Exemple de configuration sans fil hors bande (OOB) NAC

Contenu

Introduction

Ce document fournit des instructions de conception pour le déploiement hors bande (OOB) d'un système de sécurité des terminaux de Cisco Network Admission Control (NAC) dans un réseau sans fil Cisco Unified. Ces recommandations de pratique recommandée supposent qu'un réseau sans fil unifié Cisco a été déployé selon les instructions fournies du guide 3.0 de conception de mobilité d'entreprise.

La conception recommandée est la passerelle virtuelle (mode de passerelle) et solution centrale du déploiement OOB avec l'ouverture de session simple de RADIUS. Le contrôleur Sans fil de réseau local (WLC) doit être L2 placé à côté du serveur NAC. Le client s'associe au WLC, et WLC authentifie l'utilisateur. Une fois que l'authentification est terminée, le trafic d'utilisateur passe par la quarantaine VLAN du WLC au serveur NAC. Le processus d'estimation et de correction de

posture ont lieu. Une fois que l'utilisateur est certifié, l'utilisateur VLAN change de la quarantaine pour accéder au VLAN dans le WLC. Le trafic évite le serveur NAC une fois déplacé pour accéder au VLAN.

Conditions préalables

Conditions requises

Cette configuration de document est spécifique à la release NAC 4.5 et WLC 5.1

Composants utilisés

Ce document est t limité au logiciel et aux versions de matériel spécifiques.

- Serveur 3350 NAC 4.5
- Gestionnaire 3350 NAC 4.5
- WLC 2106 5.1

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.

Conventions

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

Informations générales

Aperçu de Cisco NAC

Le Cisco NAC emploie l'infrastructure réseau pour imposer la conformité de stratégie de sécurité sur tous les périphériques qui recherchent à accéder au réseau calculant des ressources. Avec l'appliance de Cisco NAC, les administrateurs réseau peuvent authentifier, autorisent, évaluent, et remediate de câble, radio, et utilisateurs distants et leurs ordinateurs avant l'accès au réseau. L'appliance de Cisco NAC identifie si les périphériques en réseau tels que des ordinateurs portables, des Téléphones IP, ou des consoles de jeux sont conformes avec des stratégies de sécurité réseau, et répare toutes les vulnérabilités avant qu'elle permette l'accès au réseau.

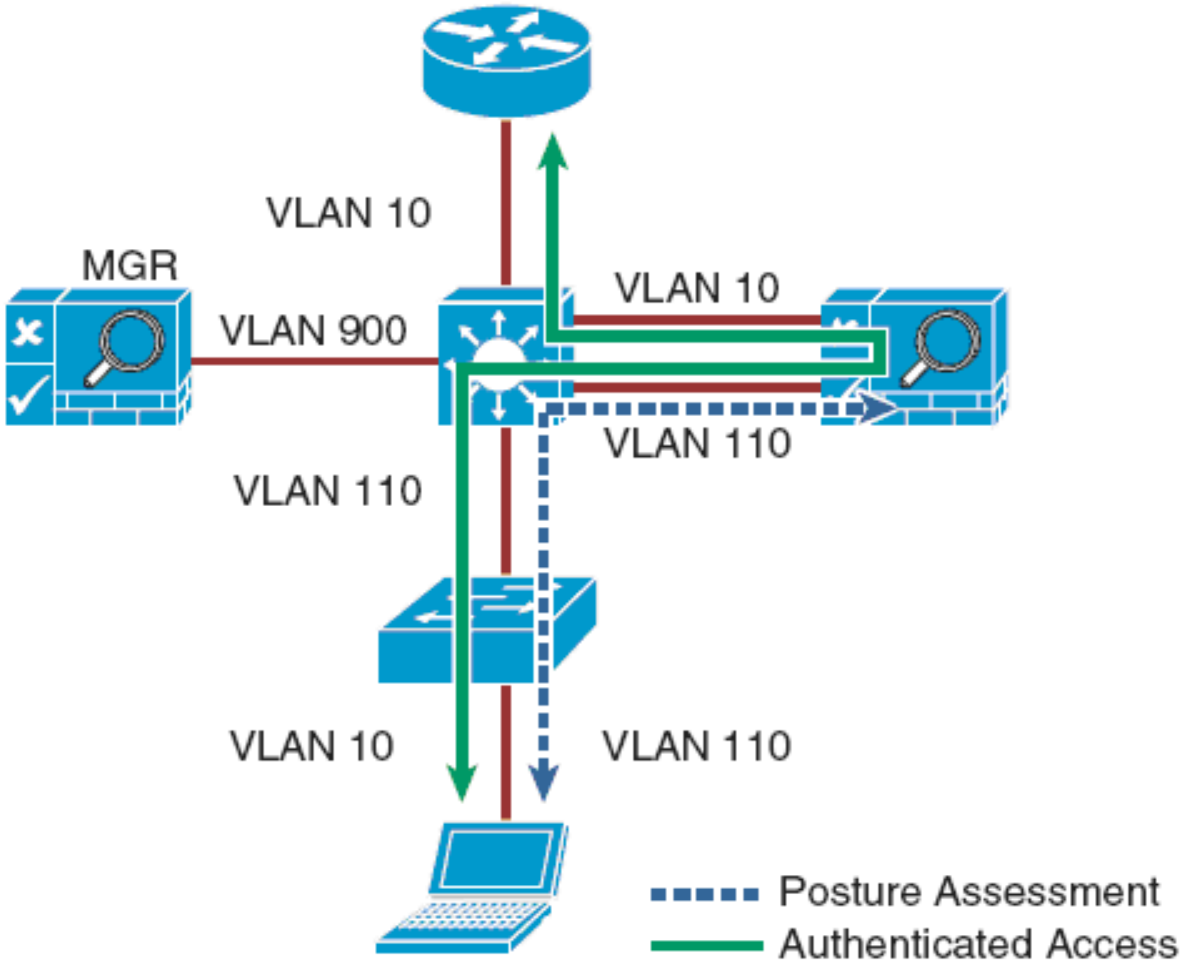
La terminologie de la conception recommandée est discutée :

Mode virtuel de passerelle (mode de passerelle)

Quand l'appliance NAC est configurée comme passerelle virtuelle, elle agit en tant que passerelle entre les utilisateurs finaux et la passerelle par défaut (routeur) pour le sous-réseau de client qui est géré. Pour un client donné VLAN, les ponts en appareils NAC trafiquent de son interface non approuvée à son interface de confiance. Quand il agit en tant que passerelle du côté non approuvé au côté de confiance de l'appliance, deux VLAN sont utilisés. Par exemple, le client

VLAN 110 est défini entre le contrôleur LAN Sans fil (WLC) et l'interface non approuvée de l'appliance NAC. Il n'y a aucune interface conduite ou a commuté l'interface virtuelle (SVI) associée avec VLAN 110 sur le commutateur de distribution. Le VLAN 10 est configuré entre l'interface de confiance de l'appliance NAC et le routeur du prochain saut interface/SVI pour le sous-réseau de client. Une règle de mappage est établie dans l'appliance NAC cette les paquets de forwards qui arrivent sur VLAN 110 VLAN 10 quand il permute les informations de balise VLAN suivant les indications de la figue 1-1. Le processus est renversé pour les paquets qui reviennent au client. Notez que, en ce mode, des BPDU ne sont pas passés du non approuvé-side VLAN à leurs homologues de faire confiance-side. L'option de mappage VLAN est habituellement choisie quand l'appliance NAC est logiquement en ligne placé entre les clients et les réseaux qui sont protégés. Cette option traversière doit être utilisée si l'appliance NAC doit être déployée en mode virtuel de passerelle avec un déploiement Sans fil unifié. Puisque le serveur NAC se rend compte des *protocoles de couche supérieure*, par défaut il permet explicitement les protocoles qui exigent de lui de se connecter au réseau dans le rôle authentifié, par exemple, les DN et le DHCP.

Passerelle virtuelle de figure 1-1 avec la cartographie VLAN

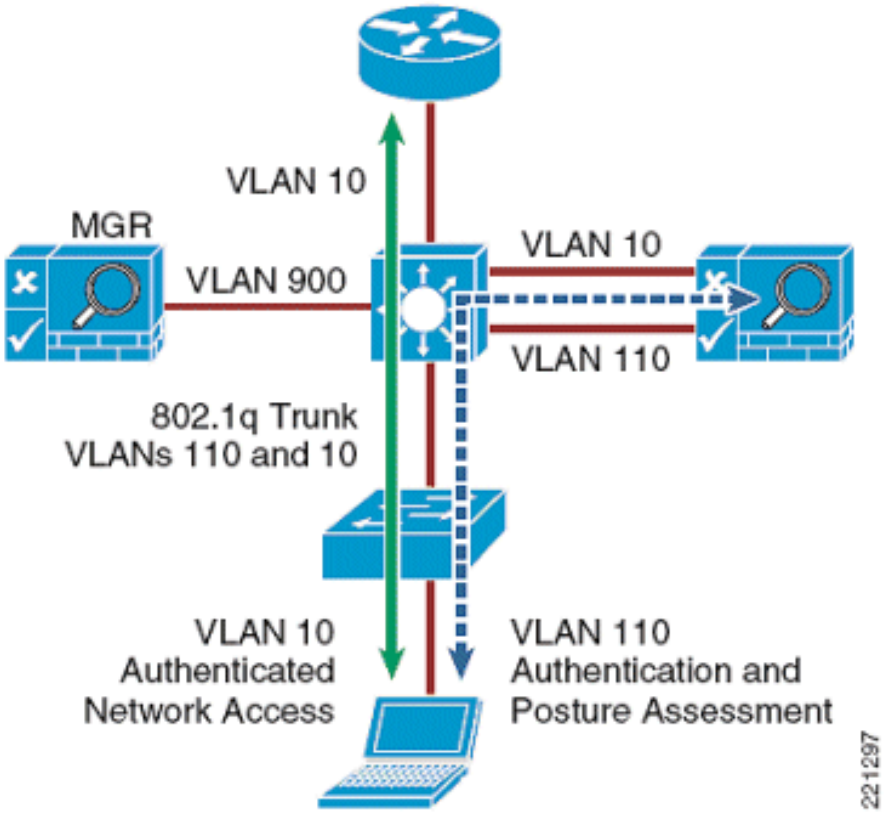


Mode hors bande

Les déploiements hors bande exigent du trafic d'utilisateur de traverser par l'appliance NAC seulement dans l'authentification, l'estimation de posture, et la correction. Quand un utilisateur est authentifié et passe tous les contrôles de stratégie, le trafic est commuté normalement par le réseau et évite le serveur NAC. Pour de plus amples informations, référez-vous au chapitre 4 de l'installation et du guide d'administration Appliance-propres d'Access Manager de Cisco NAC.

Quand l'appliance NAC est configurée de cette manière, le WLC est un périphérique géré dans le gestionnaire NAC de la même manière que cela que Cisco commutent est géré par le gestionnaire NAC. Après que l'utilisateur soit authentifié et passe l'estimation de posture, le gestionnaire NAC demande au WLC pour étiqueter le trafic d'utilisateur du NAC VLAN pour accéder au VLAN qui offre des privilèges d'accès.

Appliance de la figure 1-2 NAC en mode hors bande avec le mode virtuel de passerelle



Ouverture de session simple

L'ouverture de session simple (SSO) est une option qui n'exige pas l'intervention de l'utilisateur et est relativement simple pour implémenter. Il se sert de la capacité VPN SSO de la solution NAC, ajoutée au logiciel de Clean Access Agent qui fonctionne sur le PC client. VPN SSO emploie des enregistrements des comptes de RADIUS pour informer l'appliance NAC sur les utilisateurs authentifiés d'Accès à distance qui se connectent au réseau. De la même manière, cette caractéristique peut être utilisée en même temps que le contrôleur WLAN pour informer automatiquement le serveur NAC sur les clients sans fil authentifiés qui se connectent au réseau.

