



## ローカル認証サーバとしてのアクセスポイントの設定

---

この章では、アクセス ポイントをローカル認証サーバとして設定して、小規模無線 LAN 用のスタンドアロン認証サーバとして機能させるか、またはバックアップ認証サービスを提供する方法について説明します。アクセス ポイントはローカル認証サーバとして、最大 50 のクライアント デバイスに対して Light Extensible Authentication Protocol (LEAP; 拡張認証プロトコル) 認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) 認証、および Media Access Control (MAC; メディア アクセス制御) ベースの認証を実行します。この章の内容は、次のとおりです。

- [ローカル認証の概要 \(P. 9-2\)](#)
- [ローカル認証サーバの設定 \(P. 9-3\)](#)

## ローカル認証の概要

802.1x 認証を使用すればさらにセキュリティを強化できる小規模な無線 LAN の多くは、Remote Authentication Dial-In User Service (RADIUS) サーバにアクセスできません。802.1x 認証を使用する多くの無線 LAN でも、アクセスポイントはクライアントデバイスの認証を、遠隔地にある RADIUS サーバに依存しているため、認証トラフィックは WAN リンクを通過する必要があります。この WAN リンクに不具合が発生した場合、または何らかの理由でアクセスポイントが RADIUS サーバにアクセスできない場合、クライアントデバイスが必要とする作業が完全にローカルで行えるものであったとしても、このクライアントデバイスは無線ネットワークにアクセスできません。

WAN リンクやサーバが不具合を起こした場合にローカル認証サービスやバックアップ認証サービスを提供するために、ローカル認証サーバとして動作するアクセスポイントを設定することができます。このように設定したアクセスポイントは、LEAP 認証、EAP-FAST 認証、または MAC ベースの認証を使用して最大 50 の無線クライアントデバイスを認証できます。このアクセスポイントは毎秒最大 5 つの認証を実行できます。

ローカル認証サーバのアクセスポイントはクライアントユーザ名とパスワードを使って手動で設定します。これは、このアクセスポイントはメインの RADIUS サーバとデータベースを同期しないからです。また、クライアントが使用できる VLAN や Service Set Identifier (SSID; サービスセット ID) リストを指定することもできます。



**(注)** 使用している無線 LAN にアクセスポイントが 1 か所しかない場合、このアクセスポイントを 802.1x 認証サーバ、およびローカル認証サーバの両方として設定することができます。ただし、ローカル認証サーバとして稼働するアクセスポイントにアソシエートされているユーザは、アクセスポイントがクライアントデバイスを認証しているときにパフォーマンスが低下することに気づくかもしれません。

アクセスポイントがメインサーバに到達できない場合には、ローカル認証サーバを使用するように設定できます。または、RADIUS サーバを所有していない場合に、ローカル認証サーバを使用するようにアクセスポイントを設定したり、アクセスポイントをメイン認証サーバとして設定したりできます。ローカル認証サーバをメインサーバのバックアップとして設定する場合、アクセスポイントは定期的にメインサーバへのリンクをチェックし、メインサーバへのリンクが復元された場合は、ローカル認証サーバの使用を自動的に停止します。



### 注意

認証サーバとして使用するアクセスポイントには、使用している無線 LAN に関する詳細な認証情報が含まれているので、このアクセスポイントを物理的に保護して、構成を守る必要があります。

## ローカル認証サーバの設定

この項では、アクセスポイントをローカル認証サーバとして設定する方法について、次の項に分けて説明します。

- [ローカル認証サーバに対するガイドライン \(P. 9-3\)](#)
- [設定の概要 \(P. 9-3\)](#)
- [ローカル認証サーバ アクセスポイントの設定 \(P. 9-4\)](#)
- [他のアクセスポイントがローカル認証サーバを使用するための設定 \(P. 9-6\)](#)
- [EAP-FAST の設定 \(P. 9-7\)](#)
- [ロックされたユーザ名のロック解除 \(P. 9-10\)](#)
- [ローカル認証サーバ統計情報の表示 \(P. 9-10\)](#)
- [デバッグメッセージの使用 \(P. 9-11\)](#)

## ローカル認証サーバに対するガイドライン

アクセスポイントをローカル認証サーバとして設定する場合は、次のガイドラインに従ってください。

- 多数のクライアントデバイスにサービスを提供していないアクセスポイントを使用します。アクセスポイントを認証サーバとして使用すると、アソシエートされているクライアントデバイスに対するパフォーマンスが低下します。
- アクセスポイントを物理的に固定して、設定内容を保護してください。

