LWAPP升級工具故障排除提示

目錄

簡介

本文討論使用升級工具將自主存取點(AP)升級為輕量模式時可能會發生的一些關鍵問題。本文還提供有關如何糾正這些問題的資訊。

必要條件

需求

執行升級之前，AP必須執行Cisco IOS®軟體版本12.3(7)JA或更新版本。

思科控制器必須至少運行軟體版本3.1。

Cisco Wireless Control System(WCS)（如果使用）必須至少運行3.1版。

Windows 2000和Windows XP平台支援升級實用程式。必須使用其中一個Windows作業系統版本。

採用元件

本檔案中的資訊是根據這些存取點和無線LAN控制器。

支援此遷移的AP包括：

- 所有1121G接入點
- 所有1130AG存取點
- 所有1240AG存取點
- 所有1250系列存取點
- 對於所有基於IOS的1200系列模組化接入點（1200/1220 Cisco IOS軟體升級、1210和1230 AP）平台，它取決於無線電：如果支援802.11G、MP21G和MP31G如果支援802.11A、RM21A和RM22A1200系列接入點可使用任何支援的無線電組合進行升級：僅G、僅A或G和A。對於包含雙無線電的接入點，如果兩個無線電中的一個是受LWAPP支援的無線電的話，升級工具仍會執行升級。該工具會在詳細日誌中新增一條警告消息，指出哪些無線電不受支援。
- 所有1310 AG存取點
- 思科C3201無線行動介面卡(WMIC)**注意：**第二代802.11a無線電包含兩個部件號。

執行升級之前，存取點必須執行Cisco IOS版本12.3(7)JA或更新版本。

對於Cisco C3201WMIC，在執行升級之前，接入點必須運行Cisco IOS版本12.3(8)JK或更高版本。

這些思科無線LAN控制器支援升級到輕量模式的自治接入點：

- 2000系列控制器
- 2100系列控制器
- 4400系列控制器
- 適用於Cisco Catalyst 6500系列交換器的思科無線服務模組(WiSM)
- 思科28/37/38xx系列整合多業務路由器中的控制器網路模組
- Catalyst 3750G整合式無線LAN控制器交換器

思科控制器必須至少運行軟體版本3.1。

Cisco Wireless Control System(WCS)必須至少運行3.1版。Windows 2000和Windows XP平台支援升級實用程式。

您可以從思科軟體下載頁面下載最新版本的升級公用程式。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

升級過程 — 概述

使用者運行升級實用程式，該實用程式接受包含接入點及其憑證清單的輸入檔案。該實用程式通過遠端登入到輸入檔案中的接入點，通過一系列Cisco IOS命令來準備接入點以進行升級，其中包括建立自簽名證書的命令。此外，該實用程式還會通過遠端連線到控制器，對裝置進行程式設計，以允許對特定的自簽名證書接入點進行授權。接下來會將Cisco IOS軟體版本12.3(11)JX1載入存取點，以便其加入控制器。存取點加入控制器後，會從控制器下載完整的Cisco IOS版本。升級實用程式

生成一個輸出檔案，該檔案包括可以匯入到WCS管理軟體中的接入點清單和相應的自簽名證書金鑰雜湊值。然後WCS可以將此資訊傳送到網路上的其他控制器。

如需詳細資訊，請參閱將自治Cisco Aironet存取點升級為輕量模式的升級程式一節。

升級工具 — 基本操作

此升級工具用於將自治AP升級到輕量模式，前提是此AP與此升級相容。升級工具執行從自主模式升級到輕量模式所需的基本任務。這些任務包括：

- 基本條件檢查 — 驗證AP是否為受支援的AP、它是否運行最低軟體版本以及是否支援無線電型別。
- 確保AP已配置為根。
- 準備用於轉換的自治AP — 新增公鑰基礎設施(PKI)配置和證書層次結構，以便可對思科控制器進行AP身份驗證，並且可以為AP生成自簽名證書(SSC)。如果AP具有製造安裝證書(MIC)，則不使用SSC。
- 下載自主到輕量模式升級映像，例如12.3(11)JX1或12.3(7)JX，它允許AP加入控制器。成功下載後，此操作將重新啟動AP。
- 生成由AP MAC地址、證書型別和安全金鑰雜湊組成的輸出檔案，並自動更新控制器。輸出檔案可以匯入WCS並匯出到其他控制器。

