Configurez la radio CWA ISE et le point névralgique circule avec AireOS et nouvelle génération WLCs

Contenu

Introduction

Ce document décrit comment configurer trois cas d'utilisation d'invité dans le Cisco Identity Services Engine (ISE) avec Cisco AireOS et prochains contrôleurs LAN Sans fil de Generation(NGWC) (WLCs).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleurs LAN Sans fil de Cisco (unifiés et Access convergé)
- Cisco Identity Services Engine (ISE)

Composants utilisés

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

- Version 2.1 de Logiciel Cisco Identity Services Engine
- Contrôleur LAN Sans fil 5508 8.0.121.0 s'exécutants de Cisco
- Catalyst du contrôleur sans-fil de nouvelle génération (NGWC) 3850(WS-C3850-24P) exécutant 03.06.04.E

Configurez

Diagramme du réseau

Les étapes couvertes dans ce document décrivent la configuration typique sur Access unifié et convergé WLCs pour prendre en charge n'importe quel écoulement d'invité avec ISE.

Configurez a unifié 5508 WLC

Indépendamment du cas d'utilisation configuré dans ISE, du point de vue WLC il tous les débuts avec un point final Sans fil qui se connecte à un SSID ouvert au filtrage MAC a activé (plus dépassement et RAYON NAC d'AAA) ces points à ISE en tant que serveur d'authentification et de comptabilité. Ceci s'assure qu'ISE peut dynamiquement pousser les attributs nécessaires au WLC pour l'application réussie du portail d'invité du redirect to un ISE.

Configuration globale

1. Ajoutez ISE globalement en tant que serveur d'authentification et de comptabilité.

   - Naviguez vers la **Sécurité > l'AAA > l'authentification** et cliquez sur New
   - Écrivez l'IP de serveur ISE et le secret partagé

- Assurez-vous que l'état de serveur et le **soutien de RFC 3676** (modification de support d'autorisation ou CoA) sont deux positionnement à **activer**.
- Sous le délai de temporisation du serveur par AireOS par défaut WLCs aura 2 secondes. Selon les caractéristiques du réseau (latence, ISE et WLC dans les endroits différents, etc.) il peut être salutaire d'augmenter le délai de temporisation du serveur au moins à 5 secondes pour éviter des événements inutiles de Basculement.
- Cliquez sur **Apply**.
- S'il y a plusieurs les Noeuds de services de stratégie (le RPC) à configurer poursuivent pour créer les entrées supplémentaires de serveur.

Remarque: Cet exemple particulier de configuration inclut 2 exemples ISE

- Naviguez vers la **Sécurité > l'AAA > le RAYON > la comptabilité** et cliquez sur New
- Écrivez l'IP de serveur ISE et le secret partagé
- Assurez-vous que l'état de serveur est placé à activer
- Augmentez le délai de temporisation du serveur s'il y a lieu (le par défaut est de 2 secondes).

2. Configuration de retour.

Dans l'environnement unifié une fois que le délai de temporisation du serveur est déclenché le WLC se déplace au prochain serveur configuré. Ensuite dans la ligne du WLAN. Si pas autre est disponible puis le WLC sélectionne le prochain dans la liste globale de serveurs. Quand de plusieurs serveurs sont configurés sur le SSID (primaire, secondaire, etc.) une fois que que le Basculement se produit le WLC par défaut continue à envoyer le trafic d'authentification et (ou) de comptabilité de manière permanente à l'exemple secondaire même si le serveur primaire est de retour en ligne.

Afin d'atténuer ce retour d'enable de comportement. Naviguez vers la **Sécurité > l'AAA > le RAYON > le retour.** Le comportement par défaut est éteint. La seule manière de récupérer d'un événement de serveur-vers le bas exige l'intervention d'admin (rebondissez globalement l'état de l'admin du serveur).

Pour activer le retour vous avez deux options :

- **Passif** - En mode passif, si un serveur ne répond pas à la demande d'authentification WLC, le WLC déplace le serveur à la file d'attente inactive et place un temporisateur (intervalle dans l'option de sec). Quand le temporisateur expire, le WLC déplace le serveur à la file d'attente active indépendamment de l'état d'effectif de serveurs. Si la demande d'authentification a comme conséquence un événement de délai d'attente (qui signifie que le serveur est toujours en panne) le serveur que l'entrée est déplacée de nouveau à la file d'attente inactive et le temporisateur donne un coup de pied dedans de nouveau. Si le serveur répond avec succès de retour, il reste dans la file d'attente active. Les valeurs configurables ici disparaissent de 180 à 3600 secondes.

- **Actif -** En mode actif, quand un serveur ne répond pas à la demande d'authentification WLC, le WLC marque le serveur comme mort, puis déplace le serveur au groupe inactif de serveur et commence envoyer des messages de sonde périodiquement jusqu'à ce que ce serveur réponde. Si le serveur répond, alors le WLC déplace le serveur mort au groupe actif et cesse d'envoyer des messages de sonde.

En ce mode le WLC exige de vous d'écrire un nom d'utilisateur et un intervalle de sonde en quelques secondes (180 3600).

Remarque: La sonde WLC n'exige pas une authentification réussie. La manière, un réussi ou les authentifications défaillantes sont considérées une réponse de serveur qui est assez pour promouvoir le serveur à la file d'attente active.

Configurez l'Identifiant SSID (Service Set Identifier) de l'invité :

- Naviguez vers l'onglet WLAN et créez dessous la nouvelle option cliquent sur Go :
- Écrivez le nom de profil et le nom SSID. Cliquez sur **Apply**.
- Sous l'onglet Général sélectionnez l'interface ou le groupe d'interface à utiliser (invité VLAN).
- Sous la **Sécurité > la couche 2 > degré de sécurité de la couche 2** choisi case à cocher de **filtrage de MAC d'aucun** et d'enable.
- Sous les serveurs réglés d'authentification et de comptabilité d'**onglet AAA Servers a activé** et sélectionne vos serveurs primaires et secondaires.
- **Mise à jour intérimaire** : C'est une configuration facultative qui n'ajoute aucun avantage à cet écoulement. Si vous préférez l'activer, le WLC je devrais exécuter 8.x ou code plus élevé :

Handicapé : La caractéristique est complètement désactivée.

