LWAPP ةيقرت ةادأ ءاطخأ فاشكتسأ تلميحات وإصلاحها

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
عملية الترقية - نظرة عامة
أداة الترقية - التشغيل الأساسي
ملاحظات هامة
انواع الشهادات
المشكلة
عرض
الحلول
السبب 1
السبب 2
السبب 3
السبب 4
السبب 5
السبب 6
السبب 7
السبب 8
تلميحات أستكشاف المشكلات واصلاحها
معلومات ذات صلة

المقدمة

يناقش هذا المستند بعض المشاكل الأساسية التي قد تحدث عند إستخدام أداة الترقية لترقية نقاط الوصول (APs) المستقلة إلى وضع Lightweight. كما توفر هذه الوثيقة معلومات عن كيفية تصحيح هذه المسائل.

المتطلبات الأساسية

المتطلبات

يجب أن تقوم نقاط الوصول بتشغيل الإصدار JA(7)12.3 من برنامج Cisco IOS® أو إصدار أحدث قبل أن تتمكن من إجراء الترقية.

يجب أن تقوم وحدات التحكم من Cisco بتشغيل الإصدار 3.1 كحد أدنى من البرنامج.

يجب أن يعمل نظام التحكم اللاسلكي (WCS) من Cisco (في حالة إستخدامه) بأقل إصدار 3.1.

أداة الترقية مدعومة على نظامي Windows 2000 و Windows XP الأساسيين. يجب إستخدام أي من إصدارات نظام تشغيل Windows هذه.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى نقاط الوصول ووحدات التحكم في الشبكة المحلية اللاسلكية هذه.

نقاط الوصول التي تدعم هذا الترحيل هي:

- جميع نقاط الوصول لشبكة 1121G
- جميع نقاط الوصول 1130AG
- جميع نقاط الوصول 1240AG
- جميع نقاط الوصول من السلسلة 1250
- بالنسبة لجميع نقاط الوصول النمطية من السلسلة 1200 القائمة على IOS (ترقية برنامج Cisco IOS Software، 1200/1220 و 1210 و 1230 AP)، تعتمد على الراديو:إذا تم دعم 802.11g و MP21G و MP31Gإذا تم دعم 802.11a و RM21a و RM22aيمكن ترقية نقاط الوصول من السلسلة 1200 باستخدام أي توليفة من أجهزة الراديو المدعومة: G فقط أو A فقط أو كلا من G و A. لنقطة الوصول التي تحتوي على أجهزة راديو مزدوجة، إذا كان أحد الجهازين اللاسلكيين هو جهاز لاسلكي مدعوم من LWAPP، فإن أداة الترقية لا تزال تقوم بإجراء الترقية. تضيف الأداة رسالة تحذير إلى السجل المفصل الذي يشير إلى أي الراديو غير معتمد.
- جميع نقاط وصول AG طراز 1310
- بطاقة الواجهة Cisco C3201 Wireless Mobile Interface Card (WMIC)**ملاحظة:** تحتوي أجهزة الإرسال اللاسلكي من الجيل الثاني طراز 802.11a على رقمي أجزاء.

يجب أن تقوم نقاط الوصول بتشغيل الإصدار JA(7)12.3 من Cisco IOS أو إصدار أحدث قبل أن تتمكن من إجراء الترقية.

بالنسبة ل Cisco C3201WMIC، يجب أن تقوم نقاط الوصول بتشغيل Cisco IOS، الإصدار JK(8)12.3 أو إصدار أحدث قبل أن تتمكن من إجراء الترقية.

تدعم وحدات التحكم في شبكة LAN اللاسلكية هذه من Cisco نقاط الوصول المستقلة التي تمت ترقيتها إلى وضع Lightweight:

- وحدات التحكم من السلسلة 2000
- وحدات التحكم في السلسلة 2100
- وحدات التحكم من السلسلة 4400
- الوحدات النمطية للخدمات اللاسلكية (WiSMs) من Cisco لمحولات Cisco Catalyst 6500 Series Switches
- وحدات شبكة التحكم ضمن موجهات الخدمات المتكاملة 38xx/37/28 من Cisco
- محولات وحدة التحكم Catalyst 3750G Integrated Wireless LAN

يجب أن تقوم وحدات التحكم من Cisco بتشغيل الإصدار 3.1 كحد أدنى من البرنامج.

يجب أن يشغل نظام التحكم اللاسلكي (WCS) من Cisco الإصدار 3.1 كحد أدنى. أداة الترقية مدعومة على نظامي Windows 2000 و Windows XP الأساسيين.

