Contenu

Introduction

Ce document décrit les nouvelles caractéristiques dans le Cisco Identity Services Engine (ISE) qui permet à la redirection pour avoir lieu avec des périphériques d'accès de réseau tiers (NADs).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Écoulement d'invité sur ISE
- Protocoles de DN et DHCP

[Composants utilisés](#)

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

- Commutateur de gamme 2960 de Cisco Catalys
- Cisco ISE, version 2.1

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.

Informations générales

La fonctionnalité avancée comme l'invité, la posture et le Bring Your Own Device (BYOD) dans les réseaux modernes, exige la transmission directe entre le périphérique de client et le serveur d'AAA. Dans des versions précédentes ISE que ceci a été accompli en envoyant un dynamique réorientez URL et liste de contrôle d'accès (ACL) au NAD.

Il y a deux attributs obligatoires qui sont introduits un profil d'autorisation pour la redirection dans l'attribut-valeur Paris (AVs) :

- Paire AV de Cisco ? Réorientez l'URL : La valeur URL est dynamique et elle est créée pour chaque session. Les parties importantes de réorientent l'URL sont le nom de domaine qualifié par Fuly de noeud de service de stratégie (FQDN RPC) et l'ID de session.
- Paire AV de Cisco ? Réorientez l'ACL : Cette paire AV contient un nom d'ACL qui doit exister sur le NAD. Avec l'aide de cet ACL, le NAD décide si les paquets sont réorientés ou permis par le NAD.

L'approche traditionnelle de redirection peut seulement être mise en application avec des périphériques de Cisco NAD. Pour le support du tiers NAD, la redirection URL statique avait été ajoutée dans ISE 2.0. Tandis que cette approche est plus d'indépendant de plate-forme, elle exige toujours le support de redirection HTTP sur le NAD.

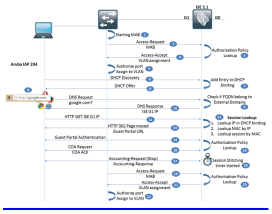
Commencer par ISE 2.1 qu'un nouveau style de réorientent a été ajouté. Cette approche n'exige pas le support de redirection HTTP sur le NAD. L'idée principale derrière cette méthode est d'utiliser l'ISE comme effondrement de DN.

Des DN et la fonctionnalité de serveur DHCP ont été ajoutés à la release ISE 2.1 afin de l'utiliser comme effondrement de DN. Maintenant le serveur ISE peut assigner des adresses IP aux utilisateurs qui doivent être réorientés et se définit en tant que serveur DNS. Ceci permet à ISE pour réorienter des connexions utilisateur à lui-même sans n'importe quelle fonctionnalité de web server sur le NAD. Cependant, le NAD devrait encore prendre en charge la modification de l'autorisation (COA) et de l'affectation dynamique VLAN.

Dans ISE, cette approche peut être utilisée pour ces écoulements de redirection :

- Écoulement d'invité : Les réponses ISE à toute demande de DN initiée par l'utilisateur avec sa propre adresse IP. Cette réponse fait établir le client une connexion HTTP avec ISE. À cet égard, ISE renvoie l'URL de réorientation utilisant la page standard du code 302 de HTTP déplacée.
- BYOD/Posture (Anyconnect seulement) ? dans les deux scénarios, l'application du ravitaillement de suppliant (NSP) ou le module indigène de posture d'Anyconnect initie une connexion à enroll.cisco.com, qui obtient réorienté à ISE utilisant les mêmes étapes que l'écoulement d'invité.

Flux des paquets



1. Le NAD commence le processus de MAB pour le périphérique connecté. Le processus de MAB sur Cisco commute des débuts selon la priorité de méthode d'authentification et pas avant que la première trame est reçue du périphérique d'extrémité.
2. L'Access-demande de MAB est envoyée à ISE.
3. ISE évalue la stratégie d'authentification et d'autorisation pour la demande entrante d'accès. Pendant l'évaluation de stratégie d'autorisation, le type de périphérique de réseau (configuration de niveau NAD) est comparé au type de périphérique de réseau défini dans le profil d'autorisation. Seulement des profils d'autorisation pour le type de périphérique assorti de réseau peuvent être sélectionnés.

   Remarque: Pour l'invité VLAN réorientez, ISE doit sélectionner un profil d'autorisation qui contiennent la redirection de Web (CWA, MDM, NSP, CPP) et l'affectation VLAN. La nécessité de client d'être assigné à un segment de réseau qui a ISE comme seul serveur DHCP.

1. ISE renvoie un Access-recevoir avec les informations VLAN.
2. Le commutateur autorise le port et applique les configurations VLAN.
3. Le DHCP d'initiés de client les découvrent. Si le PC se trouve dans le même segment qu'ISE, le paquet atteint l'ISE directement. En cas de Connectivité L3 entre le client et l'ISE, l'IP ISE devrait être configuré comme adresse auxiliaire IP sur le NAD pour le relais DHCP.
4. ISE ajoute les informations de client à sa table de liaison DHCP. L'IP de client et le MAC sont utilisés par ISE pour la consultation de session.
5. L'offre DHCP est envoyée au client. Dans cette offre, l'adresse IP ISE est spécifiée en tant que serveur DNS.
6. L'utilisateur ouvre un navigateur Web et navigue vers google.com qui déclenche une demande de DN à ISE.
7. ISE vérifie si le FQDN de cible appartient aux domaines externes. S'il fait, alors ISE envoie cette demande à un serveur DNS défini dans les configurations de pool DHCP. Sinon ISE renvoie sa propre adresse IP dans la réponse.
8. Le navigateur Web initie une connexion TCP à ISE et des demandes de google.com.
9. Àce stade consultations ISE la session authentifiée pour la requête HTTP GET entrante. C'est important pour construire le correct réorientent l'URL.

   Remarque: ISE utilise ces règles pour la consultation de session :
   1. IP de consultation en liaison DHCP
   2. MAC de consultation par l'IP
   3. Session de consultation par le MAC

1. ISE répond avec la page du HTTP 302 déplacée à l'URL de réorientation.
2. L'utilisateur est ainsi réorienté à l'invité portail et l'écoulement entier d'invité configuré sur ISE a lieu ici.
3. Après une authentification réussie d'invité, l'ISE fonctionne par les stratégies d'autorisation une fois de plus pour vérifier si des nouveaux attributs étaient ajoutés à la session et si le point final pendant l'écoulement d'invité exige la modification de l'autorisation (CoA). Une fois que la prochaine stratégie d'autorisation est identifiée, ISE prépare la demande CoA.
4. L'échange de la demande CoA/CoA ACK a lieu entre ISE et NAD. Un CoA de remise de rebond ou d'admin de port est une nécessité car ceci déclenche obtenir une nouvelle adresse IP dans la finale VLAN. Le NAD doit prendre en charge le rayon ou le CoA SNMP pour que cette étape fonctionne.