## 設定の概要

ローカル認証サーバの設定は、大きく次の4つの手順に分けて実行します。

1. ローカル認証サーバで、クライアントデバイスを認証するために使用が許可されているアクセスポイントのリストを作成します。ローカル認証サーバを使用する各アクセスポイントは、network access server (NAS) です。



**(注)** 使用するローカル認証サーバアクセスポイントがクライアントデバイスにもサービスを提供する場合は、このローカル認証サーバアクセスポイントをNASとして入力する必要があります。クライアントがこのローカル認証サーバアクセスポイントとアソシエートしている場合、このアクセスポイントはクライアント認証のために自分自身を使用します。

2. ローカル認証サーバで、ユーザグループを作成し、パラメータを各グループに対して適用されるように設定します (オプション)。
3. ローカル認証サーバで、ローカル認証サーバが認証を許可された最大 50 の LEAP ユーザ、EAP-FAST ユーザ、または MAC アドレスのリストを作成します。



**(注)** ローカル認証サーバで実行する認証タイプを指定する必要はありません。認証サーバでは、そのユーザデータベースに記録されているユーザについて、LEAP 認証、EAP-FAST 認証、または MAC アドレス認証のいずれかが自動的に実行されます。


- ローカル認証サーバを使用するアクセスポイントで、ローカル認証サーバを RADIUS サーバとして入力します。



(注) 使用するローカル認証サーバ アクセスポイントがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバの設定時に、このローカル認証サーバを RADIUS サーバとして入力する必要があります。クライアントがこのローカル認証サーバ アクセスポイントとアソシエートしている場合、このアクセスポイントはクライアント認証のために自分自身を使用します。

## ローカル認証サーバ アクセスポイントの設定

特権 EXEC モードから、次の手順に従って、アクセスポイントをローカル認証サーバとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA を有効にします。
ステップ 3	<code>radius-server local</code>	アクセスポイントをローカル認証サーバとして有効にし、認証サーバの設定モードを開始します。
ステップ 4	<code>nas ip-address key shared-key</code>	<p>ローカル認証サーバを使用する装置のリストにアクセスポイントを追加します。アクセスポイントの IP アドレスと、ローカル認証サーバとその他のアクセスポイントの間のコミュニケーションを認証するために使用される Shared Key を入力します。ローカル認証サーバを使用するアクセスポイントで、この共有キーを入力する必要があります。使用するローカル認証サーバがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバ アクセスポイントを NAS として入力する必要があります。</p> <p> (注) キー文字列の先頭にある空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーに空白を使用する場合、引用符がキーの一部である場合を除き、キーを引用符で囲まないとください。</p> <p>この手順を繰り返して、ローカル認証サーバを使用する各アクセスポイントを追加します。</p>
ステップ 5	<code>group group-name</code>	(オプション) ユーザ グループ設定モードを開始して、共有設定を割り当てることができるユーザ グループを設定します。
ステップ 6	<code>vlan vlan</code>	(オプション) ユーザ グループのメンバーが使用する VLAN を指定します。アクセスポイントにより、グループメンバーがその VLAN に移動されます。その他の VLAN 割り当ては無効になります。グループに割り当てられる VLAN は 1 つだけです。

	コマンド	目的
ステップ 7	<code>ssid ssid</code>	(オプション) 最大 20 までの SSID を入力して、ユーザグループのメンバーをそれらの SSID に制限します。アクセス ポイントは、クライアントがアソシエートに使用した SSID が、このリスト内の SSID の 1 つと一致するかどうかをチェックします。SSID が一致しない場合、このクライアントのアソシエーションが解除されます。
ステップ 8	<code>reauthentication time seconds</code>	(オプション) アクセス ポイントがグループのメンバーを再認証するまでの秒数を入力します。この再認証により、ユーザには新しい暗号キーが与えられます。デフォルトの設定は 0 です。これは、グループのメンバーを再認証する必要がないことを表しています。
ステップ 9	<code>block count count time { seconds   infinite }</code>	(オプション) パスワードの推測という攻撃から保護するために、誤ったパスワードがここで設定した回数だけ入力された後、一定の期間、そのグループメンバーをロックアウトできます。 <ul style="list-style-type: none"> <li>count : 誤ったパスワードがここで指定した回数だけ入力されると、そのユーザ名がロックアウトされます。</li> <li>time : ロックアウトの継続時間を秒単位で指定します。infinite と入力した場合、ロックされたユーザ名を管理者が手動で解除する必要があります。クライアントデバイスのロック解除手順については、「<a href="#">ロックされたユーザ名のロック解除</a>」の項 (P. 9-10) を参照してください。</li> </ul>
ステップ 10	<code>exit</code>	グループ設定モードを終了し、認証サーバ設定モードに戻ります。
ステップ 11	<code>user username { password   nhash } password [ group group-name ] [ mac-auth-only ]</code>	ローカル認証サーバを使用した認証が許可されている LEAP ユーザおよび EAP-FAST ユーザを入力します。各ユーザについて、ユーザ名とパスワードを入力する必要があります。認証サーバ データベースでよく見かけられる、パスワードの NT 値しかわからない場合は、16 進数の文字列の NT ハッシュを入力することができます。  MAC ベースの認証のためにクライアント デバイスを追加するには、ユーザ名とパスワードの両方にクライアントの MAC アドレスを入力します。このユーザ名とパスワードには、12 桁の 16 進数を入力します。数字の間にピリオドやダッシュは使用しません。たとえば、MAC アドレスが 0009.5125.d02b である場合は、ユーザ名とパスワードの両方に 00095125d02b と入力します。  ユーザを MAC 認証のみに制限するには、mac-auth-only と入力します。  このユーザをユーザグループに追加するには、グループ名を入力します。グループを指定しない場合、ユーザは特定の VLAN には割り当てられず、再認証するように強制されることはありません。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

次の例は、3つのユーザグループと数人のユーザが存在する3つのアクセスポイントによって使用されるローカル認証サーバを設定する方法を表しています。

```

AP# configure terminal
AP(config)# radius-server local
AP(config-radiusrv)# nas 10.91.6.159 key 110337
AP(config-radiusrv)# nas 10.91.6.162 key 110337
AP(config-radiusrv)# nas 10.91.6.181 key 110337
AP(config-radiusrv)# group clerks
AP(config-radiusrv-group)# vlan 87
AP(config-radiusrv-group)# ssid batman
AP(config-radiusrv-group)# ssid robin
AP(config-radiusrv-group)# reauthentication time 1800
AP(config-radiusrv-group)# block count 2 time 600
AP(config-radiusrv-group)# group cashiers
AP(config-radiusrv-group)# vlan 97
AP(config-radiusrv-group)# ssid deer
AP(config-radiusrv-group)# ssid antelope
AP(config-radiusrv-group)# ssid elk
AP(config-radiusrv-group)# reauthentication time 1800
AP(config-radiusrv-group)# block count 2 time 600
AP(config-radiusrv-group)# group managers
AP(config-radiusrv-group)# vlan 77
AP(config-radiusrv-group)# ssid mouse
AP(config-radiusrv-group)# ssid chipmunk
AP(config-radiusrv-group)# reauthentication time 1800
AP(config-radiusrv-group)# block count 2 time 600
AP(config-radiusrv-group)# exit
AP(config-radiusrv)# user jsmith password twain74 group clerks
AP(config-radiusrv)# user stpatrick password snake100 group clerks
AP(config-radiusrv)# user nick password uptown group clerks
AP(config-radiusrv)# user 00095125d02b password 00095125d02b group clerks mac-auth-only
AP(config-radiusrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radiusrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radiusrv)# user carl password 272165 group managers
AP(config-radiusrv)# user vic password lid178 group managers
AP(config-radiusrv)# end

```

## 他のアクセスポイントがローカル認証サーバを使用するための設定

ローカル認証サーバを、他のサーバを追加するのと同じ方法で、アクセスポイント上のサーバリストに追加します。アクセスポイントにRADIUSサーバを設定する手順の詳細は、[第13章「RADIUSサーバとTACACS+サーバの設定」](#)を参照してください。



(注)

使用するローカル認証サーバアクセスポイントがクライアントデバイスにもサービスを提供する場合は、ローカル認証サーバが自分自身を使用してクライアントデバイスを認証するように設定する必要があります。

ローカル認証サーバを使用するアクセスポイントで、`radius-server host` コマンドを使用して、ローカル認証サーバをRADIUSサーバとして入力します。アクセスポイントがサーバの使用を試みる順序は、アクセスポイント設定でサーバを入力した順序と同じになります。RADIUSを使用するためにアクセスポイントを初めて設定している場合は、まず、メインRADIUSサーバを入力し、最後にローカル認証サーバを入力してください。



(注) 認証ポートには 1812 を、アカウントング ポートには 1813 を入力する必要があります。ローカル認証サーバは、RADIUS アカウントング パケットを傍受するために User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ポート 1813 を監視します。アカウントング パケットはローカル認証サーバにより破棄されますが、サーバがダウンしていると RADIUS クライアントが仮定しないように、確認応答パケットを送り返します。

`radius-server deadtime` コマンドを使って、アクセス ポイントが応答のなかったサーバへ認証を試みるのを中止する間隔を設定します。これにより、要求がタイムアウトするまで待機しなくても、次に設定されたサーバを試行することができます。dead とマークされているサーバは、指定した期間 (分単位)、その他の要求にもスキップされます。この期間は最高 1440 分 (24 時間) まで指定できます。

次の例では、2 つのメイン サーバとローカル認証サーバについて、サーバのデッド タイムを 10 分間に設定する方法を示します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

この例では、メイン サーバへの WAN リンクに不具合が発生すると、LEAP 対応クライアント デバイスがアソシエートされている場合、アクセス ポイントは次の手順を実行します。

1. 最初のサーバを試し、複数回タイムアウトしたら、最初のサーバを dead とマークします。
2. 2 番目のサーバを試し、複数回タイムアウトしたら、2 番目のサーバを dead とマークします。
3. ローカル認証サーバを試し、正常に処理を終了します。

10 分間の dead-time 間隔中に、他のクライアント デバイスが認証を行う必要がある場合、このアクセス ポイントは最初の 2 つのサーバをスキップして、まず、ローカル認証サーバを試みます。デッドタイム間隔後、アクセス ポイントはメイン サーバを使用して認証を試みます。デッドタイムを設定する場合、dead サーバをスキップする必要性と、WAN リンクをチェックする必要性との間でバランスをとり、できるだけ早く、メイン サーバの使用を再開する必要があります。

メイン サーバがダウンしているときに、アクセス ポイントがそのサーバの使用を試みるたびに、認証しようとしているクライアント デバイスが認証タイムアウトを報告する可能性があります。このクライアント デバイスは、メイン サーバがタイムアウトし、アクセス ポイントがローカル認証サーバの使用を試みている場合、再試行し、正常に処理を行います。予想されるサーバタイムアウトに対応するために、シスコクライアント デバイス上でタイムアウト値を延長することができます。

アクセス ポイント設定からローカル認証サーバを削除するには、グローバル設定コマンド `no radius-server host hostname | ip-address` を使用します。

## EAP-FAST の設定

ほとんどの無線 LAN 環境における EAP-FAST 認証では、デフォルトの設定のままで問題ありません。それでも、ネットワークの要件に合わせて、クレデンシャルのタイムアウト値、機関 ID、およびサーバ キーをカスタマイズすることはできます。

## PAC の設定

この項では、Protected Access Credential (PAC) を設定する方法について説明します。EAP-FAST クライアントデバイスがローカル認証サーバに対する認証を初めて試みると、ローカル認証サーバではそのクライアントの PAC が生成されます。PAC を手動で生成し、Aironet Client Utility を使用してその PAC ファイルをインポートすることもできます。

## PAC の有効期限

PAC に有効期間を設定し、さらにその有効期間が切れた後も暫定的にその PAC を有効にしておく猶予期間を指定できます。デフォルトでは、PAC に有効期限はなく、猶予期間も無制限となっています。ユーザグループに対して有効期限と猶予期間の設定を適用できます。

PAC に有効期限と猶予期間を設定するには、次のコマンドを使用します。

```
AP(config-radsrv-group)# [no] eapfast pac expiry days [grace days]
```

2 ~ 4095 の範囲で日数を入力します。有効期限と猶予期間を無制限にリセットするには、コマンドの **no** フォームを入力します。

次の例では、ユーザグループの PAC に 100 日間の有効期限と 2 日間の猶予期間を設定します。

```
AP(config-radsrv-group)# eapfast pac expiry 100 grace 2
```



(注)

PAC が設定されているユーザグループに属していないユーザの場合、そのユーザのデフォルトの PAC 有効期間は 2 日間です (1 日のデフォルト期間と 1 日の猶予期間)。

## PAC の手動生成

ローカル認証サーバでは、EAP-FAST クライアントからの要求に応じて、そのクライアントの PAC が自動的に生成されます。しかし、クライアントデバイスによっては、PAC を手動で生成することが必要な場合もあります。コマンドを入力すると、ローカル認証サーバで PAC ファイルが生成され、指定したネットワーク上の場所にそのファイルが書き出されます。ユーザの手で、その PAC ファイルをクライアントのプロファイルにインポートします。

