Dépannage de CWA avec WLC 9800 et ISE

Table des matières

- Introduction
- Informations générales
  - Flux détaillé
- Dépannage
  - Symptôme courant d'un utilisateur non redirigé vers la page de connexion
    - La première authentification RADIUS a-t-elle réussi ?
    - Le WLC reçoit-il l'URL de redirection et l'ACL ?
    - La liste de contrôle d'accès Redirect est correcte ?
    - Le client est-il déplacé vers Web-Auth en attente ?
    - Le WLC autorise-t-il le trafic DHCP et DNS ?
    - Le serveur DHCP reçoit-il une détection/requête DHCP ?
    - La redirection automatique se produit-elle ?
    - Le navigateur n'affiche-t-il pas la page de connexion ?
    - Le client peut-il résoudre le nom d'hôte ISE ?
    - Pourquoi y a-t-il une violation de sécurité due au certificat ?
    - La connexion invité échoue-t-elle ?
    - Le certificat d'authenticité est défectueux ?
- Résumé
- Informations sur les ressources

Introduction

Ce document décrit comment dépanner l'authentification Web centrale (CWA) avec le contrôleur LAN sans fil (WLC) 9800 et Identity Services Engine (ISE).

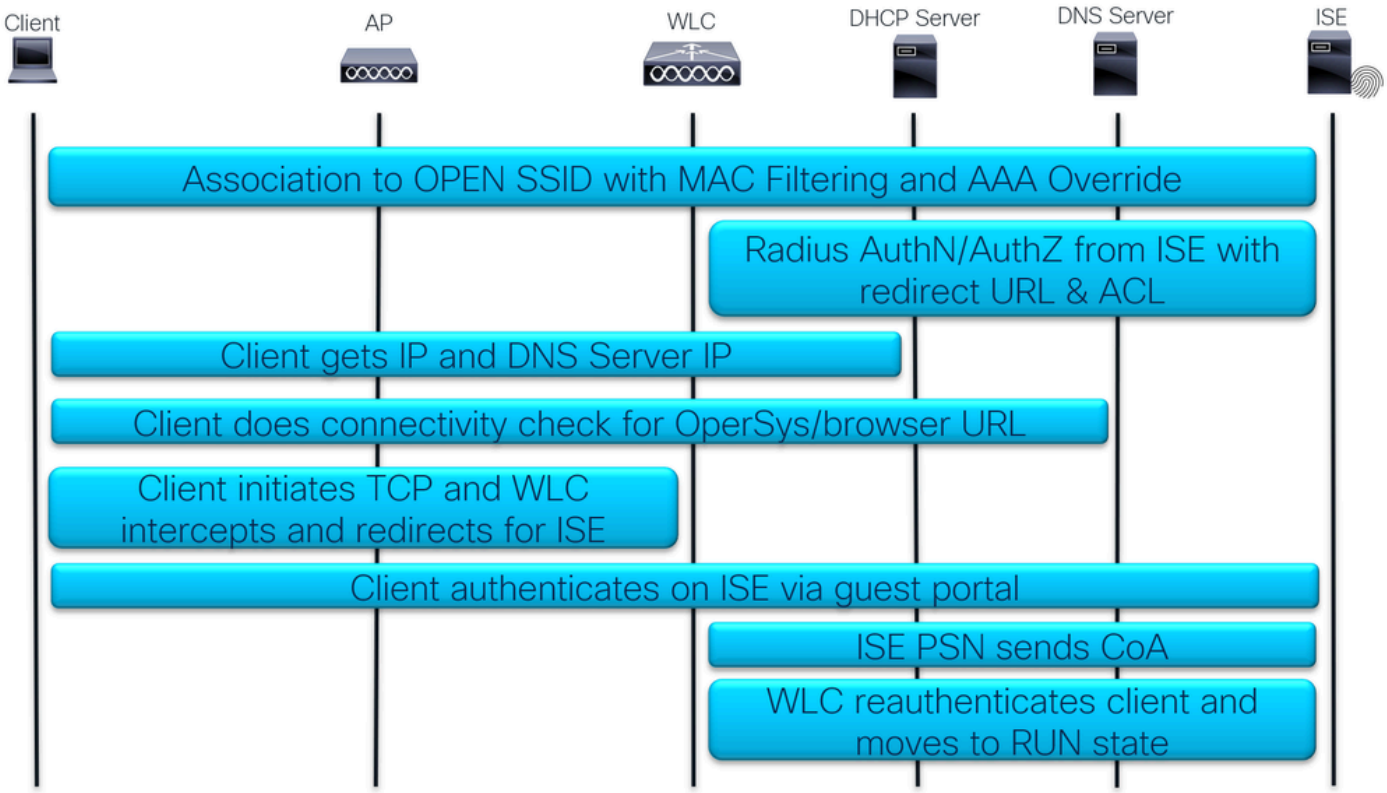
Informations générales

Les administrateurs réseau cherchant à sécuriser l'accès sans fil pour leurs périphériques personnels optent souvent pour des réseaux sans fil qui utilisent CWA. Ce document se concentre sur l'organigramme de CWA, qui aide au dépannage des problèmes courants. Il couvre les problèmes courants dans le processus, comment collecter les journaux liés à CWA, comment analyser ces journaux et comment collecter une capture de paquets intégrée (EPC) sur le WLC pour confirmer le flux de trafic.

CWA est la configuration la plus courante pour les entreprises qui permettent aux utilisateurs de

se connecter au réseau de l'entreprise à l'aide de leurs appareils personnels, également connu sous le nom de Bring Your Own Device (BYOD). Ces informations fournissent les étapes de dépannage à effectuer avant d'ouvrir un dossier TAC.

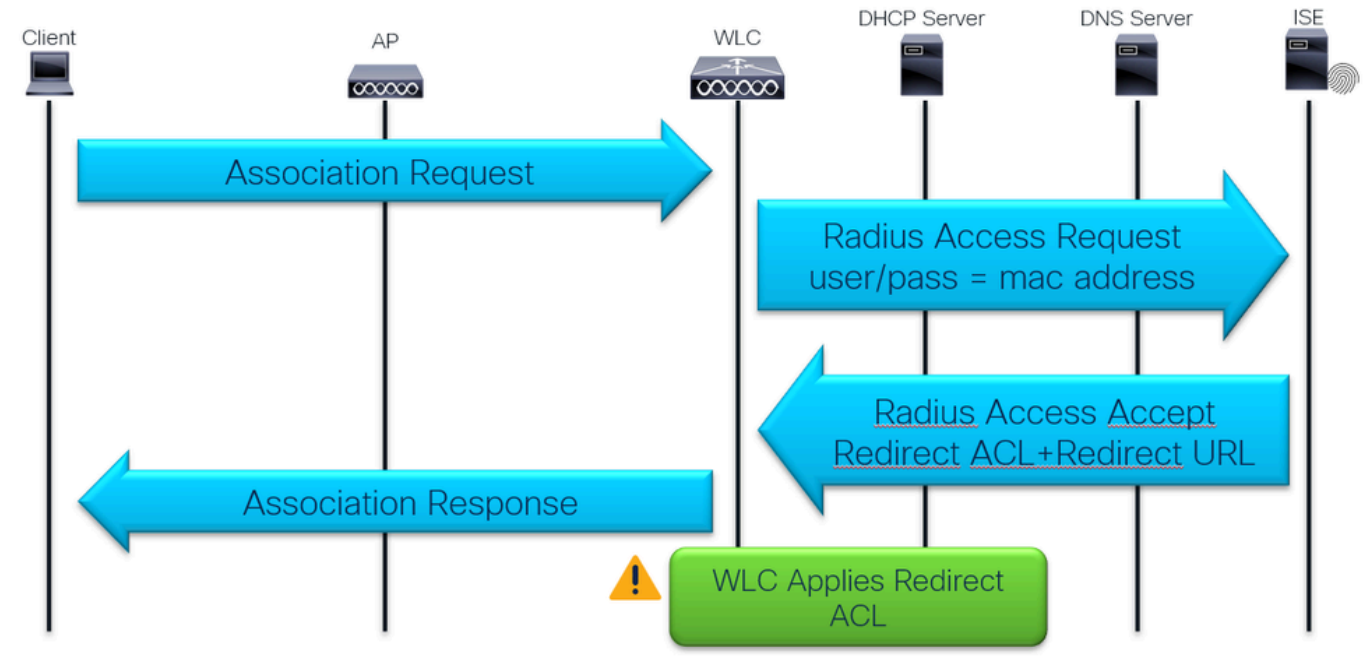
Voici le flux de paquets CWA :



Flux de paquets CWA

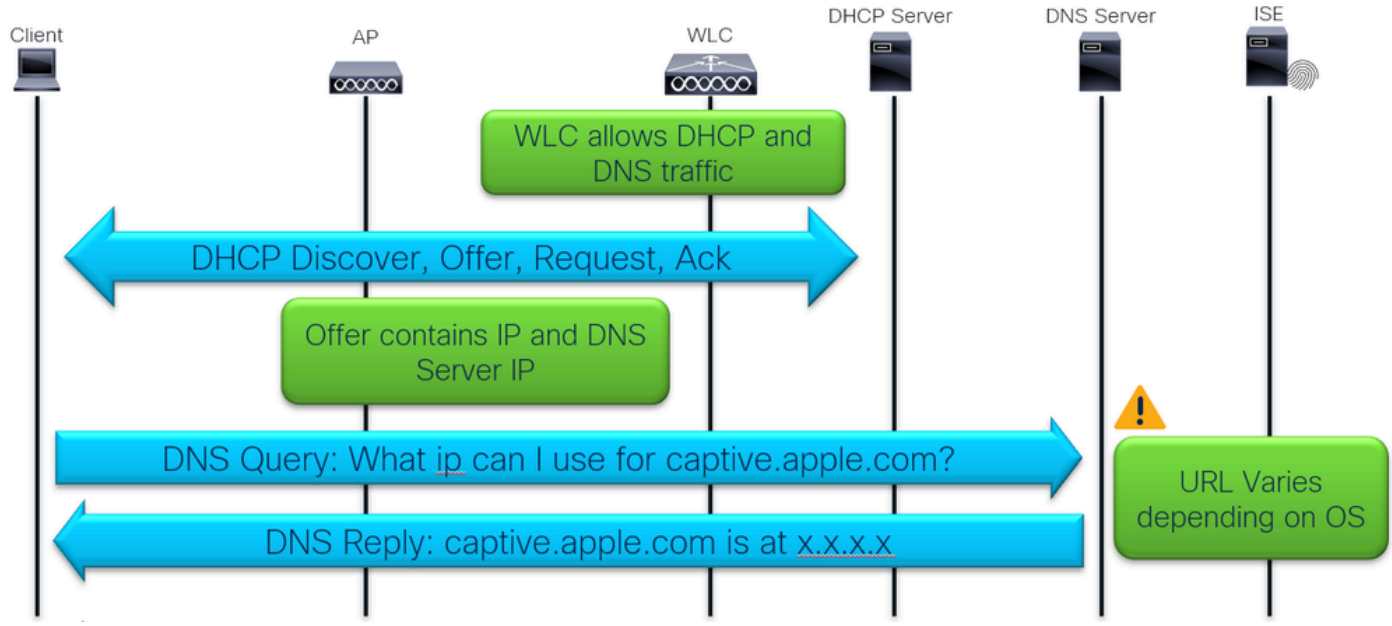
Flux détaillé

Première association et authentification RADIUS :



Première association et authentification RADIUS

DHCP, DNS et vérification de la connectivité :



DHCP, DNS et vérification de la connectivité

La vérification de connectivité est effectuée à l'aide de la détection de portail captif par le système d'exploitation ou le navigateur du périphérique client.

