ISE avec la charge statique réorientent pour l'exemple d'isolement de configuration réseau d'invité

Contenu

Introduction

Ce document décrit comment configurer le Logiciel Cisco Identity Services Engine (ISE) avec la charge statique réorientent pour les réseaux d'isolement d'invité afin de mettre à jour la Redondance. Il décrit également comment configurer le noeud de stratégie de sorte que des clients ne soient pas incités avec un avertissement invérifiable de certificat.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification Web centrale de Cisco ISE (CWA) et tous les composants relatifs
- Vérification de navigateur de validité de certificat
- Version 1.2.0.899 ou ultérieures de Cisco ISE
- Version Sans fil 7.2.110.0 du contrôleur LAN de Cisco (WLC) ou plus tard (la version 7.4.100.0 ou plus tard est préférée)

Note: CWA est décrit dans l'[authentification Web centrale](#) article de Cisco d'[exemple sur WLC et ISE configuration](#).

Composants utilisés

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

- Version 1.2.0.899 de Cisco ISE
- Version 7.4.110.0 virtuelle de Cisco WLC (vWLC)
- Version 8.2.5 de l'appliance de sécurité adaptable Cisco (ASA)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Dans beaucoup d'environnements de Bring Your Own Device (BYOD), le réseau d'invité est entièrement isolé dans le réseau interne dans une zone démilitarisée (DMZ). Souvent, le DHCP dans l'invité DMZ offre des serveurs de Name System de domaine public (DN) aux utilisateurs d'invité parce que le seul service qui est offert est accès d'Internet.

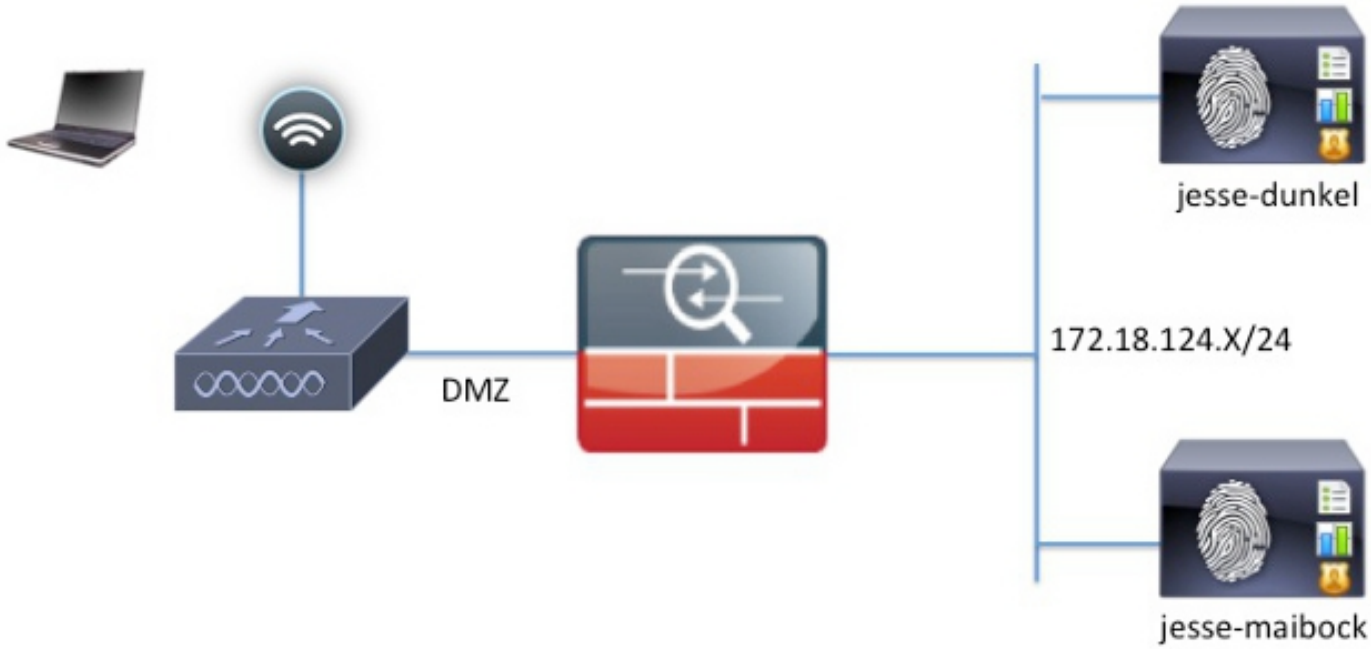
Ceci fait la redirection d'invité sur l'ISE difficile avant la version 1.2 parce que l'ISE réoriente des clients au Fully Qualified Domain Name (FQDN) pour l'authentification Web. Cependant, avec des versions 1.2 et ultérieures ISE, les administrateurs peuvent réorienter des utilisateurs d'invité à un IP address ou à un nom d'hôte statique.

Configurez

Diagramme du réseau

C'est un diagramme logique.

> **Note**: Physiquement, il y a un contrôleur sans-fil dans le réseau interne, les Points d'accès (aps) sont sur le réseau interne, et l'identification d'ensemble de services (SSID) est ancrés au contrôleur DMZ. Référez-vous à la documentation pour le pour en savoir plus de Cisco WLC.



Configuration

La configuration sur le WLC demeure sans changement d'une configuration normale CWA. Le SSID est configuré afin de permettre le filtrage MAC avec l'authentification de RADIUS, et les points de comptabilité de RADIUS vers deux Noeuds ou plus de stratégie ISE.

Ce document se concentre sur la configuration ISE.

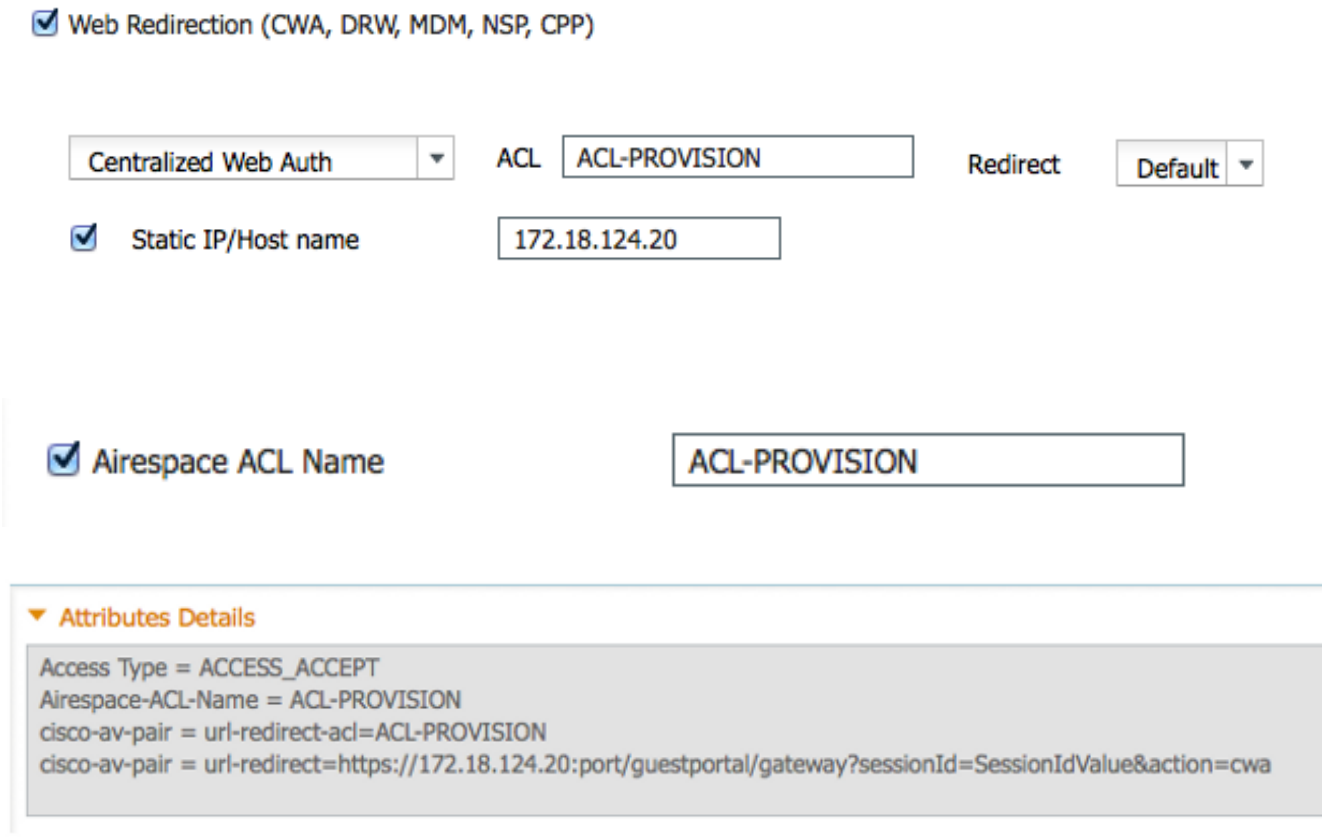
> **Note**: Dans cet exemple de configuration, les Noeuds de stratégie sont **jesse-dunkel** (172.18.124.20) et **jesse-maibock** (172.18.124.21).

