Configuración de TACACS+, RADIUS y Kerberos en switches Catalyst

Contenido

Introducción

La familia de switches Cisco Catalyst (Catalyst 4000, Catalyst 5000 y Catalyst 6000 que ejecuta CatOS) ha soportado cierto modo de autenticación, que comienza con el código 2.2. Se han agregado mejoras con las versiones posteriores. El puerto TCP 49 de TACACS+, no el puerto 49 del protocolo de datagramas de usuario (UDP) XTACACS, RADIUS o la configuración de usuario del servidor Kerberos para la autenticación, autorización y contabilidad (AAA) es el mismo que para los usuarios del router. Este documento contiene ejemplos de los comandos mínimos necesarios para habilitar estas funciones. Hay opciones adicionales disponibles en la documentación del switch para la versión en cuestión.

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.

Antecedentes

Dado que las versiones posteriores del código admiten opciones adicionales, debe ejecutar el comando **show version** para determinar la versión del código en el switch. Una vez que haya determinado la versión del código que se utiliza en el switch, utilice esta tabla para determinar qué opciones hay disponibles en su equipo y qué opciones desea configurar.

Permanezca siempre en el switch cuando agregue autenticación y autorización. Pruebe la configuración en otra ventana para evitar que se bloquee accidentalmente.

Método (mínimo)	**Cat Versión 2.2 a 5.1**	**Cat Versión 5.1 a 5.4.1**	**Cat Versión 5.4.1 a 7.5.1**	**Cat versión 7.5.1 y posterior**
Autenticación TACACS+ O	Paso A	Paso A	Paso A	Paso A
Autenticación RADIUS O	N/A	Paso B	Paso B	Paso B
Autenticación Kerberos O	N/A	N/A	Paso K	Paso K
Autenticación/autorización de nombre de usuario local	N/A	N/A	N/A	Paso C
Plus (opciones)				
Autorización de Comandos con TACACS+	N/A	N/A	Paso D	Paso D
Autorización de Exec TACACS+	N/A	N/A	Paso E	Paso E
Autorización RADIUS Exec	N/A	N/A	Paso F	Paso F
Contabilidad - TACACS+ o RADIUS	N/A	N/A	Paso G	Paso G

Autorización de activación de TACACS+	Paso H	Paso H	Paso H	Paso H
RADIUS Enable Authorization	N/A	Paso I	Paso I	Paso I
Autorización de activación de TACACS+	N/A	N/A	Paso J	Paso J

Configuration Steps

Paso A – Autenticación de TACACS+

Con las versiones anteriores del código, los comandos no son tan complejos como con algunas versiones posteriores. En el switch se pueden encontrar opciones adicionales en versiones posteriores.

1. Ejecute el comando **set authentication login local enable** para asegurarse de que haya una puerta trasera en el switch si el servidor está inactivo.
2. Ejecute el comando **set authentication login tacacs enable** para habilitar la autenticación TACACS+.
3. Ejecute el **comando set tacacs server #.#.#.#** para definir el servidor.
4. Ejecute el comando set tacacs key *your_key* para definir la clave del servidor, que es opcional con TACACS+, ya que hace que los datos de switch a servidor se cifren. Si se utiliza, debe estar de acuerdo con el servidor.**Nota:** El software Cisco Catalyst OS **no** acepta que el signo de interrogación (**?**) forme parte de ninguna clave o contraseña. El signo de interrogación se utiliza explícitamente para obtener ayuda sobre la sintaxis del comando.

Paso B – Autenticación de RADIUS

Con las versiones anteriores del código, los comandos no son tan complejos como con algunas versiones posteriores. En el switch se pueden encontrar opciones adicionales en versiones posteriores.

1. Ejecute el comando **set authentication login local enable** para asegurarse de que haya una puerta trasera en el switch si el servidor está inactivo.
2. Ejecute el comando **set authentication login radius enable** para habilitar la autenticación RADIUS.
3. Defina el servidor. En todos los demás equipos de Cisco, los puertos RADIUS predeterminados son 1645/1646 (autenticación/contabilidad).En el Catalyst, el puerto predeterminado es 1812/1813. Si utiliza Cisco Secure o un servidor que se comunica con otros equipos de Cisco, utilice el puerto 1645/1646. Ejecute el comando **set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** para definir el servidor y el comando equivalente en Cisco IOS como **radius-server source-ports 1645-1646**.
4. Defina la clave del servidor.Esto es obligatorio, ya que hace que la contraseña de switch a servidor se cifre como en RADIUS Authentication/Authorization RFC 2865 y RADIUS Accounting RFC 2866 . Si se utiliza, debe estar de acuerdo con el servidor. Ejecute el comando **set radius key *your_key.***

Paso C – Autenticación/autorización del nombre de usuario local

A partir de la versión 7.5.1 de CatOS, es posible la autenticación de usuario local. Por ejemplo, puede lograr la autenticación/autorización con el uso de un nombre de usuario y una contraseña almacenados en el Catalyst, en lugar de la autenticación con una contraseña local.

