带有SDM的Cisco IOS基于任务的访问控制：可操作组之间的配置权限分离

目录

简介

独立设备传统上支持路由和安全功能，提供管理职责一清楚划分在网络基础设施和安全服务之间的。安全和路由功能收敛在思科集成服务路由器不提供此清楚，多设备的分离。一些组织需要配置功能的隔离限制客户或服务管理群沿功能限定范围。CLI视图， Cisco IOS软件特性，寻求针对与基于任务的CLI访问的此需要。本文描述Cisco IOS基于任务的访问控制SDM支持定义的配置，并且提供背景到CLI视图的功能从Cisco IOS命令行界面的。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

许多组织委派对路由和基础建设的连接维护的对防火墙、VPN和入侵防御功能维护的责任给网络操作组和责任对安全操作组。CLI视图能限制安全功能配置和监视功能对secops组和相反地限制网络连通性、路由和其他基础建设的任务给netops组。

一些服务提供商要提供受限的配置或监听能力对客户，但是不允许客户配置或查看其它设备设置。再次， CLI视图提供对CLI功能的粒状控制限制用户或用户组执行仅已授权命令。

Cisco IOS软件提供功能限制CLI命令用授权的一个TACACS+服务器能允许或拒绝功能执行根据用户名或用户组会员的CLI命令。CLI视图提供相似的功能，但是策略控制由本地设备应用，在指定的观点的用户从AAA服务器后接收。当使用时aaa命令授权，必须由AAA服务器单个授权每命令，导致在设备和AAA服务器之间的常见的对话。CLI视图允许每台设备CLI策略控制，而aaa命令授权适用于同一项authorization命令策略所有的设备用户访问。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

连结用户与视图

用户可以关联与本地CLI视图由回归属性从AAA或在本地认证配置方面。对于本地配置，用户名配置与一另外的**查看选项卡**，匹配已配置的**parser view**名称。这些示例用户为默认SDM视图配置：

```
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
```

分配到一张给的视图的用户能临时地换成另一张视图他们是否有他们要参与的视图的密码。发出此exec命令为了更改视图：

```
enable view view-name
```

Parser view配置

CLI视图可以配置从路由器CLI，或者通过SDM。SDM为四张视图提供静态支持，如SDM CLI视图支持部分所述。为了配置从命令行界面的CLI视图，用户必须定义作为**根**视图用户，或者他们必须属于查看与对**parser view**配置的访问。没有关联与视图，并且设法配置视图的用户收到此消息：

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

CLI视图允许完整命令层级包括或排除高级管理和因此仅配置模式或者部分。三个选项是可用允许或禁止一命令或命令层级在一张给的视图：

```
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
```

CLI视图削running-config，因此Parser view配置没有显示。然而， Parser view配置是可视在startup-config。

参考基于任务的CLI访问关于视图定义的更多信息。

正在验证的Parser view关联

分配到Parser view的用户能确定哪张视图他们分配到，当他们登陆到路由器时。如果**show parser view**命令为用户意见允许，他们能发出**show parser view**命令为了确定他们的意图：

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

SDM CLI视图支持

SDM提供三个默认视图，两防火墙和VPN组件配置和监视的和一张限制的监听视图。一个另外的默认**根**视图是可用的在SDM。

SDM不提供能力修改从每个默认视图包括或排除的命令，并且不提供功能定义另外的视图。如果另外的视图从CLI定义， SDM在其**用户帐户/视图**配置方面不提供另外的视图面板。

这些视图和各自命令权限为SDM预定义：

SDM_Firewall视图

```
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视图

```
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
```

SDM_Monitor视图

```
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
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 基于任务的CLI访问
- 技术支持和文档 - Cisco Systems