Activé avec 0 intervalles : Le WLC envoie des mises à jour de comptabilité à ISE chaque fois qu'il y a un changement de l'entrée de Block(MSCB) de contrôle du poste mobile du client (IE. L'ipv4 ou l'affectation ou la modification d'ipv6 addres, l'événement d'itinérance de client, etc.) aucune mises à jour régulières supplémentaires sont envoyés.

Activé avec un intervalle intérimaire configuré : En ce mode le WLC envoie des notifications à ISE sur les modifications d'entrée MSCB du client et il envoie également des notifications périodiques supplémentaires de comptabilité à l'intervalle configuré (indépendamment de toutes modifications).

- Sous l'**Allow AAA Override d'**enable d'onglet Avancé et sous le **RAYON** choisi **NAC d'état NAC**. Ceci s'assure que le WLC applique toutes les paires de valeurs d'attribut (AVPs) qui proviennent ISE.
- Naviguez vers l'onglet général SSID et placez l'état SSID à **activer**
- **Appliquez les** modifications.

Configurez l'ACL de réorientation

Cet ACL est mis en référence par ISE et il détermine quel trafic obtient réorienté et quel trafic sera permis.

- Allez à l'**onglet Sécurité** > aux **listes de contrôle d'accès** et cliquez sur New
- C'est un exemple d'ACL

Cet ACL devrait permettre l'accès à et des services DNS et des Noeuds ISE au-dessus du port TCP 8443. Il y a un implicite refusent au bas qui signifie que le reste du trafic obtient réorienté à l'URL portail de l'invité d'ISE.

HTTPS réorientent

Cette caractéristique est prise en charge dans des versions 8.0.x d'AireOS et se lève mais elle est arrêtée par défaut. Pour activer le support HTTPS allez à la **Gestion** WLC > à la **redirection HTTP-HTTPS > HTTPS** et placez-la **activée** ou appliquez la cette commande dans le CLI :

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Les avertissements de certificat après HTTPS réorientent est activés

Après que https-réorientiez soit activé, l'utilisateur puisse éprouver des questions de confiance de certificat pendant la réorientation. Ceci est vu même s'il y a un certificat enchaîné valide sur le contrôleur et même si ce certificat est signé par une autorité de certification de confiance de tiers. La raison est que le certificat installé sur le WLC est fourni à son adresse Internet ou adresse IP d'interface virtuelle. Quand le client essaye des https : //cisco.com, le navigateur attend le certificat à fournir à cisco.com. Cependant, parce que le WLC pouvoir intercepter GET a émis par le client, il les premiers besoins d'établir la session HTTPS pour laquelle le WLC présente son certificat d'interface virtuelle pendant la phase de prise de contact SSL. Ceci fait afficher le navigateur un avertissement car le certificat présenté pendant la prise de contact SSL n'a pas été fourni au site Web d'origine que le client essaye d'accéder à (IE. cisco.com s'est opposé à l'adresse Internet de l'interface virtuelle de WLC). Vous pourriez voir différents messages d'erreur de certificat dans différents navigateurs mais tous associer au même problème.

Basculement agressif

Cette caractéristique est activée par défaut dans AireOS WLCs. Quand le Basculement agressif est activé, le WLC marque le serveur d'AAA pendant qu'insensible et lui se déplace au prochain serveur configuré d'AAA après qu'un événement de délai d'attente de rayon affecte un client.

Quand la caractéristique est désactivée le WLC bascule au prochain serveur seulement si l'événement de délai d'attente de RAYON se produit avec au moins 3 sessions de client. Cette caractéristique peut être désactivée par cette commande (aucune réinitialisation n'est exigée pour cette commande) :

```
(Cisco Controller) >config radius aggressive-failover disable
```

Pour vérifier l'état actuel de la caractéristique :

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Contournement captif

Les points finaux qui prennent en charge un mécanisme captif de Network Assistant (POUVEZ) pour découvrir un captif-portail et l'automatique-lancement une page de connexion font habituellement ceci par un pseudo-navigateur dans une fenêtre commandée tandis que d'autres

points finaux lancent un navigateur entièrement capable pour déclencher ceci. Pour des points finaux où la BOÎTE lance un pseudo-navigateur, ceci peut casser l'écoulement une fois réorienté à un portail captif ISE. Ceci affectent typiquement des périphériques IOS d'Apple et il a particulièrement des effets négatifs dans les écoulements qui exigent l'enregistrement de périphérique, le DHCP-Rlease VLAN, le contrôle de conformité, etc.

Selon la complexité de l'écoulement en service il peut être recommandé pour activer le contournement captif. Dans un tel scénario, le WLC ignore le mécanisme portail de détection de BOÎTE et le client doit ouvrir un navigateur pour initier le procédé de réorientation.

Vérifiez le statut de la caractéristique :

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..................... Disabled
Web Auth Redirect Ports ................... 80,3128
Web Auth Proxy Redirect  .................. Disable
Web Auth Captive-Bypass   ................. Disabled
Web Auth Secure Web  ...................... Enable
Web Auth Secure Redirection  .............. Enable
```

Pour activer ce type de caractéristique cette commande :

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

Le WLC alerte l'utilisateur qui pour que les modifications prennent effet un remise-système (reprise) sont nécessaires.

En ce moment un **show network summary** affiche la caractéristique comme activé, mais pour que des modifications prennent effet le WLC doivent être redémarrées.

Configurez a convergé 3850 NGWC

Configuration globale

1. **Ajoutez ISE globalement en tant que serveur d'authentification et de comptabilité**

   - Naviguez vers la **configuration > la Sécurité > le RAYON > les serveurs** et cliquez sur New
   - Écrivez l'**adresse IP du serveur** ISE, le **secret partagé**, le **délai de temporisation du serveur** et le **nombre de tentatives** qui reflète vos conditions environnementales.
   - Assurez-vous que le **soutien de RFC 3570** (support CoA) est activé.
   - Répétez le processus pour ajouter une entrée secondaire de serveur.
2. **Créez le groupe de serveurs d'ISE**

   - Naviguez vers la **configuration > la Sécurité > les groupes de serveurs** et cliquez sur New
   - Assignez un nom au groupe et écrivez une valeur de **temps d'arrêt** en quelques minutes. C'est le temps que le contrôleur maintient le serveur dans la file d'attente inactive avant qu'il soit favorisé de nouveau à la liste active de serveur.
   - De la liste disponible de serveurs ajoutez-les aux serveurs assignés colonne.
3. **Globalement dot1x d'enable**

- Naviguez vers la **configuration > l'AAA > la méthode le répertorie > général** et active le **contrôle authentique de système de dot1x**

4. **Configurez les listes de méthode**

- Naviguez vers la **configuration** > l'**AAA** > la **méthode le répertorie > authentification** et crée une nouvelle liste de méthode. Dans ce cas c'est dot1x et groupe ISE_Group (groupe de type créé dans l'étape précédente). Alors le hit **s'appliquent**

- Faites la même chose pour la comptabilité (la **configuration > l'AAA > la méthode la répertorie > comptabilité**) et l'autorisation (la **configuration > l'AAA > la méthode la répertorie > autorisation**). Ils devraient ressembler à ceci

5. **Créez la méthode de filtre d'adresses MAC d'autorisation**.

Ceci s'appelle des configurations SSID plus tard.

- Naviguez vers l'**AAA > la méthode de Configuration> le répertorie > autorisation** et clique sur New.
- Écrivez le **nom de liste de méthode**. A choisi le **groupe de type = de type de réseau** et de **groupe**.
- Ajoutez ISE_Group aux groupes de serveurs assignés champ.

Configuration SSID

1. **Créez l'invité SSID**

- Naviguez vers la **configuration > la radio > les WLAN** et cliquez sur New
- Écrivez l'ID de WLAN, le SSID et le nom de profil et cliquez sur Apply.
- Une fois dans les configurations SSID sous l'interface/groupe d'interface sélectionnez l'interface de la couche 3 de l'invité VLAN.

- Sous la **Sécurité** > la **couche 2** choisies **aucun** et à côté du **filtrage de MAC** n'écrit le nom de liste de méthode de filtre de MAC que vous avez précédemment configuré (MacFilterMethod).
- Sous l'onglet de **Sécurité** > de **serveur d'AAA** sélectionnez les listes appropriées d'authentification et d'accountings method (ISE_Method).

- Sous l'**Allow AAA Override d'**enable d'**onglet Avancé** et l'**état NAC.** Le reste des configurations devrait être ajusté selon les conditions requises de chaque déploiement (délai d'attente de session, exclusion de client, soutien des Aironet Extension, etc.).

- Naviguez vers l'onglet Général placent l'état à activer. Alors le hit **s'appliquent.**

Réorientez la configuration d'ACL

Cet ACL est mis en référence par ISE plus tard dans l'Access-recevoir en réponse à la demande initiale de MAB. Le NGWC l'emploie pour déterminer quel trafic à réorienter et quel trafic devrait

être permis.

- Naviguez vers la **configuration > la Sécurité > l'ACL > les listes de contrôle d'accès** et cliquez sur Add **nouveau**.
- Sélectionnez étendu et écrivez le nom d'ACL.
- Cette image affiche qu'un exemple d'un typique réorientent l'ACL :

  Remarque: La ligne 10 est facultative. Ceci est habituellement ajouté pour dépanner propose. Cet ACL devrait permettre l'accès au DHCP, des services DNS et également aux as du TCP 8443(Deny de port de serveurs ISE). Le trafic de HTTP et HTTPS obtient réorienté (des as d'autorisation).

Configuration de l'interface de ligne de commande (CLI)

Toute la configuration discutée dans les étapes précédentes peut également être appliquée par le CLI.

802.1x globalement activé

```
dot1x system-auth-control
```

Configuration globale d'AAA

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

Configuration de Wlan

```
 wlan Guest 1 Guest
 aaa-override
```

```
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

Réorientez l'exemple d'ACL

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

Support de HTTP et HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

Remarque: Si vous appliquez un ACL pour limiter l'accès au WLC au-dessus du HTTP, il affecte la redirection.

Configurez ISE

Cette section décrit la configuration exigée sur ISE pour prendre en charge les tous les cas d'utilisations discutés dans ce document.

Tâches communes de configuration ISE

1. Ouvrez une session à ISE et naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau** et cliquez sur Add
2. Écrivez le **nom** associé au WLC et à l'**adresse IP de** périphérique.
3. Cochez la case de **configurations d'authentification de rayon** et tapez le **secret partagé** configuré du côté WLC. Cliquez sur Submit alors.

4. Naviguez vers la **stratégie > l'authentification** et sous le **MAB** cliquez sur Edit et assurez cela sous l'**utilisation : Des points finaux internes l'**option si l'**utilisateur n'est pas trouvé** est placés **pour continuer** (elle devrait être là par défaut).

Cas d'utilisation 1 : CWA avec l'authentification d'invité dans chaque connexion utilisateur

Aperçu d'écoulement

1. L'utilisateur de sans fil se connecte à l'invité SSID.
2. WLC authentifie le point final basé sur son adresse MAC utilisant ISE comme serveur d'AAA.
3. Les retours ISE de retour et Access-reçoivent avec deux paires de valeurs d'attribut (AVPs) : URL-réorientez et URL-réorienter-acl. Une fois que le WLC s'applique cet AVPs à la session de point final, les transitions de station à DHCP-exiger et une fois qu'il saisit une adresse IP il reste dans CENTRAL_WEB_AUTH. À cette étape le WLC est prêt à commencer réorienter le HTTP du client/trafic de https.
4. L'utilisateur final ouvrent le navigateur Web et une fois que le trafic de HTTP ou HTTPS est généré, le WLC réoriente l'utilisateur au portail d'invité ISE.
5. Une fois que l'utilisateur arrive au portail d'invité il incite à entrer dans des qualifications d'invité (sponsor-créées dans ce cas).
6. Sur la validation de qualifications ISE affiche la page AUP et une fois que le client reçoit, un type dynamique Re-authenticate CoA est envoyé au WLC.
7. Le WLC retraite l'authentification de filtrage MAC sans émettre un De-authentifier au poste mobile. Ceci devrait être sans couture au point final.
8. Une fois que l'événement de ré-authentification se produit ISE réévalue des stratégies d'autorisation et cette fois le point final est donné un accès d'autorisation puisqu'il y avait un événement réussi précédent d'authentification d'invité.

Ce processus se répète chaque fois que l'utilisateur se connecte au SSID.

Configuration

1. Naviguez vers ISE et naviguez vers des **centres de travail > l'accès invité > configurent > des portails d'invité >** sélectionnent le **portail commandité d'invité** (ou créez un nouvel Commanditer-invité portail de type).
2. Sous l'**enregistrement de périphérique d'invité les** configurations décochent toutes les options et cliquent sur la **sauvegarde**.

3. Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation**. Cliquez sur **Add**.

4. Ce profil est abaissé au WLC le Réorienter-**URL** et le Réorienter-URL-**ACL** en réponse à la demande initiale de contournement d'authentification de MAC (MAB).

- Une fois le **Web centralisé** choisi vérifié de la **redirection de Web (CWA, MDM, NSP, CPP) authentique**, alors introduisent le nom d'ACL de réorientation sous le champ d'**ACL** et sous la **valeur** sélectionnent l'**invité commandité Portal(default)** (ou tout autre portail spécifique créé dans les étapes précédentes).

Le profil devrait regarder semblable celui dans cette image. Cliquez sur alors la **sauvegarde**.

Attribuez les détails au bas de page la valeur d'attribut Pairs(AVPs) comme ils sont soient poussés au WLC

5. Naviguez vers la **stratégie > l'autorisation** et insérez une nouvelle règle. Cette règle est celle qui

déclenche le procédé de réorientation en réponse à la demande initiale d'authentification MAC de WLC. (Dans ce cas appelé **Wireless_Guest_Redirect**).

6. Dans des **conditions** choisissez l'**état existant choisi de la bibliothèque**, puis dans la **condition composée** choisie de **nom d'état**. Sélectionnez un état composé prédéfini appelé **Wireless_MAB**.

> Remarque: Cette condition se compose de 2 attributs RADIUS prévus sous la forme lancée par demande d'Access le WLC (IEEE 802.11 de NAS-Port-Type= <present dans tous les requests> et type de service = appel Sans fil Check< qui se rapporte à une demande spécifique d'un bypass> d'authentification de MAC)

7. Sous des résultats, **norme** choisie > **CWA_Redirect** (profil d'autorisation créé dans l'étape précédente). Cliquez sur alors **fait** et **sauvegarde**

8. Naviguez vers la fin de la règle de **CWA_Redirect** et cliquez sur la flèche à côté de **éditent**. Sélectionnez alors le **doublon ci-dessus**.

9. Modifiez le nom car c'est la stratégie cette les correspondances de point final une fois que la session est authentifiée à nouveau sur le CoA d'ISE (dans ce cas Wireless_Guest_Access).

10. À côté du clic d'état composé de **Wireless_MAB + le** symbole pour développer les conditions et vers la fin de l'état de **Wireless_MAB** cliquent sur Add l'**attribut/valeur**.

11. Sous « l'attribut choisi » a choisi l'**accès au réseau > l'écoulement d'invité d'égaux d'UseCase**

12. Sous des **autorisations** sélectionnez **PermitAccess**. Cliquez sur alors **fait** et **sauvegarde**

Les deux stratégies devraient sembler semblables à ceci :

Cas d'utilisation 2 : CWA avec l'enregistrement de périphérique imposant l'authentification d'invité une fois par jour.

Aperçu d'écoulement

1. L'utilisateur de sans fil se connecte à l'invité SSID.
2. WLC authentifie le point final basé sur son adresse MAC utilisant ISE comme serveur d'AAA.
3. Les retours ISE de retour et Access-reçoivent avec deux paires de valeurs d'attribut (AVPs) (URL-réorientez et URL-réorienter-acl).
4. Une fois que le WLC s'applique cet AVPs à la session de point final, les transitions de station à DHCP-exiger et une fois qu'il saisit une adresse IP il reste dans CENTRAL_WEB_AUTH. À cette étape le WLC est prêt à commencer réorienter le HTTP du client/trafic de https.
5. L'utilisateur final ouvrent le navigateur Web et une fois que le trafic de HTTP ou HTTPS est généré, le WLC réoriente l'utilisateur au portail d'invité ISE.
6. Une fois que l'utilisateur arrive au portail d'invité, il obtient incité à entrer dans les qualifications sponsor-créées.
7. Sur la validation de qualifications ISE ajoute ce point final à un groupe (préconfiguré) spécifique d'identité de point final (enregistrement de périphérique).
8. La page AUP est affichée et une fois que le client reçoit, un type dynamique CoA authentifient à nouveau. Est envoyé au WLC.
9. Le WLC pour retraiter l'authentification de filtrage MAC sans émettre un De-authentifier au

poste mobile. Ceci devrait être sans couture au point final.

10. Une fois que l'événement re d'authentification se produit ISE réévalue des stratégies d'autorisation. Cette fois puisque le point final est membre du bon groupe ISE d'identité de point final renvoie un accès reçoivent sans des restrictions.
11. Puisque le point final a été enregistré dans l'étape 6, chaque fois que cela l'utilisateur revient, on lui permet sur le réseau jusqu'à ce qu'il soit retiré manuellement d'ISE, ou une stratégie de purge de point final exécute vider les points finaux répondant aux critères.

Dans ce scénario de laboratoire, l'authentification est imposée une fois par jour. Le déclencheur de ré-authentification est une stratégie de purge de point final qui retire tous les points finaux de l'identité utilisée de point final groupent chaque jour.

> Remarque: Il est possible d'imposer l'événement d'authentification d'invité basé sur le temps écoulé depuis la dernière acceptation AUP. Ceci peut être une option si vous devez imposer la connexion d'invité plus souvent qui une fois par jour (dans l'exemple toutes les 4 heures).

Configuration

1. Sur ISE naviguez vers des **centres > l'accès invité de travail > configurent > des portails d'invité >** sélectionnent le **portail commandité d'invité** (ou créez un nouvel Commanditer-invité portail de type).
2. Sous l'**enregistrement de périphérique d'invité les** configurations vérifient que l'option **enregistrent automatiquement l'invité que des périphériques** est vérifiés. Cliquez sur **Save**.

3. Naviguez vers le **centre > l'accès invité de travail > configurent > des types d'invité** ou cliquent sur juste en fonction le raccourci spécifié sous des configurations d'enregistrement de périphérique d'invité dans le portail.

4. Quand l'utilisateur de sponsor crée un compte d'invité, il lui assigne un type d'invité. Chaque type individuel d'invité peut avoir un point final enregistré qui appartient à une identité différente Group.To de point final affectent le groupe d'identité de point final que le périphérique devrait être ajouté à, sélectionnent le type d'invité les utilisations de sponsor pour ces utilisateurs d'invité (ce cas d'utilisation est basé sur l'hebdomadaire (par défaut)).

5. Une fois dans le type d'invité, sous des **options de procédure de connexion** sélectionnez le groupe de point final du **groupe d'identité de point final de** menu de baisse vers le bas **pour l'enregistrement de périphérique d'invité**

6. Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation**. Cliquez sur **Add**.

7. Ce profil est abaissé au WLC le Réorienter-**URL** et le Réorienter-URL-**ACL** en réponse à la demande initiale de contournement d'authentification de MAC (MAB).

- Une fois le **Web centralisé** choisi vérifié de la **redirection de Web (CWA, MDM, NSP, CPP) authentique**, alors introduisent le nom d'ACL de réorientation sous le champ d'**ACL** et sous la **valeur** sélectionnent le portail créé pour cet écoulement (**CWA_DeviceRegistration**).

8. Naviguez vers la **stratégie > l'autorisation** et insérez une nouvelle règle. Cette règle est celle qui déclenche le procédé de réorientation en réponse à la demande initiale d'authentification MAC de WLC. (Dans ce cas appelé **Wireless_Guest_Redirect**).

9. Dans des **conditions** a choisi l'**état existant choisi de la bibliothèque**, puis dans la **condition**

composée choisie de nom d'état. Sélectionnez un état composé prédéfini appelé Wireless_MAB.

10. Sous des résultats, norme choisie > CWA_DeviceRegistration (profil d'autorisation créé dans l'étape précédente). Cliquez sur alors fait et sauvegarde

11. Reproduisez la stratégie ci-dessus, modifiez son nom car c'est la stratégie que le point final frappe après qu'il retourne de l'événement de ré-authentification (appelé Wireless_Guest_Access).

12. Sous le groupe d'identité les détails enferment dans une boîte, groupe choisi d'identité de point final et sélectionnent le groupe que vous avez mis en référence sous l'invité Type(GuestEndpoints).

13. Sous des résultats sélectionnez PermitAccess. Cliquez sur fait et sauvegardez les modifications.

14. Créez et le stratégie de purge de point final qui efface le groupe de GuestEndpoint quotidien.

- Naviguez vers la gestion > la Gestion de l'identité > les configurations > la purge de point final
- Selon des règles de purge il devrait y avoir d'une par défaut cette suppression de GuestEndpoints de déclencheurs si le temps écoulé est plus grand que 30 jours.
- Modifiez la stratégie existante pour GuestEndpoints ou créez un neuf (au cas où le par défaut serait enlevé). Notez que les stratégies de purge exécutent chaque jour un temps défini.

