採用SDM的Cisco IOS角色型存取控制：在操作組之間分離配置許可權

目錄

簡介

傳統上，路由和安全功能由單獨的裝置支援，在網路基礎設施和安全服務之間明確劃分管理責任。思科整合多業務路由器中安全性和路由功能的融合無法提供這種清晰的多裝置分離。某些組織需要隔離配置功能，以沿功能邊界限制客戶或服務管理組。CLI檢視是Cisco IOS®軟體的一項功能，旨在通過基於角色的CLI訪問來滿足這一需求。本文檔介紹由SDM對Cisco IOS基於角色的訪問控制的支援所定義的配置，並提供從Cisco IOS命令列介面瞭解CLI檢視功能的背景資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

許多組織將維護路由和基礎設施連線的責任委託給網路操作組，將維護防火牆、VPN和入侵防禦功能的責任委託給安全操作組。CLI檢視可以將安全功能配置和監控功能限製為secops組，反之將網路連線、路由和其他基礎架構任務限製為netops組。

一些服務提供商希望為客戶提供有限的配置或監控能力，但不允許客戶配置或檢視其他裝置設定。同樣，CLI檢視提供了對CLI功能的精細控制，以限制使用者或使用者組僅執行授權命令。

Cisco IOS軟體提供了使用TACACS+伺服器限制CLI命令的功能，用於根據使用者名稱或使用者組成員身份來授權允許或拒絕執行CLI命令。CLI檢視提供類似的功能，但本地裝置在從AAA伺服器收到使用者的指定檢視後應用策略控制。使用AAA命令授權時，每個命令都必須由AAA伺服器單獨授權，這會導致裝置與AAA伺服器之間頻繁對話。CLI檢視允許按裝置CLI策略控制，而AAA命令授權對使用者訪問的所有裝置應用相同的命令授權策略。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

將使用者與檢視關聯

使用者可通過來自AAA的返回屬性或在本地身份驗證配置中與本地CLI檢視關聯。對於本地配置，使用者名稱配置有附加的**view**選項，該選項與配置的分析器視**圖名稱**匹配。這些示例使用者配置為使用預設的SDM檢視：

```
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
```

如果分配給給定檢視的使用者具有要輸入的檢視的密碼，他們可以臨時切換到另一個檢視。發出此exec命令以變更檢視：

```
enable view view-name
```

分析器檢視配置

可以從路由器CLI或通過SDM配置CLI檢視。SDM為四個檢視提供靜態支援，如SDM CLI檢視支援一節所述。要從命令列介面配置CLI檢視，必須將使用者定義為**root檢視用**戶，或者他們必須屬於有權訪問分析器檢視配置的**視**圖。未與檢視關聯且試圖配置檢視的使用者將收到以下消息：

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

CLI檢視允許在執行模式和配置模式下包含或排除完整的命令層次結構，或僅包含其中的部分。在給定檢視中，有三個選項可用於允許或禁止命令或命令層次結構：

```
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檢視截斷running-config，因此不顯示Parser View配置。但是，Parser View配置在啟動配置中可見。

有關檢視定義的詳細資訊，請參閱基於角色的CLI訪問。

驗證分析器檢視關聯

被分配到Parser View的使用者可以確定登入到路由器時分配給哪個檢視。如果對使用者檢視允許**show parser view**命令，則使用者可以發出**show parser view**命令以確定其檢視：

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

SDM CLI檢視支援

SDM提供三個預設檢視，其中兩個用於配置和監控防火牆和VPN元件，另一個是受限制的僅監控檢視。SDM中還提供了附加的預設**根檢視**。

SDM不提供修改包括在每個預設檢視中或從每個預設檢視中排除的命令的功能，也不提供定義其他檢視的功能。如果從CLI定義了其他檢視，則SDM不會在其**User Accounts/Views**（使用者帳戶/檢視）配置面板中提供其他檢視。

這些檢視和相應的命令許可權是為SDM預定義的：

SDM_防火牆檢視

```
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檢視

```
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檢視

```
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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 基於角色的CLI訪問
- 技術支援與文件 - Cisco Systems