Controle de acesso baseado em função do Cisco IOS com SDM: Separação da permissão de configuração entre grupos operacionais

Contents

Introduction

A funcionalidade de roteamento e segurança é tradicionalmente suportada em dispositivos separados, o que oferece uma divisão clara da responsabilidade de gerenciamento entre a infraestrutura de rede e os serviços de segurança. A convergência da funcionalidade de segurança e roteamento nos Cisco Integrated Services Routers não oferece essa separação clara e multidispositivo. Algumas organizações precisam de uma segregação na capacidade de configuração para restringir clientes ou grupos de gerenciamento de serviços ao longo de limites funcionais. O CLI Views, um recurso do software Cisco IOS®, procura atender a essa necessidade com o Role-Based CLI Access. Este documento descreve a configuração definida pelo suporte SDM do Cisco IOS Role-Based Access Control e oferece um plano de fundo sobre os recursos de CLI Views a partir da interface de linha de comando do Cisco IOS.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Muitas organizações delegam a responsabilidade pela manutenção do roteamento e da conectividade infraestrutural em um grupo de operações de rede e a responsabilidade pela manutenção do firewall, VPN e da funcionalidade de prevenção de invasão em um grupo de operações de segurança. As exibições de CLI podem restringir a configuração da funcionalidade de segurança e a capacidade de monitoramento ao grupo secops e, inversamente, restringir a conectividade de rede, o roteamento e outras tarefas de infraestrutura ao grupo netops.

Alguns provedores de serviços desejam oferecer aos clientes capacidade limitada de configuração ou monitoramento, mas não permitem que os clientes configurem ou visualizem outras configurações de dispositivo. Mais uma vez, as exibições CLI oferecem controle granular sobre o recurso CLI para restringir usuários ou grupos de usuários a executar somente comandos autorizados.

O software Cisco IOS ofereceu um recurso para restringir comandos CLI com um servidor TACACS+ para autorização para permitir ou negar a capacidade de executar comandos CLI com base no nome de usuário ou na associação do grupo de usuários. As exibições de CLI oferecem recursos semelhantes, mas o controle de política é aplicado pelo dispositivo local depois que a exibição especificada do usuário é recebida do servidor AAA. Quando AAA Command Authorization é usado, cada comando deve ser autorizado individualmente pelo servidor AAA, o que causa um diálogo frequente entre o dispositivo e o servidor AAA. As exibições de CLI permitem o controle de política de CLI por dispositivo, enquanto a autorização de comando AAA aplica a mesma política de autorização de comando a todos os dispositivos acessados por um usuário.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Associar usuários a uma exibição

Os usuários podem ser associados a uma exibição CLI local por um atributo return da AAA ou na configuração de autenticação local. Para a configuração local, o nome de usuário é configurado com uma opção de **visualização** adicional, que corresponde ao nome de **visualização do analisador** configurado. Estes usuários de exemplo estão configurados para as exibições SDM padrão:

```
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
```

Os usuários atribuídos a uma determinada exibição podem alternar temporariamente para outra exibição se tiverem a senha para a exibição que desejam inserir. Execute este comando exec para alterar as exibições:

```
enable view view-name
```

Configuração do modo de exibição do analisador

As exibições CLI podem ser configuradas na CLI do roteador ou através do SDM. O SDM oferece suporte estático para quatro visualizações, conforme discutido na seção Suporte a exibições CLI do SDM. Para configurar o modo de exibição CLI na interface de linha de comando, um usuário deve ser definido como um usuário **root** view ou deve pertencer ao modo de exibição com acesso à configuração **parser view**. Os usuários que não estão associados a uma exibição e que tentam configurá-la recebem esta mensagem:

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

As exibições de CLI permitem a inclusão ou exclusão de hierarquias completas de comandos para os modos executivo e de configuração, ou apenas partes delas. Três opções estão disponíveis para permitir ou não permitir um comando ou hierarquia de comandos em uma determinada exibição:

```
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
```

As exibições de CLI truncam a configuração atual para que a configuração da exibição do analisador não seja exibida. No entanto, a configuração do Parser View é visível na configuração de inicialização.

Consulte Acesso CLI Baseado em Função para obter mais informações sobre a definição de exibição.

Verificando a associação de exibição do analisador

Os usuários atribuídos a uma exibição de analisador podem determinar a qual exibição estão atribuídos quando estão conectados a um roteador. Se o comando **show parser view** for permitido para as exibições dos usuários, eles poderão emitir o comando **show parser view** para determinar sua exibição:

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

Suporte a exibições CLI SDM

O SDM oferece três visualizações padrão, duas para configuração e monitoramento de componentes de firewall e VPN e uma visualização restrita somente de monitoramento. Uma exibição **raiz** padrão adicional também está disponível no SDM.

O SDM não oferece a capacidade de modificar os comandos incluídos ou excluídos de cada visualização padrão e não oferece a capacidade de definir exibições adicionais. Se visualizações adicionais forem definidas na CLI, o SDM não oferecerá as visualizações adicionais no painel de configuração **Contas de usuário/Visualizações**.

Essas exibições e respectivas permissões de comando são predefinidas para SDM:

Exibição de SDM_Firewall

```
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
```

Exibição SDM_EasyVPN_Remote

```
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
```

Exibição de 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Acesso CLI baseado em função
- Suporte Técnico e Documentação - Cisco Systems