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

Contenu

Introduction

La fonctionnalité de routage et de Sécurité est traditionnellement prise en charge dans des périphériques distincts, qui offre une division claire de la responsabilité de Gestion entre l'infrastructure réseau et les Services de sécurité. La convergence de la Sécurité et de la fonctionnalité de routage dans les Integrated Services Router de Cisco n'offre pas cette séparation claire et à plusieurs dispositifs. Quelques organismes ont besoin d'une ségrégation de capacité de configuration pour limiter des clients ou des groupes de gestion des services le long des bornes fonctionnelles. Les vues CLI, une caractéristique de logiciel de Cisco IOS®, recherche à satisfaire ce besoin avec CLI basé sur rôle Access. Ce document décrit la configuration définie par le support SDM du contrôle d'accès basé sur rôle de Cisco IOS, et offre le fond dans les capacités des vues CLI de l'interface de ligne de commande de Cisco IOS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Beaucoup d'organismes délèguent la responsabilité de la maintenance du routage et de la Connectivité d'infrastructure à un groupe d'exploitations réseau, et la responsabilité de la maintenance du Pare-feu, du VPN, et de la fonctionnalité de prévention des intrusions à un groupe d'exécutions de Sécurité. Les vues CLI peuvent limiter la configuration de fonctionnalité de Sécurité et la capacité de surveillance au groupe de secops, et limitent réciproquement la connexion réseau, le routage, et d'autres tâches d'infrastructure au groupe de netops.

Quelques fournisseurs de services veulent offrir la configuration ou la capacité limitée de surveillance aux clients, mais ne pas permettre à des clients pour configurer ou visualiser d'autres paramètres de périphérique. De nouveau, les vues CLI offrent le contrôle granulaire de la capacité CLI pour limiter des utilisateurs ou des groupes d'utilisateurs pour exécuter seulement des commandes autorisées.

Le logiciel de Cisco IOS a offert une capacité pour limiter des commandes CLI avec un serveur TACACS+ pour que l'autorisation permette ou de refuse à la capacité pour exécuter des commandes CLI basées sur l'adhésion de nom d'utilisateur ou de groupe d'utilisateurs. Les vues CLI offrent la capacité semblable, mais le contrôle de stratégie est appliqué par le périphérique local après que la vue spécifiée de l'utilisateur soit reçue du serveur d'AAA. Quand l'autorisation de commande d'AAA est utilisée, chaque commande doit être individuellement autorisée par le serveur d'AAA, qui entraîne le dialogue fréquent entre le périphérique et le serveur d'AAA. Les vues CLI permettent le contrôle de stratégie CLI de par-périphérique, tandis que l'autorisation de commande d'AAA applique la même stratégie d'autorisation de commande à tous les périphériques des accès client.

Configurez

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

document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Utilisateurs d'associé avec une vue

Des utilisateurs peuvent être associés avec une vue CLI de gens du pays 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 supplémentaire de **vue**, qui apparie le nom configuré de **parser view**. Ces utilisateurs d'exemple sont configurés pour les vues du par défaut SDM :

```
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 qui sont assignés à un avis donné peuvent temporairement commuter à une autre vue s'ils ont le mot de passe pour la vue qu'ils veulent écrire. Émettez cette commande EXEC afin de changer des vues :

```
enable view view-name
```

Configuration de parser view

Des vues CLI peuvent être configurées du routeur CLI, ou par SDM. SDM fournit le support statique pour quatre vues, comme évoqué dans la section de support de vues SDM CLI. Afin de configurer la vue CLI de l'interface de ligne de commande, un utilisateur doit être défini en tant qu'utilisateur d'**affichage racine**, ou ils doivent appartenir pour visualiser avec l'accès à la configuration de **parser view**. Les utilisateurs qui ne sont pas associés avec une vue et qui essayent 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'intégration ou l'exclusion des hiérarchies complètes de commande pour le cadre et les modes de configuration, ou seulement les parties s'y rapportant. Trois options sont disponibles pour permettre ou rejeter une commande ou une hiérarchie de commande dans un avis donné :

```
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 vues CLI tronquent le running-config ainsi la configuration de parser view n'est pas affichée. Cependant, la configuration de parser view est visible dans le startup-config.

Référez-vous à CLI basé sur rôle Access pour plus d'informations sur la définition de vue.

Vérifier l'association de parser view

Les utilisateurs qui sont assignés à un parser view peuvent déterminer à quelle vue ils sont assignés quand ils sont ouverts une session à un routeur. Si on permet la commande de **show parser view** pour les vues standard, ils peuvent émettre la commande de **show parser view** afin de déterminer leur vue :

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

Support de vues SDM CLI

SDM offre trois vues par défaut, deux pour la configuration et la surveillance du Pare-feu et des composants VPN, et une vue réservée à la surveillance limitée. **Un affichage racine** par défaut supplémentaire est disponible dans SDM aussi bien.

SDM ne fournit pas la capacité de modifier les commandes incluses dedans ou exclues de chaque vue par défaut, et n'offre aucune capacité pour définir des vues supplémentaires. Si des vues supplémentaires sont définies du CLI, SDM n'offre pas les vues supplémentaires panneau dans sa configuration de **comptes utilisateurs/vues**.

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

Vue de 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
```

Vue de SDM_EasyVPN_Remote

```
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 de 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
```

Vérifiez

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

Dépannez

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

Informations connexes

- CLI basé sur rôle Access
- Support et documentation techniques - Cisco Systems