Configuration de base de la modification d'autorisation dans un commutateur Catalyst 1300 à l'aide de CLI

Objectif

L'objectif de cet article est de vous montrer comment effectuer une configuration de base de la fonction de changement d'autorisation (CoA) dans les commutateurs Catalyst 1300 à l'aide de l'interface de ligne de commande (CLI).

Périphériques et version du logiciel applicables

- commutateurs Catalyst 1300 | 4.1.3.36

Introduction

Change of Authorization (CoA) est une extension du protocole RADIUS qui vous permet de modifier les propriétés d'une session utilisateur AAA (Authentication, Authorization, and Accounting) ou dot1x après son authentification. Lorsqu'une stratégie pour un utilisateur ou un groupe dans AAA change, les administrateurs peuvent transmettre des paquets RADIUS CoA à partir du serveur AAA, tel qu'un moteur Cisco Identity Services Engine (ISE), pour réinitialiser l'authentification et appliquer la nouvelle stratégie.

Cisco Identity Services Engine (ou ISE) est un moteur de contrôle d'accès basé sur le réseau et d'application des politiques doté de toutes les fonctionnalités. Il fournit des services d'analyse et d'application de la sécurité, RADIUS et TACACS, la distribution des politiques, etc. Cisco ISE est actuellement le seul client d'autorisation dynamique CoA pris en charge pour les commutateurs Catalyst 1300. Reportez-vous au guide d'administration ISE pour plus d'informations.

La prise en charge CoA a été ajoutée aux commutateurs Catalyst 1300 dans la version 4.1.3.36 du microprogramme. Cela inclut la prise en charge de la déconnexion des utilisateurs et de la modification des autorisations applicables à une session utilisateur. Le périphérique prend en charge les actions CoA suivantes :

- Déconnecter la session
- Commande Disable host port CoA
- Commande Bounce host port CoA
- Commande CoA de réauthentification hôte

Dans cet article, vous trouverez les commandes pour une configuration CoA de base dans les commutateurs Catalyst 1300 utilisant l'interface de ligne de commande. Les étapes peuvent varier en fonction des paramètres et des exigences de l'utilisateur.

Table des matières

- Configuration CoA de base avec CLI
- Autres commandes de configuration CoA
- Commandes CLI en mode privilégié

Configuration CoA de base avec CLI

Configuration du serveur RADIUS et de la gestion des comptes RADIUS

Pour configurer le serveur RADIUS, en mode de configuration globale, utilisez les commandes suivantes :

Étape 1

Utilisez la commande radius-server key pour définir la clé d'authentification pour les communications RADIUS entre le périphérique et le démon RADIUS.

```
radius-server key
```

Étape 2

Utilisez la commande radius-server host pour configurer un hôte de serveur RADIUS.

```
radius-server host key priority 1 usage dot1.x
```

- L'adresse IP sera celle du serveur ISE.
- key <key-string> - Spécifie la clé d'authentification et de chiffrement pour toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au chiffrement utilisé sur le démon RADIUS.
- Priority : spécifie l'ordre dans lequel les serveurs sont utilisés, où 0 a la priorité la plus élevée. (Plage : 0-65535)
- usage dot1.x : indique que le serveur RADIUS est utilisé pour l'authentification de port 802.1x.

Étape 3

```
aaa accounting dot1x start-stop group radius
```

Configurer le serveur d'autorisation dynamique

Étape 1

À partir du mode de configuration globale, passez en mode de configuration CoA en exécutant la commande suivante :

```
aaa server radius dynamic-author
```

Étape 2

Pour configurer la clé RADIUS à partager entre le périphérique et un client CoA (plage : 0-128 caractères), utilisez la commande server-key <key-string> en mode de configuration du serveur local d'autorisation dynamique. La clé fournie dans la demande CoA doit correspondre à cette clé.

```
server-key
```

> **Note:**
> Pour ISE, la chaîne clé sera la même que celle que vous avez spécifiée pour la chaîne clé du serveur RADIUS lors de la configuration de RADIUS.

