A ferramenta de upgrade LWAPP pesquisa defeitos pontas

Índice

Introdução

Este documento discute alguns dos problemas principais que podem ocorrer ao se usar a ferramenta de atualização para atualizar pontos de acesso (APs) autônomos para o modo lightweight. Este documento também fornece informações sobre como solucionar esses problemas.

Pré-requisitos

Requisitos

Os APs devem executar a liberação 12.3(7)JA do Cisco IOS ® Software ou mais tarde antes que você possa executar a elevação.

Os controladores de Cisco devem executar um mínimo da versão de software 3.1.

Sistema de controle sem fio da Cisco (WCS) (se usado) deve executar um mínimo de versão 3.1.

A utilidade da elevação é apoiada nas Plataformas do Windows 2000 e do Windows XP. Qualquer uma destas versões do sistema operacional de Windows deve ser usada.

Componentes Utilizados

A informação neste documento é baseada nestes Access point e controladores do Wireless LAN.

Os APs que apoiam esta migração são:

- Todos os Access point 1121G
- Todos os Access point 1130AG
- Todos os Access point 1240AG
- Todos os Access point do 1250 Series
- Para todas as Plataformas com base em IOS do ponto de acesso modular do 1200 Series 1200/1220 de upgrade do Cisco IOS Software, 1210 e 1230 AP) (, depende do rádio:se 802.11G, MP21G e MP31G são apoiadosse 802.11A, RM21A e RM22A são apoiadosOs Access point do 1200 Series podem ser promovidos com toda a combinação de rádios apoiados: G somente, A somente, ou G e A. Para um Access point que contenha rádios duplos, se um dos dois rádios é um rádio LWAPP-apoiado, a ferramenta de upgrade ainda executa a elevação. A ferramenta adiciona um mensagem de advertência ao log detalhado que indica que rádio é unsupported.
- Todos os 1310 Access point AG
- Placa de interface móvel sem fio de Cisco C3201 (WMIC)**Nota:** Os rádios 802.11a de segunda geração contêm dois part numbers.

Os Access point devem executar o Cisco IOS Release 12.3(7)JA ou Mais Recente antes que você possa executar a elevação.

Para Cisco C3201WMIC, os Access point devem executar o Cisco IOS Release 12.3(8)JK ou Mais Recente antes que você possa executar a elevação.

Estes controladores de LAN do Cisco Wireless apoiam os Access point autônomos promovidos ao modo leve:

- Controladores do 2000 Series
- Controladores do 2100 Series
- Controladores do 4400 Series
- Módulos de serviços do Cisco Wireless (WiSMs) para Cisco Catalyst 6500 Series Switch
- Módulos de rede do controlador dentro do Roteadores dos Serviços integrados do 28/37/38xx Series de Cisco
- Switches integrado 3750G do controlador do Wireless LAN do catalizador

Os controladores de Cisco devem executar um mínimo da versão de software 3.1.

O Sistema de controle sem fio da Cisco (WCS) deve executar um mínimo de versão 3.1. A utilidade da elevação é apoiada nas Plataformas do Windows 2000 e do Windows XP.

Você pode transferir a versão a mais atrasada da utilidade da elevação da página das

transferências de software Cisco.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Processo de upgrade - Vista geral

O usuário executa uma utilidade da elevação que aceite um arquivo de entrada com uma lista de Access point e de suas credenciais. Os telnet de serviço público aos Access point no arquivo de entrada um a série de comandos cisco ios preparar o Access point para a elevação, que inclui os comandos criar os certificados auto-assinados. Também, os telnet de serviço público ao controlador para programar o dispositivo para permitir a autorização de Access point específicos do certificado auto-assinado. Carrega então o Cisco IOS Software Release 12.3(11)JX1 no Access point de modo que possa se juntar ao controlador. Depois que o Access point se junta ao controlador, transfere uma versão do Cisco IOS completa dele. A utilidade da elevação gerencie um arquivo de saída que inclua a lista de Access point e de valores correspondentes da chave-mistura do certificado auto-assinado que podem ser importados no software de gestão WCS. O WCS pode então enviar esta informação a outros controladores na rede.

Refira a seção do procedimento de upgrade de promover Access point autônomos do Cisco Aironet ao modo leve para mais informação.

Ferramenta de upgrade - Operação básica

Esta ferramenta de upgrade é usada para promover um AP autônomo ao modo leve forneceu o AP é compatível para esta elevação. A ferramenta de upgrade executa as tarefas básicas necessárias promover de autônomo ao modo leve. Estas tarefas incluem:

- Verificação básica da circunstância — Verifica se o AP é apoiado, se executa uma revisão mínima de software, e se os tipos de rádio estão apoiados.
- Certifique-se de que o AP está configurado como a raiz.
- Preparação do AP autônomo para a conversão — adiciona a configuração do Public Key Infrastructure (PKI) e a hierarquia do certificado de modo que a autenticação AP aos controladores de Cisco possa ocorrer, e os certificados auto-assinados (SSCs) possam ser gerados para o AP. Se o AP tem um certificado fabricação-instalado (MIC), a seguir SSCs não está usado.
- Transfere um autônomo à imagem de upgrade do modo leve, tal como 12.3(11)JX1 ou 12.3(7)JX, que permitem que o AP se junte a um controlador. Em uma transferência bem sucedida, isto recarrega o AP.
- Gerencie um arquivo de saída que consista em endereços AP MAC, no tipo do certificado, e em uma chave-mistura segura, e atualiza automaticamente o controlador. O arquivo de saída pode ser importado no WCS e ser exportado para outros controladores.

Observações importantes

Antes que você use esta utilidade, considere estas observações importantes:

- Os Access point convertidos com esta ferramenta não conectam a 40xx, a 41xx, ou a 3500 controladores.
- Você não pode promover Access point com 802.11b-only ou rádios da primeira geração 802.11a.
- Se você quer reter o endereço IP estático, o netmask, o hostname, e o gateway padrão dos Access point depois que a conversão e a repartição, você devem carregar uma destas imagens autônomas nos Access point antes que você abrigo os Access point a 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
- Se você promove Access point a LWAPP de uma destas imagens autônomas, os Access point convertidos não retêm seus endereço IP estático, netmask, hostname, e gateway padrão:12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- A ferramenta de upgrade LWAPP não libera recursos de memória do sistema operacional de Windows quando o processo de upgrade está completo. Os recursos de memória são liberados somente depois que você retira a ferramenta de upgrade. Se você promove diversos grupos de Access point, você deve retirar os grupos no meio da ferramenta para liberar recursos de memória. Se você não retira os grupos no meio da ferramenta, o desempenho da estação da elevação degrada rapidamente devido ao consumo da memória excessiva.

Tipos de Certificados

Há dois tipos diferentes dos APs:

- APs com um MIC
- APs que precisam de ter SSC

Os Certificados instalados fábrica são providos pelo termo MIC, que é um acrônimo para fabricar o certificado instalado. Os Access point do Cisco Aironet enviaram antes de julho 18, 2005, não têm o MIC, assim que estes Access point criam um certificado auto-assinado quando promovidos para operar-se no modo leve. Os controladores são programados aceitar certificados auto-assinados para a autenticação de Access point específicos.

Você deve tratar o Cisco Aironet MIC APs que usa o protocolo de pouco peso do Access point (LWAPP), como Aironet 1000 APs, e o pesquisa defeitos em conformidade. Ou seja verifique a conectividade IP, debugar a máquina de estado LWAPP, e verifique então o cripto.

Os logs da ferramenta de upgrade mostram-lhe se o AP é um MIC AP ou SSC AP. Este é um exemplo de um log detalhado da ferramenta de upgrade:

```
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
```

Neste log, a linha destacada especifica que o AP tem um MIC instalado com ele. Refira a seção de visão geral do processo de upgrade de promover Access point autônomos do Cisco Aironet ao modo leve para obter mais informações sobre dos Certificados e do processo de upgrade.

No caso de SSC APs, nenhum certificado é criado no controlador. A ferramenta de upgrade manda o AP gerar um par de chaves de Rivest, de Shamir, e de Adelman (RSA) que seja usado para assinar um certificado auto-gerado (SSC). A ferramenta de upgrade adiciona uma entrada à lista da autenticação do controlador com o MAC address do AP e da chave-mistura pública. O controlador precisa a chave-mistura pública a fim validar a assinatura de SSC.

Se a entrada não foi adicionada ao controlador, verifique o arquivo CSV da saída. Deve haver umas entradas para cada AP. Se você encontra a entrada, importe que arquivo no controlador. Se você usa o comando line interface(cli) do controlador (com uso do comando da autêntico-**lista da configuração**) ou a Web do interruptor, você deve importar um arquivo de cada vez. Com um WCS, você pode importar o arquivo CSV inteiro como um molde.

Também, verifique o domínio regulatório.

Nota: Se você manda um REGAÇO AP mas você querer a funcionalidade do Cisco IOS, você precisa de carregar uma imagem IOS Cisco autônoma nela. Inversamente, se você tem um AP autônomo e o quer o converter a LWAPP, você pode instalar uma imagem de recuperação LWAPP sobre IO autônomos.

Você pode terminar as etapas para mudar a imagem AP com o botão mode ou **comandos archive download** CLI. Refira a pesquisa de defeitos para obter mais informações sobre de como usar o reload da imagem do botão mode, que os trabalhos com IO autônomos ou a imagem de recuperação nomearam ao nome de arquivo do padrão do modelo AP.

A próxima seção discute algumas geralmente - das edições consideradas na operação da elevação e nas etapas para resolver estas edições.

Problema

Sintoma

O AP não se junta ao controlador. A seção das soluções deste original fornece as causas por ordem da probabilidade.

Soluções

Use esta seção para resolver este problema.

Causa 1

O AP não pode encontrar o controlador através da descoberta LWAPP, ou o AP não pode alcançar o controlador.

Troubleshooting

Conclua estes passos:

1. Emita o **comando debug lwapp events enable no** controlador CLI.Procure a resposta da descoberta LWAPP > da descoberta > juntam-se ao pedido > juntam-se à sequência da resposta. Se você não vê o pedido da descoberta LWAPP, significa que o AP não pode nem não encontra o controlador.Está aqui um exemplo de um bem sucedido JUNTA-SE À RESPOSTA do controlador do Wireless LAN (WLC) ao AP de pouco peso convertido (REGAÇO). Esta é a saída do **comando debug lwapp events enable**:

```
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. Verifique para ver se há a conectividade IP entre a rede AP e o controlador. Se o controlador e o AP residem na mesma sub-rede, assegure-se de que estejam interconectados corretamente. Se residem em sub-redes diferentes, assegure-se de que um roteador esteja usado entre elas e o roteamento esteja permitido corretamente entre as duas sub-redes.
3. Verifique que o mecanismo de descoberta está configurado corretamente.Se a opção do Domain Name System (DNS) é usada descobrindo o WLC, assegure-se de que o servidor DNS esteja configurado corretamente para traçar CISCO-LWAPP-CONTROLLER.local-domain com o IP address WLC. Daqui, se o AP pode resolver o nome, emite um juntar mensagem LWAPP ao IP address resolved.Se a opção 43 é usada como a opção de descoberta, assegure-se de que esteja configurada corretamente no servidor DHCP.Consulte para registrar o REGAÇO com o WLC para obter mais informações sobre do processo de descoberta e da sequência.Refira a OPÇÃO DE DHCP 43 para o exemplo de configuração de pouco peso dos Access point do Cisco Aironet para obter mais

informações sobre de como configurar a opção de DHCP 43.**Nota:** Recorde que quando você converter APs estático-endereçados, o único mecanismo de descoberta da camada 3 que funciona é o DNS porque o endereço estático é preservado durante a elevação.No AP, você pode emitir os **eventos de cliente do lwapp debugar** comanda e o **comando debug ip udp** a fim receber bastante informação para determinar exatamente o que ocorre. Você deve ver uma sequência do pacote do User Datagram Protocol (UDP) tal como este:Originado do IP AP com o IP da interface de gerenciamento do controlador.Originado do IP do gerente AP do controlador ao IP AP.Série de pacotes que é originado do IP AP ao IP do gerente AP.**Nota:** Em algumas situações, pode haver mais de um controlador e o AP puderam tentar se juntar a um controlador diferente com base na máquina de estado e nos algoritmos da descoberta LWAPP. Esta situação pôde ocorrer devido ao Balanceamento de carga dinâmico AP do padrão que o controlador executa. Esta situação pode vale o exame.**Nota:** Esta é umas saídas de exemplo do **comando 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
```

Resolução

Conclua estes passos:

1. Reveja o manual.
2. Fixe a infraestrutura de modo que apoie corretamente a descoberta LWAPP.
3. Mova o AP para a mesma sub-rede como o controlador a fim aprontá-lo.
4. Caso necessário, emita o *comando a.b.c.d do* ***IP address do controlador ap do lwapp*** a fim ajustar manualmente o IP do controlador no AP CLI:Este comando *A.B.C.D parte de* é o IP address da interface de gerenciamento do WLC.**Nota:** Este comando CLI pode ser usado em um AP que nunca se registre a um controlador, ou em um AP que mande seu padrão permitir a senha mudada quando juntado a um controlador precedente. Refira a restauração da configuração LWAPP em um AP de pouco peso (REGAÇO) para mais informação.

Causa 2

O tempo do controlador é fora do intervalo da validez do certificado.

Troubleshooting

Conclua estes passos:

1. Problemas dos comandos **debug lwapp errors enable** e debug pm pki enable.Estes **comandos debug** mostram debugar das mensagens do certificado que são passadas entre o AP e o WLC. Os comandos mostram claramente a uma mensagem que o certificado está rejeitado como fora do intervalo da validez.**Nota:** Certifique-se de levar em conta o deslocamento do Tempo Universal Coordenado (UTC).Esta é a saída do **comando debug pm pki enable no** controlador:

```
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)
```

   Nesta saída, observe a informação destacada. Esta informação mostra claramente que o **tempo do controlador é fora do intervalo da validez do certificado do AP**. Consequentemente, o AP não pode registrar-se com o controlador. Os Certificados instalados no AP têm um intervalo predefinido da validez. O tempo do controlador deve ser ajustado de tal maneira que está dentro do intervalo da validez do certificado do AP.
2. Emita o **comando show crypto ca certificates do** AP CLI a fim verificar o intervalo da validez

do certificado ajustado no AP.Este é um exemplo:

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

A saída inteira não é listada já que podem existir muitos intervalos de validade associados à saída desse comando. Você precisa considerar somente o intervalo de validade especificado pelo ponto de confiança associado: **Cisco_IOS_MIC_cert** com o nome relevante AP no campo de nome (**aqui, nome: C1200-001563e50c7e**), como destacado neste exemplo de emissor. **Esse é o intervalo de validade do certificado real a ser considerado.**

3. Emita o comando **show time** a partir da CLI do controlador para verificar se a data e a hora definidas no controlador estão dentro desse intervalo de validade.Se o tempo do controlador está acima ou abaixo deste intervalo da validez do certificado, a seguir mude o momento do controlador de cair dentro deste intervalo.

Resolução

Termine esta etapa:

Escolha **comandos > ajustam a hora no** modo GUI do controlador ou emitem o **comando time da configuração no** controlador CLI a fim ajustar o tempo do controlador.

Causa 3

Com SSC APs, a política de SSC AP é desabilitada.

Troubleshooting

Nesses casos, você vê este Mensagem de Erro no controlador:

```
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
```

Conclua estes passos:

Execute uma destas duas ações:

- Emita o comando da autêntico-**lista da mostra no** controlador CLI a fim verificar se o controlador esteja configurado para aceitar APs com SSCs.Esta é uma saída de amostra do comando da autêntico-**lista da mostra**:
  #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
  ```
- Escolha **Security > AP Policies** na GUI.

1. Verifique se a caixa de seleção **Accept Self Signed Certificate** está ativada. Se não estiver, ative-a.
2. Escolha **SSC** como o tipo de certificado.
3. Adicione o AP à lista de autorização com o endereço MAC e a chave hash.Essa chave hash pode ser obtida da saída do **comando debug pm pki enable**. Veja a causa 4 para obter informações sobre de obter o valor da chave-mistura.

Causa 4

A chave-mistura pública de SSC falta errada ou.

Troubleshooting

Conclua estes passos:

1. Emita o **comando debug lwapp events enable**.Verifique que o AP tenta se juntar.
2. Emita o comando **show auth-list** .Esse comando mostra a chave hash pública que o controlador tem em armazenamento.
3. Emita o **comando debug pm pki enable**.Esse comando mostra a chave hash pública real. A chave hash pública real deve corresponder à chave hash pública que o controlador tem em

armazenamento. Uma discrepância causa o problema. Esta é uma saída de exemplo dessa mensagem de depuração:

```
(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
```

Resolução

Conclua estes passos:

1. Copie a chave hash pública da saída do **comando debug pm pki enable** e use-a para substituir a chave hash pública na lista de autenticação.
2. Emita a autêntico-**lista da configuração adicionam o** comando do **ssc** ***AP_MAC AP_key*** a fim adicionar o MAC address e a chave-mistura AP à lista da autorização:Aqui está um exemplo deste comando:
```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Causa 5

Há uma corrupção do certificado ou da chave pública no AP.

Troubleshooting

Termine esta etapa:

Problemas dos comandos **debug lwapp errors enable** e debug pm pki enable.

Você vê mensagens que indicam os certificados ou as chaves que estão corrompidos.

Resolução

Use uma destas duas opções para resolver o problema:

- AP com MIC - Solicita uma autorização de materiais de retorno (RMA).
- SSC AP — Downgrade ao Cisco IOS Software Release 12.3(7)JA.Conclua estas etapas para fazer o downgrade:

1. Use a opção do botão de redefinição.
2. Limpe as configurações do controlador.
3. Execute a atualização novamente.

Cause 6

O controlador pôde trabalhar no modo da camada 2.

Troubleshooting

Termine esta etapa:

Verifique o modo de operação do controlador.

Os APs convertidos apenas suportam detecção na camada 3. Os AP convertidos não suportam detecção na camada 2.

Resolução

Conclua estes passos:

1. Defina o WLC para o modo de camada 3.
2. Recarregue e dê à relação do gerente AP um IP address na mesma sub-rede como a interface de gerenciamento.Se você tem uma porta do serviço, tal como a porta do serviço em uns 4402 ou em 4404, você deve tê-la em um super-rede diferente do que o gerente e interfaces de gerenciamento AP.

Causa 7

Você vê este erro durante a elevação:

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

Troubleshooting

Quando você vê este erro, termine estas etapas:

1. Verifique que seu servidor TFTP está configurado corretamente.Se você usa o servidor TFTP encaixado ferramenta de upgrade, um culpado comum é o software de firewall pessoal, que obstrui o TFTP entrante.
2. Verifique se você está usando a imagem correta para a elevação.A elevação ao modo leve exige uma imagem especial e não trabalha com as imagens de upgrade normais.

Causa 8

Você recebe este Mensagem de Erro no AP após a conversão:

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

O AP é recarregado após 30 segundos e inicia o processo novamente.

Resolução

Termine esta etapa:

Você tem um AP com SSC. Uma vez que você converte a LWAPP AP, adicionar SSC e seu MAC address sob a lista da autenticação AP no controlador.

Pesquise defeitos pontas

Estas pontas podem ser usadas quando você promove de autônomo ao modo LWAPP:

- Se o NVRAM não é cancelado quando o controlador tenta lhe escrever após a conversão, os problemas estão causados. Cisco recomenda cancelar a configuração antes que você converta um AP a LWAPP. A fim cancelar a configuração:Dos IO GUI — Vá ao **software do sistema > à configuração de sistema > restaurado aos padrões**, ou **restaure aos padrões exceto o IP**.Do CLI — Emita o **erase** e os **comandos reload da escrita no** CLI e não permita que a configuração sido salvar quando alertado.Isto igualmente faz o arquivo de texto dos APs a ser convertidos pela ferramenta de upgrade mais simples criar como as entradas se transformam < IP address >, Cisco, Cisco, Cisco.
- Cisco recomenda que você usa o tftp32. Você pode transferir o server o mais atrasado TFTPD em http://tftpd32.jounin.net/ .
- Se um Firewall ou um Access Control List são permitidos durante o processo de upgrade, a ferramenta de upgrade pode tornar-se incapaz de copiar o arquivo que contém variáveis ambientais de uma estação de trabalho a um AP.Se um Firewall ou o Access Control List obstruem a operação de cópia e você seleciona a opção do servidor TFTP da ferramenta de upgrade do uso, você não pode continuar com a elevação porque a ferramenta não pode atualizar os variáveis ambientais, e a transferência de arquivo pela rede da imagem ao AP falha.
- Verifique novamente a imagem que você está tentando promover a. A elevação dos IO às imagens LWAPP é diferente das imagens IOS normais.Sob meu computador Documents/My--> ferramentas--> as opções da pasta, certificam-se de você uncheck as **extensões de arquivo do couro cru para a** caixa de verificação **conhecida dos tipos de arquivo**.
- Certifique-se sempre usar a ferramenta de upgrade disponível a mais atrasada e promover a imagem de recuperação. As versões as mais atrasadas estão disponíveis no centro de software Wireless.
- Um AP não pode carreg um arquivo de imagem de **.tar**. É um arquivo, similar aos arquivos zip. Você precisa de unbundle o arquivo de **.tar no** flash AP com o **comando archive download**, ou então puxa a imagem inicializável fora do arquivo TAR primeiramente pôs então a imagem inicializável no flash AP.

Informações Relacionadas

- Atualização de Pontos de Acesso Autônomos Cisco Aironet para o Modo Lightweight
- Restaurando a configuração LWAPP em um AP de pouco peso (REGAÇO)
- Exemplo de configuração da OPÇÃO 43 do DHCP para os Pontos de Acesso Leves do Cisco Aironet.
- Como recuperar a chave da mistura fora do Access point e a importar no controlador
- Pode o Access point autônomo do Cisco Aironet ser convertido ao protocolo de pouco peso do Access point (LWAPP) que usa o CLI
- Suporte Técnico e Documentação - Cisco Systems