Les CWA circulent commencent quand le WLC envoie une demande de dérivation d'authentification MAC de RADIUS (MAB) à l'ISE. L'ISE répond avec un URL de réorientation au contrôleur afin de réorienter le trafic http à l'ISE. Il est important que RADIUS et le trafic http aillent même aux services de stratégie le noeud (le RPC) parce que la session est mise à jour sur un RPC simple. Ceci est normalement exécuté avec une règle simple, et le RPC insère sa propre adresse Internet dans l'URL CWA. Cependant, avec une charge statique réorientez, vous doit créer une règle pour chaque RPC afin de s'assurer que RADIUS et le trafic http sont envoyés au même RPC.

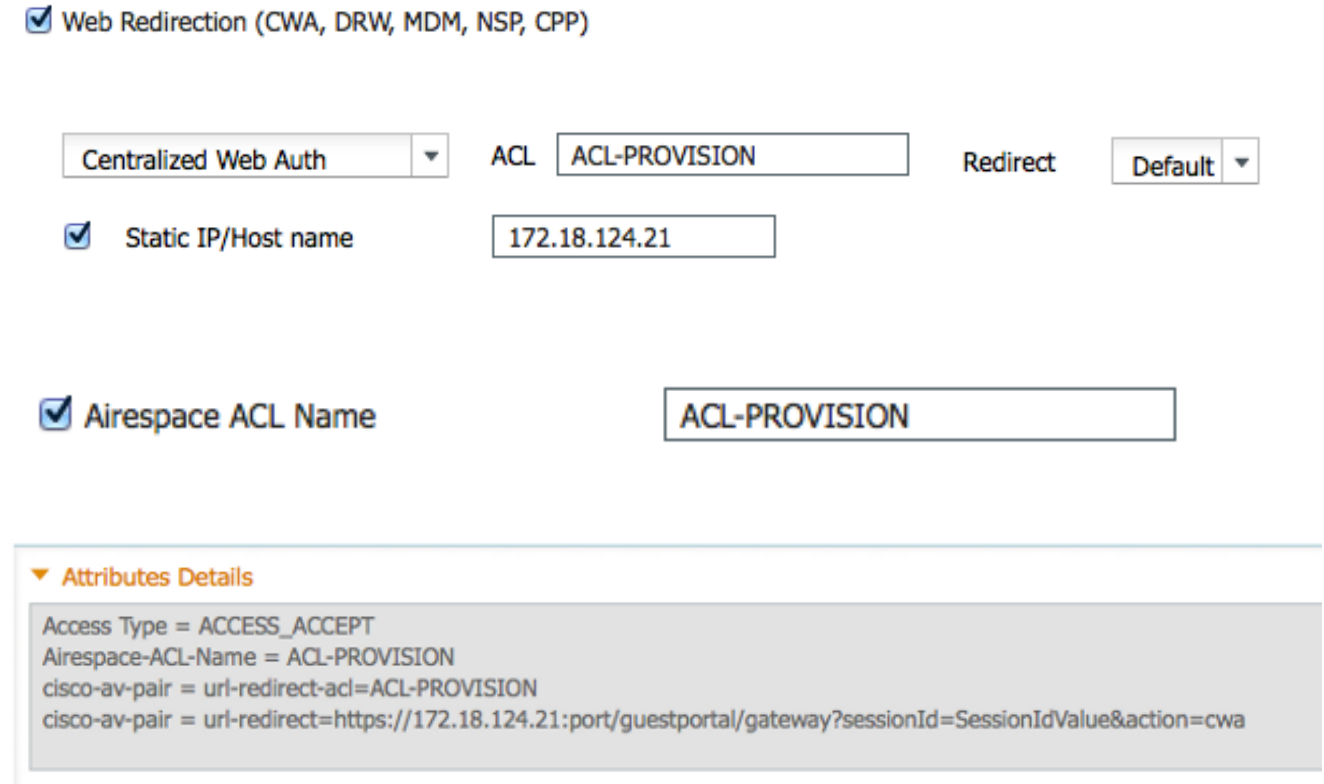
Terminez-vous ces étapes afin de configurer l'ISE :

1. Installez deux règles afin de réorienter le client à l'adresse IP RPC. Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation**.

   Ces images affichent les informations pour le nom de profil **DunkelGuestWireless** :



Ces images affichent les informations pour le nom de profil **MaibockGuestWireless** :



Note: **L'ACL-PROVISION** est une liste de contrôle d'accès locale (ACL) qui est configurée sur le WLC afin de permettre au client pour communiquer avec ISE lors de l'authentification. Référez-vous à l'[authentification Web centrale] pour en savoir plus d'article de Cisco d'[exemple sur WLC et ISE configuration].

2. Configurez l'autorisation maintient l'ordre de sorte qu'ils s'assortissent sur l'**accès au réseau :**

