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

传统上，路由和安全功能在单独的设备中受支持，这在网络基础设施和安全服务之间明确划分了管理职责。思科集成多业务路由器中安全和路由功能的融合无法提供这种清晰的多设备分离。某些组织需要分离配置功能，以限制客户或服务管理组沿职能边界。CLI视图是Cisco IOS®软件的一项功能，旨在通过基于角色的CLI访问来满足这一需求。本文档介绍SDM对Cisco IOS基于角色的访问控制的支持所定义的配置，并提供了Cisco IOS命令行界面中CLI视图功能的背景信息。

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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

许多组织将维护路由和基础设施连接的责任委托给网络运营组，并将维护防火墙、VPN和入侵防御功能的责任委托给安全运营组。CLI视图可以限制安全功能配置和监控功能到secops组，反之，可以限制网络连接、路由和其他基础设施任务到netops组。

有些服务提供商希望为客户提供有限的配置或监控功能，但不允许客户配置或查看其他设备设置。CLI视图再次提供对CLI功能的精细控制，以限制用户或用户组仅执行授权命令。

Cisco IOS软件提供了通过TACACS+服务器限制CLI命令的功能，以授权允许或拒绝基于用户名或用户组成员身份执行CLI命令的功能。CLI视图提供类似的功能，但在从AAA服务器收到用户的指定视图后，本地设备会应用策略控制。当使用AAA命令授权时，每个命令必须由AAA服务器单独授权，这会导致设备与AAA服务器之间频繁对话。CLI视图允许按设备进行CLI策略控制，而AAA命令授权将相同的命令授权策略应用于用户访问的所有设备。

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(仅限注册客户)可获取有关本节中使用的命令的详细信息。

将用户与视图关联

用户可以通过AAA或本地身份验证配置中的返回属性与本地CLI视图关联。对于本地配置，用户名配置有附加的**查看**选项，该选项与已配置的解析**器视图**名称匹配。以下示例用户配置了默认SDM视图：

```
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
```

如果分配给给定视图的用户具有要输入的视图的密码，则他们可以临时切换到另一个视图。发出以下exec命令以更改视图：

```
enable view view-name
```

解析器视图配置

CLI视图可以从路由器CLI或通过SDM进行配置。SDM为四个视图提供静态支持，如SDM CLI视图支持部分中所述。要从命令行界面配置CLI视图，用户必须定义为根视图**用户**，或者用户必须属于具有解析器视图配置访问权限**的视**图。未与视图关联且尝试配置视图的用户会收到以下消息：

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

CLI视图允许执行和配置模式或仅允许其部分包含或排除完整的命令层次结构。在给定视图中允许或禁止命令或命令层次结构的选项有三个：

```
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视图截断运行配置，因此不显示解析器视图配置。但是，在启动配置中可以看到解析器视图配置。

有关视图定义的详细信息，请参阅基于角色的CLI访问。

验证解析器视图关联

分配给解析器视图的用户可以确定在登录到路由器时分配到哪个视图。如果允**许用户**视图使用show parser view命令，则他们可以发出**show parser view命**令以确定其视图：

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

SDM CLI视图支持

SDM提供三个默认视图，两个用于配置和监控防火墙和VPN组件，另一个用于受限监控的视图。SDM中还**提供**了另一个默认根视图。

SDM不能修改每个默认视图中包含或排除的命令，也无法定义其他视图。如果从CLI定义了其他视图，SDM不会在其“用户帐户/视图”配置面**板中提供其他**视图。

为SDM预定义了以下视图和相应的命令权限：

SDM_防火墙视图

```
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

- 基于角色的CLI访问
- 技术支持和文档 - Cisco Systems