Task 3: Analysis for finding the sudden spike observed in login failure

**Identify the cause of the error:**

Most of the cases the client faces related failures are due to some backend glitch or failures.

To dig down to understand more about the error, the Newrelic tool can be used. The Http error details logged in New Relic will give more details about the failure.

The logs obtained from new relic will help to identify the cause and fix the problem.

If the issue is replicating, then debugging using the Charles proxy tool will help to identify which API is getting failed and what is the response which will helps the development team to fix the issue.

**Mitigation Plan:**

Case1: Glitch was caused due to some backend deployment.

Plans can be made to make sure that the deployments will be done during the less traffic time for the application so that the failures can be reduced.

Case2: Some issue with backend API and cannot identify the exact scenario.

Adding an additional logging mechanism which can provide the actual error code or message in the system on failure will help to understand further when similar issues happen in future.

Case3: Improve the information provide to user on error message while causing the error.

If the error was a glitch from backend and specific error code is identified while user face login issue, then a proper error message in a Lyman language can be provided to user instead of showing some technical message with error code.