Dans ce cas la condition est des membres de GuestEndpoints avec des jours écoulés moins de pendant 1 jour

Cas d'utilisation 3 : Portail de HostSpot

Aperçu d'écoulement

1. L'utilisateur de sans fil se connecte à l'invité SSID.
2. WLC authentifie le point final basé sur son adresse MAC utilisant ISE comme serveur d'AAA.
3. ISE renvoie de retour un Access-recevoir avec deux paires de valeurs d'attribut (AVPs) : URL-réorientez et URL-réorienter-acl.
4. Une fois que le WLC s'applique cet AVPs à la session de point final, les transitions de station à DHCP-exiger et une fois qu'il saisit une adresse IP il reste dans CENTRAL_WEB_AUTH. À cette étape le WLC est prêt à réorienter le HTTP du client/trafic de https.
5. L'utilisateur final ouvrent le navigateur Web et une fois que le trafic de HTTP ou HTTPS est généré, le WLC réoriente l'utilisateur au portail de point névralgique ISE.
6. Une fois dans le portail l'utilisateur est incité à recevoir une Politique d'Utilisation Acceptable.
7. ISE ajoute l'adresse MAC de point final (ID de point final) dans le groupe d'identité de point d'extrémité configuré.
8. La stratégie entretient le noeud (le RPC) ce des processus que la demande fournit une Admin-remise dynamique de type CoA au WLC.
9. Une fois que le WLC finit de traiter le CoA entrant, il fournit un De-authentifier au client (la connexion est perte pendant le temps où elle prend pour que le client revienne).
10. Une fois que le client rebranche, une nouvelle session est créée tellement là n'est aucune continuité de session de côté ISE. Il signifie que l'authentification est traitée comme nouveau thread.
11. Puisque le point final est ajouté au groupe d'identité de point d'extrémité configuré, et il y a

une stratégie d'autorisation qui vérifie si le point final fait partie de ce groupe, la nouvelle authentification apparie cette stratégie. Le résultat est accès complet au réseau d'invité.

12. L'utilisateur ne devrait pas devoir recevoir l'AUP de nouveau à moins que l'objet d'identité de point final soit purgé de la base de données ISE en raison d'une stratégie de purge de point final.

Configuration

1. Créez un nouveau groupe d'identité de point final pour déplacer ces périphériques à lors de l'enregistrement. Naviguez vers des **centres > l'accès invité > l'identité de travail groupe > des groupes d'identité de point final** et clique sur .

- Écrivez un nom de groupe (dans ce cas HotSpot_Endpoints). Ajoutez une description et aucun groupe parent n'est nécessaire.

2. Naviguez vers des **centres > l'accès invité de travail > configurent > des portails d'invité > portail** choisi de **point névralgique (par défaut**).

3. Développez les configurations portailes et sous le groupe choisi de **HostSpot_Endpoints de** groupe d'identité de point final sous le **groupe d'identité de point final.** Ceci envoie les périphériques enregistrés au groupe spécifié.

4. **Sauvegardez les** modifications.

5. Créez le profil d'autorisation qui fait appel le portail de point névralgique à l'authentification de MAB lancée par le WLC.

- Naviguez vers des **éléments de stratégie > de stratégie > des résultats > l'autorisation > des profils d'autorisation** et créez un (HotSpotRedirect).
- Une fois la **redirection de Web (CWA, MDM, NSP, CPP)** est **hotspot** choisi vérifié, puis introduit le nom d'ACL de réorientation dans le domaine d'ACL (Guest_Redirect) et comme un portail correct choisi de valeur (**portail de point névralgique (par défaut)**).

6. Créez la stratégie d'autorisation qui déclenche le résultat de HotSpotRedirect sur requête initiale de MAB de WLC.

- Naviguez vers la **stratégie > l'autorisation** et insérez une nouvelle règle. Cette règle est celle qui déclenche le procédé de réorientation en réponse à la demande initiale d'authentification MAC de WLC. (Dans ce cas appelé **Wireless_HotSpot_Redirect**).
- Dans des **conditions** choisissez l'**état existant choisi de la bibliothèque**, puis dans la **condition composée** choisie de **nom d'état**
- Sous des résultats, **norme** choisie > **HotSpotRedirect** (profil d'autorisation créé dans l'étape précédente). Cliquez sur alors **fait** et **sauvegarde**

7. Créez la deuxième stratégie d'autorisation.

- Reproduisez la stratégie ci-dessus, modifiez son nom car c'est la stratégie que le point final frappe après qu'il retourne de l'événement de ré-authentification (appelé Wireless_HotSpot_Access).
- Sous le **groupe d'identité les détails** enferment dans une boîte, **groupe** choisi d'**identité de point final** et puis le groupe que vous avez créé plus tôt (**HotSpot_Endpoints**).

- Sous des résultats sélectionnez **PermitAccess**. Cliquez sur **fait** et **sauvegardez les** modifications.

8. Configurez la stratégie de purge qui efface des points finaux avec jours plus splendides d'un temps écoulé des que 5.

- Naviguez vers la **gestion > la Gestion de l'identité > les configurations > la purge de point final** et sous la purge les règles créent un neuf.
- Sous le **groupe** choisi **> le HotSpot_Endpoints d'identité de point final de** case de **petits groupes de groupe d'identité**
- Sous le clic de **conditions créez le nouvel état (option avancée**).
- Sous l'attribut choisi choisissez *ENDPOINTPURGE : ElapsedDays GREATERTHAN* 5 jours

Vérifiez

Cas d'utilisation 1

1. L'utilisateur se connecte à l'invité SSID.
2. Il ouvre le navigateur et dès que le trafic http sera généré, le portail d'invité est affiché.
3. Une fois que l'utilisateur d'invité authentifie et reçoit l'AUP, une page de succès est affichée.
4. Un CoA d'authentifier à nouveau est envoyé (transparent au client).
5. La session de point final est authentifiée à nouveau avec l'accès complet au réseau.
6. N'importe quelle connexion ultérieure d'invité doit passer l'authentification d'invité avant d'accéder au réseau.

Écoulement des logs vivants de RAYON ISE :

Cas d'utilisation 2

1. L'utilisateur se connecte à l'invité SSID.
2. Il ouvre le navigateur et dès que le trafic http sera généré, le portail d'invité est affiché.
3. Une fois que l'utilisateur d'invité authentifie et reçoit l'AUP, le périphérique est enregistré.
4. Une page de succès est affichée et un CoA d'authentifier à nouveau est envoyé (transparent au client).
5. La session de point final est authentifiée à nouveau avec l'accès complet au réseau.
6. N'importe quelle connexion ultérieure 9s de rafale a autorisé sans imposer l'authentification d'invité tant que le point final est toujours dans le groupe d'identité de point d'extrémité configuré.

