**Summary of findings on r-001-03/22/2016 Logfile**

The initial tags which are of the form <x> that precede any statement in the log file were analysed for frequency:

1. **Count of each Tag No. at the start of the file:**

|  |  |
| --- | --- |
| Tag No | Count |
| 15 | 2751 |
| 30 | 1343 |
| 86 | 594 |
| 28 | 380 |
| 29 | 185 |
| 78 | 161 |
| 38 | 154 |
| 4 | 99 |
| 14 | 71 |
| 77 | 68 |
| 27 | 60 |
| 83 | 42 |
| 6 | 10 |
| 22 | 7 |
| 31 | 6 |
| 18 | 2 |
| 43 | 2 |
| 189 | 1 |
| 6 | 1 |
| 5 | 1 |
| 12 | 1 |

1. **Different tag names and the corresponding tag number were analysed to check if same name has multiple tag numbers.**

|  |  |  |
| --- | --- | --- |
| tag\_name | tag\_no | Frequency |
| CROND | 78 | 137 |
| NET | 189 | 1 |
| anacron | 77 | 12 |
| avahi-daemon | 28 | 1 |
|  | 30 | 22 |
| crontab | 78 | 24 |
| dhclient | 30 | 10 |
| dracut | 12 | 1 |
|  | 14 | 64 |
|  | 15 | 2751 |
| kernel | 4 | 99 |
|  | 5 | 1 |
|  | 6 | 10 |
| network | 30 | 8 |
| nscd | 29 | 27 |
| nslcd | 27 | 60 |
|  | 30 | 1 |
| ntpd | 30 | 12 |
|  | 31 | 3 |
| puppet-agent | 29 | 158 |
| rdma-ndd | 30 | 2 |
| rhnsd | 31 | 3 |
| rsyslogd | 46 | 1 |
| rsyslogd-2307 | 43 | 2 |
| run-parts( | 77 | 56 |
| sendmail | 18 | 2 |
|  | 22 | 5 |
| sm-msp-queue | 22 | 2 |
| sshd | 83 | 42 |
|  | 86 | 593 |
| systemd | 28 | 379 |
|  | 30 | 1288 |
| systemd-logind | 38 | 154 |
| usermod | 86 | 1 |
| yum | 14 | 7 |

1. **Similar check for tag number; Different tag numbers were analysed to find if there are multiple tag numbers with same tag name**

|  |  |  |
| --- | --- | --- |
| tag\_no | tag\_name | frequency |
| 4 | kernel | 99 |
| 5 | kernel | 1 |
| 6 | kernel | 10 |
| 12 | dracut | 1 |
| 14 | dracut | 64 |
|  | yum | 7 |
| 15 | dracut | 2751 |
| 18 | sendmail | 2 |
| 22 | sendmail | 5 |
|  | sm-msp-queue | 2 |
| 27 | nslcd | 60 |
| 28 | avahi-daemon | 1 |
|  | systemd | 379 |
| 29 | nscd | 27 |
|  | puppet-agent | 158 |
| 30 | avahi-daemon | 22 |
|  | dhclient | 10 |
|  | network | 8 |
|  | nslcd | 1 |
|  | ntpd | 12 |
|  | rdma-ndd | 2 |
|  | systemd | 1288 |
| 31 | ntpd | 3 |
|  | rhnsd | 3 |
| 38 | systemd-logind | 154 |
| 43 | rsyslogd-2307 | 2 |
| 46 | rsyslogd | 1 |
| 77 | anacron | 12 |
|  | run-parts( | 56 |
| 78 | CROND | 137 |
|  | crontab | 24 |
| 83 | sshd | 42 |
| 86 | sshd | 593 |
|  | usermod | 1 |
| 189 | NET | 1 |

1. **Tag Name and Number following it. There is a number following some tag names which could possibly belong to a process. Since there were 100s of these entries, we have just given some results for 1 tag as an example:**

|  |  |  |
| --- | --- | --- |
| tag\_name | tag\_name\_foll\_no | frequency |
| CROND | 384 | 1 |
|  | 393 | 1 |
|  | 394 | 1 |
|  | 491 | 1 |
|  | 932 | 1 |
|  | 1021 | 1 |
|  | 1127 | 1 |
|  | 1135 | 1 |
|  | 1223 | 1 |

1. **Times when commands have been run with frequency of commands.**

|  |  |
| --- | --- |
| 11:00 - 12:00 | 3179 |
| 17:00 - 18:00 | 269 |
| 20:00 - 21:00 | 267 |
| 23:00 - 24:00 | 261 |
| 18:00-19:00 | 260 |
| 22:00-23:00 | 257 |
| 21:00-22:00 | 255 |
| 19:00-20:00 | 255 |
| 16:00-17:00 | 214 |
| 13:00-14:00 | 193 |
| 12:00-13:00 | 179 |
| 14:00-15:00 | 178 |
| 15:00-16:00 | 172 |

1. **Time Slots and frequent commands at that time:**

**Just for the time period 11:00 AM – 12 Noon, what all commands were run and what is the frequency of each command.**

|  |  |  |
| --- | --- | --- |
| 11 | CROND | 2 |
|  | NET | 1 |
|  | avahi-daemon | 23 |
|  | dhclient | 4 |
|  | dracut | 2816 |
|  | kernel | 13 |
|  | network | 8 |
|  | nscd | 14 |
|  | nslcd | 1 |
|  | ntpd | 15 |
|  | puppet-agent | 105 |
|  | rdma-ndd | 2 |
|  | rsyslogd | 1 |
|  | rsyslogd-2307 | 2 |
|  | sendmail | 7 |
|  | sm-msp-queue | 2 |
|  | sshd | 12 |
|  | systemd | 146 |
|  | usermod | 1 |
|  | yum | 4 |