Tips voor probleemoplossing van LWAPP-upgrade

Inhoud

Inleiding

Dit document behandelt een aantal belangrijke kwesties die kunnen voorkomen wanneer u het upgradegereedschap gebruikt om autonome access points (APs) te verbeteren in lichtgewicht modus. Dit document bevat ook informatie over de manier waarop deze kwesties kunnen worden rechtgezet.

Voorwaarden

Vereisten

APs moet Cisco IOS® softwarerelease 12.3(7)JA of later uitvoeren voordat u de upgrade kunt uitvoeren.

Cisco controllers moeten een minimum aan softwareversie 3.1 uitvoeren.

Cisco Wireless Control System (WCS) (indien gebruikt) moet minimaal versie 3.1 uitvoeren.

Het upgradeprogramma wordt ondersteund op de Windows 2000- en Windows XP-platforms. Een van deze Windows-besturingssysteemversies moet worden gebruikt.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze access points en draadloze LAN-controllers.

De AP's die deze migratie ondersteunen zijn:

- Alle 1121G access points
- Alle 1130AG access points
- Alle 1240AG access points
- Alle 1250 Series access points
- Voor alle IOS-gebaseerde 1200 Series modulaire access point (1200/1220 Cisco IOS-software-upgrade, 1210 en 1230 AP) platforms is dit afhankelijk van de radio:indien 802.11G, MP21G en MP31G worden ondersteundindien 802.11A, RM21A en RM22A worden ondersteundDe 1200 Series access points kunnen met elke combinatie van ondersteunde radio's worden bijgewerkt: Alleen G, A, of zowel G als A. Voor een toegangspunt dat dubbele radio bevat, als een van de twee radio's een door LWAPP ondersteunde radio is, voert het upgrade-gereedschap nog steeds de upgrade uit. Het gereedschap voegt een waarschuwingsbericht toe aan het gedetailleerde logbestand dat aangeeft welke radio niet wordt ondersteund.
- Alle 1310 AG access points
- Cisco C3201 draadloze mobiele interfacekaart (WMIC)**Opmerking:** De tweede generatie 802.11a-radio's bevat twee onderdelennummers.

Access points moeten Cisco IOS release 12.3(7)JA of hoger uitvoeren voordat u de upgrade kunt uitvoeren.

Voor Cisco C3201WMIC moeten de access points Cisco IOS release 12.3(8)JK of hoger uitvoeren voordat u de upgrade kunt uitvoeren.

Deze Cisco draadloze LAN-controllers ondersteunen autonome access points die zijn bijgewerkt naar lichtgewicht modus:

- 2000 Series controllers
- 2100 Series controllers
- 4400 Series controllers
- Cisco draadloze servicesmodules (WiSM's) voor Cisco Catalyst 6500 Series Switches
- Netwerkmodules voor controllers binnen de Cisco 28/37/38xx Series geïntegreerde services routers
- Catalyst 3750G geïntegreerde draadloze LAN-controller-Switches

Cisco controllers moeten een minimum aan softwareversie 3.1 uitvoeren.

Cisco Wireless Control System (WCS) moet minimaal versie 3.1 uitvoeren. Het upgradehulpprogramma wordt ondersteund op de Windows 2000- en Windows XP-platforms.

U kunt de nieuwste versie van het upgradehulpprogramma downloaden van de pagina Cisco-softwaredownloads.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Upgradeproces - Overzicht

De gebruiker voert een upgrade-hulpprogramma uit dat een invoerbestand met een lijst van toegangspunten en hun referenties accepteert. Het nutselementen op de toegangspunten in het invoerbestand een reeks van Cisco IOS opdrachten om het toegangspunt voor de upgrade voor te bereiden, wat de opdrachten bevat om de zelf-ondertekende certificaten te maken. Ook het gebruiksnetwerk van de controller op de controller om de autorisatie van specifieke zelfgetekende toegangspunten mogelijk te maken. Hiermee wordt Cisco IOS-softwarerelease 12.3(11)JX1 op het access point geladen, zodat het zich bij de controller kan aansluiten. Nadat het toegangspunt zich bij de controller aansluit, downloads de volledige Cisco IOS-versie ervan. Het upgradeprogramma genereert een uitvoerbestand dat de lijst van access points en de corresponderende zelfgetekende hoofdwaswaarden bevat die in de WCS-beheersoftware kunnen worden geïmporteerd. De WCS kan deze informatie dan naar andere controllers op het netwerk sturen.

Raadpleeg het gedeelte Upgradeprocedure voor het uploaden van autonome Cisco Aironet access points naar lichtgewicht modus voor meer informatie.

Upgradegereedschap - basisbediening

Dit upgradegereedschap wordt gebruikt om een autonome AP aan lichtgewicht wijze te verbeteren op voorwaarde dat AP voor deze upgrade compatibel is. Het upgradegereedschap voert de basistaken uit die nodig zijn om van autonome naar lichtgewicht modus te upgraden. Deze taken omvatten:

- Basisconditie controle-verifieert of AP ondersteund is, of het een minimum software revisie voert en of de radiatypen worden ondersteund.
- Zorg dat AP als wortel wordt gevormd.
- Voorbereiding van de autonome AP voor conversie-voegt de PKI configuratie en de certificaathiërarchie van de Openbare Belangrijkste Infrastructuur (PKI) toe zodat de AP authenticatie aan de controllers kan voorkomen, en de zelfgetekende certificaten (SSC's) kunnen voor AP worden gegenereerd. Als de AP een productie-geïnstalleerd certificaat (MIC) heeft, dan worden SSCs niet gebruikt.
- Downloads voor een autonome to lichtgewicht modus upgrade-afbeelding, zoals 12.3(11)JX1 of 12.3(7)JX, waardoor de AP zich kan aansluiten bij een controller. Bij een succesvolle download start dit de AP opnieuw op.
- genereert een uitvoerbestand dat bestaat uit AP MAC-adressen, het certificaattype en een beveiligde key-hash en wordt automatisch de controller bijgewerkt. Het uitvoerbestand kan in WCS worden geïmporteerd en naar andere controllers worden geëxporteerd.

Belangrijke opmerkingen

Voordat u deze voorziening gebruikt, dient u deze belangrijke opmerkingen in acht te nemen:

- Access points die met dit gereedschap zijn geconverteerd, verbinden geen verbindingen met 40xx, 41xx of 3500 controllers.
- U kunt de toegangspunten niet verbeteren met 802.11b-alleen of met 802.11a-radio's van de eerste generatie.
- Als u het statische IP-adres, netmask, hostname en standaardgateway van toegangspunten na conversie en herstart wilt behouden, moet u een van deze autonome beelden op de access points laden voordat u de access points naar LWAPP converteert:12.3(7)JA12.3(7)JA112.3(7)JA212.3(7)JA312.3(7)JA412.3(8)JA12.3(8)JA112.3(8) JA212.3(8)JEA12.3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g) JA12.4(3g) JA1
- Als u toegangspunten naar LWAPP van één van deze autonome beelden verbetert, behouden de geconverteerde access points hun statische IP adres, netmask, hostname en standaardgateway niet:12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- Het LWAPP-upgradegereedschap geeft de Windows-geheugenbronnen niet vrij wanneer het upgradeproces is voltooid. Geheugenbronnen worden pas vrijgegeven nadat u de upgrade-gereedschappen hebt verlaten. Als u meerdere batches access points verbetert, moet u het gereedschap tussen batches afsluiten om geheugenbronnen vrij te geven. Als u het gereedschap niet tussen de partijen verlaat, gaat de prestatie van het upgradestation snel achteruit omdat u te veel geheugen gebruikt.

