FreeRADIUS 3 の導入

改訂履歴

2015.6.29 初出
2015.7.1 更新
2015.7.31 更新
2017.2.7 更新
2020.7.22 更新
2022.8.22 更新
2023.3.8 更新

FreeRADIUS 3 を用いて eduroam 対応の RADIUS サーバ (proxy および IdP 機能) を構築する方法について説明します。

想定

- 本ドキュメントは FreeRADIUSの3.2.0 を対象に記述。
- 機関 example.ac.jp のトップレベルのサーバ(RADIUS proxy)の設定を想定。小規模なIdPとしても利用可能とする。

> ⚠ 注: FreeRADIUS3.0.25以前にはTLSの処理が不安定になる不具合があるため、必ず3.2.0以降を使う必要があります。

- 認証方式は PEAP/EAP-TTLS両用 (MS-CHAPv2) とする。
- FreeRADIUSのファイル群は "/usr/local/freeradius/3.2.0/" 以下にインストールする。 設定ファイルは"/usr/local/freeradius/3.2.0/etc/raddb/"に入る。
- サーバ証明書は FreeRADIUS がbootstrapで自動的に作成するが、 設定後に正規のものに入れ替える(IdPのみ)。

FreeRADIUSの導入

1. FreeRADIUSのビルドにopenssl, tallocなどのライブラリが必要なので、OSにあらかじめ開発用のパッケージを導入しておきます。
2. FreeRADIUS のソースパッケージを以下のサイトからダウンロードします。
   https://www.freeradius.org/
3. ダウンロードしたファイルを展開し、ビルド後、インストールします。

```
$ tar zxf freeradius-server-3.2.0.tar.gz
$ cd freeradius-server-3.2.0
$ ./configure --prefix=/usr/local/freeradius/3.2.0
$ make
# make install
```

・makeまでは一般ユーザで構いませんが、make installはroot権限で行ってください。

FreeRADIUSの設定

1. 設定ファイルのテンプレートraddb-3.2.0-eduroamJP.tgzをダウンロードします。
2. どこか適当なディレクトリで、テンプレートを展開します。このテンプレートを参考に、raddb ディレクトリにあるファイルを書き換えます。

```
# cd /usr/local/freeradius/3.2.0/etc
# tar zxpf raddb-3.2.0-eduroamJP.tgz
```

最低限、変更が必要なファイルは、以下のとおりです。設定の注意点も示します。

- **radiusd.conf**
  認証ログを残すために "auth = yes" とする必要があります。
- **proxy.conf**
  ファイル中の<JP serverX addr> と <JP secret key> に、eduroam参加登録の際に決まるeduroam JPのアドレスと共通鍵をそれぞれ設定してください。
  realmの example を自機関名に書き換えてください。eduroam JPのサーバとの間でループが生じないように、機関レルム(例: example.ac.jp)に末尾がマッチするレルムはすべて、機関側のRADIUS proxyで終端する必要があります。
  機関内の別のRADIUS IdPに認証要求を転送する場合は、IdP1/IdP2の設定例を参考にしてください。

オプション "status_check = status-server"は、相手サーバの死活監視を効率よく行うためのものです。FreeRADIUSを含む多くのRADIUSサーバがこの機能に対応していますが、もし機関内の認証サーバ(RADIUS IdP)との接続がうまくいかない場合は、このオプションを外してみてください。

- **clients.conf**
  ファイル中の<JP serverX addr> と <JP secret key> に、eduroam参加登録の際に決まるeduroam JPのアドレスと共通鍵をそれぞれ設定してください。
  機関内の無線LANコントローラや、他のRADIUS proxyも、このファイルに記述することでアクセス許可されます。
- **mods-available/eap**
  FreeRADIUSが自動的に作成したサーバ証明書で動作確認の後、正規のサーバ証明書を用意して、ファイル中のprivate_key_password, private_key_file, certificate_file, ca_file
  を適宜書き換えて下さい。UPKI電子証明書発行サービスなどのサーバ証明書が利用できます。

> ⚠ 注意：サーバ認証において、公共のCAから発行された証明書を用いた場合、プライベートのCA証明書を端末に導入する煩雑さを回避できます。
> しかし、公共のCAを利用する場合、サーバ証明書のドメイン名を確実に確認できるように、端末を設定する必要があります。

> ⚠ 注意2: EAP-TLSのクライアント認証のフェーズでは、公共のCAを使うべきではありません (eapファイルにコメントあり)。
> サンプルのファイルでは、EAP-TLS認証が無効になるように、該当するセクションをコメントアウトしてあります

- **mods-config/files/authorize**
  基本的には空にします。テストアカウントや少人数のアカウントは、このファイルに記述できます。
- **sites-available/nonexistent, sites-enabled/nonexistent**
  FreeRADIUSのパッケージに含まれないファイルです。機関に存在しないレルムを受信した際に、その旨をエラーとして返すためのvirtual server定義です。サンプルのtarファイルに含まれているものをコピーして、Example Universityの部分を自機関の名前に書き換えてください。
- **policy.d/filter**
  FreeRADIUS 3.x系の一部に、"reject mixed case" という(不正な)ルールが有効になっているものがあります。この処理がコメントアウト（無効化）されていることを確認してください。FreeRADIUS 3.2.0では最初から無効になっているはずです。(eduroamのアカウントは、ユーザ名が case sensitive (大文字小文字を区別する)、レルム名が case insensitive (大小区別しない)です。)

動作確認

1. テスト用のアカウントを登録します (mods-config/files/authorizeに書き込む)。
2. debugモードでradiusサーバを起動します。

```
# /usr/local/freeradius/3.2.0/sbin/radiusd
-fxx -l stdout
```

   - rootで実行してください。
   - オプション -fxx -l stdout を付けているので、デーモンではなく通常のプロセスとして動作します。
3. パスを通した後、テスト用コマンドを実行します。

```
# export PATH=$PATH:/usr/local/freeradius/3.2.0/bin
# radtest ユーザ名@example.ac.jp パスワード
localhost 1 testing123
# radtest -t mschap ユーザ名@example.ac.jp パスワー
ド localhost 1 testing123

# radtest -t mschap ユーザ名@example.ac.jp パスワー
ド localhost:18120 1 testing123
```

   - radiusサーバの起動に失敗した場合には設定を見直してください。
   - テスト用コマンドで認証が成功すると"Access-Accept"と表示されます。
   - 最後のradtestはinner-tunnelの確認のためのもので、もしこれが認証失敗する場合は、実際の端末からの認証が失敗することになります。
   - 正常動作が確認できたら、オプション -fxx -l stdoutを付けないで radiusd を起動します。システム起動時に radiusd が立ち上がるように、OSのスタートアップファイルに追記します (使用しているOSやディストリビューションによって設定方法が異なります)。
4. 動作確認後は、必ずテスト用アカウントを削除して、radiusd を再起動してください。

---

eduroam JP参加時の注意事項

eduroam JPのトップレベルRADIUS proxyに接続する際に、機関側の設定不足によって認証連携がうまく動作しない例が散見されます。事務局の負担軽減のため、問い合わせの前に以下の点を確認、修正するようにお願いします。

- **RADIUSサーバ上のFirewallでRADIUSの通信がブロックされていないか?**
  OSのFirewallの設定で、RADIUSプロトコルが使用するポート(1812/udpと1813/udp)を開けてください。
- **機関のFirewallでRADIUSの通信がブロックされていないか?**
  機関のFirewallの設定で、RADIUSプロトコルが使用するポート(1812/udpと1813/udp)を開けてください。

- **正しい共通鍵を使用しているか?**
  RADIUSのサーバソフトウェアまたはアプライアンスによって、共通鍵の最大長や、利用できる字種に違いがあります。ご利用の環境に合った鍵を申請書に記入してください。
- **レルムの転送処理が正しいか?**
  自機関のレルムの付いた認証要求をeduroam JPのサーバに転送すると、動作不安定の原因になります。特に正規表現の利用には十分に注意し、このような不正な転送が行われないようにしてください。
  負荷軽減のため、レルム無しの認証要求をeduroam JPのサーバに転送しないでください。