NAC : Intégration de LDAP avec ACS 5.x et exemple de configuration plus récente

Contenu

Introduction

Ce document fournit une configuration d'échantillon afin de configurer la balise et le Système de contrôle d'accès sécurisé Cisco (ACS) 5.x et activer plus tard des périphériques de Cisco configurés pour la dérivation d'authentification MAC (MAB) de manière efficace et efficiente pour authentifier les périphériques capables non-802.1X dans le réseau authentifié.

Cisco a mis en application une caractéristique appelée MAB sur leurs Commutateurs, aussi bien que le support requis dans ACS, afin de faciliter des points finaux dans les réseaux 802.1X-enabled qui ne peuvent pas authentifier par le 802.1X. Cette fonctionnalité s'assure que les points finaux tentant de se connecter au réseau 802.1X-enabled qui ne sont pas équipés de la fonctionnalité de 802.1X, par exemple, n'ont pas un suppliant fonctionnel de 802.1X, peuvent être authentifiés avant admission, aussi bien qu'ont la stratégie d'utilisation de base de réseau imposée dans toute leur connexion.

Le MAB permet au réseau d'être configuré pour admettre les périphériques identifiés avec l'utilisation de leur adresse MAC comme laisser-passer primaire quand le périphérique ne participe pas au protocole de 802.1X. Pour que le MAB soit déployé et utilisé efficacement, l'environnement doit avoir des moyens d'identifier les périphériques dans l'environnement qui ne sont pas capables de l'authentification de 802.1X, et de mettre à jour une base de données à jour de ces

périphériques au fil du temps comme se déplace, ajoute et les modifications se produisent. Cette liste doit être remplie et mise à jour dans le serveur d'authentification (ACS) manuellement, ou par un certain alternatif signifie afin de s'assurer que les périphériques qui authentifient sur le MAC sont terminés et valides à tout moment.

Le profileur de point final de balise peut automatiser le processus de l'identification de non-authentifier des points finaux, ceux sans suppliants de 802.1X, et la maintenance de la validité de ces points finaux dans les réseaux de l'échelle variable sur la fonctionnalité de surveillance de profilage et de comportement du point final. Par une interface standard de LDAP, le système de balise peut servir de base de données externe ou de répertoire des points finaux à authentifier par le MAB. Quand une demande de MAB est reçue de l'infrastructure de périphérie, l'ACS peut questionner le système de balise afin de déterminer si un point final donné devrait être admis au réseau basé sur les informations les plus en cours sur le point final connu par la balise. Ceci empêche le besoin de configuration manuelle.

Pour une configuration semblable utilisant des versions plus tôt qu'ACS 5.x, référez-vous au NAC : Intégration de LDAP avec l'exemple de configuration ACS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Commutateur de Cisco 3750 qui exécute la version de logiciel 12.2(25)SEE2 de Cisco IOS®
- Cisco Secure ACS 5.x et plus tard

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le MAB est une fonctionnalité essentielle pour le support dynamique des périphériques tels que des imprimantes, des Téléphones IP, des télécopieurs et d'autres périphériques capables non-802.1X dans le déploiement de l'environnement post-802.1X. Sans capacité de MAB, des ports d'accès au réseau qui fournissent Connectivité aux points finaux capables non-802.1X doivent provisioned statiquement afin de ne pas tenter l'authentification de 802.1X ou par l'utilisation d'autres caractéristiques qui fournissent des options très limitées de stratégie. Pour des raisons

évidentes, ce n'est pas en soi extensible à de grands environnements d'entreprise. Le MAB étant activé en même temps que le 802.1X sur tous les ports d'accès, des points finaux capables connus non-802.1X peuvent être déplacés n'importe où l'environnement et sûrement (et sécurisé) connectez toujours au réseau. Puisque les périphériques admis au réseau sont authentifiés, différentes stratégies peuvent être appliquées aux différents périphériques.

En outre, les points finaux capables non-802.1X qui ne sont pas connus dans l'environnement, tel que les ordinateurs portables qui appartiennent aux visiteurs ou aux sous-traitants, peuvent être accès restreint fourni au réseau par le MAB si désirés.

Pendant que le nom suggère, la dérivation d'authentification MAC utilise l'adresse MAC du point final comme laisser-passer primaire. Le MAB étant activé sur un port d'accès, si un point final se connecte et ne relève pas le défi d'authentification de 802.1X, le port retourne au mode de MAB. Le commutateur qui tente le MAB d'un point final fait une demande RADIUS standard à ACS avec le MAC de la station. Il tente de se connecter au réseau et demande l'authentification du point final d'ACS avant l'admission du point final au réseau.

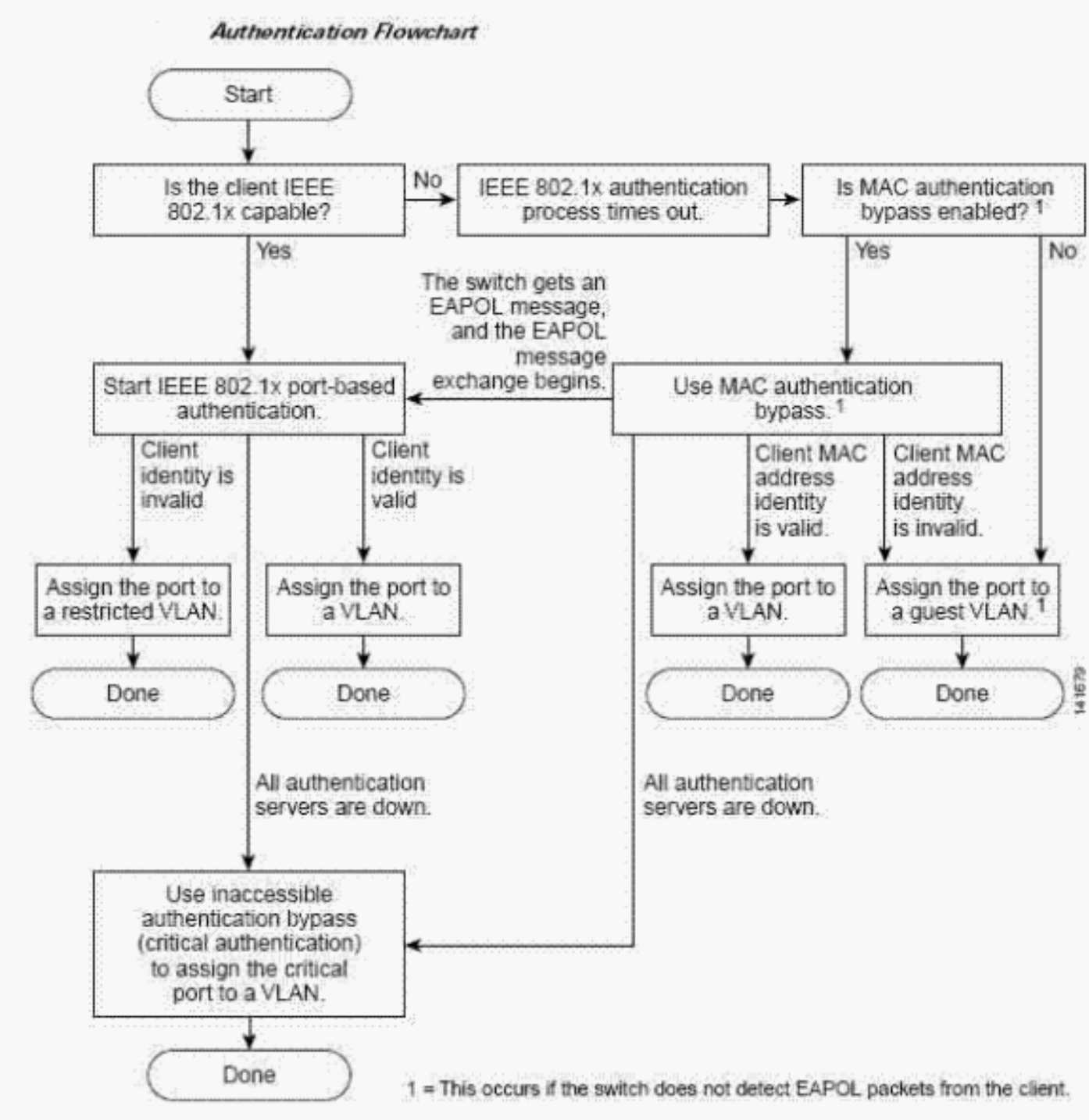
Configuration

Diagramme d'organigramme

Cet organigramme montre comment le MAB est utilisé en même temps que l'authentification de 802.1X sur l'infrastructure de périphérie de Cisco pendant que nouvelle tentative de points finaux de se connecter au réseau.

Ce document utilise ce processus d'organigramme :

Figure 1 : Écoulement d'authentification



L'ACS peut être configuré pour utiliser sa propre base de données interne ou un serveur LDAP externe afin d'authentifier des demandes d'utilisateur d'adresse MAC. Le système de profileur de point final de balise LDAP-est entièrement activé par défaut et peut être utilisé par l'ACS afin d'authentifier des demandes d'utilisateur d'adresse MAC par la fonctionnalité standard de LDAP. Puisque la balise automatise la détection aussi bien que le profilage de tous les points finaux sur le réseau, l'ACS peut questionner la balise par le LDAP afin de déterminer si le MAC est admis au réseau, et qui groupe le point final devrait être tracé. Ceci de manière significative automatise et améliore la caractéristique de MAB, en particulier dans de grands environnements d'entreprise.

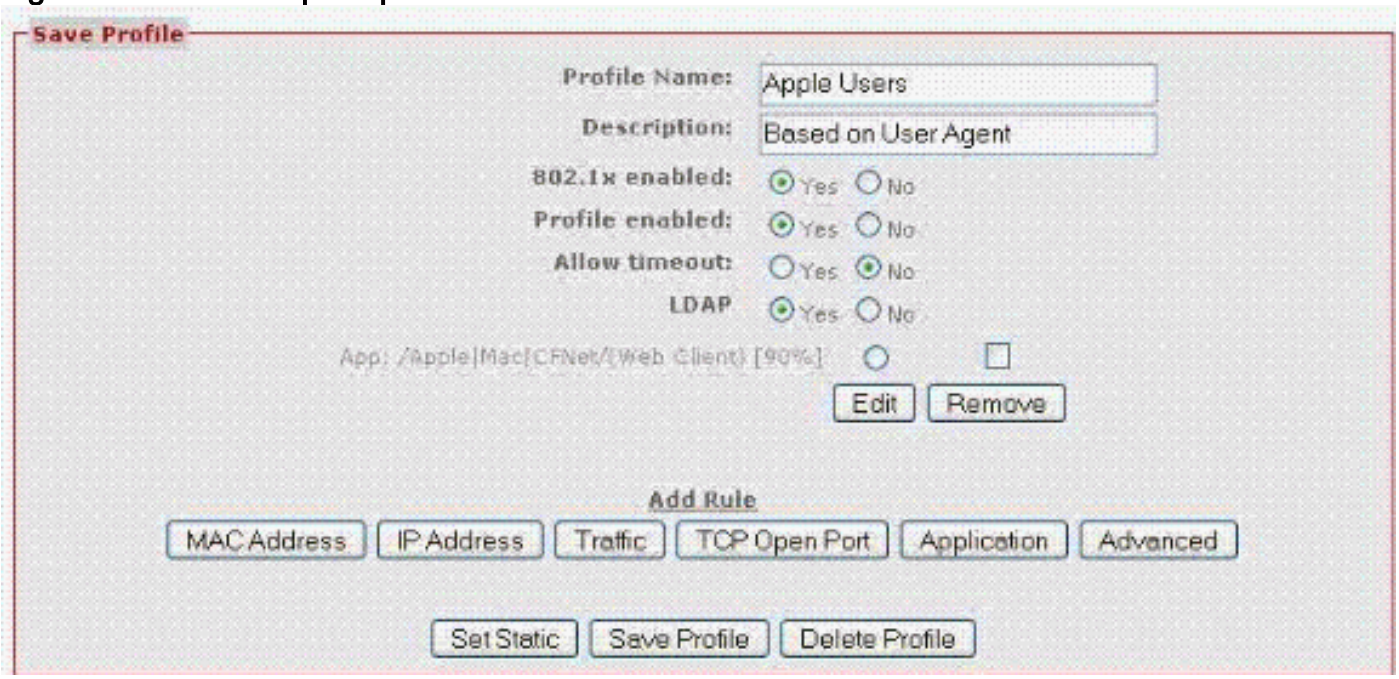
Par la fonctionnalité comportementale de surveillance fournie par la balise, des périphériques qui sont observés pour se comporter inconséquemment avec les profils activés pour le MAB transitioned sur 4 profils LDAP-activés et échouer ultérieurement la prochaine tentative régulière de ré-authentification.

Configuration système de profileur de point final de balise pour le MAB

La configuration du système de balise pour l'intégration avec ACS aux fins de support de MAB est simple car la fonctionnalité de LDAP est activée par défaut. La tâche primaire de configuration est d'identifier les profils qui contiennent les points finaux qui sont désirés pour être authentifiés par le MAB dans l'environnement, et activer alors ces profils pour le LDAP. Typiquement, les profils de balise, qui contiennent des périphériques ont possédé par l'organisation, doivent être accès au réseau fourni une fois vus sur un port pourtant sont connus pour ne pouvoir pas authentifier par le 802.1X. Typiquement, ce sont des profils qui contiennent des imprimantes, des Téléphones IP ou des UPS maniables comme exemples classiques.

Si des imprimantes profilées par la balise étaient placées dans un profil nommé *Printers*, et les Téléphones IP dans un profil nommaient des *Téléphones IP*, par exemple, alors le besoin de ces profils d'être activé pour le LDAP tels que les points finaux placés dans ces profils ont comme conséquence l'authentification réussie en tant que le téléphone IP et imprimantes connus dans l'environnement par le MAB. Si vous activez un profil pour le LDAP, ceci exige choisir la case d'option de LDAP dans la configuration de profil de point final, suivant les indications de cet exemple :

Figure 2 : Activez un profil pour le LDAP



Quand l'authentification MAC de proxys ACS à baliser par le LDAP, la requête se compose de deux sous requêtes. Chacun de ceux là doivent renvoyer un résultat valide et non nul. La première requête à baliser est si le MAC est connu pour baliser, par exemple, s'il a été découvert et ajouté à la base de données de balise. Si le point final a pour être découvert encore par la balise, le point final est considéré inconnu.

La deuxième requête n'est pas nécessaire dans le cas des points finaux que la balise n'a pas découverts et n'est pas dans sa base de données. Si le point final a été découvert et est dans la base de données de balise, la prochaine requête est de déterminer le profil en cours du point final. Si un point final a pour être profilé encore ou est actuellement dans un profil non 5 activés pour le LDAP, le résultat inconnu est retourné à l'ACS, et l'authentification du point final par la balise échoue. Il dépend de la façon dont l'ACS est configuré que ceci peut avoir comme conséquence le périphérique avec le refus de l'accès au réseau totalement, ou soit donné une stratégie qui est appropriée pour des périphériques d'inconnu ou d'invité.

Seulement dans le cas où le MAC est un point final que la balise a découvert et placé dans un profil LDAP-activé, la réponse est que le point final est connu et profilé par la balise soyez retourné à ACS. Avant tout, parce que balise de ces points finaux fournit le nom de profil en cours. Ceci permet à ACS de tracer des points finaux connus aux groupes de Cisco SecureAccess. Ceci active une détermination granulaire de stratégie faite, aussi granulaire qu'une stratégie distincte pour chaque profil LDAP-activé par balise, si désiré.

