Configurez l'authentification de la perfection 3.1 TACACS contre ISE 2.x

Contenu

Introduction

Ce document décrit comment configurer l'infrastructure principale pour authentifier par l'intermédiaire de TACACS avec ISE 2.x.

Conditions requises

Cisco recommande que vous ayez une connaissance de base de ces thèmes :

- Cisco Identity Services Engine (ISE)
- Infrastructure principale

Configurez

Cisco Prime Network Control System 3.1

Engine 2.0 de gestion d'identité de Cisco ou plus tard.

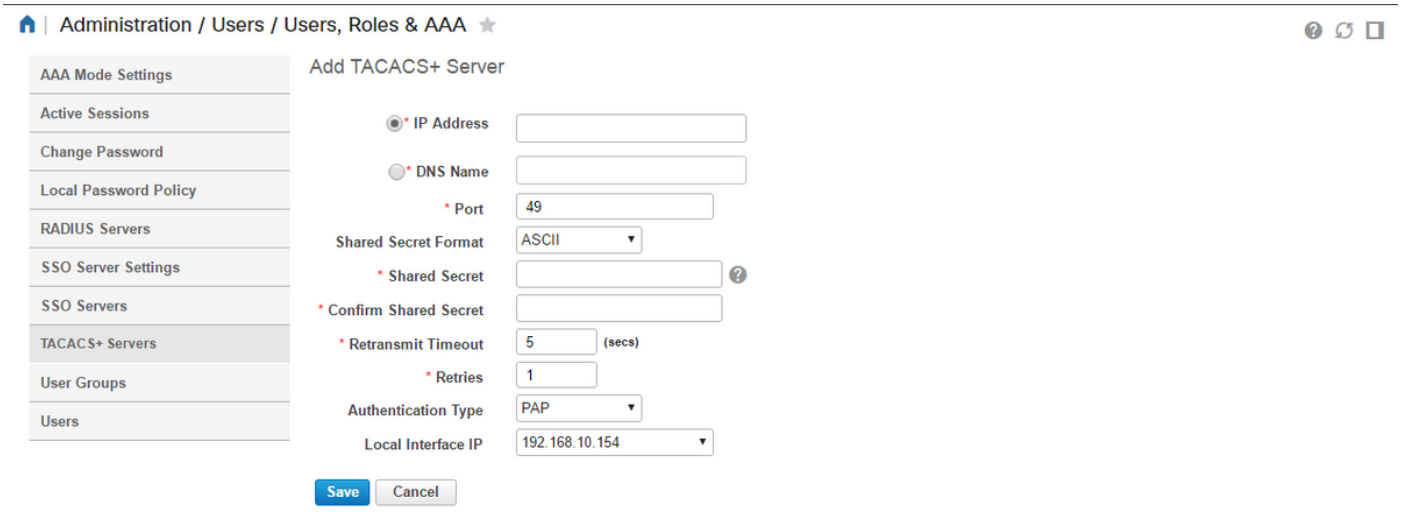
(Note : ISE prend en charge seulement TACACS commençant par la version 2.0, cependant il est possible de configurer la perfection utiliser Radius. La perfection inclut la liste d'attributs RADIUS en plus de TACACS si vous préféreriez utiliser Radius, avec une version plus ancienne d'ISE ou d'une solution de tiers.)

Configuration principale

Navigiate à l'écran suivant : Gestion/utilisateurs, rôles et AAA d'utilisateurs comme vu ci-dessous.

Une fois que là, sélectionnent l'onglet de serveurs TACACS+, puis sélectionnez l'option de serveur de l'ajouter TACACS+ dans le coin supérieur droit et choisi allez.

Sur l'écran suivant la configuration de l'entrée de serveur TACACS est disponible (ceci devra être faite pour chaque serveur TACACS individuel)



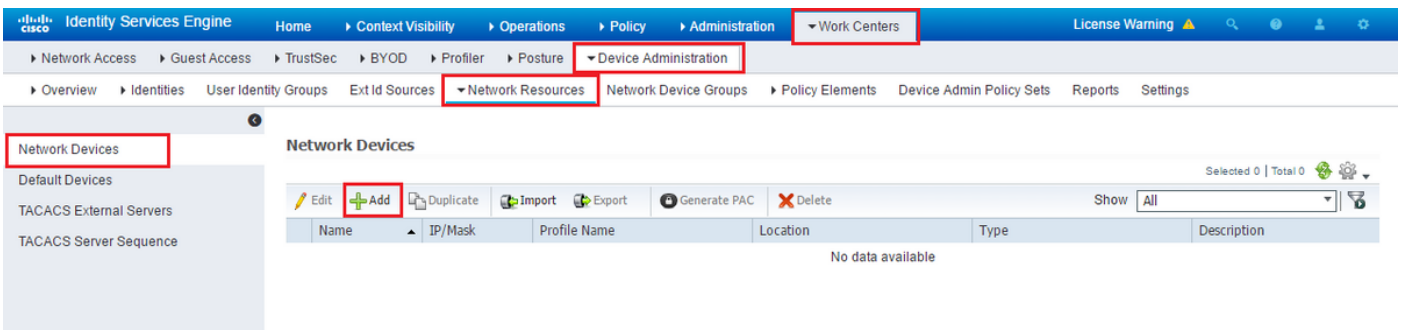
Voici que vous devrez introduire l'adresse IP ou l'adresse DNS du serveur, aussi bien que la clé secrète partagée. Veuillez également notent l'IP d'interface locale que vous voudriez utiliser, comme cette même adresse IP doit être utilisée pour le client d'AAA dans ISE plus tard.

Afin de se terminer la configuration sur la perfection. Vous devrez activer TACACS sous la gestion/utilisateurs/utilisateurs, les rôles et l'AAA sous l'onglet de configurations de mode d'AAA.

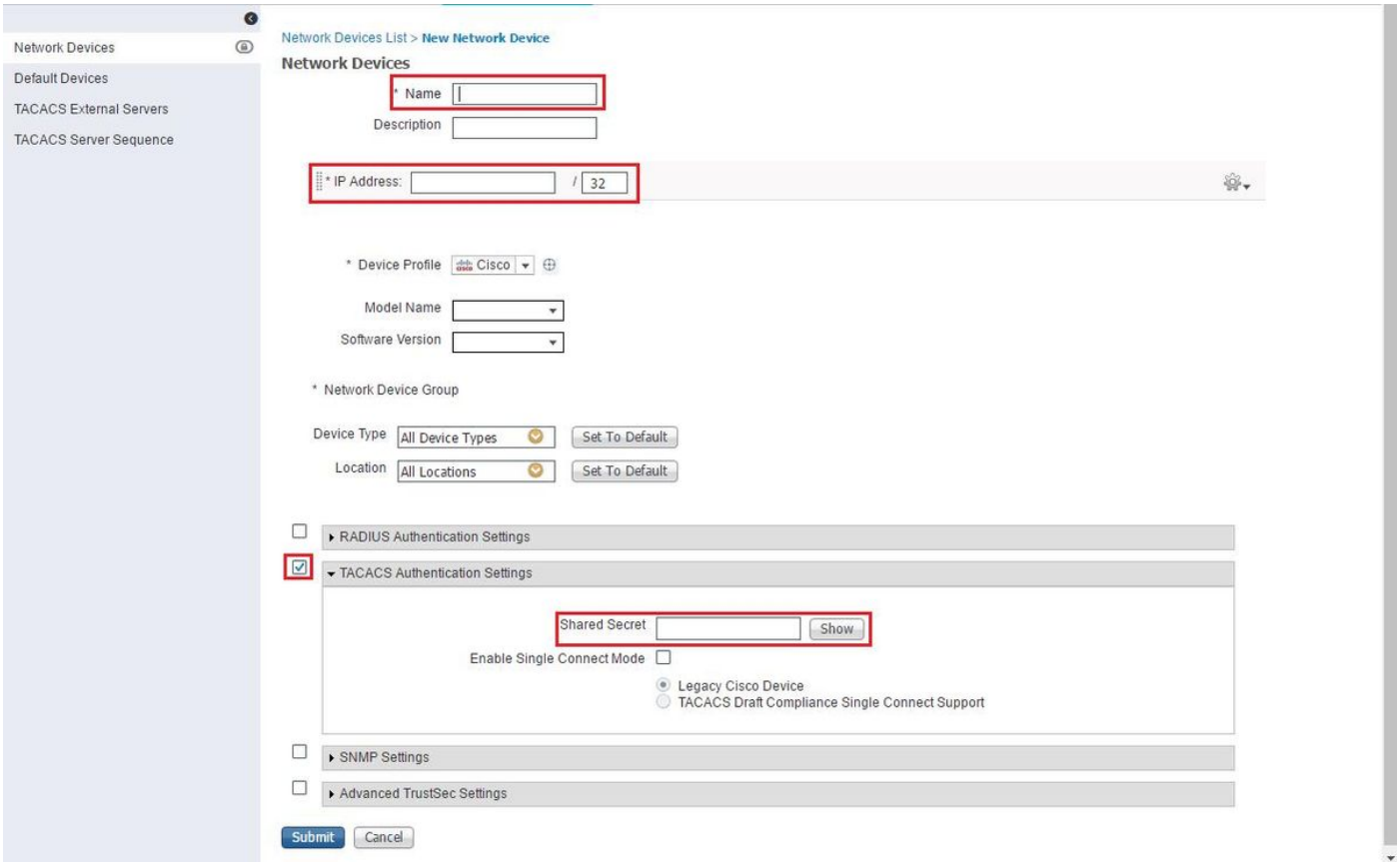
(Note : Il est recommandé pour vérifier le retour d'enable à l'option locale, avec SEULEMENT en aucune réponse de serveur ou en fonction l'aucune option de réponse ou de panne, particulièrement tout en testant la configuration)

Configuration ISE

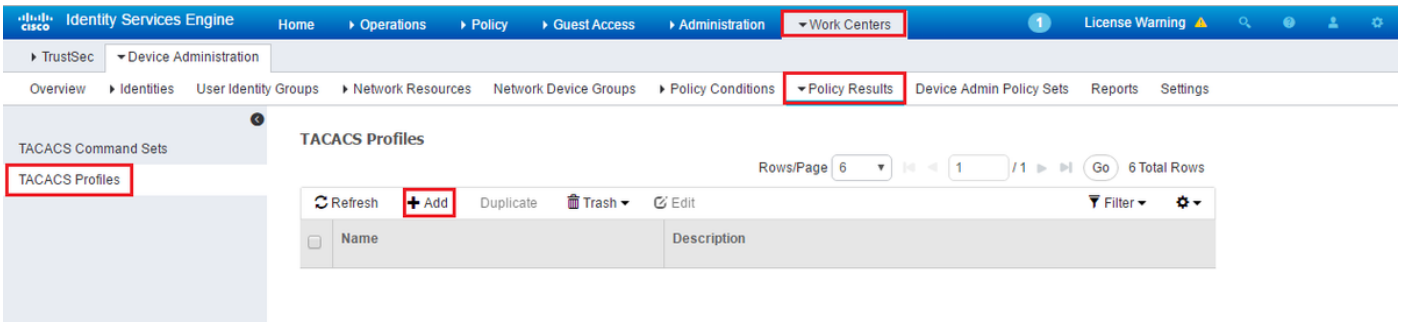
Configurez la perfection en tant que client d'AAA sur ISE aux centres de travail/à gestion de périphérique/aux ressources de réseau/aux périphériques de réseau/ajoutez



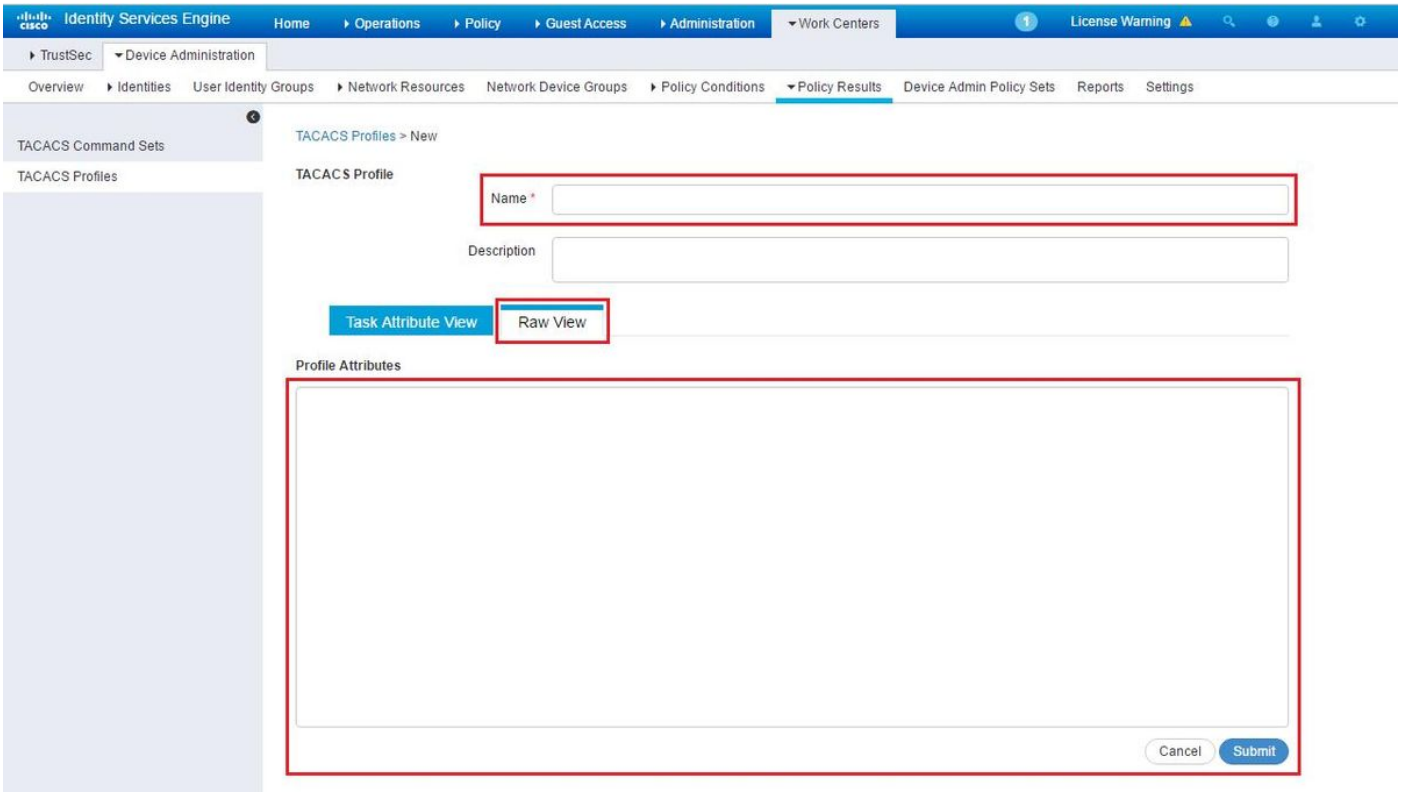
Écrivez les informations pour le serveur principal. Les attributs exigés que vous devez inclure sont nom, adresse IP, sélectionnent l'option pour TACACS et le secret partagé. Vous pouvez supplémentaire souhaiter ajouter un type de périphérique, spécifiquement pour la perfection, afin d'utiliser plus tard comme condition pour la règle d'autorisation ou d'autres informations, toutefois c'est facultative.



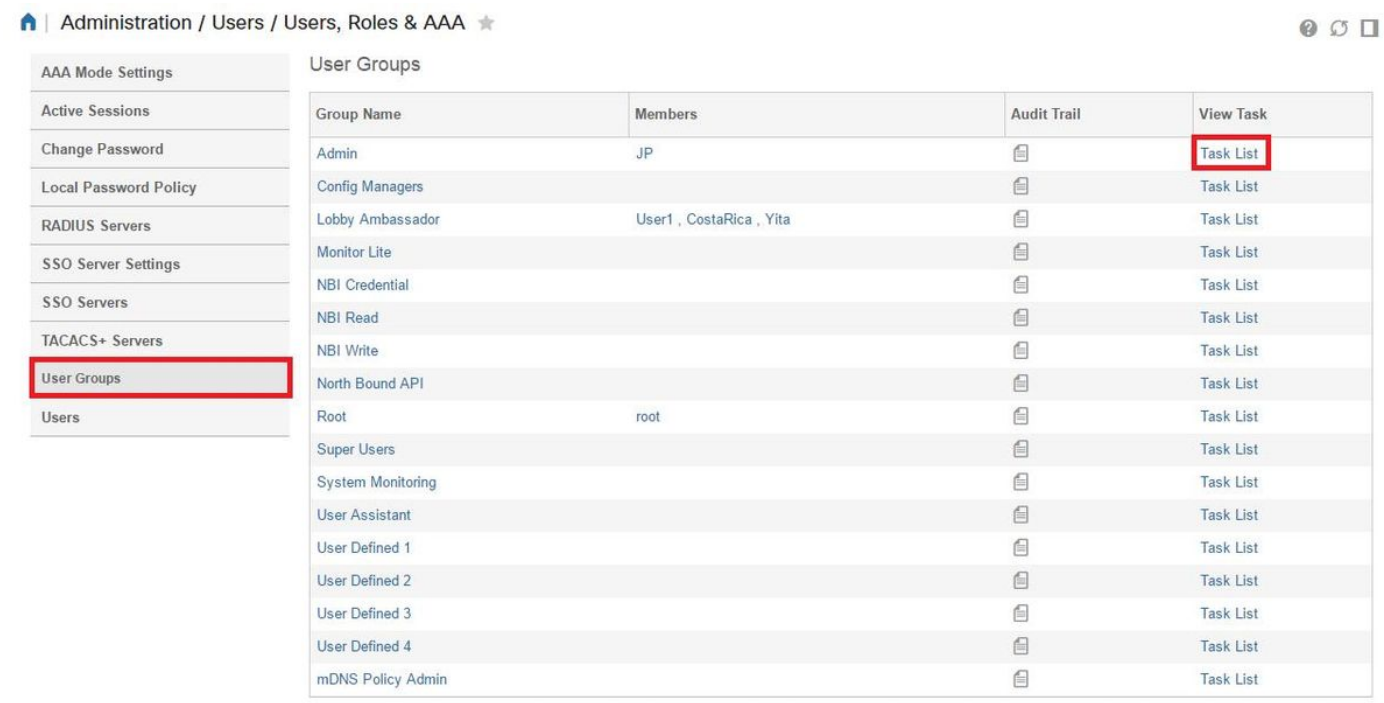
Créez alors un résultat de profil TACACS pour envoyer les attributs requis d'ISE pour amorcer, pour fournir le niveau d'accès correct. Naviguez vers des centres de travail/résultats de stratégie/profils de Tacacs et sélectionnez l'option d'ajouter.



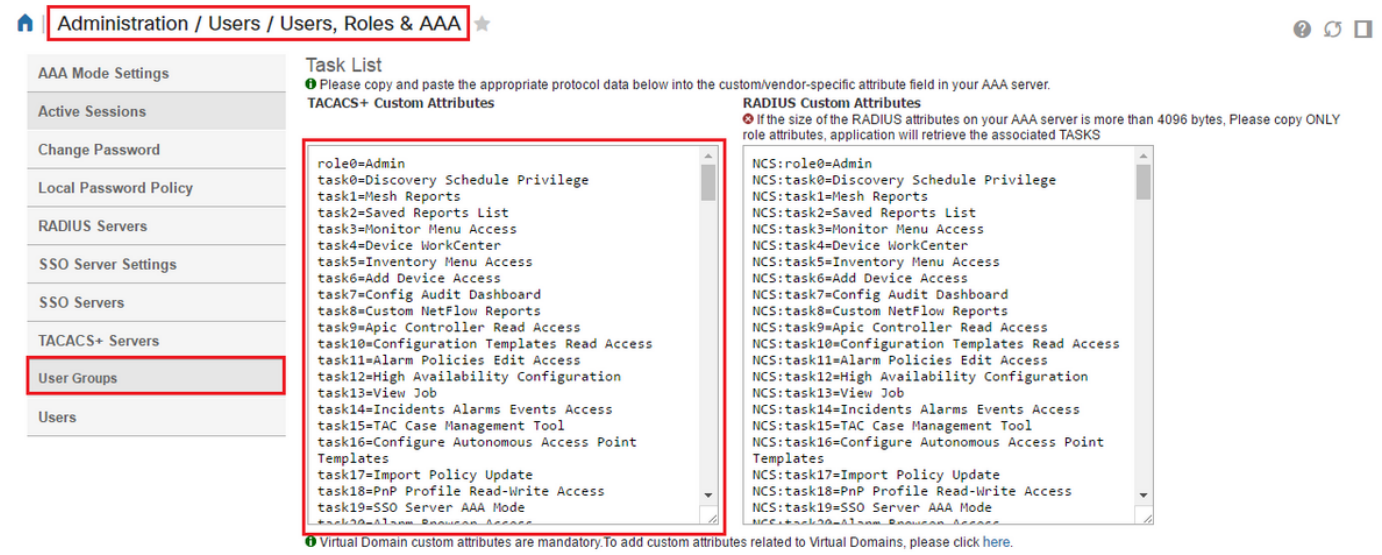
Configurez le nom, et employez l'option crue de vue afin d'écrire les attributs sous la case d'attributs de profil. Les attributs proviendront le serveur d'amorce lui-même.



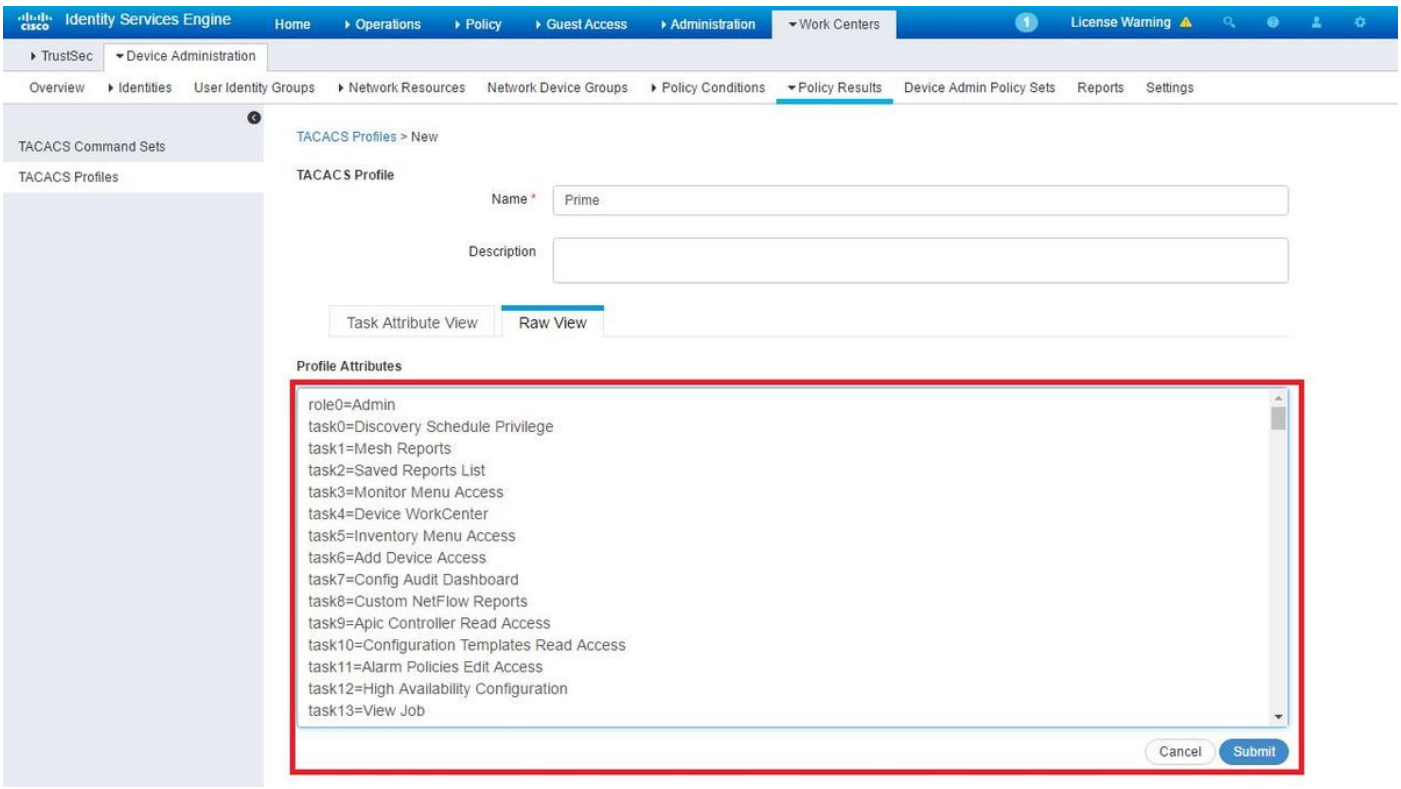
Obtenez les attributs sous la gestion/utilisateurs d'utilisateurs, les rôles et l'écran d'AAA, et sélectionnez l'onglet de groupes d'utilisateurs. Voici que vous sélectionnez le niveau du groupe de l'accès que vous souhaitez fournir. Dans cet admin d'exemple l'accès est fourni en sélectionnant la liste des tâches appropriée du côté gauche.



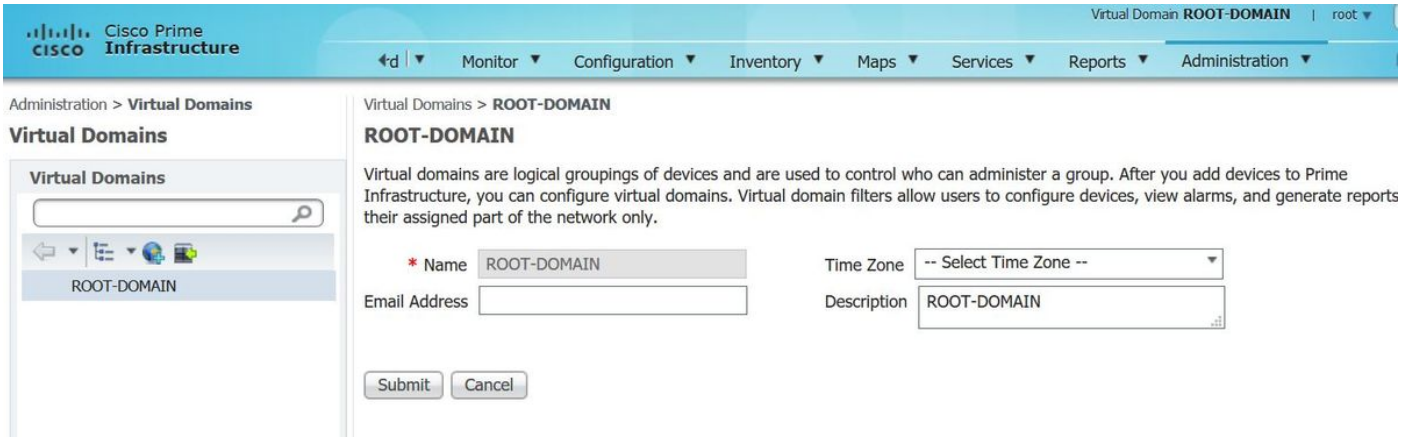
Copiez tous les attributs personnalisés TACACS.