L'attribut de **nom d'hôte ISE** et fournissent le profil approprié d'autorisation :

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then MaibockGuestWireless
✓	Default	if no matches, then DenyAccess	

Maintenant que le client est réorienté à une adresse IP, les utilisateurs reçoivent des avertissements de certificat parce que l'URL n'apparie pas les informations dans le certificat. Par exemple, le FQDN dans le certificat est **jesse-dunkel.rtpaaa.local, mais l'URL est 172.18.124.20**. Hereis un certificat d'**exemple** qui permet au navigateur pour valider le certificat avec l'adresse IP :

Issuer

* Friendly Name	jesse-dunkel.rtpaaa.local,jesse-dunkel.rtpaaa.local,172.18.124.20,172.18.124.20#RTPAAA-
Description	
Subject	CN=jesse-dunkel.rtpaaa.local
Subject Alternative Name (SAN)	DNS Name: jesse-dunkel.rtpaaa.local DNS Name: 172.18.124.20 IP Address: 172.18.124.20
Issuer	DC=local,DC=rtpaaa,CN=RTPAAA-Sub-CA1
Valid From	Thu, 19 Dec 2013 14:00:39 EST
Valid To (Expiration)	Sun, 20 Jul 2014 13:54:58 EDT
Serial Number	37 80 74 E7 00 00 00 00 00 14
Signature Algorithm	SHA1WithRSAEncryption
Key Length	2048

Protocol

- ☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling
- ☑ HTTPS: Use certificate to authenticate the ISE Web Portals

Avec l'utilisation des entrées alternatives soumises du nom (SAN), le navigateur peut valider l'URL qui inclut l'adresse IP **172.18.124.20**. Trois entrées SAN doivent être créées afin d'adresser les diverses incompatibilités de client.

3. Créez une entrée SAN pour le nom DNS et assurez-vous qu'il apparie l'entrée **CN= du** champ Subject.

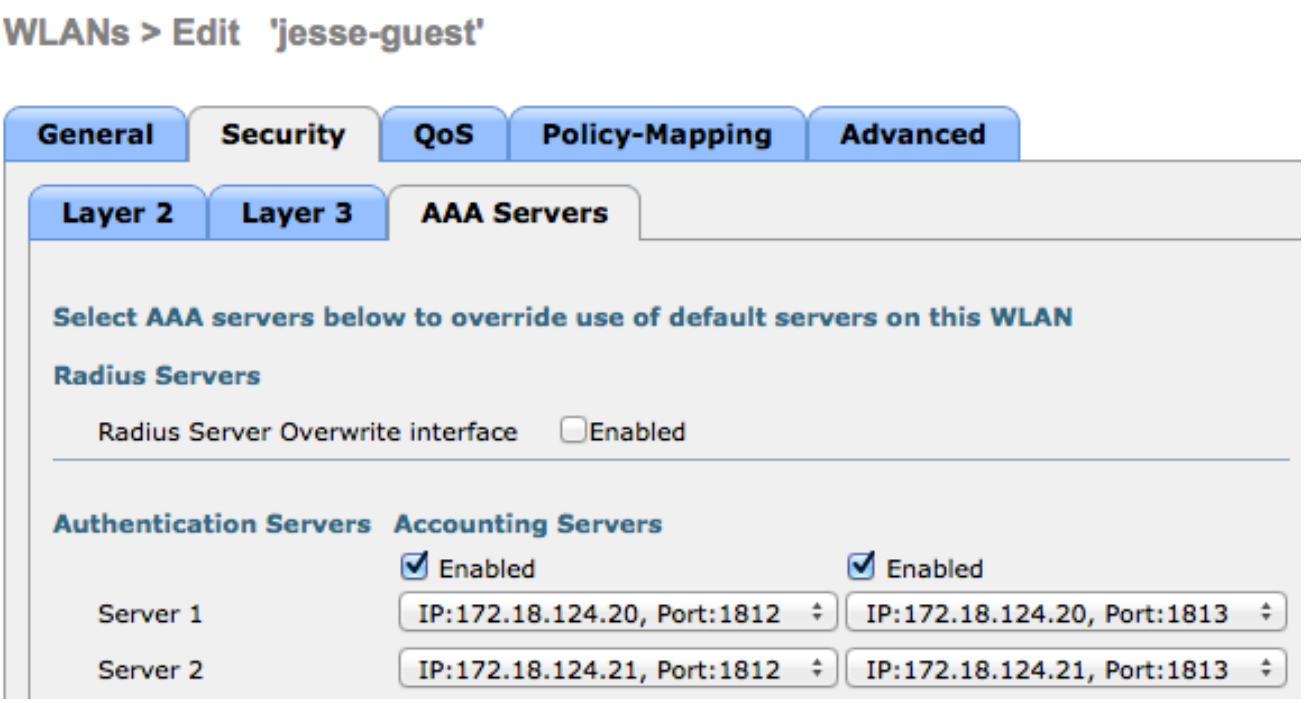
4. Créez deux entrées afin de permettre à des clients pour valider l'adresse IP ; ceux-ci sont pour le nom DNS de l'adresse IP aussi bien que l'adresse IP qui apparaît dans l'attribut d'adresse IP. Quelques clients se réfèrent seulement au nom DNS. D'autres ne reçoivent pas une adresse IP dans l'attribut de nom DNS mais mettent en référence à la place l'attribut d'adresse IP.