Configuration ACS pour le MAB et utilisation de balise comme base de données d'utilisateur externe

La configuration d'ACS pour le MAB et de l'utilisation de la balise comme base de données d'utilisateur externe exige trois étapes distinctes. La commande illustrée dans ce document suit un processus qui est efficace quand il exécute la configuration de MAB en sa totalité, et peut varier pour les systèmes qui ont été en fonction avec d'autres authentications mode déjà configurées.

Quand vous tentez le MAB pour un point final particulier qui tente de se connecter au réseau, les requêtes ACS balisent sur le LDAP afin de déterminer si la balise a découvert le MAC, et le quel balise de profil a actuellement placé l'adresse MAC dedans comme décrit plus tôt dans le document.

Dans ce document, deux profils distincts sont créés :

- BeaconKnownDevices — pour les points finaux découverts et profilés par la balise
- BeaconUnknownDevices — pour les périphériques qui ne sont pas actuellement connus par la balise

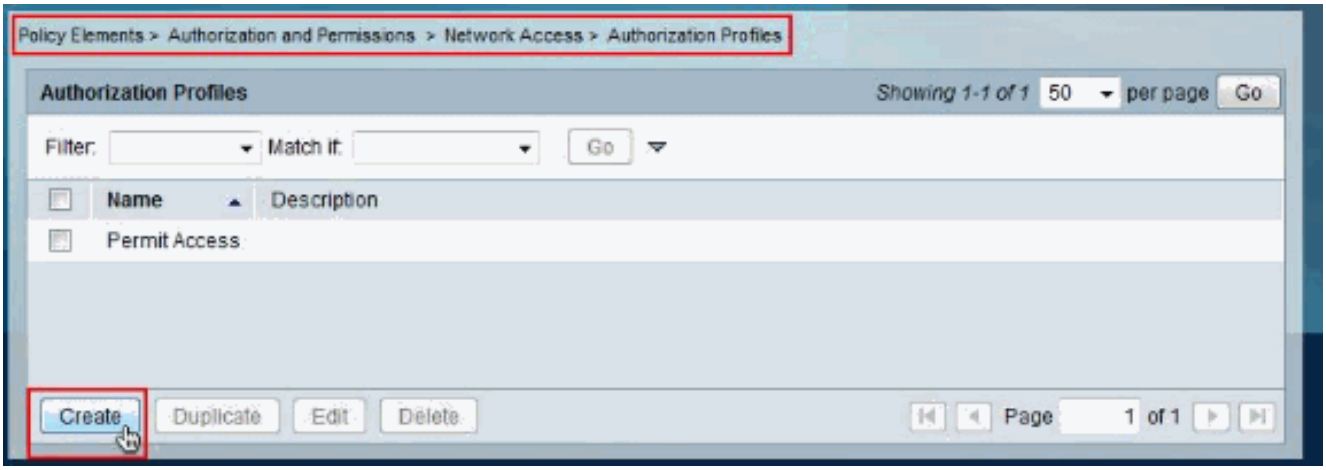
La balise n'a pas découvert le MAC, ou ne l'a pas actuellement profilé à un profil LDAP-activé. Le profil de BeaconKnownDevices mettra les points finaux dans le VLAN 10 et le profil de BeaconUnkownDevices mettra les points finaux dans VLAN 7.

Plus tard dans ce document, une connexion de LDAP au profileur de point final de balise d'ACS est créée et des groupes sont choisis du profileur de point final de balise basé sur quels points finaux seront considérés comme périphériques de BeaconKnown, et seront assignés le profil de BeaconKnownDevices (qui les mettra dans VLAN 10). Tous les périphériques inconnus que la balise n'a pas découvert le MAC, ou ne l'a pas actuellement profilé dans un profil LDAP-activé seront assignés le profil de BeaconUnkownDevices (qui les mettra dans VLAN 7).

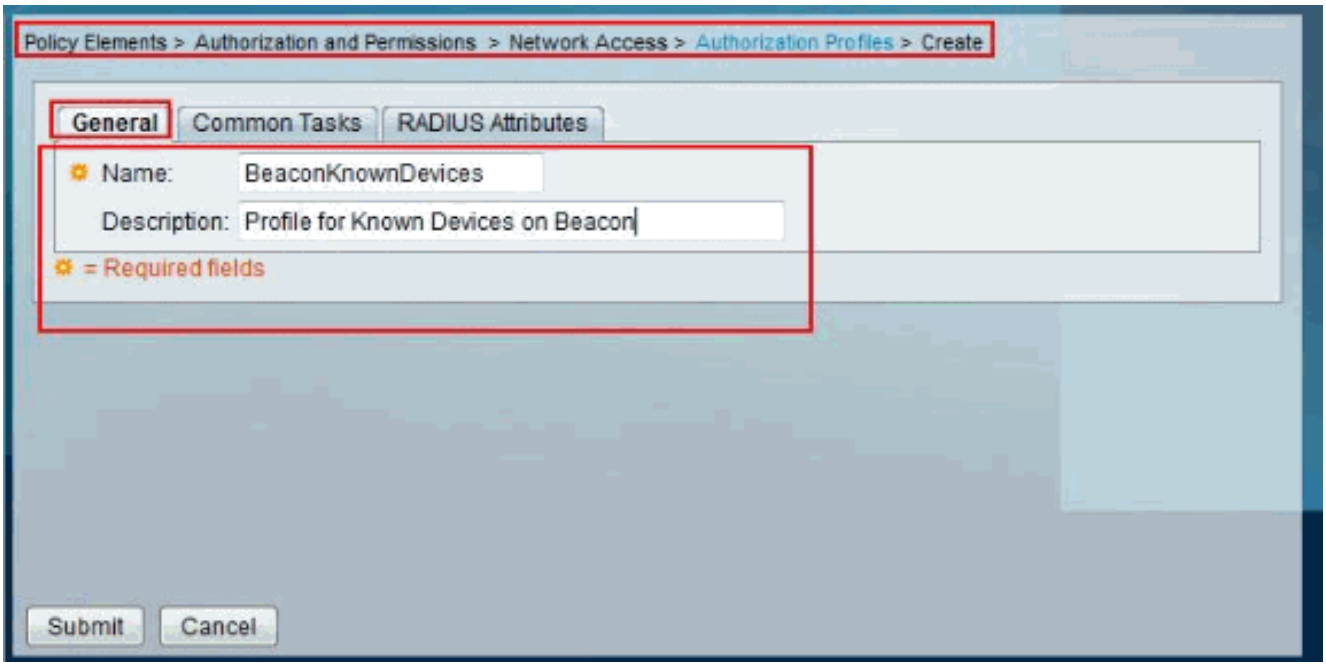
Créez un profil d'autorisation

Terminez-vous ces étapes afin de créer un profil d'autorisation :

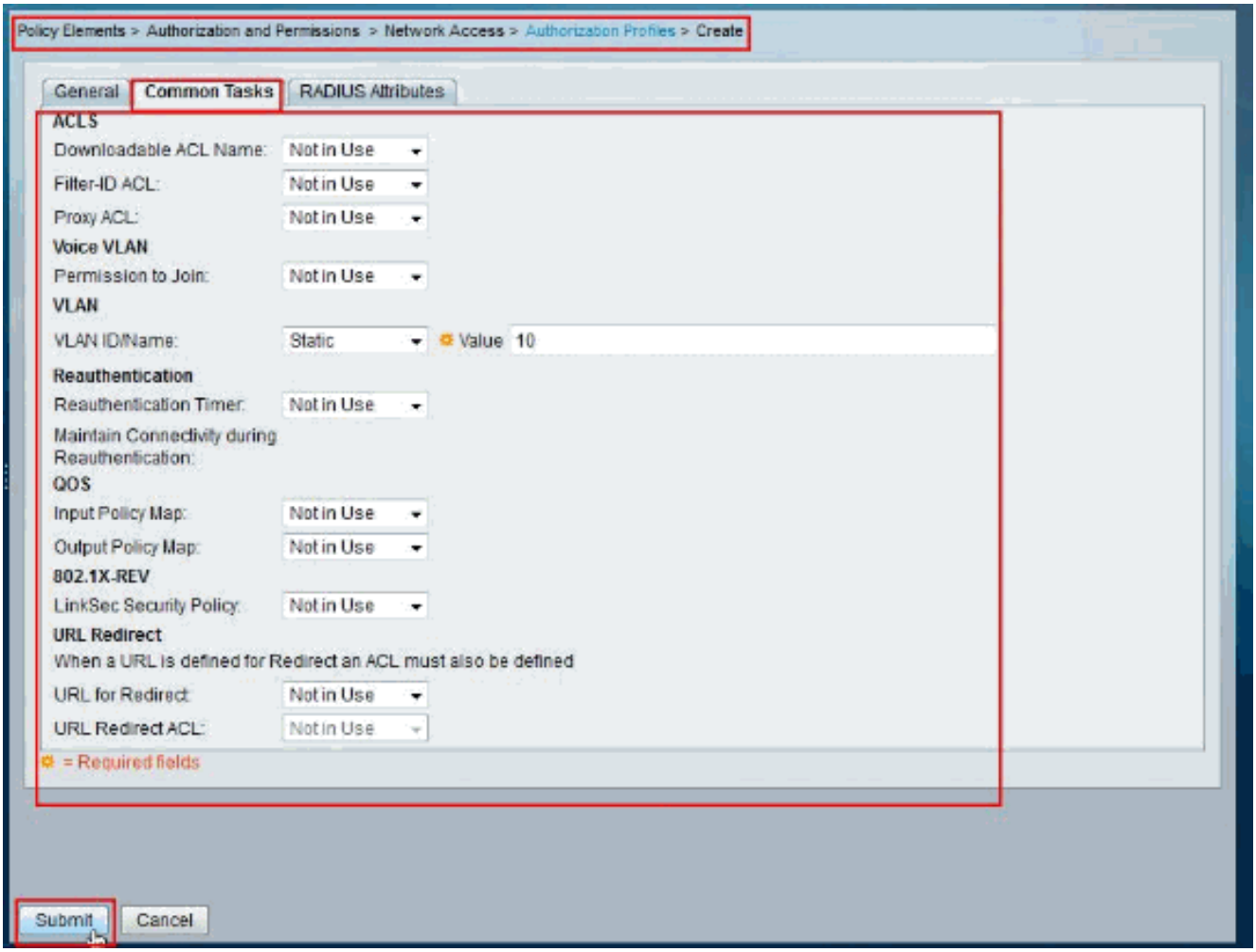
1. Choisissez les **éléments > l'autorisation de stratégie et les autorisations > l'accès au réseau > les profils** et le clic d'**autorisation créent** pour créer un nouveau profil d'autorisation.



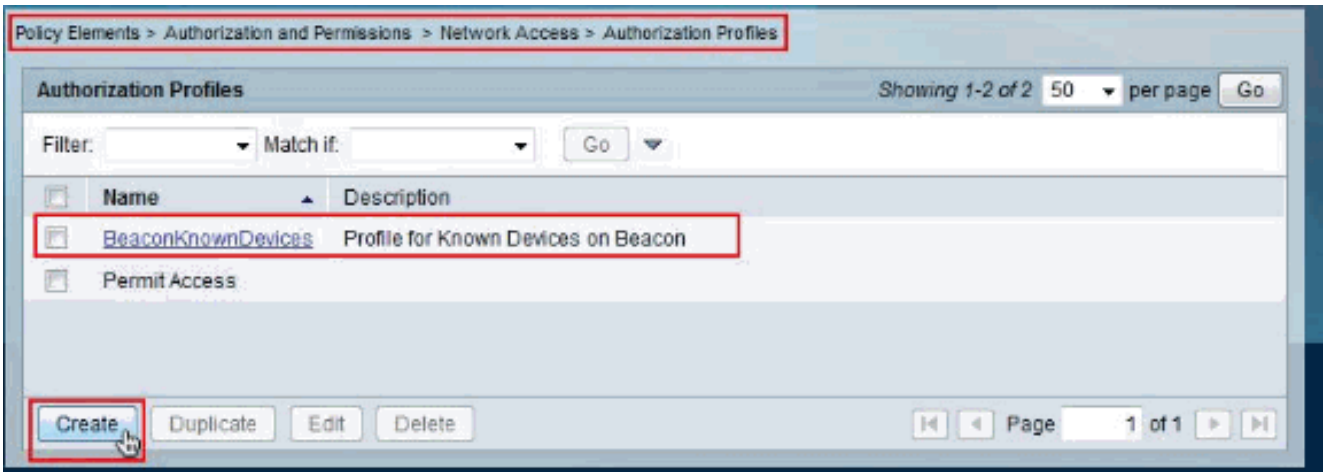
2. Fournissez le **nom du** nouveau profil d'autorisation.



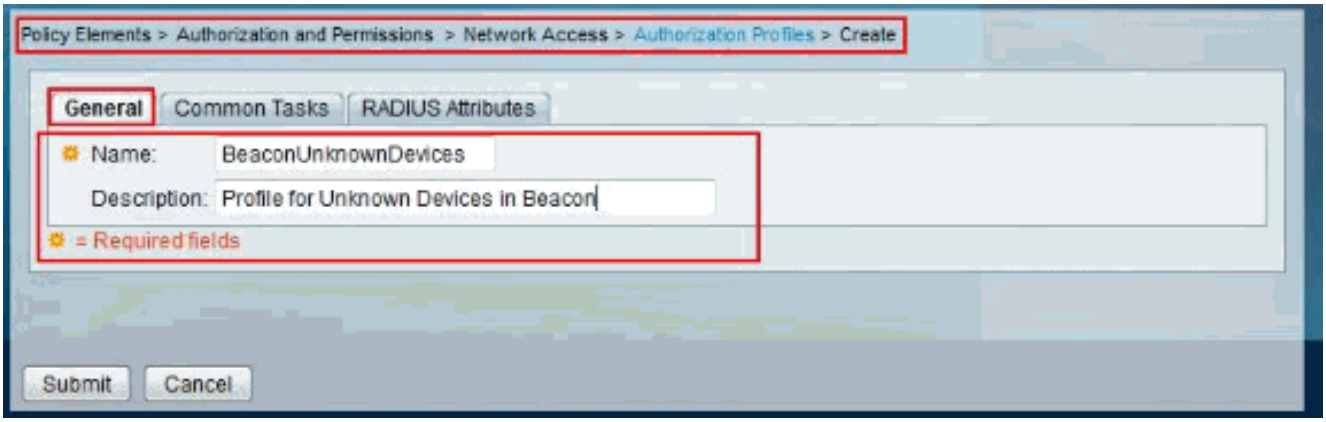
3. Dans des **fonctionnalités usuelles l'**onglet a placé le **VLAN à la charge statique** avec la **valeur** en tant que **10.** Puis, cliquez sur **Submit**.



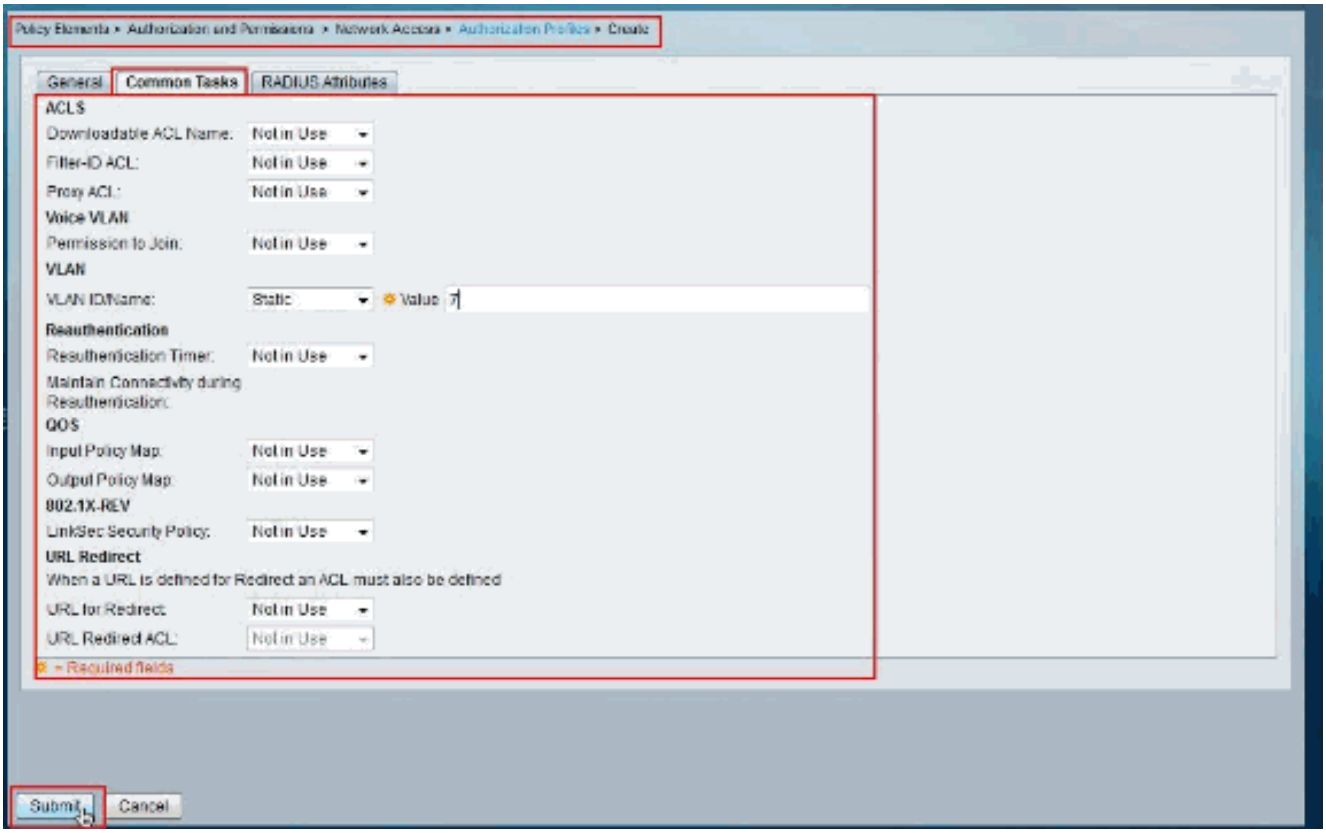
4. Choisissez les **éléments > l'autorisation de stratégie et les autorisations > l'accès au réseau > les profils** et le clic d'**autorisation créent** pour créer un nouveau profil d'autorisation.



5. Fournissez le **nom du** nouveau profil d'autorisation.



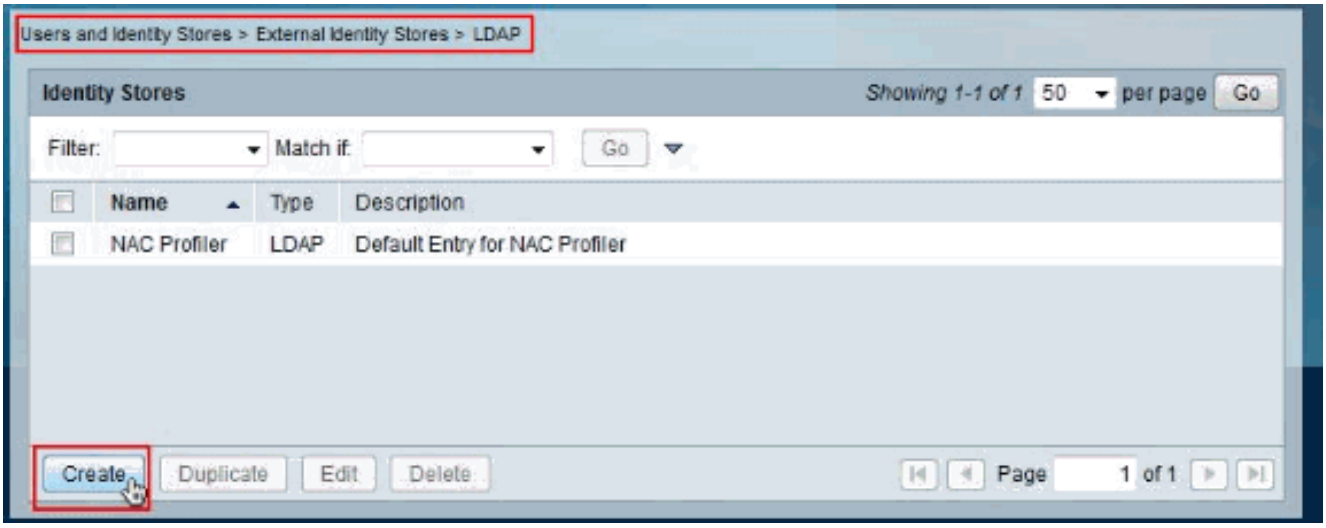
6. Dans des **fonctionnalités usuelles l'**onglet a placé le **VLAN à la charge statique** avec la **valeur** en tant que **7.** Puis, cliquez sur **Submit**.



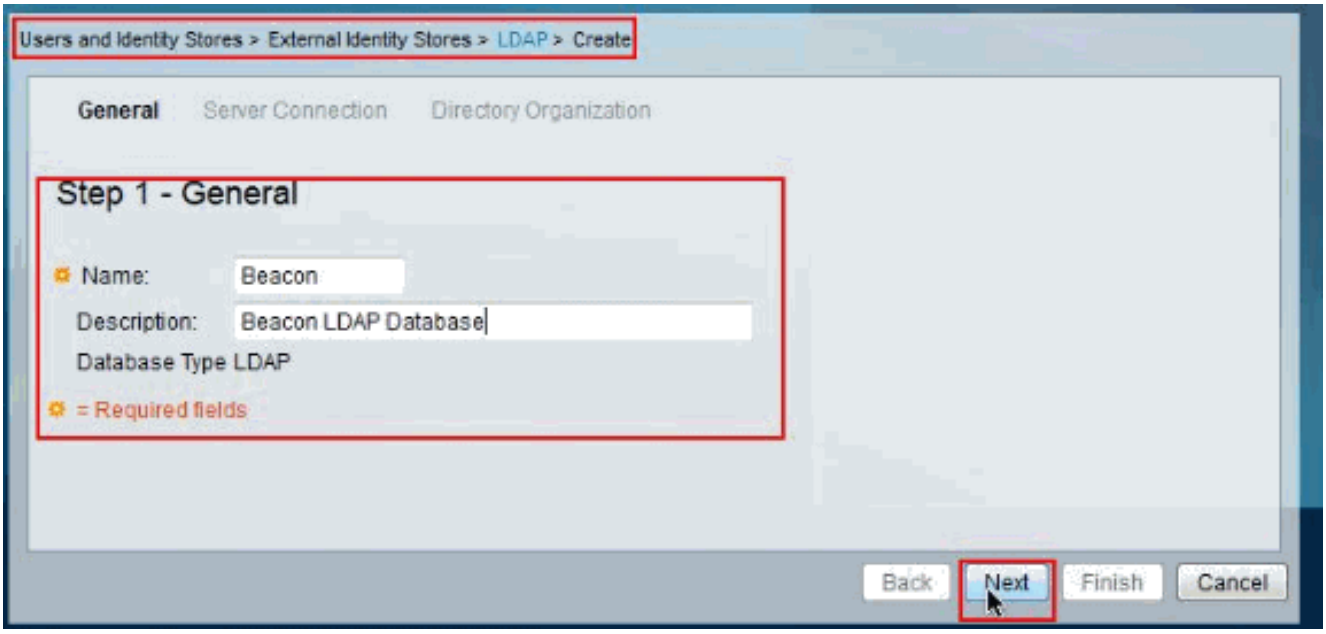
Créez une Connexion de la base de données de LDAP

Terminez-vous les étapes afin de créer une Connexion de la base de données de LDAP :

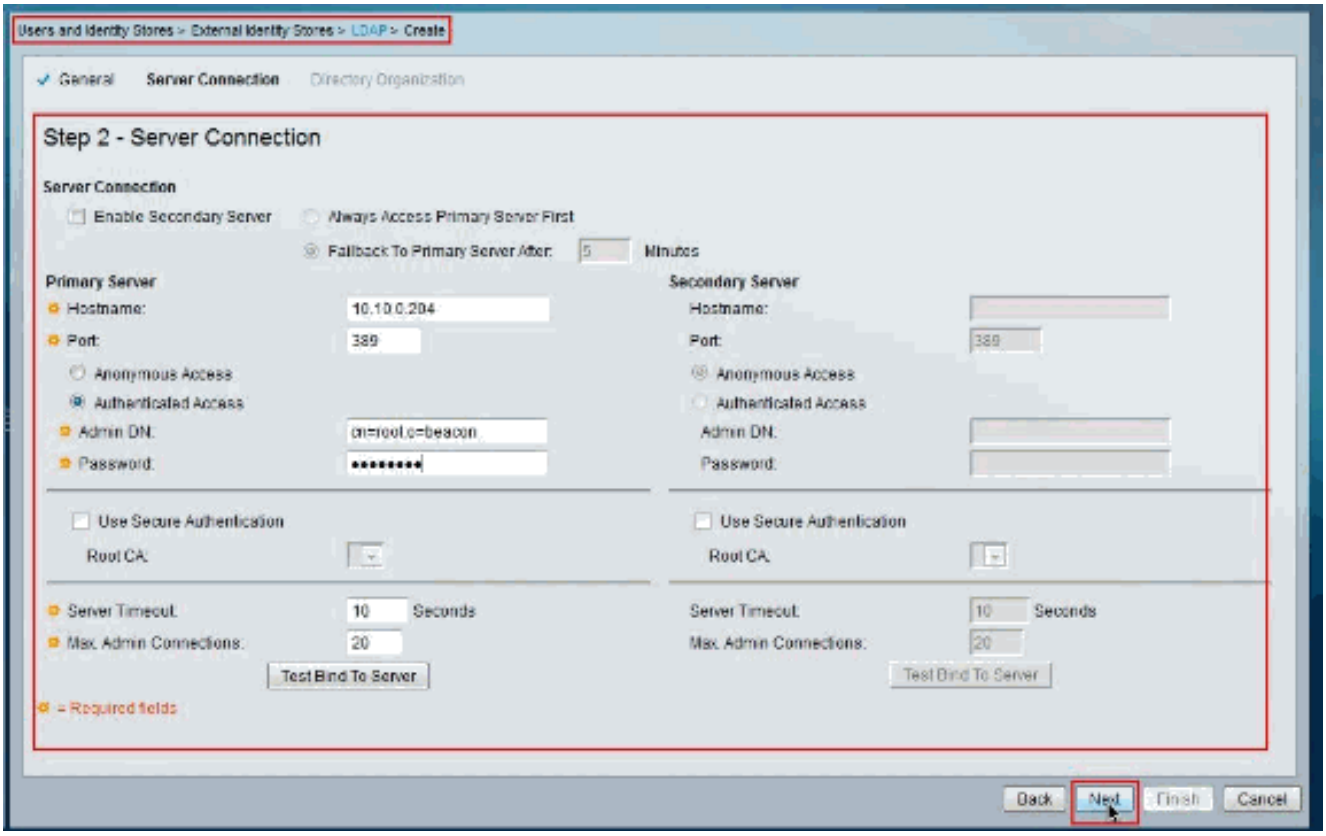
1. Choisissez les **utilisateurs et l'identité enregistre > identité externe enregistre > LDAP** et le clic **créent** pour créer une nouvelle Connexion de la base de données de LDAP.



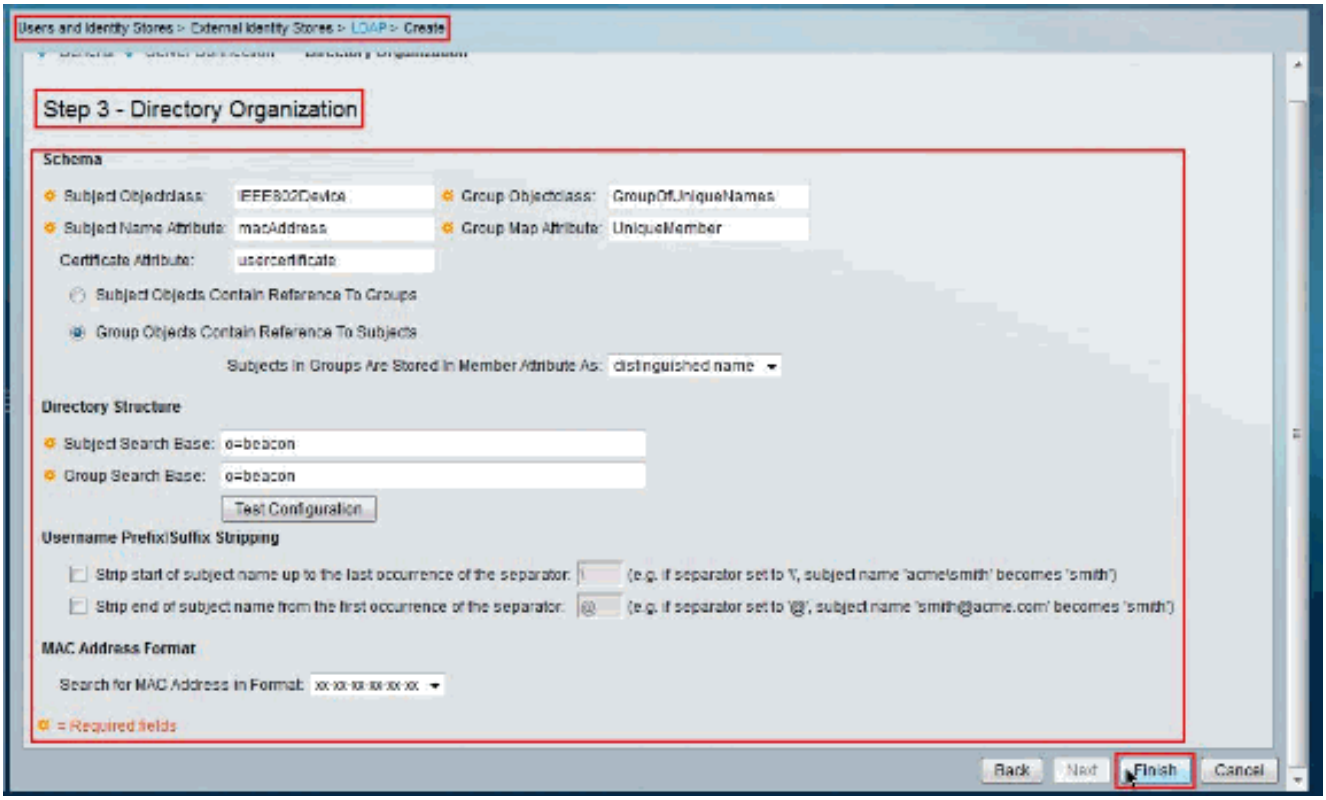
2. Fournissez un **nom** pour la nouvelle **Connexion de la base de données de LDAP** et cliquez sur
Next.



