Configurar el TACACS+, el RADIUS, y el Kerberos en el Switches del Cisco 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 TACACS+, no el puerto 49 del User Datagram Protocol (UDP) del XTACACS), RADIUS, o configuración de usuario del servidor de Kerberos para el Authentication, Authorization, and Accounting (AAA) es lo mismo que para los usuarios del router. Este documento contiene los ejemplos de los comandos mínimos necesarios para habilitar estas funciones. Las opciones adcionales están disponibles en el Switch Documentation para la versión en la pregunta.

prerrequisitos

Requisitos

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

Puesto que versiones del código posteriores soportan las opciones adcionales, usted necesita publicar el **comando show version** para determinar la versión del código en el Switch. Una vez que usted ha determinado la versión del código que se utiliza en el Switch, utilice esta tabla para determinar qué opciones están disponibles en su equipo, y qué opciones usted desea configurar.

Permanezca siempre en el Switch cuando usted agrega la autenticación y autorización. Pruebe la configuración en otra ventana para evitar accidentalmente ser bloqueada hacia fuera.

Método (mínimo)	**Versión Cat 2.2 a 5.1**	**Versión Cat 5.1 a 5.4.1**	**Versión Cat 5.4.1 a 7.5.1**	**Versión Cat 7.5.1 y posterior**
Autenticación de TACACS+ O	Paso A	Paso A	Paso A	Paso A
Autenticación de RADIUS O	N/A	Paso B	Paso B	Paso B
Autenticación de Kerberos O	N/A	N/A	Paso K	Paso K
Autenticación/autorización del nombre de usuario local	N/A	N/A	N/A	Paso C
Más (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 de RADIUS Exec	N/A	N/A	Paso F	Paso F
El considerar - TACACS+ o RADIUS	N/A	N/A	Paso G	Paso G

Autorización del permiso TACACS+	Paso H	Paso H	Paso H	Paso H
Habilitar Radius autorización	N/A	Paso I	Paso I	Paso I
Autorización del permiso TACACS+	N/A	N/A	Paso J	Paso J

Pasos de configuración

Paso A – Autenticación de TACACS+

Con las versiones anteriores del código, los comandos no son tan complejos como con algunas versiones posteriores. Las opciones adcionales en versiones posteriores pueden estar disponibles en su Switch.

1. Publique el comando del **set authentication login local enable** para aseegurarse allí es una entrada posterior en el Switch si el servidor está abajo.
2. Publique el **comando set authentication login tacacs enable** para habilitar autenticación de TACACS+.
3. Publique el comando del **set TACASCS server - - - -** para definir el servidor.
4. Publique el comando **dominante del** *your_key de los* **tacacs del conjunto** para definir la clave del servidor, que es opcional con el TACACS+, pues hace los datos del Switch-a-servidor ser cifrada. Si está utilizado, debe estar de acuerdo con el servidor.**Nota:** El software de sistema operativo del Cisco Catalyst no valida el signo de interrogación (**?**) para ser parte de ningunas claves o contraseñas. El signo de interrogación se utiliza explícitamente para la ayuda en la sintaxis de los comandos.

Paso B – Autenticación de RADIUS

Con las versiones anteriores del código, los comandos no son tan complejos como con algunas versiones posteriores. Las opciones adcionales en versiones posteriores pueden estar disponibles en su Switch.

1. Publique el comando del **set authentication login local enable** para aseegurarse allí es una entrada posterior en el Switch si el servidor está abajo.
2. Publique el comando del **set authentication login radius enable** para habilitar la autenticación de RADIUS.
3. Defina el servidor. En el resto del equipo de Cisco, los puertos del RADIUS predeterminado son 1645/1646 (autenticación/las estadísticas).En el Catalyst, el puerto predeterminado es 1812/1813. Si usted utiliza Cisco asegure o un servidor que comunica con el otro equipo de Cisco, utiliza el puerto de 1645/1646. Publique el comando del **set radius server - - - - auth-port 1645 acct-port 1646 primary** para definir el servidor y el comando equivalente en el Cisco IOS como **puertos de origen del radio-servidor 1645-1646**.
4. Defina la clave del servidor.Esto es obligatorio, pues hace la contraseña del Switch-a-servidor ser cifrada como en el RFC 2866 de las estadísticas de la autenticación de RADIUS/ del RFC 2865 y RADIUS de la autorización . Si está utilizado, debe estar de acuerdo con el servidor. Publique el comando del *your_key de la* **clave del radio del conjunto**.

Paso C – Autenticación/autorización del nombre de usuario local

Comenzando en la versión CatOS 7.5.1, la autenticación de usuario local es posible. Por ejemplo, usted puede alcanzar la autenticación/la autorización con el uso de un nombre de usuario y contraseña salvado en el Catalyst, en vez de la autenticación con una contraseña local.

Hay solamente dos niveles de privilegio para la autenticación de usuario local, 0 o 15. El nivel 0 es el nivel sin privilegios del ejecutivo. El nivel 15 es el nivel privilegiado del permiso.

Si usted agrega estos comandos en este ejemplo, el poweruser usuario llega en el enable mode en Telnet o la consola al Switch y al usuario `nonenable` llega en el modo EXEC en Telnet o la 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 habilitada del conjunto**, ese usuario puede continuar al enable mode.

Después de la configuración, se salvan las contraseñas cifraron.

La autenticación del nombre de usuario local se puede utilizar conjuntamente con el ejecutivo remoto TACACS+, las estadísticas del comando, o el RADIUS remoto exec accounting. Puede también ser utilizada conjuntamente con el ejecutivo remoto o el comando authorization TACACS+, pero no tiene sentido de utilizarlo esta manera porque el nombre de usuario necesita ser salvado en el servidor TACACS+ así como localmente en el Switch.

Paso D - Autorización del comando TACACS+

En este ejemplo, el Switch se dice para requerir la autorización para solamente los comandos configuration con el TACACS+. En caso que el servidor TACACS+ esté abajo, la autenticación no es ninguna. Esto se aplica al puerto de la consola y a la sesión telnet. Ejecutar este comando:

set authorization commands enable config tacacs none both

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

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

Envían el **comando set port enable 2/12 al** servidor para verificación TACACS+.

Nota: Con el comando authorization habilitado, a diferencia en del router donde el permiso no se considera un comando, el Switch envía el **comando enable al** servidor cuando se intenta un permiso. Aseegurese que el servidor también está configurado para permitir el **comando enable**.

Paso E - Autorización de excec con TACACS+

En este ejemplo, el Switch se dice para requerir la autorización para una sesión EXEC con el TACACS+. En caso que el servidor TACACS+ esté abajo, la autorización no es ninguna. Esto se aplica al puerto de la consola y a la sesión telnet. Publique el comando del **set authorization exec**

enable tacacs+ none both

Además del pedido de autenticación, esto envía un pedido de autorización separado al servidor TACACS+ del Switch. Si el perfil del usuario se configura para el shell/el ejecutivo en el servidor TACACS+, ese usuario puede acceder el Switch.

Esto previene a los usuarios sin el servicio del shell/del ejecutivo configurado en el servidor, tal como usuarios PPP, del registro en el Switch. Usted consigue un mensaje que lea la `autorización del modo EXEC fallada`. Además del permiso/que niega al modo EXEC para los usuarios, usted puede ser forzado en el enable mode cuando usted ingresa con el nivel de privilegio 15 asignado en el servidor. Debe el runcode en el cual se repara el Id. de bug Cisco CSCdr51314 (clientes registrados solamente).

Paso F – Autorización de ejecución de RADIUS

No hay comando de habilitar la autorización de RADIUS Exec. La alternativa es fijar el tipo de servicio (atributo de RADIUS 6) a administrativo (un valor de 6) en el servidor de RADIUS para iniciar al usuario en el enable mode en el servidor de RADIUS. Si fijan al tipo de servicio para cualquier cosa con excepción de 6-administrative, por ejemplo, 1-login, 7-shell, o 2-framed, el usuario llega el prompt exec del Switch, pero no el prompt del permiso.

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

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

Paso G - Contabilidad - TACACS+ o RADIUS

Para habilitar el TACACS+ que explica:

1. Si usted consigue el prompt del Switch, publique el comando del **set accounting exec enable start-stop tacacs+**.
2. Usuarios ese problema del switch de los de Telnet el comando del **set accounting connect enable start-stop tacacs+**.
3. Si usted reinicia el Switch, publique el comando del **set accounting system enable start-stop tacacs+**.
4. Los usuarios que realizan los comandos, publican el **set accounting commands enable que todos iniciar-detener tacacs+** ordenan.
5. Recordatorios al servidor, por ejemplo, poner al día los expedientes una vez que un minucioso para mostrar que todavía abren una sesión al usuario, publica el comando del **set accounting update periodic 1**.

Para habilitar el RADIUS que explica:

1. Los usuarios que consiguen el prompt del Switch, publican el comando del **set accounting exec enable start-stop radius**.
2. Usuarios que el Switch de los de Telnet, publica el comando del **set accounting connect enable start-stop radius**.
3. Cuando usted reinicia el Switch, publique el comando del **set accounting system enable start-stop radius**.
4. Recordatorios al servidor, por ejemplo, poner al día los expedientes una vez que un

minucioso para mostrar que todavía abren una sesión al usuario, publica el comando del **set accounting update periodic 1**.

Expedientes del Freeware TACACS+

Esta salida es un ejemplo de cómo los expedientes pueden aparecer en el servidor:

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

RADIUS en la salida del expediente de UNIX

Esta salida es un ejemplo de cómo los expedientes pueden aparecer en el servidor:

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

Step H - TACACS+ habilita la autenticación

Complete estos pasos:

1. Publique el comando del **set authentication enable local enable** para aseegurarse que hay una entrada posterior adentro si el servidor está abajo.
2. Publique el **comando set authentication enable tacacs enable** para decir el Switch enviar los pedidos de activación al servidor.

Paso I – Autenticación de habilitación RADIUS

Agregue estos comandos para conseguir el Switch para enviar el nombre de usuario `$enab15$ al` servidor de RADIUS. No todos los servidores de RADIUS soportan esta clase de un nombre de usuario. Vea el paso E para otra alternativa, por ejemplo, si usted fija un [RADIUS attribute 6 - to Administrative] del tipo de servicio, que inicia a los usuarios individuales en el enable mode.

1. Publique el comando del **set authentication enable local enable** para aseegurarse allí es una entrada posterior adentro si el servidor está abajo.
2. Publique el comando del **set authentication enable radius enable** para decir el Switch enviar los pedidos de activación al servidor si su servidor de RADIUS soporta el nombre de usuario $enab15$.

Paso J - Habilitar autorización TACACS+

La adición de este comando da lugar al Switch que envía el permiso al servidor cuando el usuario intenta habilitar. El servidor necesita tener el **comando enable** permitido. En este ejemplo, hay una Conmutación por falla a ningunos en el evento que el servidor está abajo:

set author enable enable tacacs+ none both

Paso K: autenticación de Kerberos

Refiera a controlar y a monitorear el acceso al Switch usando la autenticación, la autorización, y explicar más información sobre cómo configurar el Kerberos al Switch.

Recuperación de contraseña

Refiera a los procedimientos para recuperación de contraseña para más información sobre los procedimientos para recuperación de contraseña.

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

Comandos ip permit para seguridad adicional

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

set ip permit enable telnet

fije la *máscara del rango del* **permiso del IP|***host*

Esto permite solamente el rango o los host especificados a Telnet en el Switch.

Depuración en Catalyst

Antes de habilitar el debugging en el Catalyst, marque los registros del servidor por las razones del error. Esto es más fácil y menos perturbador al Switch. En versiones del switch anteriores, el **debug** fue realizado en el modo de ingeniería. No es necesario acceder al modo de ingeniería para ejecutar los **comandos debug** en versiones del código posteriores:

fije los tacacs de la traza|radius|Kerberos 4

Nota: Los tacacs de la traza del conjunto|radius|el comando 0 del Kerberos vuelve el Catalyst al modo del ninguno-seguimiento.

Refiera a la Página de soprte del producto del Switches para más información sobre los switches de LAN multicapas.

Información Relacionada

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