يمكنك تنزيل أحدث إصدار من أداة الترقية المساعدة من صفحة تنزيلات برامج Cisco.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

عملية الترقية - نظرة عامة

يقوم المستخدم بتشغيل أداة مساعدة للترقية تقبل ملف إدخال مع قائمة بنقاط الوصول وبيانات الاعتماد الخاصة بها. الأداة المساعدة telnet إلى نقاط الوصول في ملف الإدخال سلسلة من أوامر Cisco IOS لإعداد نقطة الوصول للترقية، والتي تتضمن الأوامر لإنشاء الشهادات الموقعة ذاتيا. كما أن الأداة المساعدة Telnet إلى وحدة التحكم لبرمجة الجهاز للسماح بتخويل نقاط وصول شهادات ذاتية التوقيع معينة. ثم يقوم بتحميل الإصدار JX1(11)12.3 من برنامج Cisco IOS Software إلى نقطة الوصول حتى يمكنها الانضمام إلى وحدة التحكم. بعد أن تنضم نقطة الوصول إلى وحدة التحكم، تقوم بتنزيل إصدار كامل من Cisco IOS منها. تقوم الأداة المساعدة للترقية بإنشاء ملف إخراج يتضمن قائمة نقاط الوصول وقيم تجزئة مفتاح شهادة ذاتية التوقيع المقابلة التي يمكن إستيرادها إلى برنامج إدارة WCS. ويمكن أن تقوم WCS بعد ذلك بإرسال هذه المعلومات إلى وحدات التحكم الأخرى على الشبكة.

أحلت التحسين إجراء قسم من يحسن مستقل cisco Aironet نقاط الوصول إلى أسلوب خفيف وزن ل كثير معلومة.

أداة الترقية - التشغيل الأساسي

تستخدم أداة الترقية هذه لترقية نقطة وصول (AP) مستقلة إلى وضع Lightweight شريطة أن تكون نقطة الوصول متوافقة لهذه الترقية. تقوم أداة الترقية بتنفيذ المهام الأساسية اللازمة للترقية من وضع التحكم الذاتي إلى وضع Lightweight. وتتضمن هذه المهام ما يلي:

- التحقق من الشروط الأساسية - يتحقق مما إذا كانت نقطة الوصول مدعومة أم لا، وما إذا كانت تشغل حدا أدنى من مراجعة البرامج، وما إذا كانت أنواع الراديو مدعومة.
- تأكد من تكوين نقطة الوصول كجذر.
- تحضير نقطة الوصول المستقلة للتحويل - يضيف تكوين البنية الأساسية للمفتاح العام (PKI) والتدرج الهرمي للشهادات بحيث يمكن أن تحدث مصادقة نقطة الوصول إلى وحدات تحكم Cisco، ويمكن إنشاء شهادات موقعة ذاتيا (SSCs) لنقطة الوصول. إذا كانت نقطة الوصول تحتوي على شهادة (MIC) مثبتة على التصنيع، فلا يتم إستخدام أجهزة SSC.
- يجلب صورة ترقية في وضع Lightweight إلى وضع SelfWeight، مثل JX1(11)12.3 أو JX(7)12.3، والتي تتيح لنقطة الوصول الانضمام إلى وحدة تحكم. على عملية تنزيل ناجحة، يقوم هذا بإعادة تشغيل نقطة الوصول.
- يولد ملف مخرجات يتكون من عناوين AP MAC، نوع الشهادة، وخط مفتاح آمن، ويقوم بتحديث وحدة التحكم تلقائيا. يمكن إستيراد ملف المخرجات إلى WCS وتصديره إلى وحدات التحكم الأخرى.

ملاحظات هامة

قبل إستخدام هذه الأداة المساعدة، ضع في الاعتبار هذه الملاحظات المهمة:

- لا تتصل نقاط الوصول المحولة باستخدام هذه الأداة بوحدات التحكم 40xx أو 41xx أو 3500.
- لا يمكنك ترقية نقاط الوصول باستخدام أجهزة 802.11b فقط أو أجهزة 802.11a من الجيل الأول.
- إن يريد أنت أن يبقى العنوان ساكن إستاتيكي، hostname، netmask، والبوابة الافتراضية من نقاط الوصول بعد التحويل وإعادة التشغيل، أنت ينبغي حملت واحد من هذه الصور الذاتية على نقاط الوصول قبل أن تخفي نقاط الوصول إلى LWAPP:12,3(7)JA12.3(7)JA112.3(7)JA212.3(7)JA312,3(7)JA412,3(8)JA12.3(8)JA112.3(8)JA 212-3(8)JEA12-3(8)JEA112-3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g) JA12.4(3g) JA1
- إذا قمت بترقية نقاط الوصول إلى LWAPP من إحدى هذه الصور الذاتية، فإن نقاط الوصول المحولة لا تحتفظ بعنوان IP الثابت، و netmask، و hostname، والبوابة الافتراضية:12,3(11)JA3(11)JA212,3(11)JA112,3(11)JA12,3
- لا تقوم أداة ترقية LWAPP بإطلاق موارد ذاكرة نظام تشغيل Windows عند اكتمال عملية الترقية. يتم إصدار موارد الذاكرة فقط بعد إنهاء أداة الترقية. إذا قمت بترقية عدة دفعات من نقاط الوصول، يجب عليك الخروج من الأداة بين الدفعات لإطلاق موارد الذاكرة. إذا لم تقم بالخروج من الأداة بين الدفعات، فإن أداء محطة الترقية

سيتدهور بسرعة بسبب الاستهلاك المفرط للذاكرة.

