Configurer l'ambassadeur du hall d'accueil du WLC 9800 avec authentification RADIUS et TACACS+

Contenu

Introduction

Ce document décrit comment configurer les contrôleurs LAN sans fil Catalyst 9800 pour l'authentification externe RADIUS et TACACS+ des utilisateurs Lobby Ambassador, avec l'utilisation d'ISE (Identity Services Engine).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800
- Concepts AAA, RADIUS et TACACS+

Components Used

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

- Gamme de contrôleurs sans fil Catalyst 9800 (Catalyst 9800-CL)
- Cisco IOS®-XE Gibraltar 16.12.1s
- ISE 2.3.0

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'utilisateur Lobby Ambassador est créé par l'administrateur du réseau. Un utilisateur Lobby Ambassador peut créer le nom d'utilisateur, le mot de passe, la description et la durée de vie d'un utilisateur invité. Il peut également supprimer l'utilisateur invité. L'utilisateur invité peut être créé via une interface utilisateur graphique ou CLI.

Configuration

Diagramme du réseau

Dans cet exemple, Lobby Ambassadors « hall » et « hallTac » sont configurés. Le « lobby » du hall d'accueil est destiné à être authentifié par le serveur RADIUS et le « lobbyTac » du hall d'accueil est authentifié par TACACS+.

La configuration sera faite d'abord pour le Lobby Ambassador RADIUS et enfin pour le Lobby Ambassador TACACS+. La configuration RADIUS et TACACS+ ISE est également partagée.

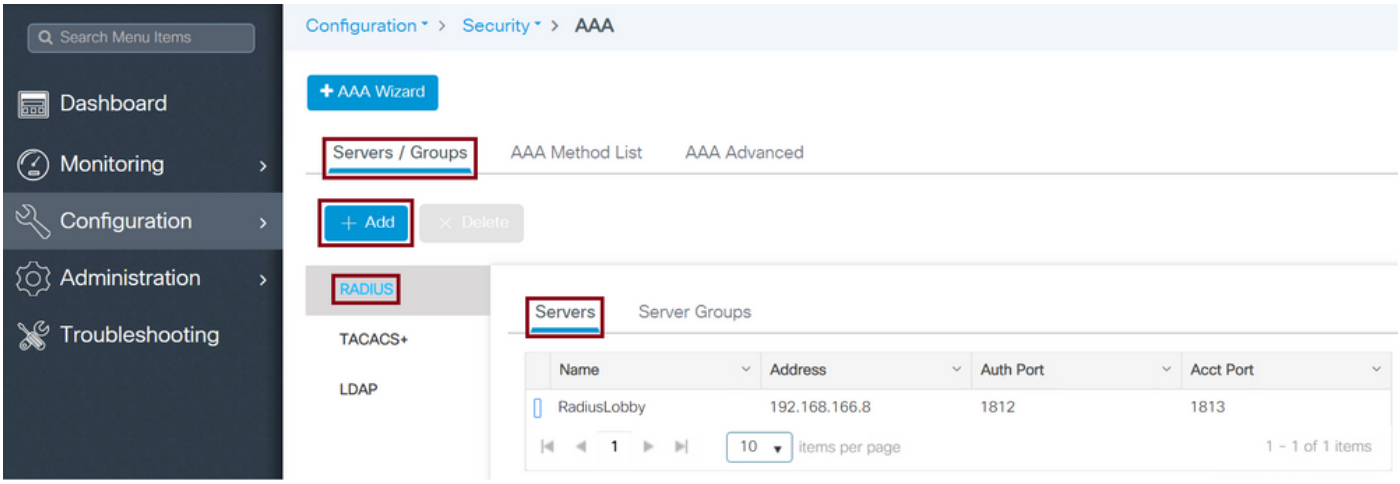
Authentifier RADIUS

Configurez RADIUS sur le contrôleur de réseau local sans fil (WLC).

Étape 1. Déclarez le serveur RADIUS. Créez le serveur RADIUS ISE sur le WLC.

IUG:

Accédez à **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, les paramètres de configuration obligatoires sont le nom du serveur RADIUS (il ne doit pas nécessairement correspondre au nom du système ISE/AAA), l'ADRESSE IP du serveur RADIUS et le secret partagé. Tous les autres paramètres peuvent être laissés par défaut ou configurés selon vos besoins.

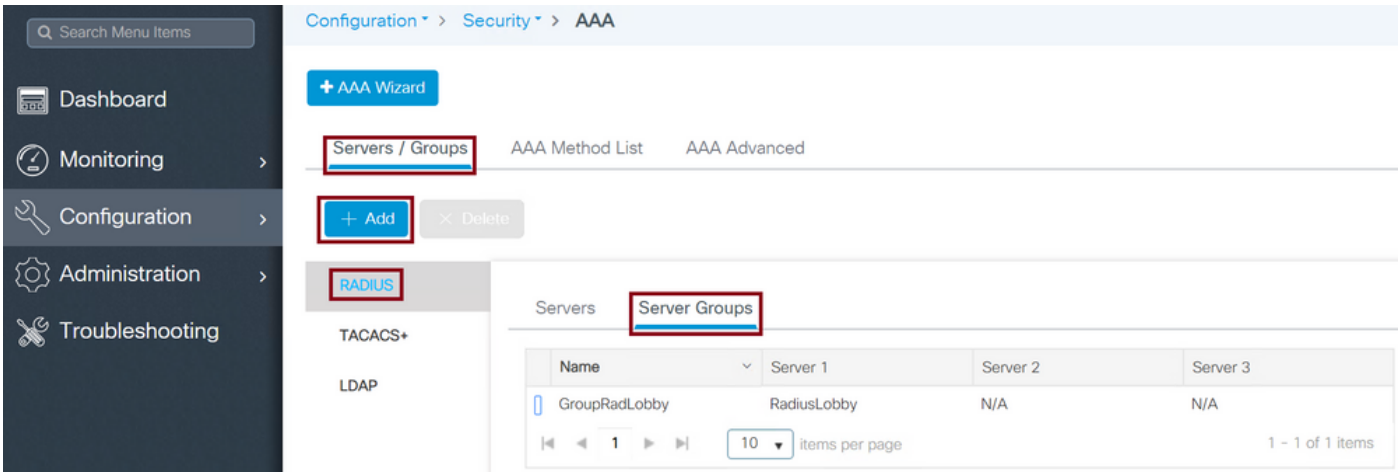
CLI :

```
Tim-eWLC1(config)#radius server RadiusLobby
Tim-eWLC1(config-radius-server)#address ipv4 192.168.166.8 auth-port 1812 acct-port 1813
Tim-eWLC1(config-radius-server)#key 0 Cisco1234
Tim-eWLC1(config)#end
```

Étape 2. Ajoutez le serveur RADIUS à un groupe de serveurs. Définissez un groupe de serveurs et ajoutez le serveur RADIUS configuré. Il s'agit du serveur RADIUS utilisé pour l'authentification de l'utilisateur Lobby Ambassador. Si plusieurs serveurs RADIUS configurés dans le WLC peuvent être utilisés pour l'authentification, la recommandation est d'ajouter tous les serveurs Radius au même groupe de serveurs. Si vous le faites, vous laissez le WLC équilibrer la charge des authentifications entre les serveurs RADIUS dans le groupe de serveurs.

IUG:

Accédez à **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre afin de donner un nom au groupe, déplacez les serveurs RADIUS configurés de la liste Serveurs disponibles vers la liste Serveurs affectés.

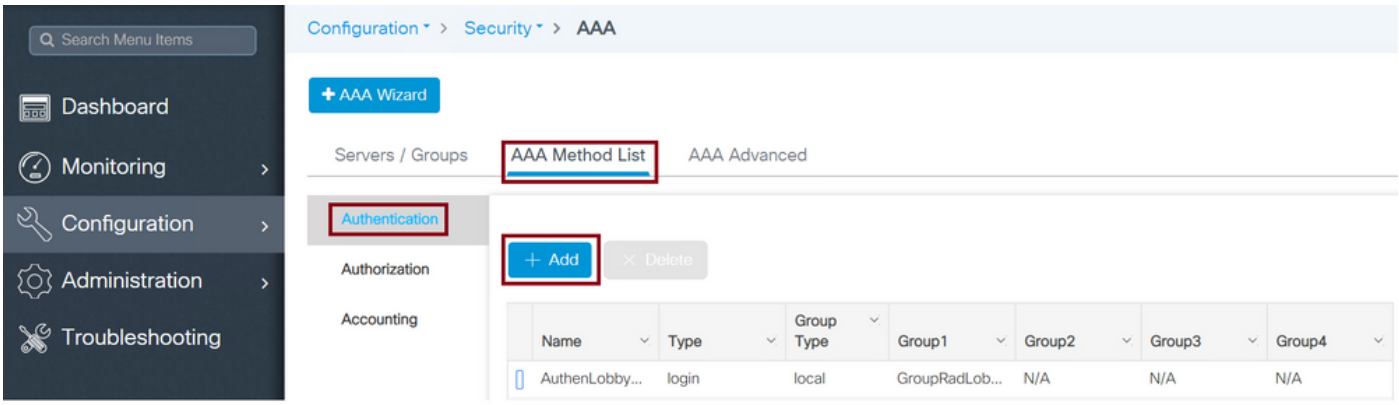
CLI :

```
Tim-eWLC1(config)#aaa group server radius GroupRadLobby
Tim-eWLC1(config-sg-radius)#server name RadiusLobby
Tim-eWLC1(config-sg-radius)#end
```

Étape 3. Créez une liste de méthodes d'authentification. La liste Authentication Method (Méthode d'authentification) définit le type d'authentification que vous recherchez et les associera également au groupe de serveurs que vous définissez. Vous saurez si l'authentification sera effectuée localement sur le WLC ou externe à un serveur RADIUS.

