مثال لإعادة توجيه ساكن إستاتيكي مع ISE لتكوين شبكات الضيوف المعزولين

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين محرك خدمات الهوية من Cisco (ISE) باستخدام إعادة توجيه ثابتة لشبكات الضيوف المعزولين للحفاظ على التكرار. كما يصف كيفية تكوين عقدة النهج بحيث لا يتم مطالبة العملاء بتحذير شهادة لا يمكن التحقق منها.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مصادقة الويب المركزية ل Cisco ISE (CWA) وجميع المكونات ذات الصلة
- التحقق من صلاحية الشهادة من خلال المستعرض
- Cisco ISE الإصدار 1.2.0.899 أو إصدار أحدث
- إصدار وحدة التحكم في شبكة LAN اللاسلكية (WLC) من Cisco 7.2.110.0 أو إصدار أحدث (يفضل الإصدار 7.4.100.0 أو إصدار أحدث)

ملاحظة: يتم وصف CWA في مصادقة الويب المركزية على مثال تكوين WLC و ISE مادة Cisco.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco ISE الإصدار 1.2.0.899
- إصدار Cisco Virtual WLC (vWLC) 7.4.110.0
- أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA)) الإصدار 8.2.5

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

في العديد من بيئات أجهزتك الخاصة (BYOD)، تكون الشبكة المضيفة معزولة بالكامل عن الشبكة الداخلية في منطقة منزوعة السلاح. غالبا ما يوفر بروتوكول DHCP الموجود في DMZ الضيف خوادم نظام اسم المجال العام (DNS) للمستخدمين الضيوف لأن الخدمة الوحيدة التي يتم تقديمها هي الوصول إلى الإنترنت.

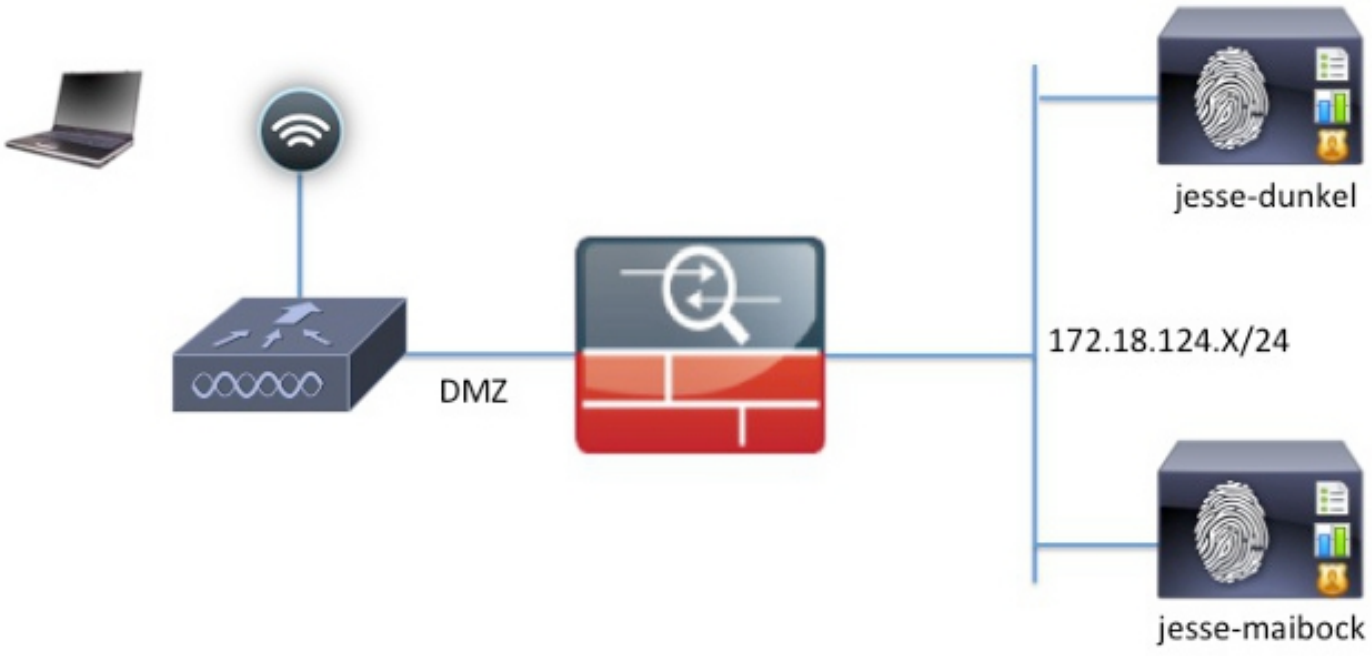
وهذا يجعل إعادة توجيه الضيف على ISE أمرا صعبا قبل الإصدار 1.2 لأن ISE يقوم بإعادة توجيه العملاء إلى اسم المجال المؤهل بالكامل (FQDN) لمصادقة الويب. ومع ذلك، باستخدام إصدارات ISE 1.2 والإصدارات الأحدث، يمكن للمسؤولين إعادة توجيه المستخدمين الضيوف إلى عنوان IP ثابت أو اسم المضيف.

التكوين

الرسم التخطيطي للشبكة

هذا رسم بياني منطقي.

ملاحظة: فعليا، هناك جهاز تحكم لاسلكي في الشبكة الداخلية، ونقاط الوصول (APs) موجودة على الشبكة الداخلية، ويتم ربط تعريف مجموعة الخدمة (SSID) بوحدة التحكم في DMZ. راجع وثائق Cisco WLCs للحصول على مزيد من المعلومات.



التكوين

يبقى التكوين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) دون تغيير من تكوين CWA العادي. يتم تكوين SSID للسماح بتصفية MAC باستخدام مصادقة RADIUS، ونقاط حساب RADIUS نحو عقدتين أو أكثر من عقد نهج ISE.

يركز هذا المستند على تكوين ISE.

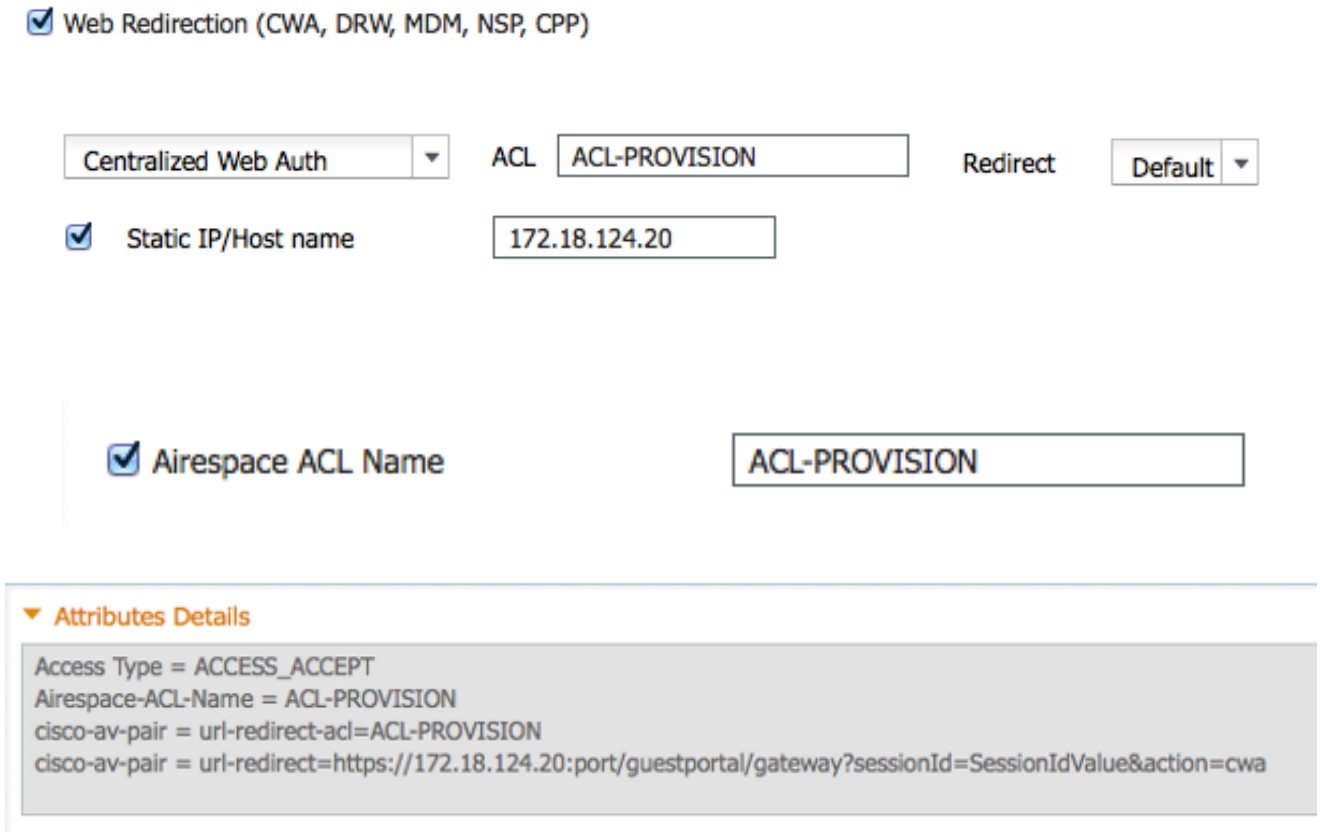
ملاحظة: في مثال التكوين هذا، تكون عقد السياسات هي **JESSE-Dunkel** (172.18.124.20) و**JESSE-Maibock** (172.18.124.21).