انواع الشهادات

هناك نوعان مختلفان من نقاط الوصول:

- نقاط الوصول بميكروفون
- نقاط الوصول التي يجب أن تحتوي على SSC

وتتم الإشارة إلى الشهادات التي يتم تثبيتها في المصنع بواسطة مصطلح MIC، وهو إختصار خاص بتصنيع الشهادات المثبتة. نقاط الوصول Cisco Aironet التي تم شحنها قبل 18 يوليو 2005، لا تحتوي على ميكروفون، لذلك تقوم نقاط الوصول هذه بإنشاء شهادة موقعة ذاتيا عند ترقيتها للعمل في وضع Lightweight. وتتم برمجة وحدات التحكم لقبول شهادات ذاتية التوقيع لمصادقة نقاط وصول محددة.

يجب عليك معالجة نقاط الوصول Cisco Aironet MIC APs التي تستخدم بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP)، مثل نقاط الوصول Aironet 1000 واستكشاف الأخطاء وإصلاحها وفقا لذلك. بمعنى آخر، تحقق من اتصال IP، وتصحيح أخطاء جهاز حالة LWAPP، ثم تحقق من التشفير.

تظهر لك سجلات أداة الترقية ما إذا كانت نقطة الوصول هي نقطة وصول MIC أو نقطة وصول SSC. هذا مثال على سجل مفصل من أداة الترقية:

```
                                .INFO  172.16.1.60  Term Length configured 16:59:07 2006/08/21
                             INFO  172.16.1.60  Upgrade Tool supported AP 16:59:07 2006/08/21
                                    INFO  172.16.1.60  AP has two radios 16:59:07 2006/08/21
                                 INFO  172.16.1.60  AP has Supported Radio 16:59:07 2006/08/21
                       INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater 16:59:07 2006/08/21
                                 INFO  172.16.1.60  Station role is  Root AP 16:59:07 2006/08/21
                    INFO  172.16.1.60  MIC is already configured in the AP 16:59:07 2006/08/21
                  ,INFO  172.16.1.60      Hardware is PowerPC405GP Ethernet 16:59:07 2006/08/21
(address is 0015.63e5.0c7e (bia 0015.63e5.0c7e
                                 INFO  172.16.1.60  Inside Shutdown function 16:59:08 2006/08/21
                                 INFO  172.16.1.60  Shutdown the Dot11Radio1 16:59:10 2006/08/21
                                 INFO  172.16.1.60  Shutdown the Dot11Radio0 16:59:11 2006/08/21
               INFO  172.16.1.60  Updating the AP with Current System Time 16:59:12 2006/08/21
                   INFO  172.16.1.60  Saving the configuration into memory 16:59:13 2006/08/21
                                    INFO  172.16.1.60  Getting  AP Name 16:59:13 2006/08/21
                 INFO  172.16.1.60  Successfully Loaded the LWAPP Recovery 16:59:58 2006/08/21
                                 Image on to the AP
                          INFO  172.16.1.60  Executing Write Erase Command 16:59:58 2006/08/21
                             INFO  172.16.1.60  Flash contents are logged 17:00:04 2006/08/21
                       INFO  172.16.1.60  Environmental Variables are logged 17:00:06 2006/08/21
                                    INFO  172.16.1.60  Reloading the AP 17:00:06 2006/08/21
               INFO  172.16.1.60  Successfully executed the Reload command 17:00:08 2006/08/21
```

في هذا السجل، يحدد الخط المبرز أن نقطة الوصول بها ميكروفون مثبت بها. أحلت التحسين عملية نظرة عامة قسم من يحسن مستقل Aironet cisco نقاط الوصول إلى أسلوب خفيف وزن ل كثير معلومة على الشهادة وعملية التحسين.

في حالة نقاط الوصول SSC APs، لا يتم إنشاء شهادة على وحدة التحكم. تحتوي أداة الترقية على نقطة الوصول (AP) إنشاء زوج مفاتيح Rivest و Shamir و (RSA و Adelman) الذي يتم إستخدامه لتوقيع شهادة تم إنشاؤها ذاتيا (SSC). تضيف أداة الترقية إدخالا إلى قائمة مصادقة وحدة التحكم باستخدام عنوان MAC لنقطة الوصول والمفاتيح العام. يحتاج جهاز التحكم إلى تجزئة المفتاح العام للتحقق من توقيع SSC.

