

Building mod_auth_radius-2.0 for Apache 2.0

Below is a brief guide to building and configuring the RADIUS authentication module for Apache 1.3.x/2.0 found on www.freeradius.org. It is by no means an exhaustive guide and, given the variance in Linux installations, it is suggested the build and install is performed by a competent System Administrator comfortable with Apache configuration and package installation on your platform.

This build was carried out on a clean install of Redhat EL 4 built without Apache on Intel based hardware. You will need to install a C compiler if you don't already have one installed to be able to build the module.

The following packages were installed prior to any work being done with the RADIUS module:

```
apr-0.9.7-1
apr-util-0.9.7-1
httpd-2.0.55-1
apr-devel-0.9.7-1
apr-util-devel-0.9.7-1
httpd-devel-2.0.55-1
```

The versions installed were binary distribution rpm files for the Intel platform taken from an official Apache mirror site.

Once installed, Apache was started and a browser window opened to the machine to prove the basic configuration was functional. This should show the basic Apache successful install page.

Next, the RADIUS module was downloaded and extracted:

ftp://ftp.freeradius.org/pub/radius/mod_auth_radius.tar

The binary installation above contains Apache configured with support for dynamic modules. Given this and assuming the above installs all work, the build and install of the Apache module is a single command:

```
apxs -i -a -c mod_auth_radius-2.0.c
```

apxs is specifically designed for building and installing Apache extension modules. It will compile the module, link it and copy it to the default Apache module location.

The tar archive contains a sample Apache configuration file and a README detailing how to configure the RADIUS module and how to specify which directories are protected.

Sample Apache 2.0.55 Configuration extracts

Below are extracts from the httpd.conf file, the main Apache 2.0 configuration file, which on my machine lives in /etc/httpd/conf.

```
# Load the RADIUS module
LoadModule radius_auth_module /usr/lib/httpd/modules/mod_auth_radius-2.0.so

# Configure the RADIUS server
<IfModule mod_auth_radius-2.0.c>
AddRadiusAuth 10.11.12.13:1812 mysecret
AddRadiusCookieValid 5
</IfModule>

# Secure a location
<Location /secure/>
AuthType Basic
AuthName "RADIUS authentication for Redhat Test Box"
AuthAuthoritative off
AuthRadiusAuthoritative on
AuthRadiusActive On
require valid-user
</Location>
```

Please note: it is possible your installation paths and module libraries may be different.

The `AddRadiusAuth 10.11.12.13:1812 mysecret`

Needs to match the settings for PINsafe, so in this example the PINsafe server would be at IP address 10.11.12.13, it would be using port 1812 for authentications and would have a shared secret of mysecret.

The `<Location /secure/>` entry shows that the path /secure requires authentication in order to access it.

Please check the README on the Free Radius site and within the tar archive for up-to-date information regarding build and install of the module. This is the only source that can be considered truly accurate.