Typen certificaten

Er zijn twee verschillende soorten AP's:

- APs met een MIC
- AP's die een SSC nodig hebben

Aangepaste geïnstalleerde certificaten worden aangeduid met de term MIC, een acroniem voor een geïnstalleerd productiecertificaat voor productieomgevingen. Cisco Aironet access points die vóór 18 juli 2005 zijn verzonden, hebben geen MIC. Deze access points maken dus een zelfondertekend certificaat wanneer ze worden bijgewerkt om in lichtgewicht modus te werken. Controllers zijn geprogrammeerd om zelf ondertekende certificaten voor de echtheidscontrole van specifieke toegangspunten te accepteren.

U moet Cisco Aironet MIC APs behandelen die Lichtgewicht Access Point Protocol (LWAPP), zoals Aironet 1000 APs, en uw probleemoplossing dienovereenkomstig gebruiken. Met andere woorden, controleer de IP connectiviteit, debug de staatsmachine van LWAPP, en controleer dan de crypto.

De logbestanden van het upgradegereedschap tonen u of AP een MIC AP of SSC AP is. Dit is een voorbeeld van een gedetailleerd logbestand uit het upgrade-gereedschap:

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO  172.16.1.60  MIC is already configured in the AP
2006/08/21 16:59:07 INFO  172.16.1.60      Hardware is PowerPC405GP Ethernet,
```

```
                                        address is 0015.63e5.0c7e (bia 0015.63e5.0c7e)
2006/08/21 16:59:08 INFO  172.16.1.60  Inside Shutdown function
2006/08/21 16:59:10 INFO  172.16.1.60  Shutdown the Dot11Radio1
2006/08/21 16:59:11 INFO  172.16.1.60  Shutdown the Dot11Radio0
2006/08/21 16:59:12 INFO  172.16.1.60  Updating the AP with Current System Time
2006/08/21 16:59:13 INFO  172.16.1.60  Saving the configuration into memory
2006/08/21 16:59:13 INFO  172.16.1.60  Getting  AP Name
2006/08/21 16:59:58 INFO  172.16.1.60  Successfully Loaded the LWAPP Recovery
                                         Image on to the AP
2006/08/21 16:59:58 INFO  172.16.1.60  Executing Write Erase Command
2006/08/21 17:00:04 INFO  172.16.1.60  Flash contents are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Environmental Variables are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Reloading the AP
2006/08/21 17:00:08 INFO  172.16.1.60  Successfully executed the Reload command
```

In dit logbestand specificeert de gemarkeerde lijn dat AP een MIC heeft geïnstalleerd met deze. Raadpleeg het gedeelte Overzicht van het upgrade-proces van Upgrade Autonomous Cisco Aironet access points naar lichtgewicht modus voor meer informatie over de certificaten en het upgradeproces.

In het geval van de SSC-AP's wordt geen certificaat voor de controller gecreëerd. Het upgrade-gereedschap heeft een toetsenbord dat op Rivest, Shamir en Adelman (RSA) is gebaseerd, dat wordt gebruikt om een zelf-gegenereerd certificaat (de SSC) te tekenen. Het upgradegereedschap voegt een ingang aan de controlelijst van de controller toe met het MAC-adres van het AP en de openbare sleutel. De controller heeft de openbare sleutelhash nodig om de handtekening van de WS te valideren.

Als de ingang niet aan de controller is toegevoegd, controleert u het uitgevoerde CSV-bestand. Voor elk AP moet er een vermelding zijn. Als u de ingang vindt, importeer dat bestand in de controller. Als u de controller opdrachtregel interface (CLI) gebruikt (met gebruik van de configuratie-**auth-list** opdracht) of het switch web, moet u één bestand tegelijk importeren. U kunt met een WCS het gehele CSV-bestand als sjabloon importeren.

Controleer ook het regelgevende domein.

Opmerking: Als u een LAP AP hebt maar u wilt Cisco IOS functionaliteit, moet u een autonoom Cisco IOS beeld op het laden laden. Omgekeerd, als u een autonome AP hebt en het in LWAPP wilt omzetten, kunt u een LWAPP terugwinningsbeeld over autonome IOS installeren.

U kunt de stappen om het AP-beeld te veranderen met de knop MODE of de opdrachten **voor het downloaden van** een CLI-**archiefbestand** voltooien. Raadpleeg Problemen oplossen voor meer informatie over het opnieuw laden van de MODE-toets, die werkt met autonoom IOS of herstelbeeld genaamd naar AP model standaard bestandsnaam.

In het volgende gedeelte worden een aantal van de meest voorkomende problemen in de upgrade-operatie besproken, evenals de stappen om deze problemen op te lossen.

Probleem

Symptoom

AP sluit zich niet aan bij de controller. Het gedeelte Oplossingen in dit document geeft de oorzaken in volgorde van waarschijnlijkheid.

Oplossingen

Gebruik dit gedeelte om dit probleem op te lossen.

Oorzaak 1

AP kan de controller niet vinden via LWAPP ontdekking, of AP kan de controller niet bereiken.

Problemen oplossen

Voer de volgende stappen uit:

1. Geef de **debug lwapp gebeurtenissen** uit **om** opdracht te geven bij de controller CLI.Kijk naar de LWAPP ontdekking > zoekingsrespons > sluit zich aan bij verzoek > sluit zich aan bij antwoordsequentie. Als u het LWAPP zoekverzoek niet ziet, betekent dit dat het AP de controller niet kan of niet vindt.Hier is een voorbeeld van een succesvol JOIN REPLY van de Draadloze LAN controller (WLC) aan de geconverteerde lichtgewicht AP (LAP). Dit is de output van de **debug lwapp gebeurtenissen** opdracht geven:

```
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
                          00:15:63:e5:0c:7e on Port 1
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
                          00:15:63:e5:0c:7e on Port 1
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
                          00:15:63:e5:0c:7e
.........................................
.........................................
......................................... // the debug output continues for
full registration process.
```

2. Controleer op IP-connectiviteit tussen het AP-netwerk en de controller. Als het controller en het AP in hetzelfde subnet wonen, zorg er dan voor dat ze correct onderling verbonden zijn. Als zij in verschillende subnetten verblijven, zorg er dan voor dat een router tussen hen wordt gebruikt en de routing wordt goed ingeschakeld tussen de twee subnetten.
3. Controleer dat het zoekmechanisme correct is ingesteld.Als de optie Domain Name System (DNS) wordt gebruikt voor het ontdekken van de WLC, zorg er dan voor dat de DNS-server correct is geconfigureerd om CISCO-LWAPP-CONTROLLER.Local-domain met het WLC IP-adres in kaart te brengen. Daarom, als AP de naam kan oplossen, geeft het LWAPP zich bij bericht aan het opgeloste IP adres aan.Als optie 43 wordt gebruikt als de zoekoptie, zorg er dan voor dat deze correct is geconfigureerd op de DHCP-server.Raadpleeg het gedeelte

LAP met de WLC registreren voor meer informatie over het zoekproces en de opeenvolging.Raadpleeg DHCP-optie 43 voor lichtgewicht Cisco Aironet access points Configuration Voorbeeld voor meer informatie over de configuratie van DHCP-optie 43.**Opmerking:** Onthoud dat wanneer u statisch behandelde APs converteert het enige Layer 3 ontdekkingsmechanisme dat werkt het DNS is omdat het statische adres tijdens de upgrade behouden blijft.Op AP, kunt u de **debug lwapp client events** opdracht geven en de **debug ip udp** opdracht om genoeg informatie te ontvangen om precies te bepalen wat gebeurt. U dient een UDP-pakketsequentie (User Datagram Protocol) te zien zoals deze:Uitgerust van AP IP met het IP van het controlebeheer interface.Gedrukt van de controller AP Manager IP naar de AP IP.Een serie pakketten die van AP IP aan de AP manager IP zijn afkomstig.**Opmerking:** In sommige situaties kan er meer dan één controller zijn en kan de AP proberen om zich aan te sluiten bij een andere controller op basis van de LWAPP-detectieset en algoritmen. Deze situatie kan zich voordoen vanwege de standaard dynamische taakverdeling die de controller uitvoert. Deze situatie kan het overwegen waard zijn.**Opmerking:** dit is een voorbeelduitvoer van de opdracht **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
```

Resolutie

Voer de volgende stappen uit:

1. Lees de handleiding.
2. Bevestig de infrastructuur zodat deze de LWAPP-ontdekking correct ondersteunt.
3. Verplaats de AP naar zelfde voorwerp zoals het controller om het te openen.
4. Indien nodig geeft u het **IP-adres van de lwapp-ap-controller op *A.B.C.D*-**opdracht af om de IP-controller handmatig in te stellen op AP CLI:Het *A.B.C.D* deel van deze opdracht is het IP-adres van de beheerinterface van de WLC.**Opmerking:** Deze CLI-opdracht kan worden gebruikt op een AP die nooit bij een controller is geregistreerd of op een AP met de standaardinstelling dat het wachtwoord kan worden gewijzigd bij aansluiting op een vorige controller. Raadpleeg het gedeelte LWAPP-configuratie op een lichtgewicht AP (LAP) voor meer informatie.

Oorzaak 2

De controletijd valt buiten de geldigheidstermijn van het certificaat.

Problemen oplossen

Voer de volgende stappen uit:

1. Geef de **debug lwapp fouten toe om pm** en **debug pm toe te passen om** opdrachten **te kunnen** uitvoeren.Deze **debug-**opdrachten tonen het debug van certificaatberichten die tussen de AP en de WLC worden doorgegeven. De opdrachten tonen duidelijk aan dat het certificaat buiten het geldigheidinterval wordt verworpen.**Opmerking:** Stel rekening met de UTC-offset (Coördinated Universal Time).Dit is de uitvoer van de **debug pm om** opdracht in de controller te zetten:

```
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
                          00:15:63:e5:0c:7e
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)
```

In deze uitvoer, merk de gemarkeerde informatie op. Uit deze informatie blijkt duidelijk dat de **controletijd buiten de geldigheidstermijn van het certificaat van het AP valt**. Daarom kan het AP niet bij de controller registreren. In de AP geïnstalleerde certificaten hebben een vooraf bepaald geldigheidinterval. De controletijd moet zodanig worden vastgesteld dat deze binnen

de geldigheidstermijn van het certificaat van het AP valt.

2. Geef de opdracht **show crypto ca certificaten** af van de AP CLI om de in de AP vastgestelde geldigheidstermijn van het certificaat te verifiëren.Dit is een voorbeeld:

```
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
.................................
.................................
.................................
```

   De gehele uitvoer is niet vermeld aangezien er veel geldigheids intervallen kunnen zijn verbonden met de uitvoer van deze opdracht. U hoeft alleen rekening te houden met het geldigheidinterval dat door het **geassocieerde Trustpoint** is gespecificeerd: **Cisco_IOS_MIC_cert** met de relevante AP naam in het naamveld (**Hier, naam: C1200-001563e50c7e**), zoals in dit uitvoervoorbeeld benadrukt. **Dit is de werkelijk te overwegen geldigheid van het certificaat.**

3. De opdracht **tijd-**inval van de controller-CLI afgeven om te controleren of de datum en de tijd die op uw controller is ingesteld binnen deze geldigheidstermijn vallen.Indien de controletstijd boven of onder dit certificaat geldigheidinterval ligt, verander dan de controletstijd die binnen dit interval moet vallen.

Resolutie

Voltooi deze stap:

Kies **Opdrachten > Tijd** in de GUI-controller of geef de opdracht **configuratietstijd** in de CLI van de controller uit om de beheertijd in te stellen.

Oorzaak 3

Met SSC AP's is het SSC AP beleid uitgeschakeld.