يبدأ تدفق CWA عندما يرسل ال WLC طلب تجاوز مصادقة MAB) MAC RADIUS) إلى ISE. ترد ISE باستخدام URL لإعادة التوجيه إلى وحدة التحكم لإعادة توجيه حركة مرور HTTP إلى ISE. من المهم أن يذهب حركة مرور RADIUS و HTTP إلى نفس عقدة خدمات السياسة (PSN) لأن الجلسة يتم الحفاظ عليها على PSN واحد. ويتم تنفيذ هذا الإجراء عادة باستخدام قاعدة واحدة، ويدرج PSN اسم المضيف الخاص به في عنوان URL الخاص بواجهة CWA. مهما، مع إعادة توجيه ساكن إستاتيكي، أنت ينبغي خلقت قاعدة لكل PSN in order to ضمنت أن ال RADIUS و HTTP حركة مرور أرسلت إلى ال نفسه PSN.

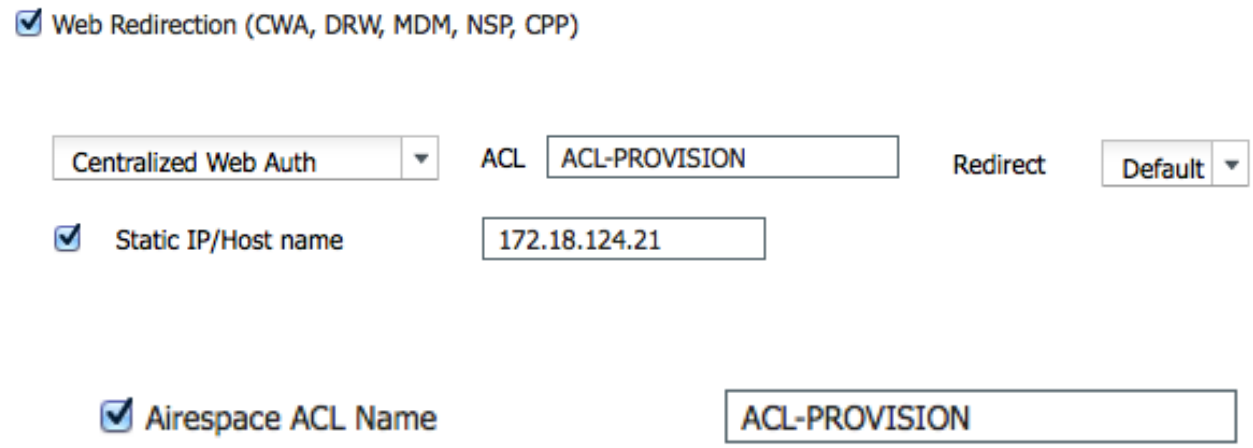
أتمت هذا steps in order to شكلت ال ISE:

قم بإعداد قاعدتين لإعادة توجيه العميل إلى عنوان IP ل PSN. انتقل إلى **السياسة > عناصر السياسة > النتائج > التخويل > ملفات تخصيص التخويل**.

