Dicas de solução de problemas da ferramenta de atualização LWAPP

Contents

Introduction

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.

Prerequisites

Requirements

Os APs devem executar o Cisco IOS® Software Release 12.3(7)JA ou posterior para que você possa executar a atualização.

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

O Cisco Wireless Control System (WCS) (se usado) deve executar no mínimo a versão 3.1.

O utilitário de atualização é suportado nas plataformas Windows 2000 e Windows XP. Qualquer uma dessas versões do sistema operacional Windows deve ser usada.

Componentes Utilizados

As informações neste documento são baseadas nesses pontos de acesso e controladores de LAN sem fio.

Os APs que suportam essa migração são:

- Todos os access points 1121G
- Todos os access points 1130AG
- Todos os access points 1240AG
- Todos os access points série 1250
- Para todas as plataformas de access point modular 1200 series baseadas em IOS (1200/1220 Cisco IOS Software Upgrade, 1210 e 1230 AP), depende do rádio:se 802.11G, MP21G e MP31G forem compatíveisse 802.11A, RM21A e RM22A forem suportadosOs pontos de acesso da série 1200 podem ser atualizados com qualquer combinação de rádios compatíveis: G apenas, A apenas, ou G e A. Para um ponto de acesso que contém rádios duplos, se um dos dois rádios for um rádio compatível com LWAPP, a ferramenta de atualização ainda executará a atualização. A ferramenta adiciona uma mensagem de aviso ao registro detalhado que indica qual rádio não é suportado.
- Todos os access points 1310 AG
- Placa de interface móvel sem fio (WMIC) Cisco C3201**Nota:** Os rádios 802.11a de segunda geração contêm dois números de peça.

Os pontos de acesso devem executar o Cisco IOS versão 12.3(7)JA ou posterior para que você possa realizar a atualização.

Para o Cisco C3201WMIC, os pontos de acesso devem executar o Cisco IOS versão 12.3(8)JK ou posterior para que você possa fazer a atualização.

Esses controladores de LAN sem fio da Cisco suportam pontos de acesso autônomos atualizados para o modo lightweight:

- Controladores série 2000
- Controladores série 2100
- Controladores série 4400
- Cisco Wireless Services Modules (WiSMs) para switches Cisco Catalyst 6500 Series
- Controlador de módulos de rede nos Integrated Services Routers da Cisco série 28/37/38xx
- Switches de controlador de LAN sem fio integrados Catalyst 3750G

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

O Cisco Wireless Control System (WCS) deve executar no mínimo a versão 3.1. O utilitário de atualização é suportado nas plataformas Windows 2000 e Windows XP.

Você pode baixar a versão mais recente do utilitário de atualização na página Downloads de

software da Cisco.

Conventions

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

Processo de atualização - Visão geral

O usuário executa um utilitário de atualização que aceita um arquivo de entrada com uma lista de pontos de acesso e suas credenciais. O utilitário faz telnet para os pontos de acesso no arquivo de entrada com uma série de comandos do Cisco IOS para preparar o ponto de acesso para a atualização, que inclui os comandos para criar os certificados autoassinados. Além disso, o utilitário faz telnet para o controlador para programar o dispositivo para permitir autorização de pontos de acesso específicos de certificado autoassinado. Em seguida, ele carrega o Cisco IOS Software Release 12.3(11)JX1 no ponto de acesso para que possa ingressar no controlador. Depois que o access point ingressa no controlador, ele faz o download de uma versão completa do Cisco IOS a partir dele. O utilitário de atualização gera um arquivo de saída que inclui a lista de pontos de acesso e os valores de hash de chave de certificado autoassinado correspondentes que podem ser importados para o software de gerenciamento do WCS. O WCS pode então enviar essas informações para outros controladores na rede.

Consulte a seção Procedimento de Upgrade de Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode para obter mais informações.

Ferramenta de atualização - Operação básica

Essa ferramenta de atualização é usada para atualizar um AP autônomo para o modo lightweight, desde que o AP seja compatível com essa atualização. A ferramenta de atualização executa as tarefas básicas necessárias para atualizar do modo autônomo para o modo lightweight. Essas tarefas incluem:

- Verificação de condição básica—Verifica se o AP é suportado, se executa uma revisão mínima de software e se os tipos de rádio são suportados.
- Verifique se o AP está configurado como Raiz.
- Preparação do AP autônomo para conversão—Adiciona a configuração de PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) e a hierarquia de certificado para que a autenticação de AP para os controladores Cisco possa ocorrer, e certificados autoassinados (SSCs) podem ser gerados para o AP. Se o AP tiver um certificado instalado na fábrica (MIC), os SSCs não serão usados.
- Faz o download de uma imagem de atualização autônoma para modo leve, como 12.3(11)JX1 ou 12.3(7)JX, que permite que o AP ingresse em uma controladora. Em um download bem-sucedido, isso reinicializa o AP.
- Gera um arquivo de saída que consiste em endereços MAC do AP, o tipo de certificado e uma chave hash segura e atualiza automaticamente o controlador. O arquivo de saída pode ser importado no WCS e exportado para outros controladores.

Notas importantes

Antes de usar este utilitário, considere estas notas importantes:

- Os pontos de acesso convertidos com esta ferramenta não se conectam aos controladores 40xx, 41xx ou 3500.
- Não é possível atualizar pontos de acesso com rádios 802.11b apenas ou 802.11a de primeira geração.
- Se quiser manter o endereço IP estático, a máscara de rede, o nome do host e o gateway padrão dos pontos de acesso após a conversão e a reinicialização, você deve carregar uma dessas imagens autônomas nos pontos de acesso antes de cobrir os pontos de acesso para o 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 atualizar pontos de acesso para o LWAPP a partir de uma dessas imagens autônomas, os pontos de acesso convertidos não retêm seu endereço IP estático, máscara de rede, nome do host e gateway padrão:12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- A ferramenta de atualização LWAPP não libera os recursos de memória do sistema operacional Windows quando o processo de atualização está concluído. Os recursos de memória são liberados somente após você sair da ferramenta de atualização. Se você atualizar vários lotes de pontos de acesso, deve sair da ferramenta entre lotes para liberar recursos de memória. Se você não sair da ferramenta entre lotes, o desempenho da estação de atualização diminui rapidamente devido ao consumo excessivo de memória.

Tipos de certificados

Há dois tipos diferentes de APs:

- APs com MIC
- APs que precisam ter um SSC

Os certificados instalados de fábrica são referenciados pelo termo MIC, que é um acrônimo para Manufacturing Installed Certificate. Os pontos de acesso Cisco Aironet enviados antes de 18 de julho de 2005 não possuem MIC, portanto esses pontos de acesso criam um certificado autoassinado quando atualizados para operar no modo lightweight. Os controladores são programados para aceitar certificados autoassinados para autenticação de pontos de acesso específicos.

Você deve tratar os APs Cisco Aironet MIC que usam LWAPP (Lightweight Access Point Protocol), como APs Aironet 1000, e solucionar problemas de acordo. Em outras palavras, verifique a conectividade IP, debugue a máquina de estado LWAPP e verifique a criptografia.

Os registros da ferramenta de atualização mostram se o AP é um AP MIC ou AP SSC. Este é um exemplo de um log detalhado da ferramenta de atualização:

```
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 registro, a linha realçada especifica que o AP tem um MIC instalado com ele. Consulte a seção Visão geral do processo de atualização de Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode para obter mais informações sobre os certificados e o processo de atualização.

No caso dos APs SSC, nenhum certificado é criado no controlador. A ferramenta de atualização faz com que o AP gere um par de chaves Rivest, Shamir e Adelman (RSA) usado para assinar um certificado gerado automaticamente (o SSC). A ferramenta de atualização adiciona uma entrada à lista de autenticação do controlador com o endereço MAC do AP e a chave hash pública. O controlador precisa da chave hash pública para validar a assinatura SSC.

Se a entrada não tiver sido adicionada ao controlador, verifique o arquivo CSV de saída. Deve haver entradas para cada AP. Se encontrar a entrada, importe esse arquivo para a controladora. Se você usar a interface de linha de comando (CLI) do controlador (com o uso do comando **config auth-list**) ou a Web do switch, será necessário importar um arquivo de cada vez. Com um WCS, você pode importar o arquivo CSV inteiro como um modelo.

Além disso, verifique o domínio regulatório.

Note: Se você tem um AP LAP, mas deseja a funcionalidade do Cisco IOS, você precisa carregar uma imagem do Cisco IOS autônomo nele. Por outro lado, se você tiver um AP autônomo e quiser convertê-lo para o LWAPP, poderá instalar uma imagem de recuperação do LWAPP sobre o IOS autônomo.

Você pode concluir as etapas para alterar a imagem do AP com o botão MODE ou os comandos **de download do arquivo** CLI. Consulte Troubleshooting para obter mais informações sobre como usar o recarregamento de imagem do botão MODE, que funciona com IOS autônomo ou imagem de recuperação nomeada para o nome de arquivo padrão do modelo AP.

A próxima seção discute alguns dos problemas mais comuns observados na operação de atualização e as etapas para resolver esses problemas.

Problema

Sintoma

O AP não ingressa no controlador. A seção Soluções deste documento fornece as causas em ordem de probabilidade.

Soluções

Use esta seção para resolver este problema.

Causa 1

O AP não consegue localizar o controlador através da descoberta LWAPP ou o AP não consegue alcançar o controlador.

Troubleshoot

Conclua estes passos:

1. Emita o comando **debug lwapp events enable** na CLI do controlador.Procure a descoberta do LWAPP > resposta de descoberta > solicitação de união > sequência de resposta de união. Se você não vir a solicitação de descoberta LWAPP, significa que o AP não pode ou não encontra a controladora.Aqui está um exemplo de uma RESPOSTA JOIN bem-sucedida do Wireless LAN Controller (WLC) para o Lightweight AP (LAP) convertido. 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 a conectividade IP entre a rede AP e o controlador. Se o controlador e o AP residirem na mesma sub-rede, certifique-se de que estejam interconectados corretamente. Se residirem em sub-redes diferentes, certifique-se de que um roteador seja usado entre elas e que o roteamento esteja ativado corretamente entre as duas sub-redes.
3. Verifique se o mecanismo de descoberta está configurado corretamente.Se a opção Domain Name System (DNS) for usada para descobrir a WLC, certifique-se de que o servidor DNS esteja configurado corretamente para mapear CISCO-LWAPP-CONTROLLER.local-domain com o endereço IP da WLC. Portanto, se o AP puder resolver o nome, ele emitirá uma mensagem de união LWAPP para o endereço IP resolvido.Se a opção 43 for usada como a

opção de descoberta, certifique-se de que ela esteja configurada corretamente no servidor DHCP.Consulte Registrar o LAP com a WLC para obter mais informações sobre o processo e a sequência de descoberta.Consulte DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example para obter mais informações sobre como configurar a opção de DHCP 43.**Observação:** lembre-se de que quando você converte APs endereçados estaticamente, o único mecanismo de descoberta de Camada 3 que funciona é o DNS porque o endereço estático é preservado durante a atualização.No AP, você pode emitir o comando **debug lwapp client events** e o comando **debug ip udp** para receber informações suficientes para determinar exatamente o que ocorre. Você deve ver uma sequência de pacotes UDP (User Datagram Protocol) como esta:Originado do IP do AP com o IP da interface de gerenciamento do controlador.Originado do IP do gerenciador de AP do controlador para o IP do AP.Série de pacotes originados do IP do AP para o IP do gerenciador do AP.**Observação:** em algumas situações, pode haver mais de um controlador e o AP pode tentar se unir a um controlador diferente com base na máquina e nos algoritmos do estado de descoberta do LWAPP. Essa situação pode ocorrer devido ao balanceamento de carga do AP dinâmico padrão executado pelo controlador. Esta situação pode ser apreciada.**Observação:** este é um exemplo de saída 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. Corrija a infraestrutura de modo que ela suporte corretamente a descoberta do LWAPP.
3. Mova o AP para a mesma sub-rede do controlador para carregá-lo primeiro.
4. Se necessário, execute o comando **lwapp ap controller ip address *A.B.C.D*** para definir manualmente o IP do controlador na CLI do AP:A parte *A.B.C.D* desse comando é o endereço IP da interface de gerenciamento da WLC.**Observação:** esse comando CLI pode ser usado em um AP que nunca se registrou em um controlador ou em um AP que teve sua senha de ativação alterada enquanto ingressou em um controlador anterior. Consulte Redefinição da configuração do LWAPP em um LAP (Lightweight AP) para obter mais informações.

Causa 2

A hora do controlador está fora do intervalo de validade do certificado.

Troubleshoot

Conclua estes passos:

1. Problemas dos comandos **debug lwapp errors enable e debug pm pki enable.**Esses comandos **debug** mostram a depuração de mensagens de certificado que são passadas entre o AP e a WLC. Os comandos mostram claramente uma mensagem de que o certificado é rejeitado como fora do intervalo de validade.**Observação:** certifique-se de considerar o deslocamento de 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 as informações realçadas. Essas informações mostram claramente

que a **hora do controlador está fora do intervalo de validade do certificado do AP**. Portanto, o AP não pode se registrar no controlador. Os certificados instalados no AP têm um intervalo de validade predefinido. A hora do controlador deve ser definida de forma que esteja dentro do intervalo de validade do certificado do AP.

2. Emita o comando **show crypto ca certificate** da CLI do AP para verificar o intervalo de validade do certificado definido 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 do AP relevante no campo de nome (**Aqui, Nome: C1200-001563e50c7e**), como destacado neste exemplo de saída. **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 a hora da controladora estiver acima ou abaixo desse intervalo de validade do certificado, altere a hora da controladora para se enquadrar nesse intervalo.

Resolução

Conclua esta etapa:

Escolha **Commands > Set Time** no modo de GUI do controlador ou emita o comando **config time** na CLI do controlador para definir a hora do controlador.

Causa 3

Com APs do SSC, a política de AP do SSC fica desativada.

Troubleshoot

Nesses casos, você verá esta mensagem de erro na controladora:

```
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 **show auth-list** na CLI da controladora para verificar se a controladora está configurada para aceitar APs com SSCs.Este é um exemplo de saída do comando **show auth-list**:

```
#show auth-list


Authorize APs against AAA ..... disabled

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


Mac Addr                  Cert Type    Key Hash

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

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

- Selecione **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.** Consulte a Causa 4 para obter informações sobre como obter o valor de hash de chave.

Causa 4

Chave hash pública SSC está errada ou ausente.

Troubleshoot

Conclua estes passos:

1. Emita o **comando debug lwapp events enable.**Verifique se o AP tenta ingressar.
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 o comando **config auth-list add ssc** ***AP_MAC AP_key*** para adicionar o endereço MAC do AP e a chave hash à lista de 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.

Troubleshoot

Conclua 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).
- AP SSC—Downgrade para o 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.

Causa 6

O controlador pode estar trabalhando no modo de camada 2.

Troubleshoot

Conclua 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. Reinicialize e forneça à interface do gerenciador de AP um endereço IP na mesma sub-rede da interface de gerenciamento.Se você tiver uma porta de serviço, como a porta de serviço em um 4402 ou 4404, deverá tê-la em uma super-rede diferente do gerenciador de AP e das interfaces de gerenciamento.

Causa 7

Este erro ocorre durante a atualização:

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

Troubleshoot

Quando este erro aparecer, faça o seguinte:

1. Verifique se o servidor TFTP está configurado corretamente.Se você usa o servidor TFTP incorporado da ferramenta de atualização, um culpado comum é o software de firewall pessoal, que bloqueia o TFTP recebido.
2. Verifique se você está usando a imagem correta para a atualização.A atualização para o modo lightweight exige uma imagem especial e não funciona com as imagens normais de atualização.

Causa 8

Você recebe esta mensagem de erro no AP após a conversão:

```
*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
```

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

Resolução

Conclua esta etapa:

Você tem um AP com SSC. Depois de converter para o AP LWAPP, adicione o SSC e seu endereço MAC na lista de Autenticação do AP no controlador.

Dicas de solução de problemas

Essas dicas podem ser usadas ao atualizar do modo autônomo para o modo LWAPP:

- Se a NVRAM não for limpa quando o controlador tentar gravar nele após a conversão, os problemas serão causados. A Cisco recomenda limpar a configuração antes de converter um AP em LWAPP. Para limpar a configuração:Na GUI do IOS—Vá para **System Software > System Configuration > Reset to Defaults** ou **Reset to Defaults Exceto IP**.Da CLI—Emita os comandos **write erase** e **reload** na CLI e não permita que a configuração seja salva quando solicitado.Isso também torna o arquivo de texto dos APs a serem convertidos pela ferramenta de atualização mais simples de criar à medida que as entradas se tornam <ip address>,Cisco,Cisco,Cisco.
- A Cisco recomenda que você use o tftp32. Você pode baixar o servidor TFTPD mais recente em http://tftpd32.jounin.net/ .
- Se um firewall ou uma lista de controle de acesso estiver habilitada durante o processo de atualização, a ferramenta de atualização poderá se tornar incapaz de copiar o arquivo que contém variáveis ambientais de uma estação de trabalho para um AP.Se um firewall ou lista de controle de acesso bloqueia a operação de cópia e você seleciona a opção Usar servidor TFTP da Ferramenta de Atualização, você não poderá prosseguir com a atualização porque a ferramenta não pode atualizar as variáveis ambientais e o carregamento da imagem para o AP falhará.
- Verifique duas vezes a imagem para a qual você está tentando atualizar. A atualização das imagens do IOS para o LWAPP é diferente das imagens normais do IOS.Em Meus documentos/Meu computador—> Ferramentas—> Opções de pasta, certifique-se de desmarcar a caixa de seleção **Ocultar extensões de arquivo para tipos de arquivo conhecidos**.
- Sempre certifique-se de usar a ferramenta de atualização e a imagem de recuperação de atualização mais recentes disponíveis. As versões mais recentes estão disponíveis no Wireless Software Center.
- Um AP não pode inicializar um arquivo de imagem **.tar**. É um arquivo, semelhante a arquivos zip. Você precisa desagrupar o arquivo **.tar** na flash do AP com o comando **archive download**, ou então puxe a imagem inicializável do arquivo tar primeiro e, em seguida, coloque a imagem inicializável na flash do AP.

Informações Relacionadas

- Atualização de access points autônomos Cisco Aironet para o modo Lightweight
- Redefinição da configuração do LWAPP em um AP leve (LAP)
- Exemplo de configuração da OPÇÃO 43 do DHCP para os Pontos de Acesso Leves do Cisco Aironet.

- Como recuperar a chave hash do ponto de acesso e importá-la para o controlador
- O ponto de acesso autônomo Cisco Aironet pode ser convertido para o LWAPP (Lightweight Access Point Protocol) usando a CLI?
- Suporte Técnico e Documentação - Cisco Systems