PAC を手動で生成するには、次のコマンドを使用します。

```
AP# radius local-server pac-generate filename username [password password] [expiry days]
```

PAC のファイル名を入力するときは、ローカル認証サーバからその PAC ファイルが書き出される場所へのフルパスを指定します (例: tftp://172.1.1.1/test/user.pac)。パスワードは省略可能で、指定しない場合は CCX クライアントで認識されるデフォルトのパスワードが使用されます。有効期間も省略可能で、指定しない場合のデフォルト期間は 1 日です。

次の例では、ローカル認証サーバでユーザ名 *joe* の PAC を生成し、パスワード *bingo* を設定してそのファイルを保護します。さらに、10 日間の有効期限をその PAC に設定して、アドレス 10.0.0.5 の Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバに PAC ファイルを書き出します。

```
AP# radius local-server pac-generate tftp://10.0.0.5 joe password bingo expiry 10
```

## 機関 ID の設定

すべての EAP-FAST 認証サーバは、Authority Identity (AID; 機関 ID) で識別されます。認証対象のクライアントには、ローカル認証サーバからその AID が送信されます。受信したクライアントは、それに一致する AID が自身のデータベースにあるか確認します。送信された AID が確認できない場合、クライアントは新しい PAC を要求します。

ローカル認証サーバに AID を割り当てるには、次のコマンドを使用します。

```
AP(config-radsvr)# [no] eapfast authority id identifier
```

```
AP(config-radsvr)# [no] eapfast authority info identifier
```

**eapfast authority id** コマンドにより、認証の際にクライアント デバイスで使用される AID が割り当てられます。

## サーバ キーの設定

ローカル認証サーバでは、生成した PAC の暗号化、およびクライアントを認証する際の PAC の復号化にサーバ キーが使用されます。ローカル認証サーバには、プライマリ キーとセカンダリ キーという 2 種類のキーが保持されていますが、PAC の暗号化ではプライマリ キーが使用されます。デフォルトでは、プライマリ キーとしてデフォルト値が使用されます。セカンダリ キーは、設定しておかない限り、使用されません。

クライアントの PAC を受信したローカル認証サーバは、プライマリ キーを使用してその PAC を復号化しようとします。プライマリ キーによる復号化に失敗した場合、セカンダリ キーが設定されていれば、それを使用して PAC を復号化しようとします。復号化に失敗した認証サーバでは、その PAC は無効として拒否されます。

サーバ キーを設定するには、次のコマンドを使用します。

```
AP(config-radsrv)# [no] eapfast server-key primary {[auto-generate] | [ [0 | 7] key]}
```

```
AP(config-radsrv)# [no] eapfast server-key secondary [0 | 7] key
```

キーには、最大 32 桁の 16 進数を設定できます。暗号化されていないキーを入力するには、キーの前に 0 を入力します。暗号化されているキーを入力するには、キーの前に 7 を入力します。ローカル認証サーバをデフォルトの設定にリセットするには、コマンドの **no** フォームを使用します。これにより、プライマリ キーとしてデフォルト値が使用されるようになります。

## アクセスポイントのクロックが原因で発生する PAC の失敗

ローカル認証サーバでは、PAC の生成と PAC の有効性確認の両方でアクセスポイントのクロックが使用されています。ただし、アクセスポイントのクロックに依存することで、PAC の失敗が発生することがあります。

Network Time Protocol (NTP; ネットワーク タイム プロトコル) サーバから時間設定を取得しているローカル認証サーバのアクセスポイントの場合、起動してから NTP サーバに同期するまでに若干の時間がかかります。この間、そのアクセスポイントでは、自身のデフォルトの時間設定が使用されることとなります。このときにローカル認証サーバで PAC が生成されていると、NTP サーバから新しい時間設定がアクセスポイントに取得された場合に、この PAC が期限切れになることがあります。また、アクセスポイントの起動から NTP 同期までの間に EAP-FAST クライアントが認証を試みると、ローカル認証サーバではそのクライアントの PAC が無効として拒否されることがあります。

さらに、NTP サーバから時間設定を取得していないローカル認証サーバが頻繁にリポートする環境の場合、そのローカル認証サーバで生成された PAC が、有効期限を過ぎても期限切れにならないことがあります。アクセスポイントのクロックは、アクセスポイントがリポートするたびにリセットされます。その結果、クロックに累積された時間が、PAC の有効期間に達しないことになります。

## ローカル認証サーバにおける認証タイプの制限

ローカル認証サーバのアクセスポイントでクライアントデバイスに対して実行できる認証は、デフォルトで LEAP 認証、EAP-FAST 認証、および MAC ベースの認証です。この認証タイプを 1 ~ 2 種類に制限できます。認証サーバの認証タイプを 1 種類に制限するには、次のように認証コマンドの `no` フォームを使用します。

```
AP(config-radsrv)# [no] authentication [eapfast] [leap] [mac]
```

デフォルトではすべての認証タイプが有効なので、コマンドの `no` フォームを使用して認証タイプを無効にします。たとえば、認証サーバで LEAP 認証のみを実行するには、次のコマンドを入力します。

```
AP(config-radsrv)# no authentication eapfast  
AP(config-radsrv)# no authentication mac
```

## ロックされたユーザ名のロック解除

ロックアウト時間が満了する前、またはロックアウト時間が `infinite` に設定されている場合でもユーザ名のロックを解除できます。ロックされたユーザ名のロックを解除するには、特権 EXEC モードに設定されているローカル認証サーバ上で、次のコマンドを入力します。

```
AP# clear radius local-server user username
```

## ローカル認証サーバ統計情報の表示

特権 EXEC モードで、次のコマンドを入力して、ローカル認証サーバが収集した統計情報を表示します。

```
AP# show radius local-server statistics
```

次の例は、ローカル認証サーバ統計情報を示しています。

```

Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Unknown NAS         : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Corrupted packet    : 0           Unknown RADIUS message : 0
No username attribute : 0       Missing auth attribute : 0
Shared key mismatch : 0           Invalid state attribute: 0
Unknown EAP message : 0           Unknown EAP auth type  : 0
Auto provision success : 0       Auto provision failure : 0
PAC refresh         : 0           Invalid PAC received  : 0

Username            Successes Failures Blocks
nicky               0         0         0
jones               0         0         0
jsmith             0         0         0
Router#sh radius local-server statistics
Successes           : 1           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Unknown NAS         : 0           Invalid packet from NAS: 0

```

統計情報の最初のセクションは、ローカル認証サーバからの累積統計情報を示しています。

2番目のセクションは、ローカル認証サーバを使用する権限を持つ各アクセスポイント(NAS)の統計情報を表示しています。このセクションのEAP-FAST統計情報には、次の情報が記録されています。

- Auto provision success : 自動的に生成された PAC の数
- Auto provision failure : 無効なハンドシェイク パケットが原因で、あるいは無効なユーザ名またはパスワードが原因で生成されなかった PAC の数
- PAC refresh : クライアントによって更新された PAC の数
- Invalid PAC received : 受信した PAC のうち、期限切れだったもの、認証サーバで復号化できなかったもの、および認証サーバのデータベースに記録されていないクライアントユーザ名に割り当てられていたものの合計数

この3番目のセクションには、個々のユーザの統計情報が表示されます。ユーザがブロックされていて、ロックアウト時間が infinite に設定されている場合、このユーザの統計行の末尾には *blocked* と表示されます。ロックアウト時間が infinite ではない場合、この行の末尾には *Unblocked in x seconds* と表示されます。

ローカル認証サーバ統計情報を 0 にリセットするには、次の特権 EXEC モード コマンドを使用します。

```
AP# clear radius local-server statistics
```

## デバッグメッセージの使用

ローカル認証サーバに対するデバッグメッセージの表示を制御するには、特権 EXEC モードで次のコマンドを入力します。

```
AP# debug radius local-server { client | eapfast | error | packets }
```

このデバッグ情報を表示するには、次のコマンド オプションを使用します。

- 失敗したクライアント認証に関連するエラー メッセージを表示するには、**client** オプションを使用します。
- EAP-FAST 認証に関連するエラー メッセージを表示するには、**eapfast** オプションを使用します。特定のデバッグ情報を選択するには、次のサブオプションを使用します。
  - **encryption** : 受信されたパケットおよび送信されたパケットの暗号化と複合化に関する情報が表示されます。
  - **events** : すべての EAP-FAST イベントに関する情報が表示されます。
  - **pac** : PAC の生成や検証など、PAC に関連するイベントの情報が表示されます。
  - **pkts** : EAP-FAST クライアントとの間で送受信されたパケットが表示されます。
- ローカル認証サーバに関連するエラー メッセージを表示するには、**error** オプションを使用します。
- 送受信された RADIUS パケットの内容が表示されるようにするには、**packets** オプションを使用します。