LaaS: Log Analytics as a Service

SMI Enterprise Automation Brazil

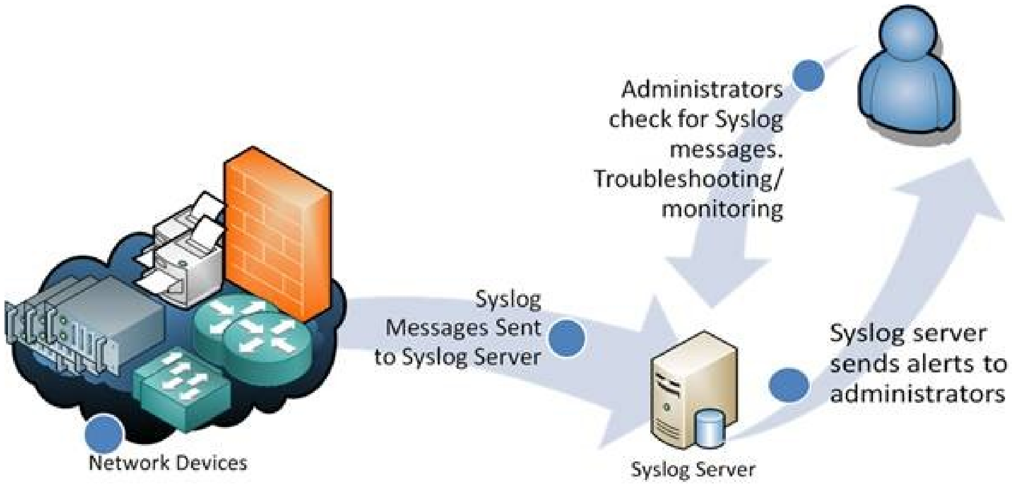
Oct-16-2017

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

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 – Author of The Universe and the Teacup

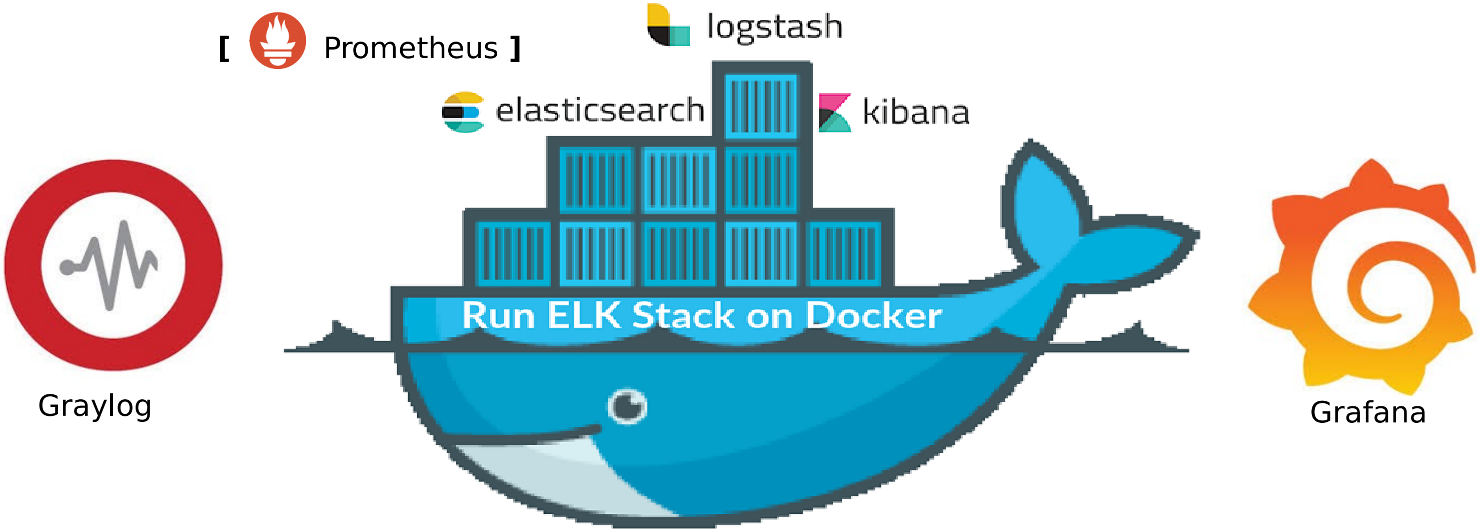
- Kernel messages
- User-level messages
- Mail System
- System Daemons
- Security/Authorization Messages
- Messages generated by syslogd
- Line Printer Subsystem

- 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

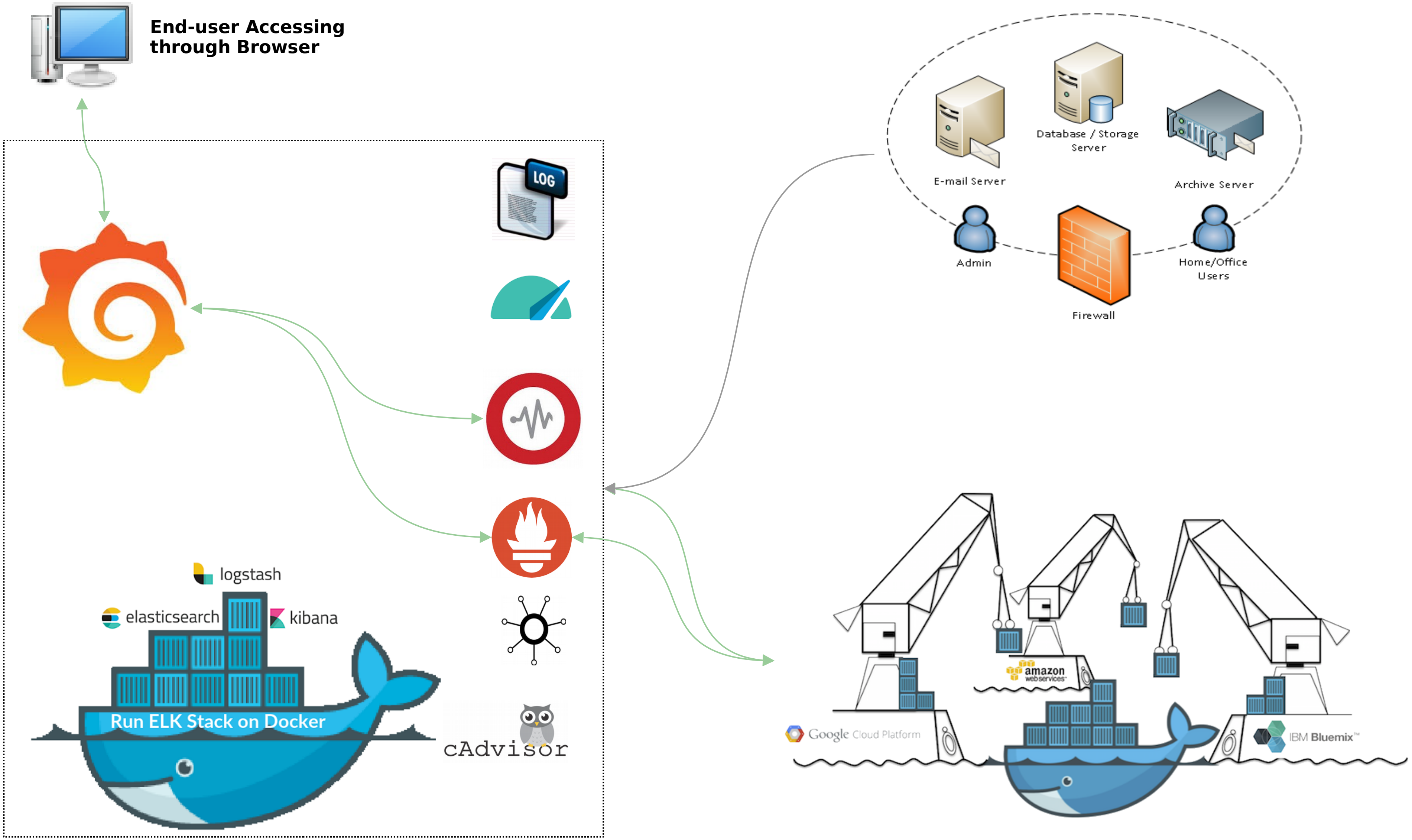
If your application writes a log, we'll track it!

What we're proposing?



- The solution is based on Open-Source softwares, designed for the Cloud Computing era to be offered as a service
- Easy deployment through docker officially signed images
- Minimum customizations required to forward the logs to a central stash
- Historic view to assist troubleshoot, analytics and creating relevant KPI's
- Quick updates with minimum downtime
- Portable 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
- Up/down monitoring *(heartbeat)* can be used to visualize ping errors by region

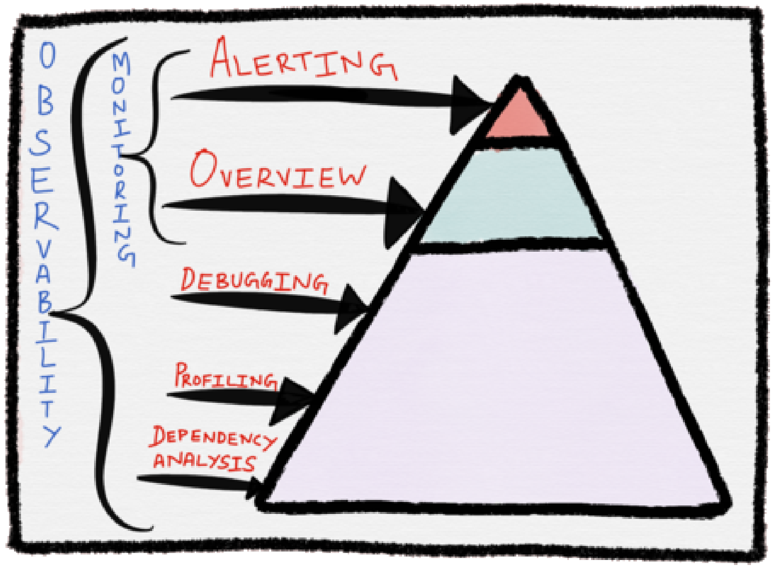
And how we're proposing?



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 Theorist)

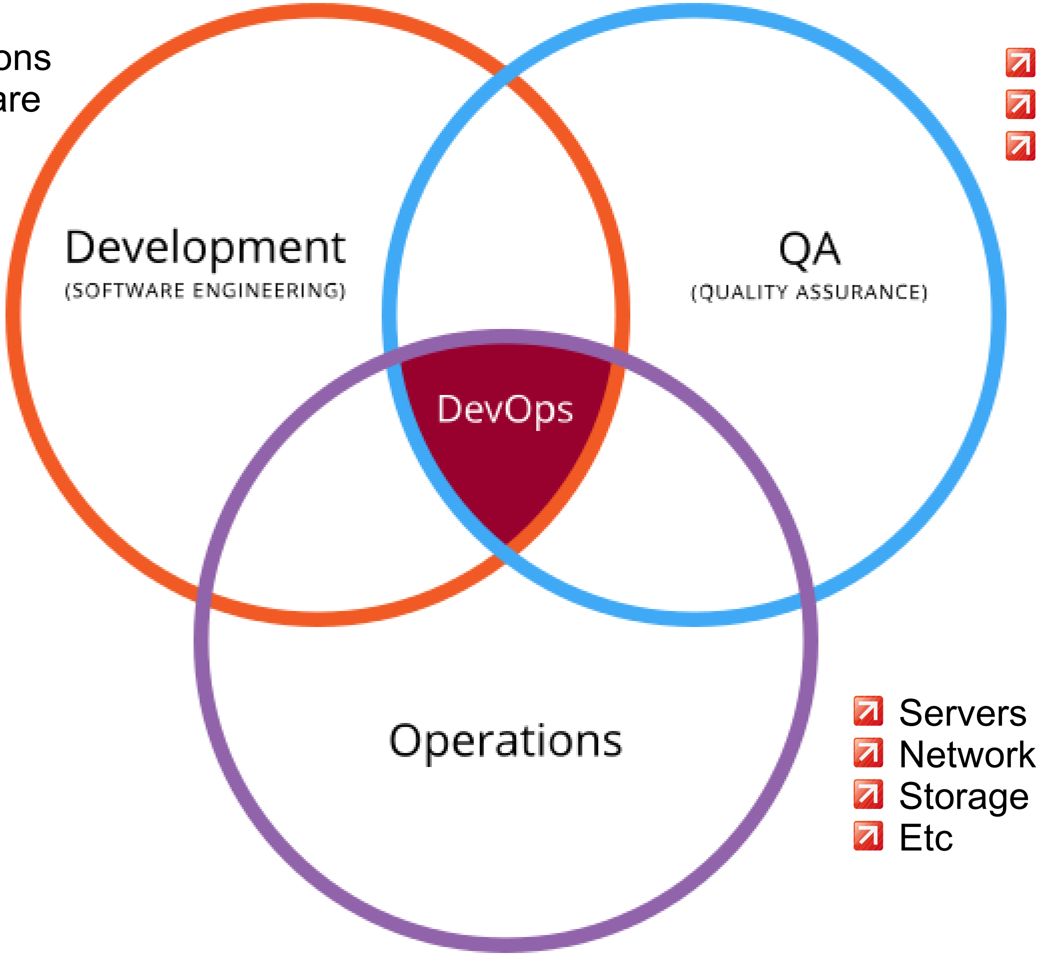


- R = Rate (Ex. Request Throughput, in requests per second)
- E = Errors (Ex: Request Error Rate, as either a throughput metric or a fraction of overall throughput)
- D = Duration (Ex: Latency, Residence Time, or Response Time; all three are widely used)

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

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

And to Who We're Offering?



- Applications
- Middleware
- Etc

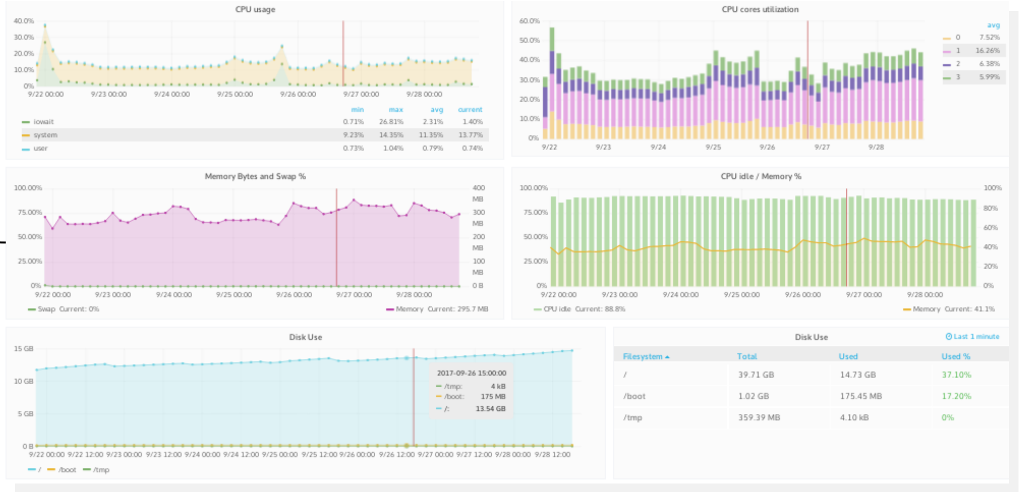
- Incident / Problem Mgt
- Change Management
- RCA's

- Servers
- Network Devices
- Storage Appliances
- Etc

- Security & Auditing

And What Does it Look Like?

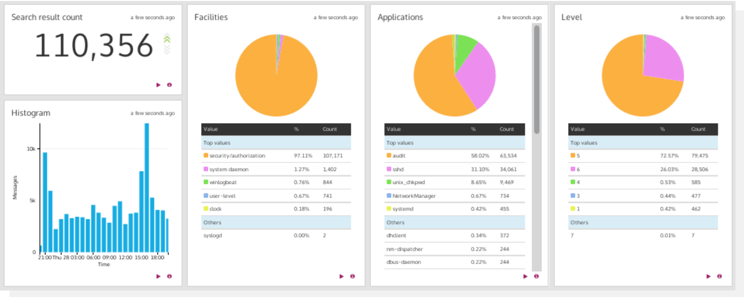
- **Single Dashboard for Windows and Linux metrics**
- Real time and historical metrics on a lightweight web page



	min	max	avg	current
iowait	0.71%	26.81%	2.31%	1.40%
system	9.23%	14.35%	11.35%	13.77%
user	0.73%	1.04%	0.79%	0.74%

Disk Use — Last 1 minute

Filesystem ▲	Total	Used	Used %
/	39.71 GB	14.73 GB	37.10%
/boot	1.02 GB	175.45 MB	17.20%
/tmp	359.39 MB	4.10 kB	0%



Facilities

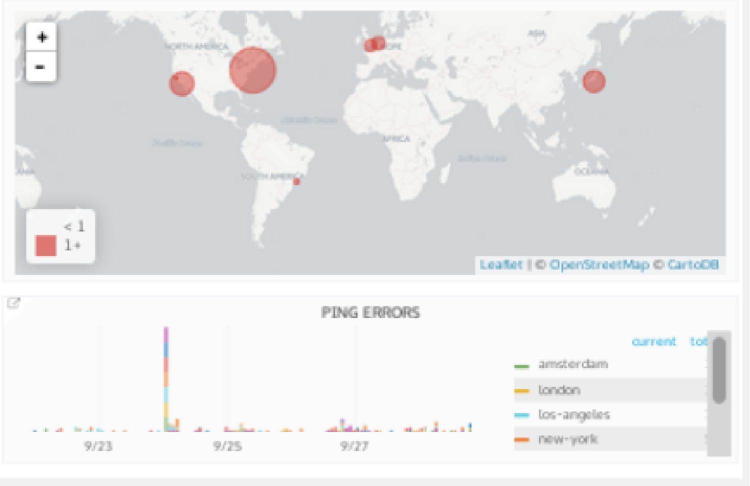
Value	%	Count
Top values		
security/authorization	97.11%	107,171
system daemon	1.27%	1,402
winlogbeat	0.76%	844
user-level	0.67%	741
clock	0.18%	196
Others		
syslogd	0.00%	2

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

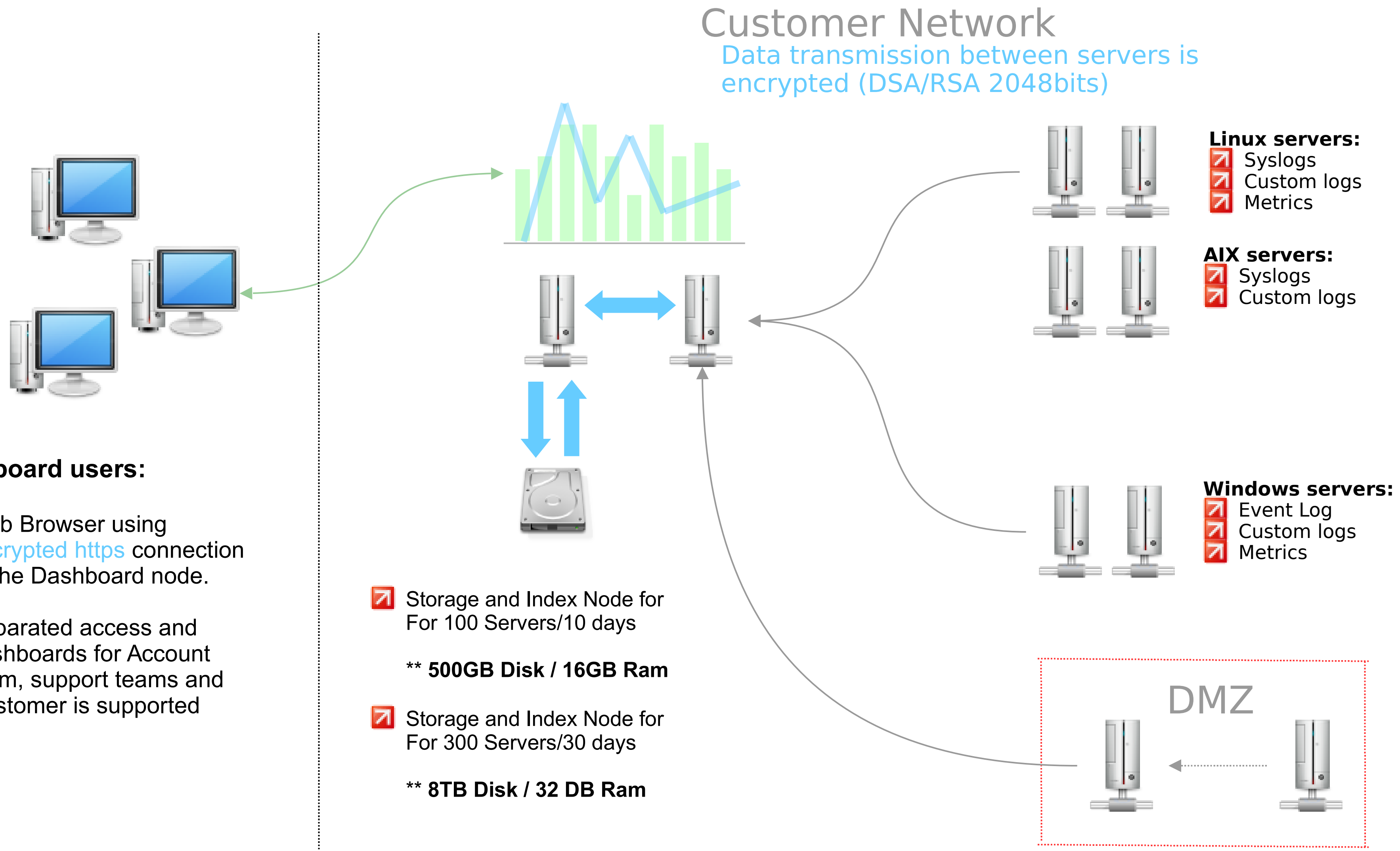


Metrics and Analytics extracted from log messages

Make audits and troubleshooting easy!

- User commands issued (containing the userID, terminal and source IP)
- Login attempts, success, sudo command success / fail (containing the ID, terminal, source IP and location)
- HTTP response errors, containing the IP and a map containing the locations
- Creativity is the limit - SMEs / Application owners can request any log analysis and dashboards.

And What’s the Basic Setup?



Customer Network

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

Linux servers:

- Syslogs
- Custom logs
- Metrics

AIX servers:

- Syslogs
- Custom logs

Windows servers:

- Event Log
- Custom logs
- Metrics

Dashboard users:

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

- Storage and Index Node for For 100 Servers/10 days

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

- Storage and Index Node for For 300 Servers/30 days

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

Who are the other competitors?

Who’s the Team?

Hugo do Prado
hprado@br.ibm.com

Felipe Silveira
fsilveir@br.ibm.com

Thank you!