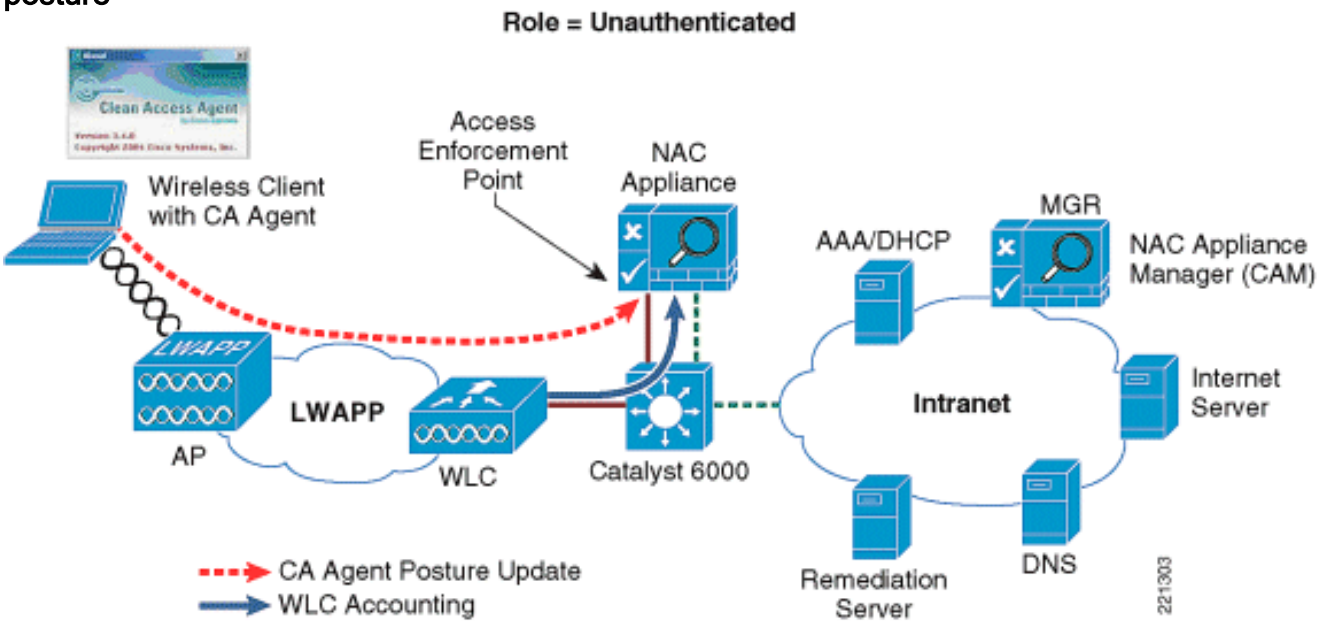
Voir les figures 1-3 par 1-6 pour des exemples d'un client Sans fil qui exécute l'authentification SSO, l'estimation de posture, la correction, et l'accès de réseau par l'appliance NAC.

Cet ordre est affiché dans la figure 1-3 :

1. L'utilisateur de sans fil exécute l'authentification 802.1x/EAP par le contrôleur WLAN à un serveur en amont d'AAA.
2. Le client obtient une adresse IP de l'AAA ou d'un serveur DHCP.
3. Après que le client reçoive une adresse IP, le WLC en avant un enregistrement de comptabilité de RADIUS (début) à l'appliance NAC, qui inclut l'adresse IP du client sans

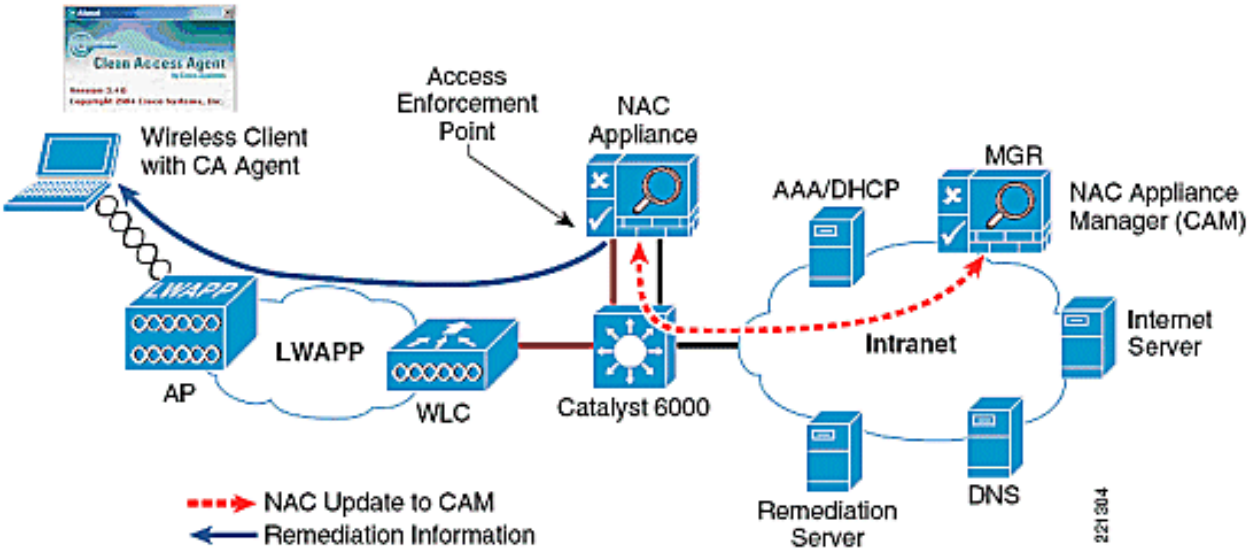
fil.**Remarque:** Le contrôleur WLC utilise un enregistrement des comptes simple de RADIUS (début) pour l'authentification client de 802.1x et l'affectation d'adresse IP, alors que les commutateurs Cisco Catalyst envoient deux enregistrements des comptes : un début de comptabilité est envoyé après l'authentification client de 802.1x, et une mise à jour intérimaire est envoyée après que le client soit assigné une adresse IP.

4. Après qu'il détecte la connexion réseau, les tentatives d'agent NAC de se connecter au CAM (avec le protocole SUISSE). Le trafic est intercepté par le serveur NAC, qui, consécutivement, questionne le gestionnaire NAC pour déterminer si l'utilisateur est dans la liste d'utilisateur en ligne. Seulement les clients qui sont authentifiés sont dans la liste d'utilisateur en ligne, qui est le cas dans l'exemple ci-dessus en raison de la mise à jour de RADIUS dans l'étape 3.
5. L'agent NAC exécute une estimation locale de la posture de Sécurité/risque de la machine cliente et en avant l'estimation au serveur NAC pour la détermination d'admission au réseau.**Procédé d'authentification client de figure 1-3 et estimation de posture**



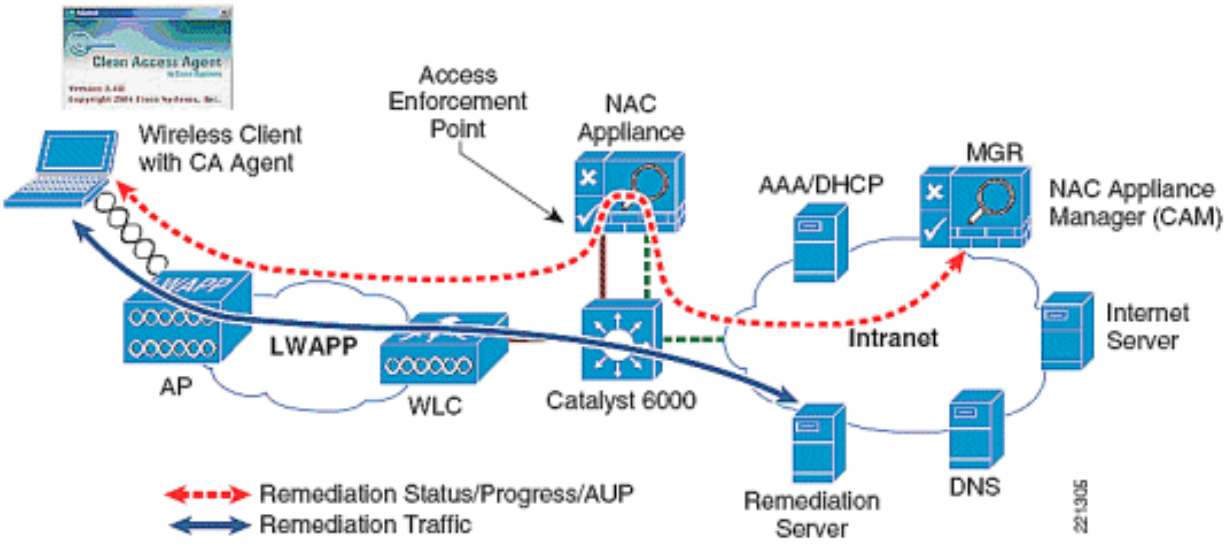
Cet ordre a lieu dans la figure 1-4 :

1. L'appliance NAC en avant l'estimation d'agent au gestionnaire d'appareils NAC (CAM).
2. Dans cet exemple, le CAM détermine que le client n'est pas dans la conformité et demande à l'appliance NAC pour mettre l'utilisateur dans un rôle de quarantaine.
3. L'appliance NAC envoie alors les informations de correction à l'agent client.**L'information sur l'évaluation de posture de figure 1-4 du CAS au CAM**



Cet ordre a lieu dans la figure 1-5 :

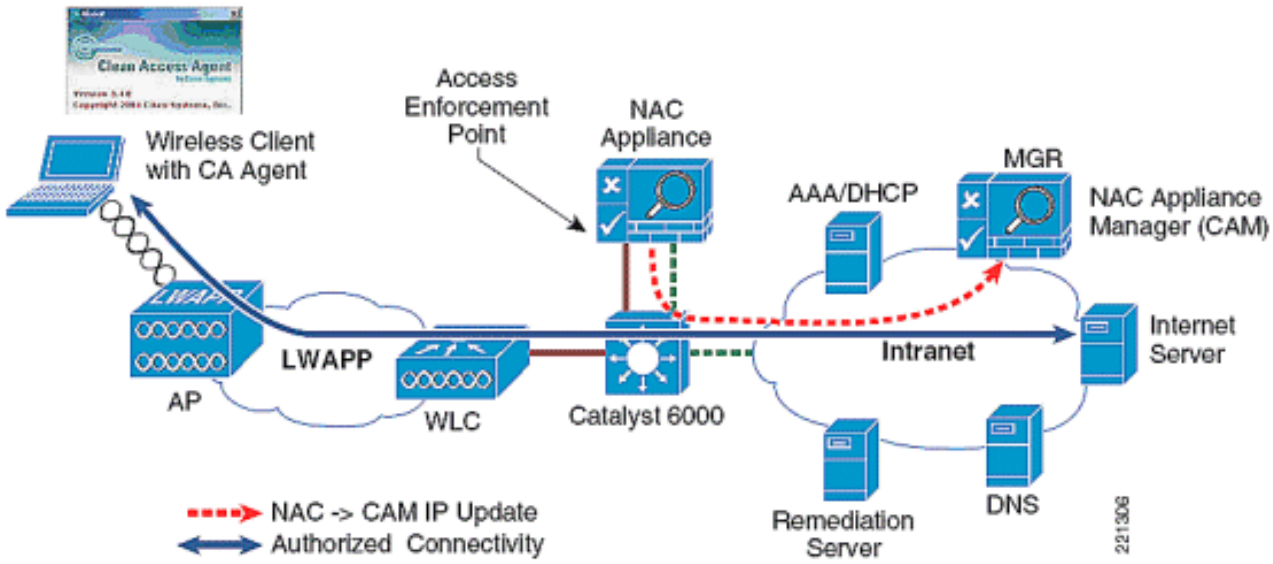
1. L'agent client affiche le temps qui demeure pour accomplir la correction.
2. L'agent guide le pas à pas d'utilisateur par le procédé de correction ; par exemple, dans la mise à jour du fichier de définition d'antivirus.
3. Après fin de correction, l'agent met à jour le serveur NAC.
4. Le CAM affiche une déclaration de la Politique d'Utilisation Acceptable (AUP) à l'utilisateur.**Procédé de correction de client de figure 1-5 avec le CAS comme périphérique d'application**