3. Dans l'onglet de **connexion au serveur** écrivez l'**adresse Internet/adresse IP du LDAP de BALISE divisent, mettent en communication, DN d'admin, le mot de passe** (GBSbeacon dans cet exemple). Cliquez ensuite sur
Next.

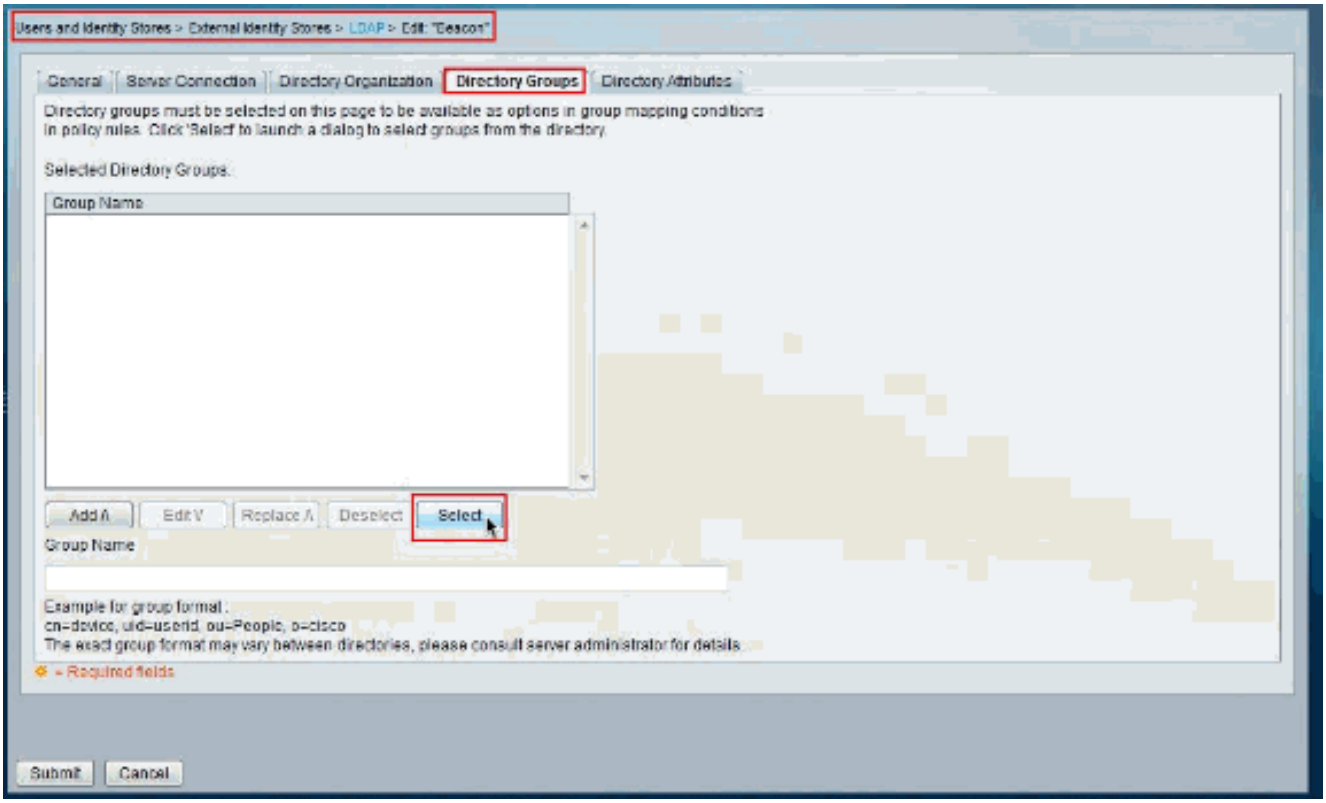


4. Dans l'onglet d'**organisation de répertoire** écrivez l'information requise. Cliquez ensuite sur **Finish**.

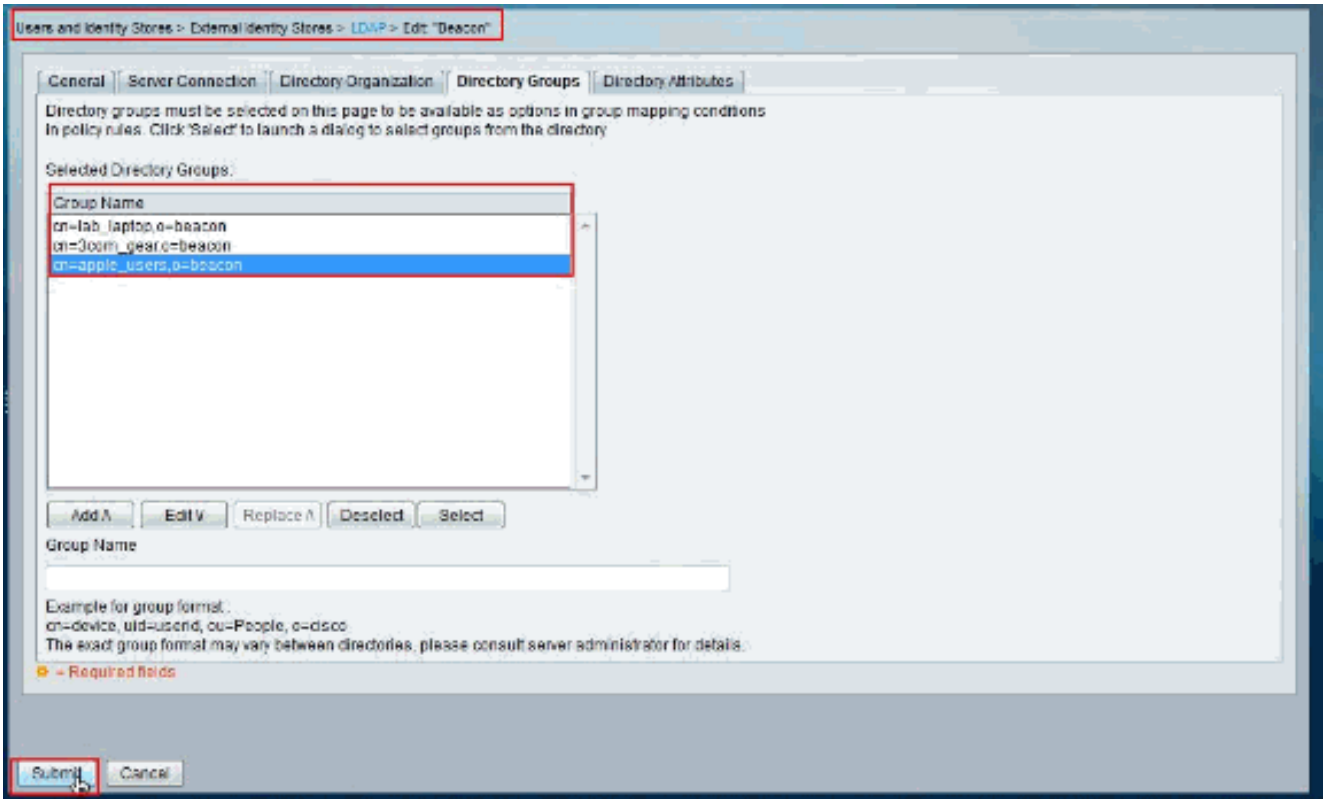


5. Cliquez sur la **connexion** de création récente de **LDAP** (balise dans cet exemple).

6. Choisissez l'onglet de **groupes de répertoire** et cliquez sur **choisi**. connexion.



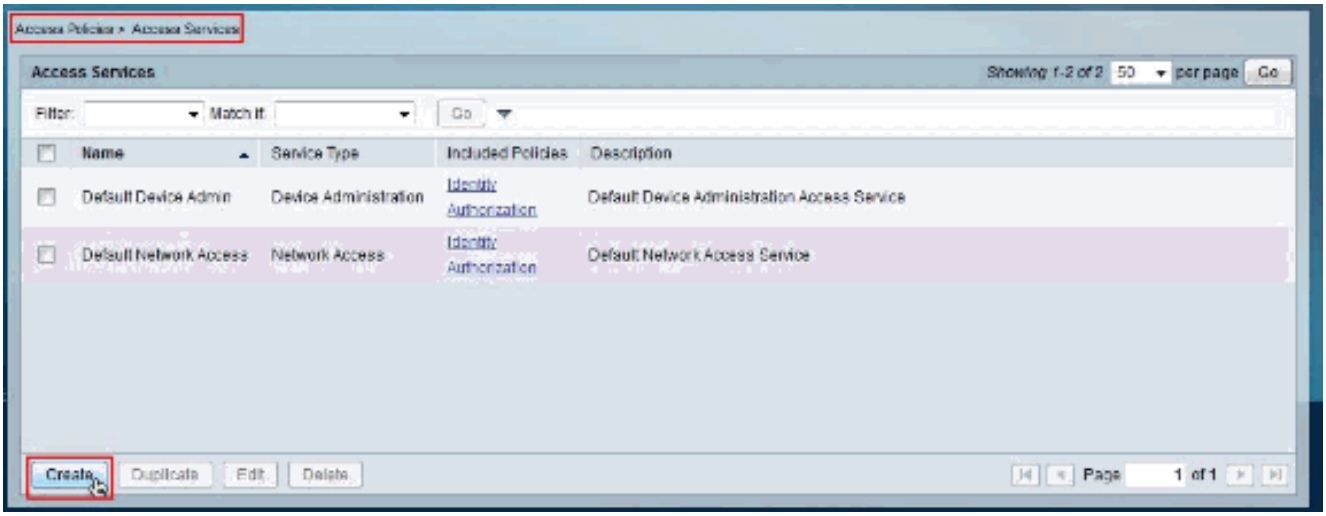
7. Sélectionnez tous les groupes dans l'écran suivant que vous voulez tracer à **BeaconKnownDevices**.
8. Dans cet exemple ces groupes, à savoir lab_laptop, 3com_gear et apple_users, sont choisis. Puis, cliquez sur **Submit**.



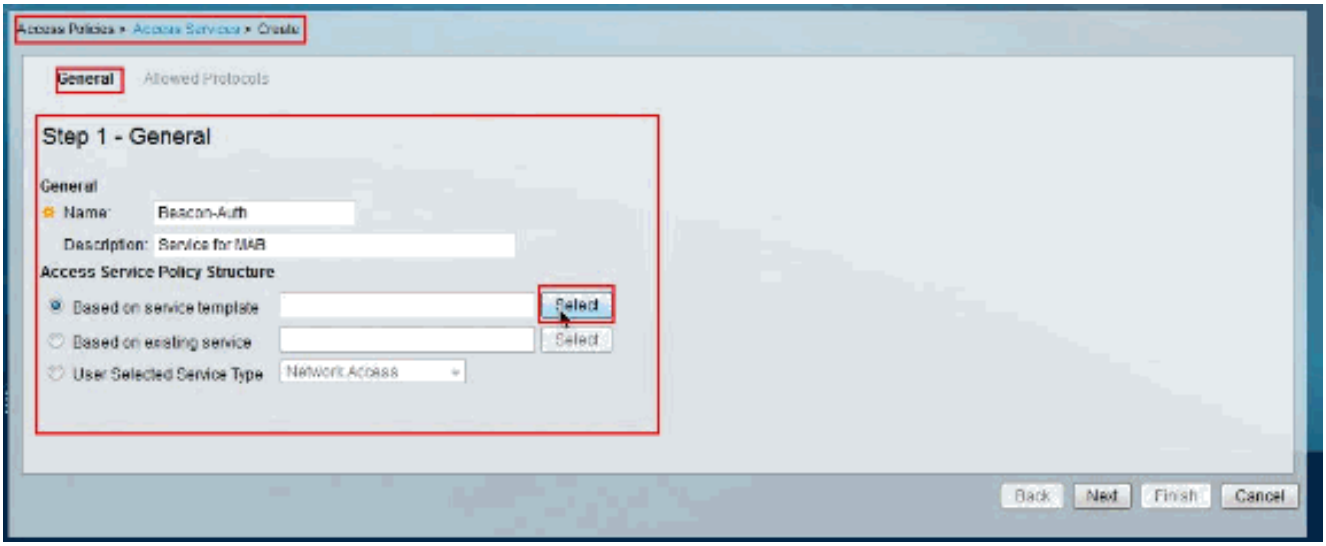
Configurez les services d'accès

Terminez-vous ces étapes afin de configurer les services d'accès :

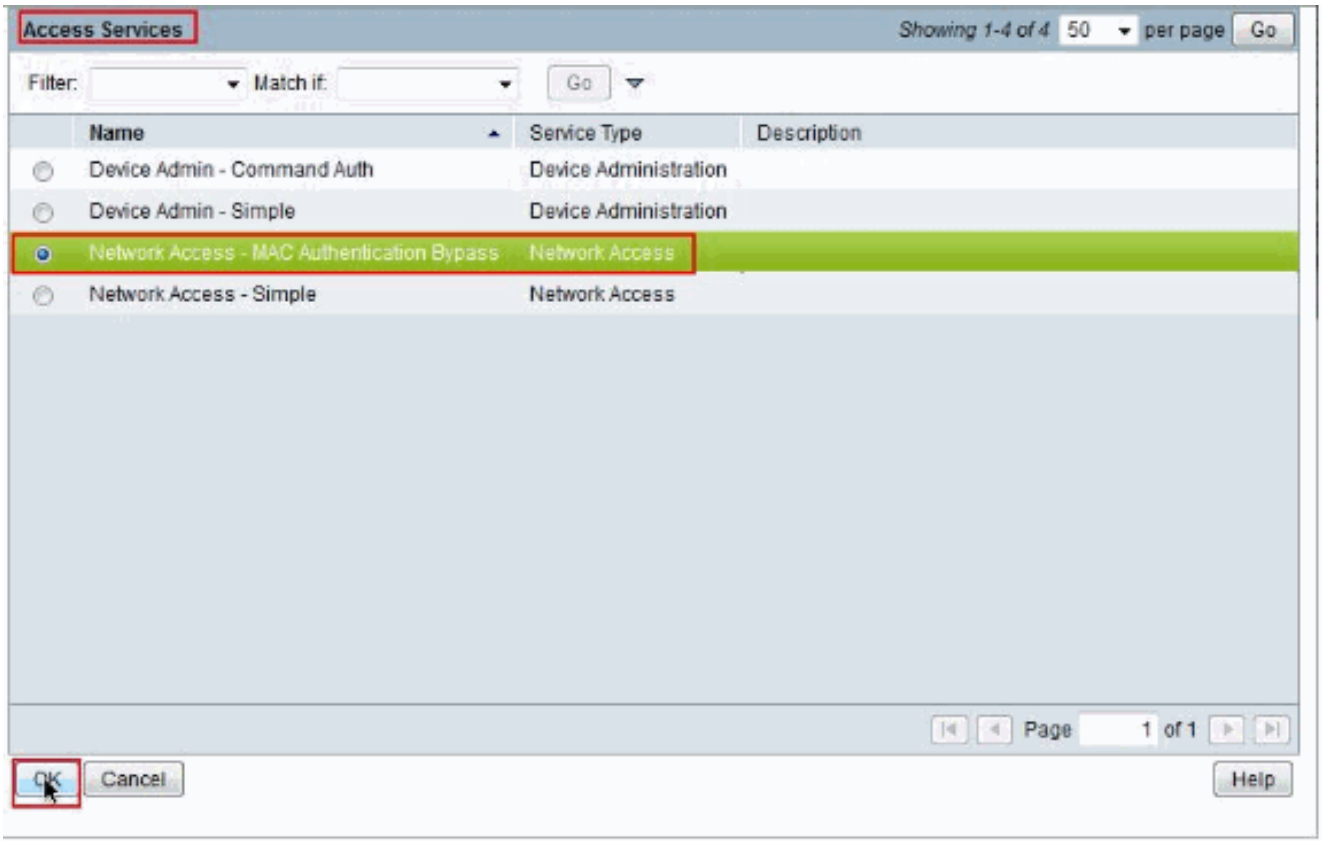
1. Choisissez les **stratégies > les services d'accès d'Access** et le clic **créent** pour créer un nouveau service
d'accès.



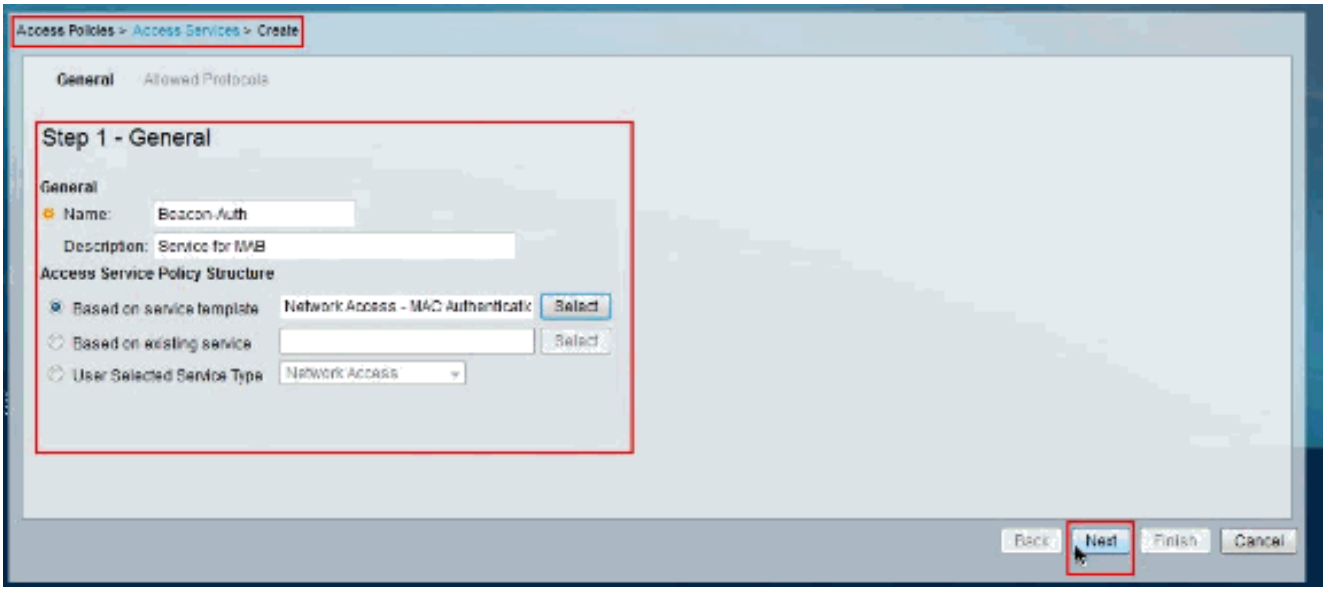
2. Dans l'**onglet Général** fournissez le **nom du** nouveau service, puis cliquez sur **choisi** à côté de **basé sur le modèle de**
service.



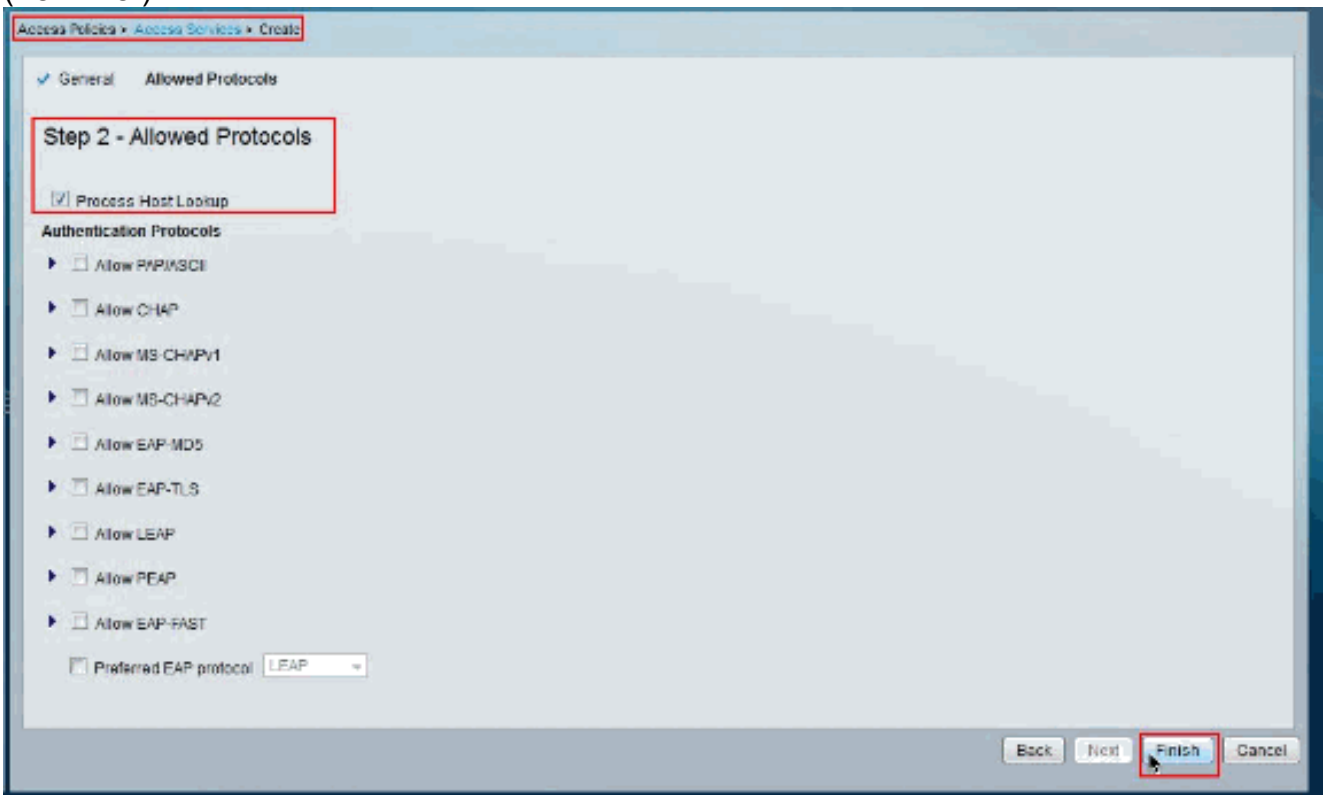
3. Choisissez l'**accès au réseau - La dérivation d'authentification MAC** et cliquent sur OK.



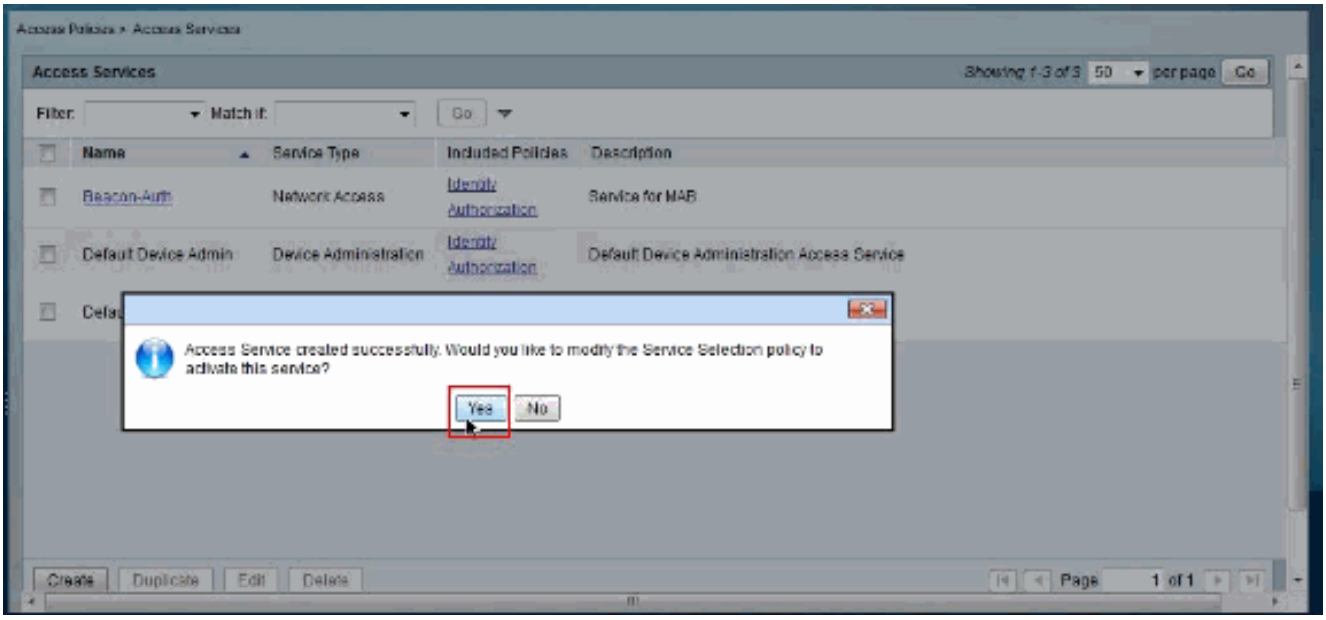
4. Cliquez sur **Next** (Suivant).



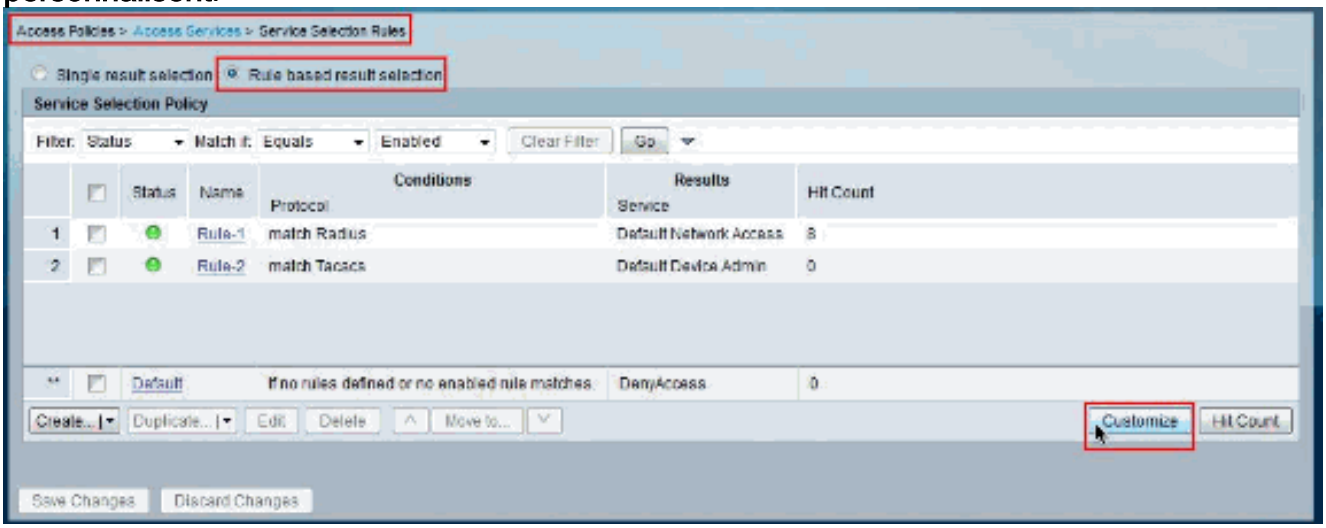
5. Cliquez sur **Finish** (Terminer).



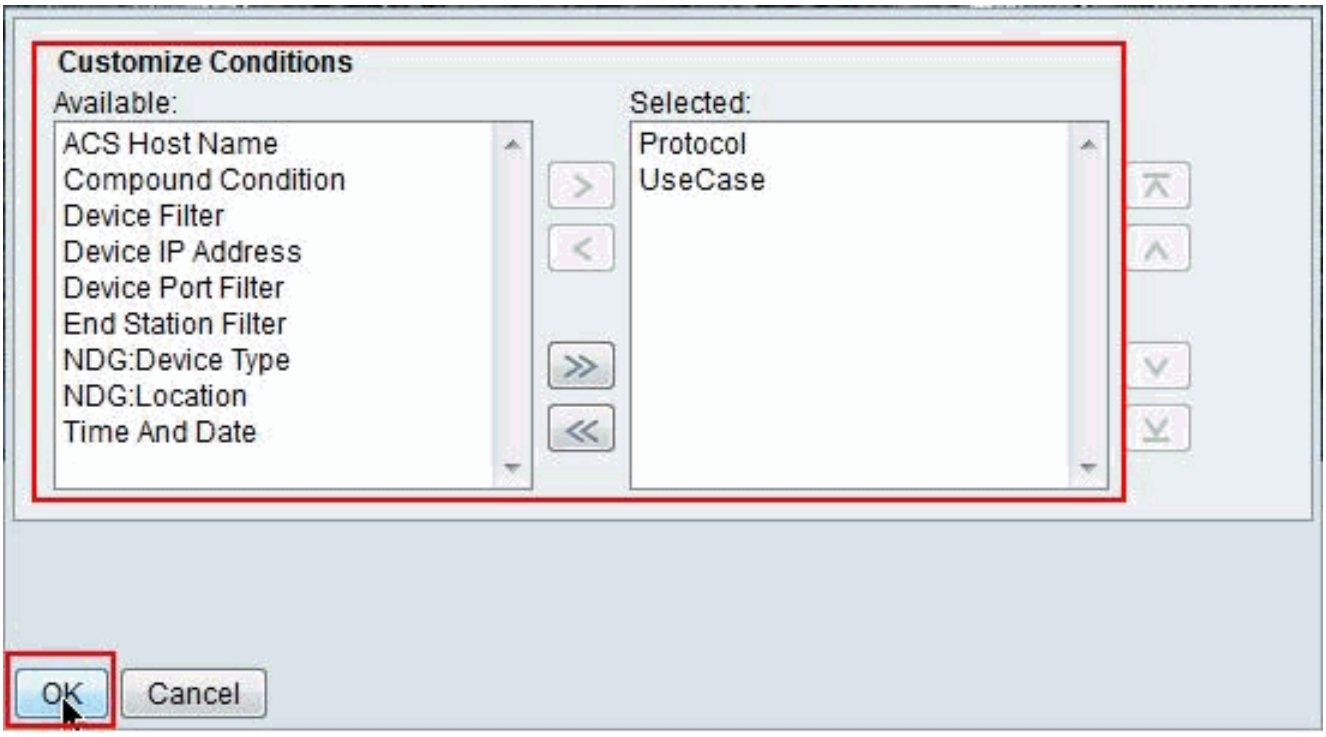
6. Cliquez sur **Yes**.