إذا لم تتم إضافة الإدخال إلى وحدة التحكم، فتحقق من ملف CSV الناتج. يجب أن تكون هناك إدخالات لكل نقطة وصول. إذا عثرت على الإدخال، فقم باستيراد هذا الملف إلى وحدة التحكم. إذا كنت تستخدم واجهة سطر الأوامر (CLI) لوحدة التحكم (باستخدام الأمر **config auth-list**) أو موقع ويب المحول، فيجب عليك إستيراد ملف واحد في كل

مرة. باستخدام WCS، يمكنك إدراج ملف CSV بأكمله كقالب.

أيضا، تحقق من المجال التنظيمي.

ملاحظة: إذا كانت لديك نقطة وصول من نقطة الوصول في الوضع Lightweight (LAP) لكنك تريد وظيفة Cisco IOS، فأنت بحاجة إلى تحميل صورة Cisco IOS مستقلة عليها. على نحو معاكس، إذا كانت لديك نقطة وصول (AP) مستقلة وتريد تحويلها إلى LWAPP، فيمكنك تثبيت صورة إسترداد LWAPP عبر IOS الذاتي.

أنت يستطيع أتمت ال steps أن يغير AP صورة مع الأسلوب زر أو CLI **أرشيف تنزيل** أمر. راجع أستكشاف الأخطاء وإصلاحها للحصول على مزيد من المعلومات حول كيفية إستخدام إعادة تحميل صورة زر الوضع، والذي يعمل مع IOS الذاتي أو صورة الاسترداد المسماة باسم اسم الملف الافتراضي لنموذج AP.

يناقش القسم التالي بعض من رأيت بشكل عام قضية في التحسين عملية والخطوات أن يحل هذا إصدار.

المشكلة

عرض

لا تنضم نقطة الوصول إلى وحدة التحكم. الحلول يزود قسم من هذا وثيقة السبب in order to احتمال.

الحلول

أستخدم هذا القسم لحل هذه المشكلة.

السبب 1

يتعذر على نقطة الوصول العثور على وحدة التحكم عبر اكتشاف LWAPP، أو يتعذر على نقطة الوصول الوصول إلى وحدة التحكم.

استكشاف الأخطاء وإصلاحها

أكمل الخطوات التالية:

1. قم بإصدار الأمر **debug lwapp events enable** في واجهة سطر الأوامر (CLI) لوحدة التحكم.ابحث عن اكتشاف LWAPP > إستجابة الاكتشاف > طلب الانضمام > تسلسل إستجابة الانضمام. إذا لم يظهر لديك طلب اكتشاف LWAPP، فهذا يعني أن نقطة الوصول لا يمكن أو لا يعثر على وحدة التحكم.هنا مثال على رد انضمام ناجح من وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) إلى نقطة الوصول في الوضع Lightweight (LAP)) المحولة. هذا هو مخرج الأمر **debug lwapp events enable**:

```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
'e5:0c:7e to 00:0b:85:33:84:a0 on port '1:00:15:63
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
e5:0c:7e on Port 1:00:15:63
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
'to 00:0b:85:33:84:a0 on port '1
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
e5:0c:7e on Port 1:00:15:63
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
'to ff:ff:ff:ff:ff:ff on port '1
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:15:63:e5:0c:7e on Port 1
Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e
```

```
                        'to 00:0b:85:33:84:a0 on port '1
    Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e
                         is 1500, remote debug mode is 0
    Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e
    ,index 51)Switch IP: 172.16.1.11, Switch Port: 12223)
  ,intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679
                         next hop MAC: 00:15:63:e5:0c:7e
      Thu May 25 06:54:05 2006: Successfully transmission of LWAPP Join-Reply to AP
                                      e5:0c:7e:00:15:63
                                       .....................................
                                    .....................................
  the debug output continues for // .....................................
                                                    .full registration process
```

2. تحقق من اتصال IP بين شبكة AP ووحدة التحكم. إذا كان جهاز التحكم والنقطة الوصول موجودين في الشبكة الفرعية نفسها، فتأكد من أنهما متصلان بشكل صحيح. إذا كانوا يقيمون في شبكات فرعية مختلفة، فتأكد من إستخدام موجه فيما بينهم وتمكين التوجيه بشكل صحيح بين الشبكتين الفرعيتين.
3. تحقق من تكوين آلية الاكتشاف بشكل صحيح.إذا تم إستخدام خيار نظام اسم المجال (DNS) لاكتشاف عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فتأكد من تكوين خادم DNS بشكل صحيح لتعيين Cisco-LWAPP-Controller.local-domain بعنوان WLC IP. وبالتالي، إذا كان يمكن لنقطة الوصول حل الاسم، فإنها تصدر رسالة انضمام إلى LWAPP إلى عنوان IP الذي تم حله.إذا تم إستخدام الخيار 43 كخيار اكتشاف، فتأكد من تكوينه بشكل صحيح على خادم DHCP.راجع تسجيل نقطة الوصول في الوضع Lightweight مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للحصول على مزيد من المعلومات حول عملية الاكتشاف والتسلسل.أحلت DHCP خيار 43 لخفيف وزن cisco Aironet نقاط الوصول تشكيل مثال ل كثير معلومة على كيف أن يشكل DHCP خيار 43.**ملاحظة:** تذكر أنه عندما تقوم بتحويل نقاط الوصول (AP) الموجهة بشكل ثابت، فإن آلية اكتشاف الطبقة الثالثة الوحيدة التي تعمل هي DNS لأن العنوان الثابت يتم الاحتفاظ به أثناء الترقية.على نقطة الوصول، يمكنك إصدار الأمر **debug lwapp client events** والأمر **debug ip udp** لتلقي معلومات كافية لتحديد ما يحدث بالضبط. يجب أن ترى تسلسل حزمة بروتوكول مخطط بيانات المستخدم (UDP) مثل هذا:مصدر من ال ap ip مع الجهاز تحكم إدارة قارن IP.مصدر من AP manager الخاص بوحدة التحكم إلى AP IP.سلسلة الحزم التي يتم الحصول عليها من AP IP إلى مدير AP IP.**ملاحظة:** في بعض الحالات، قد يكون هناك أكثر من وحدة تحكم وقد تحاول نقطة الوصول الانضمام إلى وحدة تحكم مختلفة على أساس جهاز حالة اكتشاف LWAPP والخوارزميات. قد يحدث هذا الموقف بسبب موازنة حمل نقطة الوصول الديناميكية الافتراضية التي تقوم وحدة التحكم بتنفيذها. وهذه الحالة تستحق الفحص.**ملاحظة:** هذا مثال إخراج من الأمر **debug ip udp**:

```
,(Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222
                                                    length=78
,(Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                    length=60
,(Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223*
                                                    length=75
,(Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679*
                                                    length=59
,(Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=180
,(Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                    length=89
,(Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=209
,(Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=164
```

```
,(Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=209
,(Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=287
,(Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                    length=89
,(Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679*
                                                    length=22
,(Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223*
                                                   length=222
```

قرار

أكمل الخطوات التالية:

1. راجع الدليل.
2. قم بإصلاح البنية الأساسية بحيث تدعم اكتشاف LWAPP بشكل صحيح.
3. قم بنقل نقطة الوصول إلى الشبكة الفرعية نفسها الخاصة بوحدة التحكم من أجل نسخها الأساسية.
4. إذا كان ضروريا، قم بإصدار الأمر **lwapp ap controller ip address *a.b.c.d*** لتعيين IP لوحدة التحكم يدويا في واجهة سطر الأوامر (CLI) لنقطة الوصول:ال *a.b.c.d* جزء من هذا أمر الإدارة قارن عنوان من ال WLC.**ملاحظة:** يمكن إستخدام أمر CLI هذا على نقطة وصول لم تقم بالتسجيل قط إلى وحدة تحكم، أو على نقطة وصول تم تغيير كلمة مرور التمكين الافتراضية الخاصة بها أثناء الانضمام إلى وحدة تحكم سابقة. راجع إعادة ضبط تكوين LWAPP على نقطة وصول في الوضع (Lightweight (LAP للحصول على مزيد من المعلومات.

السبب 2

وقت وحدة التحكم خارج الفاصل الزمني لصلاحية الشهادة.

استكشاف الأخطاء وإصلاحها

أكمل الخطوات التالية:

1. أصدرت **ال debug lwapp خطأ enable** و**debug pm pki enable** أمر.تظهر أوامر **تصحيح الأخطاء هذه** تصحيح أخطاء رسائل الشهادة التي يتم تمريرها بين نقطة الوصول و WLC. تظهر الأوامر بوضوح رسالة أن الشهادة رفضت خارج فترة الصلاحية.**ملاحظة:** تأكد من حساب إزاحة التوقيت العالمي المنسق (UTC).هذا هو المخرج من **ال debug pm pki enable** أمر على الجهاز التحكم:

```
                Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
                ()Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode
   ,Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California
     ,L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e
                                MAILTO=support@cisco.com
      ,Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems
                               CN=Cisco Manufacturing CA
       Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                                        e5:0c:7e:00:15:63
.Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems
                                                    .......................
```

```
.....
.....
.....
()Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
>cscoDefaultMfgCaCert<
:(Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current
2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
.validity interval: make sure the controller time is set
(Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil
```

في هذا المخرج، لاحظ المعلومات المبرزة. تُظهر هذه المعلومات بوضوح أن وقت وحدة التحكم يقع خارج الفاصل الزمني لصلاحية الشهادة الخاصة بنقطة الوصول (AP). لذلك، لا يمكن لنقطة الوصول (AP) التسجيل باستخدام وحدة التحكم. يكون للشهادات المُثبّتة في نقطة الوصول (AP) فاصل زمني للصلاحية محدد مسبقًا. يجب تعيين وقت وحدة التحكم بحيث يكون ضمن فترة صلاحية الشهادة لنقطة الوصول.

