

Useful F5 Log Queries

Introduction

If you work with F5 BIG-IP you maybe need to know for example when a cluster failover has happened or a user has done some changes.

The following will describe some useful F5 log queries which you can use on the F5 logs or any central syslog server you're sending the F5 logs to.

F5 LTM Log Queries

Check in the Admin UI at System - Logs: Local Traffic

| Research | Log Query |
|--|--|
| Show cluster switchover of a F5 BIG-IP | <div><i>HA unit 1 state change</i><div><p>“ Example output: Jul 22 21:19:04 bigip1 notice tmm1[11529]: 01340011:5: HA unit 1 state change: from 1 to 0.</p></div></div> |

F5 Audit Log Queries

Check in the Admin UI at System - Logs: Audit: List

| Research | Log Query |
|----------|-----------|
|----------|-----------|

Show which user has done changes

transaction

“ Example output:
client tmui, user username@bigip1
- transaction #1067178-8 - object 0
- create { pool_member {
pool_member_pool_name
"/Common/pool_name"
pool_member_node_name
"/Common/node1"
pool_member_port 9020
pool_member_inherit_profile 1
pool_member_update_status 1
pool_member_priority 0
pool_member_ratio 1
pool_member_conn_limit 0
pool_member_addr 1.2.3.4 } }
[Status=Command OK]: