

OpenAM Pluggable Authentication Module(PAM) integration with UNIX

- Pre-requisites

- OpenAM 13.0.0 installed
- Configure OpenAM to act as Radius Server as per: <https://backstage.forgerock.com/#!/docs/openam/13/admin-guide#chap-radius>
- Create required OpenAM Realm & Authentication Chain
- Compile and deploy PAM Radius client library for Unix OS from <http://www.freeradius.org/>

Steps -

1. Check if the PAM Radius client library (**pam_radius_auth.so**) is installed in **"/usr/lib/security/"** folder.
2. Otherwise compile the library by following instructions at http://freeradius.org/pam_radius_auth/
3. To enable PAM based authentication for SSH, add the pam auth radius library to pam.conf file.

In My Linux environment it look like following -

```
Starhub — ec2-user@ip-1
java      java      bash
[ec2-user@ip-172-31-39-244 raddb]$ sudo more /etc/pam.d/sshd
#%PAM-1.0
auth      sufficient      pam_radius_auth.so      debug
auth      required          pam_sepermit.so
auth      substack             password-auth
auth      include             postlogin
account   required          pam_nologin.so
account   include             password-auth
password  include             password-auth
# pam_selinux.so close should be the first session rule
session   required          pam_selinux.so close
session   required          pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session   required          pam_selinux.so open env_params
session   optional         pam_keyinit.so force revoke
session   include             password-auth
session   include             postlogin
```

4. Create server configuration file. An example is given in the file pam_radius_auth.conf. You will need to copy this file to /etc/raddb as "server". In My environment it appears as follows -

```
java      java
[ec2-user@ip-172-31-39-244 raddb]$ more /etc/raddb/server
# pam_radius_auth configuration file. Copy to: /etc/raddb/server
#
# For proper security, this file SHOULD have permissions 0600,
# that is readable by root, and NO ONE else. If anyone other than
# root can read this file, then they can spoof responses from the server!
#
# There are 3 fields per line in this file. There may be multiple
# lines. Blank lines or lines beginning with '#' are treated as
# comments, and are ignored. The fields are:
#
# server[:port] secret [timeout]
#
# the port name or number is optional. The default port name is
# "radius", and is looked up from /etc/services The timeout field is
# optional. The default timeout is 3 seconds.
#
# If multiple RADIUS server lines exist, they are tried in order. The
# first server to return success or failure causes the module to return
# success or failure. Only if a server fails to response is it skipped,
# and the next server in turn is used.
#
# The timeout field controls how many seconds the module waits before
# deciding that the server has failed to respond.
#
# server[:port] shared_secret      timeout (s)
#52.11.188.117:1812      secret      9
#172.31.26.70:1812      secret      60
#other-server      other-secret      3
#
# having localhost in your radius configuration is a Good Thing.
#
# See the INSTALL file for pam.conf hints.
[ec2-user@ip-172-31-39-244 raddb]$
```

5. Ensure that following flags are enabled in UNIX login configuration file -

ChallengeResponseAuthentication yes

UsePAM yes

6. Define a Radius Client in OpenAM with same shared secret defined in /etc/raddb/server file.

User: amAdmin Server: WIN-3L7QGQRH3QJ

FORGEROCK

Edit Sub Configuration - pam

Global Attributes

Client IP Address:
The IP Address of the client.

Client Secret:
This secret shared between server and client for encryption of the user password.

Log Packet Contents for this Client: YES NO
Indicates if full packet contents should be dumped to the log.

Handler Class:
The fully qualified name of a class to handle incoming RADIUS Access-Requests for this client.

Handler Class Configuration Properties

Current Values

New Value

Properties needed by the handler class for its configuration.

7. Now the setup is completed and when you login to UNIX host PAM module will perform the authentication against OpenAM radius server.