Control de acceso basado en roles de Cisco IOS con SDM: Separación del permiso de configuración entre grupos operativos

Contenido

Introducción

La funcionalidad de routing y seguridad se admite tradicionalmente en dispositivos independientes, lo que ofrece una clara división de la responsabilidad de gestión entre la infraestructura de red y los servicios de seguridad. La convergencia de la seguridad y la funcionalidad de routing en los routers de servicios integrados de Cisco no ofrece esta separación clara y multidispositivo. Algunas organizaciones necesitan una separación de las funciones de configuración para restringir a los clientes o a los grupos de gestión de servicios según los límites funcionales. Las vistas de CLI, una función de software de Cisco IOS®, buscan satisfacer esta necesidad con acceso CLI basado en roles. Este documento describe la configuración definida por el soporte de SDM del Control de Acceso Basado en Rol de Cisco IOS y ofrece información general sobre las capacidades de las Vistas CLI desde la Interfaz de Línea de Comandos de Cisco IOS.

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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Muchas organizaciones delegan la responsabilidad del mantenimiento del routing y la conectividad de la infraestructura en un grupo de operaciones de red, así como la responsabilidad del mantenimiento de la funcionalidad de firewall, VPN y prevención de intrusiones en un grupo de operaciones de seguridad. Las vistas de CLI pueden restringir la capacidad de supervisión y configuración de la funcionalidad de seguridad al grupo secops y, a la inversa, restringir la conectividad de red, el routing y otras tareas de infraestructura al grupo netops.

Algunos proveedores de servicios desean ofrecer a los clientes una capacidad de configuración o supervisión limitada, pero no permitir que los clientes configuren o vean otros ajustes de dispositivos. Una vez más, las vistas de CLI ofrecen un control granular sobre la capacidad de CLI para restringir a los usuarios o a los grupos de usuarios a ejecutar sólo comandos autorizados.

El software Cisco IOS ha ofrecido la capacidad de restringir los comandos CLI con un servidor TACACS+ para obtener autorización para permitir o denegar la capacidad de ejecutar comandos CLI basados en el nombre de usuario o la pertenencia al grupo de usuarios. Las vistas CLI ofrecen una capacidad similar, pero el control de políticas lo aplica el dispositivo local después de que se reciba la vista especificada del usuario del servidor AAA. Cuando se utiliza la Autorización de Comando AAA, cada comando debe ser autorizado individualmente por el servidor AAA, lo que causa un diálogo frecuente entre el dispositivo y el servidor AAA. Las vistas CLI permiten el control de políticas CLI por dispositivo, mientras que la autorización de comandos AAA aplica la misma política de autorización de comandos a todos los dispositivos a los que accede un usuario.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Asociar usuarios con una vista

Los usuarios se pueden asociar a una vista CLI local mediante un atributo return de AAA o en la configuración de autenticación local. Para la configuración local, el nombre de usuario se configura con una opción **view** adicional, que coincide con el **nombre** de **vista del analizador**. Estos usuarios de ejemplo se configuran para las vistas SDM predeterminadas:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Los usuarios asignados a una vista determinada pueden cambiar temporalmente a otra si tienen la contraseña para la vista que desean introducir. Ejecute este comando exec para cambiar las vistas:

```
enable view view-name
```

Configuración de Vista de analizador

Las vistas CLI se pueden configurar desde la CLI del router o a través de SDM. SDM proporciona soporte estático para cuatro vistas, como se describe en la sección Soporte de Vistas CLI de SDM. Para configurar la Vista CLI desde la Interfaz de línea de comandos, un usuario debe definirse como un usuario de vista **raíz** o debe pertenecer a la vista con acceso a la configuración de la **vista del analizador**. Los usuarios que no están asociados a una vista y que intentan configurar vistas reciben este mensaje:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

Las vistas de CLI permiten la inclusión o exclusión de jerarquías de comandos completas para los modos ejecutivo y de configuración, o sólo partes de ellas. Hay tres opciones disponibles para permitir o rechazar una jerarquía de comandos o comandos en una vista dada:

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

Las vistas de CLI truncan la configuración en ejecución para que no se muestre la configuración de Vista del analizador. Sin embargo, la configuración de Vista del analizador está visible en la configuración de inicio.

Consulte Acceso CLI basado en roles para obtener más información sobre la definición de vista.

Verificación de la Asociación de la Vista de Parser

Los usuarios asignados a una Vista de analizador pueden determinar a qué vista se asignan cuando inician sesión en un router. Si se permite el comando **show parser view** para las vistas de los usuarios, pueden ejecutar el comando **show parser view** para determinar su vista:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

Compatibilidad con vistas CLI de SDM

SDM ofrece tres vistas predeterminadas, dos para la configuración y supervisión de los componentes de firewall y VPN y una vista de solo supervisión restringida. Una vista **raíz** predeterminada adicional también está disponible en SDM.

SDM no proporciona la capacidad de modificar los comandos incluidos o excluidos de cada vista predeterminada, y no ofrece la capacidad de definir vistas adicionales. Si se definen vistas adicionales desde la CLI, SDM no ofrece las vistas adicionales en su panel de configuración **Cuentas de usuario/Vistas**.

Estas vistas y los permisos de comandos respectivos están predefinidos para SDM:

SDM_Firewall View

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
```

```
 commands configure include all no ip inspect
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

SDM_EasyVPN_Remote View

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
 commands configure include default ip dns server
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
```

```
 commands configure include default identity
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Vista SDM_Monitor

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
 commands configure include no end
 commands configure include all no interface
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include all crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include all ping ip
 commands exec include ping
```

```
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Acceso CLI Basado en Función
- Soporte Técnico y Documentación - Cisco Systems