dot1x después de que se haya autenticado. Cuando cambia una política para un usuario o grupo en AAA, los administradores pueden transmitir paquetes CoA de RADIUS desde el servidor AAA, como Cisco Identity Services Engine (ISE), para reiniciar la autenticación y aplicar la nueva política.

Cisco Identity Services Engine (o ISE) es un motor de aplicación de políticas y control de acceso basado en red con todas las funciones. Proporciona análisis y aplicación de seguridad, servicios RADIUS y TACACS, distribución de políticas y mucho más. Cisco ISE es actualmente el único cliente de autorización dinámica de CoA compatible para los switches Catalyst 1300. Consulte la guía ISE Admin para obtener más información.

La compatibilidad con CoA se ha agregado a los switches Catalyst 1300 en la versión de firmware 4.1.3.36. Esto incluye la compatibilidad con la desconexión de usuarios y el cambio de autorizaciones aplicables a una sesión de usuario. El dispositivo admite las siguientes acciones de CoA:

- Sesión de desconexión
- Desactivar el comando CoA del puerto del host
- Comando Bounce host port CoA
- Comando Reauthenticate Host CoA

En este artículo, encontrará los comandos para una configuración básica de CoA en switches Catalyst 1300 mediante CLI. Los pasos pueden variar según la configuración

y los requisitos del usuario.

Table Of Contents

Configuración básica de CoA mediante CLI

Configuración del Servidor RADIUS y la Contabilización RADIUS

Para configurar el servidor RADIUS, en el modo de configuración global, utilice los siguientes comandos:

Paso 1

Utilice el comando radius-server key para establecer la clave de autenticación para las comunicaciones RADIUS entre el dispositivo y el demonio RADIUS.

```
radius-server key
```

Paso 2

Utilice el comando radius-server host para configurar un host de servidor RADIUS.

```
radius-server host key priority 1 usage dot1.x
```

- La dirección IP será la dirección IP del servidor ISE.
- key <key-string> - Especifica la clave de autenticación y cifrado para todas las comunicaciones RADIUS entre el dispositivo y el servidor RADIUS. Esta clave debe coincidir con el cifrado utilizado en el demonio RADIUS.
- Prioridad: Especifica el orden en el que se utilizan los servidores, donde 0 tiene la prioridad más alta. (Intervalo: de 0 a 65535)
- usage dot1.x - especifica que el servidor RADIUS se utiliza para la autenticación de puertos 802.1x.

Paso 3

```
aaa accounting dot1x start-stop group radius
```

Configurar servidor de autorización dinámica

Paso 1

Desde el modo de configuración global, ingrese al modo de configuración de CoA ejecutando el comando:

```
aaa server radius dynamic-author
```

Paso 2

Para configurar la clave RADIUS que se compartirá entre el dispositivo y un cliente CoA (rango: 0-128 caracteres), utilice el comando server-key <key-string> en el modo de configuración del servidor local de autorización dinámica. La clave proporcionada en la solicitud de CoA debe coincidir con esta clave.

```
server-key
```

> **Note:**
> Para ISE, la cadena de clave será la misma cadena de clave especificada para la cadena de clave del servidor RADIUS al configurar RADIUS.

Paso 3

Introduzca la dirección IP del host del cliente CoA. La dirección IP puede ser IPv4, IPv6 o IPv6z.

```
client
```

Paso 4

```
Exit
```

Configuración de 802.1x

Para habilitar 802.1X globalmente, utilice el comando dot1x system-auth-control.

```
dot1x system-auth-control
```

Configuración de 802.1x en un puerto

Paso 1

Ingrese la configuración de la interfaz y seleccione el ID de la interfaz usando el comando interface GigabitEthernet<Interface ID>.

```
interface gi1/0/1
```

Paso 2

Para habilitar el control manual del estado de autorización de puerto, utilice el comando dot1x port-control. El modo automático permite la autenticación 802.1X en el puerto y hace que pase al estado autorizado o no autorizado, según el intercambio de autenticación 802.1X entre el dispositivo y el cliente.

```
dot1x port-control auto
```

Paso 3

Para iniciar manualmente la reautenticación de todos los puertos habilitados para 802.1X o del puerto habilitado para 802.1X especificado, utilice el comando dot1x re-authenticate en el modo EXEC privilegiado.

```
dot1x re-authenticate gi1/0/1
```

Paso 4

Para configurar el modo de aprendizaje de seguridad de puertos, utilice el comando port security mode Interface (Ethernet, Port Channel) configuration mode. El parámetro Secure delete-on-reset es un modo seguro con aprendizaje limitado de direcciones MAC seguras con el tiempo de vida de delete-on-reset.

```
port security mode secure delete-on-reset
```

Paso 5

Para salir de la configuración de la interfaz, introduzca lo siguiente:

```
exit
```

Otros comandos para la configuración de CoA

Estos son algunos de los otros comandos de CoA que se pueden utilizar en función de su configuración y configuración.

- attribute event-timestamp drop-packet: este comando se utiliza en el modo de configuración del servidor local de autorización dinámica para configurar el dispositivo para descartar una solicitud de paquete de desconexión (PoD) o una solicitud CoA que no incluyen un atributo event-timestamp.

```
attribute event-timestamp drop-packet
```

- authentication command bounce-port ignore - Para configurar el dispositivo para que ignore un comando de puerto de rebote de cambio de autorización (CoA) RADIUS, utilice el comando de autenticación bounce-port ignore en el modo de configuración global.

```
authentication command bounce-port ignore
```

- authentication command disable-port ignore - Para configurar el dispositivo para que ignore un comando de desactivación de puerto de RADIUS CoA, utilice este comando en el modo de configuración global.

```
authentication command disable-port ignore
```

- domain delimiter <character>: para configurar el delimitador de dominio de nombre de usuario para las solicitudes recibidas de PoD y CoA, utilice el comando domain delimiter en el modo de configuración del servidor local de autorización dinámica.

```
domain delimiter $
```

En este ejemplo, el carácter $ se configura como delimitador.

- desmontaje de dominio [de derecha a izquierda]: para habilitar y definir el comportamiento del desmontaje de dominio de nombre de usuario para solicitudes de CoA y PoD recibidas, utilice el comando desmontaje de dominio en el modo de configuración del servidor local de autorización dinámica.

```
domain stripping right-to-left
```

- ignore server-key: este comando se utiliza en el modo de configuración del servidor local de autorización dinámica para configurar el dispositivo para que ignore la clave del servidor CoA.

```
ignore server-key
```

Comandos CLI en el Modo Exec de Privilegio

Desde el modo exec de privilegio, puede ejecutar los comandos show en los clientes autenticados, borrar los contadores del cliente y mostrar la configuración del Servidor de autorización dinámica.

- Utilice el comando show aaa clients para mostrar las estadísticas del cliente AAA (CoA).

```
show aaa clients
```

- Utilice el comando show aaa server radius dynamic-author para mostrar la configuración de CoA.

```
show aaa server radius dynamic-author
```

- clear aaa counters se puede utilizar para borrar los contadores de clientes aaa

```
clear aaa clients counters
```

Conclusión

Ha completado un cambio básico de configuración de autorización (CoA) en el switch Catalyst 1300 mediante CLI.

Para obtener más información sobre los comandos CLI para los switches Catalyst 1300, refiérase a la Guía CLI de los Switches Catalyst de Cisco serie 1300.

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).