Configuring Drill to Use libpam4j

You can configure Drill to use libpam4j for Plain authentication between a client, such as ODBC, and the Drillbit.

Starting in MEP 5.0, you can configure Drill to use libpam4j for form-based authentication between a web client and Drillbit (web server). Form-based authentication is like Plain authentication in that a user is presented with a web form where s/he enters a username and password to access restricted web pages. When using form-based authentication, you can also configure Drill to use SPNEGO. See SPNEGO for HTTP Authentication (drill-spnego-http-authentication.html#drill-spnego-http-authentication).

Complete the following steps to configure Plain authentication (for JDBC/ODBC clients) and form-based authentication (for the web client) in Drill:

1. Add the following configurations to the `/opt/mapr/drill/drill-<version>/conf/drill-override.conf` file:

```
drill.exec:{
   cluster-id:"drillbits1",
   zk.connect:"<zk-node-hostname>:5181,<zk-node-hostname>:5181,<zk-node-hostname>:5181",
   security:{
      auth.mechanisms:[ "PLAIN"],
   },
   security.user.auth:{
      enabled:true,
      packages += "org.apache.drill.exec.rpc.user.security",
      impl:"pam4j",
      pam_profiles:[ "sudo", "login" ]
   },
   http.auth.mechanisms:[ "FORM" ]
}
```

2. (Optional) To add or remove different PAM profiles, add or delete the profile names in the `pam_profiles` array portion of the configuration:

```
pam_profiles: [ "sudo", "login" ]
```

3. Restart the Drillbit process on each Drill node, as shown:

```
/opt/mapr/drill/drill-<version>/bin/drillbit.sh restart
```