Cisco IOS Rollenbasierte Zugriffskontrolle mit SDM: Trennen der Konfigurationsberechtigung zwischen betrieblichen Gruppen

Inhalt

Einführung

Routing- und Sicherheitsfunktionen werden in der Regel auf separaten Geräten unterstützt, wodurch die Verantwortlichkeit für das Management zwischen Netzwerkinfrastruktur und Sicherheitsservices klar aufgeteilt wird. Die Konvergenz von Sicherheits- und Routing-Funktionen der Cisco Integrated Services Router bietet keine klare Trennung mehrerer Geräte. Einige Unternehmen benötigen eine Trennung der Konfigurationsfunktionen, um Kunden oder Servicemanagement-Gruppen entlang funktionaler Grenzen zu beschränken. CLI Views, eine Funktion der Cisco IOS® Software, soll diese Anforderung mit rollenbasiertem CLI-Zugriff erfüllen. Dieses Dokument beschreibt die Konfiguration, die durch die SDM-Unterstützung der rollenbasierten Zugriffskontrolle von Cisco IOS definiert wurde, und bietet Hintergrundinformationen zu den Funktionen von CLI-Ansichten über die Cisco IOS-Befehlszeilenschnittstelle.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Viele Unternehmen delegieren die Verantwortung für die Wartung von Routing- und Infrastrukturverbindungen an eine Gruppe für den Netzwerkbetrieb und die Verantwortung für die Wartung von Firewall-, VPN- und Intrusion Prevention-Funktionen an eine Gruppe für Sicherheitsverfahren. CLI-Ansichten können die Konfiguration und Überwachung von Sicherheitsfunktionen auf die Secops-Gruppe beschränken und umgekehrt die Netzwerkverbindung, das Routing und andere Infrastrukturaufgaben auf die Netops-Gruppe beschränken.

Einige Service Provider möchten Kunden nur eingeschränkte Konfigurations- oder Überwachungsmöglichkeiten anbieten, Kunden jedoch nicht die Konfiguration oder Anzeige anderer Geräteeinstellungen erlauben. Auch hier bieten CLI-Ansichten eine präzise Kontrolle über CLI-Funktionen, um die Ausführung von nur autorisierten Befehlen durch Benutzer oder Benutzergruppen zu beschränken.

Die Cisco IOS-Software bietet die Möglichkeit, CLI-Befehle mit einem TACACS+-Server für die Autorisierung einzuschränken, um die Ausführung von CLI-Befehlen basierend auf dem Benutzernamen oder der Mitgliedschaft in einer Benutzergruppe zuzulassen oder zu verweigern. CLI-Ansichten bieten ähnliche Funktionen, aber die Richtlinienkontrolle wird vom lokalen Gerät angewendet, nachdem die angegebene Ansicht des Benutzers vom AAA-Server empfangen wurde. Bei Verwendung der AAA-Befehlsautorisierung muss jeder Befehl vom AAA-Server einzeln autorisiert werden, was zu häufigen Dialogen zwischen dem Gerät und dem AAA-Server führt. CLI-Ansichten ermöglichen die gerätebasierte Kontrolle von CLI-Richtlinien, während die AAA-Befehlsautorisierung für alle Geräte, auf die ein Benutzer zugreift, dieselbe Befehlsautorisierungsrichtlinie anwendet.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Zuordnen von Benutzern zu einer Ansicht

Benutzer können einer lokalen CLI-Ansicht durch ein Rückgabeattribut aus AAA oder in der Konfiguration für die lokale Authentifizierung zugeordnet werden. Für die lokale Konfiguration wird der Benutzername mit einer zusätzlichen **Ansicht**-Option konfiguriert, die mit dem konfigurierten Namen der **Parseransicht** übereinstimmt. Diese Beispielbenutzer sind für die Standard-SDM-Ansichten konfiguriert:

```
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
```

Benutzer, die einer bestimmten Ansicht zugewiesen sind, können vorübergehend zu einer anderen Ansicht wechseln, wenn sie das Kennwort für die Ansicht haben, die sie eingeben möchten. Geben Sie diesen exec-Befehl ein, um die Ansichten zu ändern:

```
enable view view-name
```

Konfiguration der Analyseansicht

CLI-Ansichten können über die Router-CLI oder über SDM konfiguriert werden. SDM bietet statische Unterstützung für vier Ansichten, wie im Abschnitt Support für SDM CLI-Ansichten beschrieben. Um die CLI-Ansicht über die Befehlszeilenschnittstelle zu konfigurieren, muss ein Benutzer als **Stammansichtsbenutzer** definiert werden oder sie müssen zur Ansicht mit Zugriff auf die Konfiguration der **Parser-Ansicht** gehören. Benutzer, die keiner Ansicht zugeordnet sind und versuchen, Ansichten zu konfigurieren, erhalten die folgende Meldung:

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

CLI-Ansichten ermöglichen das Einfügen oder Ausschließen vollständiger Befehlshierarchien für den Exekutive- und den Konfigurationsmodus oder nur für Teile davon. Es stehen drei Optionen zur Verfügung, um eine Befehls- oder Befehlshierarchie in einer bestimmten Ansicht zuzulassen oder zu untersagen:

```
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 Views schneiden die aktuelle Konfiguration ab, sodass die Parser View-Konfiguration nicht angezeigt wird. Die Parser View-Konfiguration ist jedoch in der Startup-Konfiguration sichtbar.

Weitere Informationen zur Anzeigedefinition finden Sie unter Rollenbasierter CLI-Zugriff.

Überprüfen der Zuordnung der Parseransicht

Benutzer, die einer Parser-Ansicht zugewiesen sind, können bestimmen, welcher Ansicht sie zugewiesen sind, wenn sie bei einem Router angemeldet sind. Wenn der Befehl **show parser view** für die Benutzeransichten zulässig ist, können sie den Befehl **show parser view** ausführen, um ihre Ansicht zu bestimmen:

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

Unterstützung von SDM CLI-Ansichten

SDM bietet drei Standardansichten, zwei für die Konfiguration und Überwachung von Firewall- und VPN-Komponenten und eine nur für die Überwachung reservierte Ansicht. Eine zusätzliche Standard-**Root**-Ansicht ist auch in SDM verfügbar.

SDM bietet keine Möglichkeit, die in jeder Standardansicht enthaltenen oder aus dieser ausgeschlossenen Befehle zu ändern, und bietet keine Möglichkeit, zusätzliche Ansichten zu definieren. Wenn über die CLI zusätzliche Ansichten definiert werden, bietet SDM die zusätzlichen Ansichten im Konfigurationssatz **Benutzerkonten/Ansichten** nicht an.

Diese Ansichten und die entsprechenden Befehlsberechtigungen sind für SDM vordefiniert:

SDM_Firewall-Ansicht

```
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 View

```
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-Ansicht

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Rollenbasierter CLI-Zugriff
- Technischer Support und Dokumentation - Cisco Systems