

LaaS: Log Analytics as a Service

SMI Enterprise Automation Brazil

04-Nov-2017



Hugo do Prado

hprado@br.ibm.com

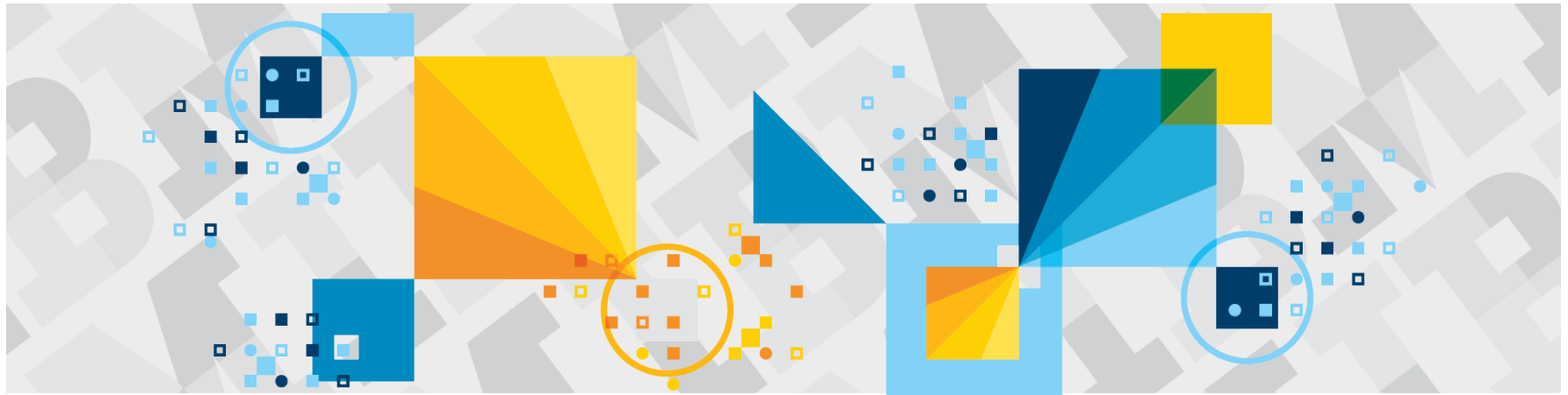
http://about.me/hugo_prado



Felipe Silveira

fsilveir@br.ibm.com

<http://about.me/felipesilveira>



github.com/IBM-SMI-Brazil/LaaS

Por quê ‘Log Analytics’ é tão Importante?



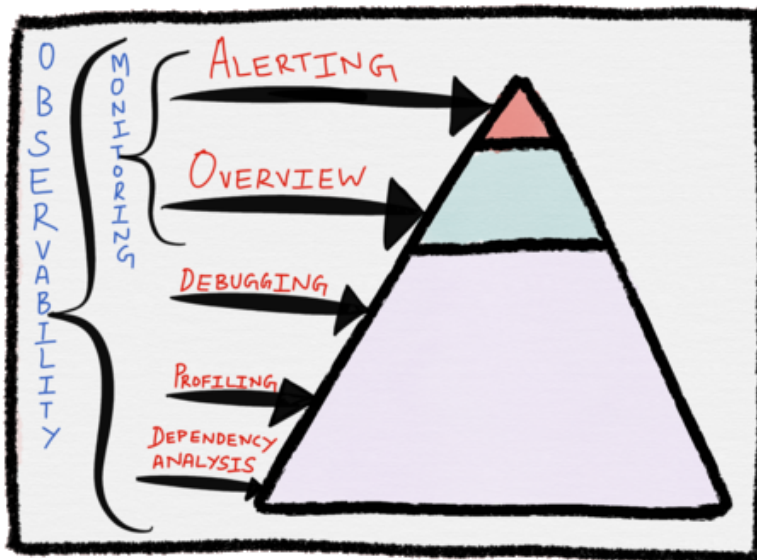
“Pessoas racionais tomarão decisões racionais se você apresentar os dados certos.”