تظهر هذه الصور معلومات اسم ملف التعريف **DunkelGuestWireless**:

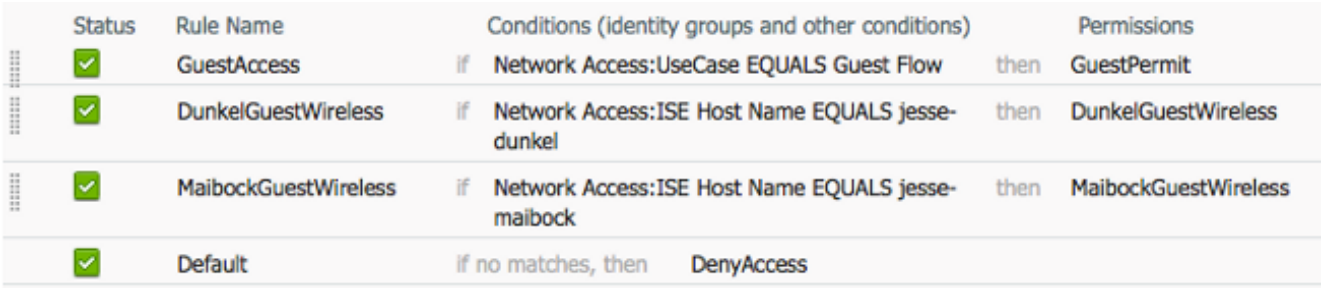


تظهر هذه الصور معلومات اسم ملف التعريف **MaibockGuestWireless**:



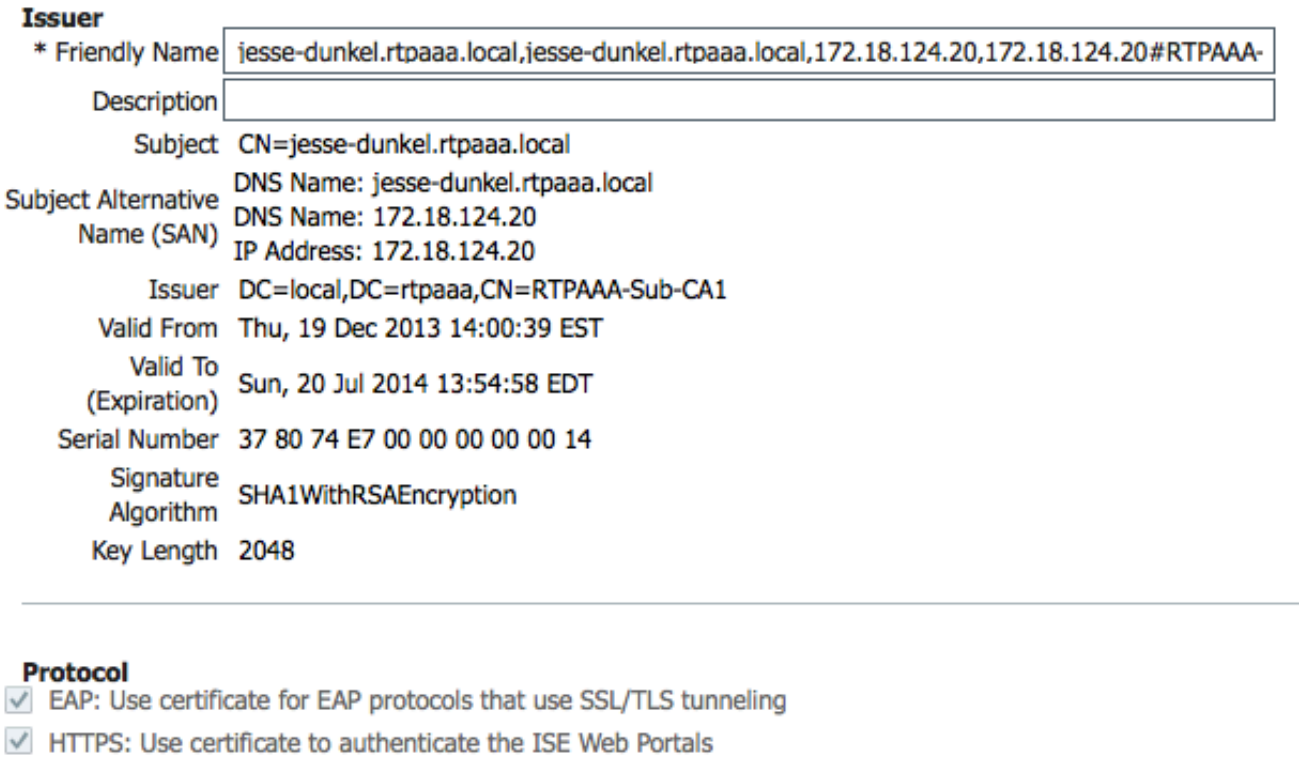
ملاحظة: **توفير قائمة التحكم في الوصول (ACL)** هو قائمة تحكم في الوصول محلية (ACL) تم تكوينها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للسماح للعميل بالاتصال ب ISE عند المصادقة. راجع المصادقة المركزية للويب على مثال تكوين WLC و ISE من Cisco للحصول على مزيد من المعلومات.