2. أصدرت **العرض crypto ca certificate** أمر من ال ap CLI in order to دققت الشهادة صحة فاصل يثبت في ال ap.وفيما يلي مثال على هذا:

```
AP0015.63e5.0c7e#show crypto ca certificates
.....
.....
.....
.....
Certificate
Status: Available
Certificate Serial Number: 4BC6DAB80000000517AF
Certificate Usage: General Purpose
:Issuer
cn=Cisco Manufacturing CA
o=Cisco Systems
:Subject
Name: C1200-001563e50c7e
ea=support@cisco.com
cn=C1200-001563e50c7e
o=Cisco Systems
l=San Jose
st=California
c=US
:CRL Distribution Point
http://www.cisco.com/security/pki/crl/cmca.crl
:Validity Date
start date: 17:22:04 UTC Nov 30 2005
end   date: 17:32:04 UTC Nov 30 2015
renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: Cisco_IOS_MIC_cert
.....
.....
.....
```

لم يتم سرد المُخرَج بالكامل حيث يمكن أن يكون هناك العديد من الفواصل الزمنية للصلاحية المرتبطة بمُخرَج هذا الأمر. تحتاج إلى مراعاة فترة الصلاحية المحددة بواسطة **TrustPoint المقترن:Cisco_IOS_MIC_CERT** مع اسم نقطة الوصول ذات الصلة في حقل الاسم (**هنا، الاسم: C1200-001563e50c7e**)، كما هو موضح في مثال الإخراج هذا. **هذا هو الفاصل الزمني الفعلي لصلاحية الشهادة الذي يجب وضعه في الاعتبار.**

3. قم بإصدار الأمر **show time** من واجهة سطر الأوامر (CLI) بوحدة التحكم للتحقق من أن التاريخ والوقت المعينين على وحدة التحكم لديك يندرجان ضمن هذا الفاصل الزمني للصلاحية.إذا كان وقت وحدة التحكم أعلى أو أسفل فترة صلاحية الشهادة هذه، فعليك تغيير وقت وحدة التحكم بحيث يقع ضمن هذه الفترة.

قرار

أكمل هذه الخطوة:

أخترت **أمر>يثبت وقت** في الجهاز تحكم gui أسلوب أو أصدرت **ال config وقت** أمر في الجهاز تحكم CLI in order to ثبت الجهاز تحكم وقت.

السبب 3

مع نقاط الوصول SSC، يتم تعطيل سياسة نقطة الوصول SSC.

استكشاف الأخطاء وإصلاحها

في مثل هذه الحالات، ترى رسالة الخطأ هذه على وحدة التحكم:

```
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                                  spamDecodeJoinReq failed:
Wed Aug  9 17:20:21 2006  [ERROR] spam_crypto.c 1509: Unable to free public key for
                                  AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                                  valid certificate in CERTIFICATE_PAYLOAD from
                                  .AP 00:12:44:b3:e5:60
Wed Aug  9 17:20:21 2006  [CRITICAL] sshpmPkiApi.c 1493: Not configured to accept
                                  Self-signed AP cert
```

أكمل الخطوات التالية:

قم بتنفيذ أحد هذين الإجرائن:

- قم بإصدار الأمر **show auth-list** في واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم للتحقق مما إذا تم تكوين وحدة التحكم لقبول نقاط الوصول مع SSCs.هذا نموذج إخراج من أمر **show auth-list**:

```
show auth-list#

Authorize APs against AAA ..... disabled

Allow APs with Self-signed Certificate (SSC) .... enabled

                                  Mac Addr                  Cert Type    Key Hash

----------------------------------------------   ----------   ----------------------

00:09:12:2a:2b:2c          SSC          1234567890123456789012345678901234567890
```

- أخترت **أمن > نهج ap** في ال gui.

1. تحقق ما إذا كان خانة الاختيار **قبول شهادة موقعة ذاتيا** ممكنة أم لا. وإذا لم تكن هناك مساحة، فقم بتمكينها.
2. أختر **SSC** كنوع الشهادة.
3. إضافة **نقطة وصول** إلى قائمة التخويل بعنوان MAC وتجزئة المفتاح.يمكن الحصول على تجزئة المفتاح هذه من إخراج الأمر **debug pm pki enable**. راجع السبب 4 للحصول على معلومات حول الحصول على قيمة التجزئة الأساسية.

