Contrôle d'accès basé sur les rôles Cisco IOS avec SDM : Séparation de l'autorisation de configuration entre groupes opérationnels

Contenu

Introduction

Les fonctionnalités de routage et de sécurité sont généralement prises en charge dans des périphériques distincts, ce qui permet une répartition claire des responsabilités de gestion entre l'infrastructure réseau et les services de sécurité. La convergence des fonctionnalités de sécurité et de routage des routeurs à services intégrés Cisco n'offre pas cette séparation claire et multipériphérique. Certaines entreprises ont besoin d'une séparation des capacités de configuration pour limiter les clients ou les groupes de gestion des services le long des limites fonctionnelles. CLI Views, une fonctionnalité du logiciel Cisco IOS®, cherche à répondre à ce besoin avec l'accès CLI basé sur les rôles. Ce document décrit la configuration définie par la prise en charge SDM du contrôle d'accès basé sur les rôles Cisco IOS et fournit un arrière-plan sur les fonctionnalités des vues CLI à partir de l'interface de ligne de commande Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

De nombreuses entreprises délèguent la responsabilité de la maintenance du routage et de la connectivité de l'infrastructure à un groupe d'opérations réseau, et la responsabilité de la maintenance des fonctionnalités de pare-feu, VPN et de prévention des intrusions à un groupe d'opérations de sécurité. Les vues CLI peuvent restreindre la configuration des fonctionnalités de sécurité et la capacité de surveillance au groupe secops, et inversement limiter la connectivité réseau, le routage et d'autres tâches d'infrastructure au groupe netops.

Certains fournisseurs de services souhaitent offrir des capacités limitées de configuration ou de surveillance aux clients, mais ne permettent pas aux clients de configurer ou d'afficher d'autres paramètres de périphérique. Une fois de plus, les vues CLI offrent un contrôle granulaire sur la capacité CLI pour limiter l'exécution des commandes autorisées par les utilisateurs ou les groupes d'utilisateurs.

La plate-forme logicielle Cisco IOS offre la possibilité de limiter les commandes CLI avec un serveur TACACS+ pour autoriser ou refuser l'exécution des commandes CLI en fonction du nom d'utilisateur ou de l'appartenance à un groupe d'utilisateurs. Les vues CLI offrent une fonctionnalité similaire, mais le contrôle de stratégie est appliqué par le périphérique local après la réception de la vue spécifiée de l'utilisateur par le serveur AAA. Lorsque l'autorisation de commande AAA est utilisée, chaque commande doit être autorisée individuellement par le serveur AAA, ce qui entraîne un dialogue fréquent entre le périphérique et le serveur AAA. Les vues CLI permettent le contrôle de la stratégie CLI par périphérique, tandis que l'autorisation de commande AAA applique la même stratégie d'autorisation de commande à tous les périphériques auxquels un utilisateur accède.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Associer des utilisateurs à une vue

Les utilisateurs peuvent être associés à une vue CLI locale par un attribut de retour d'AAA ou dans la configuration d'authentification locale. Pour la configuration locale, le nom d'utilisateur est configuré avec une option **d'affichage** supplémentaire, qui correspond au nom configuré de la **vue de l'analyseur**. Les utilisateurs suivants sont configurés pour les vues SDM par défaut :

```
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
```

Les utilisateurs affectés à une vue donnée peuvent temporairement basculer vers une autre vue s'ils ont le mot de passe de la vue qu'ils veulent saisir. Émettez cette commande exec afin de modifier les vues :

```
enable view view-name
```

Configuration de la vue d'analyseur

Les vues CLI peuvent être configurées à partir de l'interface CLI du routeur ou via SDM. SDM fournit une prise en charge statique pour quatre vues, comme indiqué dans la section Support des vues de l'interface de ligne de commande SDM. Pour configurer la vue CLI à partir de l'interface de ligne de commande, un utilisateur doit être défini comme un utilisateur **root** view, ou il doit appartenir à la vue avec l'accès à la configuration de la **vue analyseur**. Les utilisateurs qui ne sont pas associés à une vue et qui tentent de configurer des vues reçoivent ce message :

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

Les vues CLI permettent l'inclusion ou l'exclusion de hiérarchies de commandes complètes pour les modes de configuration et d'exécution, ou pour certaines parties seulement. Trois options sont disponibles pour autoriser ou interdire une hiérarchie de commande ou de commande dans une vue donnée :

```
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
```

Les affichages CLI tronquent la configuration en cours afin que la configuration de l'affichage de l'analyseur ne s'affiche pas. Cependant, la configuration de la vue de l'analyseur est visible dans la configuration de démarrage.

Référez-vous à Accès CLI basé sur les rôles pour plus d'informations sur la définition d'affichage.

Vérification de l'association d'affichage de l'analyseur

Les utilisateurs affectés à une vue de l'analyseur peuvent déterminer à quelle vue ils sont affectés lorsqu'ils sont connectés à un routeur. Si la commande **show parser view** est autorisée pour les

vues des utilisateurs, ils peuvent émettre la commande **show parser view** afin de déterminer leur vue :

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

Prise en charge des vues CLI SDM

SDM offre trois vues par défaut, deux pour la configuration et la surveillance des composants de pare-feu et de VPN et une vue de surveillance restreinte uniquement. Une vue **racine** par défaut supplémentaire est également disponible dans SDM.

SDM ne permet pas de modifier les commandes incluses dans ou exclues de chaque vue par défaut et ne permet pas de définir des vues supplémentaires. Si des vues supplémentaires sont définies à partir de l'interface de ligne de commande, SDM n'offre pas les vues supplémentaires dans son panneau de configuration **Comptes d'utilisateurs/Vues**.

Ces vues et autorisations de commande respectives sont prédéfinies pour SDM :

Vue SDM_Firewall

```
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
```

Vue SDM_Monitor

```
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
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Accès CLI basé sur les rôles
- Support et documentation techniques - Cisco Systems