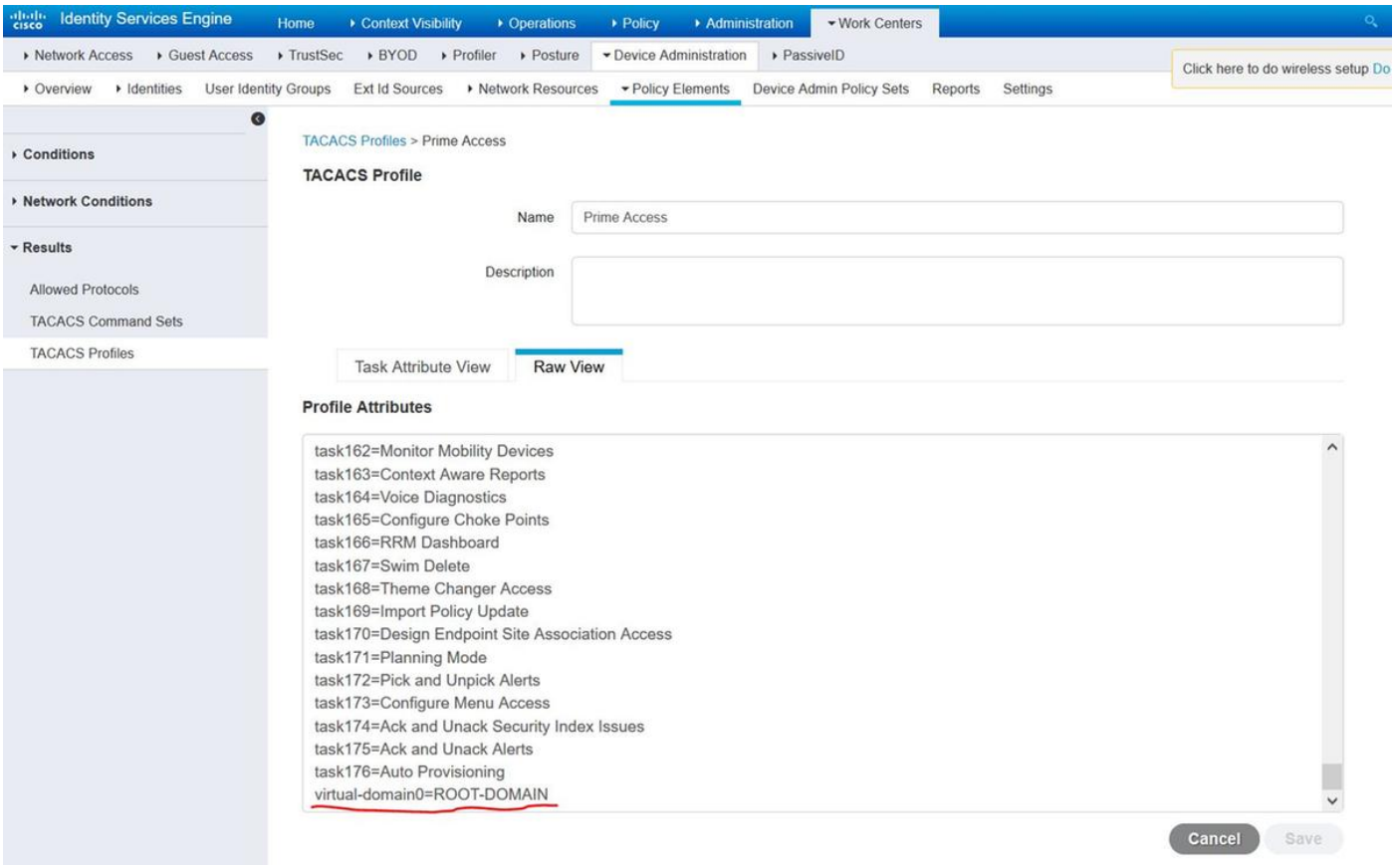
Collez-alors les dans la section brute de vue du profil sur ISE.



Les attributs personnalisés virtuels de domaine sont obligatoires. Les informations de Racine-domaine peuvent être trouvées sous la gestion principale - > les domaines virtuels.

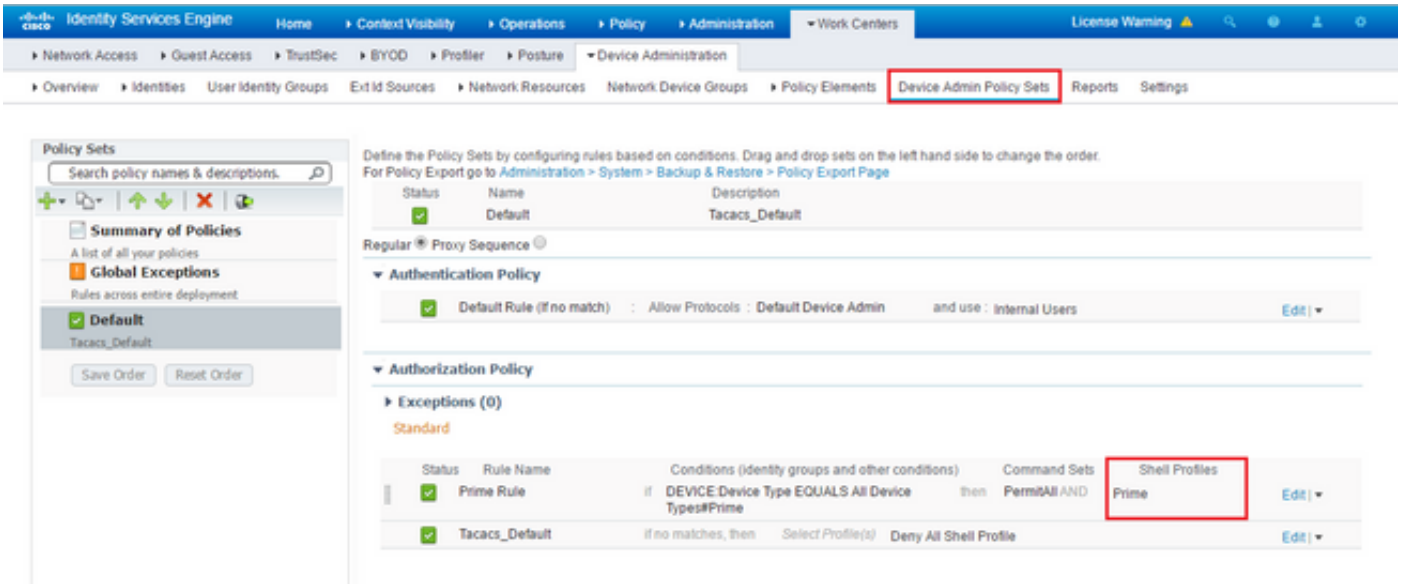


Le nom du domaine virtuel principal doit être ajouté comme nom de domaine de l'attribut **virtual-domain0="virtual** »



Une fois que cela est fait tous vous devez faire doit créer une règle d'assigner le profil de shell créé dans l'étape précédente, dans le cadre des centres de travail/de la stratégie d'admin gestion de périphérique/périphérique place

(Note : Les « conditions » varieront selon le déploiement, toutefois vous pouvez utiliser le « type de périphérique » spécifiquement pour une perfection ou un type différent de filtre tel que l'adresse IP de la perfection, en tant qu'une de « conditionne » de sorte que cette règle filtre correctement des demandes)



En ce moment la configuration devrait être complète.

Dépannez

Si cette configuration est infructueuse et si le local tombent de retour option était enable sur la perfection, vous pouvez forcer un basculer d'ISE, en retirant l'adresse IP de la perfection. Ceci fera ne pas répondre et forcer ISE l'utilisation des qualifications locales. Si le retour local est configuré pour être exécuté sur une anomalie, les comptes locaux fonctionneront et permettront d'accéder toujours au client.

S'ISE affiche une authentification réussie et apparie la règle correcte cependant la perfection rejette toujours la demande que vous pouvez souhaiter pour vérifier une deuxième fois les attributs êtes configuré correctement dans le profil et aucun attribut supplémentaire n'est envoyé.