Note: Pour plus d'informations sur la génération de certificat, référez-vous au **guide d'installation du matériel de Logiciel Cisco Identity Services Engine, version 1.2**.

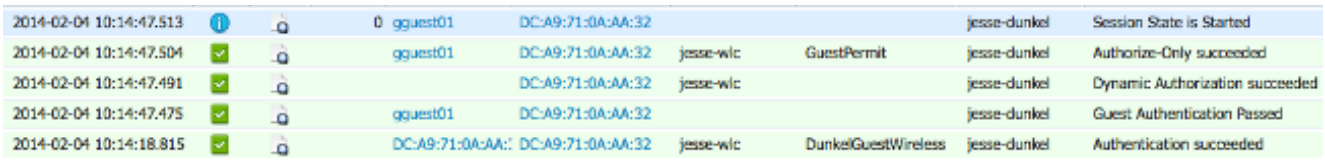
Vérifiez

Terminez-vous ces étapes afin de confirmer que votre configuration fonctionne correctement :

1. Afin de vérifier que chacun des deux règles sont fonctionnelles, placez manuellement la commande des ISE PSNs qui sont configurés sur le WLAN :



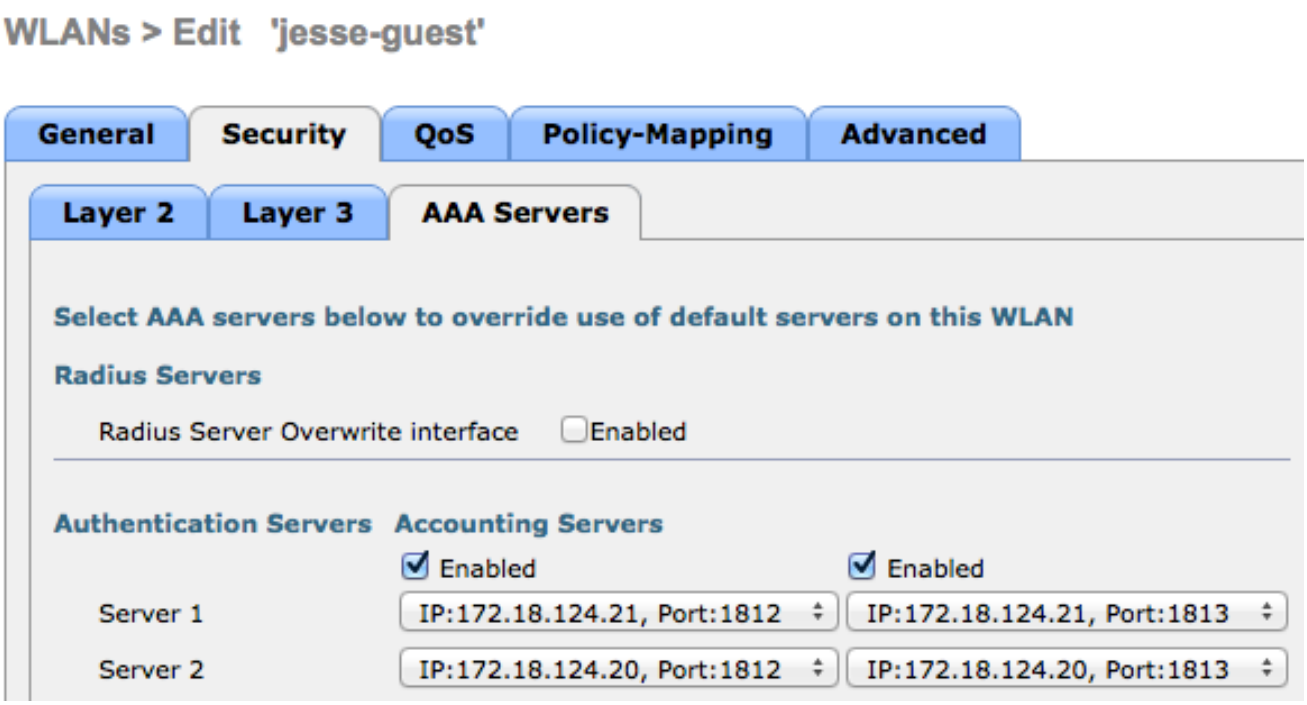
2. Connectez-vous dans l'invité SSID, naviguez vers l'**exécution > les authentifications** dans l'ISE, et vérifiez que les règles correctes d'autorisation sont frappées :



