

PSU MacAdmin 2012 - Logs, Damn Logs and Statistics

Edward Marczak (marczak@radiotope.com @marczak)

References:

Ren & Stimpy - http://en.wikipedia.org/wiki/The_Ren_%26_Stimpy_Show

Flying Spaghetti Monster - http://en.wikipedia.org/wiki/Flying_Spaghetti_Monster

Privilege Denying Dude meme - <http://knowyourmeme.com/memes/privilege-denying-dude>

<http://jezebel.com/5698261/meet-your-new-privilege+denying-dude>

Star Trek - http://en.wikipedia.org/wiki/Star_Trek

Talking Heads - http://en.wikipedia.org/wiki/Talking_Heads

Contail (Screen Saver) - <https://github.com/marczak/contail>

Logstalgia (Log visualizer) - <https://github.com/acaudwell/Logstalgia>

Splunk - <http://www.splunk.com/>

GrayLog2 - <http://graylog2.org/>

PartyLog - <http://sourceforge.net/projects/partylog2/>

PaperTail - <http://www.papertrailapp.com>

R (statistics programming language) - <http://www.r-project.org/>

Google Refine - <http://code.google.com/p/google-refine>

Syslog Facility

notice

authpriv

remoteauth

ftp

install

internal

kern

mail

Syslog Severity (Priority)

Emergency (level 0)

Alert (level 1)

Critical (level 2)

Error (level 3)

Warning (level 4)

Notice (level 5)

Info (level 6)

Debug (level 7)

Bash Logging

```
logger -p local7.notice -i "Changing interface."
```

Obj-C Logging

```
NSLog(@"theFile is now %@.", theFile);
```

Python Logging

```
import logging
```

```
import logging.handlers
```

```
logging.basicConfig(level=debug_level, format='%(levelname)s: %(message)s')
```

```
syslog = logging.handlers.SysLogHandler('/var/run/syslog')
```

```
syslog.setFormatter(logging.Formatter('%(name)s: %(message)s'))
```

```
syslog.setLevel(debug_level)
```

```
logging.getLogger().addHandler(syslog)
```

```
logging.info('This is a python log message %s', some_var)
```

Ruby Logging

```
require 'syslog'
```

```
Syslog.open('AppName')
```

```
Syslog.crit('This is a ruby log message.')
```

```
Syslog.close
```

Utilities

```
cat /path/to/file
```

```
bzcat /path/to/file.bz2
```

```
tail -f /path/to/file
```

```
less /path/to/file
```

```
syslog -k Sender UserEventAgent -k Time ge -2h
```