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

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Exigences de l'utilisateur](#)
[Rôles de l'utilisateur](#)
[Rôle de l'utilisateur de règles](#)
[Rôle de l'utilisateur de distribution](#)
[Configuration et commandes show](#)
[Effacez le rôle de l'utilisateur de session de distribution](#)
[Exemple de configuration](#)
[Conditions d'autorisation](#)
[Vérifiez](#)
[Dépannez](#)

Introduction

Ce document décrit comment limiter un utilisateur pour accéder au Nexus 5500, le Nexus 5600 et les Commutateurs du Nexus 6000 utilisant le rôle basent le contrôle d'accès (RBAC).

RBAC te permet pour définir les règles pour qu'un rôle de l'utilisateur assigné limite l'autorisation d'un utilisateur qui a accès aux exécutions de gestion de la commutation.

Vous pouvez créer et gérer un compte utilisateur et assigner les rôles qui accès de limite aux Commutateurs du Nexus 5500, du Nexus 5600 et du Nexus 6000.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Nexus 5500, Nexus 5600, commandes de configuration CLI de Commutateurs du Nexus 6000
- Services Cisco Fabric (CFS).

Composants utilisés

Les informations dans ce document sont basées sur des Commutateurs du Nexus 5500, du Nexus 5600 et du Nexus 6000 exécutant NXOS 5.2(1)N1(9) 7.3(1)N1(1).

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.

Exigences de l'utilisateur

Ce sont quelques exigences de l'utilisateur qui sont le besoin d'être accompli :

- Seulement les utilisateurs avec le rôle de réseau-admin peuvent créer des rôles.
- Seulement les utilisateurs avec le rôle de réseau-admin peuvent visualiser la sortie du **show role**.
- Même si on permet à des des utilisateurs pour exécuter toutes les commandes show, on ne leur permet pas pour visualiser le **show role de** sortie, à moins que ces utilisateurs soient assignés un rôle de réseau-admin.
- Un compte utilisateur doit avoir au moins un rôle de l'utilisateur.

Rôles de l'utilisateur

Chaque rôle peut être assigné aux plusieurs utilisateurs et chaque utilisateur peut faire partie de plusieurs rôles.

Par exemple, des utilisateurs du rôle A sont permis pour émettre des commandes show et des utilisateurs du rôle B sont permis pour apporter des modifications de configuration.

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

La commande d'accès d'autorisation prend la priorité plus de refusent la commande d'accès.

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 l'accès aux commandes de configuration.

Il y a cinq rôles de l'utilisateur par défaut :

- réseau-admin - Complete lecture-et-écrivent l'accès au commutateur entier.
- opérateur réseau - Accès en lecture complet au commutateur entier.
- volts continu-admin - Lecture-et-écrivez l'accès limité à un volts continu
- volts continu-opérateur - Accès en lecture limité à un volts continu
- San-admin - Complete lecture-et-écrivent l'accès aux administrateurs SAN.

Remarque: Vous ne pouvez pas modifier/rôles de l'utilisateur par défaut d'effacement.

Remarque: **le show role de** commande affichera le rôle disponible sur le commutateur

Rôle de l'utilisateur de règles

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

Une règle définit quelles exécutions le rôle permet à l'utilisateur pour exécuter.

Vous pouvez appliquer des règles pour ces paramètres :

- Commandez la commande A ou le groupe de commandes définies dans une expression régulière.
- Comportez les commandes qui s'appliquent à une fonction fournie par le logiciel NX-OS.
- Valeur par défaut du groupe de caractéristique ou groupe défini par l'utilisateur de caractéristiques.

Ces paramètres créent des relations hiérarchiques. Le paramètre du contrôle le plus de base est la commande.

Le prochain paramètre de contrôle est la caractéristique, qui représente toutes les commandes associées avec la configuration.

Le dernier paramètre de contrôle est le groupe de caractéristique. Le groupe de caractéristique combine les caractéristiques relatives et te permet pour gérer facilement des règles.

Le nombre personnalisé par l'utilisateur de règle détermine la commande dans laquelle les règles sont appliquées.

Les règles sont appliquées dans l'ordre décroissant.

Par exemple, la règle 1 est appliquée avant la règle 2, qui est appliquée avant la règle 3, et ainsi de suite.

La commande de règle spécifie les exécutions qui peuvent être exécutées par un rôle spécifique. Chaque règle se compose d'un nombre de règle, un type de règle (l'autorisation ou refusent),

un type de commande (par exemple, la configuration, exposition, exécutif, mettent au point), et un nom de fonctionnalité facultative (par exemple, FCOE, HSRP, VTP, interface).

Rôle de l'utilisateur de distribution

les configurations basées sur rôle emploient l'infrastructure des Services Cisco Fabric (CFS) pour activer la gestion de bases de données efficace et pour fournir un seul point de configuration dans le réseau.

Quand vous activez la distribution CFS pour une caractéristique sur votre périphérique, le périphérique appartient à un cfs region contenant d'autres périphériques dans le réseau que vous avez également activé pour la distribution CFS pour la caractéristique. La distribution CFS pour le rôle de l'utilisateur de caractéristique est désactivée par défaut.

Vous devez activer le CFS pour des rôles de l'utilisateur sur chaque périphérique auquel vous voulez distribuer des modifications de configuration.