Sólo hay dos niveles de privilegio para la autenticación de usuario local, 0 o 15. El nivel 0 es el nivel exec no privilegiado. El nivel 15 es el nivel de habilitación privilegiado.

Si agrega estos comandos en este ejemplo, el usuario `poweruser` llega al modo enable en una Telnet o consola al switch y el usuario `nonenable` llega al modo exec en una Telnet o consola al switch.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Nota: Si el usuario `nonenable` conoce la **contraseña de activación establecida**, ese usuario puede continuar activando el modo.

Después de la configuración, las contraseñas se almacenan cifradas.

La autenticación de nombre de usuario local se puede utilizar junto con el exec TACACS+ remoto, la contabilidad de comandos o la contabilidad RADIUS exec remota. También se puede utilizar junto con la autorización remota de comando o exec TACACS+, pero no tiene sentido utilizarla de esta manera porque el nombre de usuario debe almacenarse tanto en el servidor TACACS+ como localmente en el switch.

Paso D - Autorización del comando TACACS+

En este ejemplo, se indica al switch que requiera autorización sólo para los comandos de configuración con TACACS+. En el caso de que el servidor TACACS+ esté inactivo, la autenticación no es ninguna. Esto se aplica tanto al puerto de la consola como a la sesión Telnet. Ejecutar este comando:

set authorization command enable config tacacs none

En este ejemplo, puede configurar el servidor TACACS+ para permitir cuando establezca estos parámetros:

```
command=set
arguments (permit)=port 2/12
```

El comando **set port enable 2/12** se envía al servidor TACACS+ para su verificación.

Nota: Con la autorización de comandos habilitada, a diferencia del router donde enable no se considera un comando, el switch envía el comando **enable** al servidor cuando se intenta habilitar. Asegúrese de que el servidor también esté configurado para permitir el comando **enable**.

Paso E - Autorización de excec con TACACS+

En este ejemplo, se indica al switch que requiera autorización para una sesión exec con TACACS+. En el caso de que el servidor TACACS+ esté inactivo, la autorización no es ninguna. Esto se aplica tanto al puerto de la consola como a la sesión Telnet. Ejecute el comando **set authorization exec enable tacacs+ none**

Además de la solicitud de autenticación, esto envía una solicitud de autorización independiente al servidor TACACS+ desde el switch. Si el perfil de usuario está configurado para shell/exec en el servidor TACACS+, ese usuario puede acceder al switch.

Esto evita que los usuarios sin el servicio shell/exec configurado en el servidor, como los usuarios PPP, inicien sesión en el switch. Recibe un mensaje que lee `Error en la autorización del modo Exec`. Además de permitir/denegar el modo exec para los usuarios, se puede forzar al modo enable al ingresar con el nivel de privilegio 15 asignado en el servidor. Debe ejecutar el código en el que se ha corregido el ID de bug de Cisco CSCdr51314 (sólo clientes registrados).

Paso F – Autorización de ejecución de RADIUS

No hay ningún comando para habilitar la autorización de ejecución RADIUS. La alternativa es establecer el tipo de servicio (atributo RADIUS 6) en Administrativo (valor 6) en el servidor RADIUS para iniciar al usuario en el modo de activación en el servidor RADIUS. Si el tipo de servicio está configurado para algo que no sea 6-administrativo, por ejemplo, 1-login, 7-shell o 2-framed, el usuario llega al mensaje de ejecución del switch, pero no al mensaje de activación.