السبب 4

تجزئة مفتاح SSC العام غير صحيحة أو مفقودة.

استكشاف الأخطاء وإصلاحها

أكمل الخطوات التالية:

1. قم بإصدار الأمر **debug lwapp events enable**.تحقق من محاولة نقطة الوصول الانضمام.
2. قم بإصدار الأمر **show auth-list**.يعرض هذا الأمر تجزئة المفتاح العام التي تحتوي عليها وحدة التحكم في التخزين.
3. قم بإصدار الأمر **debug pm pki enable**.يعرض هذا الأمر تجزئة المفتاح العام الفعلية. يجب أن تتطابق تجزئة المفتاح العام الفعلية مع تجزئة المفتاح العام التي يمتلكها جهاز التحكم في التخزين. ثمة تباين يسبب المشكلة.
هذا نموذج إخراج لرسالة تصحيح الأخطاء هذه:

```
Cisco Controller) > debug pm pki enable)

...Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle
    <Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
                                                        >bsnOldDefaultCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
                                                    >bsnDefaultRootCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
                                                       >bsnDefaultCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
                                                      >bsnDefaultBuildCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
                                                   >cscoDefaultNewRootCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
                                                    >cscoDefaultMfgCaCert<
                Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
                                                      >bsnOldDefaultIdCert<
  Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
                                                                        Data
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
                                                                   2a864886 f70d0101
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
                                                                   3082010a 02820101
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
                                                                   cad8df69 b366fd4c
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
                                                                   ad425fa7 face8f15
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
                                                                   43b95a34 49292e11
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
                                                                   56f0ad91 2d61a389
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
                                                                   b5cf7cef 06ba4375
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
                                                                   774ce74e 9e2fde19
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
                                                                   65d8639b d63aa0e3
        Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
                                                                   9cd31041 b0734a55
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
                                                                   c54e75f2 6d28fc6b
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
                                                                   02d37140 7c9c865a
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
                                                                   7a9bac00 d13ff85f
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
                                                                   88053e8b 7fae6d67
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
                                                                   bc1acc13 0d334aa6
        Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
```

```
                                                        2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
                                                        8302b8b8 23311756
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
                                                        280cbed1 49b2d50f
    Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
            Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
                                                    9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
This is the actual SSC key-hash value. Mon May 22 06:34:14 2006: LWAPP Join-Request ---!
  MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14
                        2006: spamRadiusProcessResponse: AP Authorization failure for
                                                    00:0e:84:32:04:f0
```

قرار

أكمل الخطوات التالية:

1. انسخ تجزئة المفتاح العام من إخراج الأمر **debug pm pki enable** واستخدامه لاستبدال تجزئة المفتاح العام في قائمة المصادقة.
2. أصدرت ال ***ap_mac ap_key*** **config auth-list add ssc** أمر in order to أضفت ال ap {upper}mac address والمفتاح إلى قائمة التخويل:هذا مثال من هذا أمر:

```
Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0)
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
.This command should be on one line ---!
```

السبب 5

هناك شهادة أو تلف في المفتاح العام على نقطة الوصول.

استكشاف الأخطاء وإصلاحها

أكمل هذه الخطوة:

أصدرت ال **debug lwapp** خطأ **enable** و**debug pm pki enable** أمر.

تظهر لك رسائل تشير إلى الشهادات أو المفاتيح المُعطّلة.

قرار

استخدم أحد الخيارين التاليين لحل المشكلة:

- نقطة وصول MIC — طلب ترخيص المواد المسترجعة (RMA).
- SSC AP — الرجوع إلى الإصدار JA(7)12.3 من برنامج Cisco IOS.أتمت هذا steps in order to خفضت:

1. أستخدم خيار زر إعادة الضبط.
2. امسح إعدادات وحدة التحكم.
3. قم بتشغيل الترقية مرة أخرى.

السبب 6

قد تكون وحدة التحكم تعمل في وضع الطبقة 2.

استكشاف الأخطاء وإصلاحها

أكمل هذه الخطوة:

تحقق من وضع تشغيل وحدة التحكم.

نقاط الوصول المحولة تدعم فقط اكتشاف الطبقة 3. لا تدعم نقاط الوصول (AP) المحولة اكتشاف الطبقة 2.

قرار

أكمل الخطوات التالية:

1. اضبط عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتكون في وضع الطبقة 3.
2. أعد التمهيد وأعط واجهة مدير نقطة الوصول عنوان IP في الشبكة الفرعية نفسها الخاصة بواجهة الإدارة.إن يتلقى أنت خدمة ميناء، مثل الخدمة ميناء على 4402 أو 4404، أنت سوفت يتلقى هو في سوبر net مختلف من ال ap مدير وإدارة قارن.

السبب 7

ترى هذا خطأ أثناء الترقية:

```
FAILED   Unable to Load  the LWAPP Recovery Image on to the AP
```

استكشاف الأخطاء وإصلاحها

عندما ترى هذا خطأ، أكمل الخطوات التالية:

1. تحقق من تكوين خادم TFTP بشكل صحيح.إذا كنت تستخدم خادم TFTP المدمج بأداة الترقية، فإن الخطأ الشائع هو برنامج جدار الحماية الشخصي، والذي يمنع بروتوكول TFTP الوارد.
2. تحقق مما إذا كنت تستخدم الصورة الصحيحة للترقية.الترقية إلى وضع Lightweight تتطلب صورة خاصة ولا تعمل مع صور الترقية العادية.

السبب 8

أنت تستلم هذا خطأ رسالة على ال AP بعد التحويل:

```
Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY*
_Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and*
                    certs no certs in the SSC Private File
                                :Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG*
                Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed*
.Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT*
                            .Reload Reason: FAILED CRYPTO INIT
Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN*
```

تقوم نقطة الوصول بإعادة التحميل بعد 30 ثانية وتبدأ العملية مرة أخرى.

قرار

أكمل هذه الخطوة:

لديك نقطة وصول SSC. ما إن يحول أنت إلى LWAPP ap، أضفت ال SSC وعنوان MAC ه تحت ال ap صحة هوية قائمة في الجهاز تحكم.

تلميحات أستكشاف المشكلات وإصلاحها

يمكن إستخدام هذه التلميحات عند الترقية من وضع التحكم الذاتي إلى وضع LWAPP:

- إذا لم يتم مسح ذاكرة NVRAM عندما تحاول وحدة التحكم الكتابة إليها بعد التحويل، فهذا يعني حدوث مشاكل. توصيك Cisco بمسح التكوين قبل تحويل نقطة وصول إلى LWAPP. in order to مسح التشكيل:من واجهة المستخدم الرسومية IOS — انتقل إلى **برنامج النظام > تكوين النظام > إعادة الضبط إلى الإعدادات الافتراضية،** أو **إعادة الضبط إلى الإعدادات الافتراضية باستثناء IP**.من CLI—قم بإصدار الأمر **write erase** و**reload** في CLI ولا تسمح بحفظ التكوين عند طلبها.وهذا أيضا يجعل الملف النصي من APs أن يكون محولا بواسطة أداة الترقية أكثر بساطة للإنشاء حيث تصبح الإدخالات <ip address>،cisco،cisco،cisco.
- cisco يوصي أن يستعمل أنت ال tftp32. يمكنك تنزيل أحدث خادم TFTPD على http://tftpd32.jounin.net/ .
- في حالة تمكين جدار حماية أو قائمة تحكم في الوصول أثناء عملية الترقية، يمكن أن تصبح أداة الترقية غير قادرة على نسخ الملف الذي يحتوي على متغيرات بيئية من محطة عمل إلى نقطة وصول.إذا قام جدار حماية أو قائمة التحكم في الوصول بحظر عملية النسخ وقمت بتحديد خيار إستخدام خادم أداة الترقية TFTP، فلن يمكنك متابعة الترقية لأن الأداة لا يمكنها تحديث المتغيرات البيئية، ويفشل تحميل الصورة إلى نقطة الوصول.
- تحقق مرة أخرى من الصورة التي تحاول الترقية إليها. تختلف الترقية من صور IOS إلى صور LWAPP عن صور IOS العادية.تحت "مستنداتي/حاسبي—> أدوات—> خيارات المجلد، تأكد من إلغاء تحديد خانة الاختيار **إخفاء امتدادات الملفات لأنواع الملفات المعروفة**.
- أحرص دائما على إستخدام أحدث أداة الترقية المتاحة وترقية صورة الاسترداد. تتوفر أحدث الإصدارات في مركز البرامج اللاسلكية.
- لا يمكن لنقطة الوصول تمهيد ملف صورة **tar.** هو أرشيف، مماثل لملفات zip. أنت تحتاج أن يفك الربط **tar.** مبرد في AP برق مع **الأرشيف تنزيل** أمر، أو غير ذلك أن يسحب الصورة القابلة للتحميل من ملف tar أولا ثم يضع الصورة القابلة للتحميل في AP برق.

معلومات ذات صلة

- ترقية نقاط الوصول Cisco Aironet المستقلة إلى وضع Lightweight
- إعادة ضبط تكوين LWAPP على نقطة وصول في الوضع (Lightweight (LAP
- DHCP خيار 43 لخفيف وزن cisco Aironet نقاط الوصول تشكيل مثال
- كيفية إستعادة مفتاح التجزئة من نقطة الوصول واستيراده إلى وحدة التحكم
- يمكن تحويل نقطة الوصول المستقلة Cisco Aironet إلى بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP)) باستخدام CLI (واجهة سطر الأوامر)
- الدعم التقني والمستندات - Cisco Systems

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).