Contrôle d'accès de base de rôle Nexus N5500, 5600 et N6000 (RBAC)

Contenu

Introduction

Ce document décrit comment limiter l'accès d'un utilisateur aux commutateurs Nexus 5500, Nexus 5600 et Nexus 6000 à l'aide du contrôle d'accès par rôle (RBAC).

RBAC vous permet de définir les règles d'un rôle d'utilisateur assigné afin de restreindre l'autorisation d'un utilisateur qui a accès aux opérations de gestion du commutateur.

Vous pouvez créer et gérer un compte d'utilisateur et attribuer des rôles qui limitent l'accès aux commutateurs Nexus 5500, Nexus 5600 et Nexus 6000.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Commandes de configuration CLI des commutateurs Nexus 5500, Nexus 5600 et Nexus 6000
- Services de fabric Cisco (CFS).

Components Used

Les informations de ce document sont basées sur les commutateurs Nexus 5500, Nexus 5600 et Nexus 6000 exécutant NXOS 5.2(1)N1(9) 7.3(1)N1(1).

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.

Exigences utilisateur

Voici quelques-unes des exigences des utilisateurs qui doivent être satisfaites :

- Seuls les utilisateurs ayant un rôle d'administrateur réseau peuvent créer des rôles.
- Seuls les utilisateurs ayant un rôle admin réseau peuvent afficher le résultat de **show role**.
- Même si les utilisateurs sont autorisés à exécuter toutes les commandes show, ils ne sont pas autorisés à afficher la sortie **show role**, à moins que ces utilisateurs ne se voient attribuer un rôle admin réseau.
- Un compte d'utilisateur doit avoir au moins un rôle d'utilisateur.

Rôles utilisateur

Chaque rôle peut être attribué à plusieurs utilisateurs et chaque utilisateur peut faire partie de plusieurs rôles.

Par exemple, les utilisateurs du rôle A sont autorisés à émettre des commandes show et les utilisateurs du rôle B sont autorisés à modifier la configuration.

Si un utilisateur est affecté au rôle A et au rôle B, cet utilisateur peut émettre la commande show et apporter des modifications à la configuration.

La commande Permit access a priorité sur la commande deny access.

Par exemple, si vous appartenez à un rôle qui refuse l'accès aux commandes de configuration.

Cependant, si vous appartenez également à un rôle qui a accès aux commandes de configuration, vous avez alors accès aux commandes de configuration.

Il existe cinq rôles d'utilisateur par défaut :

- network-admin : accès en lecture-écriture complet à l'ensemble du commutateur.
- network-opérateur : accès en lecture complet à l'ensemble du commutateur.
- vdc-admin - Accès en lecture-écriture limité à un VDC
- vdc-opérateur - Accès en lecture limité à un VDC
- san-admin : accès complet en lecture-écriture aux administrateurs SAN.

Remarque : vous ne pouvez pas modifier/supprimer les rôles utilisateur par défaut.

Note: **show role** affiche le rôle disponible sur le commutateur

Règles de rôle utilisateur

La règle est l'élément de base d'un rôle.

Une règle définit les opérations que le rôle permet à l'utilisateur d'effectuer.

Vous pouvez appliquer des règles pour ces paramètres :

- Commande : commande ou groupe de commandes défini dans une expression régulière.
- Fonctionnalité : commandes qui s'appliquent à une fonction fournie par le logiciel NX-OS.
- Groupe de fonctions : groupe de fonctions défini par l'utilisateur ou par défaut.

Ces paramètres créent une relation hiérarchique. Le paramètre de contrôle le plus basique est la commande.

Le paramètre de contrôle suivant est la fonction, qui représente toutes les commandes associées à la fonction.

Le dernier paramètre de contrôle est le groupe de fonctions. Le groupe de fonctionnalités combine des fonctionnalités connexes et vous permet de gérer facilement les règles.

Le numéro de règle spécifié par l'utilisateur détermine l'ordre dans lequel les règles sont appliquées.

Les règles sont appliquées par ordre décroissant.

Par exemple, la règle 1 est appliquée avant la règle 2, qui est appliquée avant la règle 3, etc.

La commande rule spécifie les opérations qui peuvent être effectuées par un rôle spécifique. Chaque règle se compose d'un numéro de règle, d'un type de règle (autorisation ou refus),

un type de commande (par exemple, configuration, show, exec, debug) et un nom de fonction facultatif (par exemple, FCOE, HSRP, VTP, interface).

Distribution des rôles utilisateur

Les configurations basées sur les rôles utilisent l'infrastructure Cisco Fabric Services (CFS) pour permettre une gestion efficace des bases de données et fournir un point de configuration unique dans le réseau.

Lorsque vous activez la distribution CFS pour une fonction sur votre périphérique, le périphérique appartient à une région CFS contenant d'autres périphériques du réseau que vous avez également activés pour la distribution CFS pour la fonction. Par défaut, la distribution CFS de la fonction de rôle d'utilisateur est désactivée.

Vous devez activer CFS pour les rôles utilisateur sur chaque périphérique auquel vous voulez distribuer les modifications de configuration.

Une fois que vous avez activé la distribution CFS pour les rôles d'utilisateur sur le commutateur, la première commande de configuration de rôle d'utilisateur que vous entrez entraîne les actions suivantes du logiciel NX-OS du commutateur :

1. Crée une session CFS sur le commutateur.
2. Verrouille la configuration du rôle d'utilisateur sur tous les commutateurs de la région CFS

avec CFS activé pour la fonctionnalité de rôle d'utilisateur.
3. Enregistre les modifications de configuration du rôle utilisateur dans une mémoire tampon temporaire sur le commutateur.