重要附註

使用此實用程式之前，請考慮以下重要說明：

- 使用此工具轉換的接入點無法連線到40xx、41xx或3500控制器。
- 不能使用僅802.11b或第一代802.11a無線電升級接入點。
- 如果要在轉換和重新啟動後保留接入點的靜態IP地址、網路掩碼、主機名和預設網關，則必須在接入點上載入以下自主映像之一，然後才能將接入點轉換為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)JA212.3(8)JEA12.3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g)JA12.4(3g)JA1
- 如果從其中一個自治映像將接入點升級到LWAPP，則轉換後的接入點不會保留其靜態IP地址、網路掩碼、主機名和預設網關：12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- 升級過程完成後，LWAPP升級工具不會釋放Windows作業系統記憶體資源。只有在退出升級工具後，才會釋放記憶體資源。如果升級多個批次的存取點，必須在兩個批次之間退出該工具以釋放記憶體資源。如果在批處理之間不退出該工具，則由於記憶體消耗過多，升級工作站的效能會迅速降低。

憑證型別

有兩種不同的AP:

- 使用MIC的AP
- 需要具有SSC的AP

工廠安裝的證書由術語MIC引用，MIC是製造安裝證書的縮寫。在2005年7月18日之前出廠的Cisco Aironet接入點沒有MIC，因此這些接入點在升級為在輕量模式下運行時會建立自簽名證書。控制器被程式設計為接受自簽名證書以進行特定接入點的身份驗證。

您必須處理使用輕量型存取點通訊協定(LWAPP)的Cisco Aironet MIC AP（例如Aironet 1000 AP），並相應地排除故障。換句話說，請檢查IP連線，調試LWAPP狀態機，然後檢查加密。

升級工具日誌顯示AP是MIC AP還是SSC AP。以下是升級工具中詳細日誌的範例：

```
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
```

在此日誌中，突出顯示的行指定AP安裝有MIC。有關證書和升級過程的詳細資訊，請參閱將自治Cisco Aironet接入點升級到輕量模式的升級過程概述部分。

若是SSC AP，則控制器上不會建立任何憑證。升級工具讓AP生成Rivest、Shamir和Adelman(RSA)金鑰對，用於對自生成證書(SSC)進行簽名。 升級工具會向控制器驗證清單新增包含AP的MAC位址和公鑰雜湊的專案。控制器需要公鑰雜湊才能驗證SSC簽名。

如果尚未將該專案新增到控制器，請檢查輸出CSV檔案。每個AP都應該有條目。如果找到專案，請將該檔案匯入控制器。如果您使用控制器指令行介面(CLI)(使用**config auth-list**指令)或交換器網路，則一次必須匯入一個檔案。使用WCS，您可以將整個CSV檔案匯入為模板。

此外，請檢查管制範圍。

附註：如果您有LAP AP但需要Cisco IOS功能，則需要在其上載入自治Cisco IOS映像。反之，如果您有一個自治AP並希望將其轉換為LWAPP，則可以通過自治IOS安裝LWAPP恢復映像。

您可以使用MODE按鈕或CLI檔案下載命令完成更改AP**映像的**步驟。有關如何使用MODE按鈕映像重新載入的詳細資訊，請參閱故障排除，該按鈕用於自治IOS或名為AP型號預設檔名的恢復映像。

下一節將討論升級操作中常見的一些問題以及解決這些問題的步驟。

問題

症狀

AP未加入控制器。本文檔的解決方案部分按概率順序介紹了原因。

解決方案

使用此部分可以解決此問題。

原因1

AP無法通過LWAPP發現找到控制器，或AP無法到達控制器。

疑難排解

請完成以下步驟：

1. 在控制器CLI上發出**debug lwapp events enable**命令。查詢LWAPP發現>發現響應>加入請求>加入響應序列。如果您沒有看到LWAPP發現請求，則表示AP無法找到或找不到控制器。以下範例顯示從無線LAN控制器(WLC)成功應答到轉換的輕量AP(LAP)。 以下是**debug lwapp events enable**命令的輸出：

```
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. 檢查AP網路和控制器之間的IP連線。如果控制器和AP位於同一子網中，請確保它們正確連線。如果它們位於不同的子網中，請確保在它們之間使用路由器，並且這兩個子網之間的路由已正確啟用。
3. 驗證發現機制是否配置正確。如果使用域名系統(DNS)選項來發現WLC，請確保DNS伺服器已正確配置為將CISCO-LWAPP-CONTROLLER.local-domain對映到WLC IP地址。因此，如果AP可以解析名稱，它就會向解析的IP地址發出LWAPP加入消息。如果將選項43用作發現選項，請確保在DHCP伺服器上正確配置了該選項。有關發現過程和順序的詳細資訊，請參閱向WLC註冊LAP。有關如何配置DHCP選項43的詳細資訊，請參閱輕量Cisco Aironet接入點的DHCP選項43配置示例。**注意：請**記住，轉換靜態定址的AP時，唯一有效的第3層發現機制是DNS，因為靜態地址在升級期間會被保留。在AP上，可以發出**debug lwapp client events**命令和**debug ip udp**命令，以便接收足夠的資訊來確定實際發生的情況。您應該會看到使用者資料包通訊協定(UDP)封包序列，如下所示：來源為具有控制器管理介面IP的AP IP。從控制器

AP管理器IP到AP IP。源自AP IP到AP管理器IP的一系列資料包。**注意：**在某些情況下，可以有多個控制器，AP可能會嘗試根據LWAPP發現狀態機和演算法加入其他控制器。發生這種情況的原因可能是控制器執行的預設動態AP負載平衡。這種情況值得研究。**註：**以下是**debug ip udp**命令的**輸出示**例：

```
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
```

解析

請完成以下步驟：

1. 檢視手冊。
2. 修復基礎設施，使其正確支援LWAPP發現。
3. 將AP移動到與控制器相同的子網以填充它。
4. 如有必要，發出**lwapp ap controller ip address *A.B.C.D*** 命令，以便在AP CLI上手動設定控制器IP:此命令的*A.B.C.D*部分是WLC的管理介面IP地址。**注意：**此CLI命令可用於從未註冊到控制器的AP，或在加入先前控制器時更改了預設啟用密碼的AP。如需詳細資訊，請參閱在輕量AP(LAP)上重設LWAPP組態。

原因2

控制器時間超出了證書有效時間間隔。

疑難排解

請完成以下步驟：

1. 發出**debug lwapp errors enable**和**debug pm pki enable**命令。以下**debug**命令會顯示在AP和WLC之間傳遞的憑證訊息的偵錯。這些命令清楚地顯示一條消息，表明證書在有效間隔之外被拒絕。**注意：**請確保考慮到協調世界時(UTC)偏移。以下是控制器上**debug pm pki enable**指令的輸出：

```
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)
```

在此輸出中，注意突出顯示的資訊。此資訊清楚地顯示**控制器時間在AP的證書有效間隔之外**。因此，AP無法向控制器註冊。AP中安裝的證書具有預定義的有效期間隔。控制器時間的設定方式應使其在AP的證書有效性間隔內。

2. 從AP CLI發出**show crypto ca certificates**命令，以驗證AP中設定的證書有效時間間隔。範例如下：

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

整個輸出未列出，因為有許多有效間隔與此命令的輸出關聯。您只需要考慮關聯信任點指定的有效**時間間隔：Cisco_IOS_MIC_cert**在名稱欄位中具有相關AP名稱(**此處，名稱：C1200-001563e50c7e),**如本輸出示例所示。**這是要考慮的實際證書有效期間隔。**

3. 從控制器CLI發出**show time**指令，確認控制器上設定的日期和時間屬於此有效性間隔。如果控制器時間大於或小於此證書有效期間隔，請將控制器時間更改為在此間隔內。

解析

完成以下步驟：

在控制器GUI模式下選擇「**Commands > Set Time**」，或在控制器CLI中發出**config time**命令以設定控制器時間。

原因3

對於SSC AP，禁用SSC AP策略。

疑難排解

在這種情況下，您會在控制器上看到以下錯誤訊息：

```
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
```

請完成以下步驟：

執行以下兩個操作之一：

- 在控制器CLI上發出**show auth-list**命令，以檢查控制器是否已設定為接受具有SSC的AP。以下是**show auth-list**指令輸出的範例：

```
#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          12345678901234567890123456789012345678901
```

- 在GUI中選擇**Security > AP Policies**。

1. 檢查**Accept Self Signed Certificate**覈取方塊是否已啟用。如果不是，請啟用它。
2. 選擇**SSC**作為證書型別。
3. 使用MAC地址和金鑰雜湊將**AP**新增到授權清單。此金鑰雜湊可以從**debug pm pki enable** 命令的輸出中獲取。有關獲取金鑰雜湊值的資訊，請參閱原因4。

原因4

SSC公鑰雜湊錯誤或丟失。

疑難排解

請完成以下步驟：

1. 發出**debug lwapp events enable**命令。驗證AP是否嘗試加入。
2. 發出**show auth-list**指令。此命令顯示控制器儲存中的公鑰雜湊。
3. 發出**debug pm pki enable**命令。此命令顯示實際的公鑰雜湊。實際公鑰雜湊必須與控制器在儲存中的公鑰雜湊相匹配。差異導致問題。以下是此偵錯訊息的輸出範例：

```
(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
```

解析

請完成以下步驟：

1. 從**debug pm pki enable**命令輸出複製公鑰雜湊，並使用它來替換身份驗證清單中的公鑰雜湊。
2. 發出**config auth-list add ssc** ***AP_MAC AP_key*** 命令，以將AP MAC位址和金鑰雜湊新增到授權清單：以下是此命令的範例：

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

原因5

AP上的證書或公鑰損壞。

疑難排解

完成以下步驟：

發出**debug lwapp errors enable**和**debug pm pki enable**命令。

您會看到指示證書或金鑰已損壞的消息。

解析

使用以下兩個選項之一以解決問題：

- MIC AP — 請求退貨授權(RMA)。
- SSC AP — 降級到Cisco IOS軟體版本12.3(7)JA。完成以下步驟即可降級：

1. 使用重置按鈕選項。
2. 清除控制器設定。
3. 再次運行升級。

原因6

控制器可能在第2層模式下工作。

疑難排解

完成以下步驟：

檢查控制器的操作模式。

轉換後的AP僅支援第3層發現。轉換後的AP不支援第2層發現。

解析

請完成以下步驟：

1. 將WLC設定為第3層模式。
2. 重新啟動並為AP管理器介面分配與管理介面處於同一子網中的IP地址。如果您有服務埠（如4402或4404上的服務埠），則應將其置於與AP管理器和管理介面不同的超網中。

原因7

升級期間會顯示以下錯誤：

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

疑難排解

看到此錯誤時，請完成以下步驟：

1. 驗證您的TFTP伺服器是否配置正確。如果您使用嵌入的TFTP伺服器升級工具，則常見罪魁禍首是個人防火牆軟體，它會阻止傳入的TFTP。
2. 檢查您是否使用正確的映像進行升級。升級到輕量級模式需要特殊映像，無法使用普通升級映像。

原因8

轉換後，您在AP上收到以下錯誤消息：

```
*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在30秒後重新載入，然後再次開始該過程。

解析

完成以下步驟：

您有一個SSC AP。轉換為LWAPP AP後，請在控制器的AP身份驗證清單下新增SSC及其MAC地址。

疑難排解提示

從自主模式升級到LWAPP模式時可以使用以下提示：

- 如果在轉換後控制器嘗試寫入時未清除NVRAM，則會導致問題。思科建議在將AP轉換為LWAPP之前清除配置。若要清除組態：在IOS GUI中 — 轉到**System Software > System Configuration > Reset to Defaults**或**Reset to Defaults Except IP**。在CLI上 — 在CLI上發出**write erase**和**reload**命令，並在系統提示時不允許儲存配置。這也使升級工具要轉換的AP的文本檔案更易於建立，因為條目變成<ip address>、Cisco、Cisco、Cisco。
- 思科建議您使用tftp32。您可以從http://tftpd32.jounin.net/ 下載最新的TFTPD伺服器。
- 如果在升級過程中啟用防火牆或訪問控制清單，升級工具可能無法將包含環境變數的檔案從工作站複製到AP。如果防火牆或訪問控制清單阻止複製操作，並且您選擇使用升級工具TFTP伺服器選項，則無法繼續升級，因為該工具無法更新環境變數，並且上傳到AP的映像失敗。
- 仔細檢查您嘗試升級到的映像。從IOS升級到LWAPP映像的步驟不同於常規IOS映像。在「My Documents/My Computer—> Tools—> Folder Options（我的文檔/我的電腦 — >工具 — >資料夾選項）」下，確保取消選中「**Hide file extensions for known file types**(隱藏已知檔案型別的副檔名)」覈取方塊。
- 請始終確保使用最新的可用升級工具和升級恢復映像。無線軟體中心提供最新版本。
- AP無法啟動**.tar映**像檔案。它是一個存檔檔案，類似於zip檔案。您需要使用**archive download**指令將**.tar**檔案解壓縮到AP快閃記憶體中，否則請先從tar檔案中取出可啟動映像，然後將可啟動映像放入AP快閃記憶體中。

相關資訊

- **將自治Cisco Aironet接入點升級到輕量模式**
- **重置輕量AP(LAP)上的LWAPP配置**
- **輕量型 Cisco Aironet 存取點的 DHCP 選項 43 組態範例**
- **如何從接入點恢復雜湊金鑰並將其匯入控制器**
- **是否可以使用CLI將Cisco Aironet自主接入點轉換為輕量接入點協定(LWAPP)**

- 技術支援與文件 - Cisco Systems