Cet ordre a lieu dans la figure 1-6 :

1. Après qu'il reçoive l'AUP, l'appliance NAC commute l'utilisateur à un rôle (autorisé) en ligne.
2. La fonctionnalité SSO remplit liste d'utilisateur en ligne avec l'adresse IP de client. Après correction, une entrée pour l'hôte est ajoutée à la liste certifiée. Chacun des deux tables (ainsi que la table découverte de clients) sont mises à jour par le CAM (gestionnaire d'appareils NAC).
3. Le gestionnaire NAC envoie un SNMP écrivent la notification à WLC pour changer l'utilisateur VLAN de la quarantaine pour accéder au VLAN.
4. Les débuts du trafic d'utilisateur pour laisser le WLC avec la balise de l'accès VLAN. Le serveur NAC n'est plus dans le chemin pour ce trafic d'utilisateur particulier.**La figure 1-6 a certifié le contournement de client le CAS en commutant plus de pour accéder au**

VLAN



La méthode la plus transparente pour faciliter l'authentification d'utilisateur de sans fil est d'activer l'authentification VPN-SSO sur le serveur NAC et de configurer le WLCs pour expédier RADIUS rendant compte au serveur NAC. Au cas où des enregistrements des comptes devraient être expédiés à un en amont de serveur de RADIUS dans le réseau, le serveur NAC peut être configuré pour expédier le paquet de comptabilité au serveur de RADIUS.

Remarque: Si l'authentification VPN-SSO est activée sans agent de Clean Access installé sur le PC client, l'utilisateur encore est automatiquement authentifié. Cependant, ils ne sont pas automatiquement connectés par l'appliance NAC jusqu'à ce que leur navigateur Web soit ouvert et une tentative de connexion est faite. Dans ce cas, quand l'utilisateur ouvre leur navigateur Web, ils sont momentanément réorientés (sans message d'entrée en communication) dans la phase « sans agent ». Quand le processus SSO est complet, ils sont connectés à leur initialement URL demandée.

Configurez la solution de radio NAC OOB

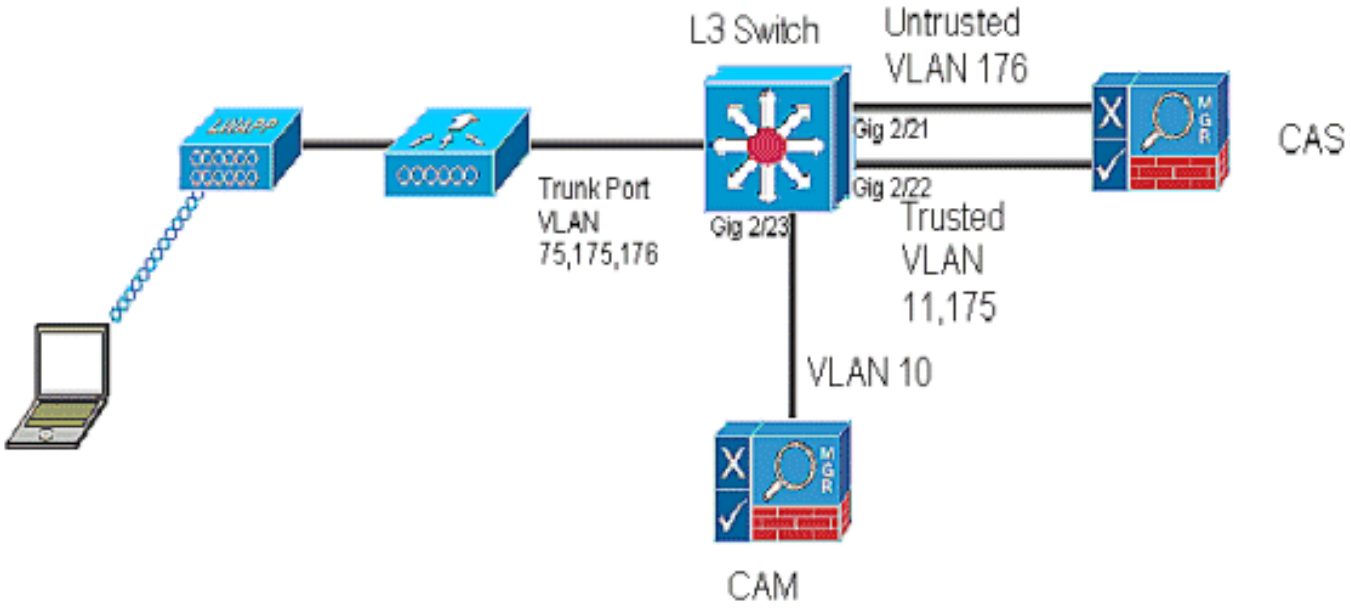
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Dans l'implémentation du courant NAC WLC intègre avec l'appliance de Cisco NAC en mode d'intrabande seulement, où l'appliance NAC doit rester dans le chemin de données même après que l'utilisateur est certifié. Une fois que l'appliance NAC se termine sa validation de posture, l'employé/invité reçoit l'accès du réseau basé sur leur rôle.

Avec la release NAC 4.5 et WLC 5.1, l'intégration des prises en charge des solutions OOB de la radio NAC avec l'appliance NAC. Quand le client associe et se termine L2Auth, il est vérifié si l'interface de quarantaine est associée au WLAN/SSID. Si oui, le trafic initial est envoyé sur l'interface de quarantaine. La circulation de client dans la quarantaine VLAN, qui est trunked à l'appliance NAC. Une fois que la validation de posture est faite, le gestionnaire NAC envoie un message de snmp set qui met à jour l'ID DE VLAN d'accès ; le contrôleur se met à jour avec l'ID DE VLAN d'accès, et la commutation de débuts du trafic de données du contrôleur directement au réseau sans serveur NAC.

Exemple de figure 2-1 de CAS autonome en mode de passerelle connecté à WLC par le commutateur



Dans la figure 2-1, le WLC est connecté à un port de joncteur réseau qui porte la quarantaine VLAN et l'accès VLAN (176 et 175). Sur le commutateur, le trafic de la quarantaine VLAN est trunked à l'appliance NAC, et le trafic de l'accès VLAN est trunked directement au commutateur Layer3. Trafiquez qui atteint la quarantaine VLAN sur l'appliance NAC est tracé pour accéder au VLAN basé sur la configuration statique de mappage. Quand les associés de client se terminent le L2 authentique, il vérifie si l'interface de quarantaine est associée ; si oui, les données sont envoyées sur l'interface de quarantaine. La circulation de client dans la quarantaine VLAN, qui est trunked à l'appliance NAC. Une fois que la validation de posture est faite, le serveur NAC (CAS) envoie un message de snmp set qui met à jour l'ID DE VLAN d'accès au contrôleur, et les débuts du trafic de données pour commuter du WLC directement au réseau sans serveur NAC.

Restrictions

- Aucun profil de port associé
- Aucun ID DE VLAN spécifié sur le gestionnaire NAC : défini sur WLC
- Le support de filtre d'adresses MAC ne peut pas utiliser l'ID DE VLAN des configurations de rôle
- Le mode de serveur virtuel hors bande de la passerelle NAC les prennent en charge seulement
- Association de la couche 2 entre le serveur WLC et NAC
- NAC ISR et WLC nanomètre ne peuvent pas être installés pour faire la radio OOB NAC

Remarque: Référez-vous au mappage VLAN dans la section virtuelle de modes de passerelle de l'appliance de Cisco NAC - le guide de configuration de Clean Access Server, libèrent 4.8(1) pour plus d'informations sur la façon configurer sans risque des VLAN en modes virtuels de passerelle.

Configuration des commutateurs Catalyst

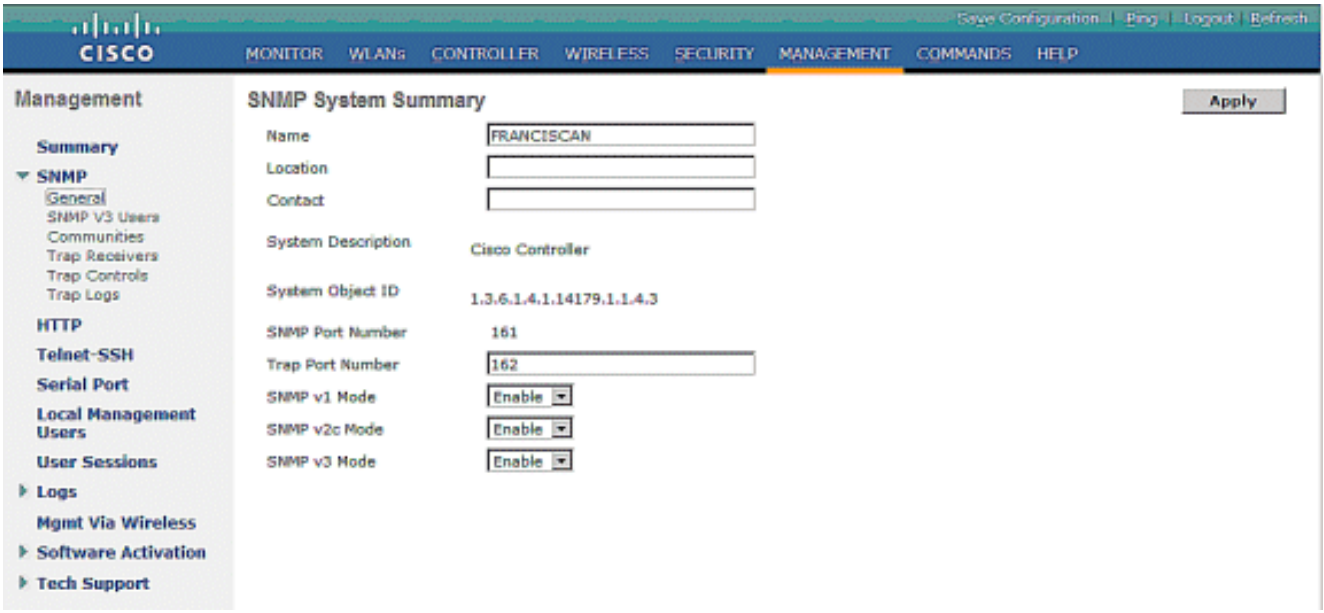
```
interface GigabitEthernet2/21
```

```
 description NAC SERVER UNTRUSTED INTERFACE
 switchport
 switchport trunk native vlan 998
 switchport trunk allowed vlan 176
 switchport mode trunk
 no ip address
!
interface GigabitEthernet2/22
 description NAC SERVER TRUSTED INTERFACE
 switchport
 switchport trunk native vlan 999
 switchport trunk allowed vlan 11,175
 switchport mode trunk
 no ip address
!
interface GigabitEthernet2/23
 description NAC MANAGER INTERFACE
 switchport
 switchport access vlan 10
 no ip address
 spanning-tree portfast
!
interface GigabitEthernet2/1
 description WLC
 switchport
 switchport trunk allowed vlan 75,175,176
 switchport trunk native vlan 75
 switchport mode trunk
 no ip address
!

interface Vlan75
Description WLC Management VLAN
 ip address 10.10.75.1 255.255.255.0
!
interface Vlan175
Description Client Subnet Access VLAN
 ip address 10.10.175.1 255.255.255.0
end
```