Linda Sanford, Senior Vice President, Enterprise Transformation, IBM

Por quê agora?

“Observabilidade é a medida de quão bem os estados internos de um sistema podem ser inferidos a partir de suas saídas externas.”

Rudolf E. Kálmán (Teoria de Controle)

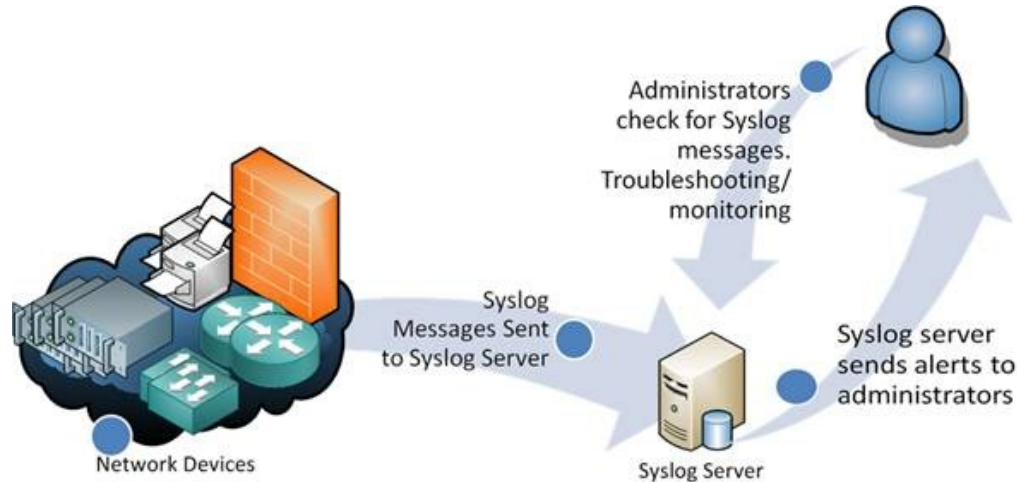


➤ R = Rate (Ex. Request Throughput, in requests per second)
➤ E = Errors (Ex: Request Error Rate, as either a throughput metric or a fraction of overall throughput)
➤ D = Duration (Ex: Latency, Residence Time, or Response Time; all three are widely used)

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

➤ Alerting Visualization
➤ Distributed System Tracing
➤ **Log Aggregation/Analytics**

O que é o SysLog e porque as pessoas usam?



Syslog é uma padrão (ou Protocolo) de produzir e enviar informações de Logs e Eventos de sistemas (Unix, Linux ou Windows) ou dispositivos (como Routers, Firewalls, Switches e etc). Através de mensagens UDP ou TCP para um coletor de mensagens centralizado, chamado de Syslog server.

Uma das principais razões do Syslog ser tão amplamente aceito é pela sua simplicidade - Há pouca ou nenhuma uniformidade no que se trata do conteúdo escrito e enviado via Syslog seja por um Dispositivo, Servidor ou Sistema Operacional -- porém ao seguir o mesmo padrão de estrutura pode-se facilmente consolidar diferentes informações na mesma visão.

“Mais dados” nem sempre é a resposta...




“Os dados de uma pessoa, são ruído para outra pessoa”

K.C. Cole – Autor de ‘O Universo e a Xícara de Chá’