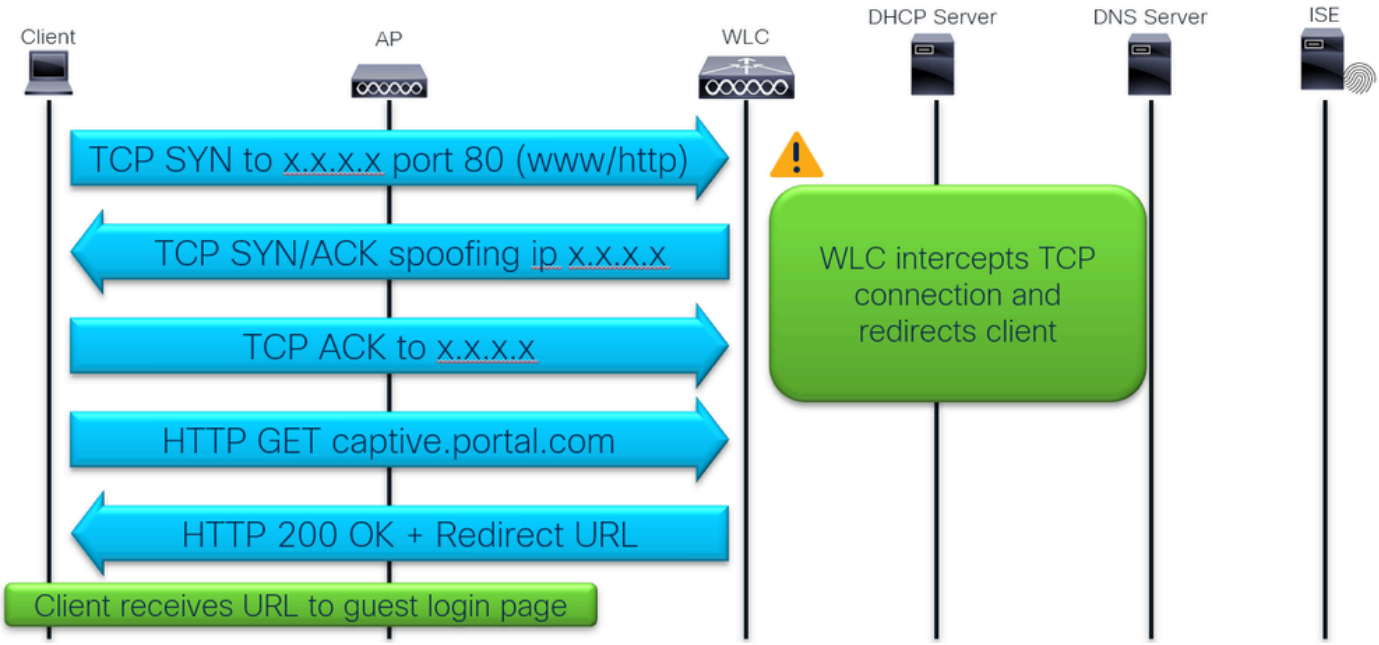
Les systèmes d'exploitation des périphériques sont pré-programmés pour exécuter une requête HTTP GET vers des domaines spécifiques :

- Apple = captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnectest.com

Les navigateurs effectuent également cette vérification à l'ouverture :

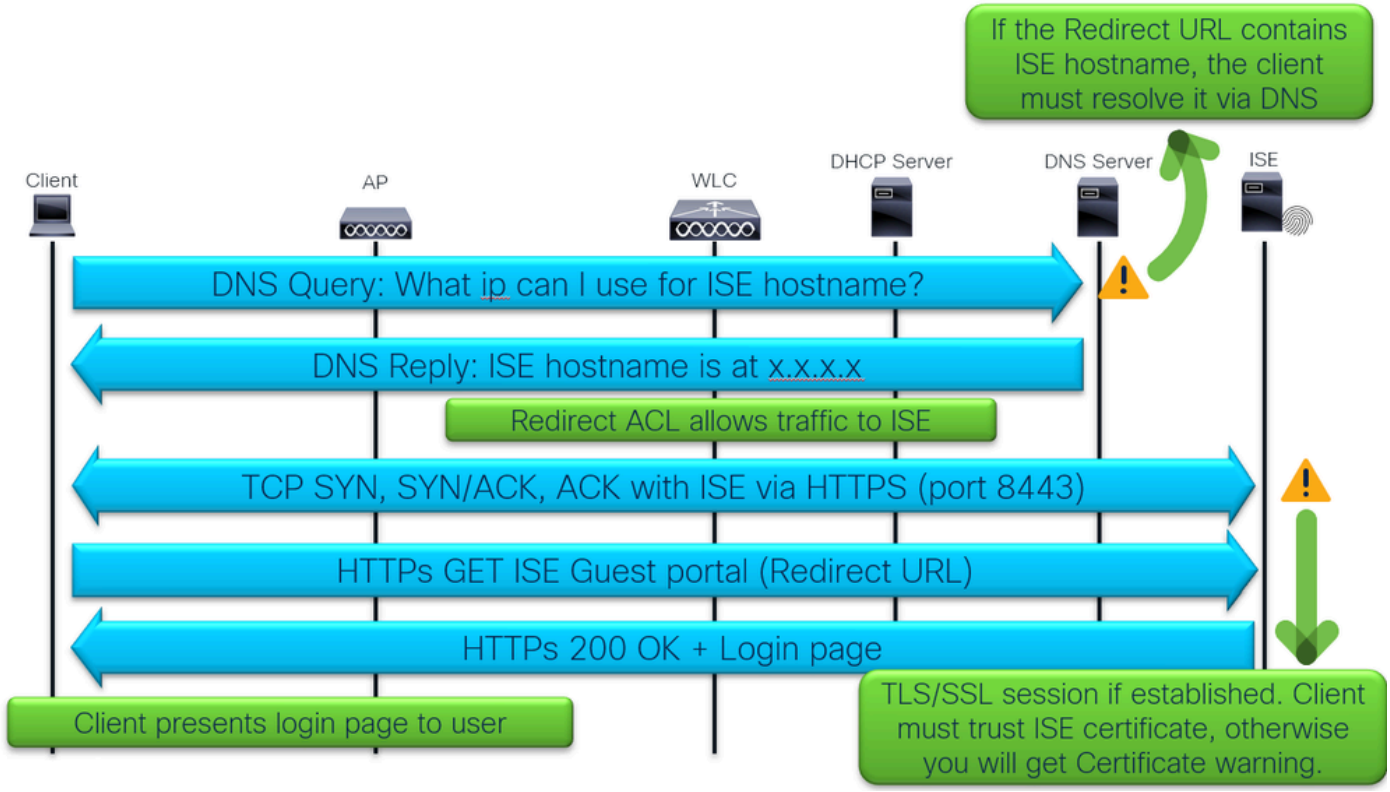
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Interception et redirection du trafic :



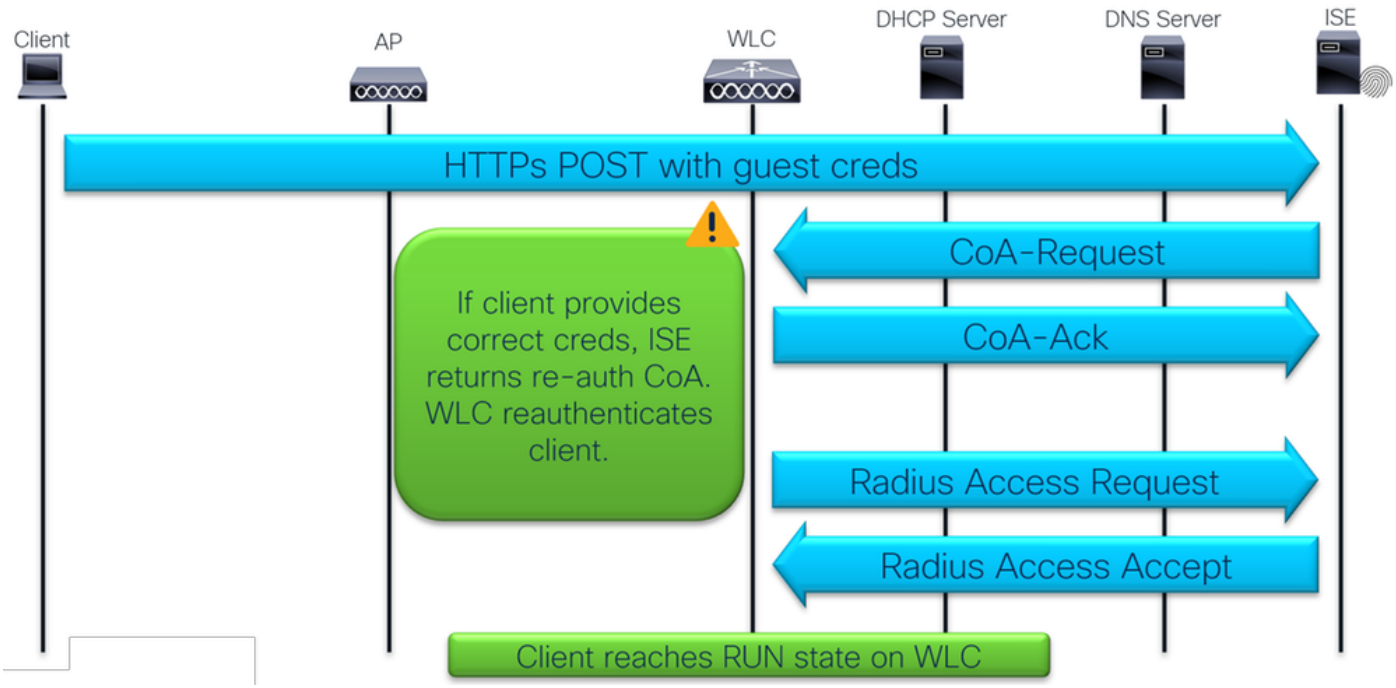
Interception et redirection du trafic

Connexion client au portail de connexion invité ISE :



Connexion du client au portail de connexion des invités ISE

Connexion client et CoA :

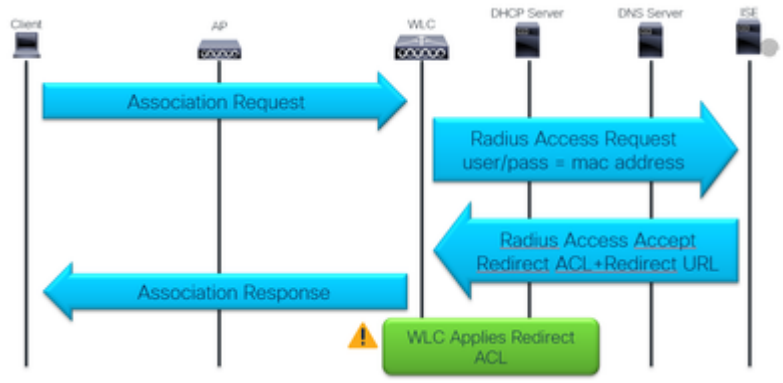


Connexion client et CoA

Dépannage

Symptôme courant d'un utilisateur non redirigé vers la page de connexion

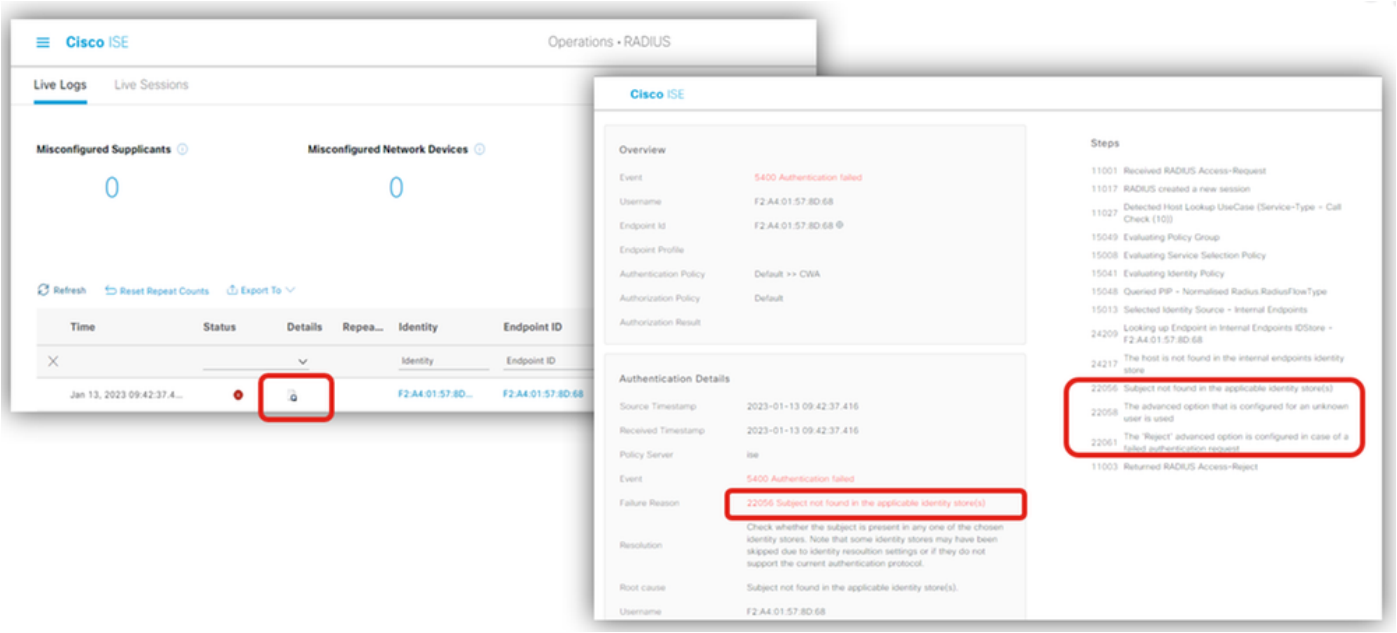
Commençons par la première partie du flux :



Première association et authentification RADIUS

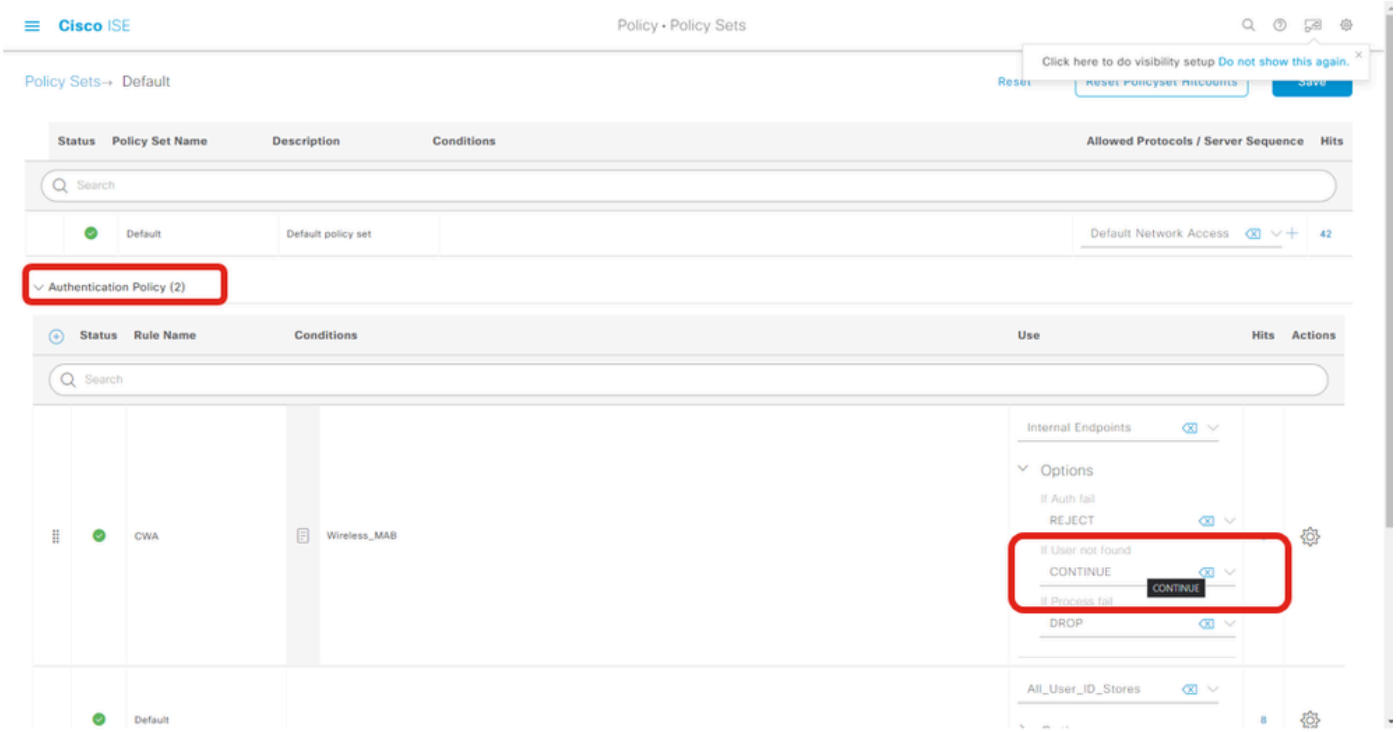
La première authentification RADIUS a-t-elle réussi ?

Vérifiez le résultat de l'authentification de filtrage MAC :



Journaux ISE Live montrant le résultat de l'authentification de filtrage MAC

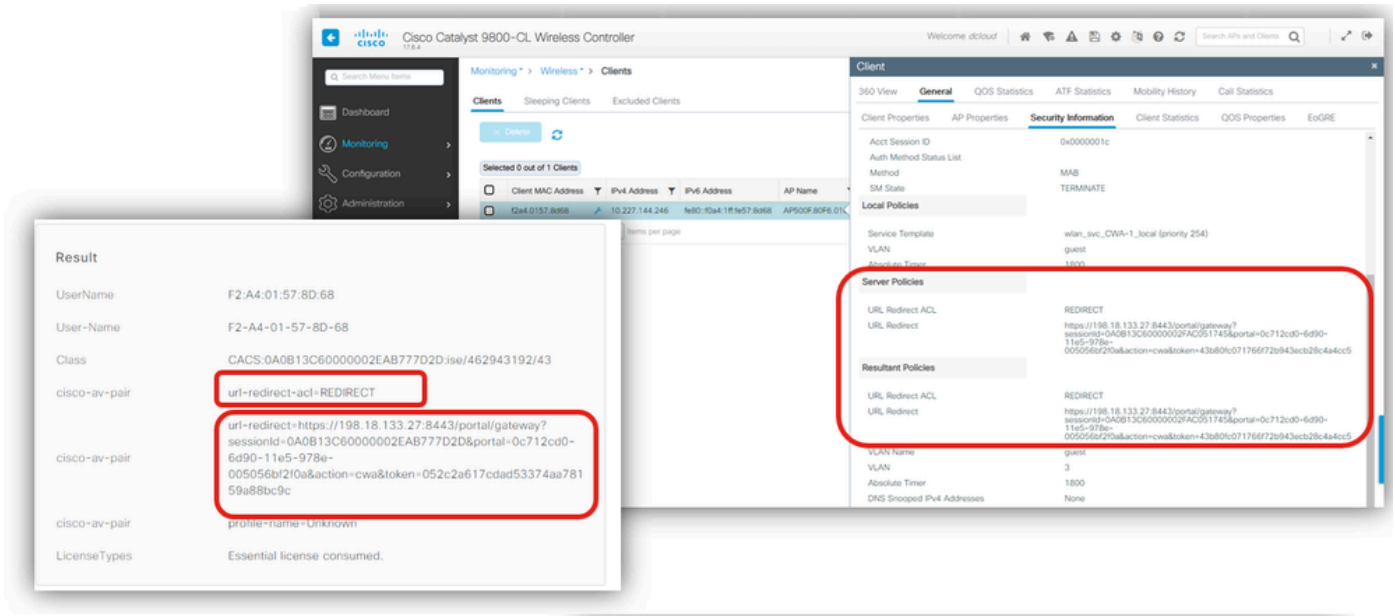
Assurez-vous que l'option avancée pour l'authentification est définie sur Continue si l'utilisateur est introuvable :



Option avancée Utilisateur introuvable

Le WLC reçoit-il l'URL de redirection et l'ACL ?

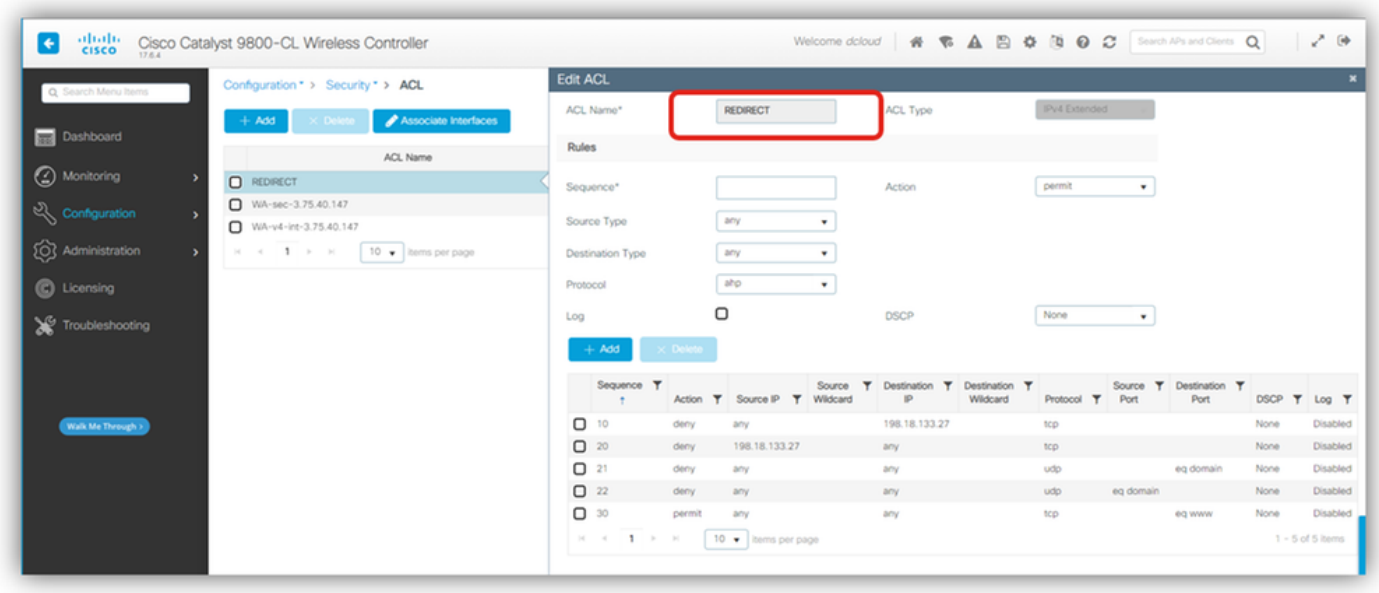
Vérifiez les journaux en direct ISE et les informations de sécurité du client WLC sous Surveillance Vérifiez que l'ISE envoie l'URL de redirection et l'ACL dans l'acceptation d'accès et qu'elle est reçue par le WLC et appliquée au client dans les détails du client :



Redirection ACL et URL

La liste de contrôle d’accès Redirect est correcte ?