Problemen oplossen

In dergelijke gevallen ziet u deze foutmelding op de controller:

```
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
```

Voer de volgende stappen uit:

Voer een van deze twee handelingen uit:

- Geef de opdracht **toonaangevende lijst** uit bij de CLI van de controller om te controleren of de controller zodanig is geconfigureerd dat hij AP's accepteert met SSC's.Dit is een voorbeelduitvoer van de opdracht **showauth-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
  ```

- Kies **Beveiliging > AP-beleid** in de GUI.

1. Controleer of het vakje **Certificaat** aanvaarden is ingeschakeld. Als dit niet het geval is, schakelt u het programma in.
2. Kies **SSC** als het certificaattype.
3. Voeg **AP** aan de vergunningslijst toe met het adres van MAC en het zeer belangrijke hash.Deze key-hash kan worden verkregen uit de uitvoer van de **debug pm om** opdracht **in te schakelen**. Zie Oorzaak 4 voor informatie over het krijgen van de belangrijke hashwaarde.

Oorzaak 4

De openbare sleutelhash van SSC is fout of ontbreekt.

Problemen oplossen

Voer de volgende stappen uit:

1. Geef de **debug lwapp gebeurtenissen uit die** opdracht **geven**.Controleer dat AP probeert toe

te voegen.

2. Geef de opdracht **showauth-list uit**.Deze opdracht toont de openbare sleutel die de controller in opslag heeft.
3. Geef de **debug pm optie uit**.Deze opdracht toont de echte hoofdhash. De echte hoofdhash moet overeenkomen met de hoofdhash van de publieke zaak die de controller in opslag heeft. Een discrepantie veroorzaakt het probleem. Dit is een voorbeelduitvoer van dit debug-bericht:

```
(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
23311756 8302b8b8
```

```
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
```

Resolutie

Voer de volgende stappen uit:

1. Kopieer de openbare key-hash van de **debug pm om** opdrachtoutput **mogelijk** te maken en gebruik deze om de openbare key-hash in de authenticatielijst te vervangen.
2. Geef de **configuratie van de auth-list** ***een*** **add-**ssc *AP_MAC-AP_key* opdracht uit om het AP MAC-adres en de key-hash aan de autorisatielijst toe te voegen:Dit is een voorbeeld van deze opdracht:
```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Oorzaak 5

Er is een certificaat of openbare sleutel corruptie op het AP.

Problemen oplossen

Voltooi deze stap:

Geef de **debug lwapp fouten toe om pm** en **debug pm toe te passen om** opdrachten **te kunnen** uitvoeren.

U ziet berichten die de certificaten of toetsen aangeven die beschadigd zijn.

Resolutie

Gebruik een van deze twee opties om het probleem op te lossen:

- MIC AP-Verzoek om een vergunning van de terugkeermaterialen (RMA).
- SSC AP-downgrade naar Cisco IOS-softwarerelease 12.3(7)JA.Voltooi deze stappen om de kwaliteit te verlagen:

1. Gebruik de optie Reset-knop.
2. Schakel de instellingen van de controller uit.
3. Start de upgrade opnieuw.

Oorzaak 6

De controller werkt mogelijk in Layer 2-modus.

Problemen oplossen

Voltooi deze stap:

Controleer de werking van de controller.

geconverteerde AP's ondersteunen alleen Layer 3 ontdekking. geconverteerde AP's ondersteunen Layer 2-ontdekking niet.

Resolutie

Voer de volgende stappen uit:

1. Stel de WLC in op Layer 3.
2. Herstart en geef de AP Manager interface een IP adres in zelfde Subnet als de beheersinterface.Als u een servicepoort hebt, zoals de servicepoort op een 4402 of 4404, moet u deze in een andere supernet hebben dan de AP manager en de beheerinterfaces.

Oorzaak 7

U ziet deze fout tijdens de upgrade:

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

Problemen oplossen

Wanneer u deze fout ziet, voert u de volgende stappen uit:

1. Controleer dat uw TFTP-server correct is geconfigureerd.Als u het upgrade-gereedschap gebruikt dat is ingesloten TFTP-server, is een gemeenschappelijke schuldige persoonlijke firewallsoftware, die het inkomende TFTP blokkeert.
2. Controleer of u het juiste beeld voor de upgrade gebruikt.De upgrade naar lichtgewicht modus heeft een speciale afbeelding nodig en werkt niet met de normale upgradeafbeeldingen.

Oorzaak 8

U ontvangt deze foutmelding op het AP na de conversie:

```
*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
```

AP herlaadt na 30 seconden en start het proces opnieuw.

Resolutie

Voltooi deze stap:

Je hebt een SSC AP. Zodra u hebt geconverteerd naar LWAPP AP, voegt u het SSC en het MAC-adres toe onder de AP-verificatielijst in de controller.

Tips voor probleemoplossing

Deze tips kunnen worden gebruikt bij het upgraden van autonome naar LWAPP-modus:

- Als NVRAM niet wordt gewist wanneer de controller na de conversie naar hem probeert te schrijven, worden er problemen veroorzaakt. Cisco raadt aan de configuratie te verwijderen voordat u AP naar LWAPP converteert. Zo verwijdert u de configuratie:Van de IOS GUI—Ga naar **systeemsoftware > Systeemconfiguratie > Terugzetten op standaardwaarden** of **Terugzetten op standaardwaarden behalve IP**.Van CLI - geef de opdrachten **voor het wissen** en **herladen** van de **schrijfmachine** aan bij CLI en laat de configuratie niet op wanneer dit wordt gevraagd.Dit maakt ook het tekstbestand van APs dat door het upgrade-gereedschap moet worden geconverteerd eenvoudiger om te maken wanneer de items <ip-adres>, Cisco, Cisco worden.
- Cisco raadt aan dat u tftp32 gebruikt. U kunt de nieuwste TFTP-server downloaden op http://tftpd32.jounin.net/ .
- Als een firewall of een toegangscontrolelijst tijdens het upgradeproces is ingeschakeld, kan het upgradegereedschap niet meer in staat zijn het bestand te kopiëren dat omgevingsvariabelen van een werkstation naar een AP bevat.Als een firewall of toegangscontrolelijst de kopieerhandeling blokkeert en u de optie Upgradegereedschap TFTP Server gebruiken selecteert, kunt u niet met de upgrade doorgaan omdat het gereedschap de omgevingsvariabelen niet kan bijwerken en het uploaden van de afbeelding naar de AP niet lukt.
- Controleer het beeld dat u wilt upgraden. De upgrade van IOS op LWAPP-afbeeldingen is anders dan de normale IOS-afbeeldingen.Controleer onder Mijn documenten/Mijn computer -> Gereedschappen -> Mapopties, of u de **bestandsextensies** van **bekende bestandstypen** verwijdert.
- Zorg er altijd voor dat u het nieuwste upgrade-gereedschap en de upgrade-afbeelding gebruikt. De laatste versies zijn beschikbaar in het Wireless Software Center.
- AP kan geen **.tar** beeldbestand starten. Het is een archief, vergelijkbaar met zip-bestanden. U moet het **.tar-**bestand ontbundelen in een AP-flitser met de opdracht **downloaden** van het **archief**, of anders eerst de herkende afbeelding uit het tar-bestand halen en vervolgens de herkende afbeelding in een AP-flitser plaatsen.

Gerelateerde informatie

- Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode (Autonome Cisco Aironet access points upgraden naar de lichtgewichtmodus)
- De LWAPP-configuratie herstellen op een lichtgewicht AP (LAP)

- Configuratievoorbeeld van DHCP-optie 43 voor lichtgewicht Cisco Aironet access points
- Hoe de hash-toets van het access point te herstellen en in de controller te importeren
- Kan Cisco Aironet Autonoom access point worden geconverteerd naar Lichtgewicht access point Protocol (LWAPP) met behulp van de CLI
- Technische ondersteuning en documentatie – Cisco Systems