Écoulement des logs vivants de RAYON ISE :

Cas d'utilisation 3

1. L'utilisateur se connecte à l'invité SSID.
2. Il ouvre le navigateur et dès que le trafic http sera généré, une page AUP est affichée.
3. Une fois que l'utilisateur d'invité reçoit l'AUP, le périphérique est enregistré.
4. Une page de succès est affichée et un CoA d'Admin-remise est envoyé (transparent au client).
5. Le point final rebranche avec l'accès complet au réseau.
6. On permet n'importe quelle connexion ultérieure de rafale sans imposer l'acceptation AUP (à

moins qu'autrement est configuré) pour tant que le point final demeure dans le groupe d'identité de point d'extrémité configuré.

Commutation locale de FlexConnect dans AireOS

Quand la commutation locale de FlexConnect est configurée l'admin de réseau doit assurer cela :

- Réorientez l'ACL est configuré comme ACL de FlexConnect.
- Réorientez l'ACL a été appliqué comme stratégie l'un ou l'autre de voie par AP elle-même sous l'onglet de **FlexConnect > WebAuthentication externe ACLs > stratégies** > choisi réorientent l'ACL et cliquent sur Apply

Ou en ajoutant l'ACL de stratégie à FlexConnect le groupe appartient à (la **radio > les groupes de FlexConnect >** sélectionnent le groupe correct > l'**ACL traçant > des stratégies** sélectionnent l'ACL de réorientation et cliquent sur Add)

L'ajout d'ACL de stratégie déclenche le WLC pour abaisser l'ACL configuré aux membres AP du groupe de FlexConnect. Le manque de faire ceci a comme conséquence un Web réorientent la question.

Scénario d'Étranger-ancre

Dans l'auto-ancrage (étranger – Des scénarios d'ancre) il est important de mettre en valeur les faits suivants :

- Réorientez les besoins d'ACL d'être défini sur l'étranger et l'ancre WLC. Même lorsqu'il est seulement imposé sur l'ancre.
- L'authentification de la couche 2 est toujours manipulée par le WLC étranger. C'est essentiel pendant les phases de conception (aussi pour le dépannage) comme toute l'authentification de RAYON et le trafic de comptabilité se produit entre ISE et le WLC étranger.

- Une fois la réorientation AVPs sont appliquées à la session de client que le WLC étranger met à jour la session de client dans l'ancre par un message de transfert de mobilité.
- En ce moment les débuts de l'ancre WLC pour imposer la réorientation utilisant le Réorienter-ACL qui a été préconfigurée.
- La comptabilité devrait être complètement arrêtée sur l'ancre WLC SSID pour éviter les mises à jour de comptabilité allant vers ISE (mettant en référence le même événement d'authentification) étant livré chacun des deux de l'ancre et étranger.
- Des ACL basée sur URL ne sont pas pris en charge dans des scénarios d'Étranger-ancre.

Dépannez

États cassés communs sur AireOS et Access convergé WLC

1. **Le client ne peut pas joindre l'invité SSID**

Un « **client d'exposition a détaillé xx : xx : xx : xx : xx : xx** » indique que le client est coincé dans le **DÉBUT**. Habituellement c'est un indicateur du WLC ne pouvant pas appliquer un attribut que le serveur d'AAA retourne.

Vérifiez que le nom d'ACL de réorientation a poussé par des correspondances ISE exactement le nom de l'ACL prédéfini sur le WLC.

Le même principe s'applique à n'importe quel autre attribut que vous avez configuré ISE pour abaisser au WLC (IDs de VLAN, noms d'interface, Airespace-ACLs, etc.). Le client devrait alors transition au DHCP et puis au CENTRAL_WEB_AUTH.

2. **Réorientez AVPs sont appliqués à la session de client mais réorientent ne fonctionne pas**

Vérifiez que l'état de gestionnaire de la stratégie du client est CENTRAL_WEB_AUTH avec une adresse IP valide selon l'interface dynamique configurée pour le SSID et également que l'ACL de réorientation et URL-réorientez les attributs sont appliqués à la session de client.

Réorientez l'ACL

Dans AIreOS WLCs l'ACL de réorientation devrait explicitement permettre le trafic qui ne devrait pas être réorienté, comme des DN et ISE sur le port TCP 8443 dans les deux directions et l'implicite refusent à IP tous les n'importe quels déclencheurs le reste du trafic à réorienter.

Dans l'accès convergé la logique est l'opposé. Refusez les as que les contournements réorientent tandis que l'autorisation ACEs des déclencheurs la réorientation. C'est pourquoi il est recommandé pour permettre explicitement le port TCP 80 et 443.

Vérifiez l'accès à ISE au-dessus du port 8443 du VLAN invité. Si tout semble bon du point de vue de configuration le moyen le plus simple d'avancer est de saisir une capture derrière l'adaptateur Sans fil du client et de vérifier où la réorientation se casse.

- Le resoultion de DN se produit-il ?
- La prise de contact de manière du TCP 3 est-elle terminée contre la page demandée ?
- Le WLC renvoie-t-il une action de réorientation après que le client initie l'OBTENIR ?
- La prise de contact de manière du TCP 3 contre ISE plus de 8443 est-elle terminée ?

3. **Le client ne peut pas accéder au réseau après ISE a poussé une modification VLAN à la fin de l'écoulement d'invité**

Une fois que le client saisissait une adresse IP au début de l'écoulement (réorientez pré l'état), si une modification VLAN est abaissée après que l'authentification d'invité se produise (CoA de courrier authentifiez à nouveau), la seule manière de forcer une release DHCP/renouvellent dans l'invité que l'écoulement (sans agent intermédiaire) est par un Java applet qui dans des périphériques mobiles ne fonctionnent pas.