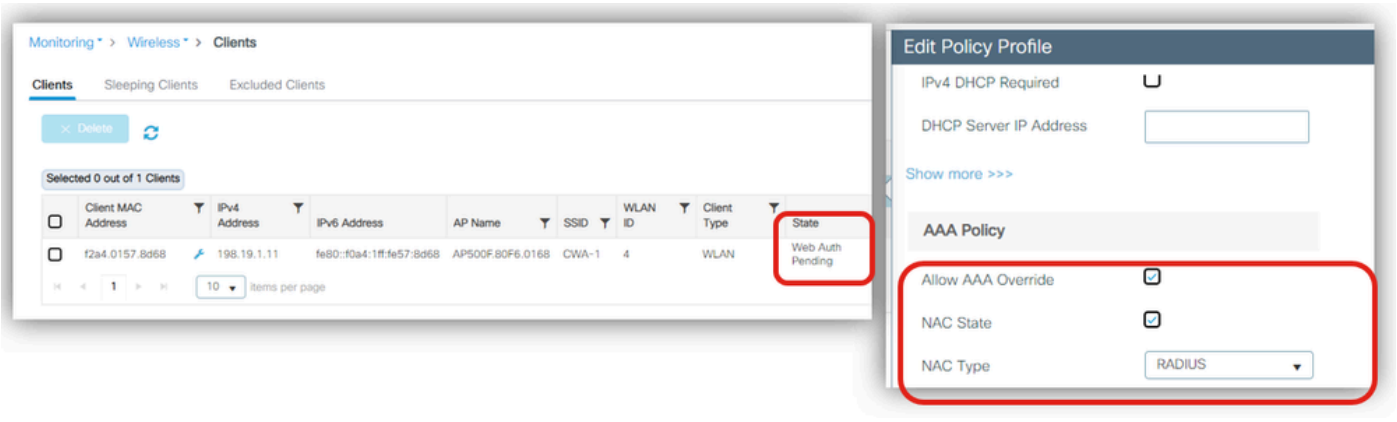
Vérifiez le nom de la liste de contrôle d'accès. Assurez-vous qu'il est exactement comme il est envoyé par l'ISE :



Vérification ACL de redirection

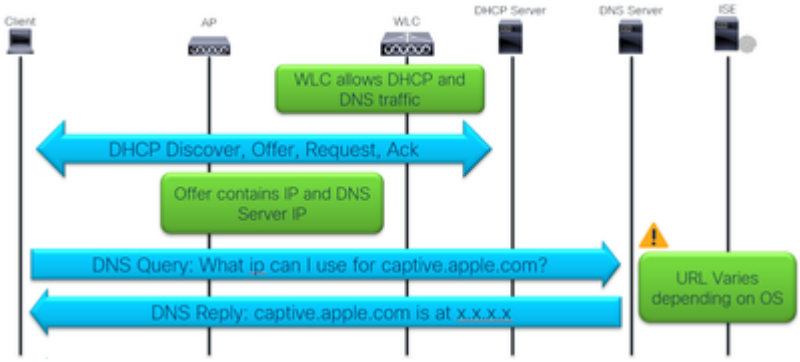
Le client est-il déplacé vers Web-Auth en attente ?

Vérifiez les détails du client pour l'état Web Auth Pending. S'il n'est pas dans cet état, vérifiez si le remplacement AAA et le contrôle d'accès réseau RADIUS sont activés dans le profil de stratégie :



Détails du client, remplacement aaa et NAC RADIUS

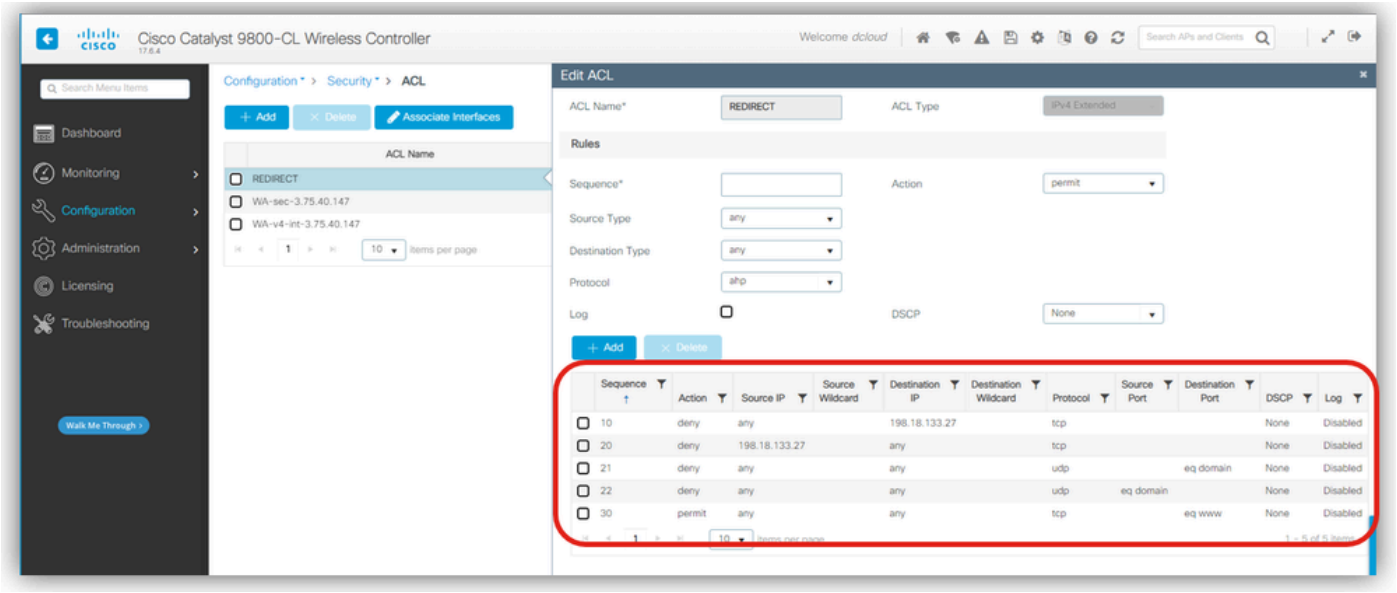
Si le problème persiste, revoyez le flux :



DHCP, DNS et vérification de la connectivité

Le WLC autorise-t-il le trafic DHCP et DNS ?

Vérifiez le contenu de la liste de contrôle d'accès redirigée dans le WLC :



Rediriger le contenu ACL dans le WLC

La liste de contrôle d'accès Redirect définit le trafic intercepté et redirigé par l'instruction permit et le trafic ignoré de l'interception et de la redirection avec une instruction deny.

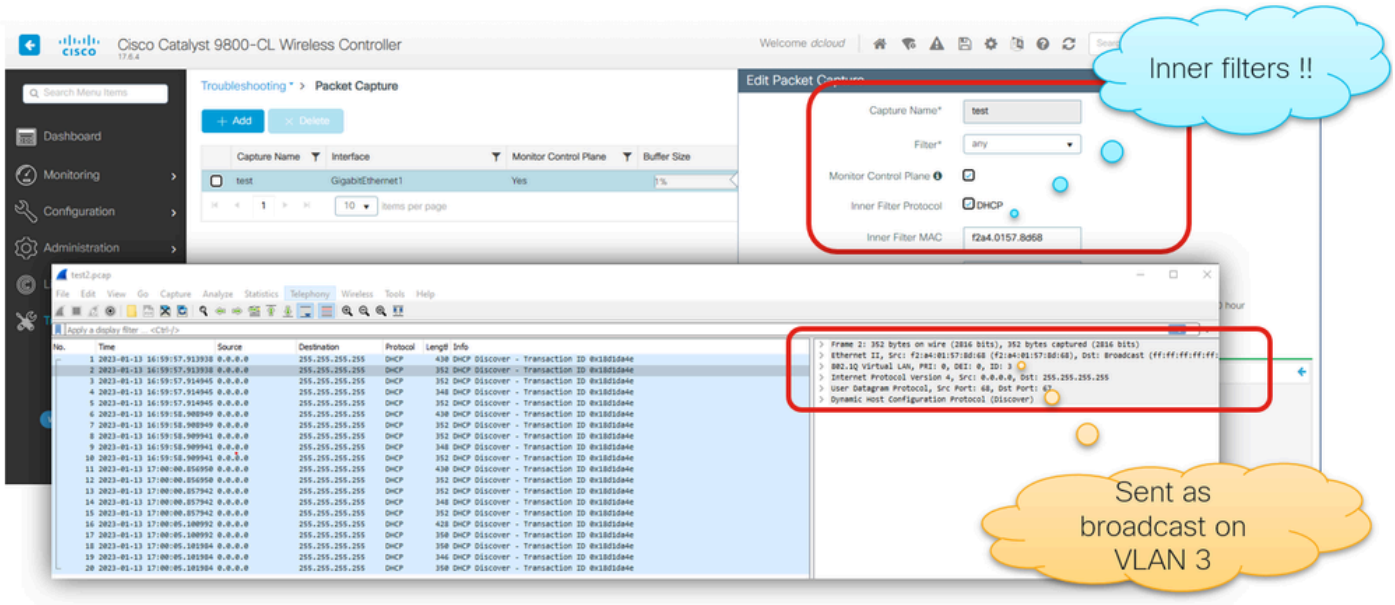
Dans cet exemple, le DNS et le trafic vers/depuis l'adresse IP ISE sont autorisés à circuler, et tout trafic TCP sur le port 80 (WWW) est intercepté.

Le serveur DHCP reçoit-il une détection/requête DHCP ?

Vérifiez auprès de l'EPC si un échange DHCP a lieu. EPC peut être utilisé avec des filtres internes tels que le protocole DHCP et/ou l'adresse MAC de filtre interne, où vous pouvez utiliser l'adresse

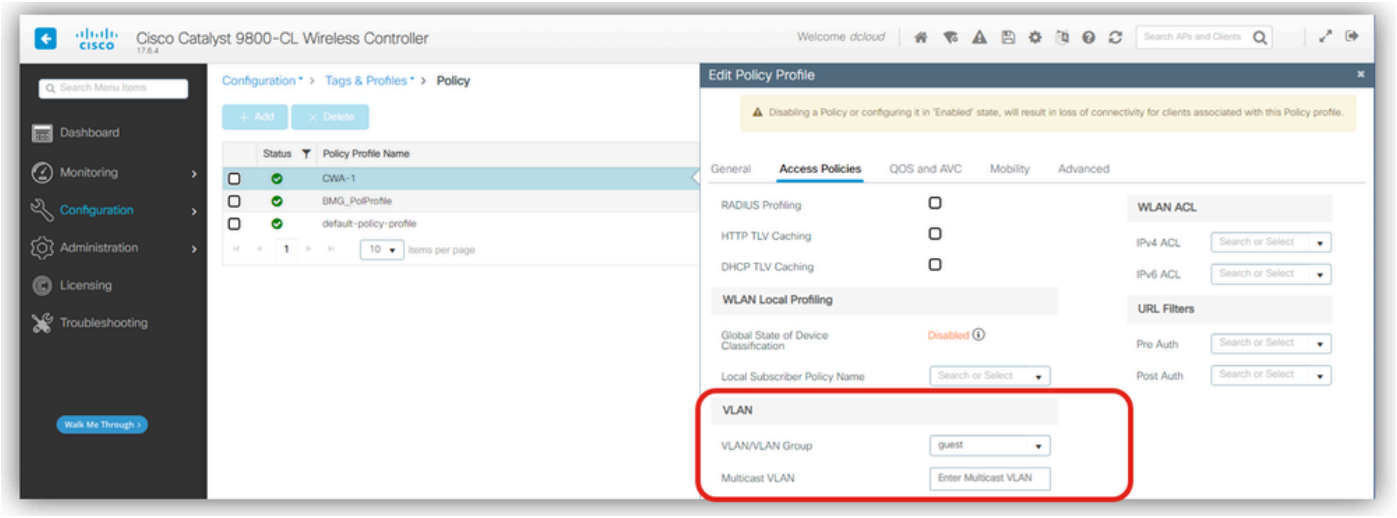
MAC du périphérique client et obtenir dans l'EPC uniquement les paquets DHCP envoyés par ou envoyés à l'adresse MAC du périphérique client.

Dans cet exemple, notez les paquets de détection DHCP envoyés en tant que diffusion sur le VLAN 3 :



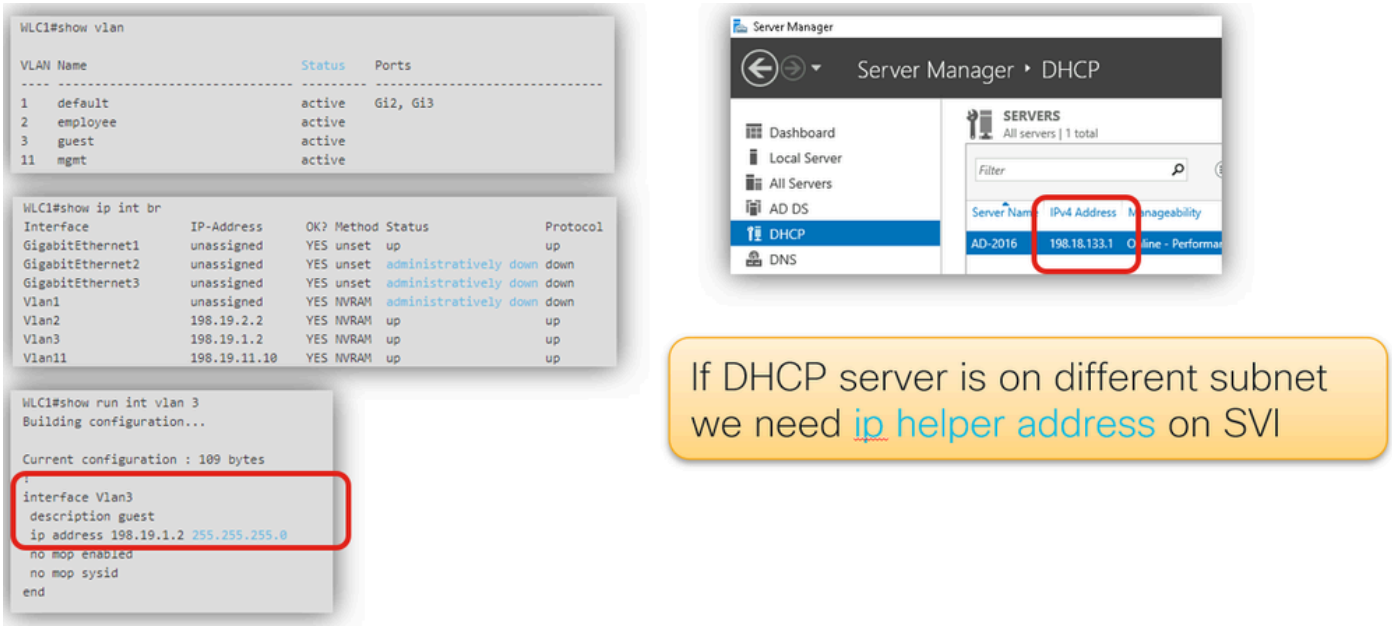
WLC EPC pour vérifier DHCP

Confirmez le VLAN client attendu dans le profil de stratégie :



VLAN dans le profil de stratégie

Vérifiez le VLAN WLC, la configuration de la ligne réseau du port de commutation et le sous-réseau DHCP :



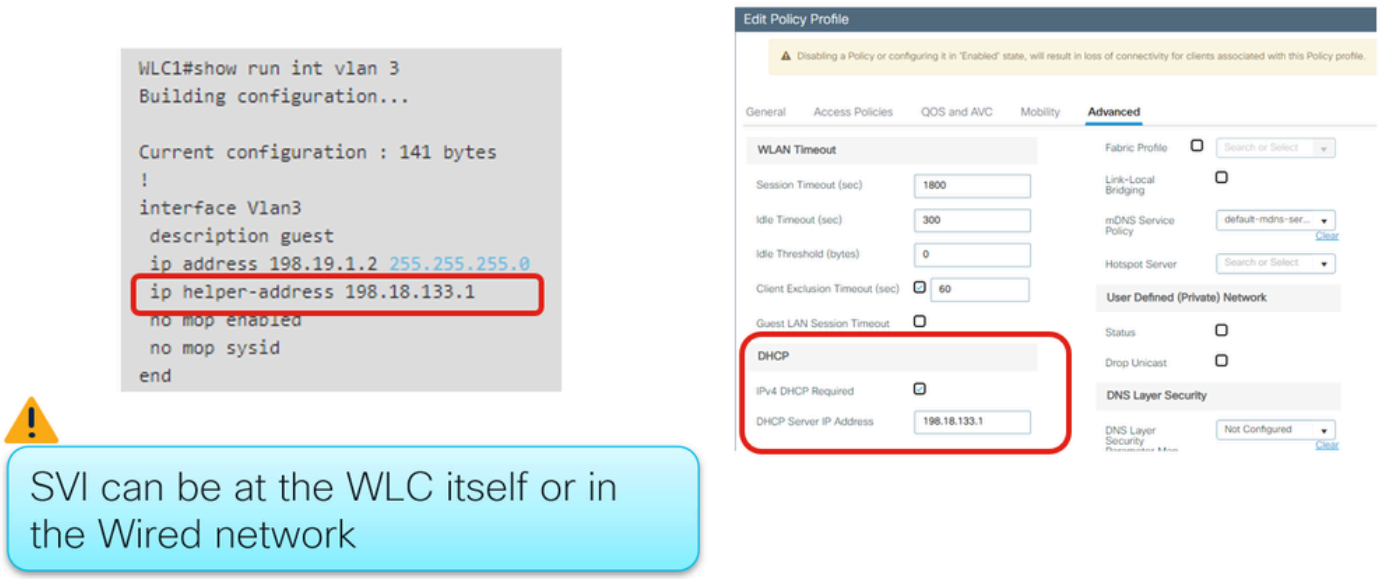
VLAN, port de commutation et sous-réseau DHCP

Le VLAN 3 existe dans le WLC et il a également une interface virtuelle de commutateur (SVI) pour le VLAN 3. Cependant, lors de la vérification de l'adresse IP du serveur DHCP, il est sur un sous-réseau différent ; par conséquent, une adresse ip helper-address est nécessaire sur l'interface SVI.

Les meilleures pratiques exigent que les interfaces SVI pour les sous-réseaux clients soient configurées dans l'infrastructure filaire, en les évitant au niveau du WLC.

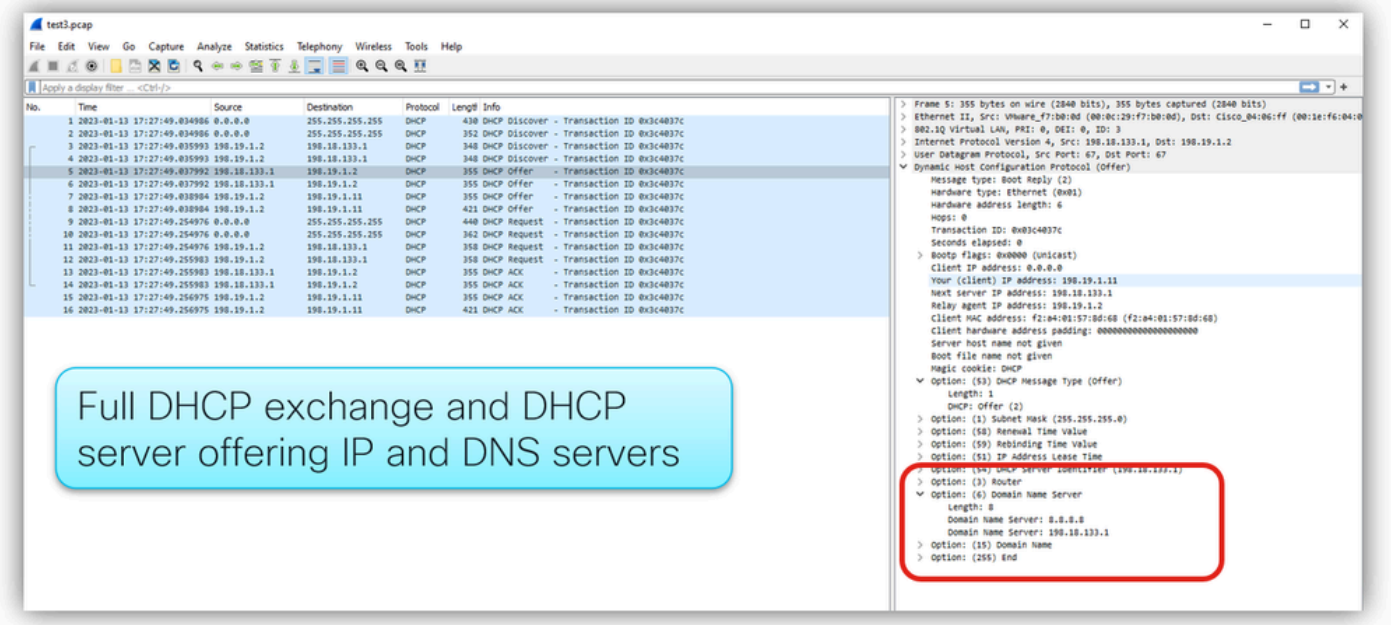
Dans tous les cas, la commande ip helper-address doit être ajoutée à l'interface SVI, quel que soit l'endroit où elle se trouve.

Vous pouvez également configurer l'adresse IP du serveur DHCP au niveau du profil de stratégie :



Adresse Ip helper au niveau de l'interface SVI ou du profil de stratégie

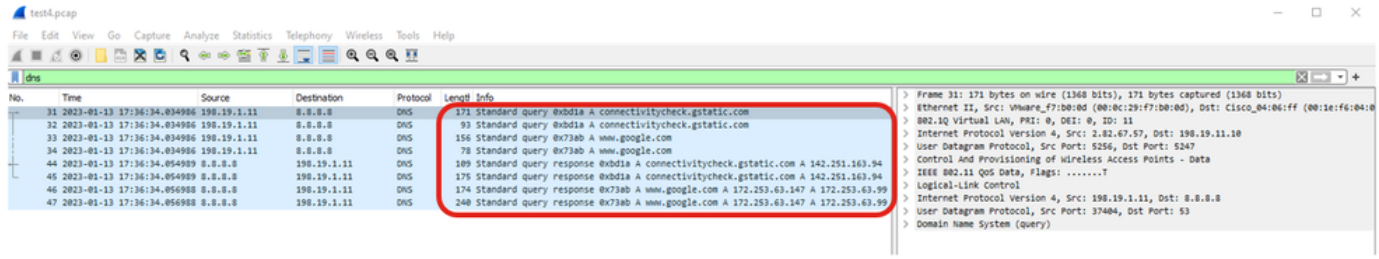
Vous pouvez ensuite vérifier auprès d'EPC si l'échange DHCP a réussi et si le serveur DHCP offre des adresses IP de serveur DNS :



Offre DHCP Détail de l'adresse IP du serveur DNS

La redirection automatique se produit-elle ?

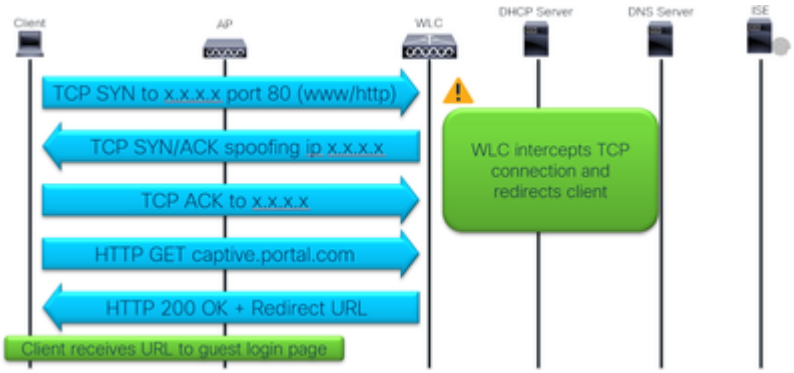
Vérifiez auprès du WLC EPC si le serveur DNS répond aux requêtes :



Requêtes et réponses DNS

- Si la redirection n'est pas automatique, ouvrez un navigateur et essayez une adresse IP aléatoire. Par exemple 10.0.0.1.
- Si la redirection fonctionne alors, il est possible que vous ayez un problème de résolution DNS.

