JumpCloud Password Hash Test Plan

**November 10, 2017**

**Document Author(s):**

Ted Power

# IntroductionThis serves as the plan for testing the described software as well as the reporting of test results. The software being tested is a hashing application that resides on a hosted server. The application will receive http ‘post’ requests from clients and respond with a ‘job-id’ value indicating the location of a hash value for the password provided in the post operation. The hash values can be retrieved using http ‘get’ requests that contain the job-id provided from the post response.

1. **Test Approach**

This software will be tested from a client system by passing commands to the server process using HTTP requests. The server side will not be monitored directly for errors that occur on the server. Only errors passed back to the client or incorrect behaviors will be detected by these tests. The test results will indicate whether the results of the tests were able to verify that the server was responding with the corrected information. The test results will issue a PASS or FAIL at end of the test to show the final result of the test.

1. **Pass/Fail Criteria**

In keeping with most programming standards, a true(1) condition will indicate a failed condition and false(0) will indicate a pass. As the test program executes any failed condition within the program will generally set a failure flag to True. If the failure flag is True at the end of the test this will be an indicator that at least one step in the step had an error condition and the entire test will be failed. Any tests that use a negative test condition as a pass will invert this logic at the end and issue a pass.

1. **Test Cases**

|  |  |  |  |
| --- | --- | --- | --- |
| Test ID | Description | Expected Results | Actual Results |
| TC-01 | Issue a shutdown and verify that the server process is immediately restarted. | Pass | Fails inconsistently |
| TC-02 | Simultaneously post passwords without retrieving the computed hash for them. This test will validate that the server can receive simultaneous posts without losing any or crashing. A status of 200 indicates the post was accepted. | Pass | Pass |
| TC-03 | Simultaneously post passwords and then retrieve computed hash for each password posted. This tests that a hash can be retrieved for each password posted. | Pass | Pass |
| TC-04 | Simultaneously post a set of passwords, issue a shutdown, and post a second set of passwords. The first set of passwords should all get issued a hash and the second set of passwords should be rejected since they were posted after the shutdown was issued. A status of 503 indicated the post was rejected. | Pass | Pass |
| TC-05 | Verify that the hash is sha512/base64. Post a set of passwords, retrieve the hash, compute a sha512/base64 hash, and compare the values. The test passes if the compared hashes match. | Pass | Fails inconsistently |

1. **Test Deliverables**

* Test log
* Test incident report
* Test summary report

# Environmental Requirements

* Hardware: User laptop and hosted server running password hash process.
* Network: Network access to server process via HTTP requests on port 80.
* Testing software/tools: Using Ubuntu 16.04 Linux on Oracle VirtualBox.

# StaffingTesting will utilize one person to develop and execute the tests.

# Schedule

|  |  |  |
| --- | --- | --- |
| Step | Duration | Owner |
| Test Plan | 2 days | Ted P. |
| Test Development | 1 wk | Ted P. |
| Test Reporting | 1 day | Ted P. |

# Risks and ContingenciesThe following risks have been identified for this project.

|  |  |  |
| --- | --- | --- |
| Risk | Risk Level | Contingencies/Mitigation |
| Server is unavailable | Low | Notify management of problem. Test completion time pushed out. |
| Network is unavailable | Low | Go to place with free Wi-Fi. Notify management of network issues. |
| Hardware failure | Low | Use backup PC. Notify management. |