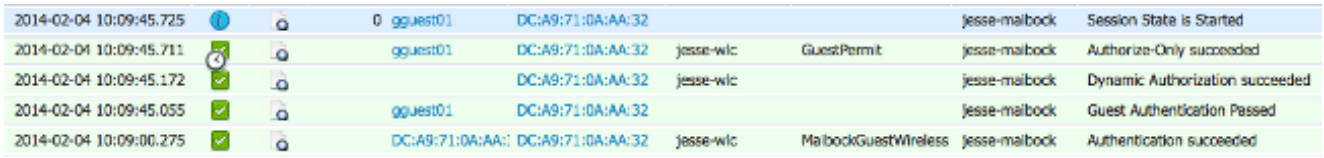
   L'authentification initiale de MAB est donnée au profil d'autorisation de **DunkelGuestWireless**. C'est la règle qui spécifiquement le **jesse-dunkel de** redirect to, qui est le premier noeud ISE. Après les logins de l'utilisateur **gguest01**, l'autorisation finale correcte de **GuestPermit** est donnée.

3. Afin d'effacer les sessions d'authentification du WLC, démontez le périphérique de client du réseau Sans fil, naviguez vers le **Monitor > Clients** sur le WLC, et supprimez la session de la sortie. Le WLC tient la session de veille pendant cinq minutes par défaut, ainsi afin de réaliser un essai valide, vous devez commencer à nouveau.

4. Renversez la commande de l'ISE PSNs sous la configuration de WLAN invité :



5. Connectez-vous dans l'invité SSID, naviguez vers l'**exécution > les authentifications** dans l'ISE, et vérifiez que les règles correctes d'autorisation sont frappées :



Pour la deuxième tentative, le profil d'autorisation de **MaibockGuestWireless** est correctement frappé pour l'authentification initiale de MAB. Semblable au premier essai au **jesse-dunkel** (étape 2), l'authentification au **jesse-maibock** frappe correctement le **GuestPermit** pour l'autorisation finale. Puisqu'il n'y a aucune informations de RPC-particularité dans le profil d'autorisation de **GuestPermit**, une règle simple peut être utilisée pour l'authentification à n'importe quel RPC.

Dépannez

La fenêtre de détails d'authentification est une vue puissante qui affiche chaque étape de l'authentification/du processus d'autorisation. Afin de l'accéder à, naviguez vers des **exécutions > des authentifications** et cliquez sur l'icône de loupe sous la colonne de détails. Employez cette fenêtre afin de vérifier que les conditions de règle d'authentification/autorisation sont configurés correctement.

Dans ce cas, le gisement de policy server est la zone primaire du foyer. Ce champ contient l'adresse Internet du RPC ISE par lequel l'authentification est entretenue :

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

Comparez l'entrée de policy server à l'état de règle et assurez-vous que la correspondance deux (cette valeur distingue les majuscules et minuscules) :

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

Note: Il est important de se souvenir que vous devez démonter du SSID et effacer l'entrée de client du WLC entre les tests.