LaaS: Log Analytics as a Service

SMI Enterprise Automation Brazil
Nov-01-2017

Hugo do Prado
hprado@br.ibm.com

http://about.me/hugo_prado

Felipe Silveira
fsilveir@br.ibm.com

http://about.me/felipesilveira

github.com/IBM-SMI-Brazil/LaaS

Why Log Analytics is Important?

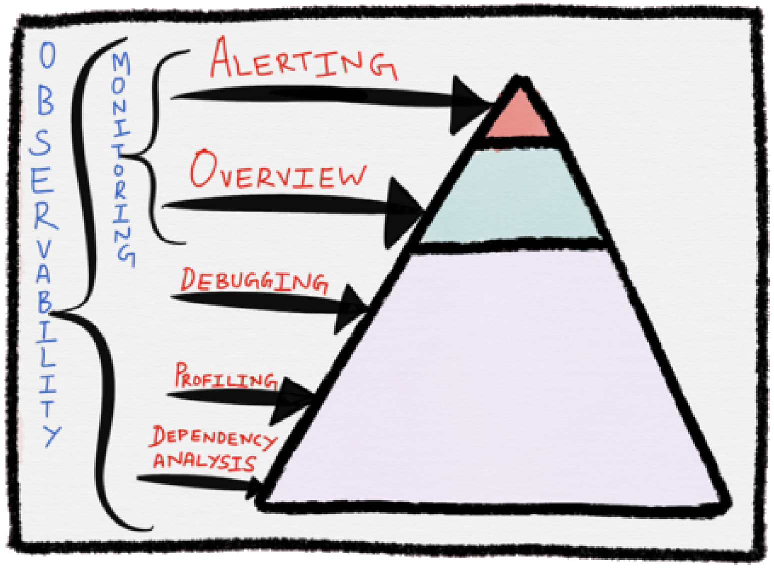
"People respond to facts. Rational people will make rational decisions if you present them with the right data."

Linda Sanford, Senior Vice President, Enterprise Transformation, IBM

But why now?

"Observability is a measure of how well internal states of a system can be inferred from knowledge of its external outputs."

Rudolf E. Kálman (Control Theory)

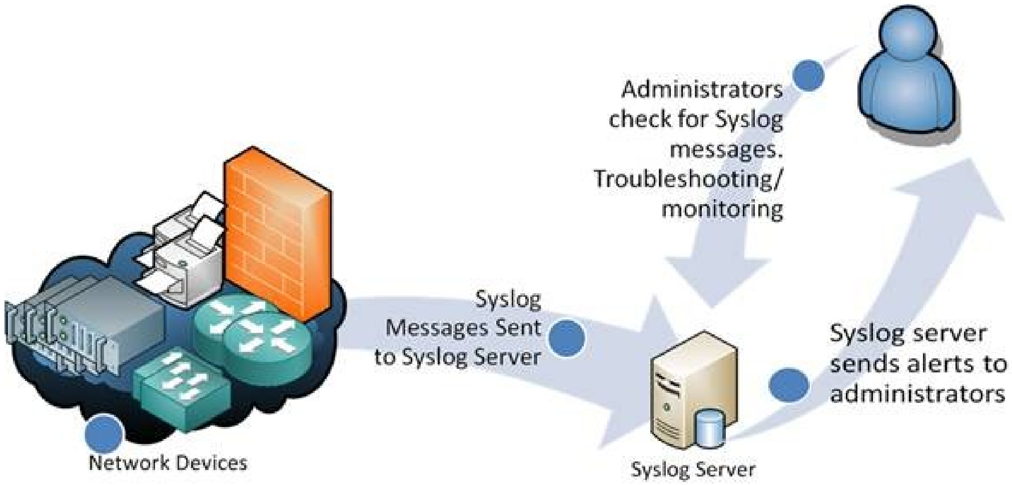


- R = Rate (Ex. Request Throughput, in requests per second)
- E = Errors (Ex: Request Error Rate, as either a throughput metric or a fraction of overall throughput)
- D = Duration (Ex: Latency, Residence Time, or Response Time; all three are widely used)

- U = Utilization, as canonically defined
- S = Concurrency
- E = Error Rate, as a throughput metric

- Alerting Visualization
- Distributed System Traccing
- **Log Aggregation/Analytics**

What is SysLog and why people use it?


Administrators check for Syslog messages. Troubleshooting/ monitoring
Syslog Messages Sent to Syslog Server
Syslog server sends alerts to administrators
Network Devices
Syslog Server

Syslog, is a standardized way (or Protocol) of producing and sending Log and Event information from Unix/Linux and Windows systems (which produces Event Logs) and Devices (Routers, Firewalls, Switches, Servers, etc) over UDP Port 514 to a centralized Log/Event Message collector which is known as a Syslog Server.

One of the main reasons Syslog was so widely accepted throughout the industry was because of its simplicity – There is little to no uniformity or standardization when it comes to the content that a Device, Server or Operating system is written and sends log information.

But more isn’t always better…

“One person’s data is another person’s noise.”

K.C. Cole – ‘The Universe and the Teacup’

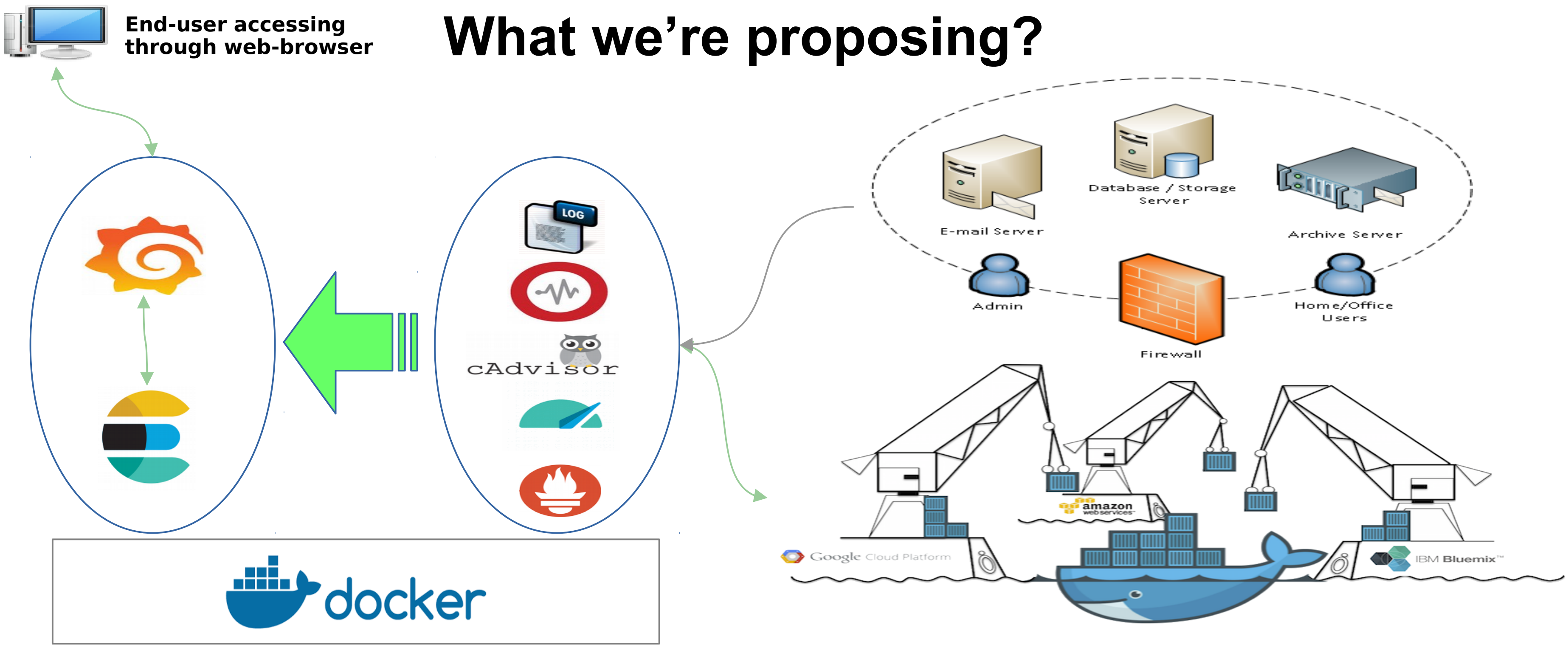
- Kernel messages
- User-level messages
- Mail System
- System Daemons
- Security/Authorization Messages
- Messages generated by syslogd
- Line Printer Subsystem

- Network News Subsystem
- UUCP Subsystem
- Clock Daemon
- Security/Authorization Messages
- FTP Daemon
- NTP Subsystem
- Log Audit
- Log Alert
- Clock Daemon

Our goal is to help supporting teams on finding patterns and trends from their logs, connecting the dots from multiple sources through a consolidated view

If your application writes a log, we'll track it!

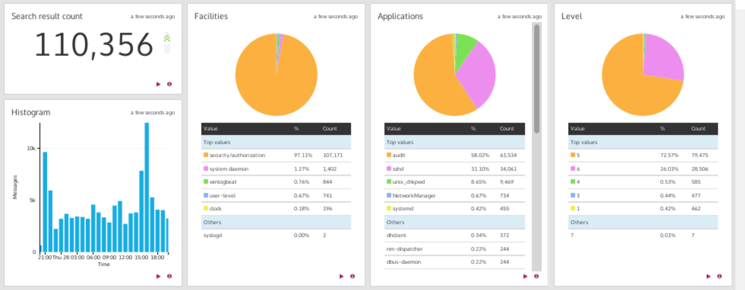
What we’re proposing?



- A scalable open-source alternative to be offered as a service
- Fast deploys through pre-customized docker images
- Minimum customization required to forward the logs to a central stash
- Historic view to assist troubleshooting, analytics and on the creation of relevant KPI’s
- Easy access to data withouth SQL queries
- Easily adaptable to Cloud, On-Premisses or Hybrid environments
- Correlates metrics and logs so you can find trends about your servers and their applications
- Can perform cross-server queries, giving a big picture of their overall performance
- Data is safely protected on a central stash, far from the access from the privilege users that have adminitrator roles on the monitored devices

And what does it look like?

- Single dashboard regardless of platform
- Real-time and historic metrics on a lightweight web page



Facilities

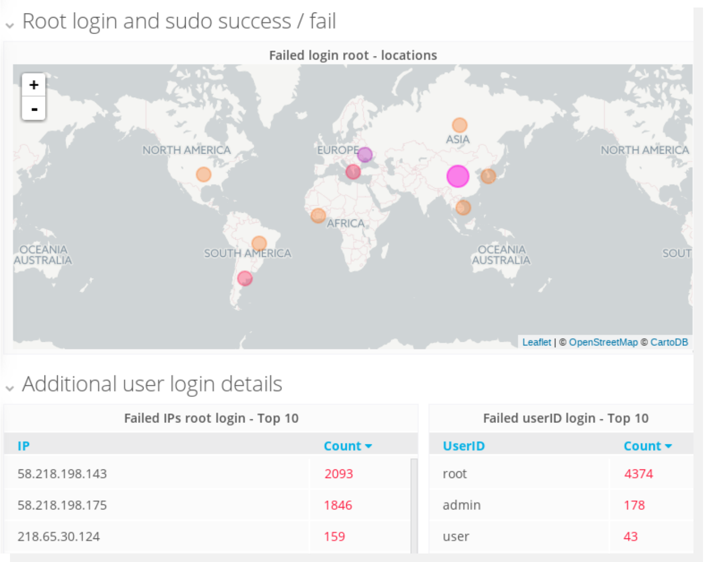
Value	%	Count
Top values		
🟧 security/authorization	97.11%	107,171
🟪 system daemon	1.27%	1,402
🟩 winlogbeat	0.76%	844
🟦 user-level	0.67%	741
🟨 clock	0.18%	196
Others		
syslogd	0.00%	2

Applications

Value	%	Count
Top values		
🟧 audit	58.02%	63,534
🟪 sshd	31.10%	34,061
🟩 unix_chkpwd	8.65%	9,469
🟦 NetworkManager	0.67%	734
🟨 systemd	0.42%	455
Others		
dhclient	0.34%	372
nm-dispatcher	0.22%	244
dbus-daemon	0.22%	244

Level

Value	%	Count
Top values		
🟧 5	72.57%	79,475
🟪 6	26.03%	28,506
🟩 4	0.53%	585
🟦 3	0.44%	477
🟨 1	0.42%	462
Others		
7	0.01%	7



⌄ Root login and sudo success / fail

Failed login root - locations

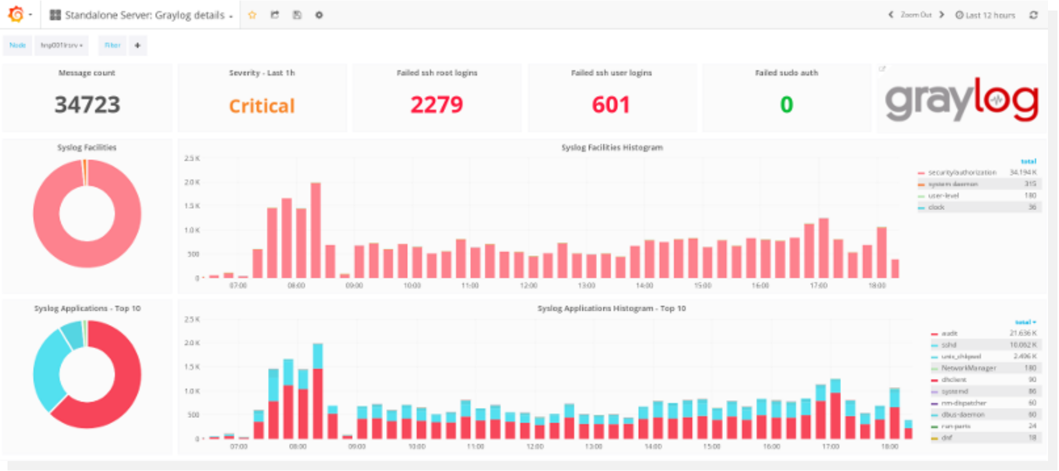
⌄ Additional user login details

Failed IPs root login - Top 10

IP	Count ▾
58.218.198.143	2093
58.218.198.175	1846
218.65.30.124	159

Failed userID login - Top 10

UserID	Count ▾
root	4374
admin	178
user	43

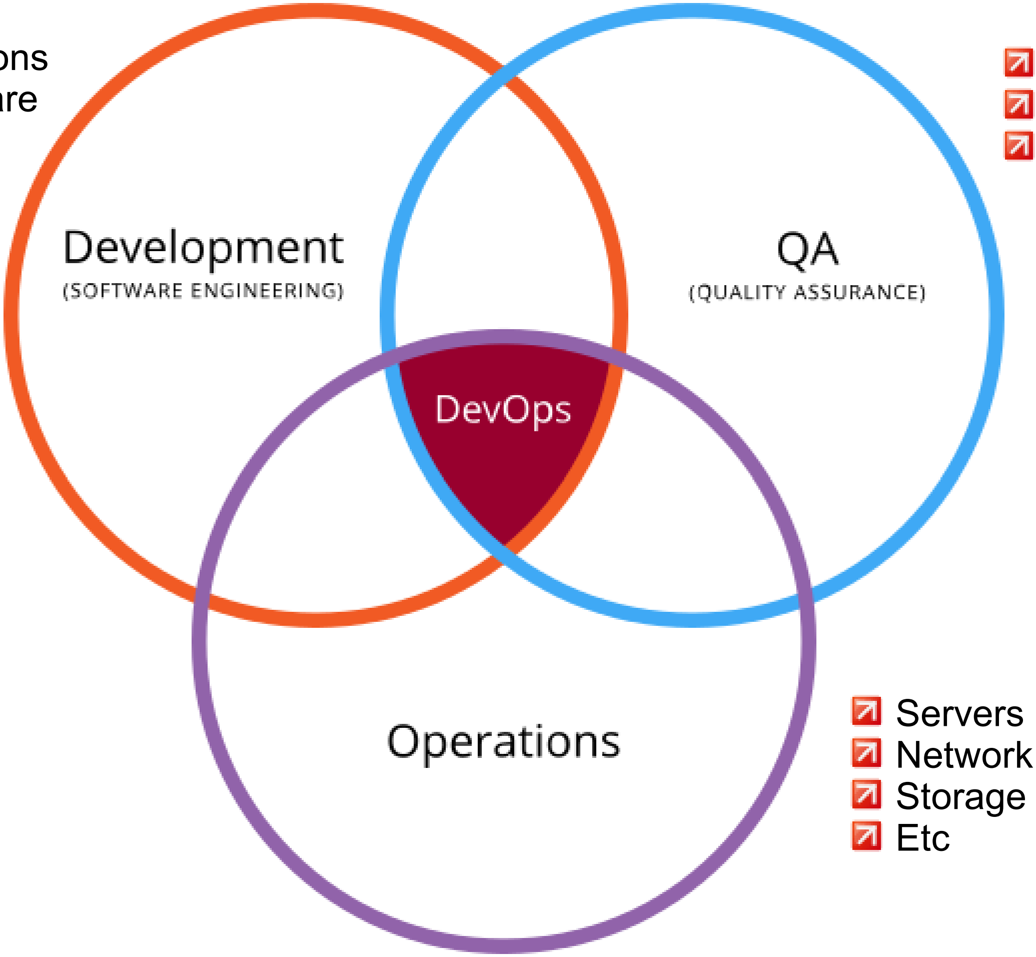


Message count	Severity - Last 1h	Failed ssh root logins	Failed ssh user logins	Failed sudo auth
34723	Critical	2279	601	0

Metrics and analytics extracted from log messages make auditing and troubleshoot easier

- History of executed commands (with userID, terminal and IP)
- Login attempts, (success/fail logins, sudo attemps, with ID, source terminal, and geo-location)
- HTTP response errors, with the IP and a geo-location on a visual map
- **Creativity is the limit, Application owners and SME’s can request almost any type of visualization!**

And to Who We're Offering?



- Applications
- Middleware
- Etc

- Incident / Problem Mgt
- Change Management
- RCA's

- Servers
- Network Devices
- Storage Appliances
- Etc

- Security & Auditing

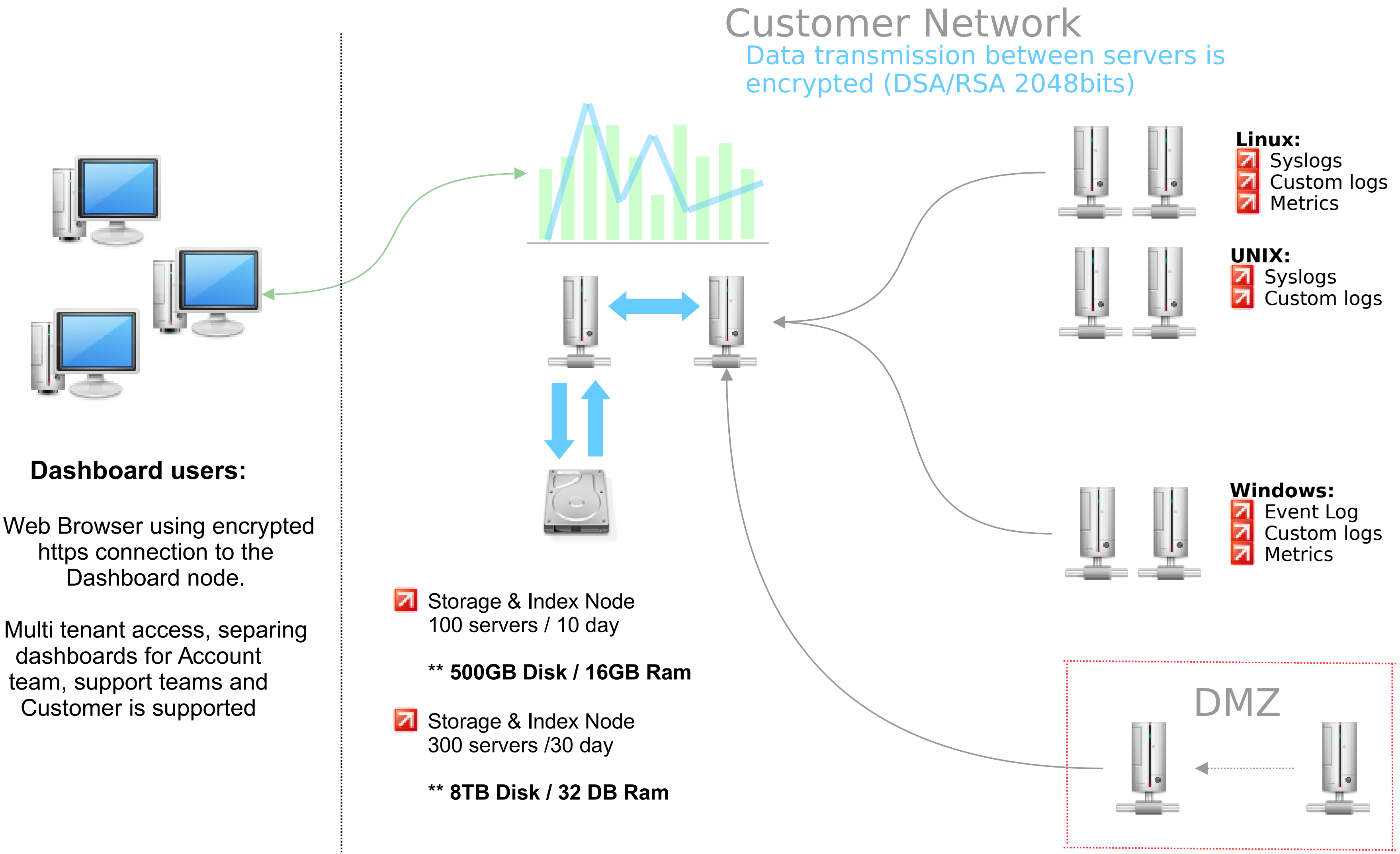
Who are the other competitors?

splunk>®

sumologic

LOGGLY

What’s the Basic Setup?



Customer Network

Data transmission between servers is encrypted (DSA/RSA 2048bits)

Dashboard users:

- Web Browser using encrypted https connection to the Dashboard node.
- Multi tenant access, separing dashboards for Account team, support teams and Customer is supported

- Storage & Index Node
  100 servers / 10 day

  ** **500GB Disk / 16GB Ram**

- Storage & Index Node
  300 servers /30 day

  ** **8TB Disk / 32 DB Ram**

Linux:

- Syslogs
- Custom logs
- Metrics

UNIX:

- Syslogs
- Custom logs

Windows:

- Event Log
- Custom logs
- Metrics

Thank you!!!