Étape 3

Saisissez l'adresse IP de l'hôte du client CoA. L'adresse IP peut être une adresse IPv4, IPv6 ou IPv6z.

```
client
```

Étape 4

```
Exit
```

Configuration de 802.1x

Pour activer 802.1X globalement, utilisez la commande dot1x system-auth-control.

```
dot1x system-auth-control
```

Configurer 802.1x sur un port

Étape 1

Entrez la configuration d’interface et sélectionnez l’ID d’interface à l’aide de la commande interface GigabitEthernet<ID d’interface>.

```
interface gi1/0/1
```

Étape 2

Pour activer le contrôle manuel de l'état d'autorisation de port, utilisez la commande dot1x port-control. Le mode Auto active l'authentification 802.1X sur le port et le fait passer à l'état autorisé ou non autorisé, en fonction de l'échange d'authentification 802.1X entre le périphérique et le client.

```
dot1x port-control auto
```

Étape 3

Pour lancer manuellement une nouvelle authentification de tous les ports compatibles 802.1X ou du port 802.1X spécifié, utilisez la commande dot1x re-authenticate en mode d'exécution privilégié.

```
dot1x re-authenticate gi1/0/1
```

Étape 4

Pour configurer le mode d’apprentissage de la sécurité des ports, utilisez la commande de mode de configuration Interface (Ethernet, Port Channel). Le paramètre Secure delete-on-reset est un mode sécurisé avec un apprentissage limité des adresses MAC sécurisées avec la durée de vie delete-on-reset.

```
port security mode secure delete-on-reset
```

Étape 5

Pour quitter la configuration de l'interface, saisissez ce qui suit :

```
exit
```

Autres commandes de configuration CoA

Voici quelques-unes des autres commandes CoA qui peuvent être utilisées en fonction de votre configuration et de votre configuration.

- attribute event-timestamp drop-packet - Cette commande est utilisée en mode de configuration du serveur local d'autorisation dynamique pour configurer le périphérique afin qu'il abandonne une demande de PoD (Packet of Disconnect) ou de CoA qui n'inclut pas d'attribut event-timestamp.

```
attribute event-timestamp drop-packet
```

- authentication, commande bounce-port ignore - Pour configurer le périphérique afin qu'il ignore

une commande de port de renvoi de changement d'autorisation (CoA) RADIUS, utilisez la commande d'authentification bounce-port ignore en mode de configuration globale.

```
authentication command bounce-port ignore
```

- authentication command disable-port ignore - Pour configurer le périphérique afin qu'il ignore une commande RADIUS CoA disable-port, utilisez cette commande en mode de configuration globale.

```
authentication command disable-port ignore
```

- délimiteur de domaine <character> - Pour configurer le délimiteur de domaine du nom d'utilisateur pour les demandes PoD et CoA reçues, utilisez la commande domain delimiter en mode de configuration du serveur local d'autorisation dynamique.

```
domain delimiter $
```

Dans cet exemple, le caractère $ est configuré comme délimiteur.

- domain stripping [de droite à gauche] - Pour activer et définir le comportement de la suppression de domaine de nom d'utilisateur pour les requêtes PoD et CoA reçues, utilisez la commande domain stripping en mode de configuration de serveur local d'autorisation dynamique.

```
domain stripping right-to-left
```

- ignore server-key : cette commande est utilisée en mode de configuration du serveur local d'autorisation dynamique pour configurer le périphérique afin qu'il ignore la clé serveur CoA.

```
ignore server-key
```

Commandes CLI en mode privilégié

En mode d'exécution privilégié, vous pouvez exécuter des commandes show sur les clients authentifiés, effacer les compteurs clients et afficher la configuration du serveur d'autorisation dynamique.

- Utilisez la commande show aaa clients pour afficher les statistiques du client AAA (CoA).

```
show aaa clients
```

- Utilisez la commande show aaa server radius dynamic-author pour afficher la configuration CoA.

```
show aaa server radius dynamic-author
```

- clear aaa counters peut être utilisé pour effacer les compteurs des clients aaa

```
clear aaa clients counters
```

Conclusion

Vous avez maintenant terminé une configuration de modification de base d'autorisation (CoA) dans le commutateur Catalyst 1300 à l'aide de l'interface de ligne de commande.

Pour plus d'informations sur les commandes CLI pour les commutateurs Catalyst 1300, référez-vous au Guide CLI des commutateurs Cisco Catalyst 1300.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.