2. قم بتكوين سياسات التخويل بحيث تتطابق على سمة **Network Access:ISE Host Name** وتقديم ملف تعريف التخويل المناسب:



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	

الآن تتم إعادة توجيه العميل إلى عنوان IP، يتلقى المستخدمون تحذيرات الشهادة لأن عنوان URL لا يطابق المعلومات الموجودة في الشهادة. على سبيل المثال، FQDN في الشهادة هو **jesse-dunkel.rtpaaa.local**، ولكن عنوان URL هو **172.18.124.20**. فيما يلي شهادة مثال تسمح للمستعرض بالتحقق من صحة الشهادة باستخدام عنوان IP:



باستخدام إدخالات "الاسم البديل للموضوع" (SAN)، يمكن للمستعرض التحقق من عنوان URL الذي يتضمن عنوان IP **172.18.124.20**. يجب إنشاء ثلاثة إدخالات لشبكة منطقة التخزين (SAN) من أجل معالجة حالات عدم توافق العملاء المختلفة.

3. قم بإنشاء إدخال SAN لاسم DNS وتأكد من تطابقه مع إدخال **CN=** من حقل الموضوع.

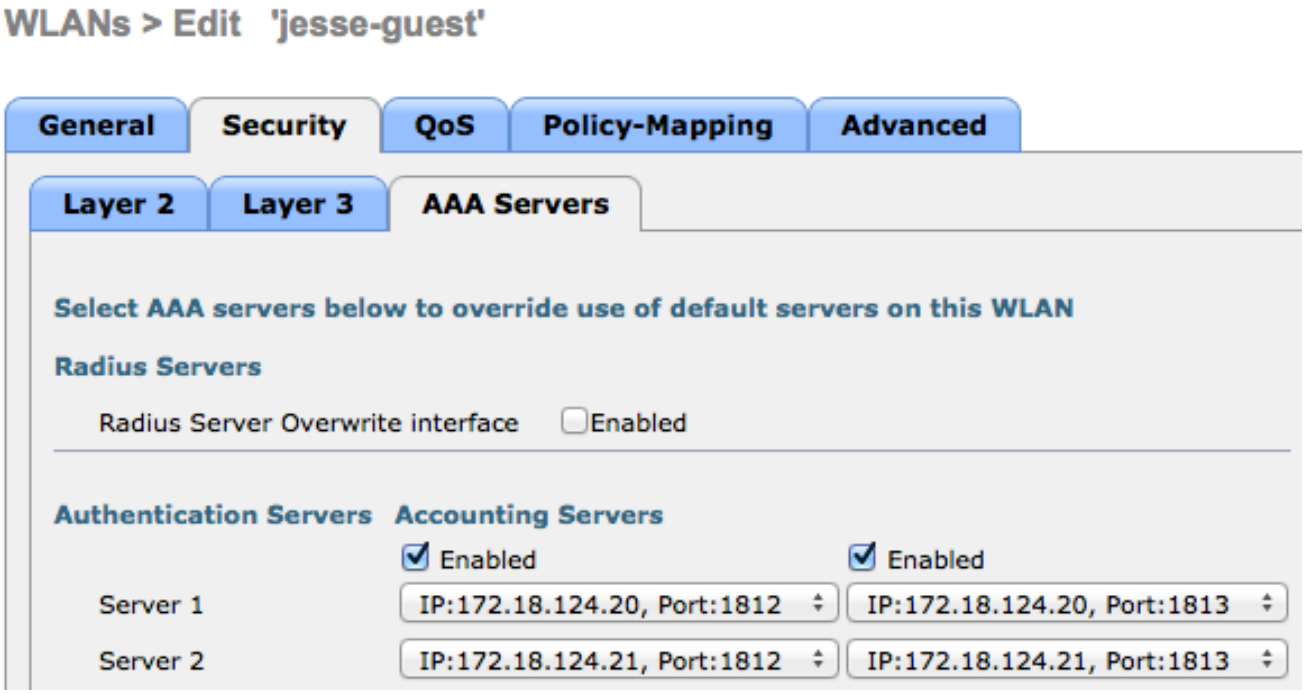
4. قم بإنشاء إدخالين للسماح للعملاء بالتحقق من صحة عنوان IP، وهما لكل من اسم DNS لعنوان IP وكذلك عنوان IP الذي يظهر في سمة عنوان IP. يشير بعض العملاء إلى اسم DNS فقط. لا يقبل آخرون عنوان IP في سمة اسم DNS ولكن بدلا من ذلك يرجعون إلى سمة عنوان IP.

ملاحظة: للحصول على مزيد من المعلومات حول إنشاء الشهادة، ارجع إلى **دليل تثبيت أجهزة محرك خدمات الهوية من Cisco، الإصدار 1.2**.

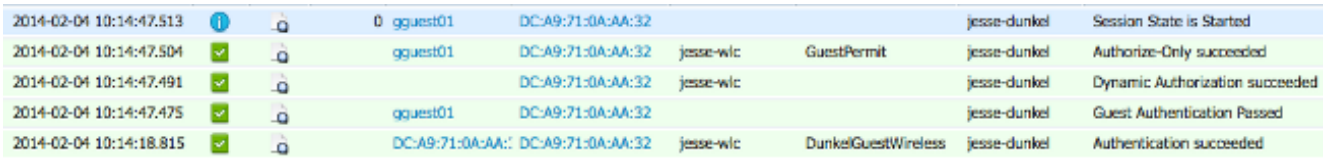
التحقق من الصحة

أكمل هذه الخطوات للتأكد من أن التكوين لديك يعمل بشكل صحيح:

1. للتحقق من أن كلا القواعد يعمل، قم بتعيين ترتيب شبكات ISE PSN التي تم تكوينها على الشبكة المحلية اللاسلكية (WLAN) يدويا:



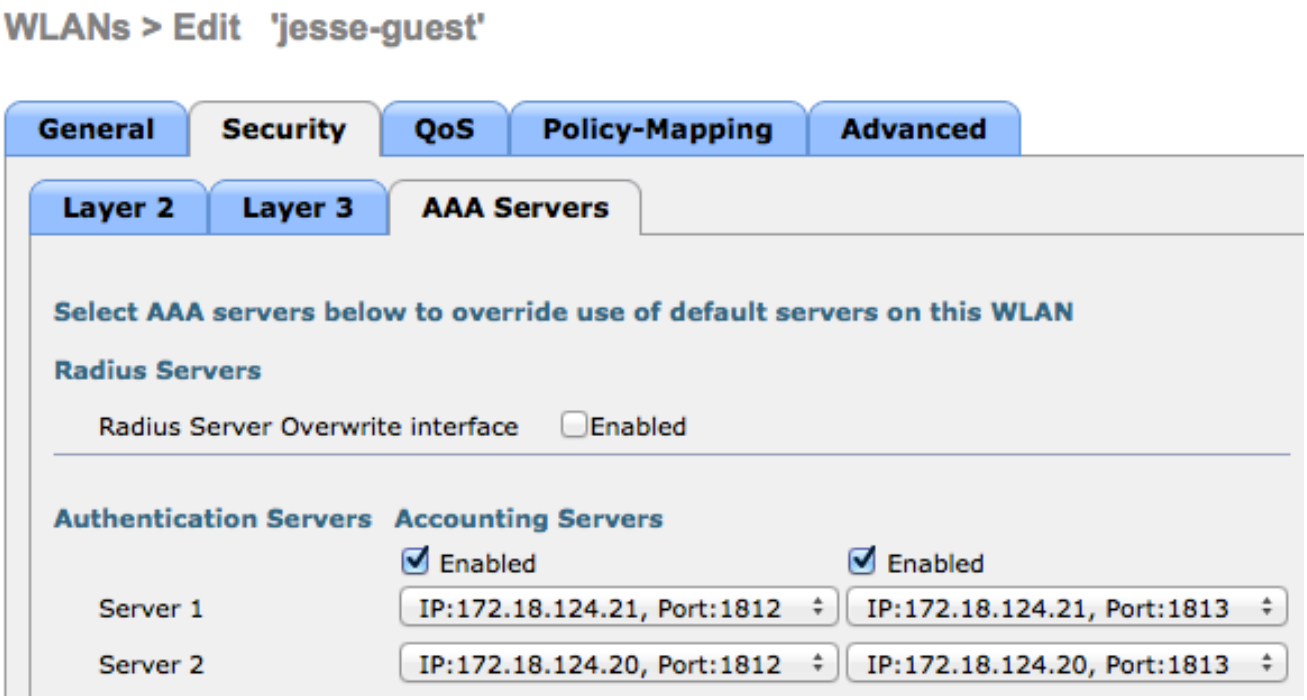
قم بتسجيل الدخول إلى SSID الضيف وانتقل إلى **العملية > المصادقة** في ISE وتحقق من الوصول إلى قواعد التخويل الصحيحة:



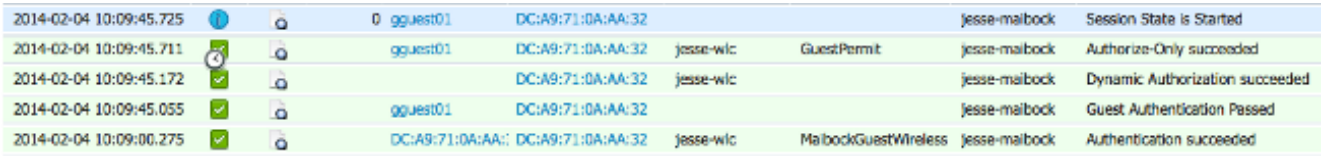
يتم إعطاء مصادقة MAB الأولية لملف تعريف تخويل **DunkelGuestWireless**. هذه هي القاعدة التي تعيد التوجيه بالتحديد إلى **جيسي-دونكل**، وهي أول عقدة ISE. بعد أن يقوم **مستخدم gguest01** بتسجيل الدخول، يتم منح الإذن النهائي الصحيح ل **GuestPermit**.

3. لمسح جلسات المصادقة من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، قم بفصل جهاز العميل عن الشبكة اللاسلكية، وانتقل إلى **مراقبة > عملاء** على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، وحذف الجلسة من الإخراج. يحتفظ عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بجلسة العمل الخاملة لمدة خمس دقائق بشكل افتراضي، لذلك يجب عليك البدء من جديد لتنفيذ إختبار صالح.

4. عكس ترتيب شبكات ISE PSN ضمن تكوين شبكة WLAN الضيف:



5. قم بتسجيل الدخول إلى SSID الضيف وانتقل إلى **العملية > المصادقة** في ISE وتحقق من الوصول إلى قواعد التخويل الصحيحة:



وفي المحاولة الثانية، يتم الوصول إلى ملف تعريف تخويل **MaibockGuestWireless** بشكل صحيح للمصادقة الأولية لمصادقة MAB. وعلى غرار المحاولة الأولى **جيسي دونكل** (الخطوة 2)، فإن المصادقة على **جيسي مايبوك** تصل بشكل صحيح إلى **تصريح الضيف** للحصول على التفويض النهائي. نظرا لعدم وجود معلومات خاصة ب PSN في ملف تعريف تفويض **GuestPermit**، يمكن إستخدام قاعدة واحدة للمصادقة على أي PSN.

استكشاف الأخطاء وإصلاحها

يعد إطار تفاصيل المصادقة طريقة عرض قوية تعرض كل خطوة في عملية المصادقة/التخويل. للوصول إليها، انتقل إلى **العمليات > عمليات التصديق** وانقر فوق أيقونة العدسة المكبرة أسفل عمود التفاصيل. أستخدم هذا الإطار للتحقق من تكوين شروط قاعدة المصادقة/التفويض بشكل صحيح.

في هذه الحالة، يكون حقل خادم النهج هو مجال التركيز الأساسي. يحتوي هذا الحقل على اسم المضيف الخاص ب ISE PSN الذي يتم من خلاله خدمة المصادقة:

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

قارن إدخال Policy Server بحالة القاعدة وتأكد من تطابق الاثنين (هذه القيمة حساسة لحالة الأحرف):

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

ملاحظة: من المهم تذكر أنه يجب قطع الاتصال ب SSID ومسح إدخال العميل من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بين الاختبارات.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).