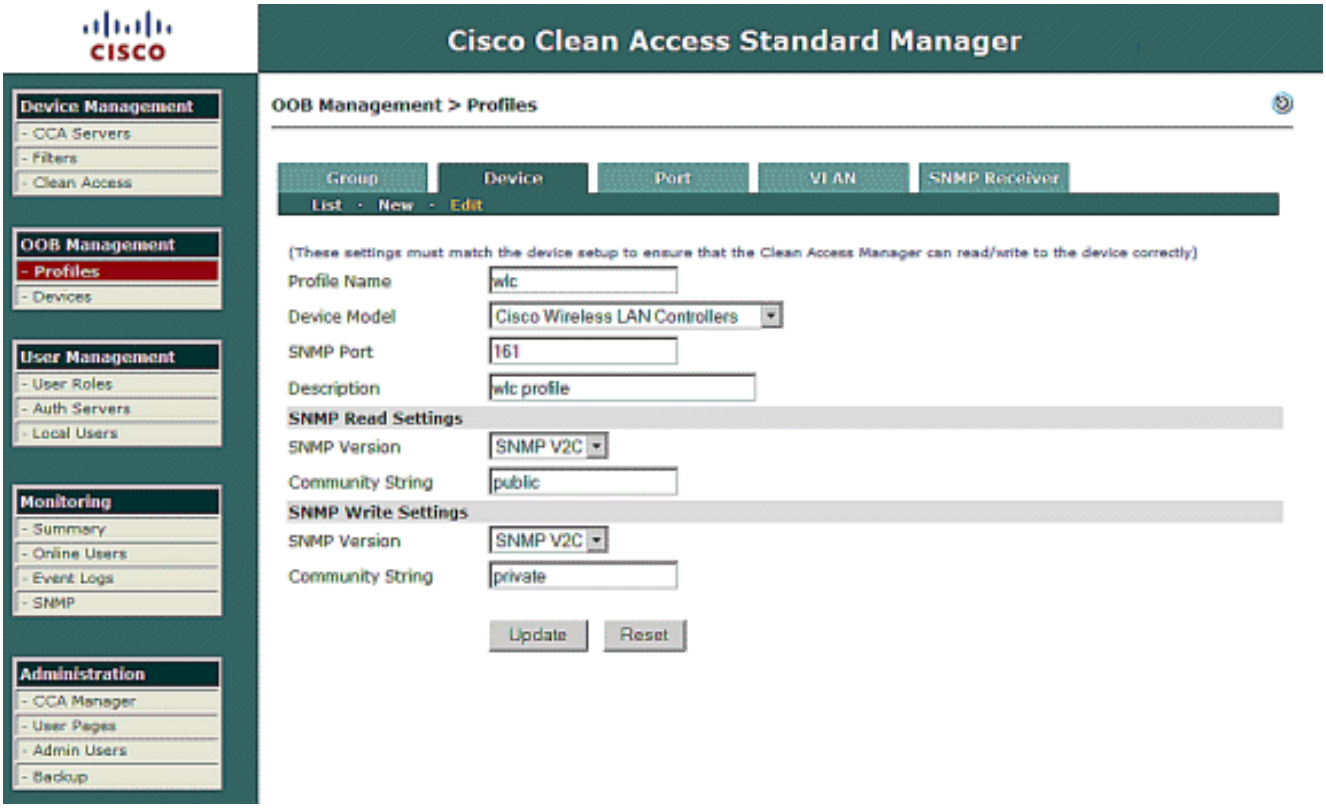
Étapes pour configurer NAC OOB sur le gestionnaire WLC et NAC

Suivez ces étapes pour configurer NAC OOB sur le gestionnaire WLC et NAC :

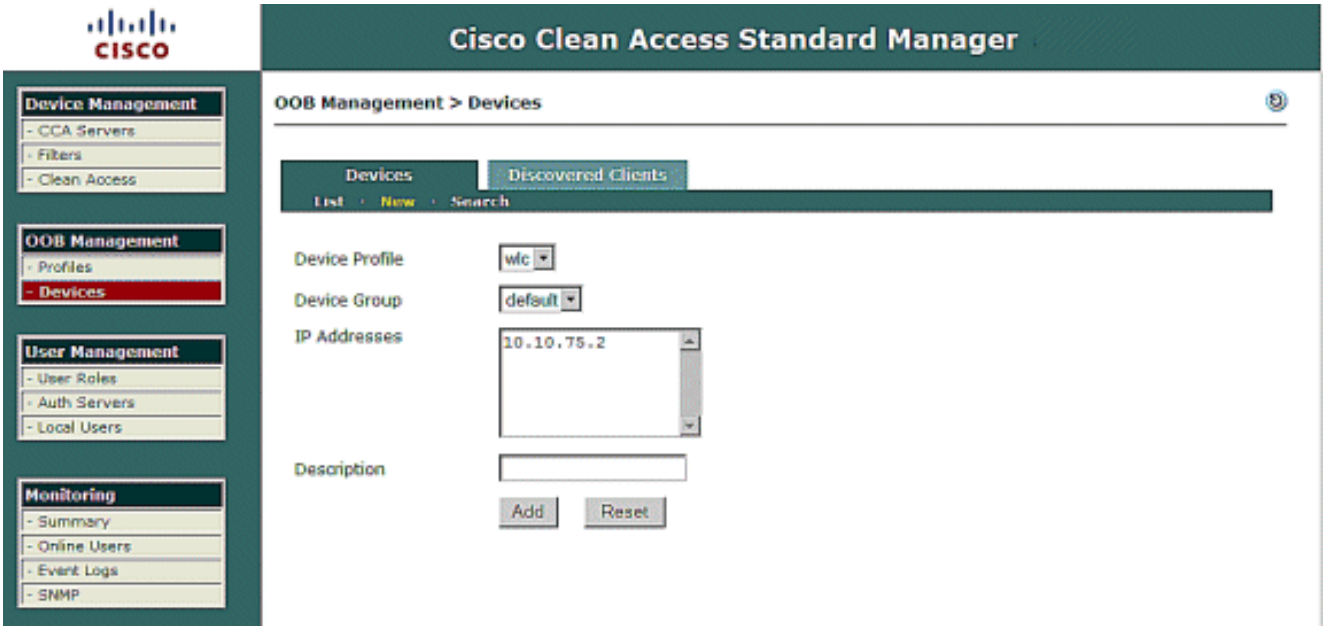
1. Mode SNMP v2 d'enable sur le contrôleur.



2. Créez un profil pour WLC sur le gestionnaire de CAM. **Profil > périphérique de Gestion du** clic **OOB > nouveau**.

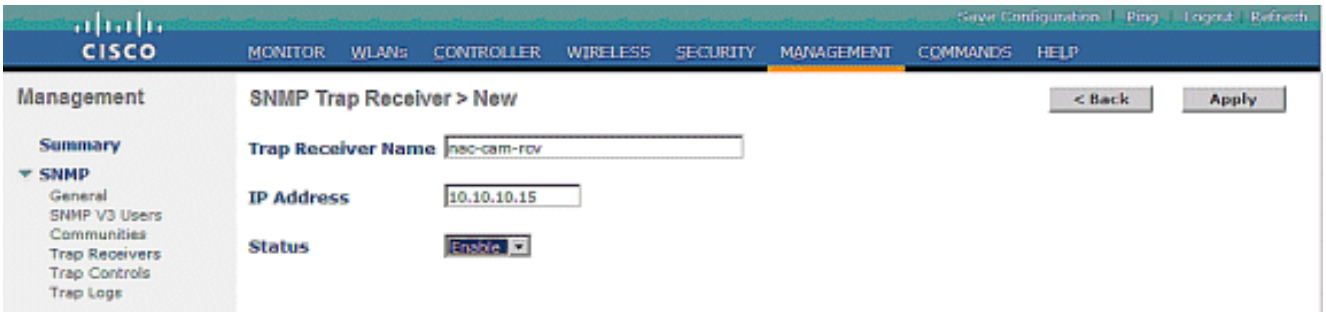


3. Une fois que le profil est créé sur le CAM, ajoutez WLC dans le profil ; allez à la **Gestion > aux périphériques OOB > nouveau** et écrivez l'adresse IP de Gestion de WLC.



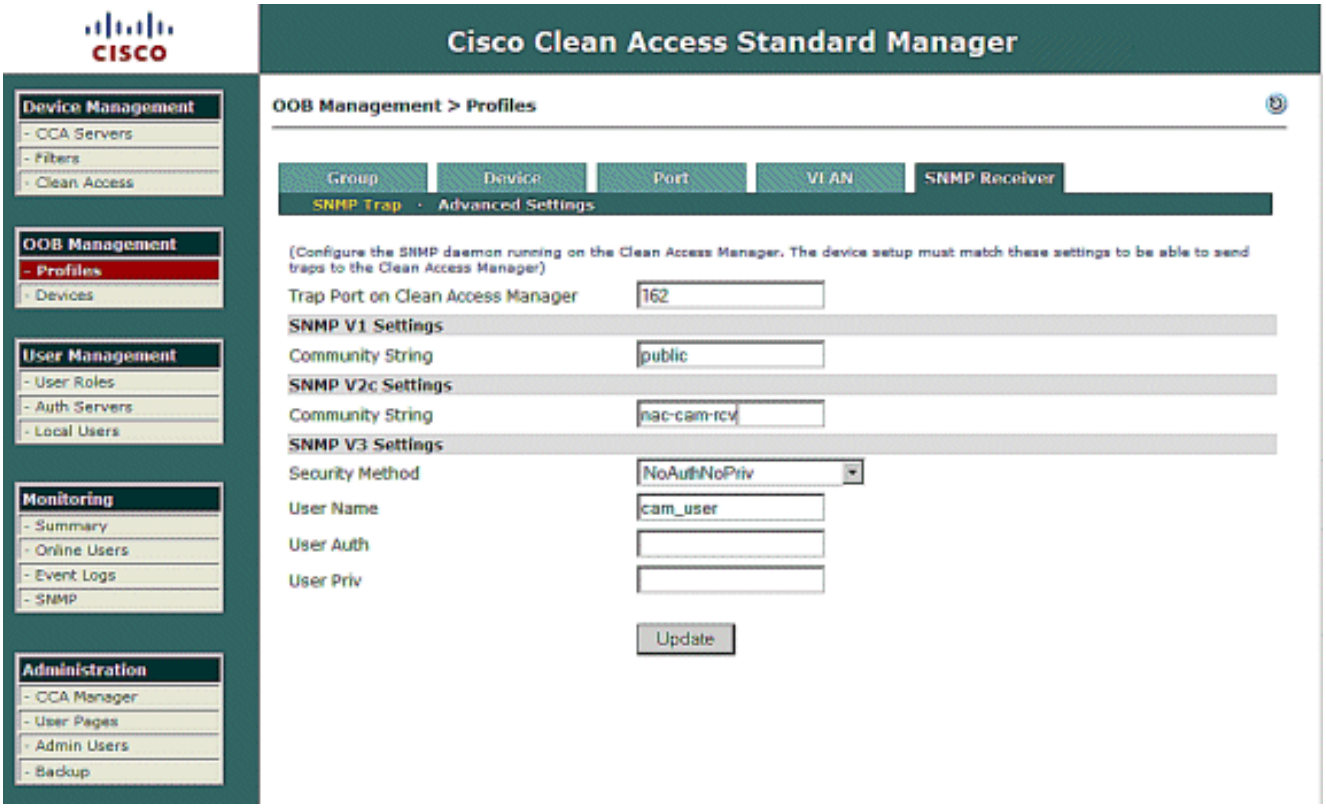
Maintenant le contrôleur est ajouté dans le gestionnaire de CAM.

4. Ajoutez le CAM en tant que récepteur de déroutement SNMP du WLC. Utilisez le nom précis du récepteur de déroutement dans le CAM comme récepteur SNMP.



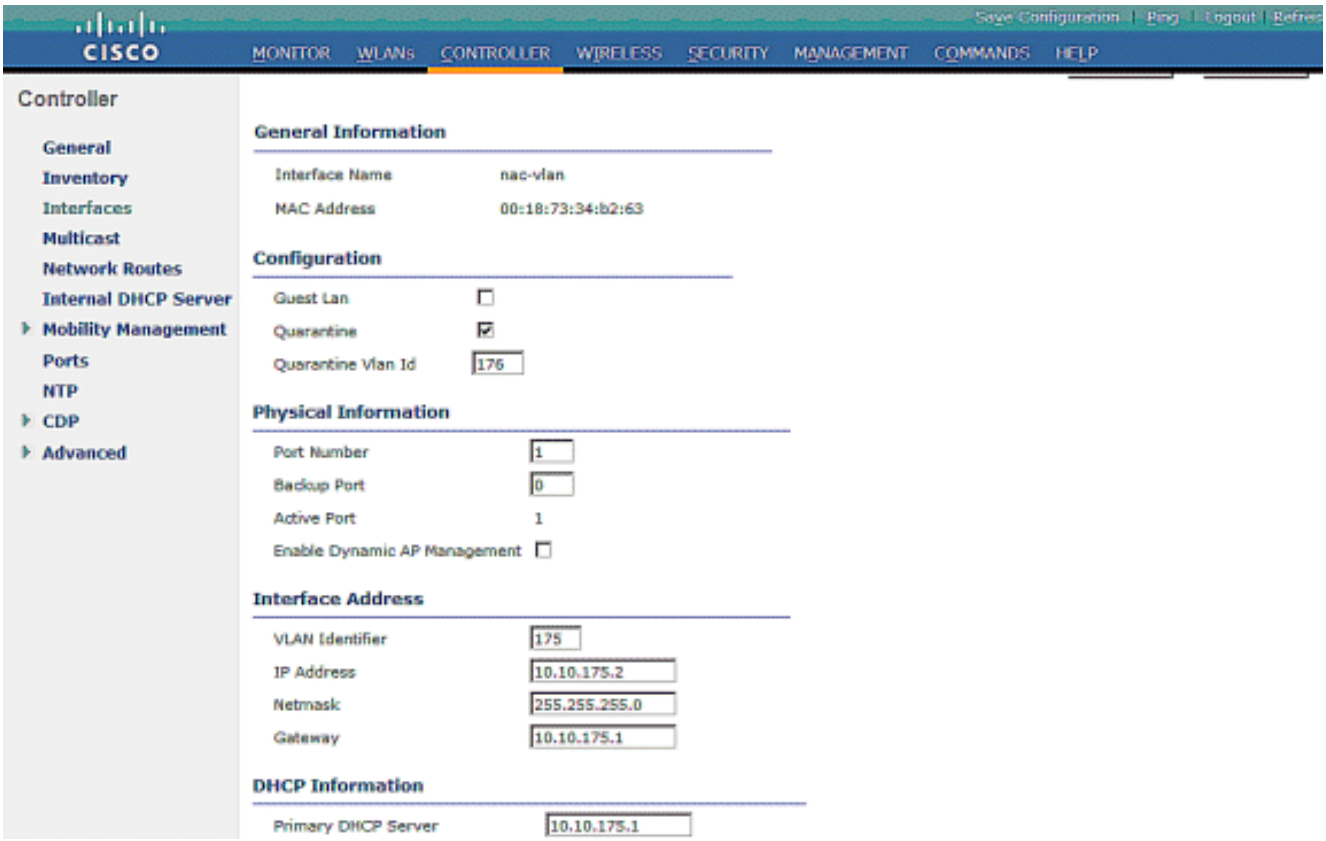
5. Configurez le récepteur de déroutement SNMP dans le CAM avec le même nom, qui est spécifié sur le contrôleur ; cliquez sur les profils sous la **Gestion OOB > le récepteur**

SNMP.

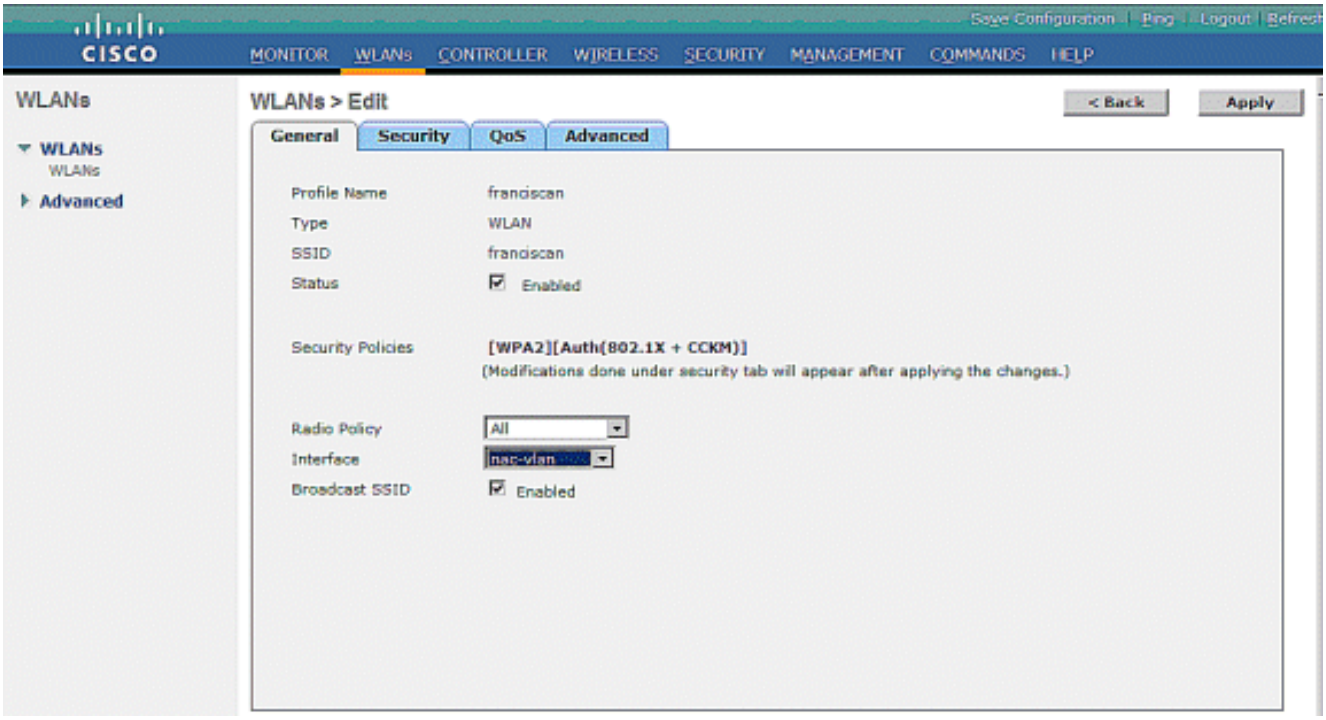


Àce stade, le WLC et le CAM peuvent parler entre eux pour des mises à jour d'état de validation et d'accès/quarantaine de posture de client.

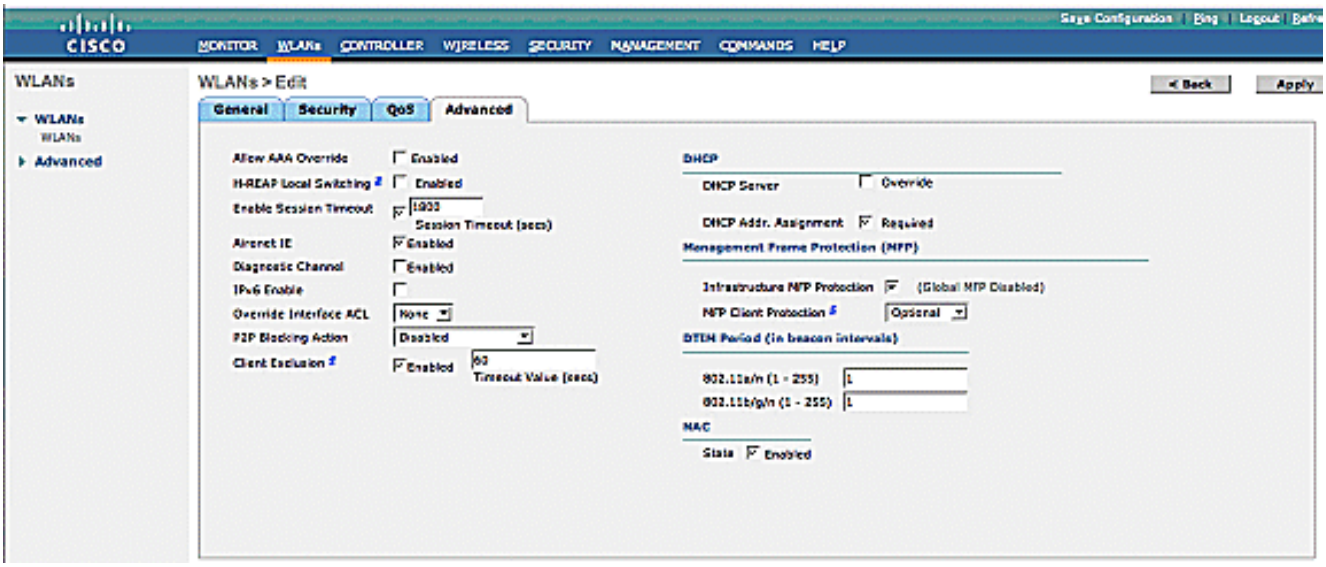
6. Dans le contrôleur, créez une interface dynamique avec l'accès et mettez en quarantaine le VLAN.



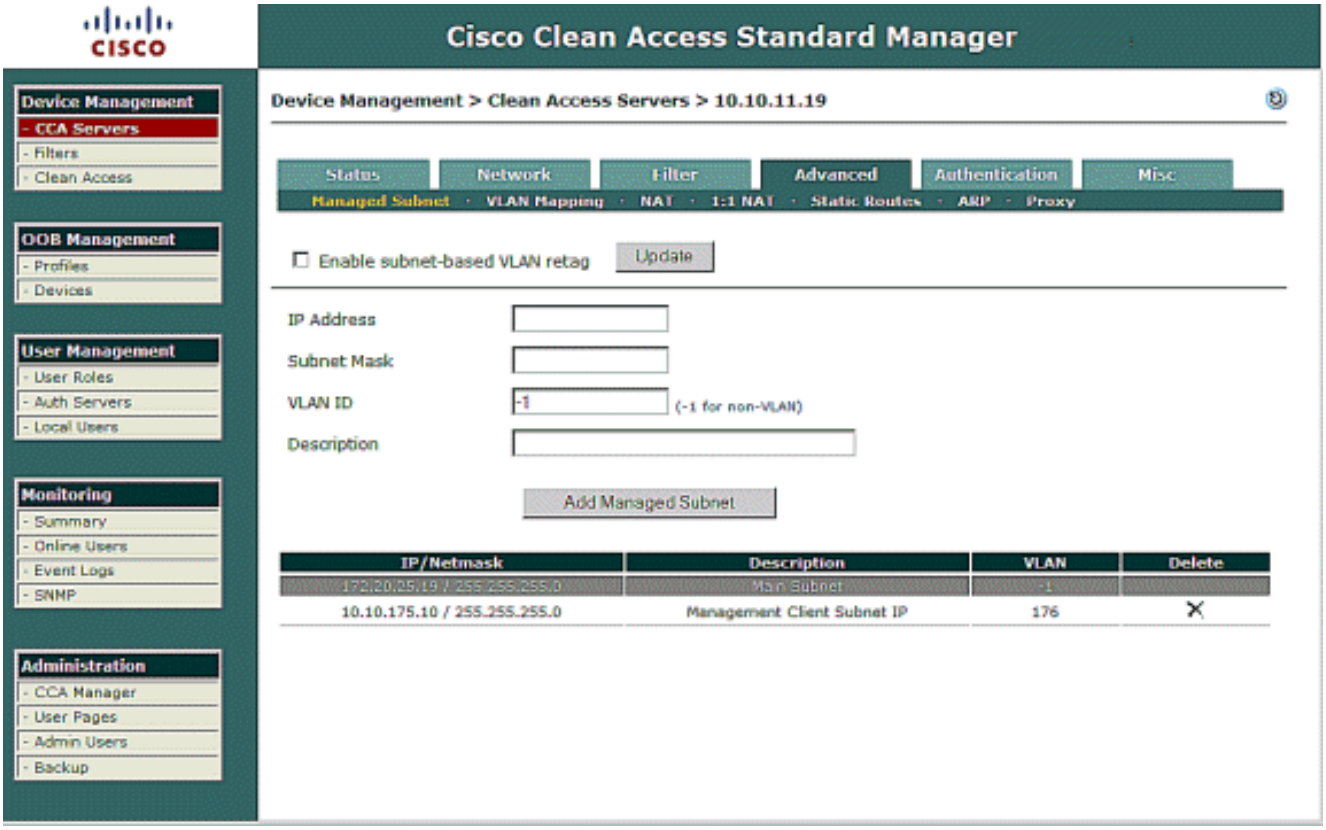
7. Créez le WLAN, et associez-le avec l'interface dynamique.



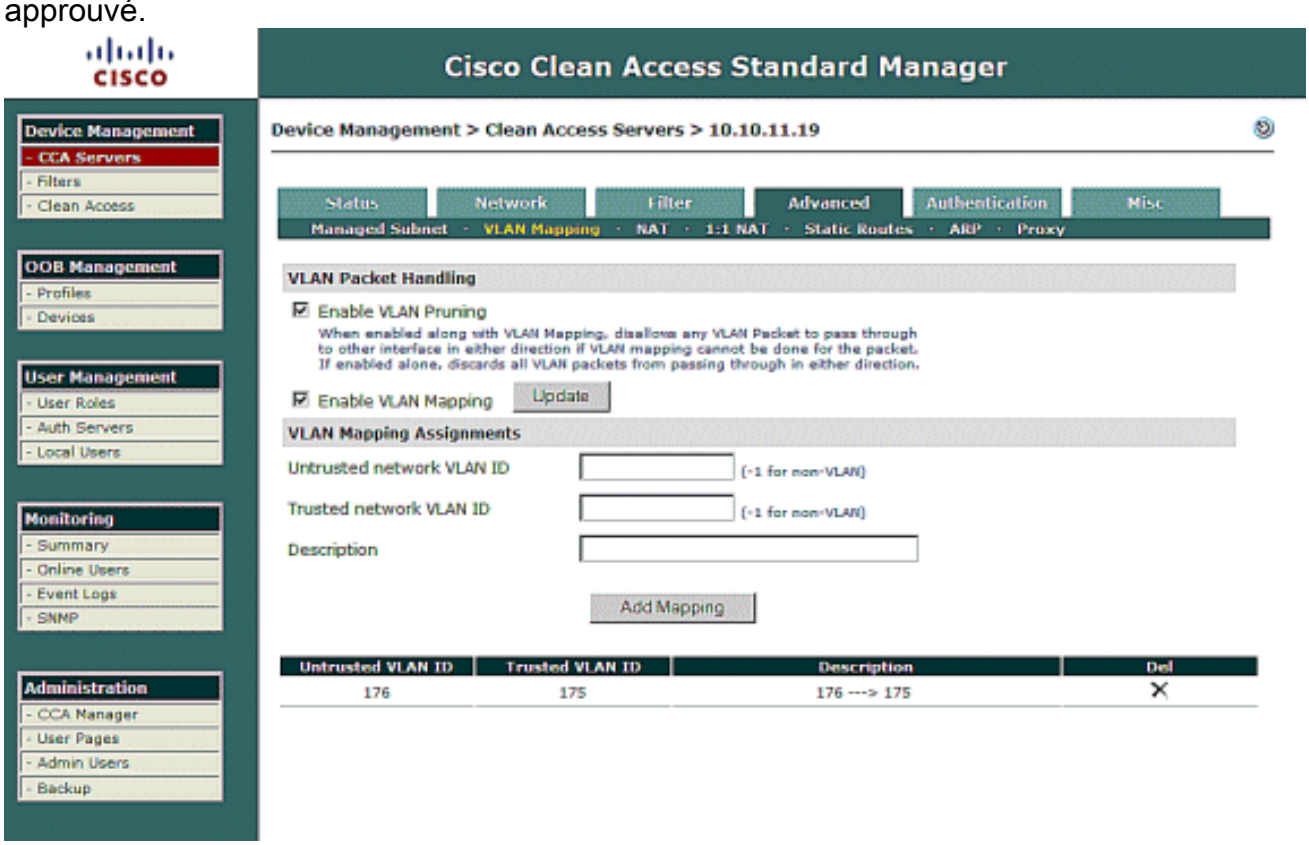
8. En conclusion, enable NAC dans le WLAN.



9. Ajoutez le sous-réseau de client dans le serveur de CAS comme sous-réseau géré ; cliquez sur le **serveur de CAS > sélectionnent votre serveur de CAS > adresse IP inutilisée >Advanced > gérée Manage de sous-réseaux de >Add du sous-réseau de client** et mettent la quarantaine VLAN (VLAN non approuvé) pour le sous-réseau géré.



10. Créez les mappages VLAN sur CAS. Choisissez le **serveur de CAS > sélectionnent votre serveur de CAS > gèrent > ont avancé > mappage VLAN**. Ajoutez l'accès VLAN comme fait confiance et mettez en quarantaine le VLAN comme non approuvé.



Configurer l'ouverture de session simple (SSO) avec la solution de radio OOB

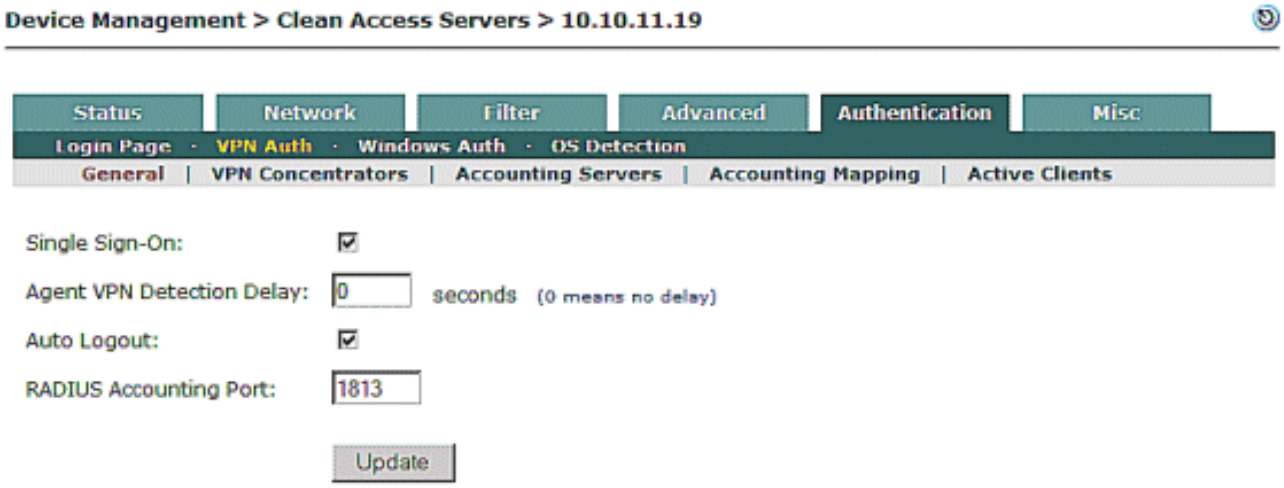
Ce sont les conditions requises d'activer la radio SSO :

1. Authentification de l'enable VPN sur le serveur NAC — WLC est défini en tant que « concentrateur VPN » dans l'appliance NAC.
2. Activez RADIUS rendant compte sur le WLC — le contrôleur qui est défini dans l'appliance NAC doit être configuré pour envoyer des enregistrements des comptes de RADIUS à l'appliance NAC pour chaque 802.1x/EAP WLAN qui est un sous-réseau géré dans le NAC.

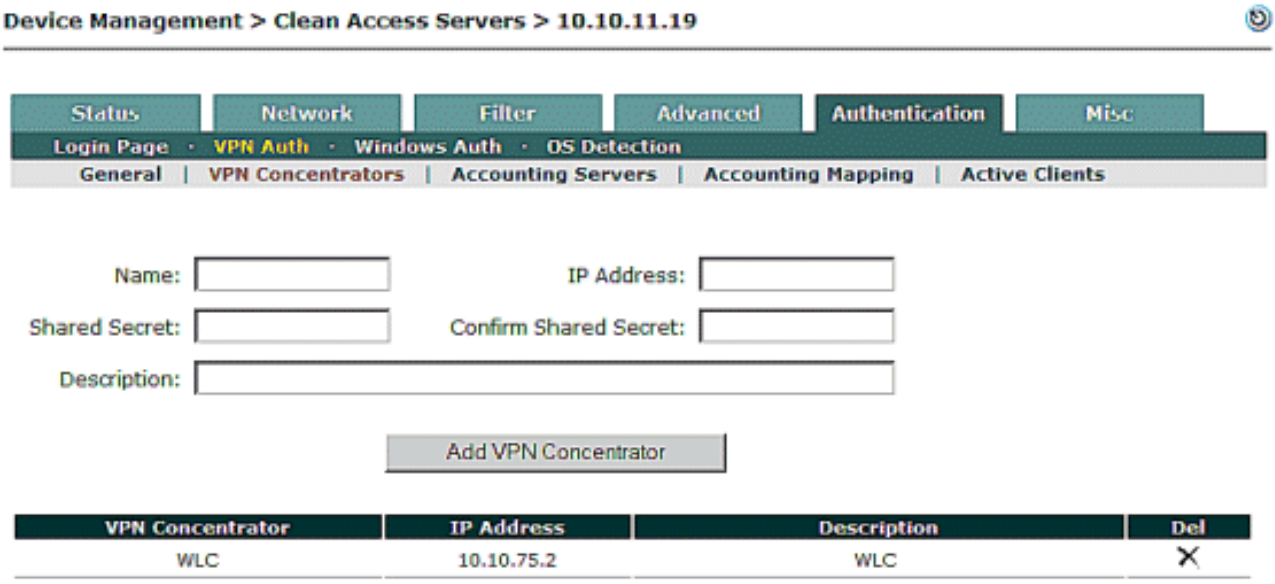
Étapes pour configurer SSO sur le gestionnaire NAC

Suivez ces étapes pour configurer SSO sur le gestionnaire NAC :

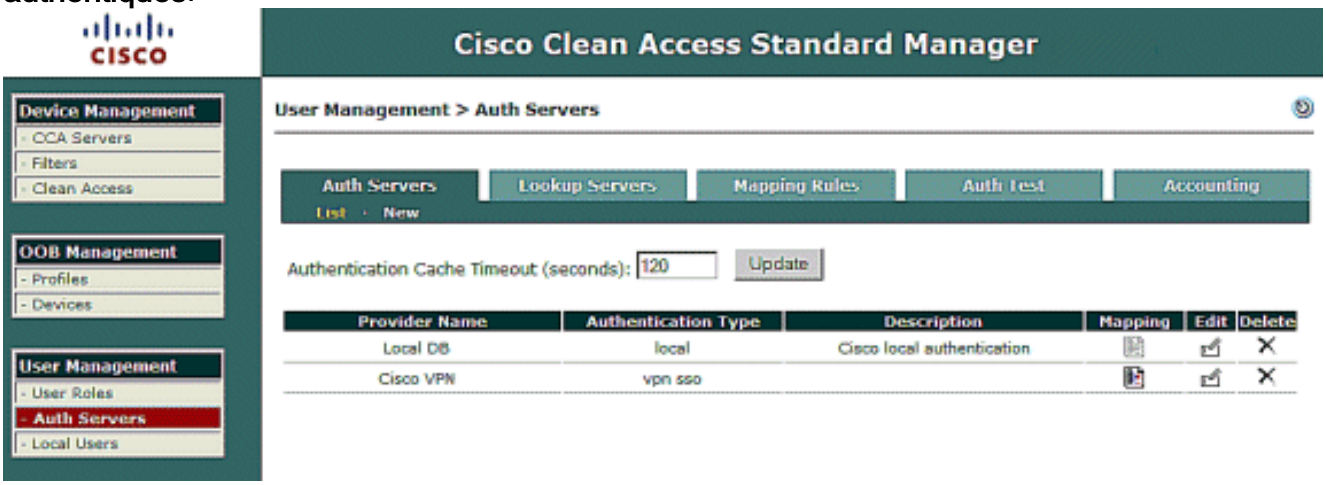
1. Du menu gauche de CAM, sous la Gestion de périphériques, choisissez le **serveur de CCA**, et puis cliquez sur le lien de **serveur NAC**.
2. De la page d'état de serveur, choisissez l'onglet d'**authentification** et puis le sous-menu **authentique VPN**. Voir la figure 3-1.**Figure 3-1 activant le célibataire Signe-sur le serveur NAC**



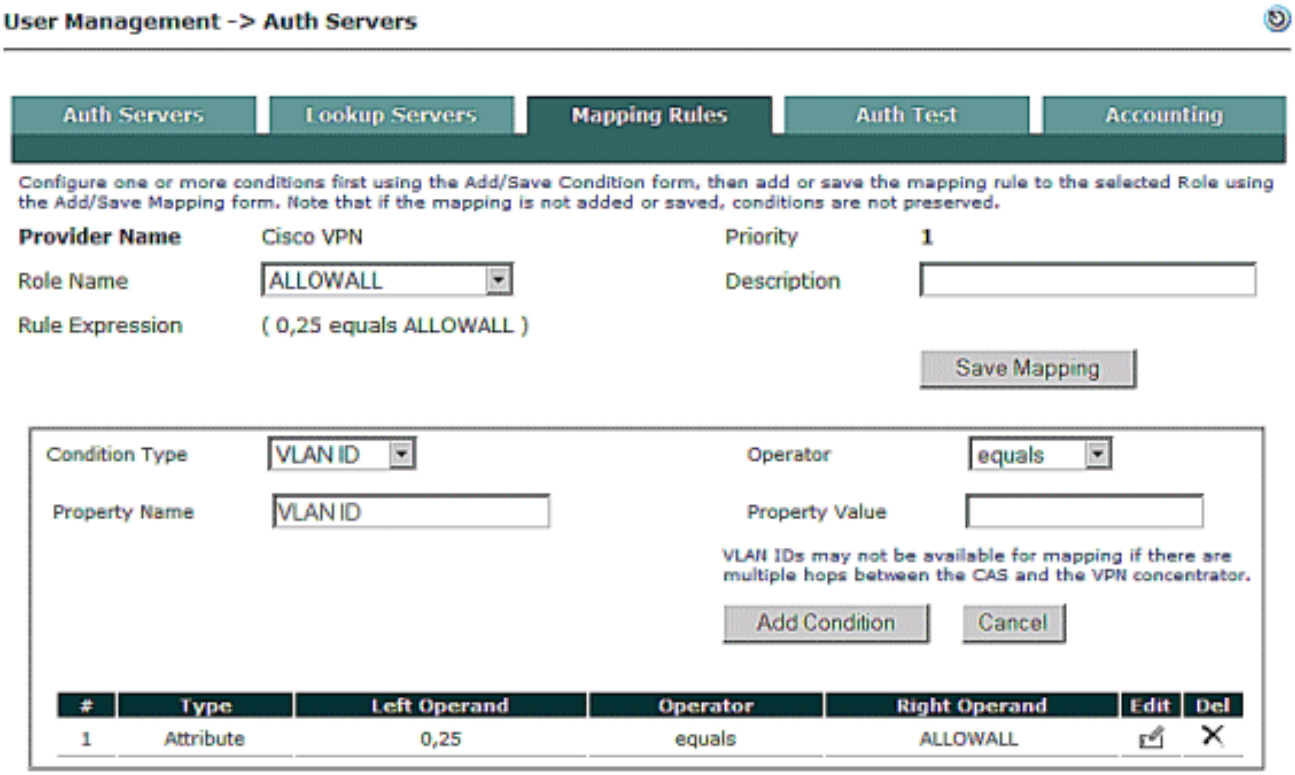
3. Choisissez les **concentrateurs VPN plaçant** (figure 3-2) pour ajouter une nouvelle entrée de WLC. Remplissez champs d'entrée pour l'adresse IP de Gestion WLC et le secret partagé que vous voulez utiliser entre le serveur WLC et NAC.**La figure 3-2 ajoutent WLC comme un client RADIUS sous la section de concentrateur VPN**



4. Pour le mappage de rôle, ajoutez le nouveau serveur d'authentification avec le **sso de vpn de** type sous la **gestion des utilisateurs > les serveurs authentiques**.

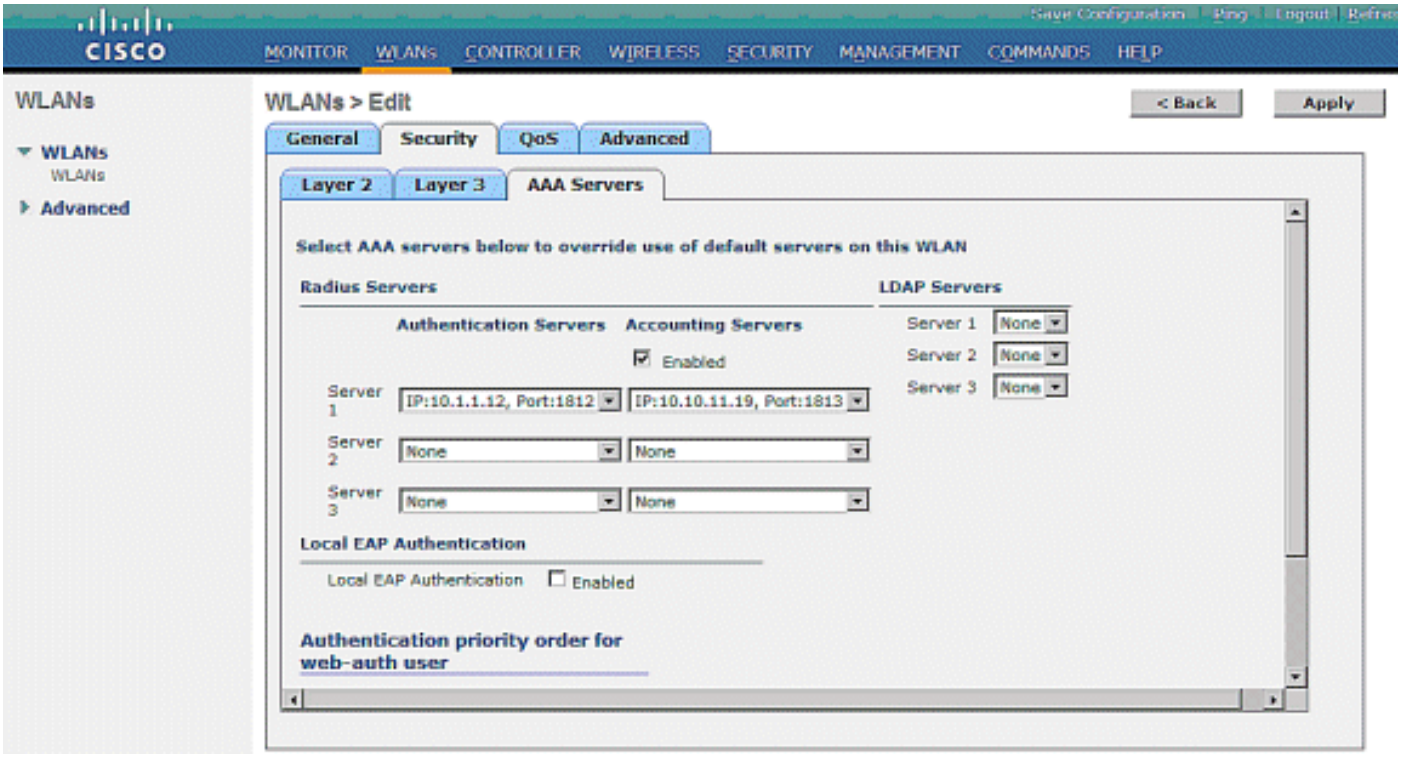


5. Cliquez sur l'icône de **mappage** et puis ajoutez la **règle de mappage**. Le mappage varie la personne à charge sur la valeur de l'attribut 25 de classe que WLC introduit le paquet de comptabilité. Cette valeur d'attribut est configurée dans le serveur de RADIUS et varie basé sur l'autorisation d'utilisateur. Dans cet exemple, la valeur d'attribut est **ALLOWALL**, et elle est placée dans le rôle **AllowAll**.



Étapes pour configurer SSO sur le contrôleur LAN Sans fil

La comptabilité de RADIUS doit être configurée sur le WLC pour réaliser la capacité simple d'ouverture de session avec le serveur NAC.