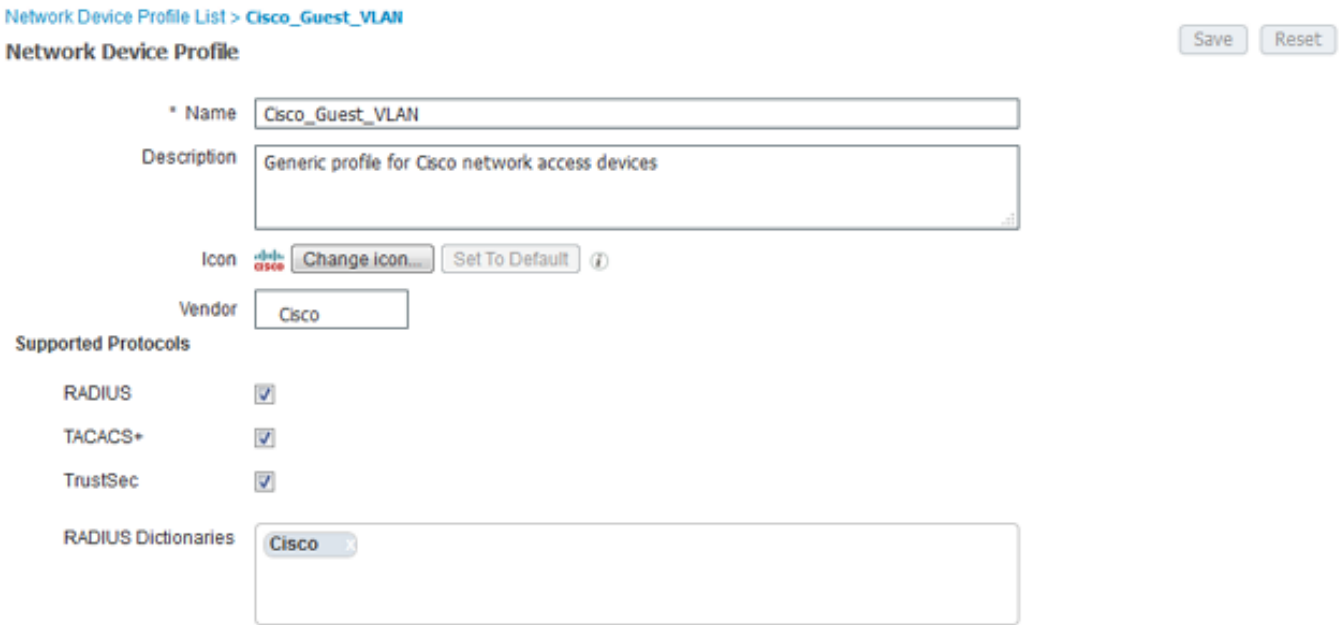
5. L'arrêt de Comptabilité-demande pour la session déconnectée est envoyé à ISE. ISE reconnaît cette demande en envoyant une Comptabilité-réponse.
6. ISE met en marche un temporisateur piquant de session (20 secondes par défaut). Pendant ce temps tous les attributs de session (ex : GUEST_TYPE, l'écoulement case=Guest d'utilisation) sont gardés par ISE. Au cas où une nouvelle demande d'accès du même ID de station d'appel serait reçue pendant ce temps, tous les attributs de session sont liés à la nouvelle session.
7. Une nouvelle Access-demande de MAB est envoyée pour le périphérique d'extrémité après que rebond de port CoA.
8. ISE identifie la stratégie d'authentification/autorisation pour la nouvelle demande. À ce stade ISE utilise des attributs de session et/ou des attributs de point final pour la sélection correcte de stratégie.
9. Access-Recevoir est envoyé avec les informations de la finale VLAN. Une liste de contrôle d'accès téléchargeable (DACL) peut être envoyée à la place, pour limiter le trafic sur le par défaut VLAN aussi bien.
10. Le commutateur autorise le port dans le nouveau VLAN et applique un DACL si inclus.

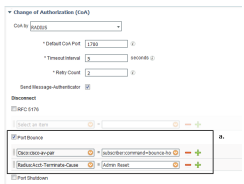
Configurez

Configurez ISE

1. Créez le profil de périphérique de réseau

Pour cet exemple particulier, Cisco commutent utilisé comme NAD. Par conséquent, le profil de périphérique existant de réseau de Cisco reproduit et modifié au besoin. Naviguez vers la gestion > les ressources de réseau > les profils de périphérique de réseau et ajoutez le nouveau profil.





2. Créez le périphérique de réseau

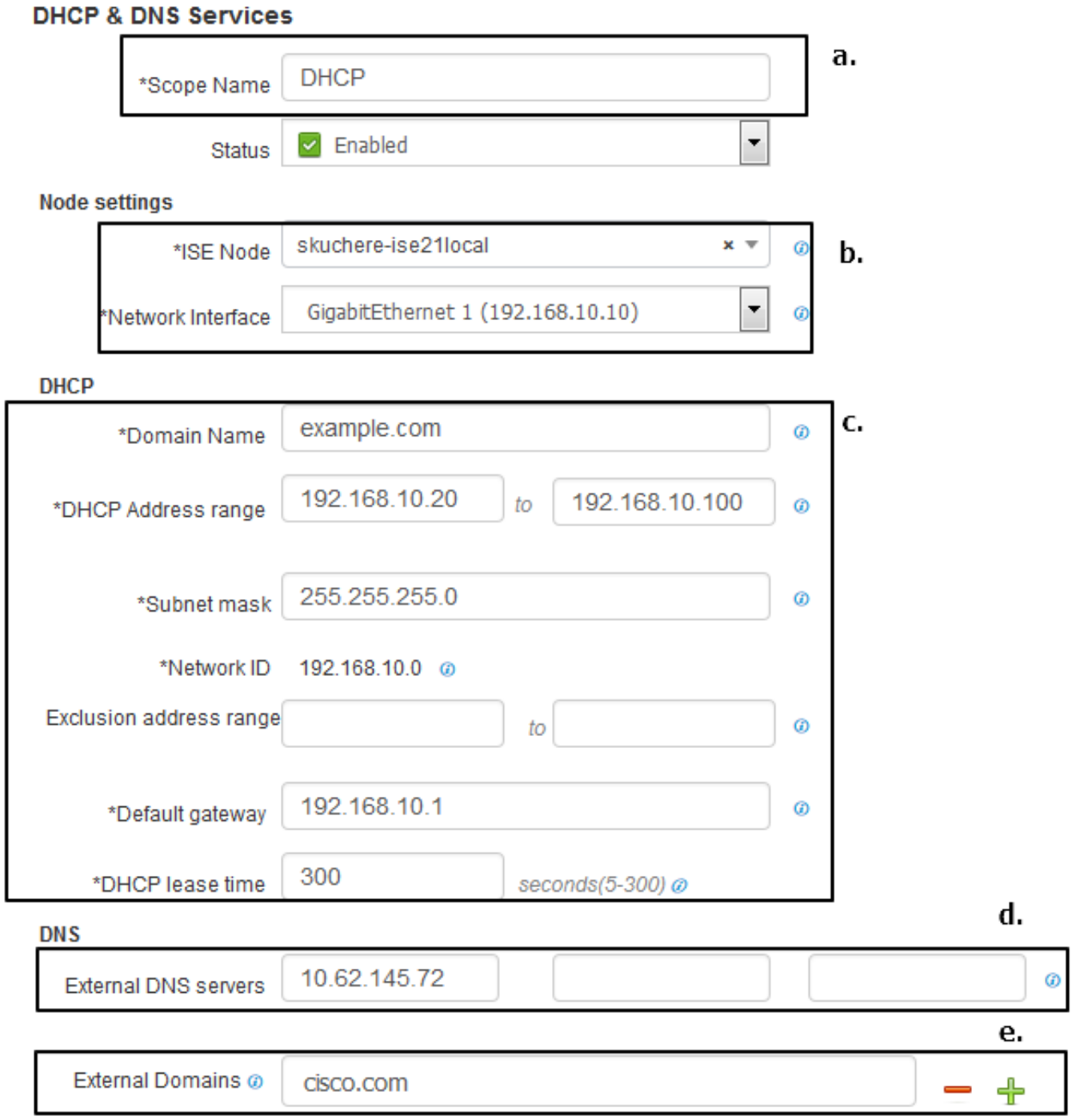
Naviguez vers la gestion > les ressources de réseau > les périphériques de réseau afin d'ajouter le nouveau périphérique.

a. Configuration de note pour le profil de périphérique de réseau.

b. Toutes autres configurations sont standard.

3. Configurez le serveur DHCP

Le groupe de serveur DHCP est lié à un noeud particulier ISE et à son interface. Naviguez vers la gestion > le système > les configurations > le DHCP et les services DNS > ajoutent



a. Les besoins de nom de portée de DHCP d'être configuré.

b. Sélectionnez le noeud sur lequel les DN et les services DHCP qui devraient s'exécuter et l'interface sur ce noeud qui devrait être utilisé.

c. Définissez la plage d'adresses IP DHCP, la passerelle par défaut, les adresses exclues de la portée et la durée de bail DHCP.

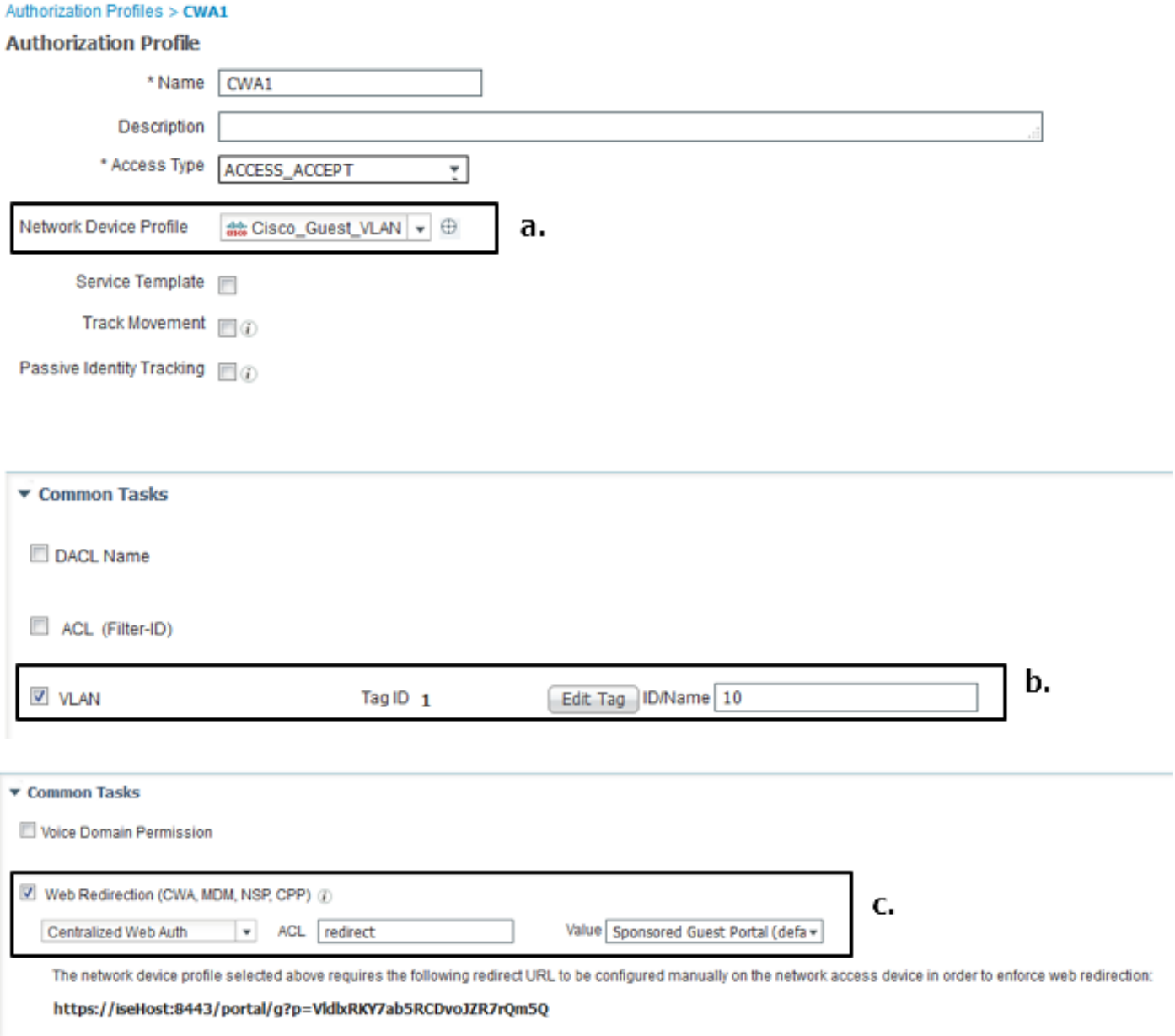
d. Sur option, définissez les adresses IP externes de serveur DNS. Ceux-ci devraient être questionnés pour les domaines externes.

e. Sur option, définissez les noms externes de domaines. L'ISE questionne les serveurs DNS externes et renvoie l'adresse IP réelle au lieu de ses propres moyens.

4. Configurez le profil d'autorisation

Naviguez vers la stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation. Deux profils d'autorisation sont nécessaires pour l'écoulement complet d'invité :

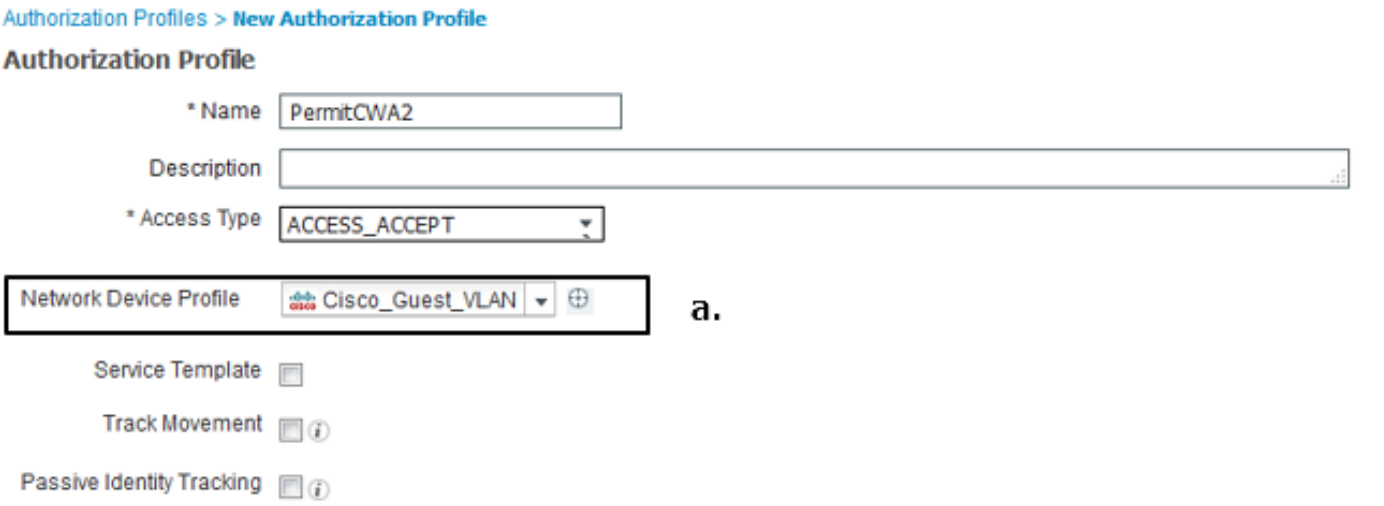
- Réorientez le profil d'autorisation (CWA1)
- Profil d'autorisation d'Access d'autorisation (PermitCWA2)

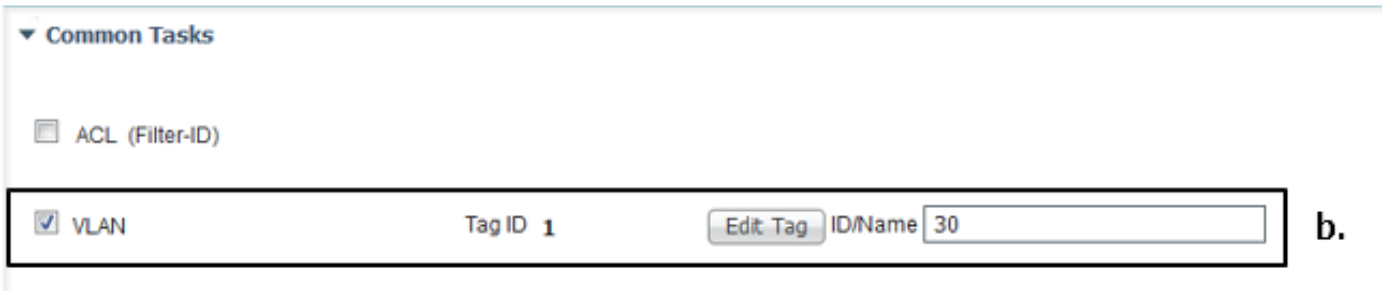


a. Profil de périphérique de réseau : Seulement les demandes d'authentification provenant NADs assigné à ce profil peuvent avoir comme conséquence ce profil d'autorisation,

configurations **B.** VLAN : Les VLAN définis ici doivent exister sur le NAD. Est-ce queinterface ISE configurée pour le DHCP devrait ou appartenir à ce VLAN ou devrait être configurée comme aide IP sur la passerelle entretenant ce VLAN.

c. Réorientez les configurations : Pour l'exemple en cours l'authentification Web centrale a été définie en tant que réorientent type, et portail commandité d'invité défini comme portail d'invité. La forme demande toujours le nom d'ACL de réorientation. Puisque le profil de périphérique de réseau a été modifié pour l'URL statique réorientez, ce nom d'ACL ne sera jamais envoyé au NAD.



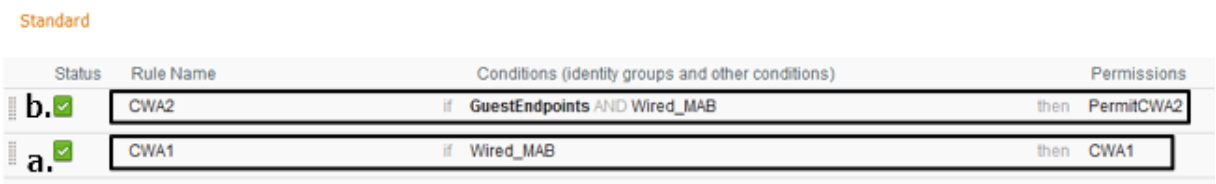


a. Profil de périphérique de réseau : Seulement les demandes d'authentification provenant NADs assigné à ce profil peuvent avoir comme conséquence ce profil d'autorisation,

configurations **B.** VLAN : Après avoir assigné un port de client à ce VLAN, l'utilisateur devrait obtenir une adresse IP d'un serveur DHCP régulier.

