# JumpCloud Hash Test – Test Summary

The JumpCloud password hash test was executed on 11/27/2017. Five test cases were created for this application based on the information described in the requirement document provide by HR to the candidate. Two of the test cases consistently fail, TC-01 - Issue a shutdown and verify that the server process is immediately restarted, and TC-05 – Verify that the hash returned from the server process is SHA512/Base64 encoded.

TC-01 fails inconsistently depending on when the server process was started and whether it was restarted by the host system or via a shutdown request issued by the client. When restarted by a shutdown request the server process will take anywhere from 10 – 30 minutes on average to restart.

TC-05 also fails inconsistently. The test computes a SHA512/base64 hash and compares that value to the hash returned by the server. If any of the hashes differ then the test is failed. The server does not appear to be incorrectly computing the hash, rather it appears to be storing the wrong hash in the wrong location.

In general, this was a difficult test to run because the server consistently took a very long time to restart whenever a shutdown was issued. In a normal situation I would expect to have access to the server host so that errors from the server could also be retrieved if they exist. Problems like the restart delay would normally be brought to the attention of the developers as soon as they are realized, which would have helped speed up the testing process.

With respect to other tests, I would probably increase the number of passwords passed to the server in tc-02 to see if it could handle a lot more than the 1000 that I posted in this test. I would also recommend a 48 - 72 hour test to ensure the server process was able to handle a continuous stream of password hashes.