Aula 09

Monitoramento de LOGs em Servidores

Prof. Roitier Campos Gonçalves

Definição

"Em computação, log de dados é uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais."

Fonte: https://pt.wikipedia.org/wiki/Log_de_dados

Logs

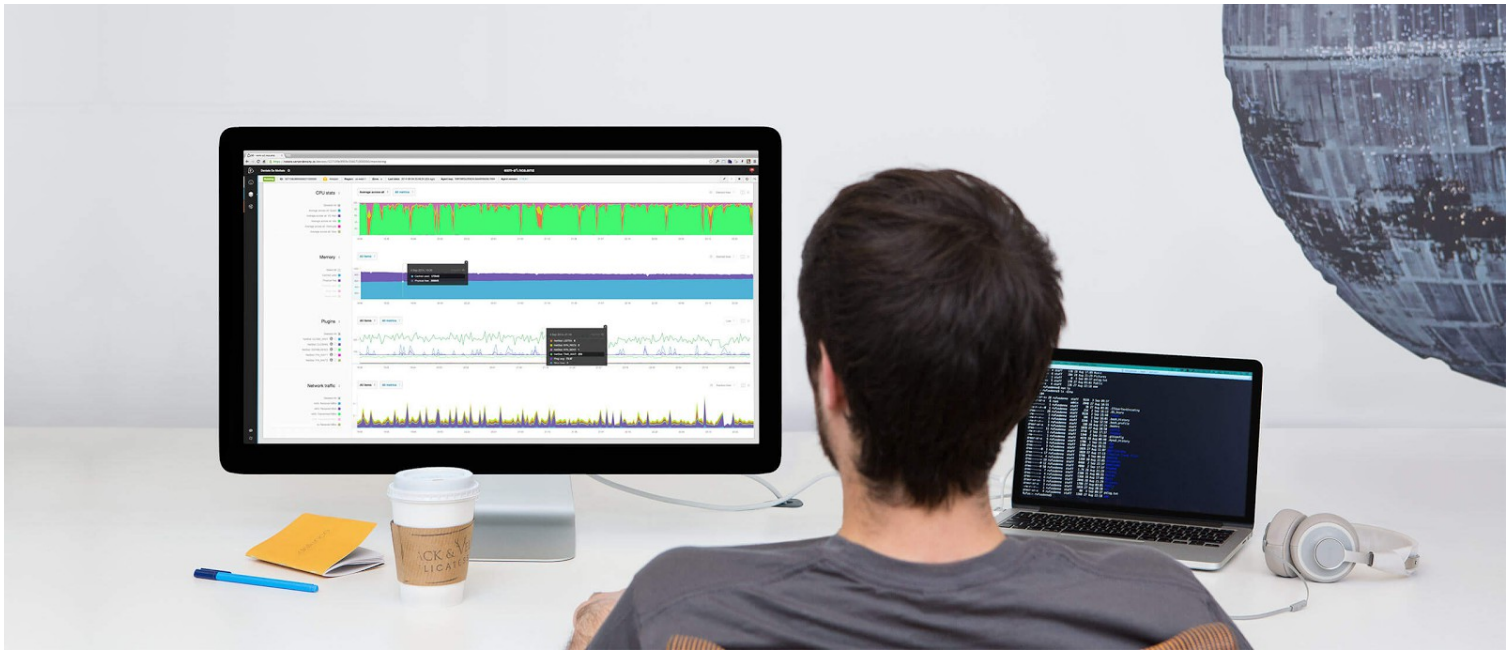
- Contam a “história” do sistema. q
- Contêm registros de eventos, avisos e erros.
- Auxiliam na detecção de problemas.
- São administrados pelo syslog.
- Embora alguns daemons não utilizem o syslog.

É necessário analisar logs se o sistema está funcionando corretamente? Por quê?

Logs

Nos LOGs encontramos eventos normais, além de avisos e erros registrados pelo kernel e por outros daemons e programas.

Os logs devem ser utilizados pelo administrador não só na resolução de problemas, mas também para acompanhar a saúde do sistema.



Principais arquivos

- # /var/log/messages
- # /var/log/auth.log
- # /var/log/daemon.log
- # /var/log/syslog

auth.log

O arquivo auth.log é responsável por guardar todas as informações de logins e tentativas de logins não sucedidas que foram efetuadas no servidor. Monitorando esse arquivo é possível identificar possíveis invasões, tentativas de brute force e ataques DDoS que estão ou foram realizadas no servidor.

```
# tail -f /var/log/auth.log
```

Syslog

O Syslog, assim como o arquivo Messages que será visto logo abaixo é o arquivo centralizador dos logs do sistema. Várias aplicações usam esse arquivo para gerar relatórios administrativos sobre o desempenho do servidor.

```
# tail -f /var/log/syslog
```

messages

O arquivo Messages contém mensagens diversas do sistema.

Ao contrário do SysLog que é mais customizável em relação de quais arquivos do diretório /var/log ele vai ler, o messages não é tão amigável no que diz respeito a customização.

```
# tail -f /var/log/messages
```

Gerenciando os Logs do Apache

O apache, por defaut possui 2 arquivos de logs centralizados, o log de acesso e o log de erros.

Os dois arquivos podem ser encontrados na pasta /var/log/apache/.

```
# tail -f /var/log/apache2/access.log
```

```
# tail -f /var/log/apache2/error.log
```

Samba

O servidor SaMBa também possui arquivos de log bem enxutos, e dependo da parametrização do arquivo smb.conf ele pode gerar logs individuais por clientes dentro da pasta no formato /var/log/samba/log.172.16.0.1, por exemplo.

O arquivo de logs responsável por monitorar o servidor smb e nmbd do sistema é o samba.log

```
# tail -f /var/log/samba.log
```

Verificando os últimos logins do Linux com Last

O comando last permite filtrar os últimos logins do servidor com os IP's , usuários e tempo de login de cada sessão, além de aplicar filtros a partir de arquivos, usuários e períodos. Ele exibe todas as informações referentes a entrada (login) e saída (logout) de usuários do sistema.

last -x → Mostra os últimos logins do sistema)

last roitier → Mostra os últimos logins do usuário “roitier”

O comando lastb funciona da mesma forma do comando last. Entretanto, ele usa, por padrão, o arquivo /var/log/btmp que possui informações sobre as tentativas mal sucedidas de se logar ao sistema.

lastb

Gerenciando os Logs do Apache

Em vez de texto, alguns arquivos dentro do /var/log mantêm informações em modo binário, como os arquivos lastlog e faillog.

Para a leitura do conteúdo desses arquivos, são utilizados os comandos:

lastlog → lista o último login de cada usuário;

last → lista os últimos logins feitos no sistema;

faillog → lista as tentativas malsucedidas de logins no sistema.