IUG:

Accédez à **Configuration > Security > AAA > AAA Method List > Authentication > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, indiquez un nom, sélectionnez l'option de type **Connexion** et affectez le groupe de serveurs créé précédemment.

Type de groupe en tant que local.

IUG:

Si vous sélectionnez le type de groupe comme 'local', le WLC vérifie d'abord si l'utilisateur existe dans la base de données locale et retourne ensuite au groupe de serveurs uniquement si l'utilisateur Lobby Ambassador n'est pas trouvé dans la base de données locale.

CLI :

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

> **Note**: Veuillez être conscient du bogue CSCvs87163 lorsque vous utilisez local en premier. Ceci est corrigé dans la section 17.3.

Type de groupe en tant que groupe.

IUG:

Si vous sélectionnez le type de groupe comme 'group' et qu'aucune option locale de secours n'est

activée, le WLC vérifiera l'utilisateur par rapport au groupe de serveurs et ne vérifiera pas sa base de données locale.

CLI :

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Type de groupe en tant que groupe et l'option de secours vers local est cochée.

IUG:

Si vous sélectionnez Group Type comme 'group' et que l'option fallback to local est activée, le WLC vérifiera l'utilisateur par rapport au groupe de serveurs et n'interrogera la base de données locale que si le serveur RADIUS expire dans la réponse. Si le serveur répond, le WLC ne déclenchera pas une authentification locale.

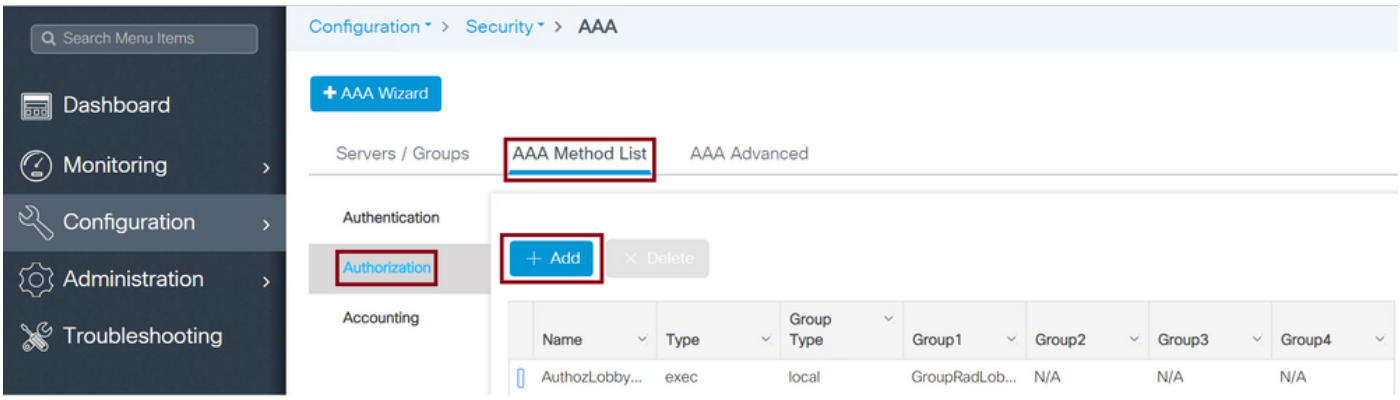
CLI :

```
Tim-eWLC1(config)#aaa authentication login AuthenLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

Étape 4. Créez une liste de méthodes d'autorisation. La liste des méthodes d'autorisation définit le type d'autorisation dont vous avez besoin pour le Lobby Ambassador qui, dans ce cas, sera 'exec'. Il sera également attaché au même groupe de serveurs défini. Il permet également de sélectionner si l'authentification sera effectuée localement sur le WLC ou externe à un serveur RADIUS.

IUG:

Accédez à **Configuration > Security > AAA > AAA Method List > Authorization > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre pour fournir un nom, sélectionnez l'option de type 'exec' et affectez le groupe de serveurs créé précédemment.

Sachez que le type de groupe s'applique de la même manière qu'il a été expliqué dans la section Authentication Method List.

CLI :

Type de groupe en tant que local.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod local group GroupRadLobby
Tim-eWLC1(config)#end
```

Type de groupe en tant que groupe.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby
Tim-eWLC1(config)#end
```

Le type de groupe en tant que groupe et l'option de secours vers local est cochée.

```
Tim-eWLC1(config)#aaa authorization exec AuthozLobbyMethod group GroupRadLobby local
Tim-eWLC1(config)#end
```

Étape 5. Attribuez les méthodes. Une fois les méthodes configurées, elles doivent être affectées aux options de connexion au WLC afin de créer l'utilisateur invité tel que line VTY (SSH/Telnet) ou HTTP (GUI).

Ces étapes ne peuvent pas être effectuées à partir de l'interface utilisateur graphique, donc elles doivent être effectuées à partir de l'interface de ligne de commande.

Authentification HTTP/GUI :

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AuthenLobbyMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozLobbyMethod
Tim-eWLC1(config)#end
```

Lorsque vous modifiez les configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS :

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

Ligne VTY.

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AuthenLobbyMethod
Tim-eWLC1(config-line)#authorization exec AuthozLobbyMethod
Tim-eWLC1(config-line)#end
```

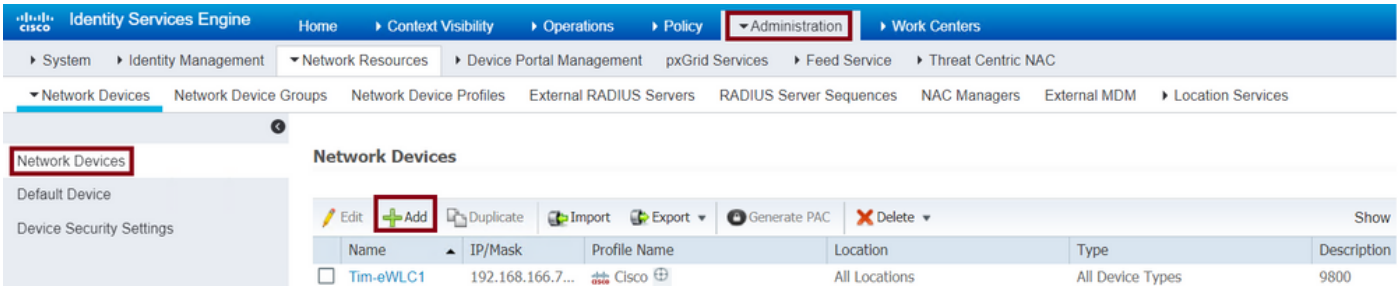
Étape 6. Cette étape n'est requise que dans les versions logicielles antérieures à 17.5.1 ou 17.3.3 et n'est pas requise après les versions où CSCvu29748 a été mis en oeuvre. Définissez l'utilisateur distant. Le nom d'utilisateur créé sur ISE pour le Lobby Ambassador doit être défini en tant que nom d'utilisateur distant sur le WLC. Si le nom d'utilisateur distant n'est pas défini dans le WLC, l'authentification passera correctement, cependant, l'utilisateur se verra accorder un accès complet au WLC au lieu de n'avoir accès qu'aux privilèges Lobby Ambassador. Cette configuration ne peut être effectuée que via l'interface de ligne de commande.

CLI :

```
Tim-eWLC1(config)#aaa remote username lobby
```

Configurer ISE - RADIUS

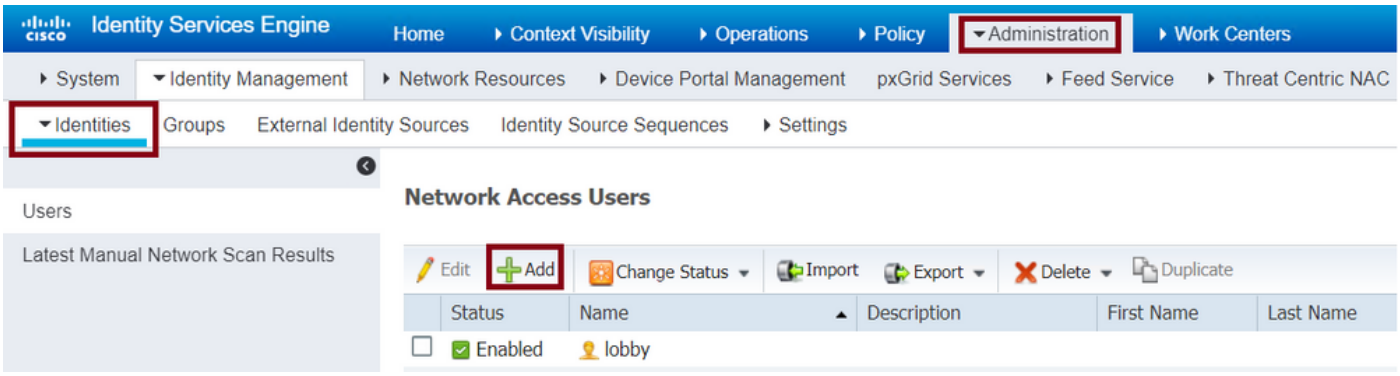
Étape 1. Ajoutez le WLC à ISE. Accédez à **Administration > Network Resources > Network Devices > Add**. Le WLC doit être ajouté à ISE. Lorsque vous ajoutez le WLC à ISE, activez les paramètres d'authentification RADIUS et configurez les paramètres nécessaires comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, indiquez un nom, IP ADD, activez les paramètres d'authentification RADIUS et, sous Protocol Radius, saisissez le secret partagé requis.

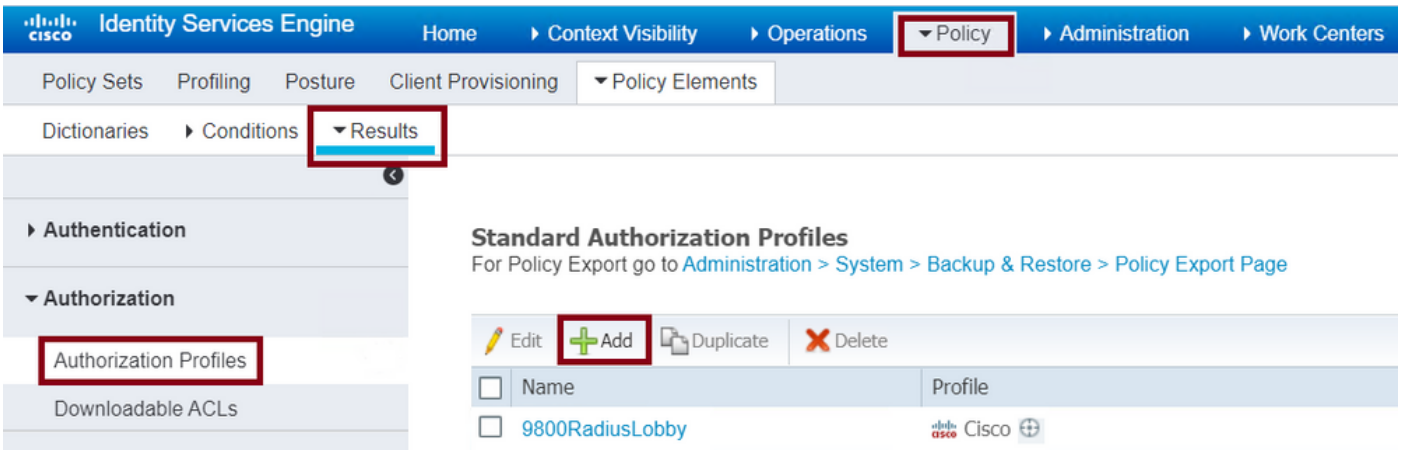
Étape 2. Créez l'utilisateur Lobby Ambassador sur ISE. Accédez à **Administration > Identity Management > Identities > Users > Add**.

Ajoutez à ISE le nom d'utilisateur et le mot de passe attribués à Lobby Ambassador qui crée les utilisateurs invités. Il s'agit du nom d'utilisateur que l'administrateur attribuera à l'ambassadeur du hall d'entrée.

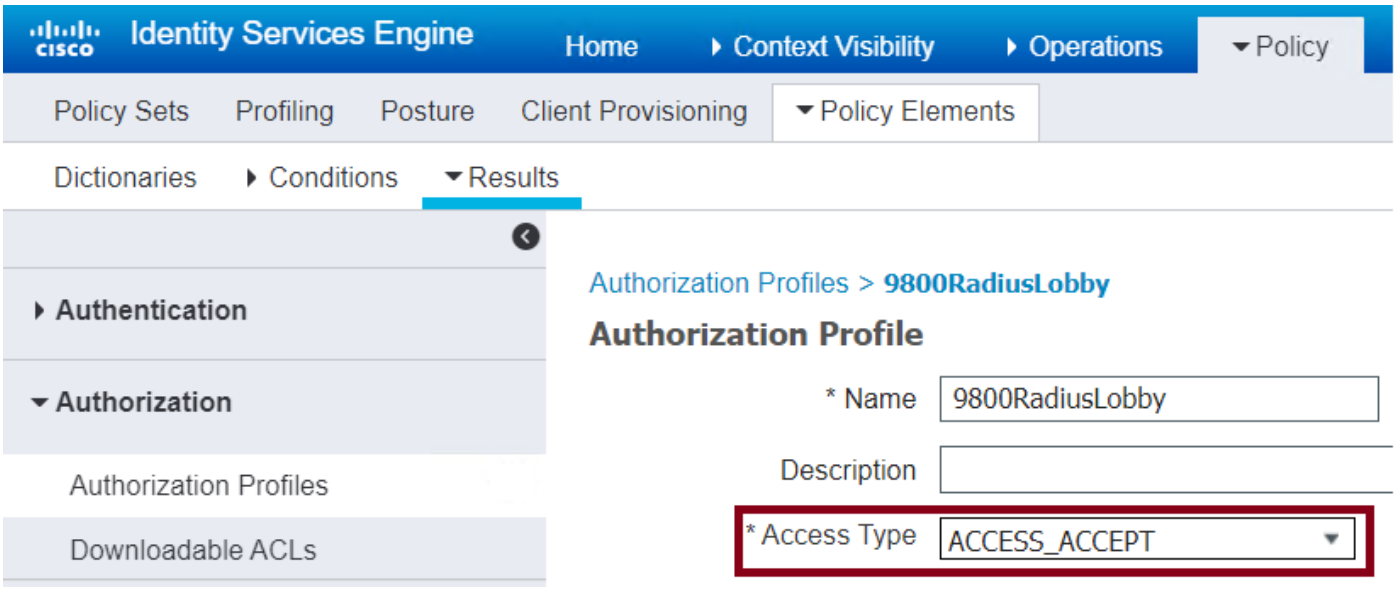


Lorsque la fenêtre de configuration s'ouvre, indiquez le nom et le mot de passe de l'utilisateur Lobby Ambassador. Vérifiez également que l'état est Activé.

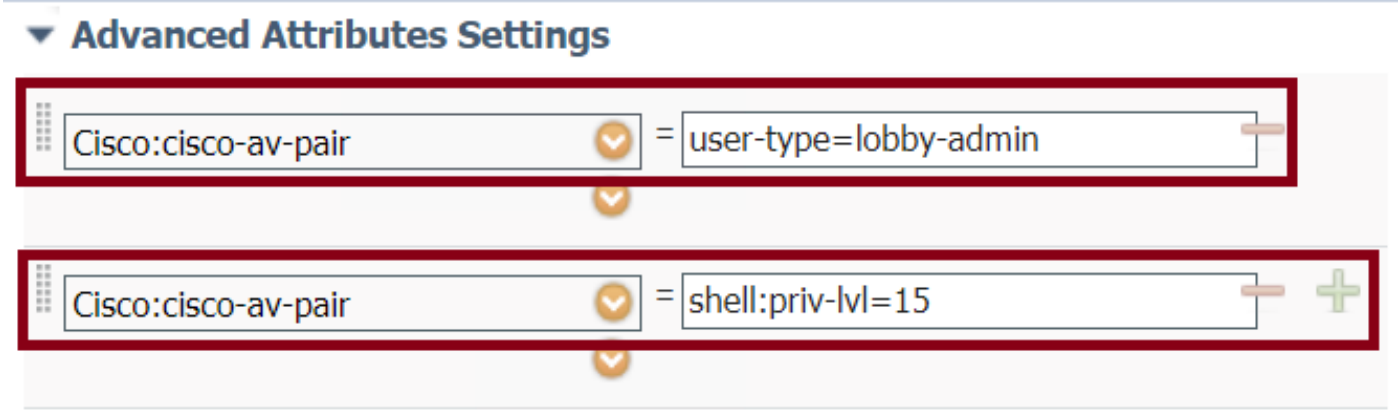
Étape 3. Créez un profil d'autorisation des résultats. Accédez à **Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation > Ajouter**. Créez un profil d'autorisation de résultat afin de retourner au WLC un Access-Accepcept avec les attributs nécessaires comme indiqué dans l'image.



Assurez-vous que le profil est configuré pour envoyer un Access-Accept comme indiqué dans l'image.



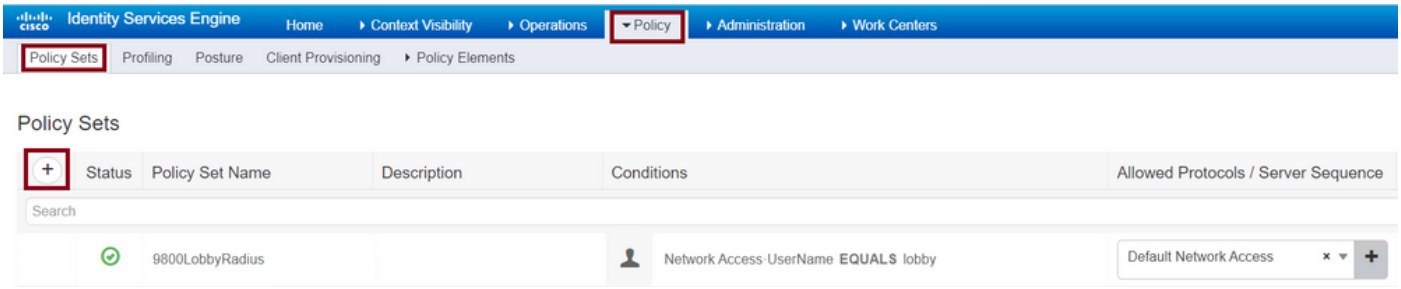
Vous devez ajouter les attributs manuellement sous Paramètres des attributs avancés. Les attributs sont nécessaires pour définir l'utilisateur comme Lobby Ambassador et pour fournir le privilège afin de permettre à Lobby Ambassador d'apporter les changements nécessaires.



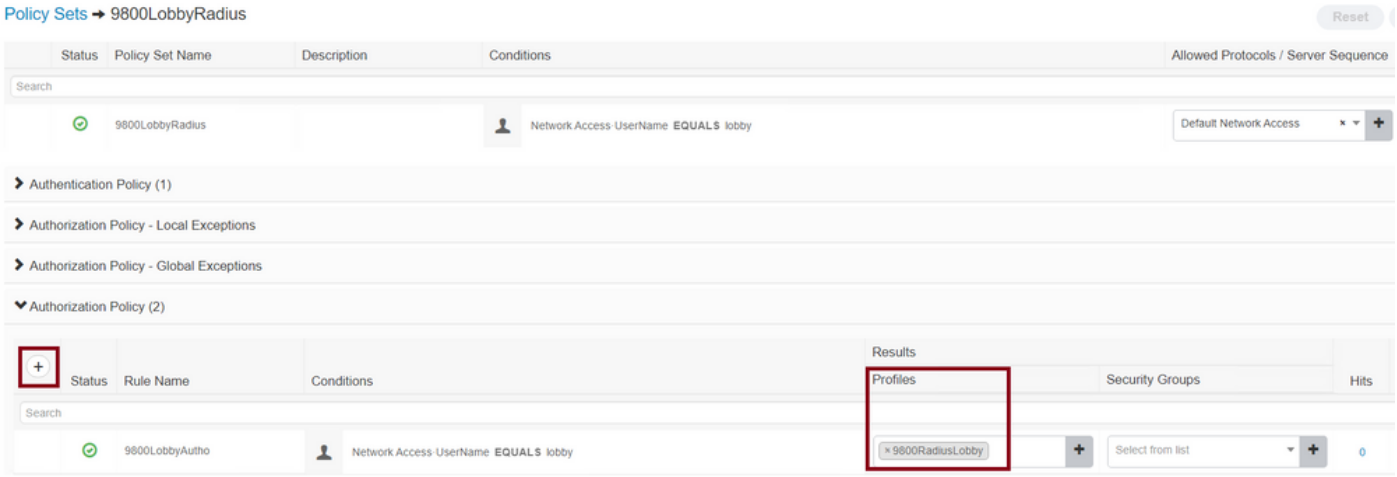
Étape 4. Créez une stratégie afin de traiter l'authentification. Accédez à **Stratégie > Jeux de stratégies > Ajouter**. Les conditions de configuration de la stratégie dépendent de la décision de l'administrateur. La condition Network Access-Username et le protocole Default Network Access sont utilisés ici.

Il est obligatoire de s'assurer, dans la stratégie d'autorisation, que le profil configuré sous l'autorisation des résultats est sélectionné, de sorte que vous pouvez renvoyer les attributs

nécessaires au WLC comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, configurez la stratégie d'autorisation. La stratégie d'authentification peut être laissée par défaut.



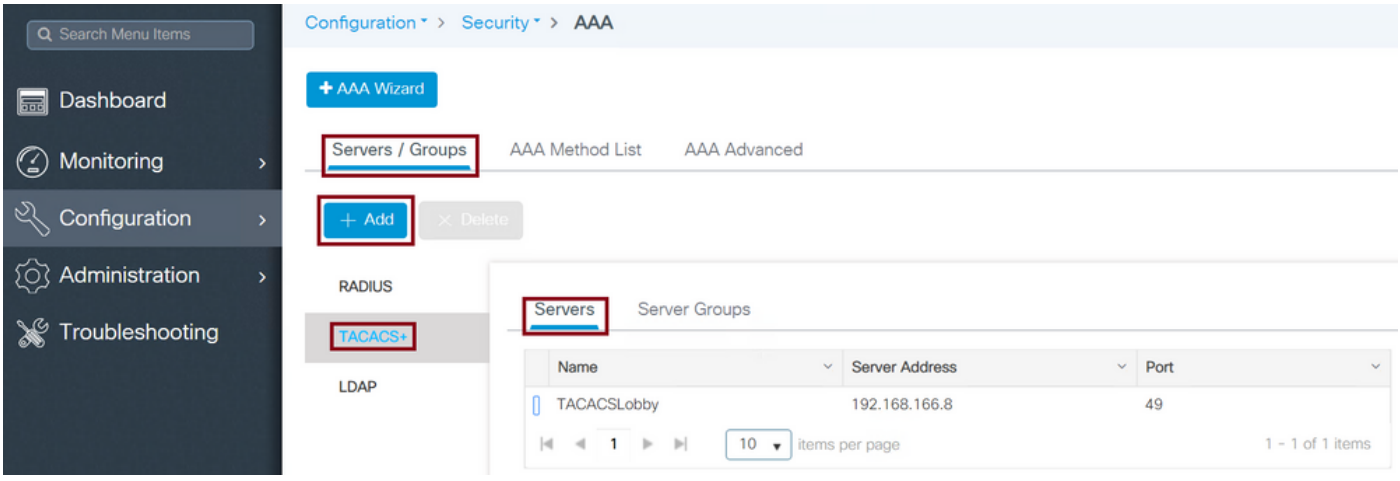
Authentifier TACACS+

Configurer TACACS+ sur WLC

Étape 1 : déclaration du serveur TACACS+ Créez le serveur ISE TACACS dans le WLC.

IUG:

Naviguez jusqu'à **Configuration > Security > AAA > Servers/Groups > TACACS+ > Servers > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, les paramètres de configuration obligatoires sont le nom du serveur TACACS+ (il ne doit pas nécessairement correspondre au nom système

ISE/AAA), l'ADRESSE IP du serveur TACACS et le secret partagé. Tous les autres paramètres peuvent être laissés par défaut ou configurés selon les besoins.

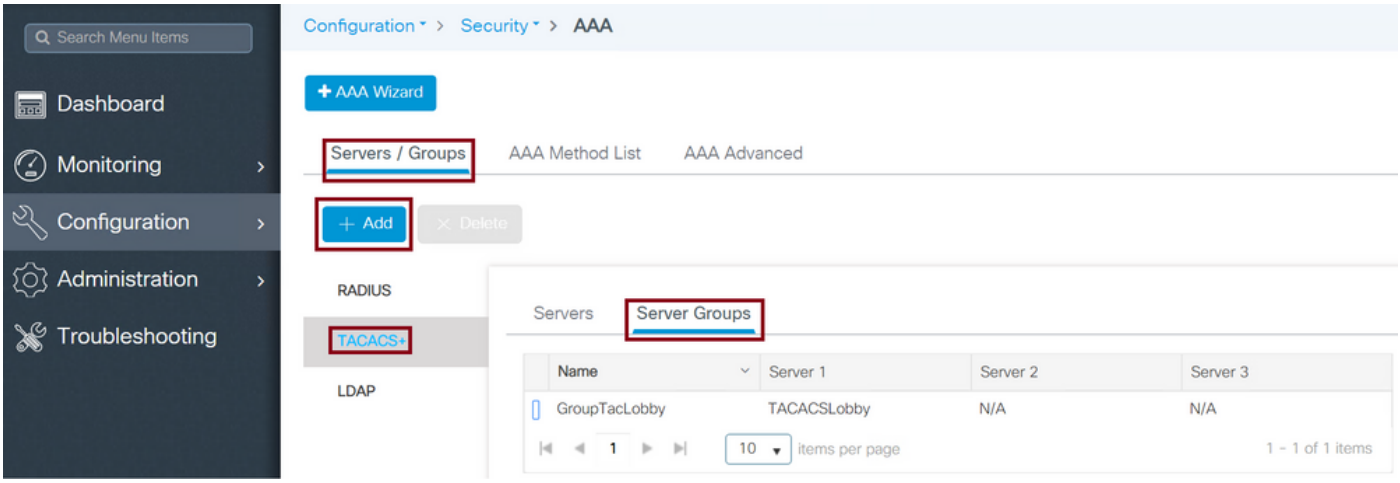
CLI :