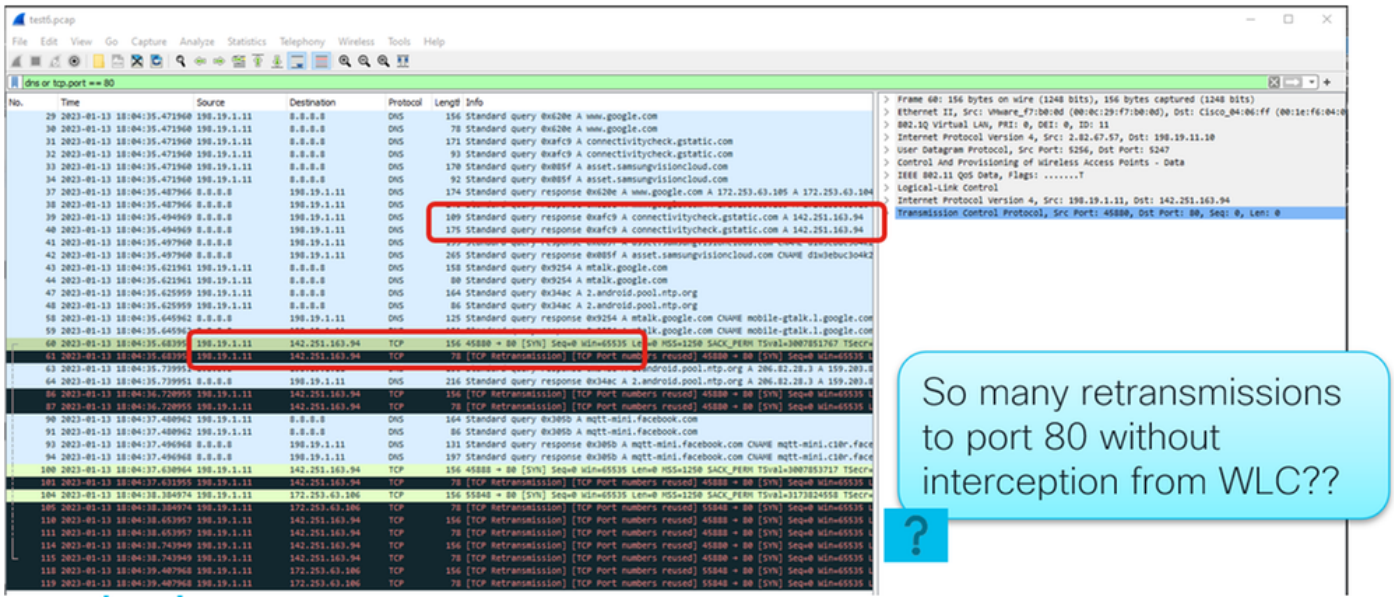
Si le problème persiste, revoyez le flux :



Interception et redirection du trafic

Le navigateur n'affiche-t-il pas la page de connexion ?

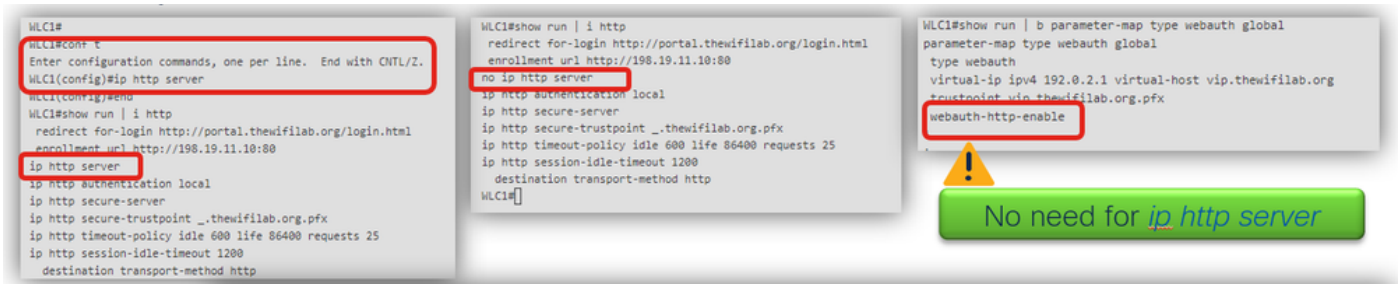
Vérifiez si le client envoie le TCP SYN au port 80 et si le WLC l'intercepte :



Retransmissions TCP vers le port 80

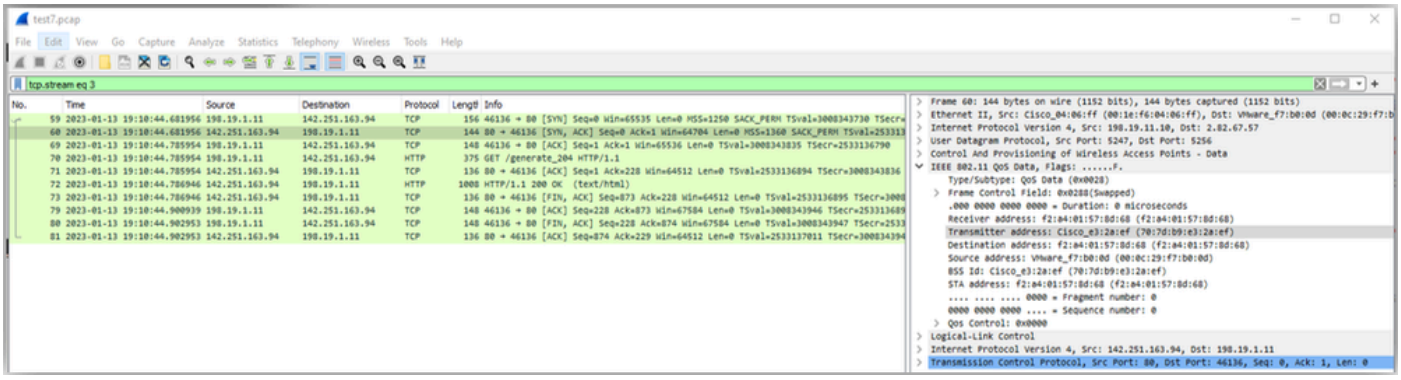
Dans cet exemple, le client envoie des paquets TCP SYN au port 80 mais n'obtient aucune réponse et effectue des retransmissions TCP.

Assurez-vous que vous avez la commande ip http server dans la configuration globale ou la commande webauth-http-enable dans le paramètre-map global :



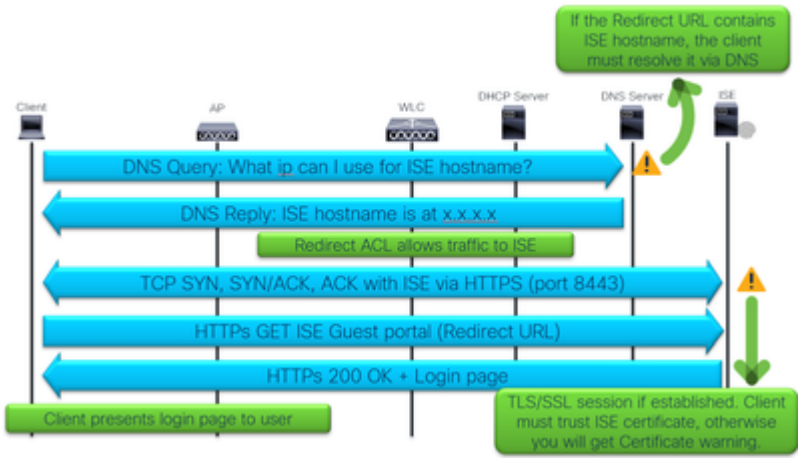
commandes d'interception http

Une fois la commande appliquée, le WLC intercepte le trafic TCP et usurpe l'adresse IP de destination pour répondre au client et le rediriger.



Interception TCP par WLC

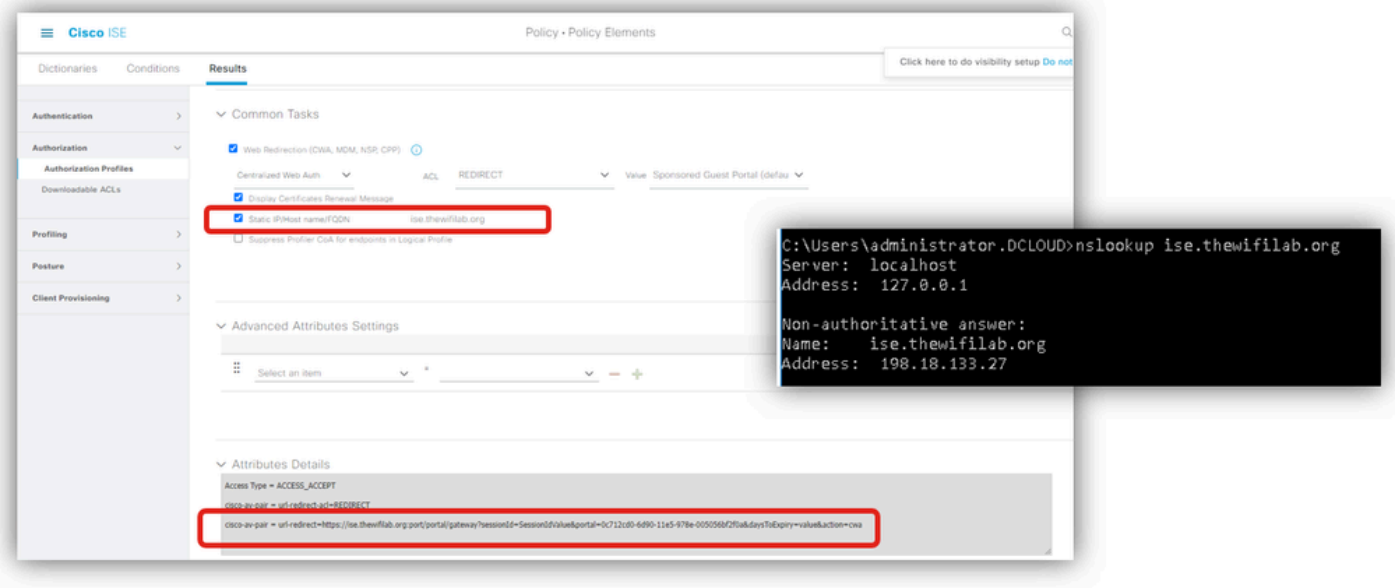
Si le problème persiste, poursuivez avec le flux :



Connexion du client au portail de connexion des invités ISE

Le client peut-il résoudre le nom d'hôte ISE ?

Vérifiez si l'URL de redirection utilise une adresse IP ou un nom d'hôte, et si le client résout le nom d'hôte ISE :

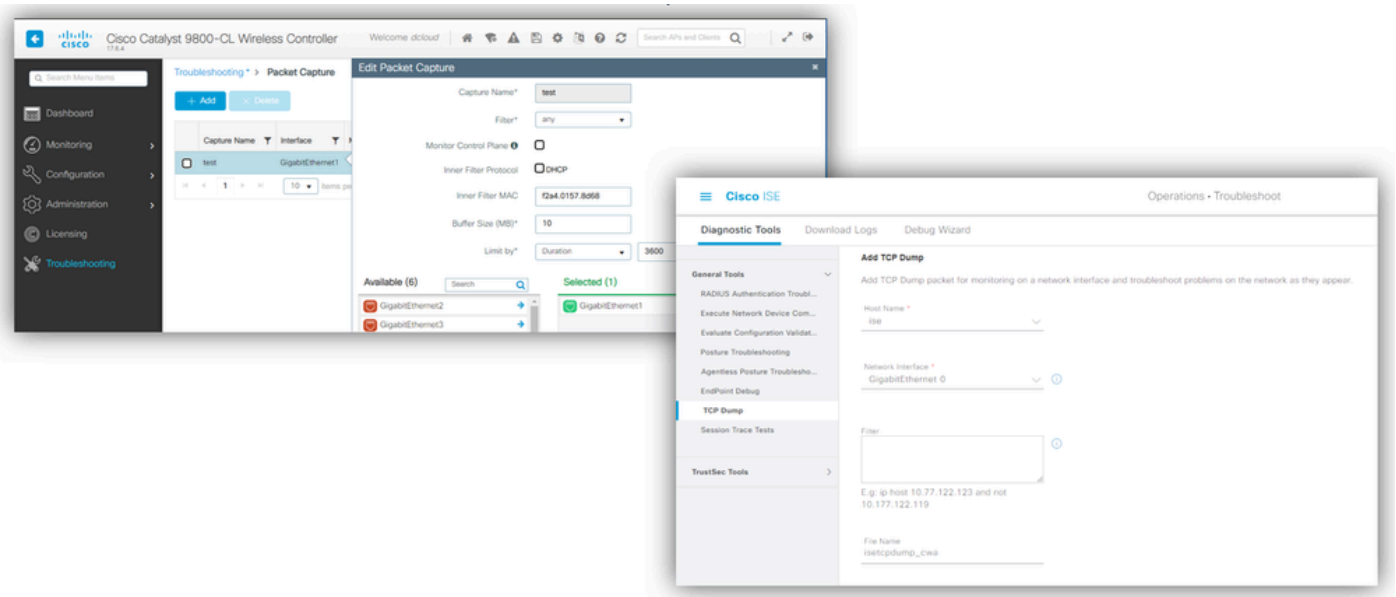


Résolution des noms d'hôte ISE

Un problème courant se produit lorsque l'URL de redirection contient le nom d'hôte ISE, mais que le périphérique client ne parvient pas à résoudre ce nom d'hôte en adresse IP ISE. Si un nom d'hôte est utilisé, assurez-vous qu'il est résoluble via DNS.

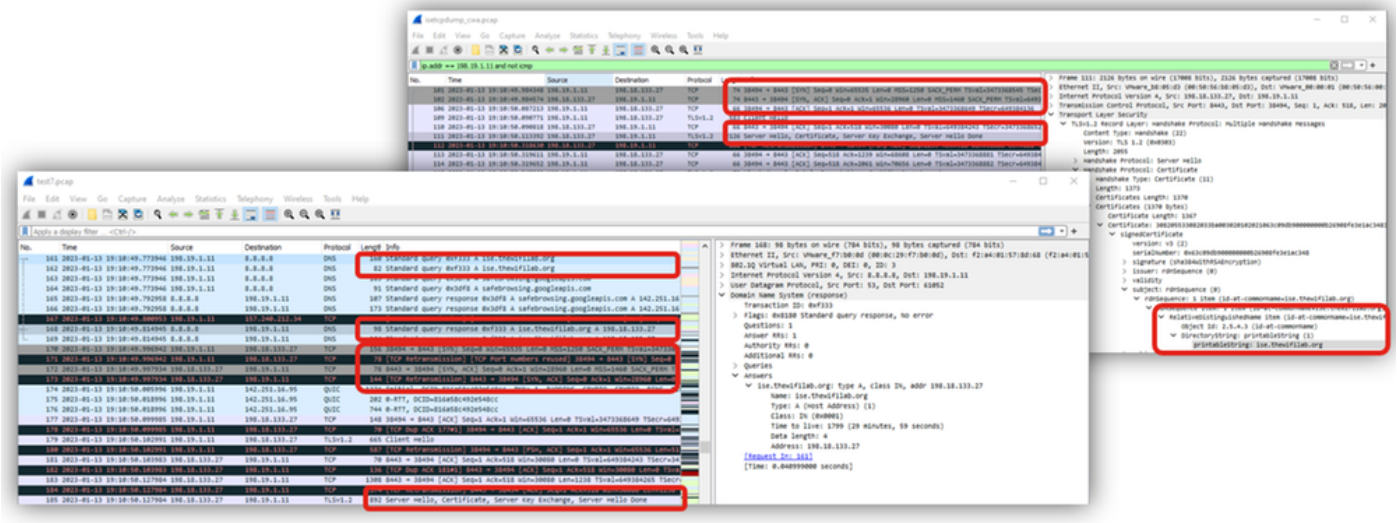
La page de connexion ne se charge toujours pas ?

Vérifiez avec WLC EPC et ISE TCPdump si le trafic client atteint le noeud ISE Policy Services Node (PSN). Configurez et lancez les captures sur le WLC et l'ISE :



WLC EPC et ISE TCPDump

Après la reproduction du problème, collecter les captures et corréler le trafic. Dans cet exemple, le nom d'hôte ISE est résolu, suivi de la communication entre le client et ISE sur le port 8443 :



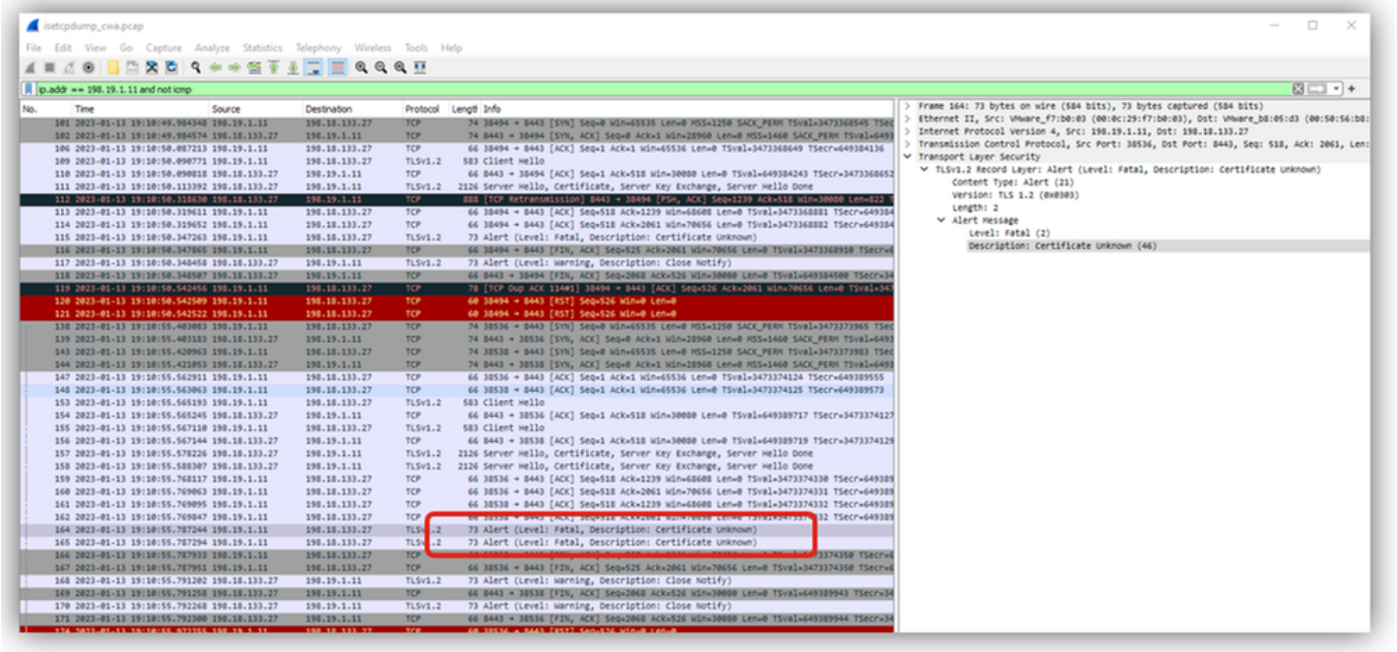
Trafic WLC et ISE

Pourquoi y a-t-il une violation de sécurité due au certificat ?

1. Si vous utilisez un certificat auto-signé sur ISE, il est attendu que le client lance un avertissement de sécurité lorsqu'il tente de présenter la page de connexion au portail ISE.

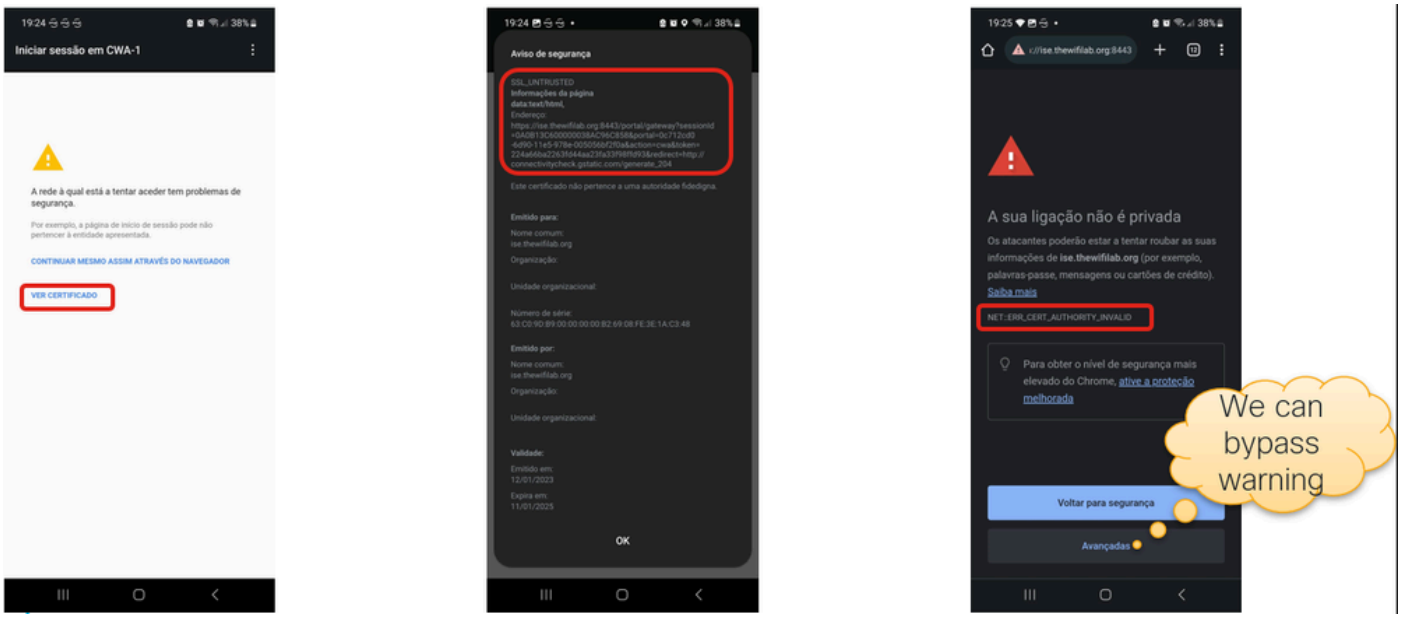
Sur le WLC EPC ou le TCPdump ISE, vous pouvez vérifier si le certificat ISE est approuvé.

Dans cet exemple, la connexion se ferme à partir du client avec une alerte (niveau : Fatal, Description : Certificate Unknown), ce qui signifie que le certificat ISE est inconnu (approuvé)



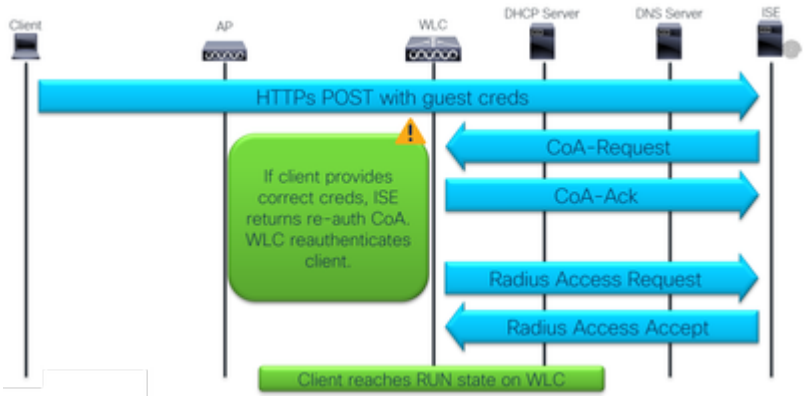
Certificat ISE non approuvé

Si cette case est cochée du côté client, vous voyez ces exemples de résultats :



Périphérique client qui ne fait pas confiance au certificat ISE

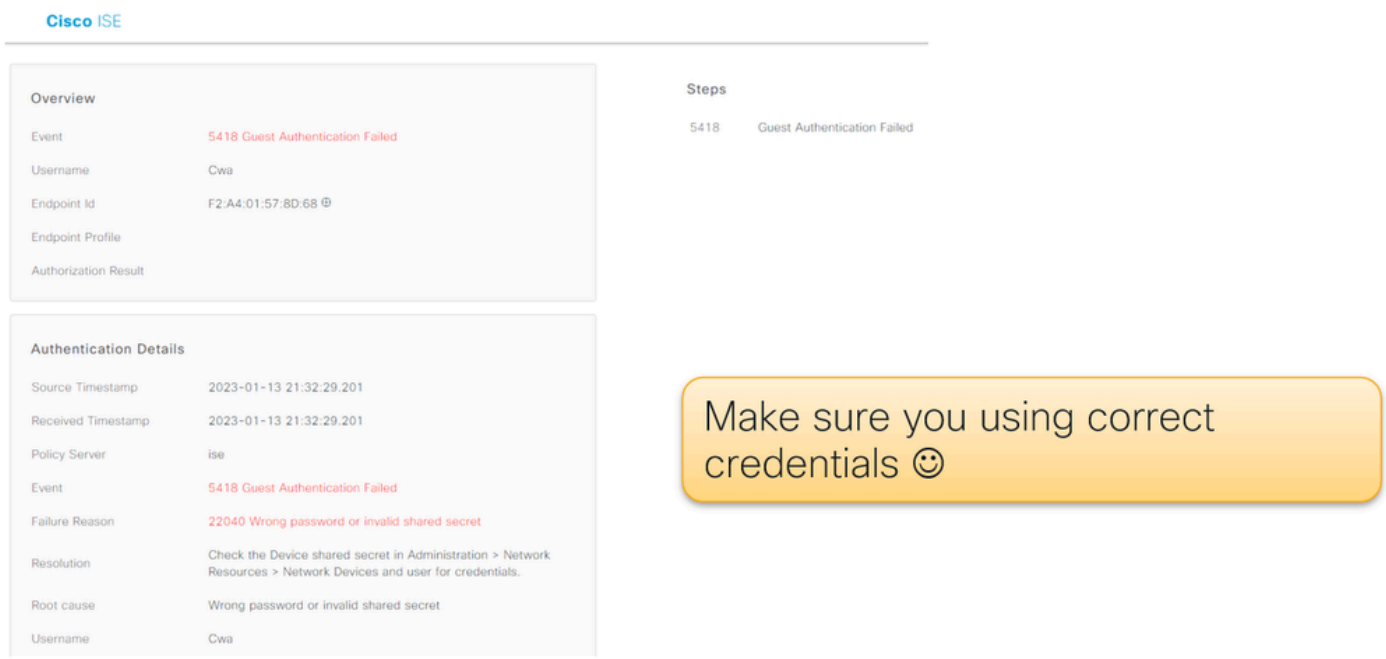
Si la redirection fonctionne mais que la connexion échoue, vérifiez la dernière partie du flux :



Connexion client et CoA

La connexion invité échoue-t-elle ?

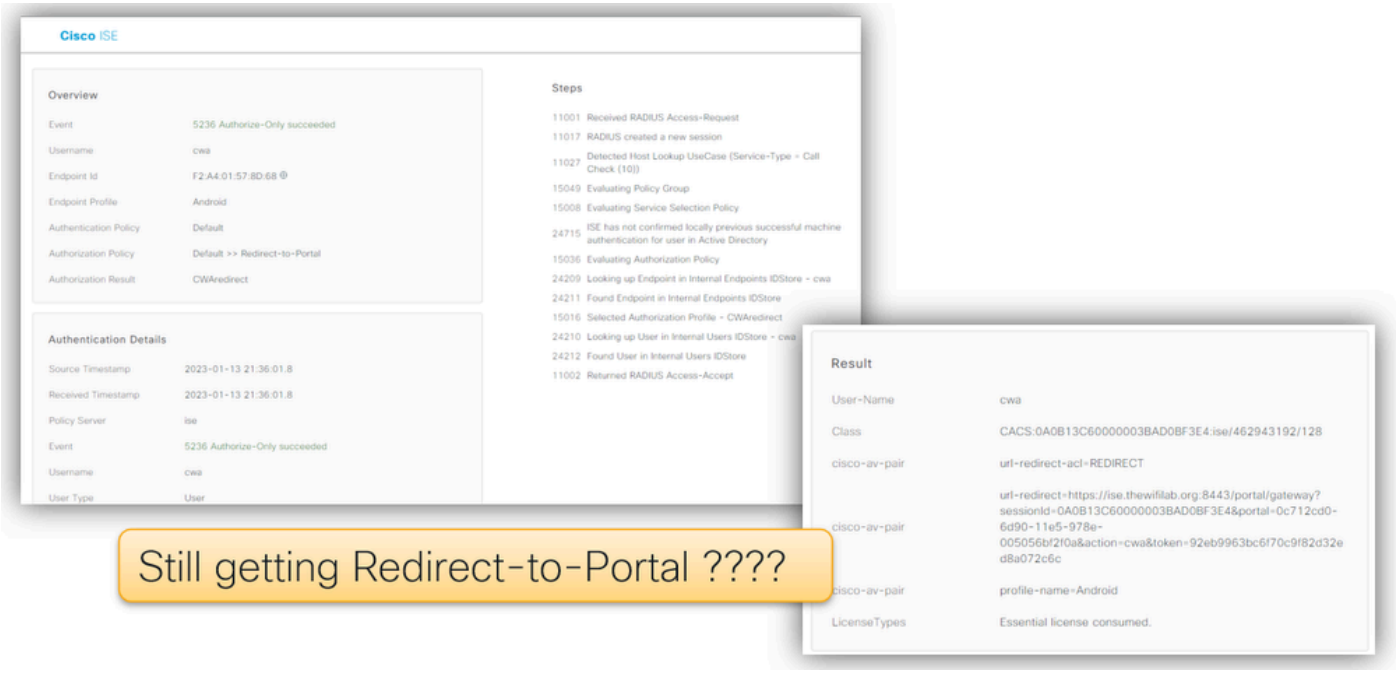
Recherchez les erreurs d'authentification dans les journaux ISE. Vérifiez que les informations d'identification sont correctes.



L'authentification des invités échoue en raison de références incorrectes

La connexion réussit-elle mais le client ne passe pas à l'état d'exécution ?

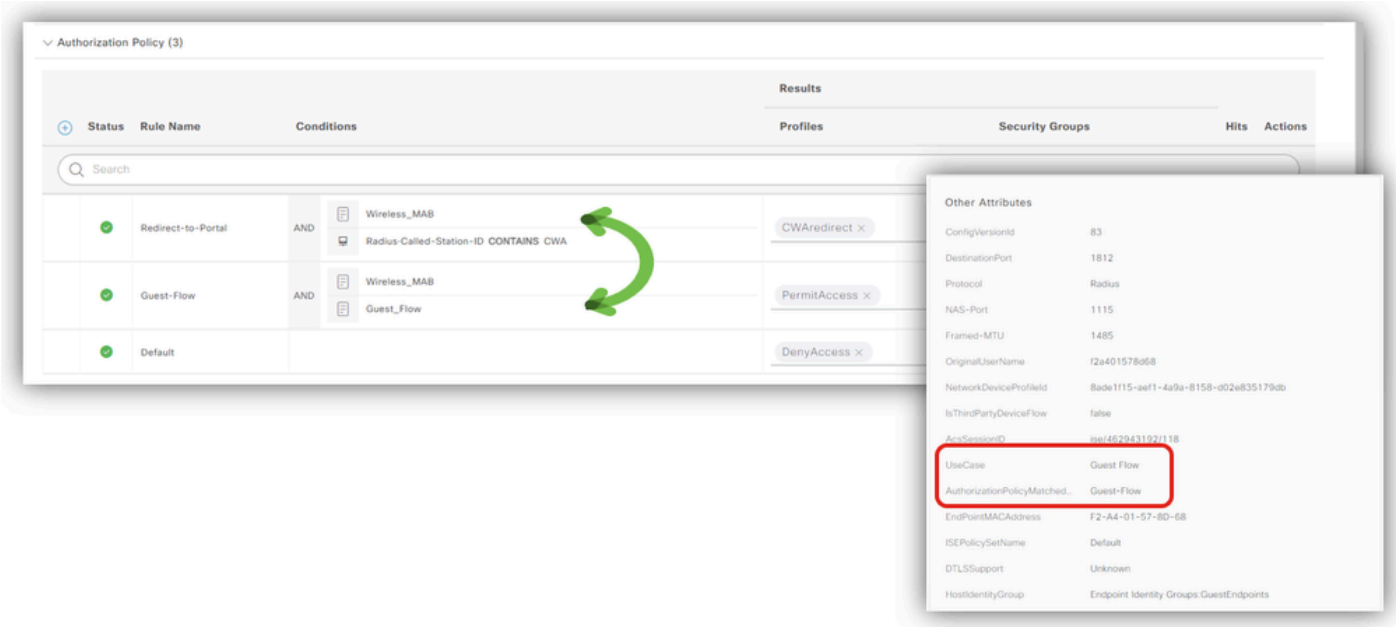
Consultez les journaux ISE pour connaître les détails et les résultats de l'authentification :



Boucle de redirection

Dans cet exemple, le client reçoit à nouveau le profil d'autorisation contenant l'URL de redirection et la liste de contrôle d'accès de redirection. Il en résulte une boucle de redirection.

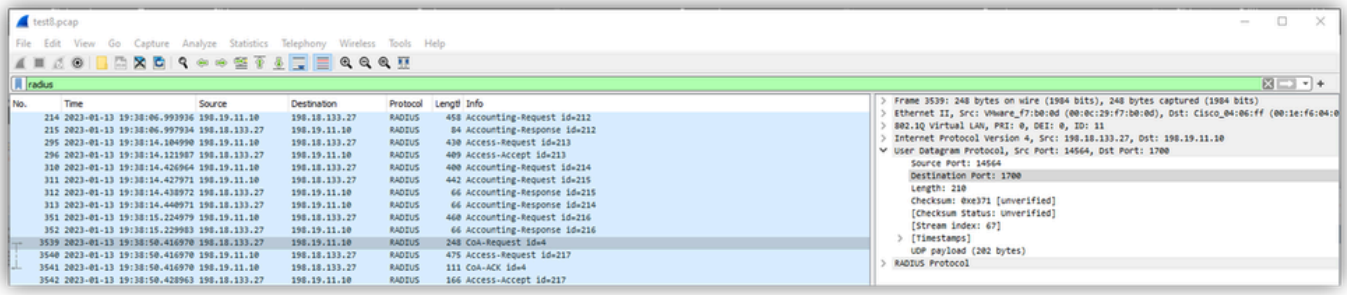
Vérifiez le jeu de stratégies. La règle de vérification Guest_Flow doit être placée avant la règle de redirection :



Règle Guest_Flow

Le certificat d'authenticité est défectueux ?

Avec EPC et ISE TCPDump, vous pouvez vérifier le trafic CoA. Vérifiez si le port CoA (1700) est ouvert entre le WLC et ISE. Assurez-vous que le secret partagé correspond.



trafic CoA

Remarque : Sur les versions 17.4.X et ultérieures, assurez-vous de configurer également la clé du serveur CoA lorsque vous configurez le serveur RADIUS. Utilisez la même clé que le secret partagé (ils sont identiques par défaut sur ISE). L'objectif est de configurer éventuellement une clé différente pour CoA que le secret partagé si c'est ce que votre serveur RADIUS a configuré. Dans Cisco IOS® XE 17.3, l'interface utilisateur Web utilisait

simplement le même secret partagé que la clé CoA.

À partir de la version 17.6.1, RADIUS (y compris CoA) est pris en charge par ce port. Si vous souhaitez utiliser le port de service pour RADIUS, vous devez disposer de la configuration suivante :

<#root>

```
aaa server radius dynamic-author
 client 10.48.39.28
```

vrf

Mgmt-intf

```
 server-key cisco123

interface GigabitEthernet0
```

vrf

forwarding

Mgmt-intf

```
 ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
 server name nicoISE
```

ip

vrf

forwarding

Mgmt-intf

ip

radius

source

-interface GigabitEthernet0

Résumé

Voici la liste de contrôle CWA résumée :

- Assurez-vous que le client se trouve sur le VLAN correct et obtient une adresse IP et un DNS.
- Obtenez les détails du client sur le WLC et exécutez des captures de paquets pour voir l'échange DHCP.
- Vérifiez que le client peut résoudre les noms d'hôte via DNS.
- Envoyez une requête ping au nom d’hôte depuis l’invite de commandes.
- Le WLC doit être à l'écoute sur le port 80.
- Vérifiez la commande globale ip http server ou la commande de mappage de paramètre global webauth-http-enable.
- Pour supprimer l'avertissement de certificat, installez un certificat approuvé sur ISE.
- Il n'est pas nécessaire d'installer un certificat approuvé sur le WLC dans CWA.
- Définissez l'option Authentication Policy at ISE Advanced sur Continue si l'utilisateur est introuvable.
- Autorisez les utilisateurs invités sponsorisés à se connecter et à obtenir la redirection d'URL et la liste de contrôle d'accès.

Principaux outils utilisés pour le dépannage :

- • EPC WLC

- : Filtres internes : Protocole DHCP, adresse MAC.
- Moniteur WLC
- : Vérifiez les détails de sécurité du client.
- Suivi WLC RA
- : Débogue avec des informations détaillées du côté WLC.
- Journaux en direct ISE
- : Détails d'authentification.
- ISE TCPDump
- : Collectez les captures de paquets sur l'interface PSN ISE.

Informations sur les ressources

- Configurer l'authentification Web centrale (CWA) sur le WLC Catalyst 9800 et ISE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.