Ceci laisse le client noir-troué dans VLAN X avec une adresse IP de VLAN Y. Ceci devrait être considéré tout en prévoyant la solution.

4. **ISE affiche la « erreur interne du HTTP 500, message non trouvé de session de rayon » dans l'invité le navigateur que de client pendant réorientent**

C'est habituellement un indicateur de la perte de session sur ISE (la session a été terminée). La raison la plus commune pour ceci rend compte a configuré sur l'ancre WLC quand l'Étranger-ancre a été déployée. Pour réparer cette comptabilité de débronchement sur l'ancre et laisser l'authentification et la comptabilité étrangères de traitement.

5. **Les débranchements de client et demeure déconnecté ou se connecte à un SSID différent après avoir reçu l'AUP dans le portail du point névralgique d'ISE**.

Ceci peut être prévu dans le point névralgique dû à la modification dynamique de l'autorisation (CoA) impliquée dans cet écoulement (admin CoA remis à l'état initial) ce des causes le WLC pour fournir un deauth à la station Sans fil. La majorité de points finaux Sans fil n'ont aucune question à revenir au SSID après que le De-authentifier se produise, mais dans certains cas le client se connecte à un autre SSID préféré en réponse à l'événement De-authenitcate. Rien ne peut être fait d'ISE ou de WLC pour empêcher ceci pendant qu'il incombe au client sans fil à coller à l'original SSID, ou pour se connecter à un autre SSID (préféré) disponible.

Dans ce cas l'utilisateur de sans fil devrait manuellement se connecter de nouveau au point névralgique SSID.

AireOS WLC

(Cisco Controller) >debug client <MAC addr>
Les positionnements de client de debug POUR DÉBUGGER un ensemble de composants impliqués dans l'ordinateur d'état de client change.

(Cisco Controller) >debug client <MAC addr>
Composants de debug aaa

(Cisco Controller) >debug client <MAC addr>
Ceci peut être des ressources en incidence selon la quantité d'utilisateurs qui se connectent par le MAB ou le dot1x SSID. Ces composants dans le niveau de DEBUG enregistrent des transactions d'AAA entre WLC et ISE et impriment les paquets RADIUS sur l'écran.

C'est essentiel si vous qu'ISE puisse ne pas fournir les attributs prévus, ou si le WLC ne les traite pas correctement.

Le Web-Auth réorientent

(Cisco Controller) >debug client <MAC addr>
Ceci peut être utilisé pour vérifier que le WLC déclenche avec succès la réorientation. C'est un exemple de la façon dont la réorientation devrait ressembler à met au point :

(Cisco Controller) >debug client <MAC addr>

NGWC

Les positionnements de client de debug POUR DÉBUGGER un ensemble de composants impliqués dans l'ordinateur d'état de client change.

(Cisco Controller) >debug client <MAC addr>
Ce composant imprime les paquets RADIUS (authentification et comptabilité) sur l'écran. C'est pratique quand vous devez vérifier qu'ISE livre l'AVPs droit et vérifier également que le CoA est envoyé et traité correctement.

(Cisco Controller) >debug client <MAC addr>
Ceci tout des transitions d'AAA (authentification, autorisation et comptabilité) où les clients sans fil sont impliqués. Il est essentiel vérifier ce que WLC analyse correctement l'AVPs et les applique à la session de client.

(Cisco Controller) >debug client <MAC addr>
Ceci peut activé quand vous suspectez une question de réorientation sur le NGWC.

```
(Cisco Controller) >debug client <MAC addr>
```

ISE

Logs vivants de RAYON

Vérifiez la demande initiale de MAB a été traité correctement dans ISE et cet ISE refoule les attributs prévus. Naviguez vers les **exécutions > le RAYON > vivent des logs** et filtrent la sortie utilisant le MAC de client sous l'**ID de point final**. Une fois que l'événement d'authentification est trouvé, cliquez sur en fonction les détails et vérifiez alors les résultats poussés en tant qu'élément du recevoir.

TCPDump

Cette caractéristique peut être utilisée quand une examination plus profonde l'échange de paquet RADIUS entre ISE et le WLC est nécessaire. De cette façon vous pouvez montrer qu'ISE envoie les attributs corrects dans l'Access-recevoir sans devoir activer met au point du côté WLC. Pour commencer une capture utilisant TCDDump pour naviguer vers des **exécutions > dépannez > les outils >General > le TCPDump d'outils de diagnostic.**

C'est un exemple d'un écoulement correct capturé par TCPDump

Voici l'AVPs envoyé en réponse à la demande initiale de MAB (deuxième paquet dans le tir d'écran ci-dessus).

```
(Cisco Controller) >debug client <MAC addr>
```

Debugs de point final :

Si vous devez plonger plus profond dans les processus ISE qui comportent des décisions politiques, la sélection portaile, l'authentification d'invité, le CoA manipulant, etc. le moyen le plus simple d'approcher ceci est d'activer des **debugs d'Endpoit** au lieu de devoir placer les composants complets pour mettre au point de niveau.

Pour activer ceci, naviguez vers des **exécutions > le dépannage > le DiagnosticTools > les outils généraux** > le **debug de point final.**

Une fois dans le point final mettez au point la page, écrivez l'adresse MAC de point final et cliquez sur le début si prêt à recréer la question.

Une fois le débogage a été arrêté pour cliquer sur en fonction le lien qui identifie l'ID de point final pour télécharger la sortie de débogage.

Informations connexes

Constructions d'AireOS recommandées par TAC

Guide de configuration Sans fil de contrôleur de Cisco, version 8.0.

Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.1

Configuration Sans fil universelle NGWC avec le Cisco Identity Services Engine