LWAPP アップグレード ツールのトラブルシューティングのヒント

内容

概要

このドキュメントでは、Autonomous アクセス ポイント（AP）を Lightweight モードにアップグレードするためにアップグレードツールを使用するときに発生する可能性がある重要な問題について説明します。このドキュメントでは、これらの問題を修正する方法も説明します。

前提条件

要件

アップグレードを実行するには、APでCisco IOS®ソフトウェアリリース12.3(7)JA以降が稼働している必要があります。

シスコ製コントローラでは、ソフトウェア バージョン 3.1 以降が稼働していることが必要です。

Cisco Wireless Control System（WCS）では、バージョン 3.1 以降が稼働していることが必要です（使用している場合）。

アップグレード ユーティリティは、Windows 2000 と Windows XP のプラットフォームでサポートされています。これらの Windows オペレーティング システムのどちらかのバージョンを使用する必要があります。

使用するコンポーネント

このドキュメントの情報は、次のアクセスポイントとワイヤレスLANコントローラに基づくものです。

この移行をサポートするAPは次のとおりです。

- すべての1121Gアクセスポイント
- すべての1130AGアクセスポイント
- すべての1240AGアクセスポイント
- すべての1250シリーズアクセスポイント
- すべてのIOSベースの1200シリーズモジュラアクセスポイント（1200/1220 Cisco IOSソフトウェアアップグレード、1210、および1230 AP）プラットフォームでは、無線に依存します。802.11G、MP21G、およびMP31Gがサポートされている場合802.11Aの場合、RM21AとRM22Aがサポートされます1200シリーズアクセスポイントは、サポートされている無線の任意の組み合わせでアップグレードできます。G only、A only、またはGとAの両方。デュアル無線を含むアクセスポイントの場合、2つの無線の1つがLWAPPでサポートされている無線である場合、アップグレードツールはアップグレードを実行します。このツールは、サポートされていない無線を示す警告メッセージを詳細ログに追加します。
- すべての1310 AGアクセスポイント
- Cisco C3201 Wireless Mobile Interface Card(WMIC)**注：第2**世代の802.11a無線には、2つの部品番号が含まれています。

アップグレードを実行するには、アクセスポイントでCisco IOSリリース12.3(7)JA以降が稼働している必要があります。

Cisco C3201WMICでは、アップグレードを実行する前に、アクセスポイントでCisco IOSリリース12.3(8)JK以降が稼働している必要があります。

次のCiscoワイヤレスLANコントローラは、Lightweightモードにアップグレードされた自律アクセスポイントをサポートします。

- 2000 シリーズ コントローラ
- 2100 シリーズ コントローラ
- 4400 シリーズ コントローラ
- Cisco Catalyst 6500シリーズスイッチ向けCiscoワイヤレスサービスモジュール(WiSM)
- Cisco 28/37/38xxシリーズサービス統合型ルータ内のコントローラネットワークモジュール
- Catalyst 3750G統合ワイヤレスLANコントローラスイッチ

シスコ製コントローラでは、ソフトウェア バージョン 3.1 以降が稼働していることが必要です。

Cisco Wireless Control System(WCS)では、バージョン3.1以上を実行する必要があります。アップグレードユーティリティは、Windows 2000およびWindows XPプラットフォームでサポートさ

れています。

最新バージョンのアップグレードユーティリティは、Cisco Softwareダウンロードページからダウンロードできます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

アップグレードプロセス：概要

ユーザは、アクセスポイントとそのクレデンシャルのリストを含む入力ファイルを受け入れるアップグレードユーティリティを実行します。ユーティリティは、自己署名証明書を作成するコマンドを含む、アップグレード用のアクセスポイントを準備するための一連のCisco IOSコマンドを入力ファイルのアクセスポイントにTelnetします。また、ユーティリティはコントローラにTelnetで接続し、特定の自己署名証明書アクセスポイントの許可を許可するようにデバイスをプログラムします。次に、Cisco IOSソフトウェアリリース12.3(11)JX1をアクセスポイントにロードして、コントローラに加入できるようにします。アクセスポイントがコントローラに加入すると、アクセスポイントから完全なCisco IOSバージョンがダウンロードされます。アップグレードユーティリティは、アクセスポイントのリストと、WCS管理ソフトウェアにインポートできる対応する自己署名証明書キーハッシュ値を含む出力ファイルを生成します。WCSは、この情報をネットワーク上の他のコントローラに送信できます。

詳細については、『Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順』の「アップグレード手順」のセクションを参照してください。

アップグレード ツール：基本的な動作

このアップグレード ツールは、Autonomous AP を Lightweight モードにアップグレードするために使用します。ただし、このアップグレードに対して AP の互換性があることが必要です。アップグレード ツールは、Autonomous から Lightweight モードにアップグレードするために必要な基本的なタスクを実行します。これには、次のようなタスクがあります。

- 基本条件チェック：APがサポート対象かどうか、最低限のソフトウェアリビジョンを実行しているか、無線タイプがサポートされているかどうかを確認します。
- APがルートとして設定されていることを確認します。
- Autonomous APの変換準備：Public Key Infrastructure(PKI)設定と証明書階層を追加して、シスココントローラへのAP認証を行い、APに自己署名証明書(SSC)を生成できるようにします。Manufacturing-Installed Certificate（MIC; 製造元でインストールされる証明書）が AP にある場合、SSC は使用されません。
- 12.3(11)JX1や12.3(7)JXなどの自律型からLightweightへのアップグレードイメージをダウンロードします。これにより、APはコントローラに加入できます。ダウンロードに成功すると、AP がリブートされます。
- AP の MAC アドレス、証明書の種類、およびセキュア キー ハッシュが格納された出力ファイルが生成され、コントローラが自動的に更新されます。この出力ファイルは WCS にインポートして、他のコントローラにエクスポートできます。

重要事項

このユーティリティを使用する前に、次の重要事項を考慮してください。

- このツールで変換されたアクセスポイントは、40xx、41xx、または3500コントローラに接続しません。
- 802.11b専用または第1世代の802.11a無線では、アクセスポイントをアップグレードできません。
- 変換およびリブート後も、アクセスポイントのスタティックIPアドレス、ネットマスク、ホスト名、デフォルトゲートウェイを維持するには、アクセスポイントをLWAPPに変換する前に、次のいずれかの自律イメージをアクセスポイントにロードする必要があります。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
- 次の自律イメージの1つからアクセスポイントをLWAPPにアップグレードすると、変換されたアクセスポイントはスタティックIPアドレス、ネットマスク、ホスト名、デフォルトゲートウェイを保持しません。12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- アップグレードプロセスが完了しても、LWAPPアップグレードツールはWindowsオペレーティングシステムのメモリリソースを解放しません。メモリリソースは、アップグレードツールを終了した後にのみ解放されます。複数のバッチのアクセスポイントをアップグレードする場合は、バッチ間でツールを終了して、メモリリソースを解放する必要があります。バッチの間にツールを終了しない場合、メモリの消費が過剰なため、アップグレードステーションのパフォーマンスが急速に低下します。

証明書の種類

次の 2 つの種類の AP があります。

- MIC が設定された AP
- SSC が必要な AP

出荷時にインストールされた証明書は、MICという用語で参照されます。これは、Manufacturing Installed Certificateの略語です。2005年7月18日より前に出荷されたCisco Aironetアクセスポイントにはmicがないため、これらのアクセスポイントはLightweightモードで動作するようにアップグレードすると、自己署名証明書を作成します。コントローラは、特定のアクセスポイントの認証のために自己署名証明書を受け入れるようにプログラムされています。

Cisco Aironet の MIC AP は、Lightweight Access Point Protocol (LWAPP; Lightweight アクセス ポイント プロトコル) を使用する Aironet 1000 の AP などと同様に扱って、同様にトラブルシューティングする必要があります。つまり、IP の接続性を確認し、LWAPP ステート マシンをデバッグして、次に暗号化を確認します。

アップグレード ツールのログには、AP が MIC AP か SSC AP かが表示されます。次にアップグレード ツールの詳細ログの例を示します。

```
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
```

この口グの強調表示されている部分は、MIC が AP にインストールされていることを示しています。証明書とアップグレード プロセスの詳細については、『Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順』の「アップグレード プロセスの概要」のセクションを参照してください。

SSC AP の場合は、証明書がコントローラに作成されません。アップグレード ツールにより、自己生成証明書（SSC）の署名に使用する Rivest, Shamir, Adelman（RSA）キー ペアが AP に生成されます。 アップグレード ツールは、その AP の MAC アドレスと公開キー ハッシュをコントローラの認証リストのエントリとして追加します。公開キー ハッシュは、コントローラが SSC の署名を検証するために必要です。

コントローラにエントリが追加されていない場合は、出力 CSV ファイルを確認します。このファイルには、AP ごとのエントリがあります。エントリが見つかったら、そのファイルをコントローラにインポートします。コントローラのコマンドライン インターフェイス（CLI）（config auth-list コマンド）またはスイッチの Web を使用する場合は、ファイルを 1 回に 1 つずつインポートする必要があります。WCS を使用すれば、CSV ファイル全体をテンプレートとしてインポートできます。

規制区域も確認します。

注：LAP APがあるが、Cisco IOS機能を必要とする場合は、自律型Cisco IOSイメージをロードする必要があります。逆に、Autonomous APを使用していて、それをLWAPPに変換する場合は、Autonomous IOS上にLWAPPリカバリイメージをインストールできます。

MODEボタンまたはCLIのarchive downloadコマンドを使用して、APイメージを変更する手順**を実行できます**。MODEボタンイメージのリロードを使用する方法の詳細については、『トラブルシューティング』を参照してください。このリロードは、自律型IOSまたはAPモデルのデフォルトのファイル名で動作します。

次のセクションでは、アップグレード操作で一般的に発生する問題とその解決方法について説明します。

問題

症状

AP がコントローラに加入しない。このドキュメントの「解決策」セクションでは、確率の順に原因を説明しています。

解決方法

このセクションを使用して、問題を解決してください。

原因 1

AP が LWAPP ディスカバリ経由でコントローラを見つけられないか、あるいは、AP がコントローラに到達できない。

トラブルシュート

次のステップを実行します。

1. コントローラの CLI で debug lwapp events enable コマンドを発行します。[LWAPP discovery] > [discovery response] > [join request] > [join response sequence]を探します。LWAPP ディスカバリ要求が見つからない場合は、AP がコントローラを見つけられないか、見つからないことを意味しています。変換済 Lightweight AP（LAP）への、Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）からの正しい JOIN REPLY の例を次に示します。 次に示すのは、debug lwapp events enable コマンドの出力です。

```
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. AP ネットワークとコントローラの間の IP の接続性を確認します。コントローラと AP が同じサブネットにある場合は、正しく相互接続されていることを確認します。別々のサブネットにある場合は、両者の間にルータが使用されており、2 つのサブネットの間でルーティングが正しく有効になっていることを確認します。
3. ディスカバリ メカニズムが正しく設定されていることを確認します。WLC の検出に Domain Name System（DNS; ドメイン ネーム システム）オプションを使用する場合は、DNS サーバが正しく設定されていて、CISCO-LWAPP-CONTROLLER.local-domain が WLC の IP アドレスに正しくマッピングされていることを確認します。次に、AP が名前を解決できれば、AP は解決済 IP アドレスに対して LWAPP 加入メッセージを発行します。ディスカバリ オプションとしてオプション 43 を使用する場合は、DHCP サーバでそのオプションが正しく設定されていることを確認します。ディスカバリの処理とシーケンスの詳細に

ついては、『WLC への LAP の登録』を参照してください。DHCPオプション43の設定方法の詳細は、『Lightweight Cisco Aironetアクセスポイント用DHCPオプション43の設定例』を参照してください。**注：スタティックにアドレス指定されたAPを変換する**と、動作する唯一のレイヤ3ディスカバリメカニズムがDNSであることに注意してください。これは、アップグレード中にスタティックアドレスが保持されるためです。debug lwapp client events コマンドと debug ip udp コマンドを AP 上で実行すれば、何が起こっているかを正確に判断するのに十分な情報が得られます。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のパケット シーケンスが表示されます。コントローラの管理インターフェイスの IP が設定された AP の IP を発信元とするパケット。コントローラの AP マネージャの IP を発信元として AP の IP へ発信されたパケット。AP の IP を発信元として AP マネージャの IP へ発信された一連のパケット。**注：状況に応じ**て、複数のコントローラが存在する場合があり、LWAPPディスカバリ状態のマシンとアルゴリズムに基づいて、APが別のコントローラに加入しようとする場合があります。このような状況が発生する可能性があるのは、コントローラがデフォルトで実行する動的 AP ロード バランシングのためです。このような状況が発生したら、調査が必要な場合があります。**注：次に、debug ip udp**コマンドの出力例を示します。

```
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
```

解決方法

次のステップを実行します。

1. マニュアルを確認します。
2. LWAPP ディスカバリが正しくサポートされるように、インフラストラクチャを修正します。
3. プライミングを行うために、コントローラと同じサブネットに AP を移動します。
4. コントローラの IP を手動で設定するために、必要に応じて lwapp ap controller ip address A.B.C.D コマンドを AP の CLI で実行します。このコマンドの A.B.C.D の部分には、WLC の管理インターフェイスの IP アドレスを指定します。**注：このCLIコマンド**は、コントローラに登録されていないAPや、以前のコントローラに加入している間にデフォルトのイネーブルパスワードが変更されたAPで使用できます。詳細は、『Lightweight AP(LAP)でのLWAPP設定のリセット』を参照してください。

原因 2

コントローラの時刻が、証明書の有効期間内ではない。

トラブルシュート

次のステップを実行します。

1. **debug lwapp errors enable** コマンドと **debug pm pki enable** コマンドを実行します。これらのデバッグ コマンドでは、AP と WLC の間で渡された証明書メッセージのデバッグ情報が表示されます。これらのコマンドでは、有効期間内ではないので拒否された証明書のメッセージが明確に表示されます。**注：協定世界時**(UTC)オフセットを考慮してください。次に、コントローラ上での **debug pm pki enable** コマンドの出力を示します。

```
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)
```

この出力の強調表示されている部分に注目してください。この情報では、コントローラの時刻が AP の証明書の有効期間内ではないことがはっきり示されています。そのため、AP はコントローラに登録できません。AP にインストールされている証明書には、有効期間が事前に定義されています。コントローラの時刻は、AP の証明書の有効期間内になるように設定する必要があります。

2. AP に設定されている証明書の有効期間を確認するために、AP の CLI から show crypto ca certificates コマンドを実行します。次に例を示します。

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

このコマンドの出力に関連する有効期間は多数になる場合があるので、出力全体は示していません。考慮する必要があるのは、関連する AP の名前が名前フィールドに Cisco_IOS_MIC_certに、関連するAP名を名前フィールドに入力します(Here, Name:C1200-001563e50c7e)を参照してください。**考慮する必要がある実際の証明書の有効期間はこの部分です。**

3. コントローラに設定されている日付と時刻が有効期間内であることを確認するため、コントローラの CLI から **show time** コマンドを発行します。コントローラの時刻がこの証明書の有効期間の前後になっている場合は、期間内になるようにコントローラの時刻を変更します。

解決方法

次の手順を実行します。

コントローラのGUIモードで**Commands > Set Timeの順に選択**するか、コントローラのCLIで**config timeコマンドを**発行して、コントローラの時刻を設定します。

原因 3

SSC AP の場合に、SSC AP のポリシーが無効になっている。

トラブルシュート

そのような場合には、次のエラー メッセージがコントローラに表示されます。

```
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
```

次のステップを実行します。

次のいずれかの操作を行います。

- SSC で AP を受け入れるようにコントローラが設定されているかどうかを調べるために、コントローラの CLI で show auth-list コマンドを実行します。show auth-list コマンドの出力例を次に示します。

```
#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
```

- GUI で [Security] > [AP Policies] を選択します。

1. [Accept Self Signed Certificate] チェックボックスにチェックマークが付いているかどうかを確認します。チェックマークが付いていない場合は、チェックマークを付けます。
2. 証明書の種類として [SSC] を選択します。
3. MAC アドレスとキー ハッシュを指定して、AP を認証リストに追加します。このキー ハッシュは、**debug pm pki enable コマンドの出力から取得できます。**キー ハッシュの値の取得方法については、「原因 4」を参照してください。

原因 4

SSC の公開キー ハッシュが間違っているか存在しない。

トラブルシュート

次のステップを実行します。

1. **debug lwapp events enable** コマンドを実行します。AP が加入しようとしていることを確認します。
2. **show auth-list** コマンドを実行します。このコマンドは、コントローラに保存されている公開キー ハッシュを表示します。
3. **debug pm pki enable** コマンドを実行します。このコマンドは、実際の公開キー ハッシュを

表示します。実際の公開キー ハッシュは、コントローラに保存されている公開キー ハッシュと一致している必要があります。不一致があると問題が発生します。このデバッグ メッセージの出力例を次に示します。

```
(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
```

解決方法

次のステップを実行します。

1. **debug pm pki enable** コマンドの出力から公開キー ハッシュをコピーして、認証リストの公開キー ハッシュを置き換えます。
2. AP の MAC アドレスとキー ハッシュを認証リストに追加するために、config auth-list add ssc AP_MAC AP_key コマンドを発行します。このコマンドの例を次に示します。

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

原因 5

AP の証明書または公開キーが破損している。

トラブルシュート

次の手順を実行します。

debug lwapp errors enable コマンドと **debug pm pki enable** コマンドを実行します。

破損している証明書またはキーを示すメッセージが表示されます。

解決方法

次の 2 つのオプションのどちらかを使用して、問題を解決してください。

- MIC AP：Return Materials Authorization（RMA）を要求します。—
- SSC AP:Cisco IOSソフトウェアリリース12.3(7)JAにダウングレードします。ダウングレードするには、次の手順を実行します。

1. リセット ボタンのオプションを使用します。
2. コントローラの設定をクリアします。
3. アップグレードを再び実行します。

原因 6

コントローラがレイヤ 2 モードで動作している可能性がある。

トラブルシュート

次の手順を実行します。

コントローラの動作モードを確認します。

変換後の AP ではレイヤ 3 のディスカバリだけがサポートされます。変換後の AP ではレイヤ 2 のディスカバリはサポートされません。

解決方法

次のステップを実行します。

1. WLC がレイヤ 3 モードになるように設定します。
2. リブートして、AP マネージャのインターフェイスに、管理インターフェイスと同じサブネットの IP アドレスを設定します。4402 または 4404 のサービス ポートのようなサービス ポートがある場合は、AP マネージャ インターフェイスと管理インターフェイスとは別のスーパーネットに設定する必要があります。

原因 7

アップグレード中に次のようなエラーが表示される。

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

トラブルシュート

このエラーが表示されるときには、次の手順を実行します。

1. TFTP サーバが正しく設定されていることを確認します。アップグレード ツールが内蔵された TFTP サーバを使用している場合は、多くの場合、着信 TFTP を遮断するパーソナル ファイアウォール ソフトウェアが原因です。
2. アップグレード用に正しいイメージを使用しているかどうかを確認します。Lightweight モードにアップグレードするためには、特殊なイメージが必要で、通常のアップグレード イメージでは正しく動作しません。

原因 8

変換後、APに次のエラーメッセージが表示されます。

```
*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
```

AP は 30 秒後にリロードし、プロセスをもう一度開始します。

解決方法

次の手順を実行します。

SSC AP を用意します。LWAPP APに変換したら、コントローラの[AP Authentication]リストに

SSCとそのMACアドレスを追加します。

トラブルシュートのヒント

次のヒントは、AutonomousモードからLWAPPモードにアップグレードするときに使用できます。

- コントローラが変換後にNVRAMに書き込もうとしたときにNVRAMがクリアされない場合、問題が発生します。APをLWAPPに変換する前に、設定をクリアすることを推奨します。設定をクリアするには、次の手順を実行します。IOS GUIから、[System Software] > **[System Configuration] > [Reset to Defaults]に移動するか、[Reset to Defaults Except IP]に移動します**。CLIから：CLIで**write erase**コマンドと**reload**コマンドを発行し、プロンプトが表示されたら設定を保存しないようにします。これにより、アップグレードツールで変換されるAPのテキストファイルは、エントリが<ip address>、Cisco、Cisco、Ciscoになるほど簡単に作成できます。
- tftp32を使用することをお勧めします。最新のTFTPDサーバはhttp://tftpd32.jounin.net/からダウンロードできます 。
- アップグレードプロセス中にファイアウォールまたはアクセスコントロールリスト(ACL)が有効になっていると、アップグレードツールで、ワークステーションからAPに環境変数を含むファイルをコピーできなくなる可能性があります。ファイアウォールまたはアクセスコントロールリストがコピー操作をブロックし、[アップグレードツールTFTPサーバの使用(Use Upgrade Tool TFTP Server)]オプションを選択した場合、ツールは環境変数を更新できず、APへのイメージのアップロードが失敗するため、アップグレードを続行できません。
- アップグレードしようとしているイメージを再確認します。IOSからLWAPPイメージへのアップグレードは、通常のIOSイメージとは異なります。[マイドキュメント/マイコンピュータ]—> [ツール]—> [フォルダオプション]で、[既知のファイルの種類に対してファイル拡張子を非表示にする]チェックボックスをオフにしてください。
- 常に最新のアップグレードツールとアップグレードリカバリイメージを使用してください。最新バージョンは、Wireless Software Centerで入手できます。
- APが.tarイメージファイルを**ブートで**きません。zipファイルに似たアーカイブです。**.tar**ファイルを**archive download**コマンドを使用してAPフラッシュにバンドル解除する必要があります。そうでない場合は、ブート可能なイメージをtarファイルから引き出してから、ブート可能なイメージをAPフラッシュに配置します。

関連情報

- Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順
- Lightweight AP（LAP）での LWAPP 設定のリセット
- Lightweight Cisco Aironet アクセス ポイント用 DHCP オプション 43 の設定例
- アクセスポイントからハッシュキーを回復して、コントローラにインポートする方法
- Cisco Aironet Autonomous Access Point（AP；自律アクセスポイント）は、CLIを使用してLightweight Access Point Protocol(LWAPP)に変換できますか。
- テクニカル サポートとドキュメント – Cisco Systems