Configuración de la configuración de ejecución completa para usuarios con niveles de privilegio bajos

Contenido

Introducción

Este documento describe el proceso de configuración para mostrar la configuración de ejecución completa para los usuarios con niveles de privilegio bajos.

Prerequisites

Requirements

Se requiere una comprensión básica de los niveles de privilegio de Cisco para comprender este documento. La información básica es suficiente para explicar la comprensión de los niveles de privilegio requeridos.

Componentes Utilizados

Los componentes utilizados para los ejemplos de configuración de este documento eran ASR1006, pero cualquier dispositivo Cisco IOS® o Cisco IOS XE funciona de forma similar.

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

Este documento describe los pasos de configuración sobre cómo mostrar la configuración de ejecución completa para los usuarios que iniciaron sesión en el router con niveles de privilegio bajos. Para comprender el siguiente problema y la siguiente solución alternativa, es necesario comprender los niveles de privilegio. Los niveles de privilegio disponibles oscilan entre 0 y 15, y permiten al administrador personalizar los comandos que están disponibles en cada nivel de privilegio. De forma predeterminada, los tres niveles de privilegio en un router son:

- Nivel 0: sólo incluye comandos básicos (deshabilitar, habilitar, salir, ayudar y cerrar sesión)
- Nivel 1: incluye todos los comandos disponibles en el modo de comandos EXEC de usuario
- Nivel 15: incluye todos los comandos disponibles en el modo de comando EXEC privilegiado

Los niveles restantes entre estos niveles mínimo y máximo no están definidos hasta que el administrador les asigne comandos o usuarios. Por lo tanto, el administrador puede asignar a los usuarios diferentes niveles de privilegio entre estos niveles de privilegio mínimo y máximo para separar a qué tienen acceso los diferentes usuarios. El administrador puede asignar comandos individuales (y varias otras opciones) a un nivel de privilegio individual para que este esté disponible para cualquier usuario de este nivel. Por ejemplo:

```
Router(config)# username user1 privilege 7 password P@ssw0rD1
Router(config)# privilege exec level 7 show access-lists
```

Con esta configuración, cuando el usuario 1 se conecta al router, puede ejecutar el show access-lists y/o cualquier otra cosa habilitada en ese nivel de privilegio. Sin embargo, no se puede decir lo mismo para habilitar el show running-config , como se explica más adelante en la instrucción del problema.

Problema de configuración

Al configurar diferentes niveles de acceso al router para diferentes usuarios, es una aplicación común que un administrador de red intente asignar determinados usuarios para que solo tengan acceso a show y no proporcionar acceso a ningún configuration comandos. Esta es una tarea sencilla para la mayoría show , ya que puede otorgar acceso a través de una configuración simple según lo siguiente:

```
Router(config)# username test_user privilege 10 password testP@ssw0rD
Router(config)# privilege exec level 10 show
Router(config)# privilege exec level 10 show running-config
```

Con este ejemplo de configuración, la segunda línea puede permitir el test_user para tener acceso a una plétora de comandos relacionados con show, que normalmente no están disponibles en este nivel de privilegio. Sin embargo, el show running-config se trata de manera diferente a la mayoría de los comandos show. Incluso con la tercera línea de código de ejemplo, sólo un código omitido o

abreviado `show running-config` se muestra para el usuario a pesar de que el comando se haya especificado en el nivel de privilegio correcto.

```
User Access Verification

Username: test_user
 Password:
 Router#
 Router#show privilege
 Current privilege level is 10
 Router#
 Router#show running-config
 Building configuration...

Current configuration : 121 bytes
 !
 ! Last configuration change at 21:10:08 UTC Mon Aug 28 2017
 !
 boot-start-marker
 boot-end-marker
 !
 !
 !
 end

Router#
```

Como puede ver, este resultado no muestra ninguna configuración y no sería útil para un usuario que intenta recopilar información sobre la configuración del router. Esto se debe a que el `show running-config` muestra todos los comandos que el usuario puede modificar en su nivel de privilegio actual. Se ha diseñado como una configuración de seguridad para evitar que el usuario tenga acceso a comandos que se han configurado previamente desde su nivel de privilegio actual. Esto es un problema cuando se intenta crear un usuario con acceso a los comandos show, como `show running-config` es un comando estándar que los ingenieros deben recopilar inicialmente al solucionar problemas.

Solución de configuración y verificación

Como solución a este dilema, existe otra versión de la tradicional `show run` que omite esta limitación del comando.

```
Router(config)# show running-config view full
 Router(config)# privilege exec level 10 show running-config view full
```

La adición de `view full` al comando (y, a su vez, el nivel de privilegio del comando para permitir al usuario el acceso al comando), ahora permite al usuario ver el `show running-config` sin comandos omitidos.

```
Username: test_user
 Password:
 Router#
 Router#show privilege
 Current privilege level is 10
 Router#
 Router#show running-config view full

Building configuration...

Current configuration : 2664 bytes
 !
 ! Last configuration change at 21:25:45 UTC Mon Aug 28 2017
 !
 version 15.4
 service timestamps debug datetime msec
 service timestamps log datetime msec
 no platform punt-keepalive disable-kernel-core
 !
 hostname Router
 !
 boot-start-marker
 boot system flash bootflash:packages.conf
 boot system flash bootflash:asr1000rp1-adventerprisek9.03.13.06a.S.154-3.S6a-ext.bin
 boot-end-marker
 !
 vrf definition Mgmt-intf
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
 !
 enable password <omitted>
 !
 no aaa new-model
 !
 no ip domain lookup
 !
 subscriber templating
 !
 multilink bundle-name authenticated
 !
 spanning-tree extend system-id
 !
 username test_user privilege 10 password 0 testP@ssw0rD
 !
 redundancy
  mode sso
 !
 cdp run
 !
 interface GigabitEthernet0/2/0
  no ip address
  shutdown
  negotiation auto
 !
 interface GigabitEthernet0/2/1
  no ip address
  shutdown
```

```
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address <omitted>
 negotiation auto
 cdp enable
!
ip forward-protocol nd
!
control-plane
!
!
privilege exec level 10 show running-config view full
alias exec show-running-config show running-config view full
!
line con 0
 stopbits 1
line aux 0
 exec-timeout 0 1
 no exec
 transport output none
 stopbits 1
line vty 0 4
login local
!
end
Router#
```

Sin embargo, esto plantea la pregunta, al proporcionar al usuario acceso a esta versión del comando, ¿no plantea esto el riesgo de seguridad inicial que intentaba resolverse diseñando una versión omitida?

Como solución alternativa a la solución y para garantizar la coherencia en un diseño de red seguro, puede crear un alias para el usuario que ejecute la versión completa de `show running-config` sin proporcionar acceso/conocimiento al usuario, como se muestra aquí:

```
Router(config)# alias exec show-running-config show running-config view full
```

En este ejemplo, el `show running-config` es el nombre de alias y, cuando el usuario inicia sesión en el router, puede introducir este nombre de alias en lugar del comando y recibir el resultado esperado sin conocer el comando real que se está ejecutando.

Nota: A partir de la versión 16.X, dependiendo de la plataforma, también es necesario agregar permisos a los archivos mediante el comando (config)#file privilege <level>.

Conclusión

En conclusión, este es solo un ejemplo de cómo tener más control al crear administrativamente el

acceso de privilegios de usuario en diferentes niveles. Hay una plétora de opciones para crear varios niveles de privilegio y acceso a diferentes comandos, y este es un ejemplo de cómo asegurar que un usuario de show only todavía tenga acceso a la configuración de ejecución completa cuando no tiene acceso a ningún comando de configuración.

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).