Les modifications restent dans la mémoire tampon temporaire du commutateur jusqu'à ce que vous les engagiez explicitement à être distribuées aux périphériques de la région CFS.

Lorsque vous confirmez les modifications, le logiciel NX-OS effectue les actions suivantes :

1. Applique les modifications à la configuration en cours sur le commutateur.
2. Distribue la configuration de rôle utilisateur mise à jour aux autres commutateurs de la région CFS.
3. Déverrouille la configuration du rôle utilisateur dans les périphériques de la région CFS.
4. Termine la session CFS.

Ces configurations sont distribuées :

- Noms et descriptions des rôles
- Liste des règles des rôles

Commandes Configuration et Show

	Commande	Objectif
Étape 1.	configurer le terminal Exemple : switch# **configure terminal** switch(config)#	Passe en mode de configuration globale.
Étape 2.	**nom de rôle** *role-name* Exemple : switch(config)# **nom de rôle UserA** switch(config-role)#	Spécifie un rôle utilisateur et passe en mode de configuration de rôle.
Étape 3.	**vlan policy deny** Exemple : switch(config-role)# **vlan policy deny** switch(config-role-vlan)#	Passe en mode de configuration de la stratégie de vlan de rôle.
Étape 4.	**permit vlan** vlan-*id* Exemple : switch(config-role-vlan)# **permit vlan 1**	Spécifie le VLAN auquel le rôle peut accéder. Répétez cette commande pour autant de VLAN que nécessaire.
Étape 5.	**sortir** Exemple : switch(config-role-vlan)# **exit** switch(config-role)#	Quitte le mode de configuration de la stratégie de VLAN de rôle.
Étape 6.	**show role** Exemple : switch(config-role)# **show role**	(Facultatif) Affiche la configuration du rôle.
Étape 7.	**show role** {**en attente** |	(Facultatif) Affiche la configuration du rôle d'utilisateur en attente de

	en attente-diff} Exemple : switch(config-role)# **show role en attente**	distribution
Étape 8.	**role commit** Exemple : switch(config-role)# **role commit**	(Facultatif) Applique les modifications apportées à la configuration du rôle d'utilisateur dans la base de données temporaire à la configuration en cours et distribue la configuration du rôle d'utilisateur à d'autres commutateurs si vous avez activé la distribution de la configuration CFS pour la fonctionnalité de rôle d'utilisateur.
Étape 9.	**copy running-config startup-config** Exemple : switch# **copy running-config startup-config**	(Facultatif) Copie la configuration en cours dans la configuration de démarrage.

Ces étapes permettent la distribution de la configuration des rôles :

	Commande	**Objectif**
Étape 1.	switch# **config t** switch(config)#	Passe en mode de configuration.
Étape 2.	switch(config)# **role distribute**	Active la distribution de la configuration des rôles.
	switch(config)#**no role distribute**	Désactive la distribution de configuration des rôles (par défaut).

Ces étapes valident les modifications de configuration des rôles :

	Commande	**Objectif**
Étape 1	Nexus# **config t** Nexus(config)#	Passe en mode de configuration.
Étape 2	Nexus(config)# **role commit**	Valide les modifications apportées à la configuration du rôle.

Ces étapes permettent de supprimer les modifications de configuration des rôles :

	Commande	**Objectif**
Étape 1	Nexus# **config t** Nexus(config)#	Passe en mode de configuration.
Étape 2	Nexus(config)# **role abort**	Ignore les modifications apportées à la configuration du rôle et efface la base de données de configuration en attente.

Pour afficher les informations de compte d'utilisateur et de configuration RBAC, effectuez l'une des tâches suivantes :

Commande	**Objectif**
show role	Affiche la configuration du rôle utilisateur.
show role feature	Affiche la liste des fonctions.
show role feature-group	Affiche la configuration du groupe de fonctions.

Effacer la session de distribution des rôles utilisateur

Vous pouvez effacer la session de distribution des services de fabric Cisco en cours (le cas échéant) et déverrouiller le fabric pour la fonction de rôle d'utilisateur.

Attention : Toute modification de la base de données en attente sera perdue lorsque vous

émettrez cette commande.

	Commande	Objectif
Étape 1	**clear role session** **Exemple :** switch# clear role session	Efface la session et déverrouille le fabric.
Étape 2	**show role session status** **Exemple :** switch# show role état session	(Facultatif) Affiche l'état de la session CFS du rôle utilisateur.

Exemple de configuration

Dans cet exemple, nous allons créer un TAC de compte d'utilisateur avec les autorisations d'accès suivantes :

- Accès à la commande clear
- Accès à la commande de configuration
- Accès à la commande debug
- Accès à la commande exec
- Accès à la commande show
- Accès au VLAN 1-10 uniquement

```
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end

C5548P-1# show role name Cisco

Role: Cisco
  Description: new role
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 1-10
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  5       permit  command                         show
  4       permit  command                         exec
  3       permit  command                         debug
  2       permit  command                         config
  1       permit  command                         clear
```

```
C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
        this user account has no expiry date
        roles:Cisco
```

Exigences de licence

Product (produit)	Exigences de licence
NX-OS	Les comptes d'utilisateurs et RBAC ne requièrent aucune licence.

Vérification

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

Dépannage

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