Configuring PAM

Describes how PAM works with MapR.

MapR uses Pluggable Authentication Modules (PAM) (http://en.wikipedia.org/wiki/Pluggable_Authentication_Modules) for password verification in a variety of places. Make sure PAM is installed and configured on the node running the `mapr-apiserver` , or other components that will use PAM to verify passwords.

There are typically several PAM modules (profiles), configurable via configuration files in the `/etc/pam.d/` directory. Any component verifying user passwords tries the following three profiles in order:

1. sudo (`/etc/pam.d/sudo`)
2. sshd (`/etc/pam.d/sshd`)
3. mapr-admin (If you have created the `/etc/pam.d/mapr-admin` profile and the component checks beyond the first two profiles.)

The profile configuration file (for example, `/etc/pam.d/sudo`) should contain an entry corresponding to the authentication scheme used by your system. For example, if you are using the simplest form of local OS authentication, check for an entry similar to the following - consult with your Unix system administrator if you are uncertain:

```
auth    sufficient      pam_unix.so  # For local OS Auth
```

Component-specific PAM Configurations

Some ecosystem components have unique requirements that require setup of a component-specific PAM configuration. See the Ecosystem Guide (../c_ecosystem_intro.html#concept_rkw_gxk_tt) for the specific Ecosystem component.