```
Tim-eWLC1(config)#tacacs server TACACSLobby
Tim-eWLC1(config-server-tacacs)#address ipv4 192.168.166.8
Tim-eWLC1(config-server-tacacs)#key 0 Cisco123
Tim-eWLC1(config-server-tacacs)#end
```

Étape 2. Ajoutez le serveur TACACS+ à un groupe de serveurs. Définissez un groupe de serveurs et ajoutez le serveur TACACS+ souhaité configuré. Il s'agit des serveurs TACACS+ utilisés pour l'authentification.

IUG:

Accédez à **Configuration > Security > AAA > Servers / Groups > TACACS > Server Groups > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, donnez un nom au groupe et déplacez les serveurs TACACS+ souhaités de la liste Serveurs disponibles vers la liste Serveurs affectés.

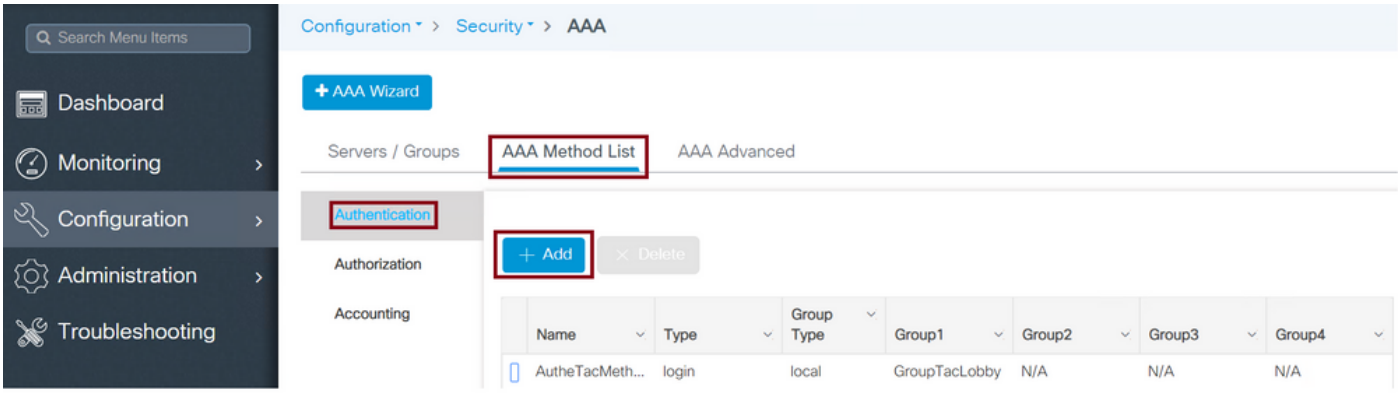
CLI :

```
Tim-eWLC1(config)#aaa group server tacacs+ GroupTacLobby
Tim-eWLC1(config-sg-tacacs+)#server name TACACSLobby
Tim-eWLC1(config-sg-tacacs+)#end
```

Étape 3. Créez une liste de méthodes d'authentification. La liste des méthodes d'authentification définit le type d'authentification qui est nécessaire et qui sera également associé au groupe de serveurs configuré. Il permet également de sélectionner si l'authentification peut être effectuée localement sur le WLC ou externe à un serveur TACACS+.

IUG:

Accédez à **Configuration > Security > AAA > AAA Method List > Authentication > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, indiquez un nom, sélectionnez l'option de type **Connexion** et affectez le groupe de serveurs créé précédemment.

Type de groupe en tant que local.

IUG:

Si vous sélectionnez le type de groupe comme 'local', le WLC vérifie d'abord si l'utilisateur existe dans la base de données locale et retourne ensuite au groupe de serveurs uniquement si l'utilisateur Lobby Ambassador n'est pas trouvé dans la base de données locale.

> **Note**: Veuillez être conscient de ce bogue CSCvs87163qui est fixé au point 17.3.

CLI :

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

Type de groupe en tant que groupe.

IUG:

Si vous sélectionnez le type de groupe en tant que groupe et qu'aucune option locale de secours n'est activée, le WLC vérifiera l'utilisateur par rapport au groupe de serveurs et ne vérifiera pas sa base de données locale.

CLI :

```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Le type de groupe en tant que groupe et l'option de secours vers local est cochée.

IUG:

Si vous sélectionnez le type de groupe 'group' et que l'option de restauration locale est activée, le WLC vérifiera l'utilisateur par rapport au groupe de serveurs et n'interrogera la base de données locale que si le serveur TACACS expire dans la réponse. Si le serveur envoie un rejet, l'utilisateur ne sera pas authentifié, même s'il existe dans la base de données locale.

CLI :

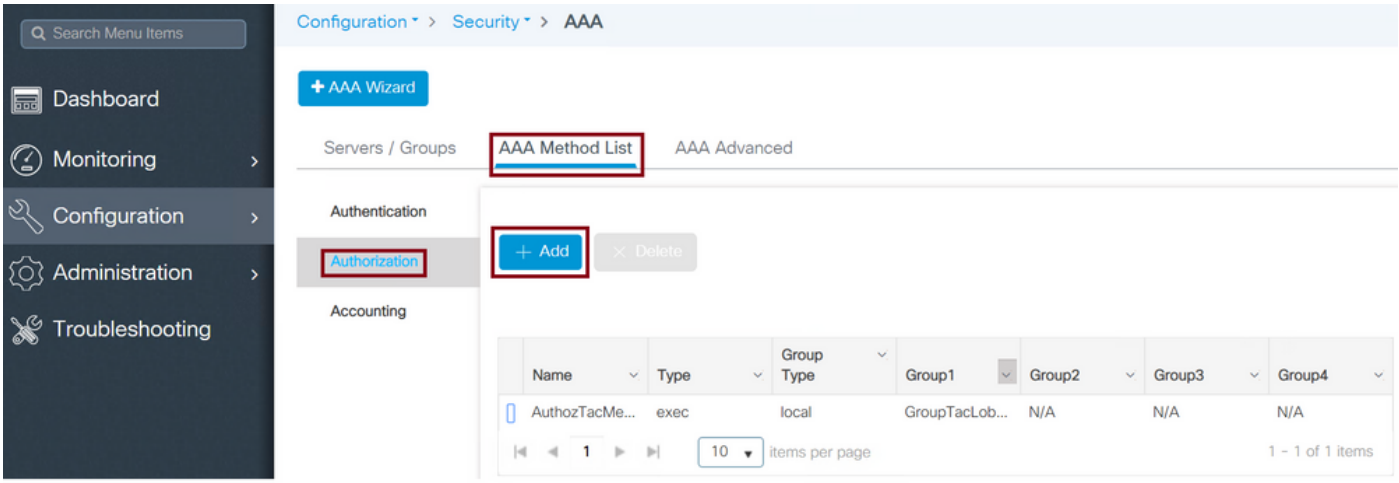
```
Tim-eWLC1(config)#aaa authentication login AutheTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Étape 4. Créez une liste de méthodes d'autorisation.

La liste des méthodes d'autorisation définit le type d'autorisation nécessaire pour le Lobby Ambassador qui, dans ce cas, sera exec. Il est également attaché au même groupe de serveurs configuré. Il est également autorisé à sélectionner si l'authentification est effectuée localement sur le WLC ou externe à un serveur TACACS+.

IUG:

Accédez à **Configuration > Security > AAA > AAA Method List > Authorization > + Add** comme indiqué dans l'image.



Lorsque la fenêtre de configuration s'ouvre, indiquez un nom, sélectionnez l'option de type exec et affectez le groupe de serveurs créé précédemment.

N'oubliez pas que le type de groupe s'applique de la même manière qu'il est expliqué dans la partie de la liste des méthodes d'authentification.

CLI :

Type de groupe en tant que local.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod local group GroupTacLobby
Tim-eWLC1(config)#end
```

Type de groupe en tant que groupe.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby
Tim-eWLC1(config)#end
```

Le type de groupe en tant que groupe et l'option de retour arrière vers local sont cochés.

```
Tim-eWLC1(config)#aaa authorization exec AuthozTacMethod group GroupTacLobby local
Tim-eWLC1(config)#end
```

Étape 5. Attribuez les méthodes. Une fois les méthodes configurées, elles doivent être affectées aux options afin de se connecter au WLC pour créer l'utilisateur invité tel que la ligne VTY ou HTTP (GUI). Ces étapes ne peuvent pas être effectuées à partir de l'interface utilisateur

graphique, donc elles doivent être effectuées à partir de l'interface de ligne de commande.

Authentification HTTP/GUI :

```
Tim-eWLC1(config)#ip http authentication aaa login-authentication AutheTacMethod
Tim-eWLC1(config)#ip http authentication aaa exec-authorization AuthozTacMethod
Tim-eWLC1(config)#end
```

Lorsque vous apportez des modifications aux configurations HTTP, il est préférable de redémarrer les services HTTP et HTTPS :

```
Tim-eWLC1(config)#no ip http server
Tim-eWLC1(config)#no ip http secure-server
Tim-eWLC1(config)#ip http server
Tim-eWLC1(config)#ip http secure-server
Tim-eWLC1(config)#end
```

Ligne VTY :

```
Tim-eWLC1(config)#line vty 0 15
Tim-eWLC1(config-line)#login authentication AutheTacMethod
Tim-eWLC1(config-line)#authorization exec AuthozTacMethod
Tim-eWLC1(config-line)#end
```

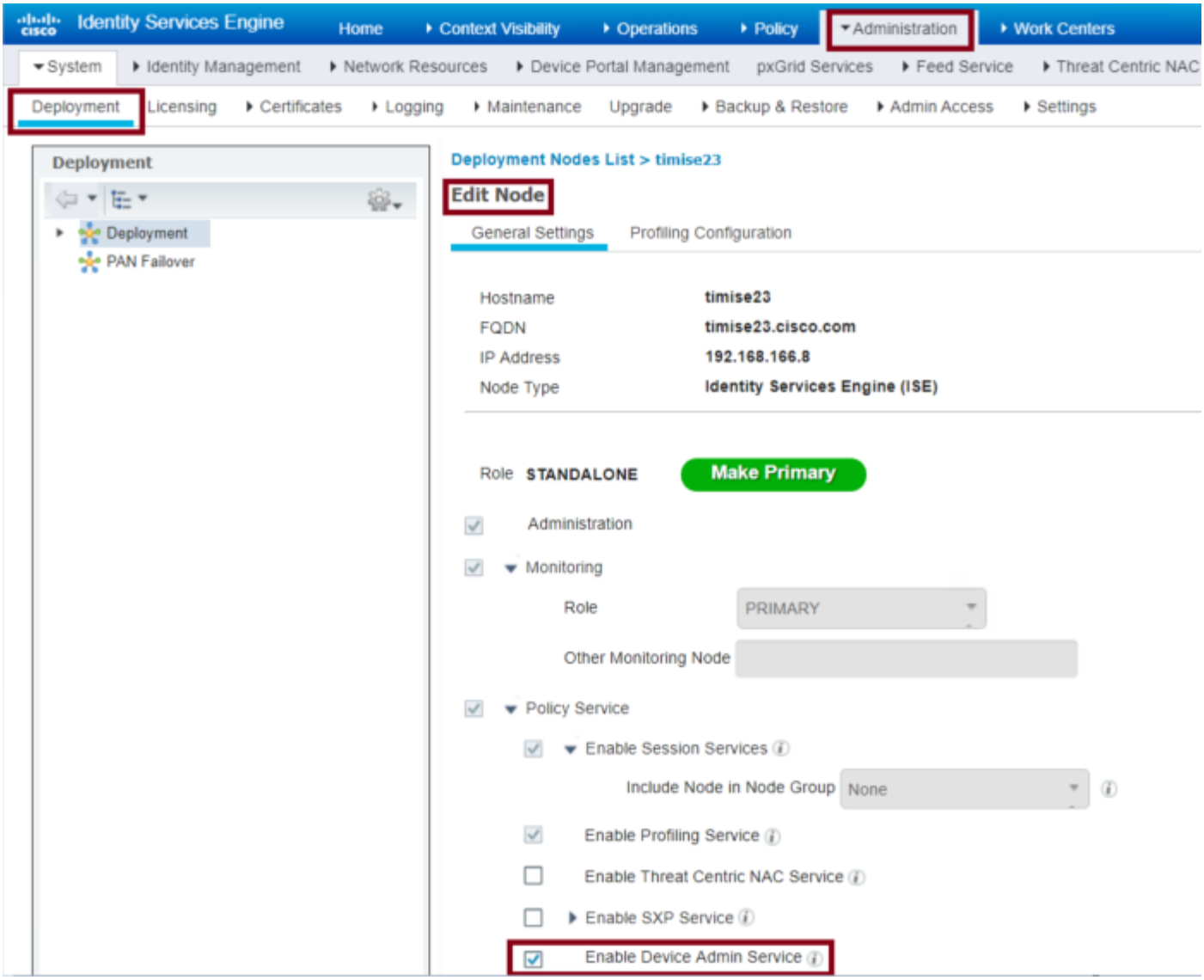
Étape 6. Définissez l'utilisateur distant. Le nom d'utilisateur créé sur ISE pour le Lobby Ambassador doit être défini en tant que nom d'utilisateur distant sur le WLC. Si le nom d'utilisateur distant n'est pas défini dans le WLC, l'authentification passera correctement, cependant, l'utilisateur se verra accorder un accès complet au WLC au lieu de n'avoir accès qu'aux privilèges Lobby Ambassador. Cette configuration ne peut être effectuée que via l'interface de ligne de commande.

CLI :

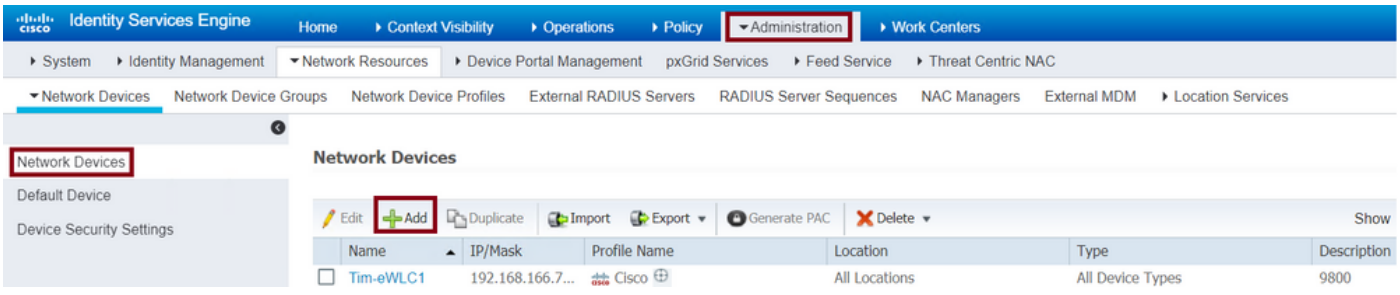
```
Tim-eWLC1(config)#aaa remote username lobbyTac
```

Configurer ISE - TACACS+

Étape 1. Activer l'administrateur du périphérique Accédez à **Administration > System > Deployment**. Avant de continuer, sélectionnez **Activer le service d'administration de périphériques** et assurez-vous que ISE a été activé comme indiqué dans l'image.

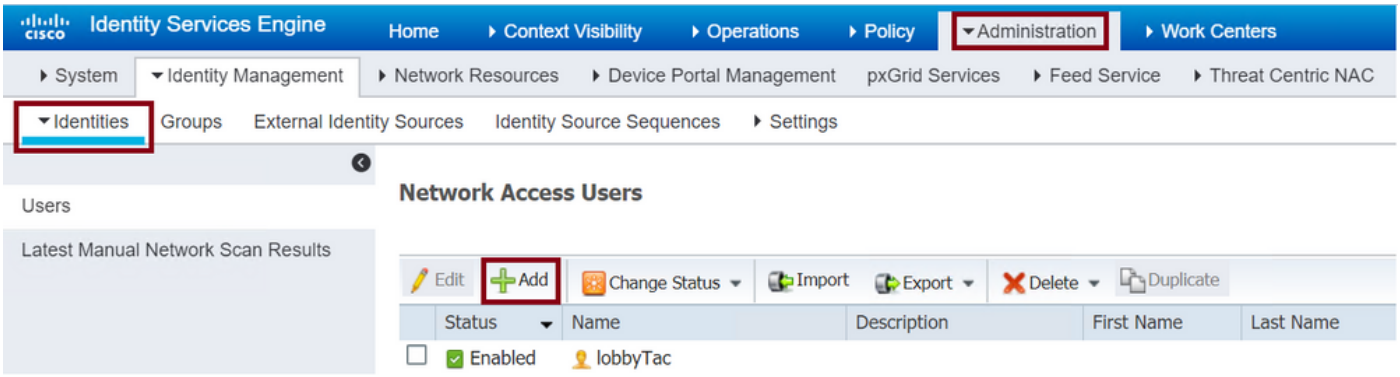


Étape 2. Ajoutez le WLC à ISE. Accédez à **Administration > Network Resources > Network Devices > Add**. Le WLC doit être ajouté à ISE. Lorsque vous ajoutez le WLC à ISE, activez les paramètres d'authentification TACACS+ et configurez les paramètres nécessaires comme indiqué dans l'image.



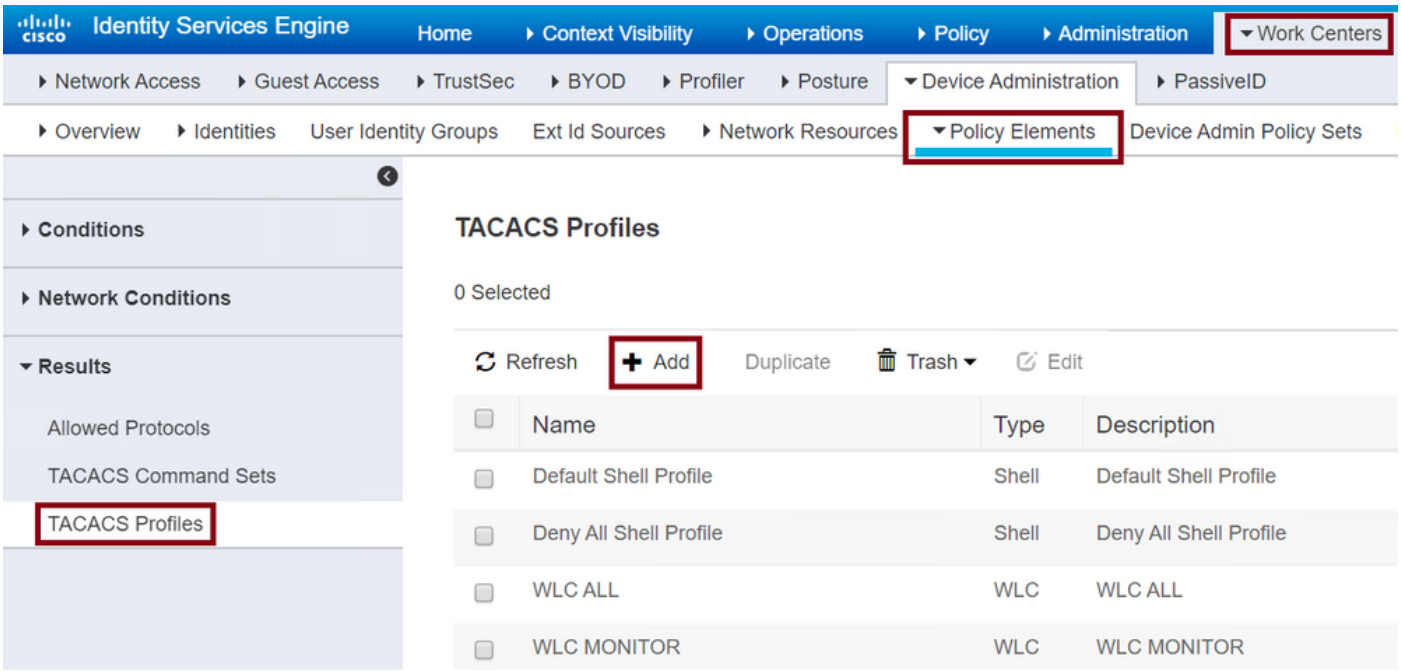
Lorsque la fenêtre de configuration s'ouvre pour fournir un nom, IP ADD, activez les paramètres d'authentification TACACS+ et saisissez le secret partagé nécessaire.

Étape 3. Créez l'utilisateur Lobby Ambassador sur ISE. Accédez à **Administration > Identity Management > Identities > Users > Add**. Ajoutez à ISE le nom d'utilisateur et le mot de passe attribués à Lobby Ambassador qui créera les utilisateurs invités. Il s'agit du nom d'utilisateur que l'administrateur attribue à l'ambassadeur du hall d'entrée, comme illustré sur l'image.

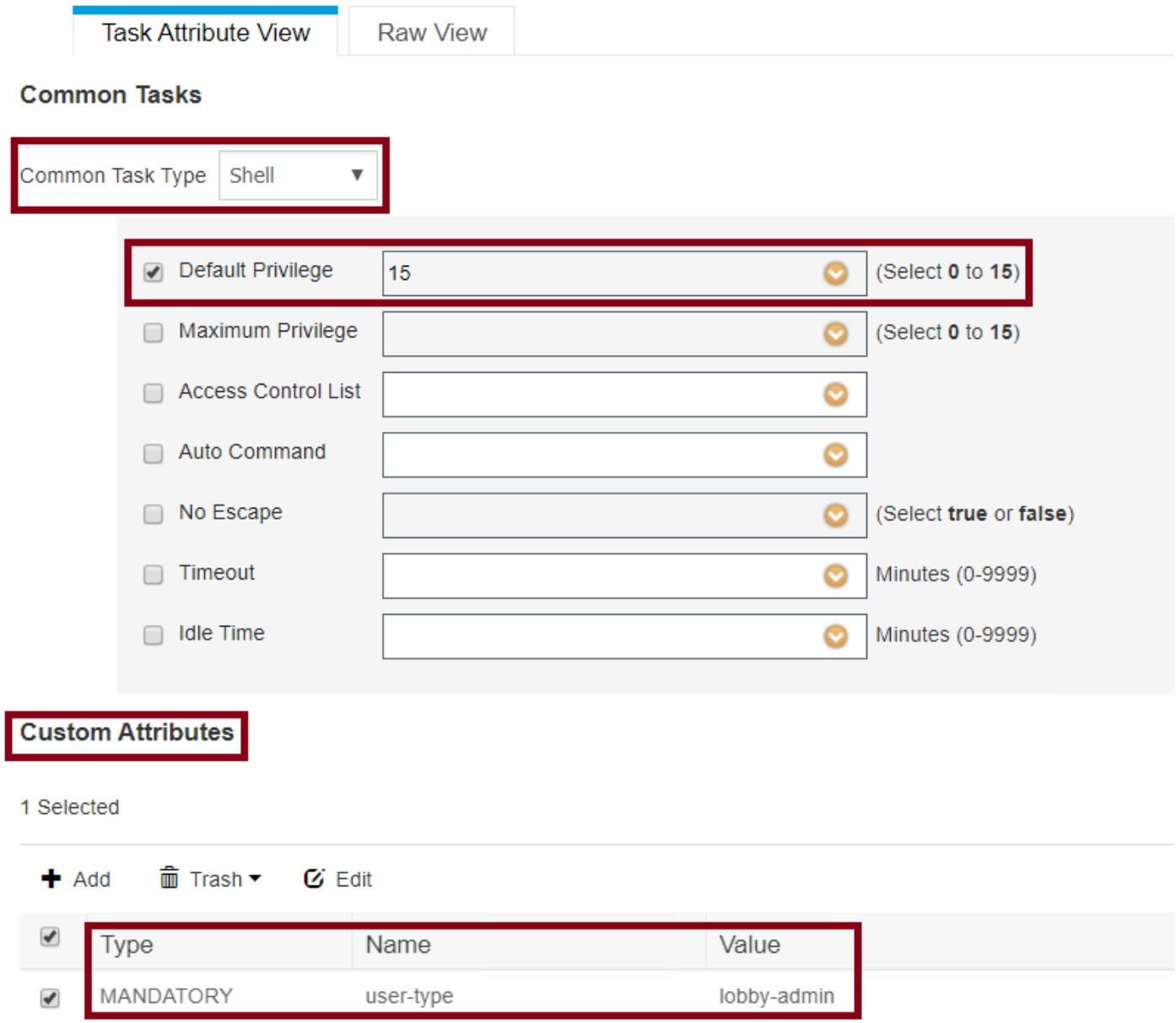


Lorsque la fenêtre de configuration s'ouvre, indiquez le nom et le mot de passe de l'utilisateur Lobby Ambassador. Vérifiez également que l'état est Activé.

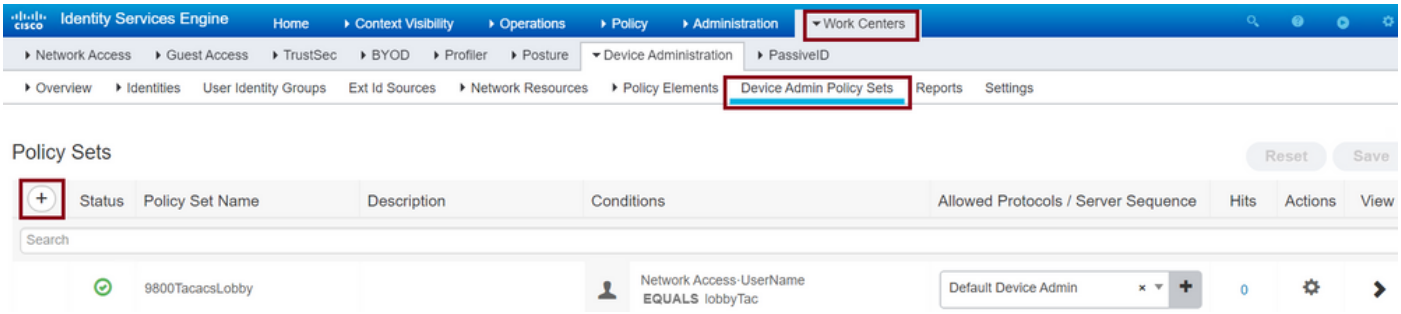
Étape 4. Créez un profil TACACS+ de résultats. Accédez à **Centres de travail > Administration des périphériques > Eléments de stratégie > Résultats > Profils TACACS** comme indiqué dans l'image. Avec ce profil, renvoyez les attributs nécessaires au WLC afin de placer l'utilisateur en tant qu'ambassadeur de hall d'entrée.



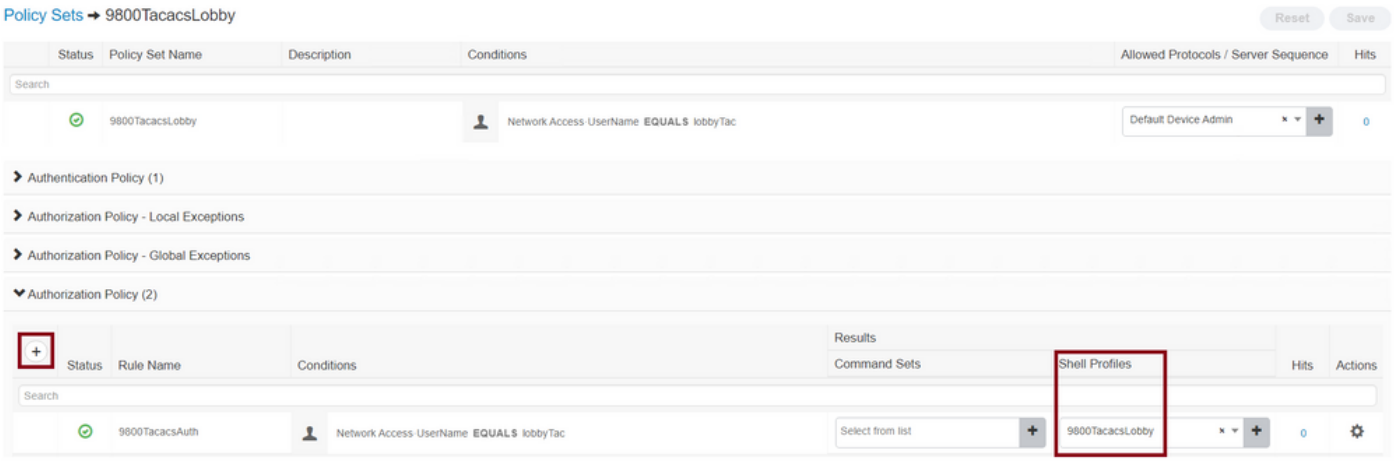
Lorsque la fenêtre de configuration s'ouvre, indiquez un nom pour le profil, configurez également un paramètre Privilégié par défaut 15 et un attribut personnalisé comme type obligatoire, nom comme type utilisateur et valeur hall-admin. Laissez également le **type de tâche commun** être sélectionné en tant que Shell comme indiqué dans l'image.



Étape 5. Créer un jeu de stratégies. Accédez à **Centres de travail > Administration des périphériques > Jeux de stratégies d'administration des périphériques** comme indiqué dans l'image. Les conditions de configuration de la stratégie dépendent de la décision de l'administrateur. Pour ce document, la condition Network Access-Username et le protocole Default Device Admin sont utilisés. Il est obligatoire de s'assurer, dans le cadre de la stratégie d'autorisation, que le profil configuré dans le cadre de l'autorisation des résultats est sélectionné, de sorte que vous pouvez renvoyer les attributs nécessaires au WLC.



Lorsque la fenêtre de configuration s'ouvre, configurez la stratégie d'autorisation. La stratégie d'authentification peut être laissée par défaut, comme l'illustre l'image.

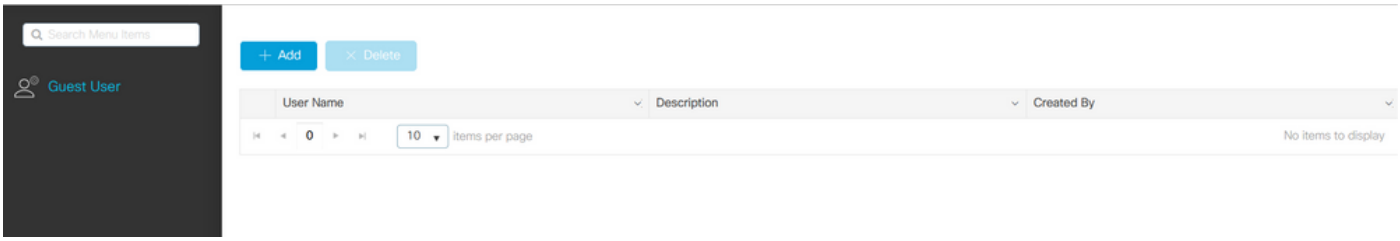


Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

```
show run aaa
show run | sec remote
show run | sec http
show aaa method-lists authentication
show aaa method-lists authorization
show aaa servers
show tacacs
```

Voici à quoi ressemble l'interface utilisateur graphique de Lobby Ambassador après une authentification réussie.



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Authentifier RADIUS

Pour l'authentification RADIUS, ces débogages peuvent être utilisés :

```
Tim-eWLC1#debug aaa authentication
Tim-eWLC1#debug aaa authorization
Tim-eWLC1#debug aaa attr
Tim-eWLC1#terminal monitor
```

Assurez-vous que la bonne liste de méthodes est sélectionnée dans le débogage. En outre, les attributs requis sont retournés par le serveur ISE avec le nom d'utilisateur, le type d'utilisateur et le privilège appropriés.

```
Feb 5 02:35:27.659: AAA/AUTHEN/LOGIN (00000000): Pick method list 'AuthenLobbyMethod'
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(0):
7FBA5500C870 0 00000081 username(450) 5 lobby
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(1):
7FBA5500C8B0 0 00000001 user-type(1187) 4 lobby-admin
Feb 5 02:35:27.681: ADD-DELETE: AAA/ATTR(00000000): add attr: sublist(0x7FBA5500C860) index(2):
7FBA5500C8F0 0 00000001 priv-lvl(335) 4 15(F)
Feb 5 02:35:27.683: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host
192.168.166.104 by user 'lobby' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
```

Authentifier TACACS+

Pour l'authentification TACACS+, ce débogage peut être utilisé :

```
Tim-eWLC1#debug tacacs
Tim-eWLC1#terminal monitor
```

Assurez-vous que l'authentification est traitée avec le nom d'utilisateur et l'ADD IP ISE appropriés. En outre, l'état « PASS » doit être vu. Dans le même débogage, juste après la phase d'authentification, le processus d'autorisation sera présenté. Dans cette autorisation, la phase s'assure que le nom d'utilisateur approprié est utilisé avec l'ADD IP ISE approprié. À partir de cette phase, vous devriez être en mesure de voir les attributs configurés sur ISE qui indiquent le WLC en tant qu'utilisateur Lobby Ambassador avec le privilège approprié.

Exemple de phase d'authentification :

```
Feb 5 02:06:48.245: TPLUS: Queuing AAA Authentication request 0 for processing
Feb 5 02:06:48.245: TPLUS: Authentication start packet created for 0(lobbyTac)
Feb 5 02:06:48.245: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.250: TPLUS: Received authen response status GET_PASSWORD (8)
Feb 5 02:06:48.266: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.266: TPLUS: Received authen response status PASS (2)
```

Exemple de phase d'autorisation :

```
Feb 5 02:06:48.267: TPLUS: Queuing AAA Authorization request 0 for processing
Feb 5 02:06:48.267: TPLUS: Authorization request created for 0(lobbyTac)
Feb 5 02:06:48.267: TPLUS: Using server 192.168.166.8
Feb 5 02:06:48.279: TPLUS(00000000)/0/7FB7819E2100: Processing the reply packet
Feb 5 02:06:48.279: TPLUS: Processed AV priv-lvl=15
Feb 5 02:06:48.279: TPLUS: Processed AV user-type=lobby-admin
Feb 5 02:06:48.279: TPLUS: received authorization response for 0: PASS
```

Les exemples de débogage mentionnés précédemment pour RADIUS et TACACS+ ont les étapes clés pour une connexion réussie. Les débogages sont plus détaillés et le résultat sera plus grand. Afin de désactiver les débogages, cette commande peut être utilisée :

```
Tim-eWLC1#undebug all
```