- 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

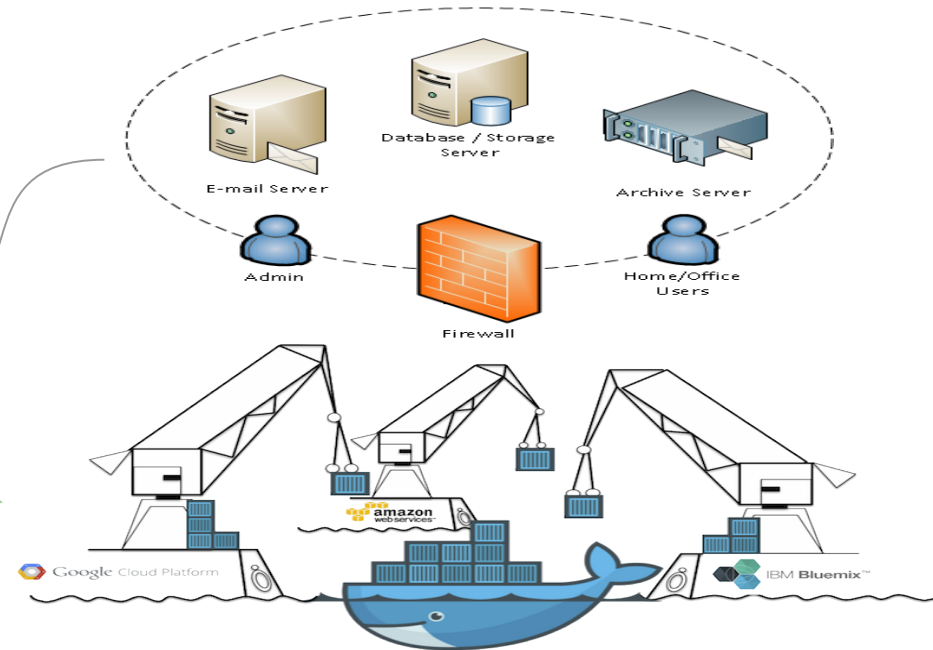
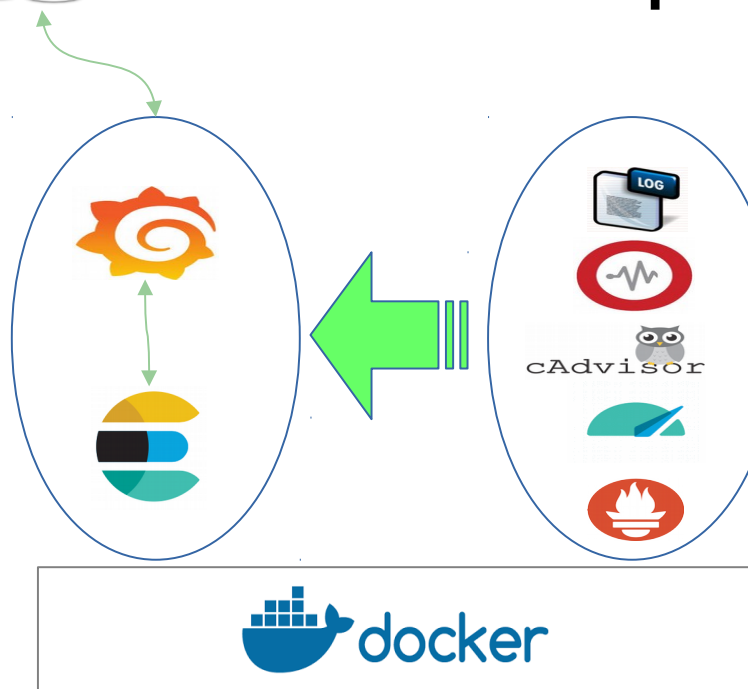
A hand is shown pointing towards the right side of the frame. In the background, there are several white icons on a dark blue background: a person walking, a group of three people, and a person sitting. There are also white speech bubbles. The overall theme is digital communication and data analysis.

**Nosso objetivo é ajudar
nossos clientes e outros
times a encontrar padrões e
tendências a partir dos seus
logs, conectando as pontas
soltas, das diversas fontes
de dados diferentes em uma
visão consolidada**

**Se a sua aplicação pode
escrever um log, nós
podemos acompanhar!**

Acesso do usuário final via Browser

E qual a proposta?

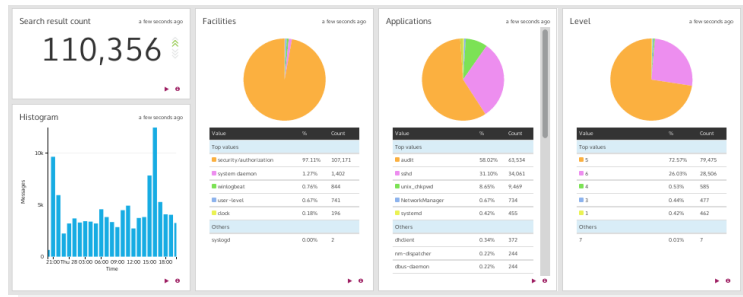


- ✔ Uma alternativa Open-Source escalável para ser oferecida como um serviço
- ✔ Deploy fácil via imagens docker pré-prontas
- ✔ Mínimo de customização possível para envio dos logs para um repositório central
- ✔ Visão histórica para ajudar no troubleshoot e na criação de KPI's relevantes
- ✔ Acesso rápido e visual aos dados sem necessidade de queries em SQL

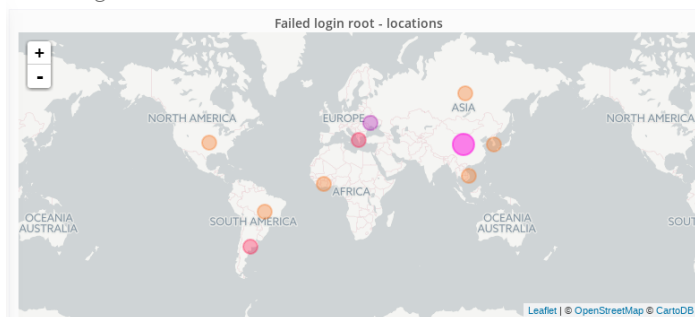
- ✔ Adaptável para ambientes Cloud, On-Premises ou Híbridos
- ✔ Correlação de métricas e logs para identificar tendências tanto de infra quanto de aplicações
- ✔ Possibilidade de cruzar informações com ferramentas de monitoração / performance
- ✔ Segurança dos dados em um repositório central longe do acesso de usuários com acesso privilegiado

E como é a “cara” desse negócio?

- Visão única independente de plataforma
- Métricas em tempo real ou por visão histórica

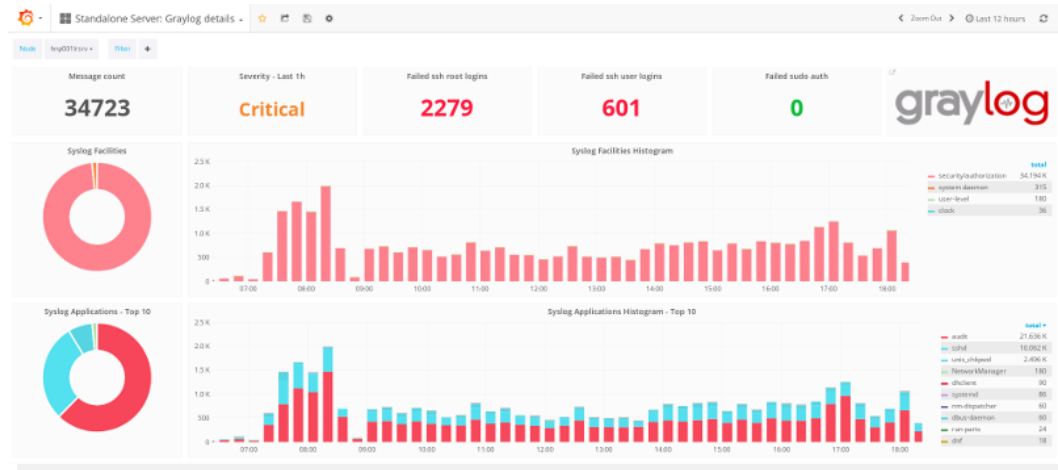


✓ Root login and sudo success / fail



✓ Additional user login details

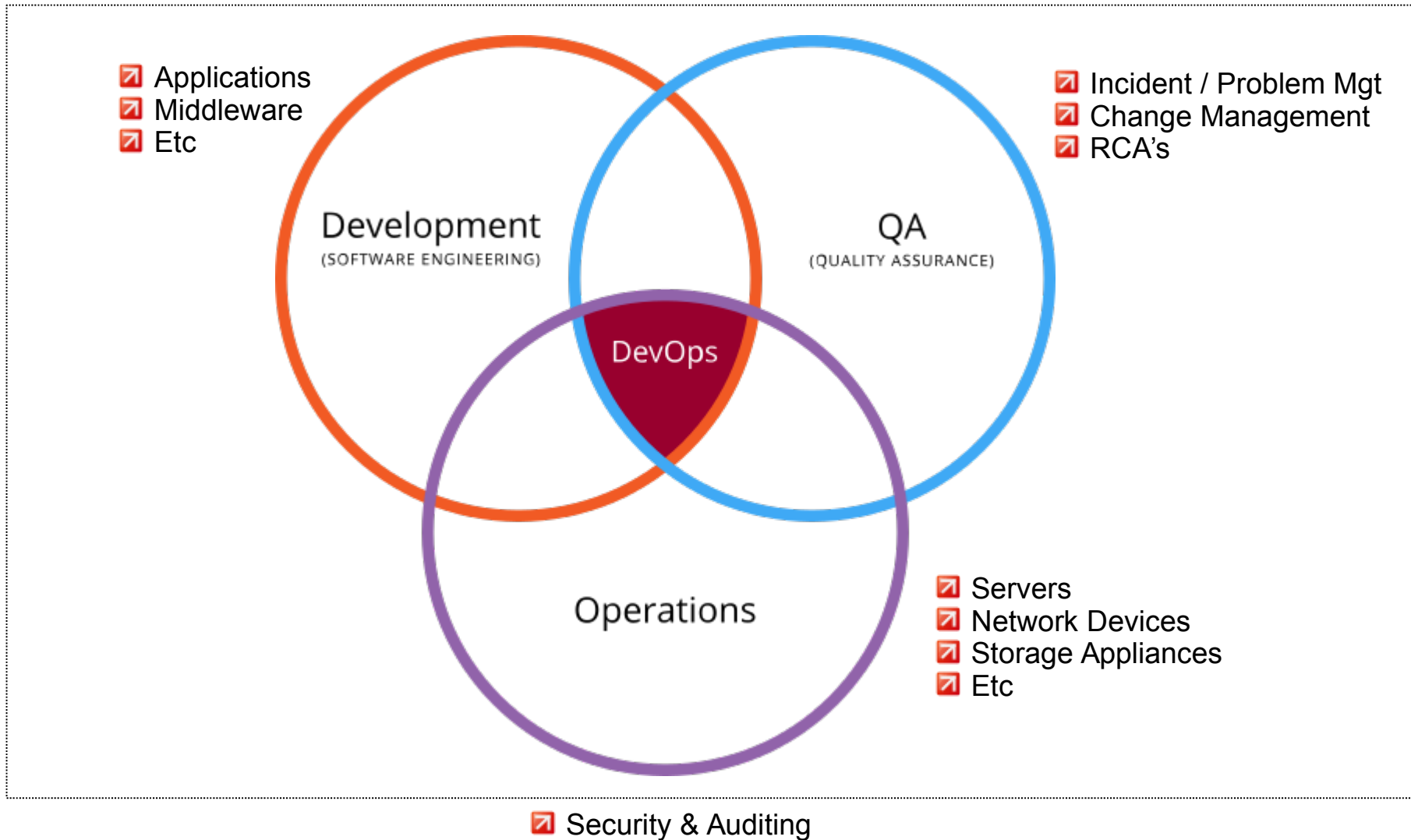
Failed IPs root login - Top 10		Failed userID login - Top 10	
IP	Count	UserID	Count
58.218.198.143	2093	root	4374
58.218.198.175	1846	admin	178
218.65.30.124	159	user	43



Métricas e análises extraídas de logs facilitam tanto auditoria como troubleshoot!

- Histórico de comandos executados (com userID, terminal e IP)
- Tentativas de login, (success, sudo, e falhas de acesso com ID, terminal, de origem e geo-localização)
- Totais de Erros de resposta HTTP, por IP's ou geolocalização em um mapa visual
- Criatividade é o limite, Administradores ou Desenvolvedores podem solicitar praticamente qualquer tipo de visualização!**

Quem pode usar?

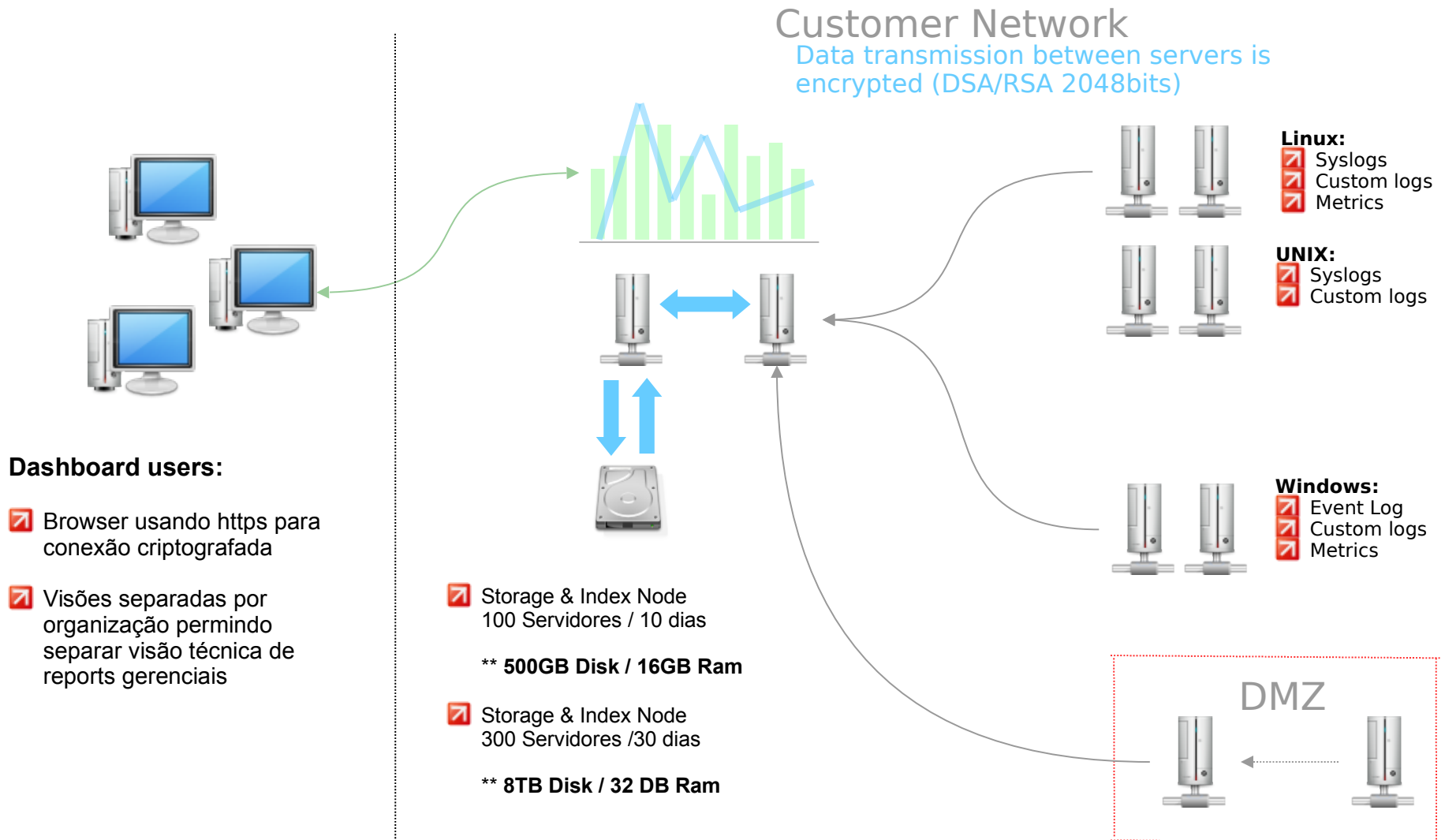


Quem são os concorrentes?

splunk® >  sumologic

LOGGLY

O que eu preciso pra rodar isso tudo?



Obrigado!!!

