O Cisco IOS Papel-baseou o controle de acesso com SDM: Separando a permissão da configuração entre grupos operacionais

Índice

Introdução

A funcionalidade do roteamento e da Segurança é apoiada tradicionalmente nos dispositivos separados, que oferece uma divisão clara da responsabilidade de gerenciamento entre o infraestrutura de comunicação de rede e os Serviços de segurança. A convergência da Segurança e da funcionalidade de roteamento no Roteadores dos Serviços integrados de Cisco não oferece este claro, separação do multi-dispositivo. Algumas organizações precisam uma segregação da capacidade da configuração de restringir clientes ou grupos de gerenciamento do serviço ao longo dos limites funcionais. As opiniões CLI, uns recursos de software de Cisco IOS®, procuram endereçar esta necessidade com acesso Papel-baseado CLI. Este documento descreve a configuração definida pelo apoio SDM do controle de acesso Papel-baseado Cisco IOS, e oferece o fundo nas capacidades de opiniões CLI da interface de linha de comando do Cisco IOS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

Muitas organizações delegam a responsabilidade para a manutenção do roteamento e da Conectividade infraestrutural a um grupo de operações de rede, e a responsabilidade para a manutenção do Firewall, do VPN, e da funcionalidade da prevenção de intrusão a um grupo de operações da Segurança. As opiniões CLI podem restringir a configuração e a potencialidade de monitoramento da funcionalidade da Segurança ao grupo dos secops, e restringem inversamente a conectividade de rede, o roteamento, e outras tarefas infraestruturais ao grupo dos netops.

Alguns provedores de serviços querem oferecer capacidade limitada da configuração ou da monitoração aos clientes, mas não permitir que os clientes configurem ou ver ajustes do outro dispositivo. Mais uma vez, as opiniões CLI oferecem o controle granulado sobre a capacidade CLI de restringir usuários ou grupos de usuário para executar somente comandos autorizados.

O Cisco IOS Software ofereceu uma capacidade de restringir comandos CLI com um servidor para autorização TACACS+ à capacidade do permit or deny de executar os comandos CLI baseados na sociedade username ou de grupo de usuário. As opiniões CLI oferecem a capacidade similar, mas o controle de política está aplicado pelo dispositivo local depois que a opinião especificada o usuário é recebida do servidor AAA. Quando a autorização do comando aaa é usada, cada comando deve individualmente ser autorizado pelo servidor AAA, que causa o diálogo frequente entre o dispositivo e o servidor AAA. As opiniões CLI permitem o controle de política do por-dispositivo CLI, visto que a autorização do comando aaa aplica a mesma política do comando authorization a todos os dispositivos acessos de 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.

Associe usuários com uma vista

Os usuários podem ser associados com uma opinião local CLI por um atributo do retorno do AAA ou na configuração da autenticação local. Para a configuração local, o username é configurado com uma opção adicional da **vista**, que combine o **nome de visualização** configurado do **parser**. Estes usuários do exemplo são configurados para as opiniões do padrão SDM:

```
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 que são atribuídos a uma vista dada podem temporariamente comutar a uma outra vista se têm a senha para a vista que querem incorporar. Emita este comando exec a fim mudar vistas:

```
enable view view-name
```

Configuração da opinião do Parser

As opiniões CLI podem ser configuradas do roteador CLI, ou com o SDM. O SDM fornece o apoio estático para quatro vistas, como discutido na seção de suporte das opiniões SDM CLI. A fim configurar a opinião CLI da interface de linha de comando, um usuário deve ser definido como um usuário da opinião da **raiz**, ou devem pertencer para ver com o acesso à configuração da **opinião do parser**. Os usuários que não são associados com uma vista e que tentam configurar vistas recebem esta mensagem:

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

As opiniões CLI permitem a inclusão ou a exclusão de hierarquias do comando complete para o executivo e os modos de configuração, ou somente as parcelas disso. Três opções estão disponíveis permitir ou recusar um comando ou uma hierarquia do comando em uma 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
```

As opiniões CLI truncam a executar-configuração assim que a configuração da opinião do Parser não é indicada. Contudo, a configuração da opinião do Parser é visível na partida-configuração.

Consulte o acesso Papel-baseado CLI para obter mais informações sobre da definição da vista.

Verificando a associação da opinião do Parser

Os usuários que são atribuídos a uma opinião do Parser podem determinar que vista estão atribuídos quando são entrados a um roteador. Se é permitido ao **comando view do parser da mostra as** opiniões de usuários, podem emitir o **comando view do parser da mostra** a fim determinar sua opinião:

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

Apoio das opiniões SDM CLI

O SDM oferece três visualizações padrão, dois para a configuração e a monitoração do Firewall e dos componentes VPN, e uma opinião restringida da monitoração-somente. Uma opinião adicional da **raiz do** padrão está disponível no SDM também.

O SDM não fornece a capacidade para alterar os comandos incluídos dentro ou excluídos de cada visualização padrão, e não oferece nenhuma capacidade de definir vistas adicionais. Se as vistas adicionais são definidas do CLI, o SDM não oferece as vistas adicionais painel na sua configuração das **contas de usuário/vistas**.

Estas vistas e permissões respectivas do comando são predefinidas para o SDM:

Opinião 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
```

Opinião de 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
```

Opinião 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.

Troubleshooting

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

Informações Relacionadas

- Acesso Papel-baseado CLI
- Suporte Técnico e Documentação - Cisco Systems