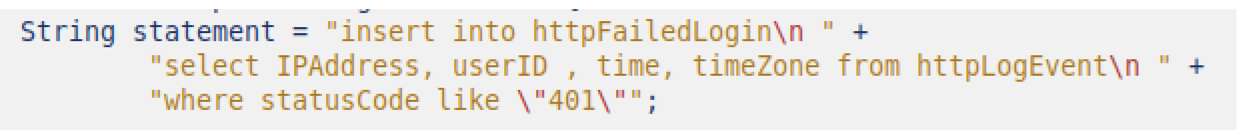
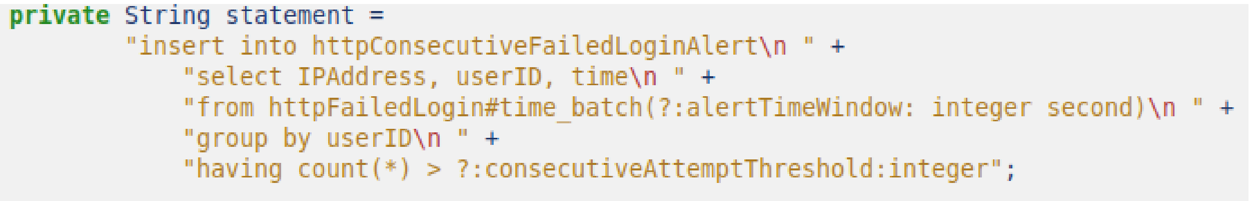
TASK : Classify Apache log messages for UnauthorizedAccessEvent

- Elements of the log used: IPAdress, userID, time, timezone.
- EPL statements:

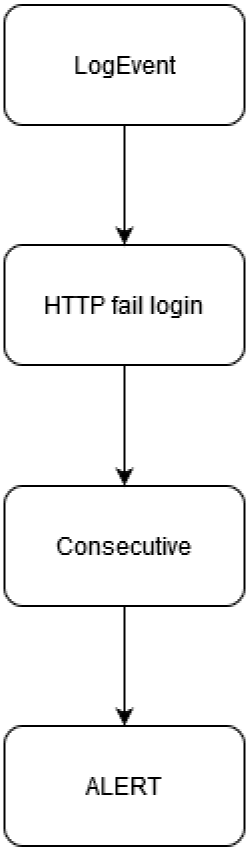


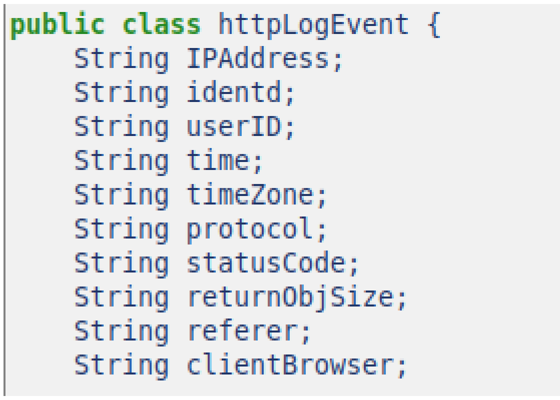
```
String statement = "insert into httpFailedLogin\n " +
        "select IPAddress, userID , time, timeZone from httpLogEvent\n " +
        "where statusCode like \"401\"";
```



```
private String statement =
        "insert into httpConsecutiveFailedLoginAlert\n " +
            "select IPAddress, userID, time\n " +
            "from httpFailedLogin#time_batch(?:alertTimeWindow: integer second)\n " +
            "group by userID\n " +
            "having count(*) > ?:consecutiveAttemptThreshold:integer";
```

- Event hierarchy





```
public class httpLogEvent {
    String IPAddress;
    String identd;
    String userID;
    String time;
    String timeZone;
    String protocol;
    String statusCode;
    String returnObjSize;
    String referer;
    String clientBrowser;
```

- In case of the status code is 401 is repeated, means that multiple fail login or unauthorized access, in the access.log in the path: /var/log/apache2/access.log, the web server will alert them based on their IPAddress, userID.