Intrusion Report #4- 2:00 PM - 4:00 PM

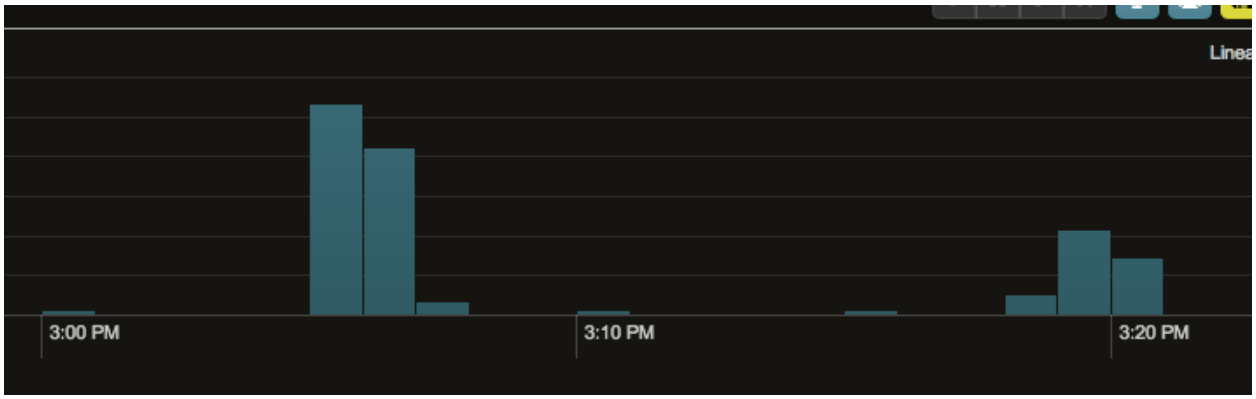
Team 14 - Honeybadger

State of team14.isucdc.com

All services are now online and operating as intended. There have been no major incidents to report in the past two hours. However, there was some increased activity around 2:50 - 3:00 PM. These findings are outlined below.

Web

Around 3:05 PM, we had an unusual amount of traffic to our web application. There were approximately 50 requests in less than a minute.This is what our traffic graph looked like:

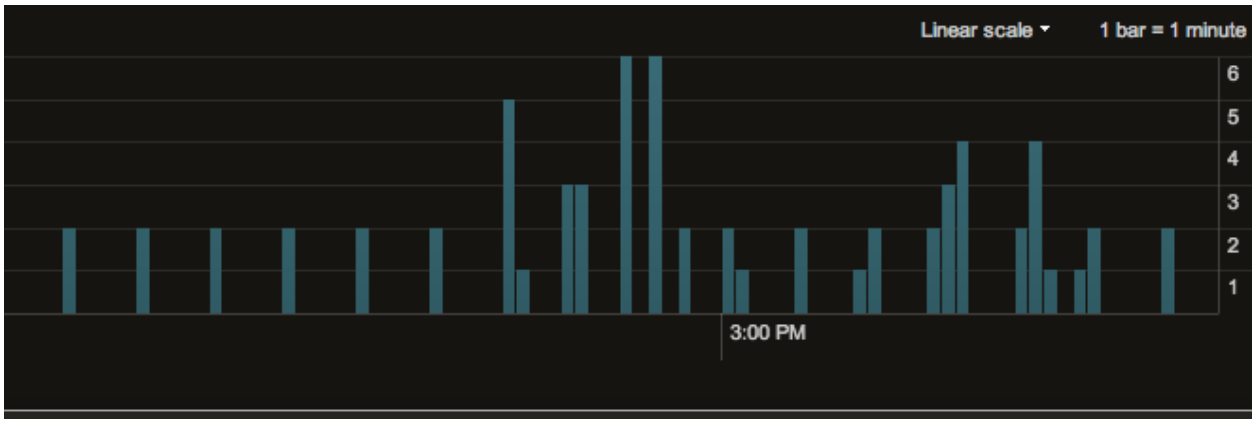


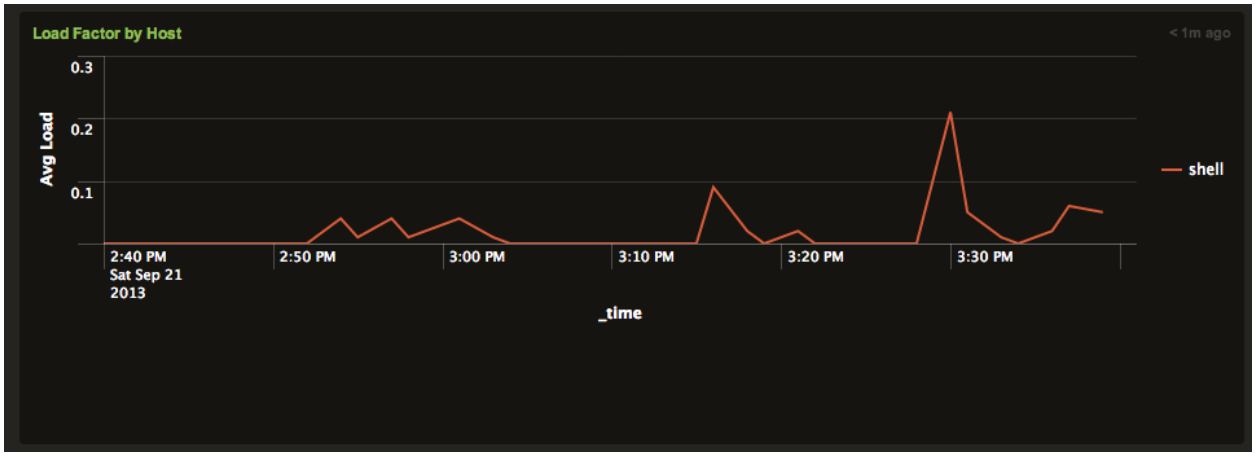
Shell

Examples of shell auth failures from 2:00 to 4:00:

Sep 21 14:53:31 shell sshd[13909]: Failed password for ben from 199.100.101.16 port 59710 ns
Sep 21 14:55:37 shell sudo: pam_unix(sudo:auth): authentication failure; logname=matt uid=10048 euid=0 tty=/dev/pts/7 ruser=matt rhost= user=matt

A graph of the failures is here:

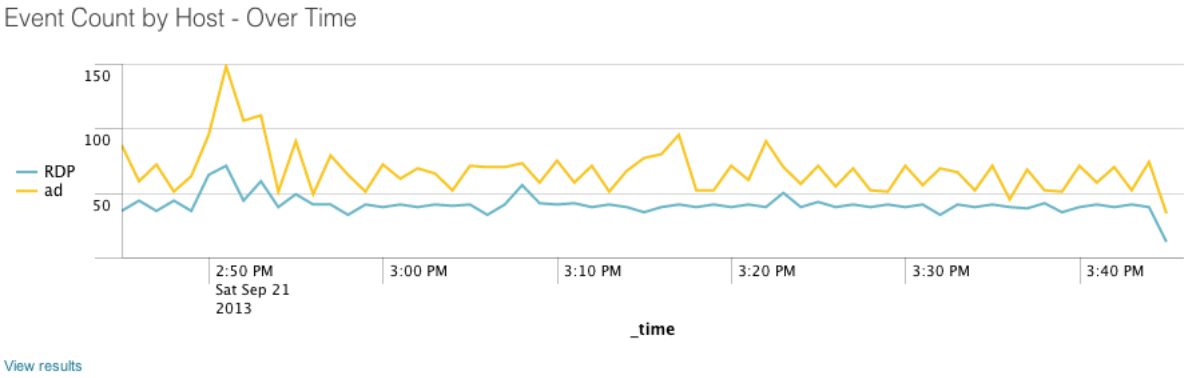




This is the load factor for the shell box from 2:40 until 3:40. The few bumps just before 3:00 seem to correlate with the peak ssh failures around the same time.

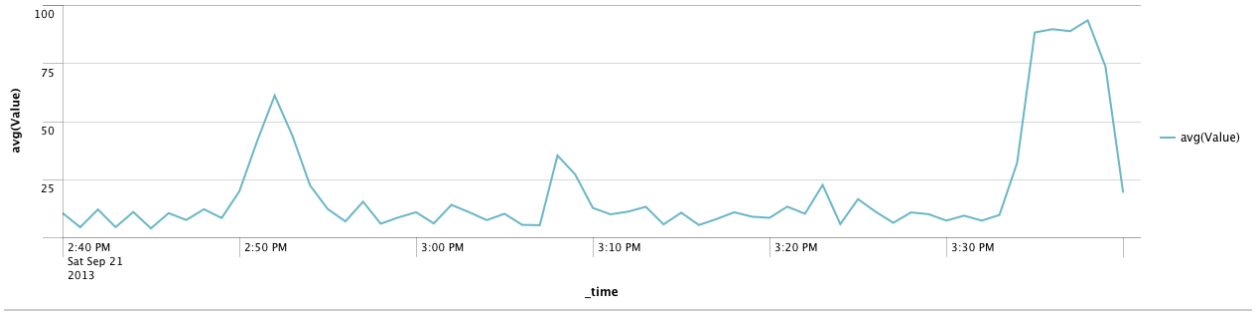
AD

We had some increased events around 2:50. This was similar to the RDP service, as well as others.



RDP

We have noticed a rapid increase on the cpu load on the RDP server over last half hour (since 3:30 PM)



Owncloud

We have not seen any unusual activity on this service. We have had no failed SSH logins in the last two hours.

We had a peak request amount of 33 around 3:20 PM. This can be seen here: