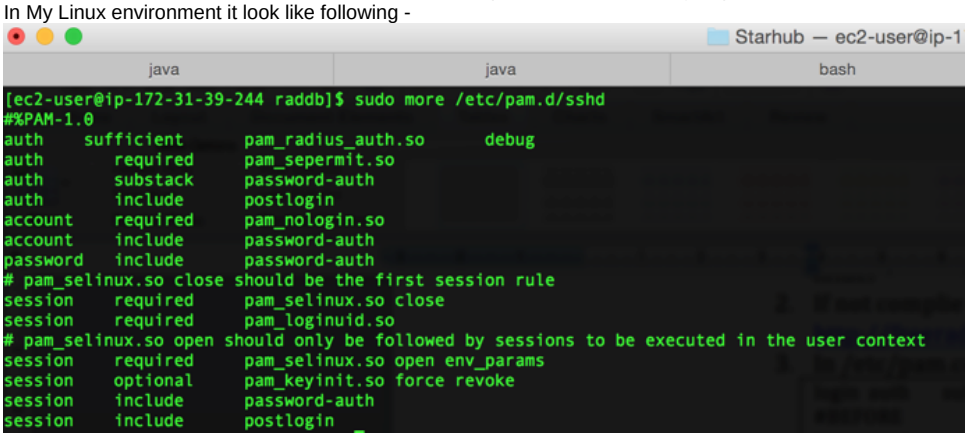
OpenAM Pluggable Authentication Module(PAM) integration with UNIX

- Pre-requisites

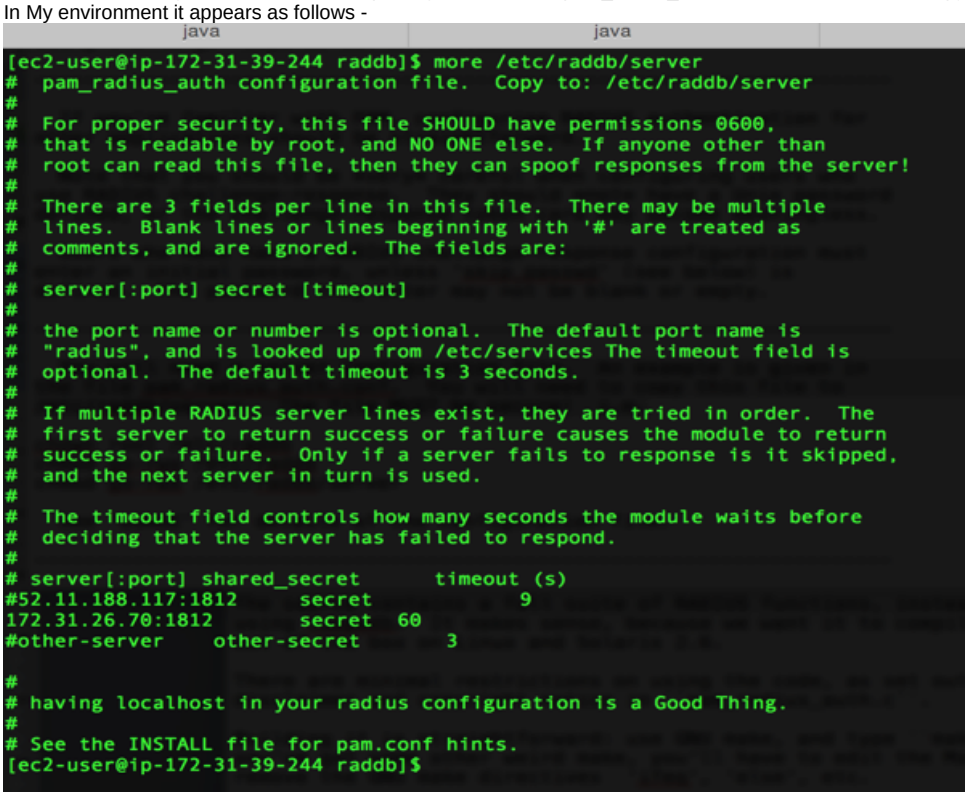
  - OpenAM 13.0.0 installed
  - Configure OpenAM to act as Radius Server as per: https://backstage.forgerock.com/#!/docs/openam/13/admin-guide#chap-radius
  - Create required OpenAM Realm & Authentication Chain
  - Compile and deploy PAM Radius client library for Unix OS from http://www.freeradius.org/

Steps -

1. Check if the PAM Radius client library (**pam_radius_auth.so**) in 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 -



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 -

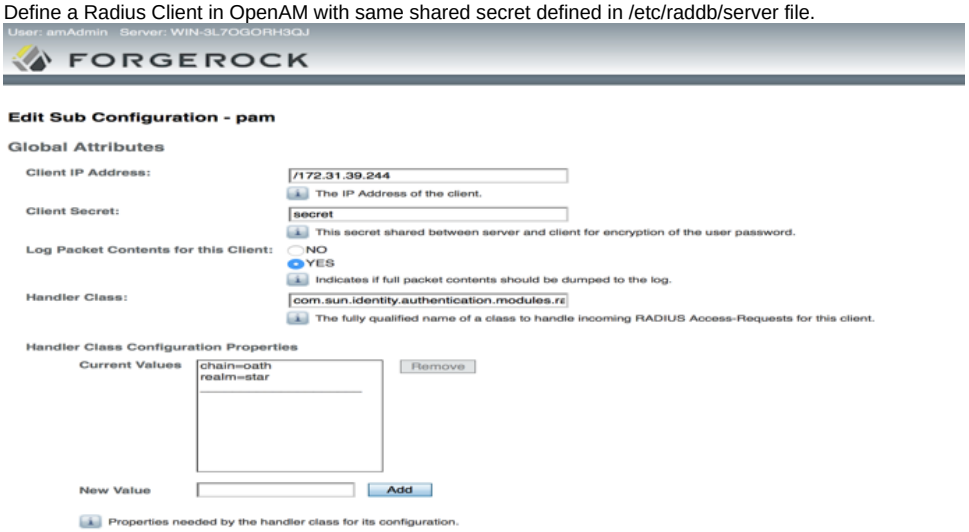


5. Ensure that following flags are enabled in UNIX login configuration file -

   ChallengeResponseAuthentication yes

   UsePAM yes

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



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