Après que vous activiez la distribution CFS pour des rôles de l'utilisateur sur le commutateur, le

premier rôle de l'utilisateur de commande de configuration que vous écrivez des causes le logiciel du commutateur NX-OS pour prendre à ces actions :

1. Crée une session CFS sur le commutateur.
2. Verrouille le rôle de l'utilisateur de configuration sur tous les Commutateurs dans le cfs region avec le CFS activé pour le rôle de l'utilisateur de caractéristique.
3. Enregistre le rôle de l'utilisateur de modifications de configuration dans une mémoire tampon provisoire sur le commutateur.

Les modifications restent dans la mémoire tampon provisoire sur le commutateur jusqu'à ce que vous les commettiez explicitement à distribuer aux périphériques dans le cfs region.

Quand vous commettez les modifications, le logiciel NX-OS prend ces mesures :

1. Applique les modifications à la configuration en cours sur le commutateur.
2. Distribue le rôle de l'utilisateur mis à jour de configuration aux autres Commutateurs dans le cfs region.
3. Déverrouille le rôle de l'utilisateur de configuration dans les périphériques dans le cfs region.
4. Termine la session CFS.

Ces configurations sont distribuées :

- Roles names et descriptions
- Liste de règles pour les rôles

Configuration et commandes show

	Commande	But
Étape 1.	**configure terminal** Exemple : **configure terminal** **de** switch# switch(config)#	Entre le mode de configuration globale.
Étape 2.	*role name de* **role name** Exemple : **role name UserA** **de** switch(config)# commutateur (config-rôle) #	Spécifie un rôle de l'utilisateur et écrit le mode de configuration de rôle.
Étape 3.	**vlan policy deny** Exemple : commutateur (config-rôle) # **vlan policy deny** commutateur (config-rôle-VLAN) #	Entre le mode de configuration de politique de VLAN de rôle.
Étape 4.	VLAN-id de **permit vlan** Exemple :	Spécifie le VLAN que le rôle peut accéder à. Répétez cette commande pour autant de VLAN comme nécessaires.

	commutateur (config-rôle-VLAN) **# permit vlan 1 sortie** Exemple : commutateur (config-rôle-VLAN)	
Étape 5.	**# sortie** commutateur (config-rôle) #	Annule le mode de configuration de politique de VLAN de rôle.
Étape 6.	**show role** Exemple : commutateur (config-rôle) #	(Facultatif) affiche la configuration de rôle.
Étape 7.	**show role** {**en suspens | en suspens-diff**} Exemple : commutateur (config-rôle) #	(Facultatif) affiche le rôle de l'utilisateur de configuration en suspens pour la distribution
Étape 8.	**show role pending role commit** Exemple : commutateur (config-rôle) # **role commit**	(Facultatif) s'applique le rôle de l'utilisateur de modifications de configuration dans la base de données provisoire à la configuration en cours et distribue le rôle de l'utilisateur de configuration à d'autres swithces si vous avez activé la distribution de configuration CFS pour le rôle de l'utilisateur de caractéristique.
Étape 9.	**copy running-config startup-config** Exemple : **copy running-config startup-config de** switch#	(Facultatif) copie la configuration en cours sur la configuration de démarrage.

Ces étapes activent la distribution de configuration de rôle :

	Commande	But
Étape 1.	**configuration t de** switch# switch(config)#	Écrit le mode de configuration.
Étape 2.	**role distribute de** switch(config)# **role distribute de** switch(config)#no	Active la distribution de configuration de rôle. Distribution de configuration de rôle de débronchements (par défaut).

Ces modifications de configuration de rôle de validation d'étapes :

	Commande	But
Étape 1	**Configuration t de** Nexus# Nexus(config)#	Écrit le mode de configuration.
Étape 2	**Role commit de** Nexus(config)#	Commet les modifications de configuration de rôle.

Ces modifications de configuration de rôle d'écart d'étapes :

	Commande	But
Étape 1	Configuration t de Nexus# Nexus(config)#	Écrit le mode de configuration.
Étape 2	Role abort de Nexus(config)#	Jette les modifications de configuration de rôle et efface la base de donnée configuration en attente.

Pour afficher le compte utilisateur et les informations de configuration RBAC, effectuez une de ces tâches :

Commande	But
show role	Affiche le rôle de l'utilisateur de configuration.
show role feature	Affiche la liste de caractéristique.
show role feature-group	Affiche la configuration de groupe de caractéristique.

Effacez le rôle de l'utilisateur de session de distribution

Vous pouvez effacer la session actuelle de distribution de Services Cisco Fabric (le cas échéant) et déverrouiller la matrice pour le rôle de l'utilisateur de caractéristique.

> **Attention** : Tous les changements de la base de données en attente seront perdus quand vous émettez cette commande.

	Commande	But
Étape 1	session claire de rôle de switch# **Exemple :** session claire de rôle de switch#	Efface la session et déverrouille la matrice.
Étape 2	état de show role session **Exemple :** état de show role session de switch#	(Facultatif) affiche le rôle de l'utilisateur CFS d'état de sess

Exemple de configuration

Dans cet exemple, nous allons créer un compte utilisateur TAC avec des ces permission d'accès :

- Access à la commande claire
- Access à la commande de configuration
- Access à la commande de débogage
- Access à la commande EXEC
- Access à la commande show
- Accédez à au VLAN 1-10 seulement

```
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
```

Conditions d'autorisation

Produit Condition requise de permis

NX-OS Les comptes utilisateurs et les RBAC n'exigent aucun permis.

Vérifiez

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

Dépannez

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