How to use setup-openam.sh and run-setup.sh for OPENAM-12627

NOTE: You need jq utility for the script to run https://stedolan.github.io/jq/

Preparation

1. Install OpenAM 5.5.1
2. Adjust setup-openam.sh script and run-setup.sh to fit your environment setting :
   openam_host="openam.internal.example.com"
   openam_ip="172.28.XXX.XXX"
   openam_port=8080
   openam_url="http://${openam_host}:${openam_port}/openam"
   Note that script uses “openam” as application context.
   Also, change demo/changeit and amadmin/password
3. Run setup-openam.sh script to create FQDN mapping, Push Auth module etc
   If script runs successfully, you will see the following messages :
   {"com.sun.identity.urlconnection.useCache":false,"com.iplanet.am.serverMode":true,"com.sun.embedded.sync.servers":"on","com.sun.embedded.replicationport":""
   :
   {"type":"Transaction","authenticationStrategy":"AuthenticateToServiceConditionAdvice","strategySpecifier":"pushService"},"resourceTypeUuid":"76656a38-5f8e-401b-83aa-4ccb74ce88d2","lastModifiedBy":"id=amadmin,ou=user,dc=openam,dc=forgerock,dc=org","lastModifiedDate":"2018-03-16T02:48:44.71Z","createdBy":"id=amadmin,ou=user,dc=openam,dc=forgerock,dc=org","creationDate":"2018-03-16T02:48:44.71Z"}
   Restart OpenAM server for configuration to take affect
4. Restart OpenAM server instance

Running Transactional Authorization (Success Case)

1. Run run-setup.sh script
2. Step through the process by hitting [Enter] button until you see this message :
   complete transaction Datastore authentication module callbacks
   caller = demo user with password : changeit
   Demo password is valid

   + jq .
   + curl -X POST 'http://openam.internal.example.com:8080/openam/json/authenticate?authIndexType=composite_advice&authIndexValue=%3CAdvices%3E%0A%3CAttributeValuePair%3E%0A%3CAttribute%20name%3D%22TransactionConditionAdvice%22%2F%3E%0A%3CValue%3Ecf311ec8-9050-46a8-aae9-0334f1d469e8%3C%2FValue%3E%0A%3C%2FAttributeValuePair%3E%0A%3C%2FAdvices%3E' --header 'Content-Type: application/json' --header 'iPlanetDirectoryPro: USKVsq-AG9KXa9...AA' --data '{"authId":"eyJ0eXAi...WWPFc","template":"","stage":"LDAP1","header":"Sign in","callbacks":[{"type":"NameCallback","output":[{"name":"prompt","value":"User Name:"}],"input":[{"name":"IDToken1","value":"demo"}]},{"type":"PasswordCallback","output":[{"name":"prompt","value":"Password:"}],"input":[{"name":"IDToken2","value":"changeit"}]}]}'*
   {
   *"tokenId": "USKVsq-AG9KXa93uCqj7SVZQKaQ.*AA...AA*",*
   "successUrl": "http://example.com:80/index.html",
   "realm": "/"
   }
   + set +x
   Press enter to continue
   Demo user was authenticated with a correct password in transactional context, meaning it was performed in accordance to https://backstage.forgerock.com/docs/am/5.5/authorization-guide/#transactional-authorization-rest step 4
3. Press [Enter] to move on to policy evaluation to complete transactional authorization.
   re-evaluate transaction policy
   subject = demo user
   caller = agent user
   + jq .
   + curl --request POST 'http://openam.internal.example.com:8080/openam/json/realms/root/policies?_action=evaluate' --header 'Content-Type: application/json' --header 'iPlanetDirectoryPro:

```
4n22VdXcH5lBmahMyv23pGyfIgo.*AAJ....QAA*' --data '{
    "application": "iPlanetAMWebAgentService",
    "resources": ["http://example.com:80/index.html"],
    "subject": {
    "ssoToken": "USKVsq-AG9KXa93uCqj7SVZQKaQ.*AAJ....AA*"
 },
 "environment": {
    "foo": ["bar"],
    "TxId": ["cf311ec8-9050-46a8-aae9-0334f1d469e8"]
    } }'
 % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
100 511 0 121 100 390 959 3091 --:--:-- --:--:-- --:--:-- 3120
[{
    "advices": {},
    "ttl": 0,
    "resource": "http://example.com:80/index.html",
    "actions": {
    "POST": true,
    "GET": true
    },
    "attributes": {}
 }]
+ set +x
Press enter to continue
```

Note that you are getting policy evaluation result and transactional authorization is successful.

Running Transactional Authorization (Failure Case)

1. Edit run-setup.sh script line 277 and change demo 's passwd to an invalid password

   ```
   demo_password="changeit123"
   ```

2. Run run-setup.sh script again

   ```
   complete transaction Datastore authentication module callbacks
   caller = demo user with password : changeit1
   Demo password is invalid <============
   + jq .
   + curl -X POST 'http://openam.internal.example.com:8080/openam/json/authenticate?
   authIndexType=composite_advice&authIndexValue=%3CAdvices%3E%0A%3CAttributeValuePair%3E%0A
   %3CAttribute%20name%3D%22TransactionConditionAdvice%22%2F%3E%0A%3CValue%3Eef50788d-c9d6-
   4419-8801-803a3e43ae78%3C%2FValue%3E%0A%3C%2FAttributeValuePair%3E%0A%3C%2FAdvices%3E'
   --header 'Content-Type: application/json' --header 'iPlanetDirectoryPro: Cikmhbw1..QAA*' --header 'cookie:
   iPlanetDirectoryPro=CIkmhbw146ARF...QAA*' --data '
   {"authId":"eyJ0eXAiOiJKV1QiLCJhbGciOi...V8ABk","template":"","stage":"Datastore1","header":"Sign
   in","callbacks":[{"type":"NameCallback","output":[{"name":"prompt","value":"User Name:"}],"input":
   [{"name":"IDToken1","value":"demo"}]},{"type":"PasswordCallback","output":
   [{"name":"prompt","value":"Password:"}],"input":[{"name":"IDToken2","value":"changeit1"}]}]}'
   {
      "tokenId": "Cikmhbw146ARFHuK...MQAA*",
      "successUrl": "http://example.com:80/index.html",
      "realm": "/"
   }
   + set +x
   Press enter to continue
   ```

   Note the response to /authenticate endpoint returns HTTP response code 200 and gives you tokenId and success Url even though authentication should've failed. **THIS SUCCESS MESSAGE CONFUSES USER WHY THEY ARE NOT GETTING POLICY EVALUATION RESULT**

3. Step through and finish policy evaluation.

   ```
   re-evaluate transaction policy
   subject = demo user
   caller = agent user
   + jq .
   + curl --request POST 'http://openam.internal.example.com:8080/openam/json/realms/root/policies?
   _action=evaluate' --header 'Content-Type: application/json' --header 'iPlanetDirectoryPro:
   smchxnGUeQCIovXlLmZg3I....QAA*' --data ' {
   ```

```
    "application": "iPlanetAMWebAgentService",
    "resources": [ "http://example.com:80/index.html"],
    "subject": {
    "ssoToken": "Cikmhbw146ARFHuK103zs...QAA*"
    },
    "environment": {
        "foo": ["bar"],
        "TxId": ["ef50788d-c9d6-4419-8801-803a3e43ae78"]
} }'
 % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
100 489 0 99 100 390 570 2248 --:--:-- --:--:-- --:--:-- 2241
[ {
 "advices": {},
 "ttl": 0,
 "resource": "http://example.com:80/index.html",
 "actions": {},
 "attributes": {
```