为LWAPP-Converted AP添加自签名证书手工到控制器

目录

简介

本文解释您能使用为了手工添加自签名证书的方法(SSCs)到Cisco无线LAN (WLAN)控制器(WLC)。

接入点(AP)的SSC在AP有权限注册的网络的所有WLCs应该存在。 通常，请应用SSC对在同样移动组的所有WLCs。 当SSC的新增内容对WLC的不通过升级工具时发生，您必须手工添加SSC到与使用的WLC在本文的步骤。 您也需要此步骤，当AP移动向不同的网络时或，当另外的WLCs被添加到现有的网络时。

您能辨别此问题，当轻量AP协议(LWAPP)时-已转换AP不联合对WLC。当您排除故障关联问题时，您看到这些输出，当您发出这些调试时：

- 当您发出**enable命令时调试下午的pki**，您看到：`(Cisco Controller) >debug pm pki enable Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode() Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744 Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744 Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: Mac Address in subject is 00:XX:XX:XX:XX Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: **Cert is issued by Cisco Systems.** Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: **SSC is not allowed by config; bailing...** Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: called with (nil) Thu Jan 26 20:22:50 2006: sshpmFreePublicKeyHandle: NULL argument.`

- 当您发出**debug lwapp events enable命令时**，您看到：`(Cisco Controller) >`**`debug lwapp errors enable`** `.... Thu Jan 26 20:23:27 2006: Received LWAPP DISCOVERY REQUEST from AP 00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1' Thu Jan 26 20:23:27 2006: Successful transmission of LWAPP Discovery-Response to AP 00:13:5f:f8:c3:70 on Port 1 Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to 06:0a:10:10:00:00 on port '1' Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca cert table Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode() Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Mac Address in subject is 00:14:6a:1b:32:1a` **`Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems. Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: SSC is not allowed by config; bailing... Thu Jan 26 20:23:27 2006: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:13:5f:f9:dc:b0. Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil) Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument. Thu Jan 26 20:23:27 2006: Unable to free public key for AP 00:13:5F:F9:DC:B0 Thu Jan 26 20:23:27 2006: spamDeleteLCB: stats timer not initialized for AP 00:13:5f:f9:dc:b0 Thu Jan 26 20:23:27 2006: spamProcessJoinRequest : spamDecodeJoinReq failed`**

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- WLC不包含升级工具生成的SSC。
- AP包含SSC。
- Telnet在WLC和AP启用。
- pre-LWAPP Cisco IOS软件编码最低版本在将升级的AP。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件3.2.116.21没有安装的SSC的思科2006 WLC
- 与SSC的Cisco Aironet 1230系列AP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在思科中集中化WLAN体系结构， AP在轻量级模式运行。一思科WLC的AP关联与使用LWAPP。LWAPP 是一种 Internet 工程任务组 (IETF) 草案协议，它定义了设置和路径验证操作以及运行时操作的控制消息传递。此外，LWAPP 也定义了数据流量的隧道机制。

轻量AP (LAP)发现与使用的一WLC LWAPP发现机制。LAP然后发送WLC LWAPP加入请求。WLC发送LAP允许LAP加入WLC的LWAPP加入答复。当LAP加入对WLC时， LAP下载WLC软件，如果在LAP的版本和WLC不配比。随后， LAP是完全受WLC的控制。

LWAPP通过一个安全密钥分配获取在AP和WLC之间的来控制通信。安全密钥分配要求已经在LAP和WLC的已配置X.509数字证书。出厂安装的证书可以通过术语"MIC"来标识，它是厂商预装证书 (Manufacturing Installed Certificate) 的缩写。在七月18前运送的Aironet AP， 2005年，没有MICs。因此，当他们在轻量级模式时，转换运行这些AP创建SSC。控制器被设定为接受 SSC，以便可以验证特定 AP 的身份。

这是升级进程：

1. 除他们的登录凭证之外，用户运行接受有AP和他们的IP地址列表的一个输入文件的升级工具。
2. 工具建立有AP的远程登录会话并且发送在输入文件的一系列的Cisco IOS软件命令为了准备升级的AP。这些include命令命令创建SSCs。并且，工具建立一远程登录会话以WLC为了编程设备允许特定SSC AP的授权。
3. 工具然后装载在AP上的Cisco IOS软件版本12.3(7)JX，以便AP能加入WLC。
4. 在AP加入WLC后， AP下载从WLC的一个完整Cisco IOS软件版本。升级工具生成包括AP和对应的SSC key-hash值列表可以导入到无线控制系统的输出文件(WCS)管理软件。
5. WCS能然后发送此信息到在网络的其他WLCs。

在AP加入WLC后，您能重新指定AP到在您的网络的所有WLC，如果需要。

找出SHA1密钥哈希

如果执行AP转换的计算机是可用的，您能从在Cisco升级工具目录的.csv文件获取安全散列算法1 (SHA1)密钥哈希。 如果.csv文件不可用，您能发出一**debug命令**在WLC为了获取SHA1密钥哈希。

完成这些步骤：

1. 打开AP并且连接它对网络。
2. 启用在WLC命令行界面(CLI)的调试。命令是**调试下午pki enable (event)**。(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 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
```

添加SSC到WLC

任务

本部分提供有关如何配置本文档所述功能的信息。

GUI 配置

完成从GUI的这些步骤：

1. 选择**安全> AP策略**并且点击**已启用**此外接受自签证书。
2. 选择从证书类型下拉菜单的**SSC**。
3. 输入AP和哈希密钥的MAC地址，并且单击**添加**。

CLI 配置

从 CLI 中完成以下这些步骤：

1. Enable (event)接受在WLC的自签证书。命令是**设置auth-list ap-policy ssc enable (event)**。
   `(Cisco Controller) >config auth-list ap-policy ssc enable`
2. 添加AP MAC地址并且切细密钥对authorization list。命令是**config auth-list add ssc AP_MAC AP_key**。`(Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

验证

使用本部分可确认配置能否正常运行。

GUI验证

完成这些步骤：

1. 在AP Policies窗口，请验证AP MAC地址和SHA1密钥哈希在AP Authorization list地区出现。
2. 在所有AP窗口，请验证所有AP注册与WLC。

CLI验证

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **显示验证管理列表**—显示AP authorization list。
- **显示ap摘要**—显示所有已连接AP摘要。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 无线 LAN 控制器 (WLC) 故障排除常见问题
- Cisco 无线 LAN 控制器配置指南 3.2 版
- 无线 LAN 控制器和轻量接入点基本配置示例
- 技术支持和文档 - Cisco Systems