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.

All possible F5 Log Messages can be found here:

https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/releasenotes/related/log-messages.html

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 See here: 01340001 : HA Connection with peer %la:%d for traffic-group %s established 01340002 : HA Connection with peer %la:%d for traffic-group %s lost	**HA Connection with peer** Example output: " Apr 8 07:56:42 bigip1 err slot1 tmm3[20728]: 01340001:3: HA Connection with peer 1.2.3.4:32770 for traffic-group /Common/traffic-group-1 established.
TMM is very busy or is stalled. See here: K10095: Error Message: Clock advanced by <number> ticks Any value higher than 1000 does show a problem with too high load.	**Clock advanced by** Example output: " Apr 8 16:12:59 bigip1 notice slot1 tmm[18639]: 01010029:5: Clock advanced by 103 ticks

A Virtual Server is under high load	Syncookie counter
See here: [01010038 : Syncookie counter %d exceeded vip threshold %u for virtual = %A:%d](#) If the message shows multiple times there's maybe an attack going on or a high load on the Virtual Server.	Example output: > " Mar 21 09:24:33 bigip1 warning slot1 tmm1[20805]: 01010038:4: Syncookie counter 1500 exceeded vip threshold 1499 for virtual = 1.2.3.4:443
Pool Member change	**now has available members**
See here: [01010221 : Pool %s now has available members](#) The pool may have had no available members due to administrative action, monitors, connection limits, or other constraints on pool member selection.	Example output: > " Apr 8 16:33:53 bigip1 notice slot1 tmm1[18800]: 01010221:5: Pool /Common/pool_MyPool now has available members
Status change detected on Pool	**monitor status up**
See here: [01070727 : "Pool %s member %s:%u monitor status up."](#) This message is logged when a status change is detected for the pool member.	Example output: > " Apr 8 16:17:42 bigip1 notice slot1 mcpd[5587]: 01070727:5: Pool /Common/pool_MyPool member /Common/_auto_1.2.3.4:443 monitor status up. [/Common/https_Monitor: up] [was down for 0hr:1min:59sec]
Machine Boot or mcpd restart	**The MCP is up and running**
See here: [01070427 : Initialization complete. The MCP is up and running](#) the **mcpd** process generates this message during the normal boot process after the configuration loads and **mcpd** reaches a running phase. **Services are down when mcpd is restarted.**	Example output: > " notice mcpd[<PID>]: 01070427:5: Initialization complete. The MCP is up and running

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]:

Revision #14
Created 23 July 2024 13:49:51 by Peter Baumann
Updated 8 April 2025 18:03:18 by Peter Baumann