SDM을 통한 Cisco IOS 역할 기반 액세스 제어: 운영 그룹 간 구성 권한 분리

목차

소개

라우팅 및 보안 기능은 일반적으로 별도의 디바이스에서 지원되며, 이는 네트워킹 인프라와 보안 서비스 간에 관리 책임을 명확히 분담합니다. Cisco Integrated Services Router의 보안 및 라우팅 기능이 통합되어도 이러한 명확한 다중 장치 분리는 제공되지 않습니다. 일부 조직에서는 기능별 경계를 따라 고객 또는 서비스 관리 그룹을 제한하기 위해 구성 기능을 분리해야 합니다. Cisco IOS® 소프트웨어 기능인 CLI 보기는 역할 기반 CLI 액세스로 이러한 요구 사항을 해결합니다. 이 문서에서는 Cisco IOS Role-Based Access Control의 SDM 지원에 의해 정의된 컨피그레이션에 대해 설명하며, Cisco IOS Command-Line Interface에서 CLI 뷰의 기능에 대한 배경을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

많은 조직이 라우팅 및 인프라 연결의 유지 관리를 네트워크 운영 그룹에 위임하고 방화벽, VPN 및 침입 방지 기능의 유지 관리를 보안 운영 그룹에 위임합니다. CLI 보기는 보안 기능 컨피그레이션 및 모니터링 기능을 secops 그룹으로 제한하고, 반대로 네트워크 연결, 라우팅 및 기타 인프라 작업을 netops 그룹으로 제한할 수 있습니다.

일부 통신 사업자는 고객에게 제한된 컨피그레이션 또는 모니터링 기능을 제공하기를 원하지만, 고객이 다른 디바이스 설정을 구성하거나 볼 수는 없습니다. 다시 한 번, CLI 보기는 CLI 기능을 세부적으로 제어하여 사용자 또는 사용자 그룹이 인증된 명령만 실행하도록 제한합니다.

Cisco IOS 소프트웨어는 사용자 이름 또는 사용자 그룹 멤버십에 따라 CLI 명령을 실행하는 권한을 허용하거나 거부할 수 있도록 TACACS+ 서버에서 CLI 명령을 제한하는 기능을 제공합니다. CLI 보기는 유사한 기능을 제공하지만 AAA 서버에서 사용자의 지정된 보기를 수신한 후 로컬 디바이스에 의해 정책 제어가 적용됩니다. AAA 명령 권한 부여를 사용할 경우 모든 명령은 AAA 서버에서 개별적으로 권한을 부여해야 합니다. 그러면 디바이스와 AAA 서버 간에 빈번하게 대화 상자가 발생합니다. CLI 보기는 디바이스별 CLI 정책 제어를 허용하는 반면 AAA 명령 권한 부여는 사용자가 액세스하는 모든 디바이스에 동일한 명령 권한 부여 정책을 적용합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

사용자와 보기 연결

사용자는 AAA 또는 로컬 인증 컨피그레이션의 반환 특성을 통해 로컬 CLI 보기에 연결할 수 있습니다. 로컬 컨피그레이션의 경우 사용자 이름은 구성된 **파서 보기** 이름과 일치하는 추가 **보기** 옵션으로 구성됩니다. 다음 예제 사용자는 기본 SDM 보기에 대해 구성됩니다.

```
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
```

지정된 보기에 할당된 사용자가 입력하려는 보기에 대한 암호가 있는 경우 일시적으로 다른 보기로 전환할 수 있습니다. 뷰를 변경하려면 다음 exec 명령을 실행합니다.

```
enable view view-name
```

파서 보기 구성

CLI 보기는 라우터 CLI 또는 SDM을 통해 구성할 수 있습니다. SDM은 SDM CLI Views Support 섹션에서 설명한 대로 네 가지 보기에 대한 정적 지원을 제공합니다. 명령줄 인터페이스에서 CLI 보기를 구성하려면 사용자를 **루트** 보기 사용자로 정의하거나 **파서 보기** 구성에 액세스할 수 있는 보기**에** 속해야 합니다. 보기에 연결되지 않은 사용자 및 보기를 구성하려고 하는 사용자는 다음 메시지를 받습니다.

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

CLI 보기를 사용하면 전체 및 컨피그레이션 모드 또는 그 부분만 포함하거나 제외할 수 있습니다. 지정된 보기에서 명령 또는 명령 계층 구조를 허용하거나 허용하지 않는 세 가지 옵션을 사용할 수 있습니다.

```
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 보기는 Parser View 컨피그레이션이 표시되지 않도록 running-config를 자릅니다. 그러나 Parser View 컨피그레이션은 startup-config에 표시됩니다.

보기 정의에 대한 자세한 내용은 역할 기반 CLI 액세스를 참조하십시오.

파서 보기 연결 확인

Parser View에 할당된 사용자는 라우터에 로그인할 때 할당된 보기를 결정할 수 있습니다. 사용자 보기에 대해 **show parser view** 명령을 사용할 수 있는 경우 **show parser view** 명령을 실행하여 해당 보기를 확인할 수 있습니다.

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

SDM CLI 보기 지원

SDM은 3개의 기본 보기를 제공하며, 2개는 방화벽 및 VPN 구성 요소의 구성 및 모니터링에 사용되며 1개는 제한된 모니터링 전용 보기를 제공합니다. SDM에서도 기본 **루트** 보기를 추가로 사용할 수 있습니다.

SDM은 각 기본 뷰에 포함되거나 제외되는 명령을 수정할 수 있는 기능을 제공하지 않으며 추가 보기를 정의할 수 있는 기능도 제공하지 않습니다. CLI에서 추가 보기를 정의하면 SDM은 **User Accounts/Views** 컨피그레이션 패널에서 추가 보기를 제공하지 않습니다.

다음 보기 및 각 명령 권한은 SDM에 대해 미리 정의되어 있습니다.

SDM_방화벽 보기

```
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 보기

```
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_모니터 보기

```
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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 역할 기반 CLI 액세스
- 기술 지원 및 문서 – Cisco Systems