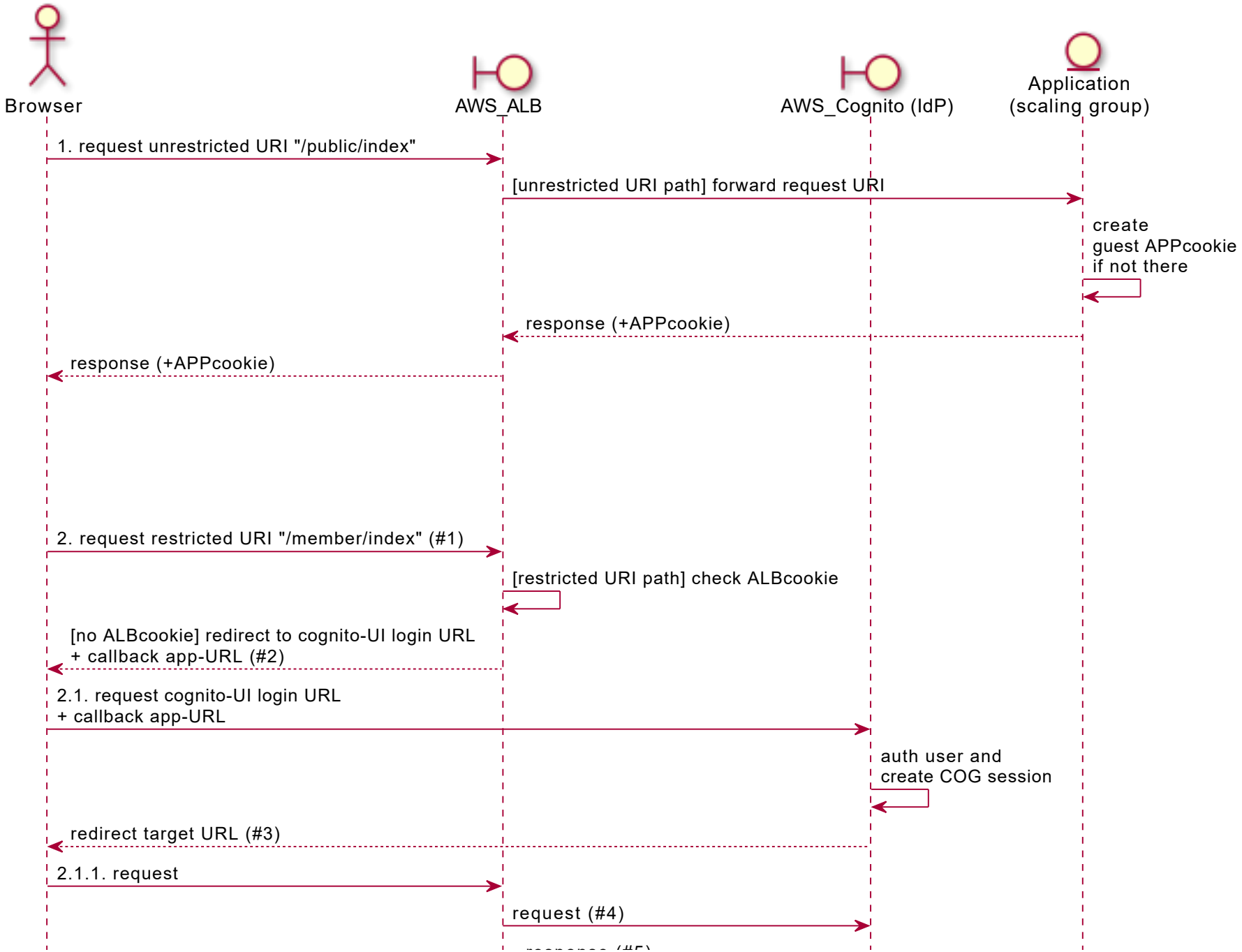
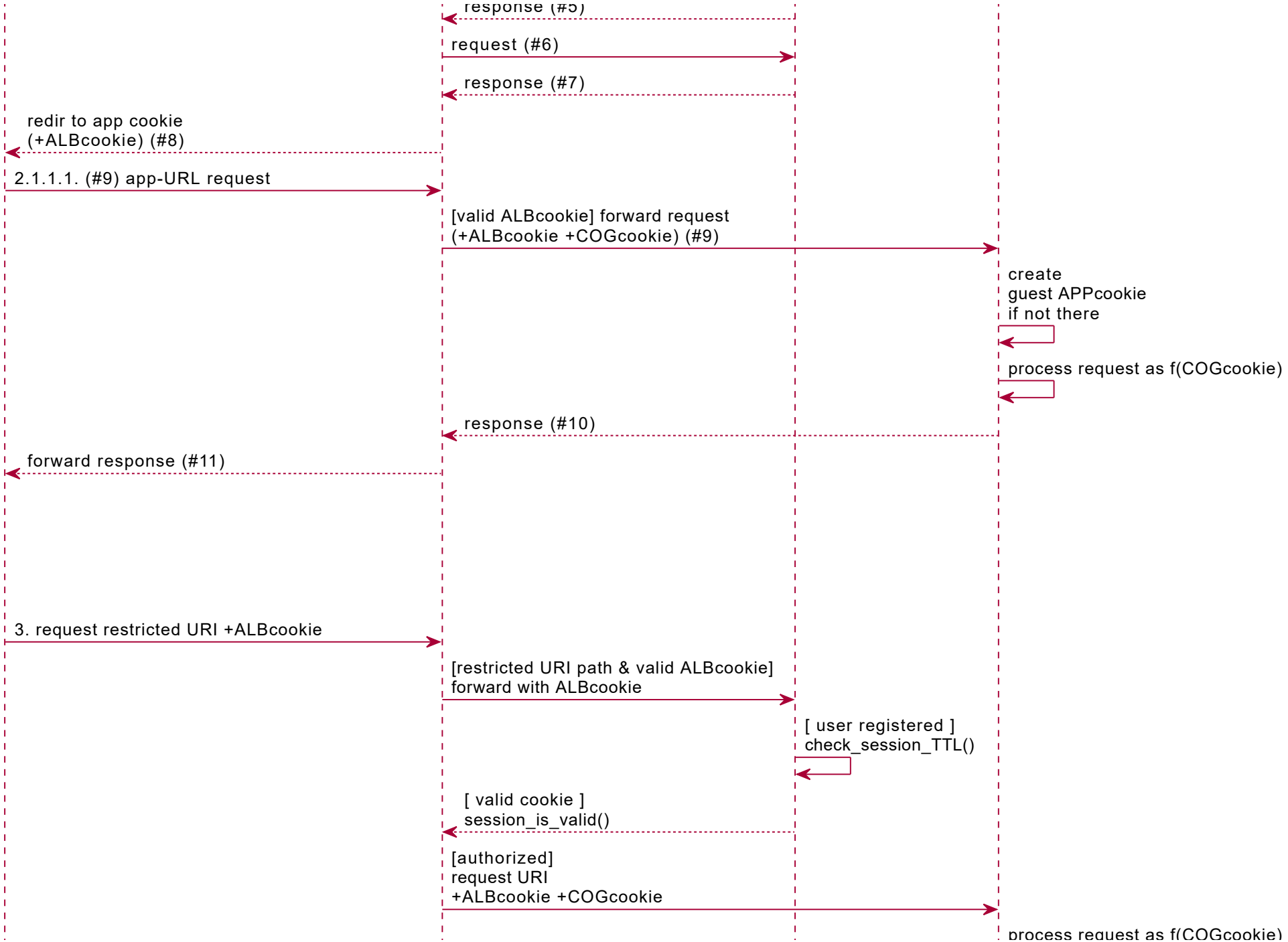
multiccy AUTH sequence diagram

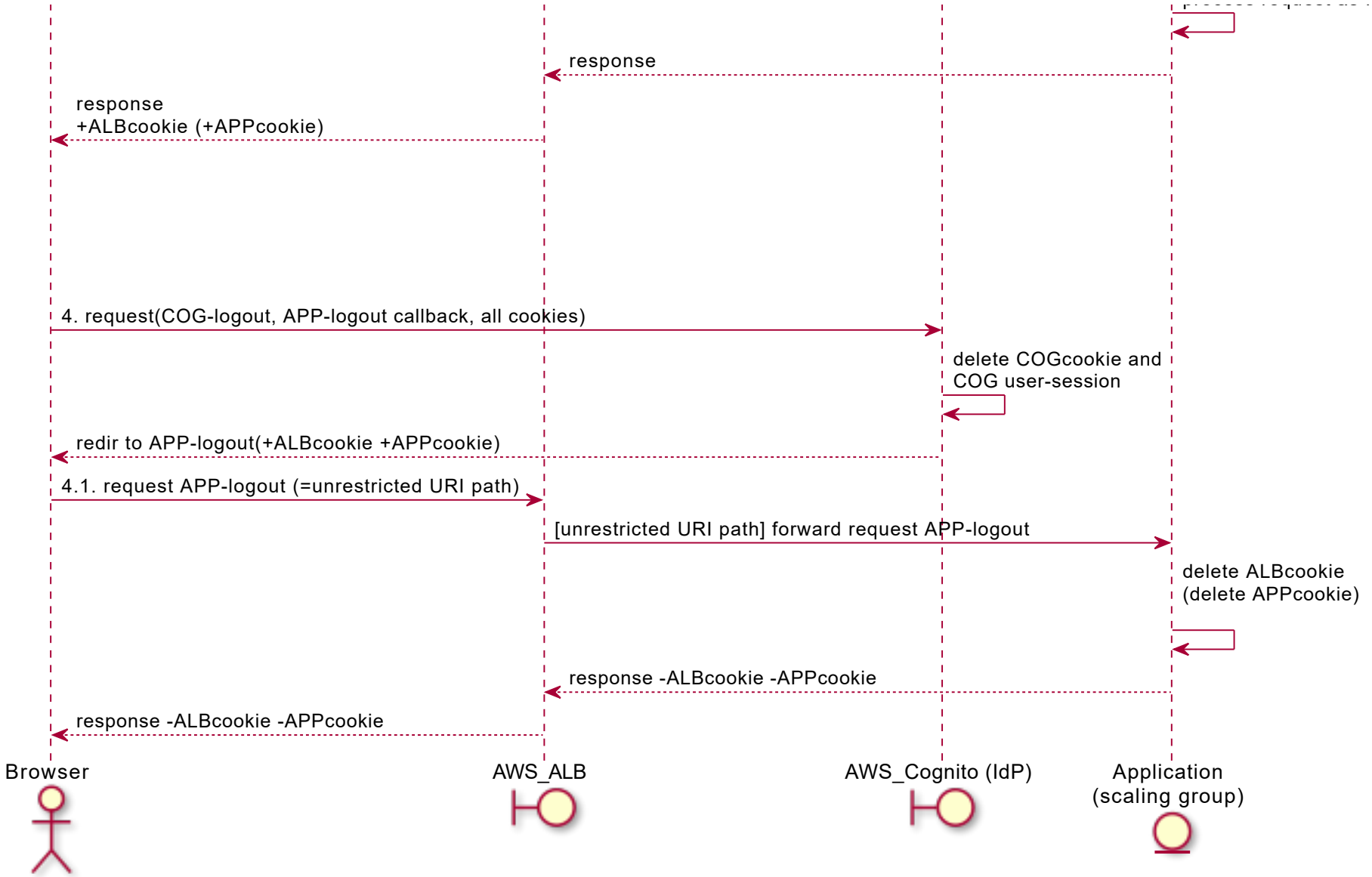
This is the sequence diagram of the http requests between your browser and
the application multiccy .
The IAM is managed by the combo AWS ALB + AWS Cognito IdP + AWS Cognito hosted UI.
With this combination, your application
does NOT have to:

- keep a users database;
- implement sign in, sign up, password reset services and emailing;
- use a session-management database like Redis/Dynamodb;
  should:
- be using the http header 'X-Amzn-Oidc-Identity', which is the authenticated cognito user id, as a session userid
- delete the AWSELBAuthSessionCookie in the logout callback URL call

---


Browser
AWS_ALB
AWS_Cognito (IdP)
Application
(scaling group)
1. request unrestricted URI "/public/index"
[unrestricted URI path] forward request URI
create
guest APPcookie
if not there
response (+APPcookie)
response (+APPcookie)
2. request restricted URI "/member/index" (#1)
[restricted URI path] check ALBcookie
[no ALBcookie] redirect to cognito-UI login URL
+ callback app-URL (#2)
2.1. request cognito-UI login URL
+ callback app-URL
auth user and
create COG session
redirect target URL (#3)
2.1.1. request
request (#4)


response (#5)
request (#6)
response (#7)
redir to app cookie
(+ALBcookie) (#8)
2.1.1.1. (#9) app-URL request
[valid ALBcookie] forward request
(+ALBcookie +COGcookie) (#9)
create
guest APPcookie
if not there
process request as f(COGcookie)
response (#10)
forward response (#11)
3. request restricted URI +ALBcookie
[restricted URI path & valid ALBcookie]
forward with ALBcookie
[user registered]
check_session_TTL()
[valid cookie]
session_is_valid()
[authorized]
request URI
+ALBcookie +COGcookie
process request as f(COGcookie)



by wrapping your application with AWS ALB + AWS Cognito + AWS Cognito hosted UI, the changes to apply to your application are:

- using request.getHeader('X-Amzn-Oidc-Identity') (= the authenticated cognito user id) as a session userid

- deleting the AWSELBAuthSessionCookie in the logout callback URL

ref: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html
the numbers in the AWS doc workflow are referenced as (#1) above.

cookies:

- X-Amzn-Oidc-Identity = cognito user id
- X-Amzn-Oidc-Data = JWT with e.g. username inside
- AWSELBAuthSessionCookie-xxx = ALB session cookie
- JSESSIONID = application session - irrelevant.

---

back to app-multiccy

© 2023 Alberto Moscatelli. All rights reserved. | Powered by Wiki.js