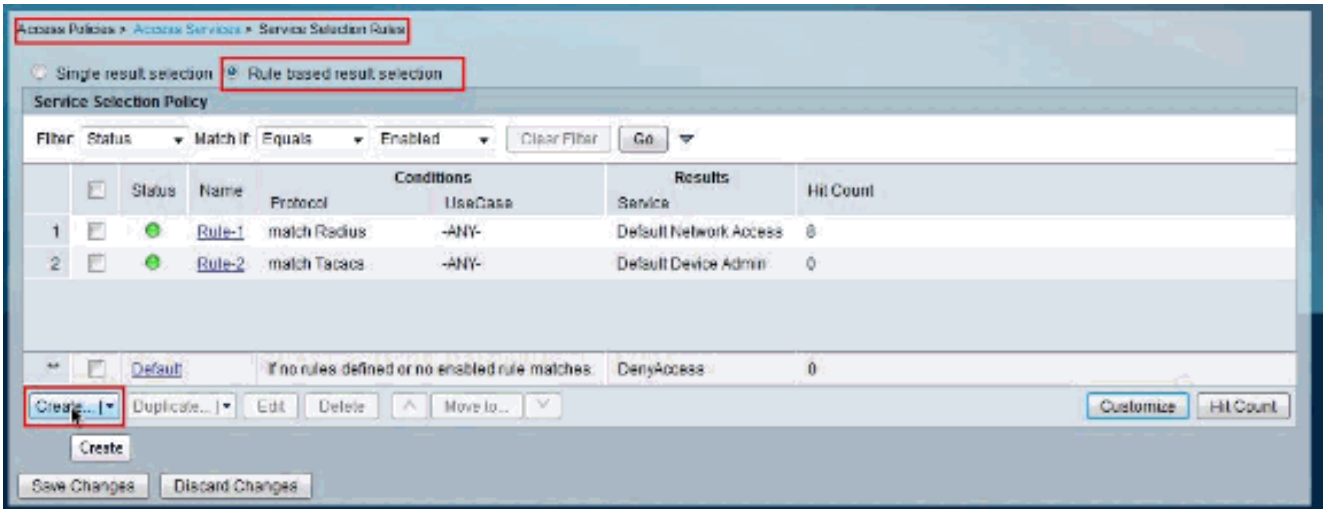
7. Le clic **personnalisent**.



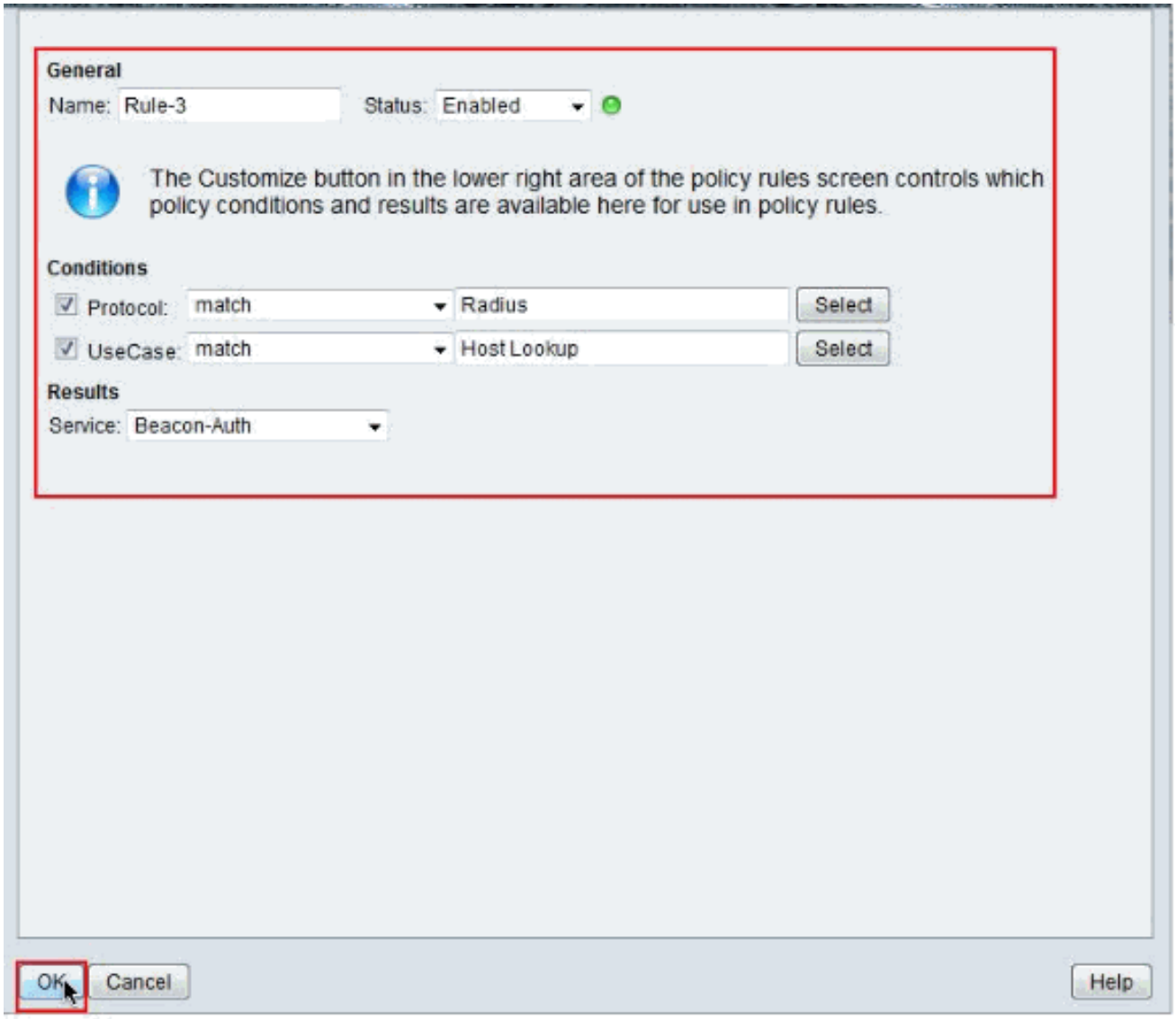
8. Déplacez **UseCase de sélectionné disponible** et cliquez sur OK.



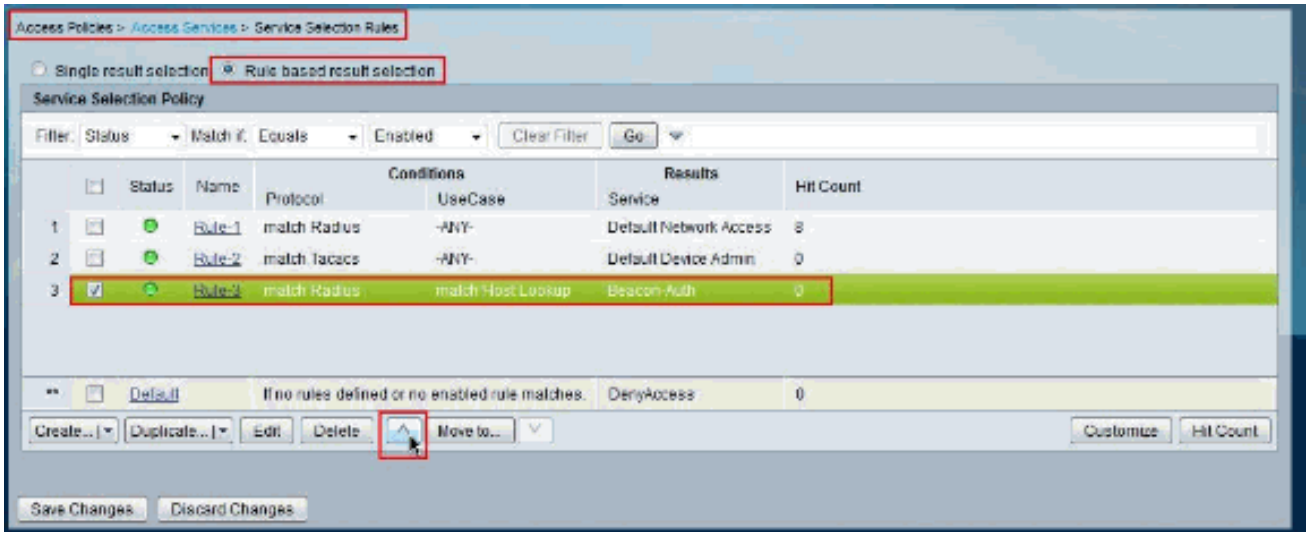
9. Le clic **créent** pour créer une nouvelle **règle de sélection de service**.



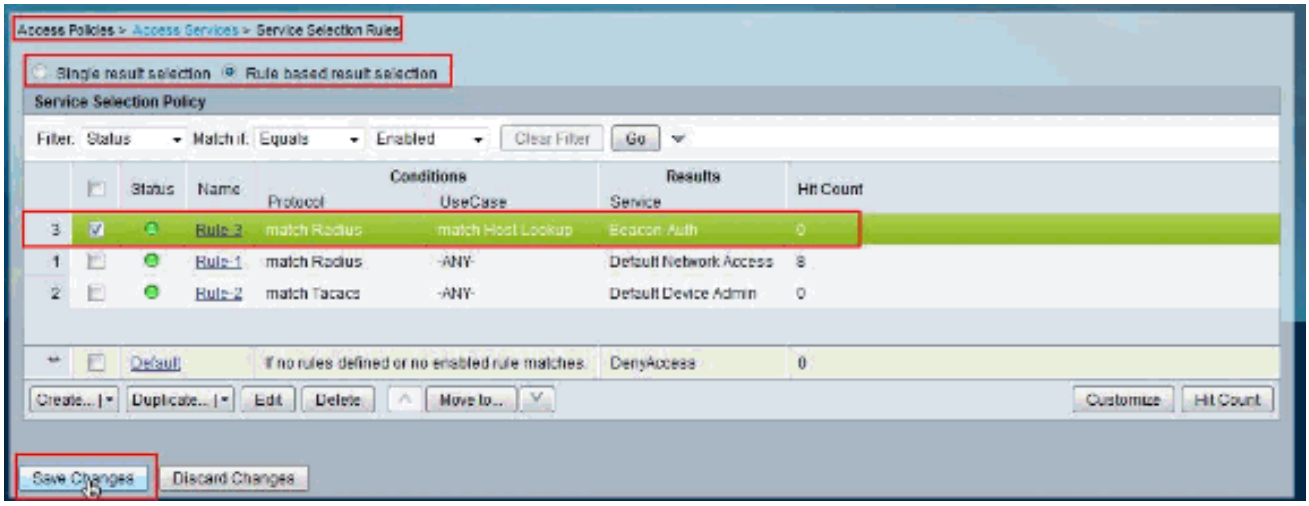
10. **Protocol** choisi et **rayon d'**utilisation comme valeur. De même, **UseCase** choisi et utilisation **hébergent la consultation** comme valeur. Choisissez la **balise-Auth** comme service et cliquez sur
OK.



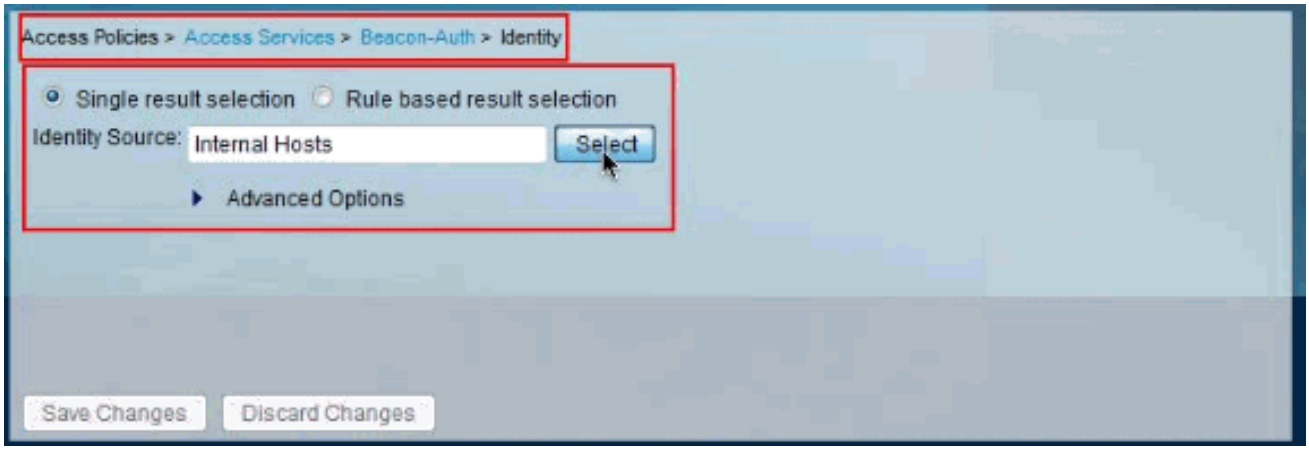
11. Déplacez la règle de création récente au dessus.



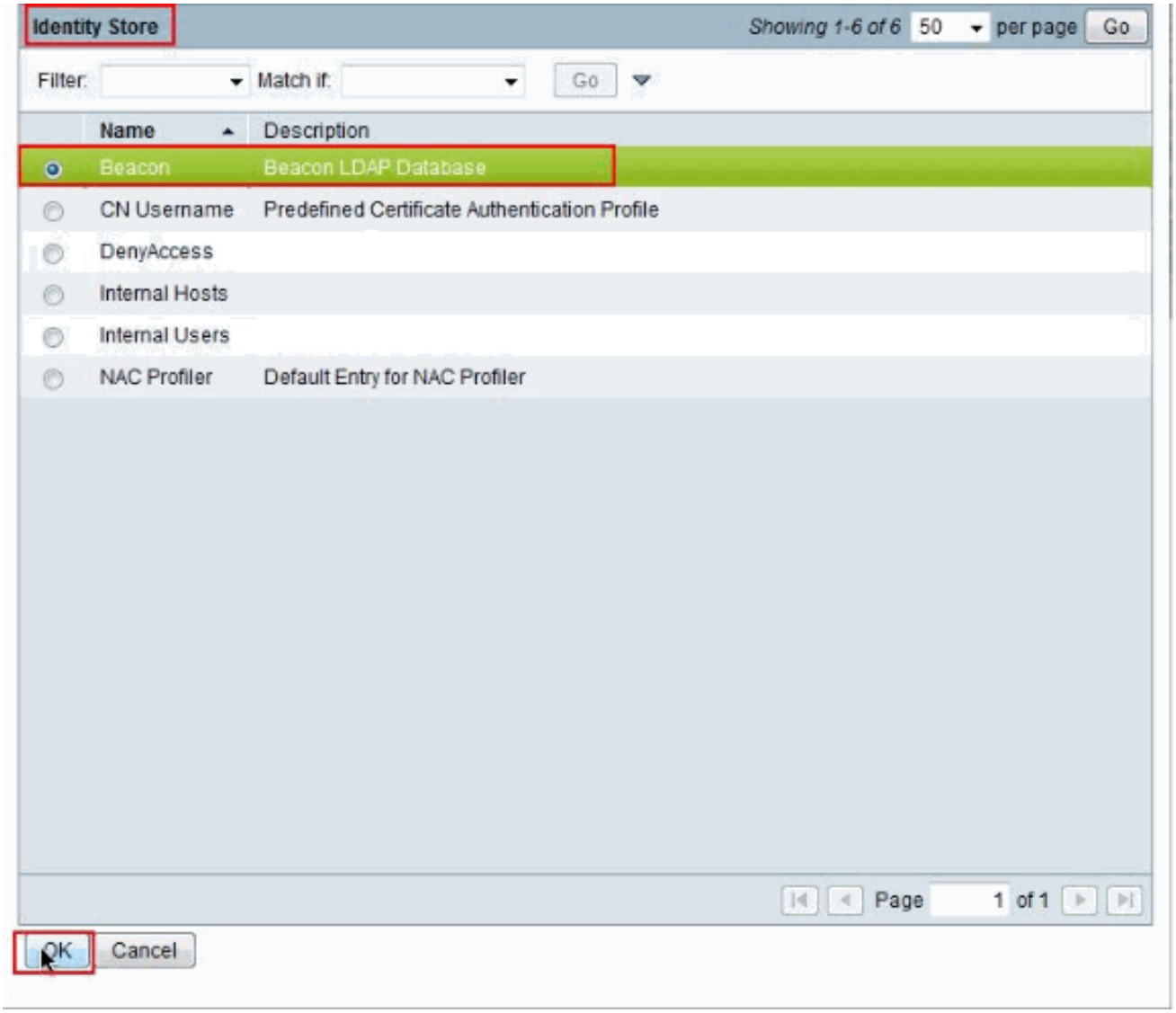
12. **Modifications de sauvegarde de** clic.



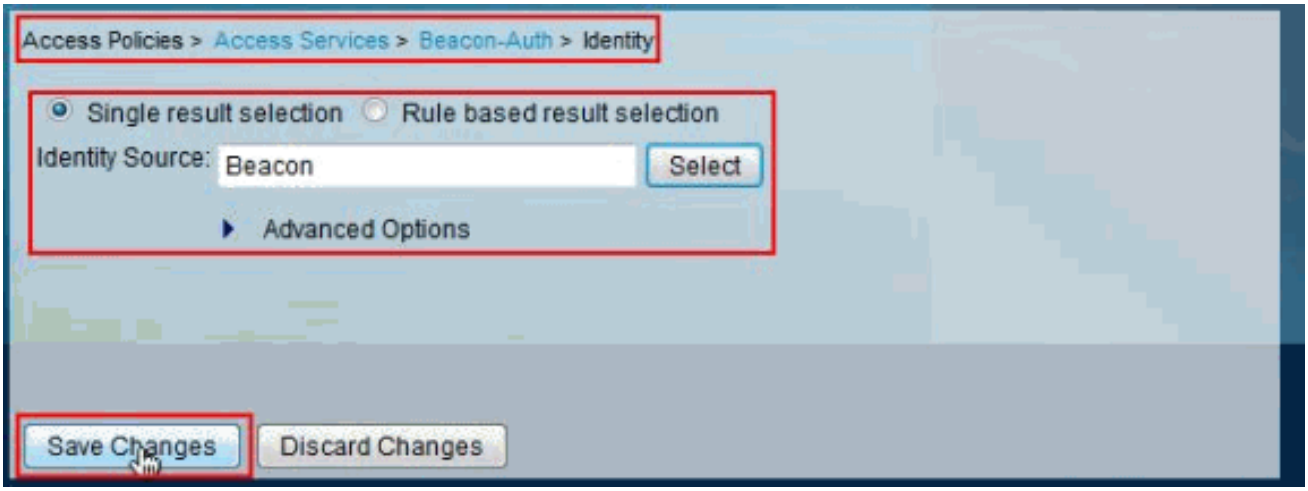
13. Choisissez les **stratégies > les services d'accès > la balise-Auth > l'identité d'Access** et cliquez sur **choisi** à côté de la **source d'identité**.



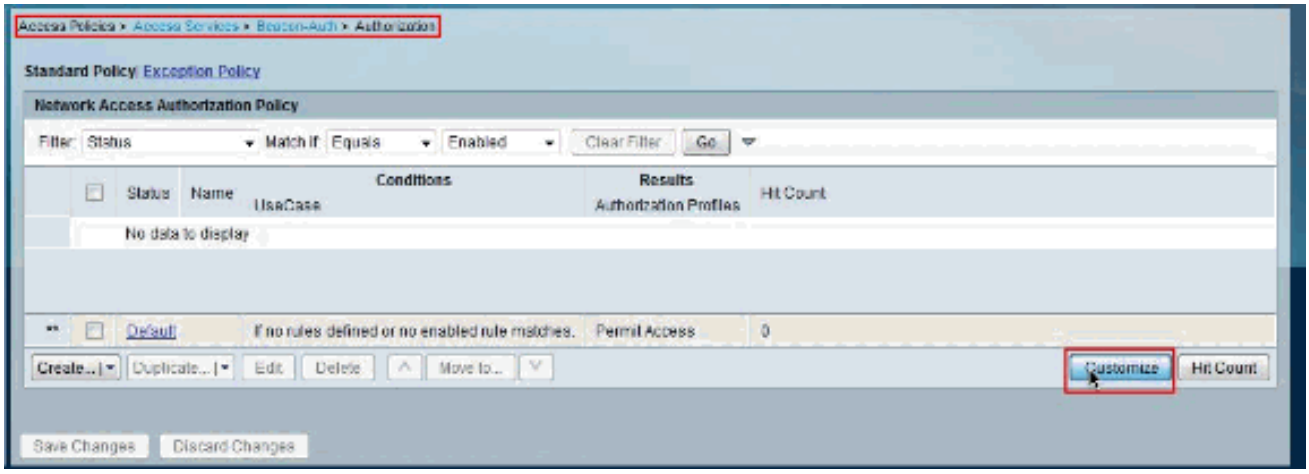
14. Choisissez la **balise** et cliquez sur OK.



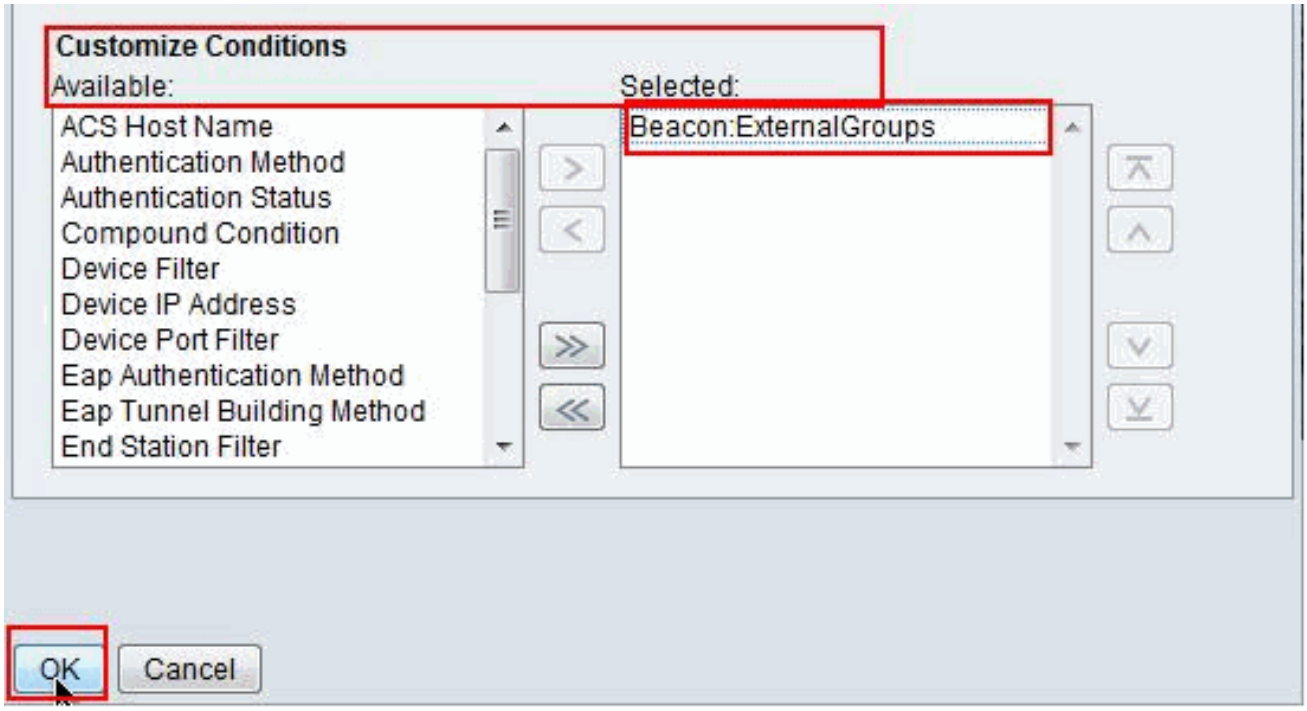
15. **Modifications de sauvegarde de**
clic.



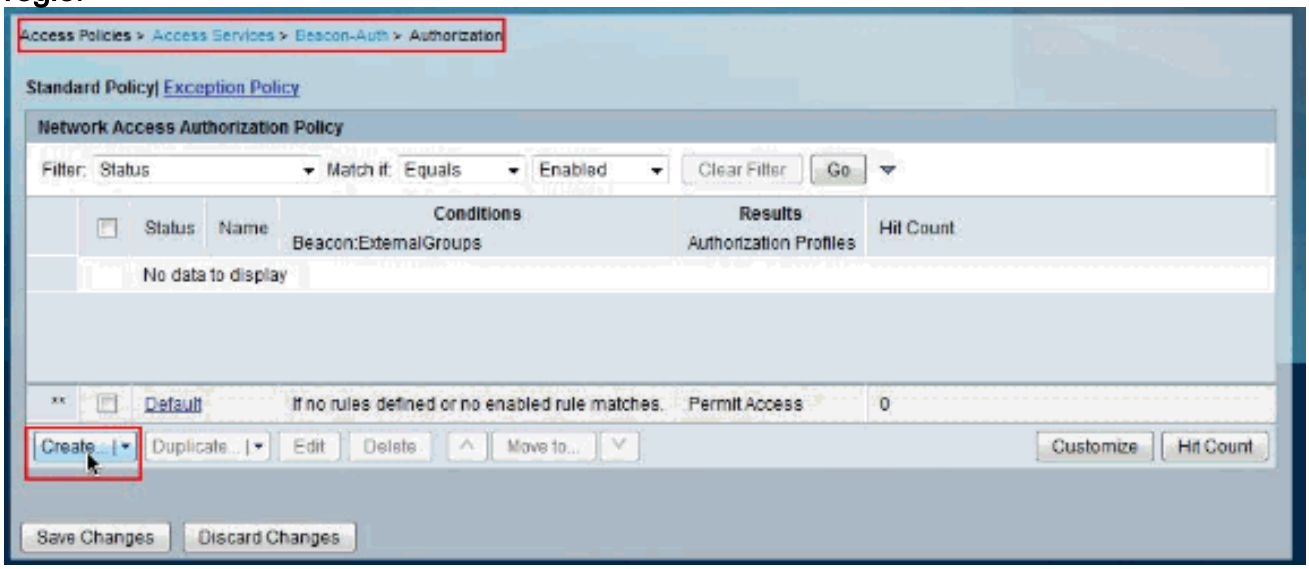
16. Choisissez les **stratégies > les services d'accès > la balise-Auth > l'autorisation d'Access** et le clic
personnalisent.



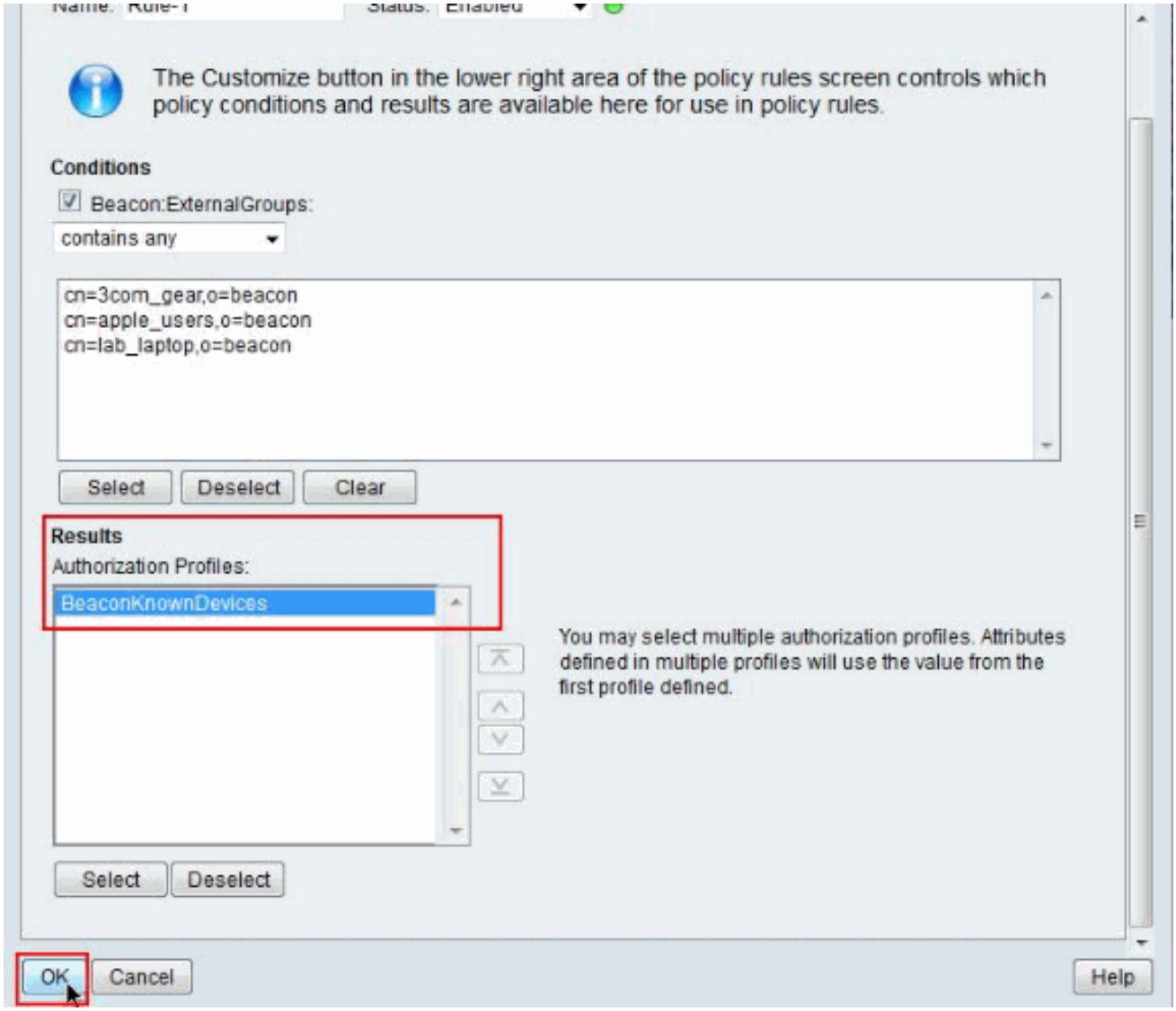
17. **Balise de** mouvement **: ExternalGroups de disponible a sélectionné** et clique sur OK.



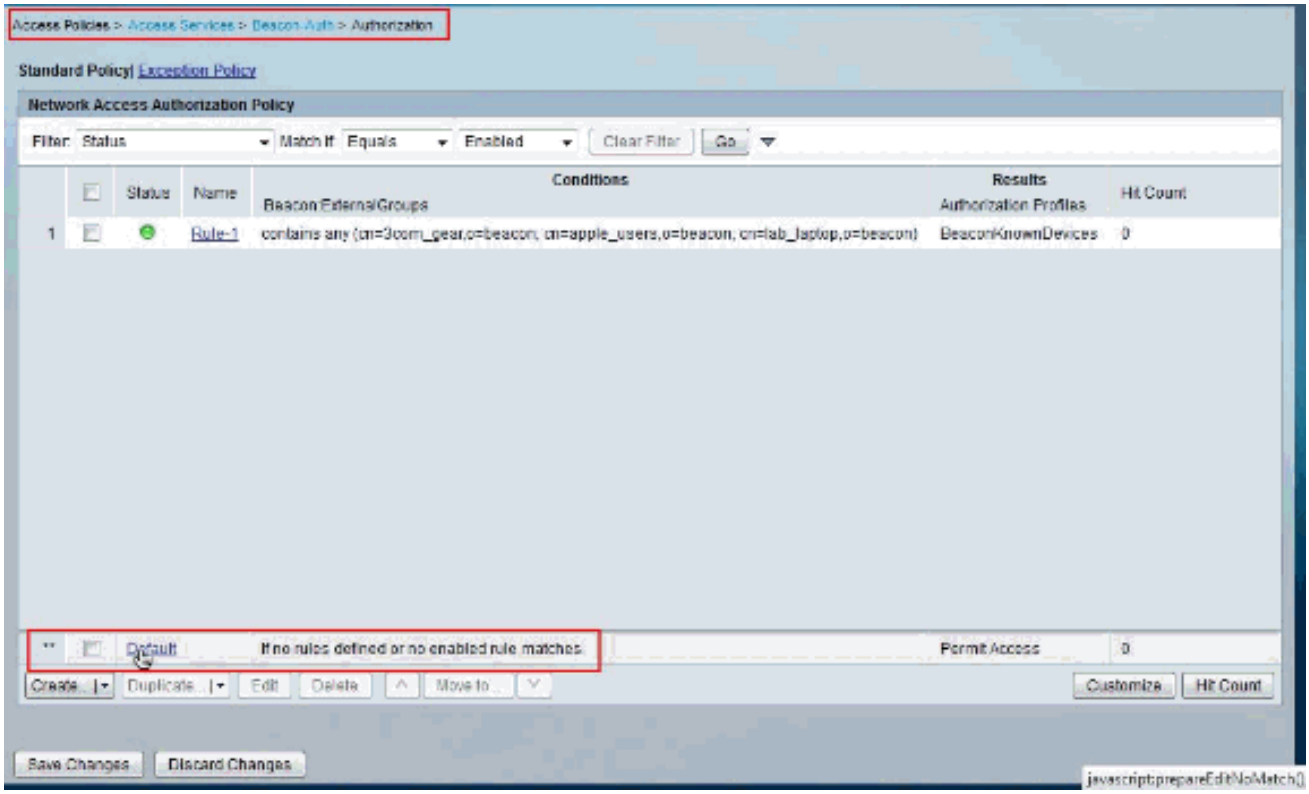
18. Le clic **créent** pour créer une nouvelle **règle**.



19. Choisissez 3com_users, apple_users et lab_laptop comme les conditions et l'autorisation profilent **BeaconKnownDevices** comme résultat. Puis, cliquez sur OK.

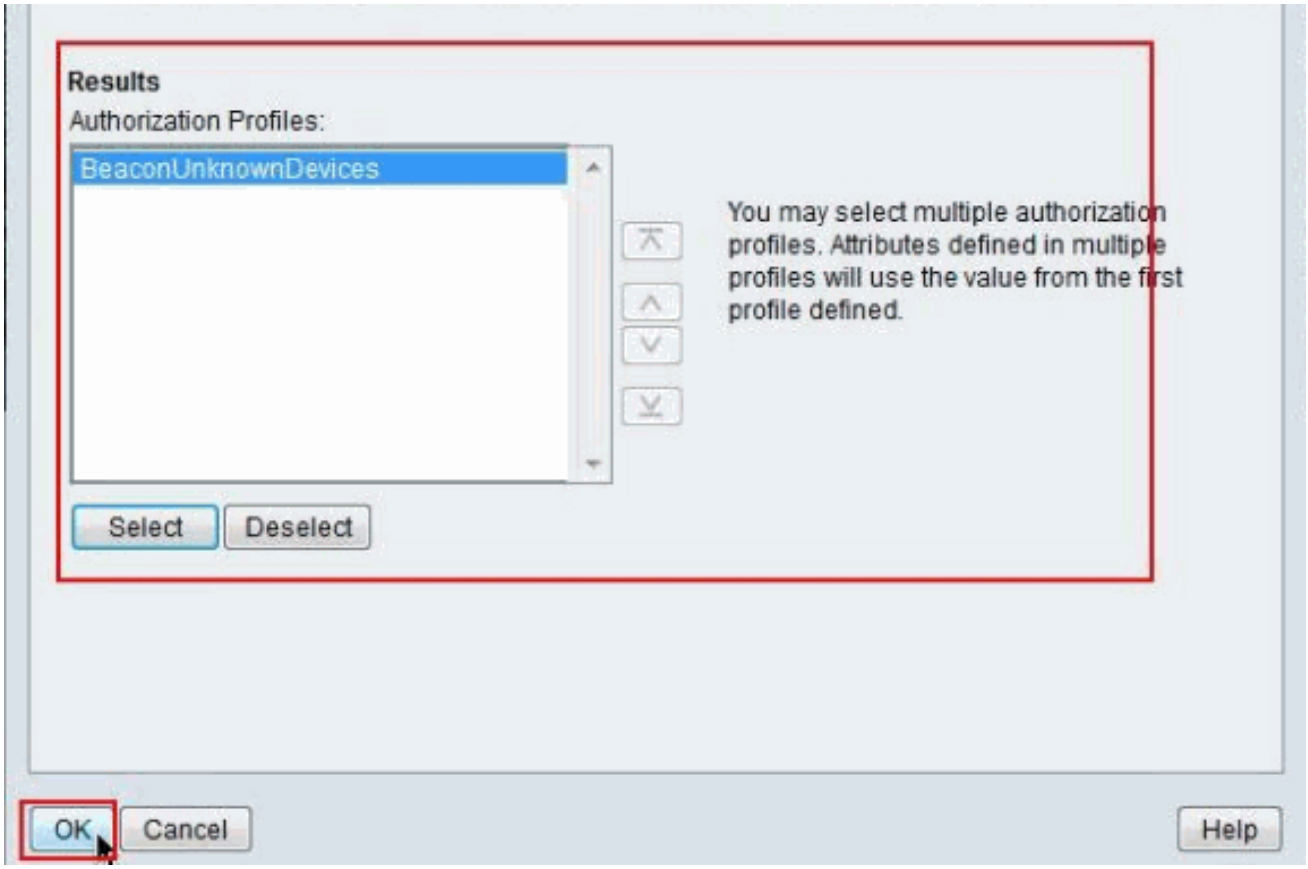


20. **Par défaut de**
clic.

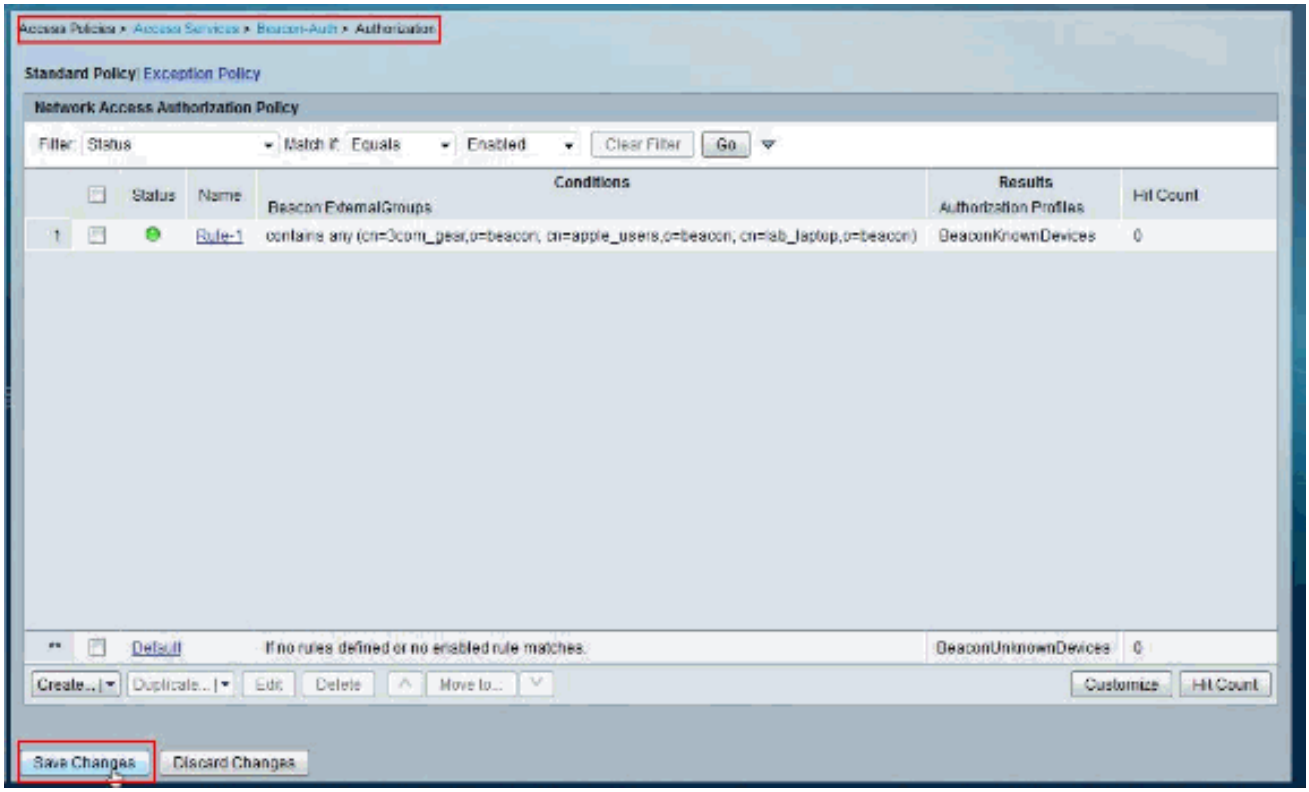


21. Choisissez 3com_users, apple_users et lab_laptop comme les conditions et l'autorisation

profilent **BeaconUnKnownDevices** comme résultat. Puis, cliquez sur OK.



22. **Modifications de sauvegarde de** clic.



Ceci remplit la procédure.

Commutez la configuration pour la dérivation d'authentification MAC

Cette configuration de commutateur fournit à un exemple de configuration pour l'authentification

de 802.1X le MAB activé, et à la réaffectation dynamique VLAN exigée afin d'appliquer des attributs RADIUS retournés de l'ACS.

Commutateur

```
switch#show running-config ! version 12.2 no service pad
service timestamps debug uptime service timestamps log
datetime service password-encryption service sequence-
numbers ! ! aaa new-model aaa authentication login
default line aaa authentication enable default enable
aaa authentication dot1x default group radius aaa
authorization network default group radius aaa
accounting dot1x default start-stop group radius ! aaa
session-id common switch 1 provision ws-c3750g-24ts ip
subnet-zero ip routing no ip domain-lookup ! ! ! ! ! !
dot1x system-auth-control no file verify auto spanning-
tree mode pvst spanning-tree extend system-id ! vlan
internal allocation policy ascending ! ! interface Port-
channel1 switchport trunk encapsulation dot1q switchport
trunk allowed vlan 5,7,9,10 ! interface Port-channel2
description LAG/trunk to einstein switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk ! interface Port-channel3
description "LAG to Edison" switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk ! interface
GigabitEthernet1/0/1 switchport trunk encapsulation
dot1q switchport trunk allowed vlan 5,7,9,10 channel-
group 1 mode passive ! interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,7,9,10 channel-group 1 mode passive !
interface GigabitEthernet1/0/3 switchport trunk
encapsulation dot1q switchport trunk allowed vlan
5,7,9,10 channel-group 1 mode passive ! interface
GigabitEthernet1/0/4 switchport access vlan 7 switchport
mode access ! interface GigabitEthernet1/0/5 switchport
access vlan 5 switchport mode access spanning-tree
portfast ! interface GigabitEthernet1/0/6 switchport
trunk encapsulation dot1q switchport trunk allowed vlan
5,7,9 switchport mode trunk switchport nonegotiate !
interface GigabitEthernet1/0/7 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/8 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/9 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/10 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/11 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/12 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/13 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/14 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/15 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/16 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/17 switchport access vlan 5
```

```
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/18 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/19 switchport mode access dot1x mac-
auth-bypass dot1x pae authenticator dot1x port-control
auto dot1x timeout quiet-period 10 dot1x timeout reauth-
period 60 dot1x timeout tx-period 10 dot1x timeout supp-
timeout 10 dot1x max-req 1 dot1x reauthentication dot1x
auth-fail max-attempts 1 spanning-tree portfast !
interface GigabitEthernet1/0/20 switchport mode access
dot1x mac-auth-bypass dot1x pae authenticator dot1x
port-control auto dot1x timeout quiet-period 10 dot1x
timeout reauth-period 60 dot1x timeout tx-period 10
dot1x timeout supp-timeout 10 dot1x max-req 1 dot1x
reauthentication dot1x auth-fail max-attempts 1
spanning-tree portfast ! interface GigabitEthernet1/0/21
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/22
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/23
switchport access vlan 10 spanning-tree portfast !
interface GigabitEthernet1/0/24 switchport access vlan
10 spanning-tree portfast ! interface
GigabitEthernet1/0/25 ! interface GigabitEthernet1/0/26
! interface GigabitEthernet1/0/27 ! interface
GigabitEthernet1/0/28 ! interface Vlan1 no ip address
shutdown ! interface Vlan5 ip address 10.1.1.10
255.255.255.0 ! interface Vlan9 ip address 10.9.0.1
255.255.0.0 ! interface Vlan10 ip address 10.10.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! interface Vlan11 ip address 10.11.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! ip default-gateway 10.1.1.1 ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.30.0.0
255.255.0.0 10.10.0.2 ip route 10.40.0.0 255.255.0.0
10.10.0.2 ip http server ip http secure-server ! ! snmp-
server community public RW snmp-server host 10.1.1.191
public radius-server host 10.10.0.100 auth-port 1645
acct-port 1646 key 7 05090A1A245F5E1B0C0612 radius-
server source-ports 1645-1646 ! control-plane ! ! line
con 0 password 7 02020D550C240E351F1B line vty 0 4
password 7 00001A0803790A125C74 line vty 5 15 password 7
00001A0803790A125C74 ! end
```

Vérifiez

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

Informations connexes

- Dispositif Cisco NAC (Clean Access)
- Système de contrôle d'accès sécurisé Cisco
- Support et documentation techniques - Cisco Systems