Accès client d'ACS Limited avec le RAYON sur l'exemple de configuration de Nexus

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Configuration des rôles faits sur commande sur le Nexus](#)
[Configurez le Nexus pour l'authentification et l'autorisation](#)
[Configuration d'ACS](#)
[Vérifiez](#)
[Vérification de rôle de Nexus](#)
[Rôle de l'utilisateur de vérification d'affectation de Nexus](#)
[Dépannez](#)

Introduction

Ce document décrit comment fournir l'accès restreint aux utilisateurs de Nexus de sorte qu'ils puissent seulement sélectionner des commandes limitées avec le Cisco Secure Access Control Server (ACS) en tant que serveur de RAYON. Par exemple, vous pourriez vouloir qu'un utilisateur puisse ouvrir une session à un privilégié ou à un mode de configuration et seulement être laissé sélectionner des commandes d'interface. Afin de réaliser ceci, vous devez créer un rôle fait sur commande pour l'utilisateur sur le serveur de RAYON qui est utilisé.

Conditions préalables

Conditions requises

Le serveur de RAYON (ACS dans cet exemple) et le Nexus doivent pouvoir se contacter et exécuter des authentifications.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 5.x ACS
- Commutateurs de Nexus 7000

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.

Configurez

Configuration des rôles faits sur commande sur le Nexus

Afin de créer un rôle qui fournit seulement l'accès lecture/écriture pour la commande d'interface, entrez :

```
switch(config)# role name Limited-Access
switch(config-role)# rule 1 permit read-write feature interface
```

Des règles d'accès supplémentaires d'autorisation sont définies avec cette syntaxe :

```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

Configurez le Nexus pour l'authentification et l'autorisation

1. Afin de créer un utilisateur local sur le commutateur avec de pleins privilèges pour le retour, sélectionnez la commande de **nom d'utilisateur** :
   `Switch(config)#username admin privilege 15 password 0 cisco123!`
2. Afin de fournir l'adresse IP du serveur de RAYON (ACS), entrez :
   ```
   switch# conf terminal
   switch(config)# Radius-server host 10.10.1.1 key cisco123
   authenticationaccounting
   switch(config)# aaa group server radius RadServer
   switch(config-radius)#server 10.10.1.1
   switch(config-radius)# use-vrf Management
   ```
   Remarque: La clé doit apparier le secret partagé configuré sur le serveur de RAYON pour ce périphérique de Nexus.
3. Afin de tester la disponibilité du serveur de RAYON, sélectionnez la commande d'**AAA de test** :
   `switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH`
   Le test d'authentification devrait échouer avec un rejet du serveur puisqu'il n'est pas encore configuré. Cependant, il confirme que le serveur est accessible.
4. Afin de configurer des authentifications de connexion, entrez :
   ```
   Switch(config)#aaa authentication login default group Radserver
   Switch(config)#aaa accounting default group Radserver
   Switch(config)#aaa authentication login error-enable
   ```
   Vous ne devez pas s'inquiéter de la méthode locale de retour ici, parce que des retours de Nexus aux gens du pays seule si le serveur de RAYON est indisponible.

Configuration d'ACS

1. Naviguez vers des **éléments de stratégie > l'authentification et des autorisations > le profil d'accès au réseau > d'autorisation** afin de créer un profil d'autorisation.
2. Écrivez un nom pour le profil.
3. Sous les **attributs personnalisés** tabulez, écrivez ces valeurs :
   Type de dictionnaire : Rayon-CiscoAttribut : Cisco-poids du commerce-pairesCondition requise : ObligatoireValeur : shell : roles=Limited_Access
4. Soumettez les modifications afin de créer un rôle basé sur attribut pour le commutateur de Nexus.
5. Créez une nouvelle règle d'autorisation ou éditez une règle en cours dans la stratégie correcte d'accès. Des demandes RADIUS sont traitées par la stratégie d'accès au réseau par défaut.
6. Dans la région de **conditions**, choisissez les conditions appropriées. Dans la région de **résultats**, choisissez le **profil de Limited_Access**.

7. Cliquez sur **OK**.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérification de rôle de Nexus

Écrivez le **show role de** commande sur le Nexus afin d'afficher les rôles définis et avez configuré des règles d'accès.

```
switch# show role  (Displays all the roles and includes
custom roles that you have created and their permissions.)

Role: network-admin

Description: Predefined network admin role has access to all
commands on the switch.
------------------------------------------------------------------
Rule Perm Type Scope Entity
------------------------------------------------------------------
1 permit read-write

Role:Limited_Access
Description: Predefined Limited_Access role has access to these commands.
------------------------------------------------------------------
Rule Perm Type Scope Entity
------------------------------------------------------------------
1 permit read-write feature Interface
```

Rôle de l'utilisateur de vérification d'affectation de Nexus

Ouvrez une session au Nexus avec le nom d'utilisateur et mot de passe configuré sur l'ACS. Après procédure de connexion, sélectionnez la commande de **show user-account** afin de vérifier que l'utilisateur de test a le rôle de Limited_Access :

```
switch# show user-account
user:admin
this user account has no expiry date
roles:network-admin

user:Test
this user account has no expiry date
roles:Limited_Access
```

Une fois que le rôle d'accès client est confirmé, commutez dans le mode de configuration et tentez de sélectionner une commande autre qu'une commande d'interface. L'utilisateur devrait être refusé l'accès.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

- **show role** - Affiche la définition de rôle et les règles d'accès configurées.
- **show user-account** - Affiche les détails de compte utilisateur et inclut l'affectation de rôle.

Dépannez

Cette section fournit des informations que vous pouvez employer afin de dépanner votre configuration de commutateur.

Terminez-vous ces étapes sur le commutateur pour l'affectation de rôle :

1. Vérifiez que le groupe d'AAA est utilisé pour l'authentification avec le **show running-config aaa** et les commandes de **show aaa authentication**.
2. Pour le RAYON, vérifiez l'association de Virtual Routing and Forwarding (VRF) avec le groupe d'AAA avec le **show aaa authentication** et les commandes de **show running-config radius**.
3. Si ces commandes vérifient que l'association est correcte, écrivez le **debug radius toute la** commande afin d'activer se connecter de suivi.
4. Vérifiez que les attributs corrects sont poussés de l'ACS.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **show running-config D.C.A.**
- **authentification de show aaa**
- **show running-config radius**
- **debug radius tout**