5. Configurez les stratégies d'autorisation pour l'accès invité

Naviguez vers la stratégie > l'autorisation. Configurez deux stratégies : un pour réorientent l'action et l'autre pour l'accès client après authentification sur le portail d'invité.



a. La première stratégie d'autorisation apparie le MAB de câble pendant qu'une méthode d'authentification et le profil d'autorisation de réorientation est assignée en conséquence.

b. La deuxième stratégie d'autorisation peut être basée sur des attributs de session (écoulement de cas d'utilisation = d'invité/type groupe externe d'invité d'AD si des utilisateurs d'invité authentifiés utilisant l'AD) ou sur des attributs de point final (groupe d'identité de point final). L'enregistrement de périphérique doit être activé sur le portail d'invité utiliser le groupe d'identité de point final.

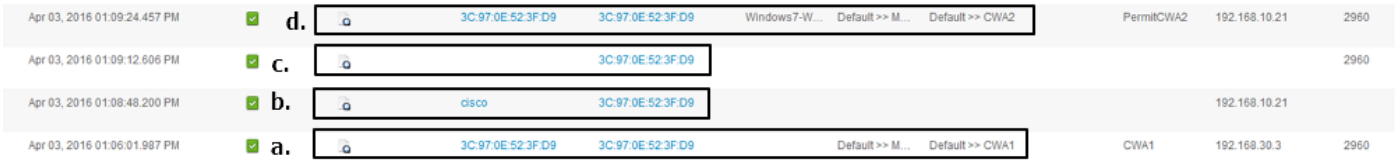
Configurez le NAD

Cisco commutent a été configuré pour le MAB sur l'interface et a le support COA.

> Remarque: Le centre d'assistance technique Cisco (TAC) n'offre aucun soutien de configuration de la tierce partie NADs.

Vérifiez

Un écoulement réussi d'invité ressemble à ceci dans les exécutions > le rayon Livelog ISE :



a. C'est la première authentification de MAB. Le profil d'autorisation avec réorientent est sélectionné en conséquence.

b. C'est l'authentification d'invité. Après que cette action ISE fasse une réévaluation de stratégie pour décider si le CoA est nécessaire.

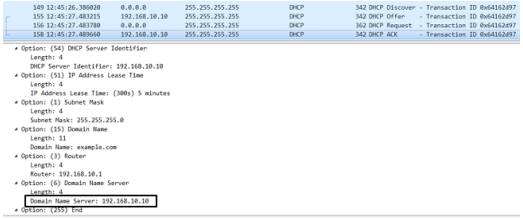
c. Un CoA a été avec succès terminé.

d. C'est la deuxième authentification de MAB. Le profil d'autorisation pour l'accès invité est sélectionné en conséquence.

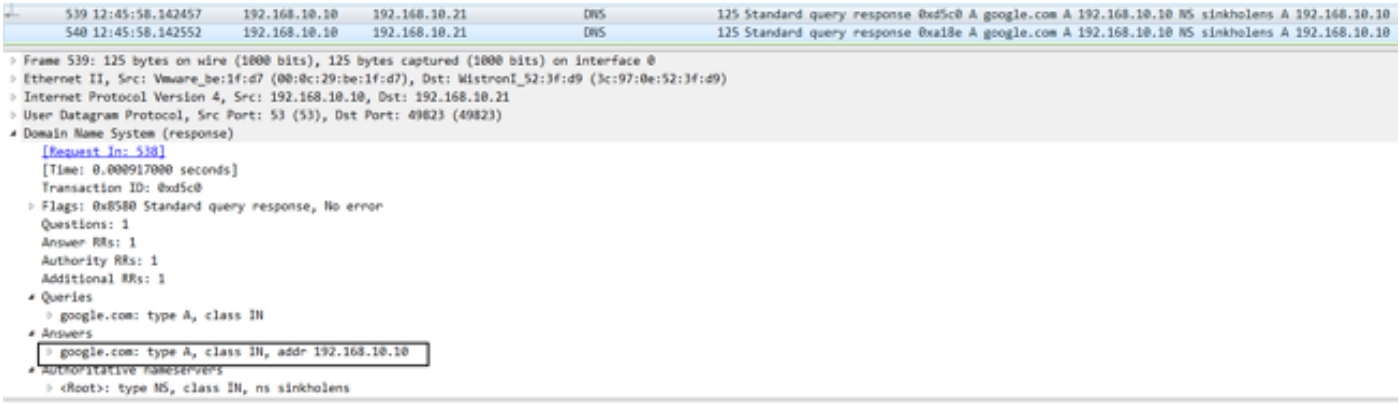
Dépannez

Vérifiez si l'adresse IP est assignée au client correctement. Ceci peut être fait en collectant une capture de paquet sur le client ou l'ISE.

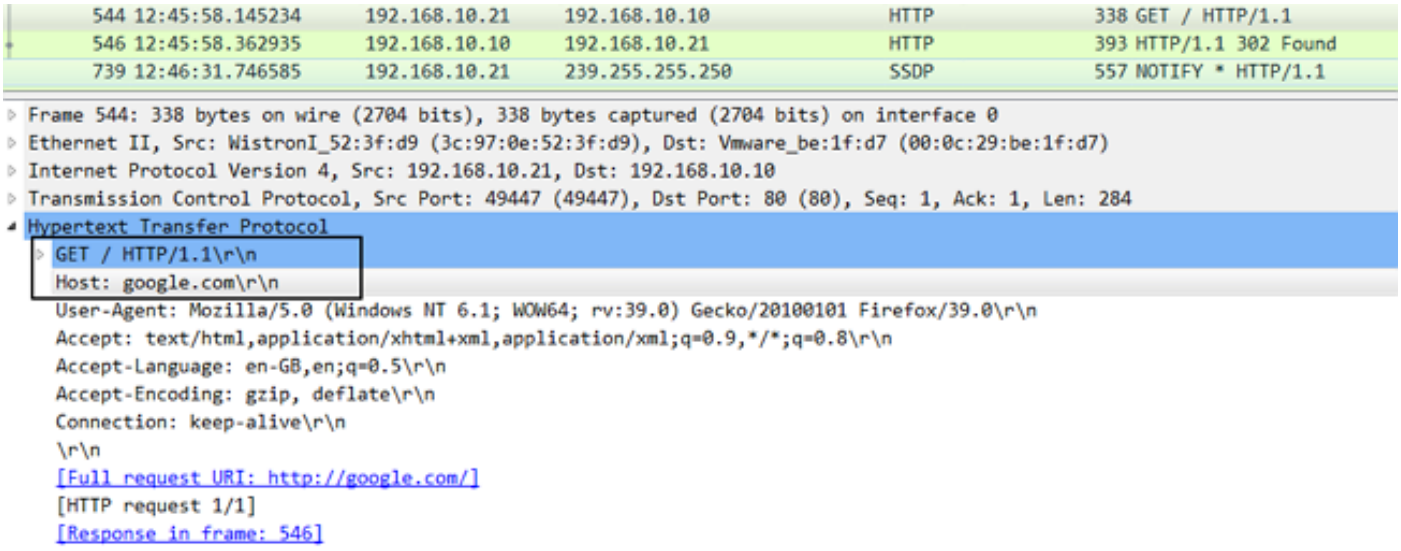
Cette capture du client affiche à une prise de contact réussie DHCP avec l'IP de DN mêmes que l'ISE.



Vérifiez s'ISE agit correctement en tant qu'effondrement de DN. Une capture de paquet peut aider à confirmer si la demande va à ISE et si l'ISE répond à lui avec sa propre adresse IP :



Vérifiez si le HTTP réorientent des travaux correctement. Après qu'il obtienne l'adresse IP de ressource et établisse une connexion TCP à ISE, le client envoie une requête HTTP GET à l'ISE. Ceci peut être confirmé dans une capture de paquet de côté client :



En même temps, ISE détermine si n'importe quelle session existe pour ce client. Ce processus de consultation de session sur ISE peut être signé log de prrt-Gestion :

Après la consultation de session, ISE renvoie l'URL de réorientation au client dans une réponse du HTTP 302 :