Vérifier

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

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines

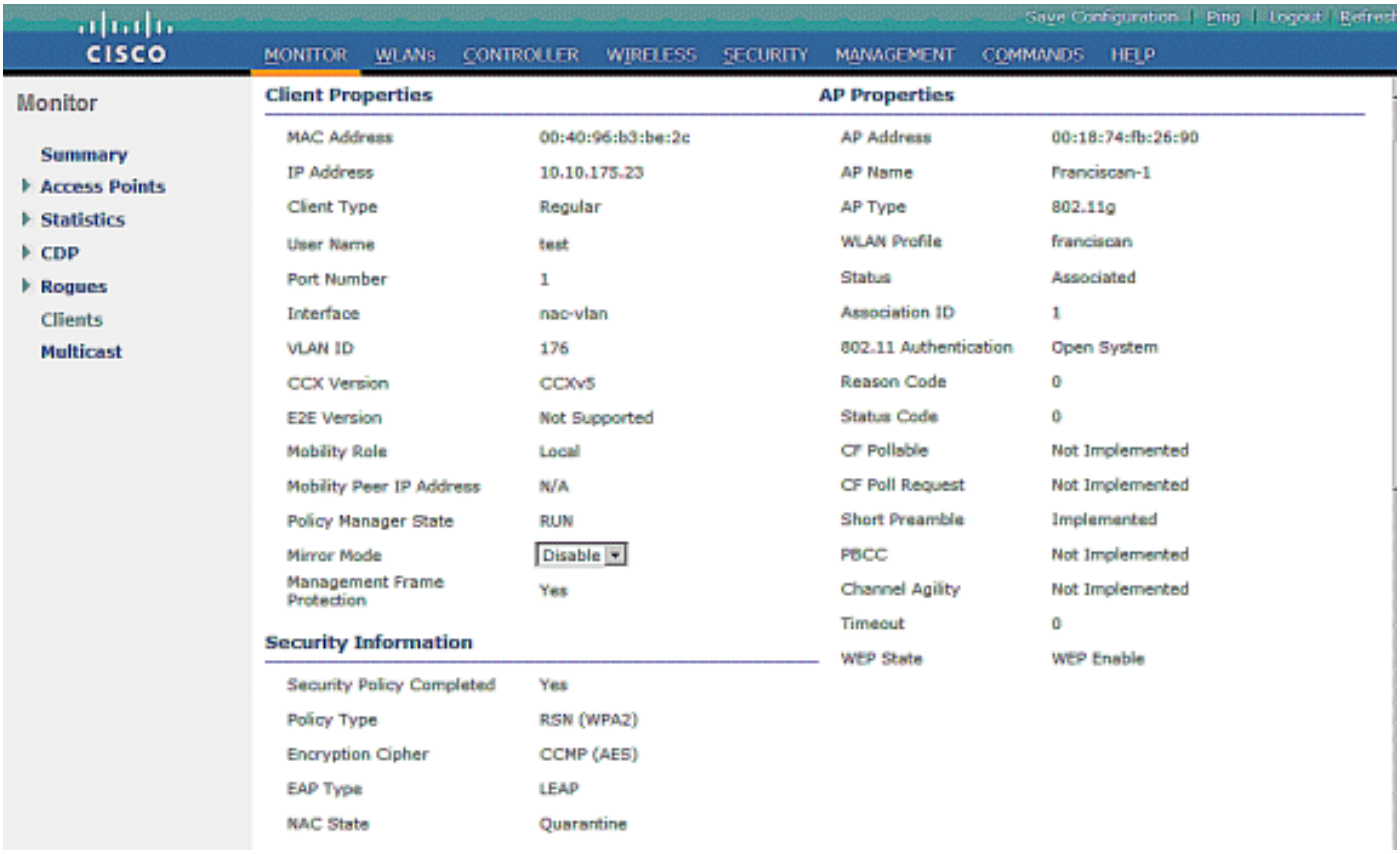
commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Commandes de CISCO WLC CLI pour la vérification

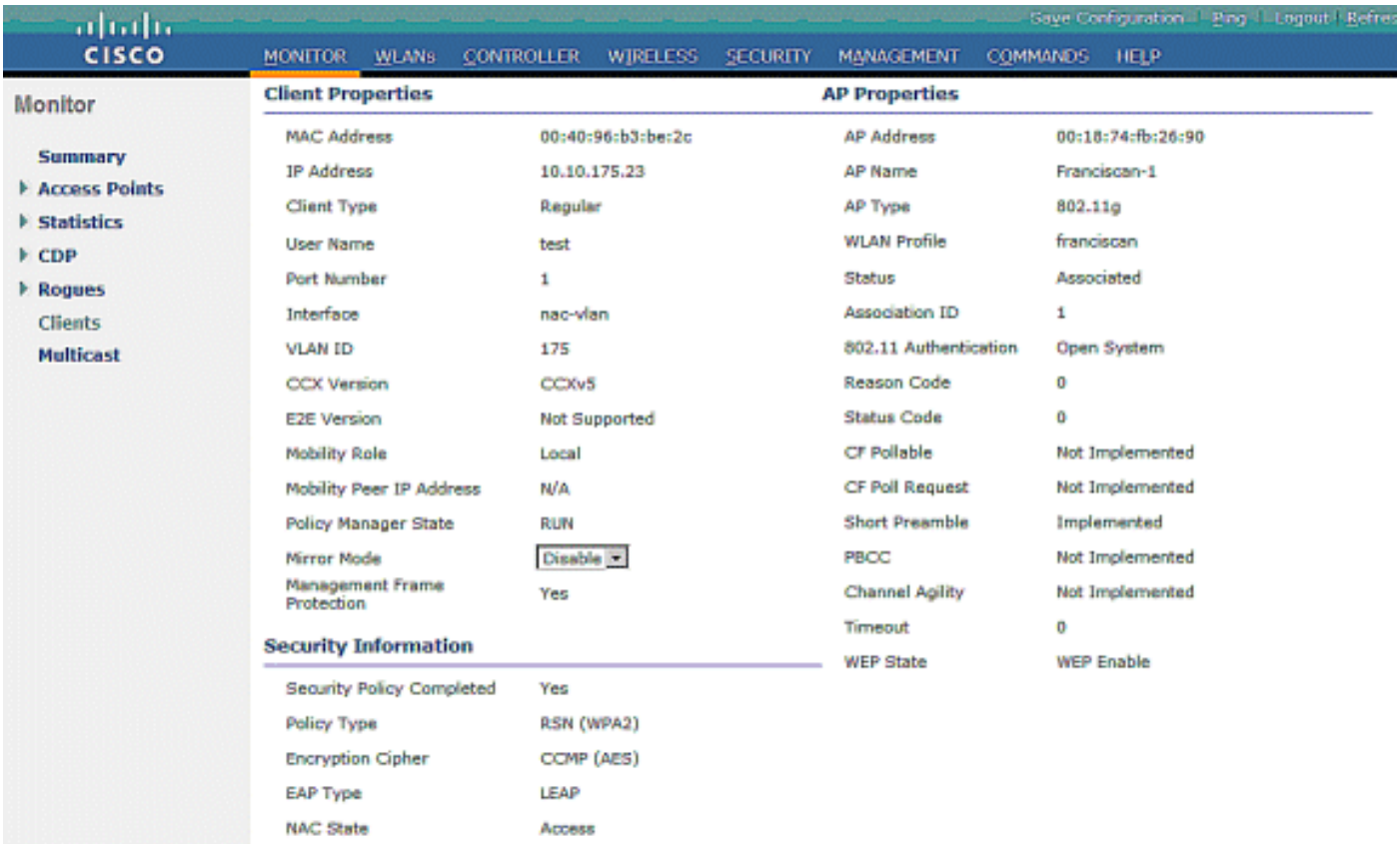
```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
----------------------------------------------- ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
virtual           N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name................................. management
MAC Address.................................... 00:18:73:34:b2:60
IP Address..................................... 10.10.75.2
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.10.75.1
VLAN........................................... untagged
Quarantine-vlan................................ 0
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.10.75.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
AP Manager..................................... No
Guest Interface................................ No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name................................. nac-vlan
MAC Address.................................... 00:18:73:34:b2:63
IP Address..................................... 10.10.175.2
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.10.175.1
VLAN........................................... 175
Quarantine-vlan................................ 176
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.10.175.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
AP Manager..................................... No
Guest Interface................................ No
```

Vérification d'état de client de GUI WLC

Au commencement le courant est dans un état de quarantaine jusqu'à ce que l'analyse de posture soit faite dans l'appliance NAC.



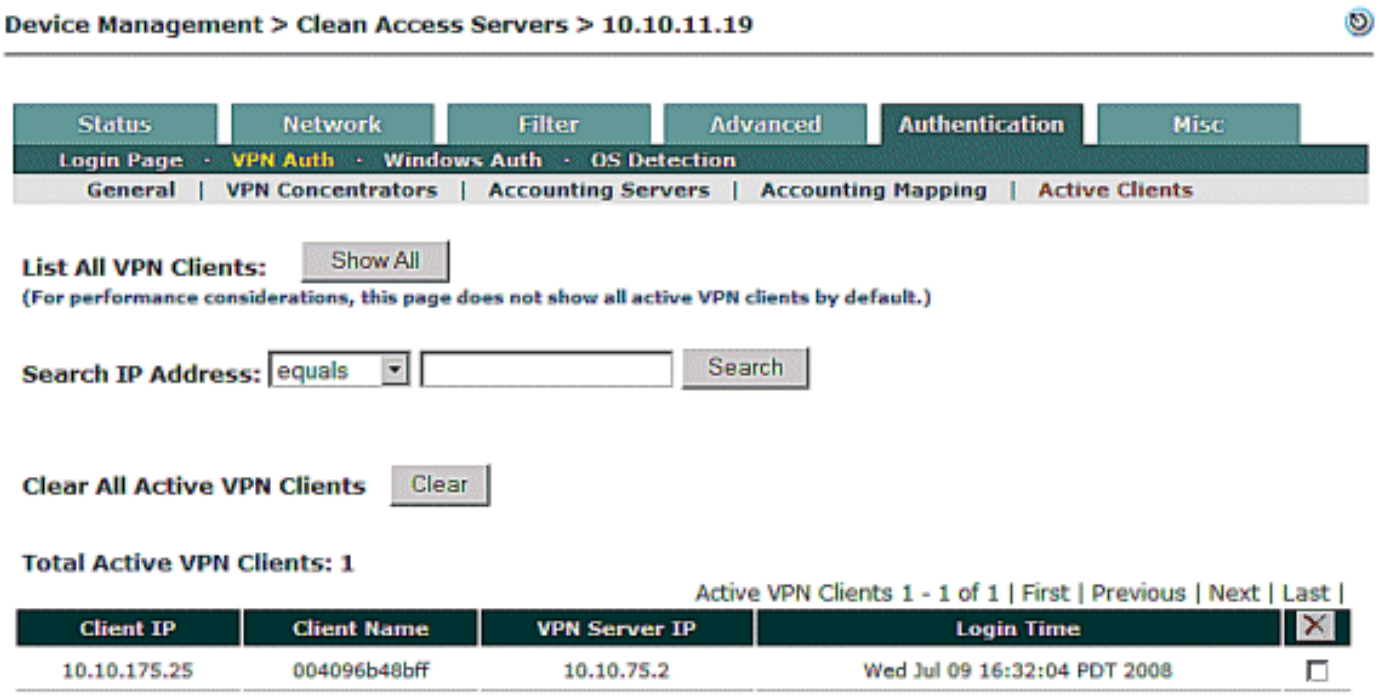
L'état NAC du client doit être **Access** après que l'analyse de posture soit terminée.



Vérification de l'ouverture de session simple sur le serveur NAC avec WLC

Sous le VPN authentique, allez au paragraphe **actif de client** vérifier si le paquet de début de traçabilité est arrivé du WLC. Cette entrée apparaît avec l'agent de CCA installé sur la machine cliente.

Vous devez ouvrir un navigateur pour compléter le processus simple d'ouverture de session sans agent. Quand l'utilisateur ouvre le navigateur, le processus SSO a lieu, et l'utilisateur révèle dans la liste d'utilisateur en ligne (OUL). Avec le paquet d'arrêt de traçabilité de RADIUS, l'utilisateur est retiré de la liste active de client.



Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Informations connexes

- Service RADIUS (Remote Authentication Dial-In User Service)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems