Consejos de Troubleshooting de la Herramienta de Upgrade de LWAPP

Contenido

Introducción

En este documento se describen algunos de los principales problemas que pueden surgir al utilizar la herramienta de upgrade para hacer un upgrade de puntos de acceso (APs) autónomos al modo ligero. El documento también proporciona información sobre cómo solucionar estos problemas.

prerrequisitos

Requisitos

Para poder realizar el upgrade, los APs deben ejecutar Cisco IOS® Software Release 12.3(7)JA o posterior.

Los controladores de Cisco deben ejecutar como mínimo la versión 3.1 del software.

Cisco Wireless Control System (WCS) (si se utiliza) debe ejecutar como mínimo la versión 3.1.

La utilidad de upgrade es compatible con las plataformas Windows 2000 y Windows XP. Hay que utilizar una de estas versiones del sistema operativo Windows.

Componentes Utilizados

La información de este documento se basa en estos puntos de acceso y controladores de LAN inalámbrica.

Los APs que soportan esta migración son:

- Todos los Puntos de acceso 1121G
- Todos los puntos de acceso de la serie 1130AG
- Todos los puntos de acceso de la serie 1240AG
- Todos los puntos de acceso de la serie 1250
- Para todas las plataformas de punto de acceso modular de la serie 1200 basadas en IOS (Upgrade de Cisco IOS Software 1200/1220, 1210 y 1230 AP), depende de la radio:si se soportan 802.11G, MP21G y MP31Gsi se soportan 802.11A, RM21A y RM22ASe puede hacer un upgrade de los puntos de acceso de la serie 1200 con cualquier combinación de radios soportadas: G solamente, A solamente, o G y A. Para un punto de acceso que contenga radios duales, si una de las dos radios es una radio soportada por LWAPP, la herramienta de upgrade efectuará el upgrade. La herramienta añade un mensaje de advertencia al log detallado que indica qué radio no se soporta.
- Todos los puntos de acceso de la serie 1310 AG
- Cisco C3201 Wireless Mobile Interface Card (WMIC)**Nota:** Las radios 802.11a de segunda generación contienen dos números de parte.

Para poder realizar el upgrade, los puntos de acceso deben ejecutar Cisco IOS Release 12.3(7)JA o posterior.

Para poder realizar el upgrade con Cisco C3201WMIC, los puntos de acceso deben ejecutar Cisco IOS Release 12.3(8)JK o posterior.

Estos controladores de LAN inalámbrica de Cisco soportan puntos de acceso autónomos con un upgrade al modo ligero:

- Controladores de la serie 2000
- Controladores de la serie 2100
- Controladores de la serie 4400
- Cisco Wireless Services Modules (WiSMs) para Cisco Catalyst 6500 Series Switches
- Módulos de red de controlador en los Cisco 28/37/38xx Series Integrated Services Routers
- Switches de Controlador de LAN Inalámbrica Integrado Catalyst 3750G

Los controladores de Cisco deben ejecutar como mínimo la versión 3.1 del software.

Cisco Wireless Control System (WCS) debe ejecutar como mínimo la versión 3.1. La utilidad de upgrade es compatible con las plataformas Windows 2000 y Windows XP.

Puede descargar la versión más reciente de la utilidad de upgrade desde la página de Descargas

de Software de Cisco.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Proceso de Upgrade - Descripción General

El usuario ejecuta una utilidad de upgrade que acepta un archivo de entrada con una lista de puntos de acceso y sus credenciales. La utilidad envía mediante telnet una serie de comandos de Cisco IOS a los puntos de acceso especificados en el archivo de entrada para preparar el punto de acceso para el upgrade, que incluye los comandos para crear los certificados autofirmados. Además, la utilidad se conecta mediante telnet al controlador para programar el dispositivo a fin de permitir la autorización de puntos de acceso con certificado autofirmado específicos. A continuación, carga Cisco IOS Software Release 12.3(11)JX1 en el punto de acceso de modo que pueda unirse al controlador. Una vez que el punto de acceso se ha unido al controlador, descarga de éste una versión completa de Cisco IOS. La utilidad de upgrade genera un archivo de salida que incluye la lista de puntos de acceso y de valores hash de llave de certificado autofirmado correspondientes que se puede importar en el software de administración de WCS. El WCS puede enviar esta información a otros controladores de la red.

Refiera a la sección Procedimiento de Upgrade de Upgrade de los Puntos de Acceso Autónomos de Cisco Aironet al Modo Ligero para obtener más información.

Herramienta de Upgrade - Funcionamiento Básico

Esta herramienta de upgrade se utiliza para hacer un upgrade de un AP autónomo al modo ligero siempre que el AP sea compatible con este upgrade. La herramienta de upgrade realiza las tareas básicas necesarias para hacer el upgrade de modo autónomo a modo ligero. Entre estas tareas se incluyen:

- Verificación básica de estado: verifica si se soporta el AP, si ejecuta una revisión mínima del software y si se soportan los tipos de radio.
- Aseegurese que el AP está configurado como raíz.
- Preparación del AP autónomo para la conversión: añade la configuración de Public Key Infrastructure (PKI) y la jerarquía de certificados de modo que se pueda realizar la autenticación de AP en los controladores Cisco y se puedan generar los certificados autofirmados (SSCs) para el AP. Si el AP tiene un certificado (MIC) instalado de fábrica, no se utilizan SSCs.
- Descarga una Imagen de Upgrade de Modo Autónomo a Modo Ligero, como 12.3(11)JX1 ó 12.3(7)JX, que permite que el AP se una a un controlador. Si la descarga finaliza correctamente, se reinicia el AP.
- Genera un archivo de salida que consta de direcciones MAC del AP, el tipo de certificado, y un hash de llave segura, y actualiza automáticamente el controlador. El archivo de salida se puede importar en el WCS y se puede exportar a otros controladores.

Notas importantes

Antes de utilizar esta utilidad, tenga en cuenta estas notas importantes:

- Los puntos de acceso convertidos con esta herramienta no se conectan a controladores 40xx, 41xx o 3500.
- No puede hacer un upgrade de puntos de acceso con radios solamente 802.11b o 802.11a de primera generación.
- Si se desea conservar la dirección IP estática, la máscara de red, el nombre de host y el gateway predeterminado de los puntos de acceso después de la conversión y el reinicio, se debe cargar una de estas imágenes autónomas en los puntos de acceso antes de convertir los puntos de acceso 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
- Si se hace un upgrade de puntos de acceso a LWAPP a partir de una de estas imágenes autónomas, los puntos de acceso convertidos no conservarán su dirección IP estática, la máscara de red, el nombre de host y el gateway predeterminado:12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- La herramienta de upgrade de LWAPP no libera recursos de memoria del sistema operativo de Windows tras finalizar el proceso de upgrade. Los recursos de memoria solamente se liberan cuando se cierra la herramienta de upgrade. Si se hace un upgrade de varios lotes de puntos de acceso, hay que cerrar la herramienta entre lotes para liberar recursos de memoria. Si no cierra la herramienta entre lotes, el rendimiento de la estación de la upgrade se degradará rápidamente debido a un consumo excesivo de memoria.

Tipos de Certificados

Hay dos tipos distintos de APs:

- APs con MIC
- APs que necesitan un SSC

Los certificados instalados de fábrica se designan con el término MIC, las siglas de Manufacturing Installed Certificate (certificado instalado de fábrica). Los puntos de acceso Cisco Aironet suministrados antes del 18 de julio de 2005 no tienen MIC, por lo que crean un certificado autofirmado cuando se hace el upgrade para funcionar en modo ligero. Los controladores se programan para aceptar certificados autofirmados para la autenticación de puntos de acceso específicos.

Debe tratar los APs MIC Cisco Aironet que utilicen el protocolo Lightweight Access Point Protocol (LWAPP), como APs Aironet 1000, y resolver los problemas. Es decir, hay que verificar la conectividad IP, ejecutar el debug de la máquina de estado de LWAPP y, a continuación, verificar la criptografía.

Los logs de la herramienta de upgrade indican si el AP es un AP MIC o un AP SSC. A continuación se muestra un ejemplo de log detallado de la herramienta 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
```

En este log, la línea resaltada especifica que el AP tiene un MIC instalado. Refiérase a la sección Descripción General del Proceso de Upgrade de Upgrade de Puntos de Acceso Cisco Aironet Autónomos al Modo Ligero para obtener más información sobre los certificados y el proceso de upgrade.

En el caso de los APs SSC, no se crea ningún certificado en el controlador. La herramienta de upgrade hace que el AP genere un par de llaves RSA (Rivest, Shamir, Adelman) que se utiliza para firmar un certificado autogenerado (el SSC). La herramienta de upgrade añade una entrada a la lista de autenticación del controlador con la dirección MAC del AP y el hash de llave pública. El controlador necesita el hash de llave pública para validar la firma del SSC.

Si no se ha añadido la entrada al controlador, verifique el archivo CSV de salida. Debe contener entradas para cada AP. Si encuentra la entrada, importe el archivo en el controlador. Si utiliza la interfaz de línea de comandos (CLI) del controlador (con el comando **config auth-list**) o la red de switch, deberá importar un archivo cada vez. Con un WCS, puede importar todo el archivo CSV como una plantilla.

Verifique también el dominio regulador.

Nota: Si tiene un AP LAP pero desea la funcionalidad de Cisco IOS, debe cargar en él una imagen de Cisco IOS autónoma. Y a la inversa, si tiene un AP autónomo y desea convertirlo a LWAPP, puede instalar una imagen de recuperación de LWAPP sobre el IOS autónomo.

Puede completar los pasos para cambiar la imagen de AP con el botón MODE o los comandos **archive download** de la CLI. Refiérase a la sección Troubleshooting para obtener más información sobre cómo utilizar la recarga de imagen con el botón MODE, que funciona con el IOS autónomo o la imagen de recuperación designados con el nombre de archivo predeterminado del modelo de AP.

En la siguiente sección se describen algunos de los problemas más frecuentes de la operación de upgrade y los pasos necesarios para resolverlos.

Problema

Síntoma

El AP no se une al controlador. En la sección Soluciones de este documento se especifican las causas ordenadas por probabilidades.

Soluciones

Utilice esta sección para solucionar el problema.

Causa 1

El AP no encuentra el controlador mediante detección de LWAPP, o el AP no puede alcanzar el controlador.

Troubleshooting

Complete estos pasos:

1. Ejecute el comando **debug lwapp events enable command** en la CLI del controlador.Busque la secuencia de detección de LWAPP > respuesta de detección > solicitud de unión > respuesta de unión. Si no ve la solicitud de detección de LWAPP, significa que el AP no encuentra o no puede encontrar el controlador.A continuación se muestra un ejemplo de JOIN REPLY del controlador de Wireless LAN (WLC) al Lightweight AP (LAP) convertido. Ésta es la salida del 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 si hay conectividad IP entre la red AP y el controlador. Si el controlador y el AP residen en la misma subred, asegúrese de que estén interconectados correctamente. Si residen en subredes distintas, asegúrese de que se utiliza un router entre ellos y que el ruteo entre las dos subredes esté habilitado correctamente.
3. Verifique que el mecanismo de detección esté configurado correctamente.Si se utiliza la opción Domain Name System (DN) para detectar el WLC, asegúrese de que el servidor DNS esté configurado correctamente para asociar CISCO-LWAPP-CONTROLLER.local-domain con la dirección IP del WLC. Por lo tanto, si el AP puede resolver el nombre, emite un mensaje de unión LWAPP a la dirección IP resuelta.Si se utiliza la opción 43 como la opción de detección, asegúrese de que esté configurada correctamente en el servidor DHCP.Refiérase a Registro de LAP con el WLC para obtener más información sobre el proceso y la secuencia de detección.Refiérase a la Ejemplo de Opción 43 de DHCP para la Configuración de Puntos de Acceso Cisco Aironet en Modo Ligero para obtener más información sobre cómo configurar la opción 43 de DHCP.**Nota:** Recuerde que cuando se convierten los AP con dirección estática, el único mecanismo de detección de la Capa 3 que funciona es DNS, ya que preserva la dirección estática durante el upgrade.En el AP, puede emitir el comando **debug lwapp client events** y el comando debug ip udp para recibir la información suficiente para determinar qué ocurre exactamente. Debe ver una secuencia de

paquetes de User Datagram Protocol (UDP), como la siguiente:Enviados desde la dirección IP del AP con la dirección IP de la interfaz de administración de controladores.Enviados desde la dirección IP del administrador de AP a la dirección IP del AP.Serie de paquetes que se envían desde la dirección IP del AP a la dirección IP del administrador de AP.**Nota:** En algunas situaciones puede haber más de un controlador y el AP puede intentar unirse a un controlador distinto en función de los algoritmos y la máquina de estado de detección de LWAPP. Esta situación puede producirse a causa del balanceo dinámico de carga de AP predeterminado que realiza el controlador. Merece la pena analizar esta situación.**Nota:** A continuación se muestra un ejemplo de salida del 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
```

Resolución

Complete estos pasos:

1. Revise el manual.
2. Corrija la infraestructura para que soporte correctamente la detección de LWAPP.
3. Mueva el AP a la misma subred que el controlador para prepararlo.
4. En caso necesario, emita el comando **lwapp ap controller ip address A.B.C.D** para establecer manualmente el IP del controlador regulador en la CLI de AP:La parte *A.B.C.D* de este comando es la dirección IP de la interfaz de administración del WLC.**Nota:** Este comando de CLI se puede utilizar en un AP que nunca se ha registrado en un controlador, o en un AP al que se le haya modificado su contraseña de habilitación predeterminado cuando estaba unido a un controlador anterior. Refiérase a Restablecimiento de la Configuración de LWAPP en un Lightweight AP (LAP) para obtener más información.

Causa 2

La hora del controlador está fuera del intervalo de validez del certificado.

Troubleshooting

Complete estos pasos:

1. Ejecute los comandos **debug lwapp errors enable** y debug pm pki enable.Estos comandos de **debug** muestran el debug de los mensajes de certificado que se pasan entre el AP y el WLC. Los comandos muestran claramente muestran un mensaje que indica que se ha rechazado el certificado porque está fuera del intervalo de validez.**Nota:** Asegúrese de tener en cuenta la diferencia de Tiempo Universal Coordinado (UTC).A continuación se muestra la salida del comando **debug pm pki enable** en el 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)` En esta salida, observe la información resaltada. Esta información muestra claramente que la **hora del controlador está fuera del intervalo de validez del certificado del AP**. Por lo tanto, el AP no puede registrarse con el controlador. Los certificados instalados en el AP tienen un intervalo de validez predefinido. La hora del controlador debe establecerse de forma que esté dentro del intervalo de validez del certificado del AP.
2. Ejecute el comando **show crypto ca certificates** desde la CLI del AP para verificar el intervalo de la validez del certificado establecido en el AP.Aquí tiene un ejemplo:`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`** `.....`
   `..... .....` No se muestra la salida entera porque puede haber muchos intervalos de validez asociados a la salida de este comando. Debe considerar solamente el intervalo de validez especificado por el **punto de confianza asociado**: **Cisco_IOS_MIC_cert** con el nombre de AP correspondiente en el campo de nombre (aquí, Name: **C1200-001563e50c7e**), como se ilustra en este ejemplo de salida. **Éste es el intervalo de validez del certificado real que se considerará.**
3. Ejecute el comando **show time** desde la CLI del controlador para verificar que la fecha y la hora ajustadas en su controlador estén dentro de este intervalo de validez.Si la hora del controlador es anterior o posterior al intervalo de validez de este certificado, cambie la hora del controlador para que esté dentro de este intervalo.

Resolución

Siga este paso:

Elija **Commands > Set Time** en el modo de interfaz gráfica de usuario del controlador o ejecute el comando config time desde la CLI del controlador para establecer la hora del controlador.

Causa 3

Para los APs de SSC se inhabilita la política de AP de SSC.

Troubleshooting

En estos casos, verá este mensaje de error en el 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
```

Complete estos pasos:

Realice una de estas dos acciones:

- Ejecute el comando **show auth-list** desde la CLI del controlador para verificar si éste está configurado para aceptar APs con SSCs.A continuación se muestra un ejemplo de salida del 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 12345678901234567890123456789012345678901234567890`
- Elija **Security > AP Policies** en la GUI.

1. Compruebe si la casilla de verificación **Accept Self Signed Certificate** está marcada. Si no, márquela.
2. Elija **SSC** como tipo de certificado.
3. Añada el **AP** a la lista de autorización con la dirección MAC y la llave hash.Esta llave hash se puede obtener de la salida del comando **debug pm pki enable**. Vea la Causa 4 para obtener información sobre cómo conseguir el valor de la llave hash.

Causa 4

El hash de llave pública SSC falta o es incorrecto.

Troubleshooting

Complete estos pasos:

1. Ejecute el comando **debug lwapp events enable**.Verifique que el AP intenta unirse.
2. Ejecute el comando **show auth-list**.Este comando muestra la llave hash pública que el controlador tiene en almacenamiento.
3. Ejecute el comando **debug pm pki enable**.Este comando muestra la llave hash pública real. La llave hash pública real debe coincidir con la llave hash pública que el controlador tiene en almacenamiento. Una discrepancia causa el problema. Éste es un ejemplo de salida de este mensaje de debug:`(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`

Resolución

Complete estos pasos:

1. Copie la llave hash pública de la salida del comando **debug pm pki enable** y utilícela para sustituir la llave hash pública de la lista de autenticación.
2. Ejecute el comando **config auth-list add ssc AP_MAC AP_key** para añadir la dirección MAC del AP y la llave hash a la lista de autorización:Éste es un ejemplo de este comando:`(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

Causa 5

Se han producido daños en el certificado o la llave pública en el AP.

Troubleshooting

Siga este paso:

Ejecute los comandos **debug lwapp errors enable** y debug pm pki enable.

Ve mensajes que indican los certificados o llaves dañados.

Resolución

Utilice una de estas dos opciones para resolver el problema:

- MIC AP — Solicite una autorización de devolución de materiales (RMA).
- SSC AP — Vuelva a la versión anterior, Cisco IOS Software Release 12.3(7)JA.Complete estos pasos para volver a la versión anterior:

1. Utilice la opción de botón de restablecimiento.
2. Borre la configuración del controlador.
3. Ejecute de nuevo el upgrade.

Causa 6

El controlador podría estar funcionando en modo de capa 2.

Troubleshooting

Siga este paso:

Compruebe el modo de funcionamiento del controlador.

Los AP convertidos soportan solamente la detección de capa 3. Los AP convertidos no soportan la detección de capa 2.

Resolución

Complete estos pasos:

1. Ajuste el WLC para estar en el modo de capa 3.
2. Reinicie y asigne una dirección IP a la interfaz del administrador de AP en la misma subred que la interfaz de administración.Si tiene un puerto de servicio, como el puerto de servicio en 4402 o 4404, debe tenerlo en una superred distinta que la de las interfaces de administrador de APs y de administración.

Causa 7

Verá este error durante el upgrade:

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

Troubleshooting

Si ve este error, siga estos pasos:

1. Verifique que el servidor TFTP está correctamente configurado.Si utiliza el servidor TFTP incorporado en la Herramienta de Upgrade, una causa común es el software de firewall, que bloquea el TFTP de entrada.
2. Verifique si utiliza la imagen correcta para el upgrade.Este ugprade al modo ligero requiere una imagen especial y no funciona con las imágenes de upgrade normales.

Causa 8

Recibe este mensaje de error en el AP después de la conversión:

```
*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
```

El AP se recarga después de 30 segundos y el proceso se inicia de nuevo.

Resolución

Siga este paso:

Tiene un AP SSC. Una vez convertido en AP de LWAPP, añada el SSC y su dirección MAC a la lista de autenticación de AP en el controlador.

Consejos para Troubleshooting

Estos consejos pueden utilizarse al hacer un upgrade desde el modo autónomo al modo LWAPP:

- Si no se borra la NVRAM cuando el controlador intenta escribir en ella tras la conversión, pueden producirse problemas. Cisco recomienda borrar la configuración antes de convertir un AP a LWAPP. Para borrar la configuración:Desde la GUI de IOS: vaya a **System Software > System Configuration > Reset to Defaults**, o Reset to Defaults Except IP.Desde la CLI: ejecute los comandos **write erase** y reload, y no permita que se guarde la configuración cuando se le pregunte si desea hacerlo.Esto también hace que resulte más fácil crear el archivo de texto de APs que va a ser convertido por la Herramienta de Upgrade, ya que las entradas serán <dirección ip>, Cisco, Cisco, Cisco.
- Cisco recomienda utilizar tftp32. Puede descargar el servidor TFTPD más reciente desde http://tftpd32.jounin.net/ .
- Si se habilita un firewall o una lista de control de acceso durante el proceso de upgrade, es posible que la herramienta de upgrade no pueda copiar el archivo que contiene las variables de entorno desde una estación de trabajo a un AP.Si un firewall o una lista de control de acceso bloquean la operación de copia y se elige la opción Use Upgrade Tool TFTP Server, no se podrá continuar el upgrade porque la herramienta no podrá actualizar las variables de entorno, y no se podrá subir la imagen al AP.
- Verifique minuciosamente la imagen a la que intenta hacer el upgrade. El upgrade de

imágenes de IOS a LWAPP difiere de las imágenes IOS normales.En Mis documentos/Mi PC--> herramientas--> Opciones de carpeta, asegúrese de desmarcar la casilla de verificación **Ocultar extensiones de archivos**.
- Asegúrese de utilizar siempre las versiones más recientes de la Herramienta de Upgrade y de la Imagen de Recuperación de Upgrade. Las versiones más recientes están disponibles en el Wireless Software Center.
- Un AP no puede iniciar un archivo de imagen **.tar**. Es un archivo comprimido, similar a los archivos zip. Debe desempaquetar el archivo **.tar** en la memoria flash del AP con el comando archive download, o extraer primero la imagen de inicio del archivo tar y después colocar la imagen de inicio en la memoria flash del AP.

Información Relacionada

- Actualizar los puntos de acceso autónomos del Cisco Aironet al modo ligero
- Restablecimiento de la Configuración de LWAPP en un Lightweight AP (LAP)
- Ejemplo de Opción 43 de DHCP para la Configuración de Puntos de Acceso Cisco Aironet en Modo Ligero
- Cómo recuperar la clave del hash del Punto de acceso e importarla sobre el regulador
- Se puede el Punto de acceso autónomo del Cisco Aironet convertir al protocolo del Lightweight Access Point (LWAPP) usando el CLI
- Soporte Técnico y Documentación - Cisco Systems