Agregue estos comandos en el switch para la autenticación y autorización:

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Paso G - Contabilidad - TACACS+ o RADIUS

Para habilitar la contabilización TACACS+ para:

1. Si obtiene el mensaje del switch, ejecute el **comando set accounting exec enable start-stop tacacs+**.
2. Los usuarios que envían Telnet fuera del switch emiten el **comando set accounting connect enable start-stop tacacs+**.
3. Si reinicia el switch, ejecute el **comando set accounting system enable start-stop tacacs+**.
4. Los usuarios que realizan comandos, emiten el **comando set accounting enable all start-stop tacacs+**.
5. Recordatorios al servidor, por ejemplo, para actualizar los registros una vez por minuto para mostrar que el usuario aún está conectado, ejecute el comando **set accounting update regular 1**.

Para habilitar la contabilización RADIUS para:

1. Los usuarios que reciben el mensaje del switch, emiten el comando **set accounting exec enable start-stop radius**.
2. Los usuarios que Telnet sale del switch, emiten el comando **set accounting connect enable start-stop radius**.
3. Cuando reinicie el switch, ejecute el **comando set accounting system enable start-stop**

radius.

4. Recordatorios al servidor, por ejemplo, para actualizar los registros una vez por minuto para mostrar que el usuario aún está conectado, ejecute el comando **set accounting update regular 1**.

Registros gratuitos de TACACS+

Este resultado es un ejemplo de cómo pueden aparecer los registros en el servidor:

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS en Salida de Registro UNIX

Este resultado es un ejemplo de cómo pueden aparecer los registros en el servidor:

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
```

```
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

Step H - TACACS+ habilita la autenticación

Complete estos pasos:

1. Ejecute el comando **set authentication enable local enable** para asegurarse de que haya una puerta trasera en caso de que el servidor esté inactivo.
2. Ejecute el comando **set authentication enable tacacs enable** para decirle al switch que envíe solicitudes de habilitación al servidor.

Paso I – Autenticación de habilitación RADIUS

Agregue estos comandos para que el switch envíe el nombre de usuario `$enab15$` al servidor RADIUS. No todos los servidores RADIUS admiten este tipo de nombre de usuario. Consulte el paso E para obtener otra alternativa, por ejemplo, si establece un tipo de servicio [atributo RADIUS 6 - a Administrativo], que inicia a usuarios individuales en el modo habilitar.

1. Ejecute el comando **set authentication enable local enable** para asegurarse de que haya una puerta trasera en caso de que el servidor esté inactivo.
2. Ejecute el comando **set authentication enable radius enable** para decirle al switch que envíe solicitudes de habilitación al servidor si su servidor RADIUS soporta el nombre de usuario $enab15$.

Paso J - Habilitar autorización TACACS+

La adición de este comando da como resultado que el switch envíe enable al servidor cuando el usuario intenta habilitar. El servidor debe tener el comando **enable** permitido. En este ejemplo, hay una conmutación por fallas a ninguno en caso de que el servidor esté inactivo:

set autor enable enable tacacs+ none ambos

Paso K: autenticación de Kerberos

Consulte Control y Monitoreo del Acceso al Switch Usando Autenticación, Autorización y Contabilización para obtener más información sobre cómo configurar Kerberos en el switch.

Recuperación de contraseña

Refiérase a Procedimientos de Recuperación de Contraseña para obtener más información sobre

los procedimientos de Recuperación de Contraseña.

Esta página es el índice de procedimientos de recuperación de contraseña para los productos de Cisco.

Comandos ip permit para seguridad adicional

Para mayor seguridad, el Catalyst se puede configurar para controlar el acceso Telnet a través de los comandos **ip permit**:

set ip permit enable telnet

set ip permit *range mask*|*host*

Esto permite solamente el rango o los hosts especificados para Telnet en el switch.

Depuración en Catalyst

Antes de habilitar la depuración en el Catalyst, verifique los registros del servidor por los motivos de falla. Esto es más fácil y menos disruptivo para el switch. En versiones anteriores del switch, la **depuración** se realizó en el modo de ingeniería. No es necesario acceder al modo de ingeniería para ejecutar los comandos **debug** en versiones posteriores del código:

set trace tacacs|radius|kerberos 4

Nota: El comando **set trace tacacs|radius|kerberos 0** devuelve el Catalyst al modo sin seguimiento.

Consulte Página de Soporte de Productos de Switches para obtener más información sobre los Switches LAN multicapa.

Información Relacionada

- Comparación de TACACS+ y RADIUS
- RADIUS, TACACS+ y Kerberos en la Documentación de Cisco IOS
- Página de soporte de RADIUS
- Página de soporte de TACACS/TACACS+
- Página de soporte de Kerberos
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems