LWAPP 変換された AP のために自己署名証明書を手作業でコントローラに追加

目次

概要

このドキュメントでは、Cisco Wireless LAN（WLAN）Controller（WLC; ワイヤレス LAN コントローラ）に Self-Signed Certificate（SSC; 自己署名証明書）を手動で追加するために使用できる方法を説明します。

Access Point（AP）の SSC は AP に登録するべき権限があるネットワークのすべての WLCs にあるはずです。 一般に、同じモビリティグループのすべての WLCs に SSC を適用して下さい。 WLC への SSC の付加がアップグレード ユーティリティによって発生しないとき、この資料のプロシージャの使用の WLC に手動で SSC を追加して下さい。 AP が別のネットワークに変えられるか、または追加 WLCs が存在するネットワークに追加されるときまたこのプロシージャを必要とします。

Lightweight AP Protocol（LWAPP; Lightweight AP プロトコル）で変換された AP が WLC に関連付けられないときには、この問題が発生している可能性があります。 関連付けの問題をトラブルシューティングするときに、次の dubug コマンドを使用すると、次のような出力が表示されます。

- debug pm pki enable コマンドを発行すると、次のように表示されます。
```
(Cisco Controller) >debug pm pki enable
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b3744
Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems,
```

```
MAILTO=support@cisco.com, CN=C1130-00146a1b3744 Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: Mac Address in subject is 00:XX:XX:XX:XX Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: Cert is issued by Cisco Systems. Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: SSC is not allowed by config; bailing... Thu Jan 26 20:22:50 2006:
sshpmFreePublicKeyHandle: called with (nil) Thu Jan 26 20:22:50 2006:
sshpmFreePublicKeyHandle: NULL argument.
```

- debug lwapp events enable コマンドを発行すると、次のように表示されます。

```
(Cisco Controller) >debug lwapp errors enable .... Thu Jan 26 20:23:27 2006: Received LWAPP
DISCOVERY REQUEST from AP 00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1' Thu Jan 26
20:23:27 2006: Successful transmission of LWAPP Discovery-Response to AP 00:13:5f:f8:c3:70
on Port 1 Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to
06:0a:10:10:00:00 on port '1' Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca
cert table Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user
cert Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode() Thu Jan 26
20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco
Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006:
sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems,
MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006:
sshpmGetIssuerHandles: Mac Address in subject is 00:14:6a:1b:32:1a Thu Jan 26 20:23:27 2006:
sshpmGetIssuerHandles: Cert is issued by Cisco Systems. Thu Jan 26 20:23:27 2006:
sshpmGetIssuerHandles: SSC is not allowed by config; bailing... Thu Jan 26 20:23:27 2006:
LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP
00:13:5f:f9:dc:b0. Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil) Thu
Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument. Thu Jan 26 20:23:27 2006:
Unable to free public key for AP 00:13:5F:F9:DC:B0 Thu Jan 26 20:23:27 2006: spamDeleteLCB:
stats timer not initialized for AP 00:13:5f:f9:dc:b0 Thu Jan 26 20:23:27 2006:
spamProcessJoinRequest : spamDecodeJoinReq failed
```

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- アップグレード ユーティリティで生成された SSC が WLC に格納されていない。
- AP には SSC が格納されている。
- WLC と AP で Telnet が有効になっている。
- Cisco 前LWAPP IOS® ソフトウェアコードの最小バージョンはアップグレードされるべき AP にあります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- SSC がインストールされていない、ファームウェア 3.2.116.21 が稼働する Cisco 2006 WLC
- SSC がインストールされている Cisco Aironet 1230 シリーズ AP

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

背景説明

シスコの中央集中型 WLAN アーキテクチャでは、Lightweight モードで AP が動作します。 AP は LWAPP を使用して Cisco WLC と関連付けられます。 LWAPP は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) のドラフト プロトコルであり、設定とパス認証、および実行時の動作に対する制御メッセージを定義します。 また、LWAPP では、データ トラフィックのトンネリング メカニズムも定義しています。

Lightweight AP (LAP) は、LWAPP ディスカバリ メカニズムを使用して WLC を検出します。 次に、LAP は LWAPP 加入要求を WLC に送信します。 WLC は、LAP が WLC に加入できるようにする LWAPP 加入応答を LAP に送信します。 LAP と WLC のリビジョンが一致しない場合は、LAP が WLC に加入する際に、LAP が WLC のソフトウェアをダウンロードします。 その後、LAP は完全に WLC に制御されるようになります。

LWAPP は、セキュア キーを配布することにより、AP と WLC の間の制御通信のセキュリティを確保しています。 セキュア キーの配布には、プロビジョニング済の X.509 デジタル証明書が LAP と WLC の両方に必要です。 プレインストール済みの証明書は、「MIC」という用語で呼ばれます。これは Manufacturing Installed Certificate (製造元でインストールされる証明書) の略語です。 2005 年 7 月 18 日よりも前に出荷された Aironet AP には MIC がインストールされていません。 そのため、これらの AP では、Lightweight モードで動作するように変換された際に、SSC が作成されます。 コントローラは、個々の AP の認証に SSC を受け入れるようプログラムされています。

アップグレード プロセスを次に示します。

1. ログイン クレデンシャルに加えて、AP とその IP アドレスのリストが設定されたファイルを入力として処理するアップグレード ユーティリティをユーザが実行します。
2. AP との Telnet セッションがユーティリティによって確立され、AP のアップグレードを準備するために、入力ファイルに指定されている一連の Cisco IOS ソフトウェアのコマンドが送信されます。 これらのコマンドには、SSC を作成するコマンドが含まれています。 また、特定の SSC AP の認証が許可されるようにデバイスをプログラムするために、WLC との Telnet セッションもこのユーティリティによって確立されます。
3. 次に AP が WLC に加入できるように、Cisco IOS ソフトウェア リリース 12.3(7)JX がユーティリティによって AP にロードされます。
4. AP が WLC に加入すると、完全な Cisco IOS ソフトウェアのバージョンを AP が WLC からダウンロードします。 Wireless Control System (WCS) の管理ソフトウェアへのインポートが可能な AP とそれに対応する SSC キー ハッシュ値のリストが格納された出力ファイルが、アップグレード ユーティリティによって生成されます。
5. これで、WCS はこの情報をネットワーク上の他の WLC に送信できます。

AP が WLC に加入した後は、必要に応じてネットワーク上の任意の WLC に AP を再割り当てできます。

SHA1 キー ハッシュの検索

AP 変換を実行された コンピュータが利用できる場合、シスコの Upgrade Tool ディレクトリにある .csv ファイルからのセキュアハッシュアルゴリズム 1 (SHA1) キー ハッシュを得ることができます。 .csv ファイルが利用できない場合、SHA1 キー ハッシュを取得するために WLC の **debug コマンドを**発行できます。

次の手順を実行します。

1. AP の電源を投入してネットワークに接続します。
2. WLC のコマンドライン インターフェイス (CLI) のデバッグ機能を有効にします。そのために、debug pm pki enable コマンドを発行します。(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** 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**

WLC への SSC の追加

タスク

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

GUI 設定

GUI から次の手順を実行します。

1. **> AP ポリシー**『Security』 を選択 し、側受け入れます自己 署名入り認証を『Enabled』 をクリック して下さい。
2. Certificate Type ドロップダウン メニューから SSC を選択します。
3. AP の MAC アドレスとハッシュ キーを入力して、Add をクリックします。

CLI 設定

CLI から次の手順を実行します。

1. Accept Self Signed Certificate を WLC で有効にします。コマンドは、config auth-list ap-policy ssc enable になります。`(Cisco Controller) >`**`config auth-list ap-policy ssc enable`**
2. AP の MAC アドレスとキー ハッシュを認証リストに追加します。コマンドは、config auth-list add ssc AP_MAC AP_key になります。`(Cisco Controller) >`**`config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9`** *`!--- This command should be on one line.`*

確認

ここでは、設定が正常に動作していることを確認します。

GUI による確認

次の手順を実行します。

1. AP Policies ウィンドウで、AP の MAC アドレスと SHA1 キー ハッシュが AP Authorization List 領域に表示されることを確認します。
2. All APs ウィンドウで、すべての AP が WLC に登録されていることを確認します。

CLI による確認

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- show auth-list AP 認証リストが表示されます。
- show ap summary 接続されているすべての AP の概要が表示されます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ワイヤレス LAN コントローラ（WLC）に関する FAQ
- Cisco ワイヤレス LAN コントローラ設定ガイド、リリース 3.2
- Wireless LAN Controller と Lightweight アクセス ポイントの基本設定例
- テクニカルサポートとドキュメント - Cisco Systems