Suggerimenti per la risoluzione dei problemi relativi allo strumento di aggiornamento LWAPP

Sommario

Introduzione

In questo documento vengono illustrati alcuni dei problemi principali che possono verificarsi quando si utilizza lo strumento di aggiornamento per aggiornare i punti di accesso autonomi alla modalità lightweight. Questo documento fornisce anche informazioni su come risolvere questi problemi.

Prerequisiti

Requisiti

Prima di poter eseguire l'aggiornamento, gli access point devono eseguire il software Cisco IOS® versione 12.3(7)JA o successive.

I controller Cisco devono eseguire almeno la versione software 3.1.

Cisco Wireless Control System (WCS) (se utilizzato) deve eseguire almeno la versione 3.1.

L'utilità di aggiornamento è supportata sulle piattaforme Windows 2000 e Windows XP. È necessario utilizzare una di queste versioni del sistema operativo Windows.

Componenti usati

Per la stesura del documento, sono stati usati questi access point e controller LAN wireless.

I punti di accesso che supportano questa migrazione sono:

- Tutti i punti di accesso 1121G
- Tutti i punti di accesso 1130AG
- Tutti i punti di accesso 1240AG
- Access point serie 1250
- Per tutte le piattaforme con access point modulare basate su IOS serie 1200 (aggiornamento software Cisco IOS 1200/1220, 1210 e 1230 AP), dipende dalla radio:se sono supportati 802.11G, MP21G e MP31Gse sono supportati 802.11A, RM21A e RM22AGli access point serie 1200 possono essere aggiornati con qualsiasi combinazione di radio supportate: Solo G, solo A o entrambi G e A. Per un punto di accesso che contiene due radio, se una delle due radio è supportata da LWAPP, lo strumento di aggiornamento continua a eseguire l'aggiornamento. Lo strumento aggiunge un messaggio di avviso al registro dettagliato che indica quale radio non è supportata.
- Tutti gli access point 1310 AG
- Cisco C3201 Wireless Mobile Interface Card (WMIC)**Nota:** le radio 802.11a di seconda generazione contengono due numeri di parte.

Prima di poter eseguire l'aggiornamento, i punti di accesso devono eseguire Cisco IOS versione 12.3(7)JA o successive.

Per Cisco C3201WMIC, i punti di accesso devono eseguire Cisco IOS versione 12.3(8)JK o successive prima di poter eseguire l'aggiornamento.

Questi controller LAN wireless Cisco supportano punti di accesso autonomi aggiornati alla modalità lightweight:

- controller serie 2000
- controller serie 2100
- controller serie 4400
- Cisco Wireless Services Module (WiSM) per switch Cisco Catalyst serie 6500
- Moduli di rete controller all'interno dei Cisco serie 28/37/38xx Integrated Services Router
- Switch Catalyst 3750G Integrated Wireless LAN Controller

I controller Cisco devono eseguire almeno la versione software 3.1.

Cisco Wireless Control System (WCS) deve eseguire almeno la versione 3.1. L'utilità di aggiornamento è supportata sulle piattaforme Windows 2000 e Windows XP.

Èpossibile scaricare l'ultima versione dell'utility di aggiornamento dalla pagina Download di software Cisco.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Processo di aggiornamento - Panoramica

L'utente esegue un'utilità di aggiornamento che accetta un file di input con un elenco di punti di accesso e le relative credenziali. L'utilità invia una telnet ai punti di accesso nel file di input con una serie di comandi Cisco IOS per preparare il punto di accesso per l'aggiornamento, inclusi i comandi per creare i certificati autofirmati. Inoltre, l'utilità si collega al controller per programmare il dispositivo in modo da consentire l'autorizzazione di punti di accesso con certificati autofirmati specifici. Quindi carica il software Cisco IOS versione 12.3(11)JX1 sul punto di accesso in modo che possa collegarsi al controller. Quando il punto di accesso si unisce al controller, scarica una versione completa di Cisco IOS dal controller. L'utilità di aggiornamento genera un file di output che include l'elenco dei punti di accesso e dei corrispondenti valori hash della chiave del certificato autofirmati che è possibile importare nel software di gestione WCS. Il Sistema colori Windows può quindi inviare queste informazioni ad altri controller della rete.

Per ulteriori informazioni, consultare la sezione Procedura di aggiornamento di Aggiornamento dei Cisco Aironet Access Point autonomi in modalità Lightweight.

Strumento di aggiornamento - Funzionamento di base

Questo strumento di aggiornamento viene utilizzato per aggiornare un punto di accesso autonomo alla modalità lightweight, a condizione che il punto di accesso sia compatibile per questo aggiornamento. Lo strumento di aggiornamento esegue le attività di base necessarie per l'aggiornamento dalla modalità autonoma alla modalità lightweight. Tali attività includono:

- Verifica delle condizioni di base - Verifica se l'access point è supportato, se esegue una revisione software minima e se i tipi di radio sono supportati.
- Verificare che l'access point sia configurato come root.
- Preparazione dell'access point autonomo per la conversione - Aggiunge la configurazione dell'infrastruttura a chiave pubblica (PKI) e la gerarchia dei certificati in modo da consentire l'autenticazione dell'access point ai controller Cisco e la generazione di certificati autofirmati (SSC) per l'access point. Se l'access point dispone di un certificato di fabbricazione installato (MIC), gli SSC non vengono utilizzati.
- Scarica un'immagine di aggiornamento autonoma in modalità Lightweight, ad esempio 12.3(11)JX1 o 12.3(7)JX, che consente all'access point di collegarsi a un controller. Una volta completato il download, l'access point viene riavviato.
- Genera un file di output costituito da indirizzi MAC AP, tipo di certificato e hash di chiave protetta e aggiorna automaticamente il controller. Il file di output può essere importato in WCS ed esportato in altri controller.

Note importanti

Prima di utilizzare questa utilità, tenere presenti le note seguenti:

- I punti di accesso convertiti con questo strumento non si connettono ai controller 40xx, 41xx o 3500.
- Non è possibile aggiornare i punti di accesso con radio 802.11b-only o 802.11a di prima generazione.
- Se si desidera mantenere l'indirizzo IP statico, la netmask, il nome host e il gateway predefinito dei punti di accesso dopo la conversione e il riavvio, è necessario caricare una delle immagini autonome seguenti sui punti di accesso prima di convertirli in 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 si aggiornano i punti di accesso a LWAPP da una di queste immagini autonome, i punti di accesso convertiti non conservano il proprio indirizzo IP statico, la netmask, il nome host e il gateway predefinito:12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- Lo strumento di aggiornamento LWAPP non rilascia le risorse di memoria del sistema operativo Windows al termine del processo di aggiornamento. Le risorse di memoria vengono rilasciate solo dopo aver chiuso lo strumento di aggiornamento. Se si aggiornano più batch di punti di accesso, è necessario chiudere lo strumento tra i batch per rilasciare le risorse di memoria. Se non si esce dallo strumento tra un batch e l'altro, le prestazioni della stazione di aggiornamento diminuiscono rapidamente a causa di un consumo eccessivo di memoria.

Tipi di certificati

Esistono due tipi diversi di access point:

- AP con MIC
- AP che richiedono un SSC

Ai certificati preinstallati viene fatto riferimento con il termine MIC, acronimo di Manufacturing Installed Certificate. I Cisco Aironet Access Point forniti prima del 18 luglio 2005 non dispongono di MIC, quindi questi access point creano un certificato autofirmato quando vengono aggiornati per funzionare in modalità Lightweight. I controller sono programmati per accettare certificati autofirmati per l'autenticazione di punti di accesso specifici.

Ènecessario trattare i Cisco Aironet MIC AP che usano Lightweight Access Point Protocol (LWAPP), come Aironet 1000 AP, e risolvere i problemi di conseguenza. In altre parole, controllare la connettività IP, eseguire il debug sulla macchina a stati LWAPP e quindi controllare la crittografia.

I log dello strumento di aggiornamento mostrano se l'access point è un access point MIC o SSC. Questo è un esempio di un log dettagliato dello strumento di aggiornamento:

```
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
```

In questo registro, la riga evidenziata specifica che l'access point ha un MIC installato con esso. Per ulteriori informazioni sui certificati e sul processo di aggiornamento, consultare la sezione Panoramica del processo di aggiornamento dei Cisco Aironet Access Point autonomi in modalità Lightweight.

Nel caso degli access point SSC, non viene creato alcun certificato sul controller. Lo strumento di aggiornamento consente all'AP di generare una coppia di chiavi Rivest, Shamir e Adelman (RSA) utilizzata per firmare un certificato generato automaticamente (SSC). Lo strumento di aggiornamento aggiunge una voce all'elenco di autenticazione del controller con l'indirizzo MAC dell'access point e l'hash della chiave pubblica. Il controller ha bisogno dell'hash della chiave pubblica per convalidare la firma SSC.

Se la voce non è stata aggiunta al controller, controllare il file CSV di output. Devono essere presenti voci per ogni punto di accesso. Se si trova la voce, importare il file nel controller. Se si usa l'interfaccia della riga di comando del controller (CLI) (con il comando **config auth-list**) o il Web dello switch, è necessario importare un file alla volta. Con un sistema WCS è possibile importare l'intero file CSV come modello.

Verificare inoltre il dominio normativo.

Nota: Se si dispone di un LAP AP ma si desidera la funzionalità Cisco IOS, è necessario caricare su di esso un'immagine Cisco IOS autonoma. Al contrario, se si dispone di un access point autonomo e si desidera convertirlo in LWAPP, è possibile installare un'immagine di ripristino LWAPP su IOS autonomo.

Per completare la procedura di modifica dell'immagine AP, usare il pulsante MODE o i comandi di **download dell'archivio** CLI. Per ulteriori informazioni su come utilizzare il pulsante MODE image reload, che funziona con IOS autonomo o un'immagine di ripristino denominata nel nome file predefinito del modello AP, fare riferimento a Risoluzione dei problemi.

Nella sezione successiva vengono illustrati alcuni dei problemi più comuni dell'operazione di aggiornamento e le procedure per risolverli.

Problema

Sintomo

L'access point non si unisce al controller. La sezione Soluzioni di questo documento fornisce le cause in ordine di probabilità.

Soluzioni

Utilizzare questa sezione per risolvere il problema.

Causa 1

L'access point non riesce a trovare il controller tramite l'individuazione LWAPP oppure non riesce a raggiungere il controller.

Risoluzione dei problemi

Attenersi alla seguente procedura:

1. Eseguire il comando **debug lwapp events enable** dalla CLI del controller.Cercare LWAPP discovery > discovery response > join request > join response sequence. Se la richiesta di rilevamento LWAPP non viene visualizzata, significa che l'access point non riesce o non trova il controller.Di seguito è riportato un esempio di un'operazione JOIN riuscita tra il controller WLC (Wireless LAN Controller) e il Lightweight AP (LAP) convertito. Questo è l'output 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. Verificare la connettività IP tra la rete AP e il controller. Se il controller e l'access point risiedono nella stessa subnet, verificare che siano correttamente interconnessi. Se risiedono in subnet diverse, verificare che tra di esse venga utilizzato un router e che il routing tra le due subnet sia abilitato correttamente.
3. Verificare che il meccanismo di rilevamento sia configurato correttamente.Se per individuare il WLC viene utilizzata l'opzione DNS (Domain Name System), verificare che il server DNS sia configurato correttamente per eseguire il mapping di CISCO-LWAPP-CONTROLLER.local-domain all'indirizzo IP del WLC. Pertanto, se l'access point è in grado di risolvere il nome, invia un messaggio di join LWAPP all'indirizzo IP risolto.Se l'opzione di rilevamento è l'opzione 43, verificare che sia configurata correttamente sul server DHCP.Per ulteriori informazioni sul processo di rilevamento e la sequenza, consultare il documento

sulla registrazione del LAP sul WLC.Per ulteriori informazioni su come configurare l'opzione DHCP 43, consultare il documento sull'esempio di configurazione dell'opzione DHCP 43 sui Cisco Aironet Lightweight Access Point.**Nota:** quando si convertono i punti di accesso con indirizzo statico, l'unico meccanismo di rilevamento di livello 3 che funziona è il DNS, in quanto l'indirizzo statico viene mantenuto durante l'aggiornamento.Sull'access point, è possibile usare il comando **debug lwapp client events** e il comando **debug ip udp** per ricevere informazioni sufficienti a determinare esattamente cosa si verifica. Dovrebbe essere visualizzata una sequenza di pacchetti UDP (User Datagram Protocol) come la seguente:Originato dall'IP dell'access point con l'IP dell'interfaccia di gestione del controller.Originato dall'indirizzo IP del controller AP manager all'indirizzo IP dell'access point.Serie di pacchetti provenienti dall'IP dell'access point e diretti all'IP di AP manager.**Nota:** in alcune situazioni possono essere presenti più controller e l'access point potrebbe tentare di collegarsi a un controller diverso sulla base della macchina a stati di individuazione LWAPP e degli algoritmi. Questa situazione può verificarsi a causa del bilanciamento del carico dinamico predefinito del punto di accesso eseguito dal controller. Questa situazione può meritare un esame.**Nota:** questo è un output di esempio 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
```

Risoluzione

Attenersi alla seguente procedura:

1. Rivedi il manuale.
2. Correggere l'infrastruttura in modo che supporti correttamente il rilevamento LWAPP.
3. Spostare l'access point sulla stessa subnet del controller per impostarlo come primo.
4. Se necessario, usare il comando **lwapp ap controller ip address *A.B.C.D*** per impostare manualmente l'IP del controller sulla CLI dell'access point:La parte *A.B.C.D* di questo comando è l'indirizzo IP dell'interfaccia di gestione del WLC.**Nota:** questo comando CLI può essere usato su un access point che non è mai stato registrato a un controller o su un access point la cui password predefinita di abilitazione è stata modificata mentre era stato aggiunto a un controller precedente. Per ulteriori informazioni, fare riferimento a Ripristino della configurazione di LWAPP su un Lightweight AP (LAP).

Causa 2

L'ora del controller non rientra nell'intervallo di validità del certificato.

Risoluzione dei problemi

Attenersi alla seguente procedura:

1. Eseguire i comandi **debug lwapp errors enable** ed **debug pm pki enable**.Questi comandi di **debug** mostrano il debug dei messaggi di certificato passati tra l'AP e il WLC. I comandi mostrano chiaramente un messaggio che indica che il certificato è rifiutato in quanto non compreso nell'intervallo di validità.**Nota:** assicurarsi di tenere conto dell'offset UTC (Coordinated Universal Time).Di seguito viene riportato l'output del comando **debug pm pki enable** sul controller:

```
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)
```

In questo output, notate le informazioni evidenziate. Queste informazioni indicano

chiaramente che l'**ora** del **controller non rientra nell'intervallo di validità del certificato dell'access point**. Pertanto, l'access point non può registrarsi con il controller. I certificati installati nel punto di accesso hanno un intervallo di validità predefinito. L'ora del controller deve essere impostata in modo da rientrare nell'intervallo di validità del certificato del punto di accesso.

2. Utilizzare il comando **show crypto ca certificates** dalla CLI dell'access point per verificare l'intervallo di validità del certificato impostato nell'access point.Questo è un esempio:

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

L'intero output non è elencato, in quanto possono esistere molti intervalli di validità associati all'output di questo comando. È necessario considerare solo l'intervallo di validità specificato dal **trust point associato: Cisco_IOS_MIC_cert** con il nome dell'access point appropriato nel campo del nome (**qui, Nome: C1200-001563e50c7e**), come evidenziato nell'esempio di output. **Intervallo di validità effettivo del certificato da considerare.**

3. Usare il comando **show time** dalla CLI del controller per verificare che la data e l'ora impostate sul controller rientrino in questo intervallo di validità.Se l'ora del controller è superiore o inferiore all'intervallo di validità del certificato, modificare l'ora del controller in modo che rientri in tale intervallo.

Risoluzione

Eseguire questo passaggio:

Scegliere **Comandi > Imposta ora** in modalità GUI del controller o usare il comando **config time** nella CLI del controller per impostare l'ora del controller.

Causa 3

Sugli access point SSC, il criterio è disabilitato.

Risoluzione dei problemi

In questi casi, viene visualizzato questo messaggio di errore sul controller:

```
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
```

Attenersi alla seguente procedura:

Eseguire una delle due azioni seguenti:

- Per verificare se il controller è configurato per accettare i punti di accesso con SSC, usare il comando **show auth-list** sulla CLI del controller.Di seguito viene riportato un esempio di output 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          1234567890123456789012345678901234567890
  ```
- Selezionare **Security > AP Policies** nella GUI.

1. Verificare se la casella di controllo **Accetta certificato autofirmato** è attivata. In caso contrario, attivarla.
2. Scegliere **SSC** come tipo di certificato.
3. Aggiungere l'**access point** all'elenco delle autorizzazioni con l'indirizzo MAC e l'hash della chiave.Questo hash di chiave può essere ottenuto dall'output del comando **debug pm pki enable**. Per informazioni su come ottenere il valore hash della chiave, vedere la Causa 4.

Causa 4

L'hash della chiave pubblica SSC è errato o mancante.

Risoluzione dei problemi

Attenersi alla seguente procedura:

1. Eseguire il comando **debug lwapp events enable**.Verificare che l'access point tenti di unirsi.
2. Eseguire il comando **show auth-list**.Questo comando mostra l'hash della chiave pubblica che il controller ha in archivio.
3. Eseguire il comando **debug pm pki enable**.Con questo comando viene visualizzato l'hash della chiave pubblica effettivo. L'hash della chiave pubblica effettivo deve corrispondere all'hash della chiave pubblica presente nell'archivio del controller. Il problema è causato da una discrepanza. Di seguito è riportato un esempio di output del messaggio di 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
```

Risoluzione

Attenersi alla seguente procedura:

1. Copiare l'hash della chiave pubblica dall'output del comando **debug pm pki enable** e utilizzarlo per sostituire l'hash della chiave pubblica nell'elenco di autenticazione.
2. Utilizzare il comando **config auth-list add ssc** *AP_MAC AP_key* per aggiungere l'indirizzo MAC AP e l'hash della chiave all'elenco di autorizzazioni:Questo è un esempio di comando:
```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Causa 5

Certificato o chiave pubblica danneggiati nell'access point.

Risoluzione dei problemi

Eseguire questo passaggio:

Eseguire i comandi **debug lwapp errors enable** ed **debug pm pki enable**.

Vengono visualizzati messaggi che indicano i certificati o le chiavi danneggiati.

Risoluzione

Per risolvere il problema, utilizzare una delle due opzioni seguenti:

- MIC AP - Richiesta di autorizzazione restituzione materiali (RMA).
- SSC AP—Downgrade al software Cisco IOS versione 12.3(7)JA.Completare questi passaggi per declassare:

1. Usare l'opzione del pulsante Reimposta.
2. Cancella le impostazioni del controller.
3. Eseguire di nuovo l'aggiornamento.

Causa 6

Èpossibile che il controller funzioni in modalità layer 2.

Risoluzione dei problemi

Eseguire questo passaggio:

Controllare la modalità di funzionamento del controller.

Gli access point convertiti supportano solo il rilevamento di layer 3. Gli access point convertiti non supportano l'individuazione di layer 2.

Risoluzione

Attenersi alla seguente procedura:

1. Impostare il WLC in modalità layer 3.
2. Riavviare e assegnare all'interfaccia di AP Manager un indirizzo IP nella stessa subnet dell'interfaccia di gestione.Se si dispone di una porta di servizio, ad esempio la porta di servizio su uno switch 4402 o 4404, è necessario che questa si trovi in una supernet diversa rispetto a Gestione access point e alle interfacce di gestione.

Causa 7

Durante l'aggiornamento viene visualizzato questo errore:

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

Risoluzione dei problemi

Quando viene visualizzato questo errore, attenersi alla seguente procedura:

1. Verificare che il server TFTP sia configurato correttamente.Se si utilizza il server TFTP incorporato nello strumento di aggiornamento, un responsabile comune è il software firewall personale, che blocca il server TFTP in entrata.
2. Verificare di utilizzare l'immagine corretta per l'aggiornamento.L'aggiornamento alla modalità lightweight richiede un'immagine speciale e non funziona con le normali immagini di aggiornamento.

Causa 8

Dopo la conversione viene visualizzato questo messaggio:

```
*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
```

L'access point viene ricaricato dopo 30 secondi e riavvia il processo.

Risoluzione

Eseguire questo passaggio:

Si dispone di un punto di accesso SSC. Una volta eseguita la conversione in LWAPP AP, aggiungere il SSC e il relativo indirizzo MAC nell'elenco di autenticazione AP del controller.

Suggerimenti per la risoluzione dei problemi

Questi suggerimenti possono essere utilizzati quando si esegue l'aggiornamento dalla modalità autonoma alla modalità LWAPP:

- Se la NVRAM non viene cancellata quando il controller tenta di scrivervi dopo la conversione, si verificano problemi. Cisco consiglia di cancellare la configurazione prima di convertire un access point in LWAPP. Per cancellare la configurazione:Dalla GUI di IOS: selezionare **System Software > System Configuration > Reset to Defaults** (Software di sistema > Configurazione di sistema > Ripristina valori predefiniti) o **Reset to Defaults Except IP** (Ripristina valori predefiniti **tranne IP)**.Dalla CLI: eseguire i comandi **write erase** e **reload** dalla CLI e non consentire il salvataggio della configurazione quando richiesto.Ciò rende anche più semplice la creazione del file di testo degli access point che devono essere convertiti dallo strumento di aggiornamento, in quanto le voci diventano <indirizzo ip>,Cisco,Cisco,Cisco.
- Cisco consiglia di utilizzare il protocollo tftp32. È possibile scaricare l'ultimo server TFTPD all'indirizzo http://tftpd32.jounin.net/ .
- Se durante il processo di aggiornamento viene attivato un firewall o un elenco di controllo di accesso, lo strumento di aggiornamento potrebbe non essere in grado di copiare il file contenente le variabili di ambiente da una workstation a un punto di accesso.Se l'operazione di copia è bloccata da un firewall o da un elenco di controllo di accesso e si seleziona l'opzione Usa server TFTP dello strumento di aggiornamento, non sarà possibile procedere con l'aggiornamento perché lo strumento non è in grado di aggiornare le variabili di ambiente e il caricamento dell'immagine nell'access point non riesce.
- Controllare l'immagine a cui si sta tentando di eseguire l'aggiornamento. L'aggiornamento da immagini IOS a immagini LWAPP è diverso dalle normali immagini IOS.In Documenti/Risorse del computer—> Strumenti—> Opzioni cartella, deselezionare la casella di controllo **Nascondi le estensioni dei file per i tipi di file conosciuti**.
- Accertarsi sempre di utilizzare l'ultimo strumento di aggiornamento disponibile e l'immagine di ripristino dell'aggiornamento. Le versioni più recenti sono disponibili in Wireless Software Center.
- Un access point non può avviare un file di immagine **.tar**. È un archivio simile ai file zip. È necessario separare il file **.tar** nel flash AP con il comando **archive download**, altrimenti estrarre prima l'immagine di avvio dal file tar e poi metterla nel flash AP.

Informazioni correlate

- Aggiornamento dei Cisco Aironet Access Point autonomi in modalità Lightweight
- Ripristino della configurazione di LWAPP su un Lightweight AP (LAP)
- Esempio di configurazione dell'opzione DHCP 43 sui Cisco Aironet Lightweight Access Point
- Come ripristinare la chiave hash del punto di accesso e importarla nel controller

- È possibile convertire il Cisco Aironet Autonomous Access Point in Lightweight Access Point Protocol (LWAPP) usando la CLI?
- Documentazione e supporto tecnico – Cisco Systems