ARQUIVOS DE LOG

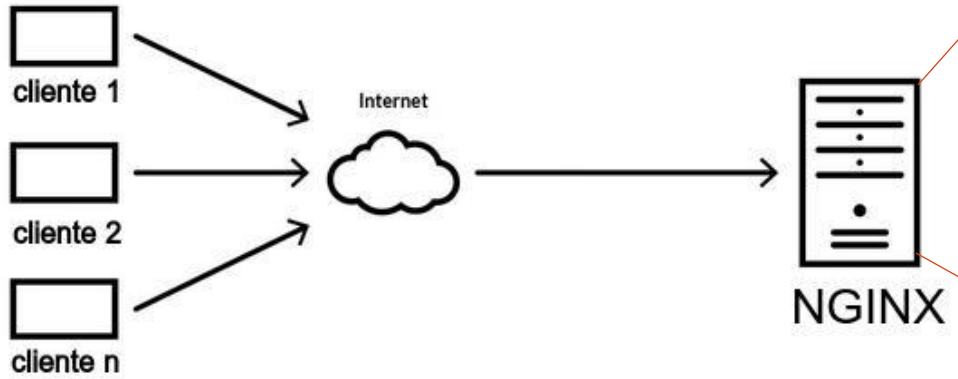
Por Sediane Carmem Lunardi Hernandes

AGENDA

- Review servidor NGINX
- O que são logs e para que servem?
- Manipulando arquivos de log

SERVIDOR WEB NGINX

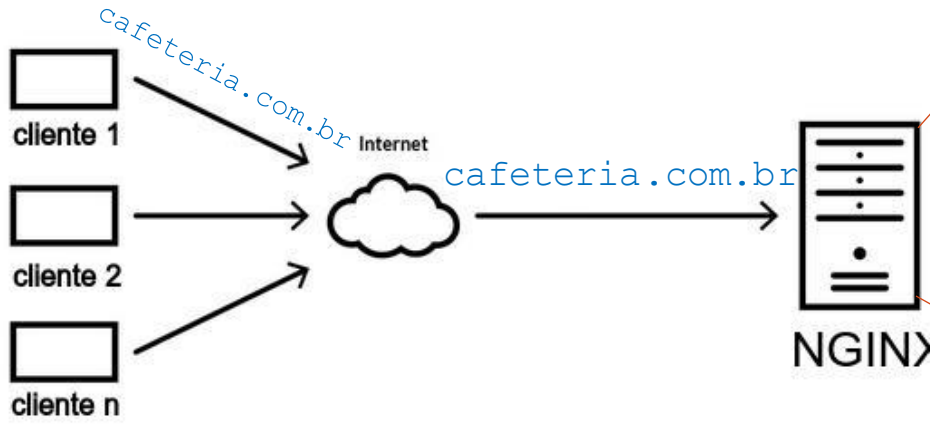
Servidor web (executa o tempo todo aguardando conexões na porta 80 – default)




```
/etc/nginx
    - sites-available
        - cafeteria.com.br
        - loja.com.br
        - sorveteria.com.br
    - sites-enabled
        - ap1 --> cafeteria.com.br
        - ap2 --> loja.com.br
        - ap3 --> sorveteria.com.br
    - snippets (segurança)
    - ...
```

Servidores virtuais – virtual hosts (vhosts)

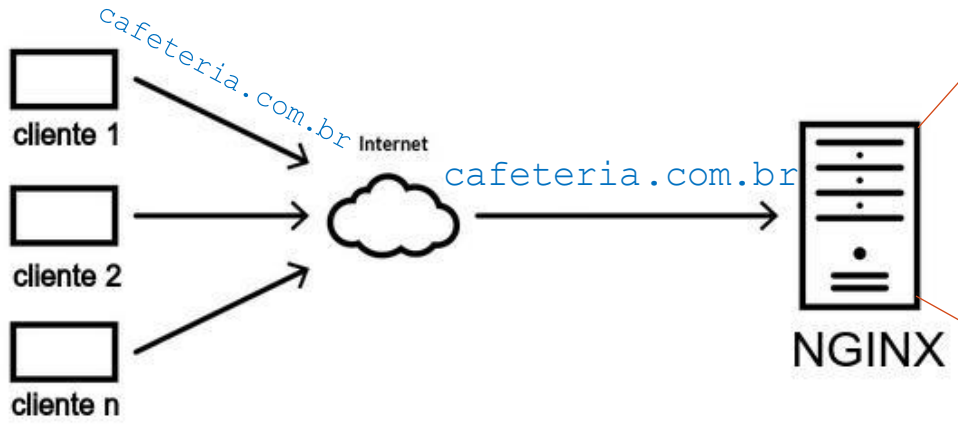
SERVIDOR WEB NGINX (CONT.)




```
/etc/nginx
    - sites-available
        - cafeteria.com.br
        - loja.com.br
        - sorveteria.com.br
    - sites-enabled
        - ap1 --> cafeteria.com.br
        - ap2 --> loja.com.br
        - ap3 --> sorveteria.com.br
    - ...
```

Servidores virtuais – virtual hosts (vhosts)

SERVIDOR WEB NGINX (CONT.)

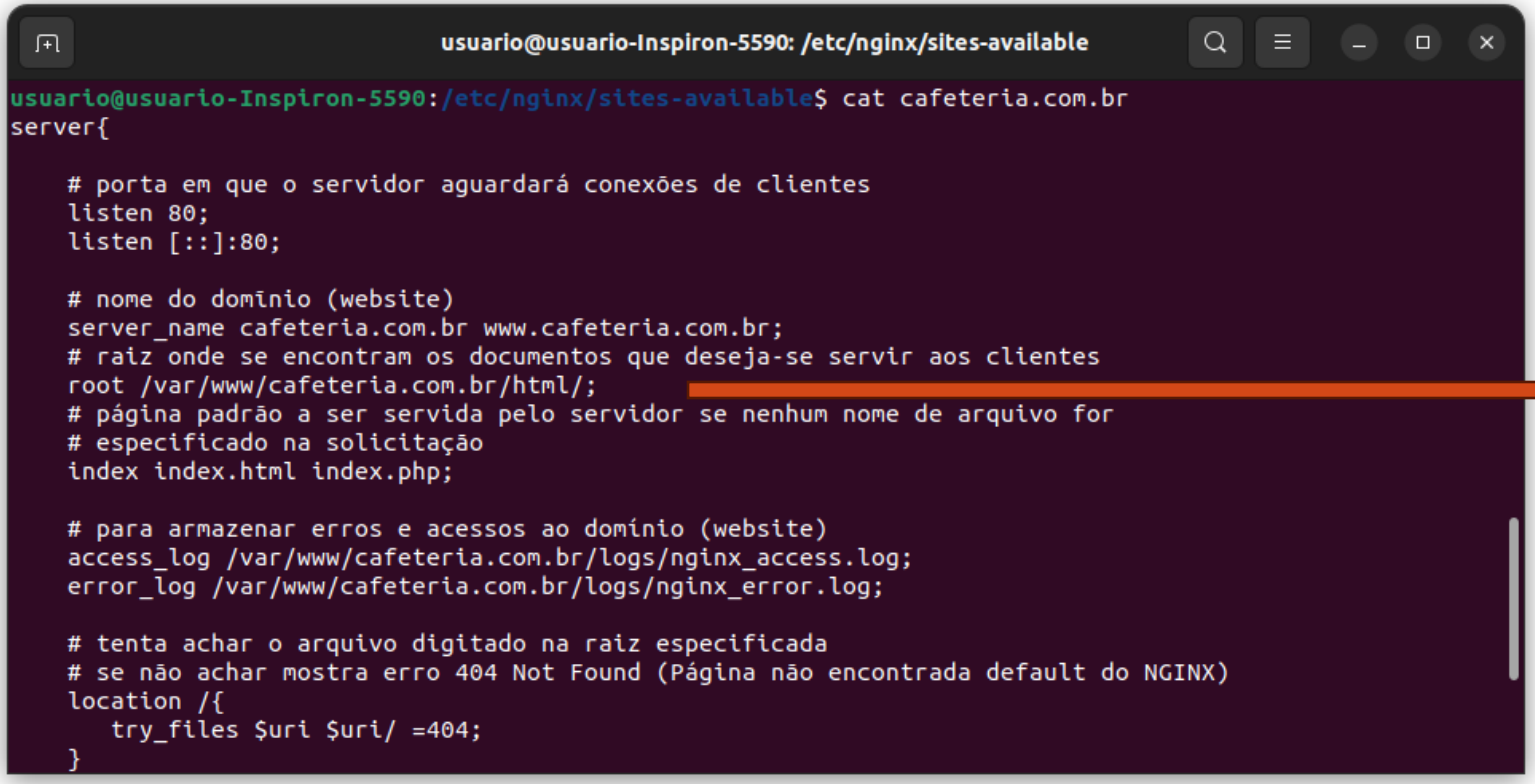



```
/etc/nginx
    - sites-available
        - cafeteria.com.br
        - loja.com.br
        - sorveteria.com.br
    - sites-enabled
        - ap1 --> cafeteria.com.br
        - ap2 --> loja.com.br
        - ap3 --> sorveteria.com.br
    - ...
```

Servidores virtuais – virtual hosts (vhosts)

```
usuario@usuario-Inspiron-5590: /etc/nginx/sites-available
usuario@usuario-Inspiron-5590:/etc/nginx/sites-available$ cat cafeteria.com.br
server{

    # porta em que o servidor aguardará conexões de clientes
    listen 80;
    listen [::]:80;

    # nome do domínio (website)
    server_name cafeteria.com.br www.cafeteria.com.br;
    # raiz onde se encontram os documentos que deseja-se servir aos clientes
    root /var/www/cafeteria.com.br/html/;
    # página padrão a ser servida pelo servidor se nenhum nome de arquivo for
    # especificado na solicitação
    index index.html index.php;

    # para armazenar erros e acessos ao domínio (website)
    access_log /var/www/cafeteria.com.br/logs/nginx_access.log;
    error_log /var/www/cafeteria.com.br/logs/nginx_error.log;

    # tenta achar o arquivo digitado na raiz especificada
    # se não achar mostra erro 404 Not Found (Página não encontrada default do NGINX)
    location /{
        try_files $uri $uri/ =404;
    }
```

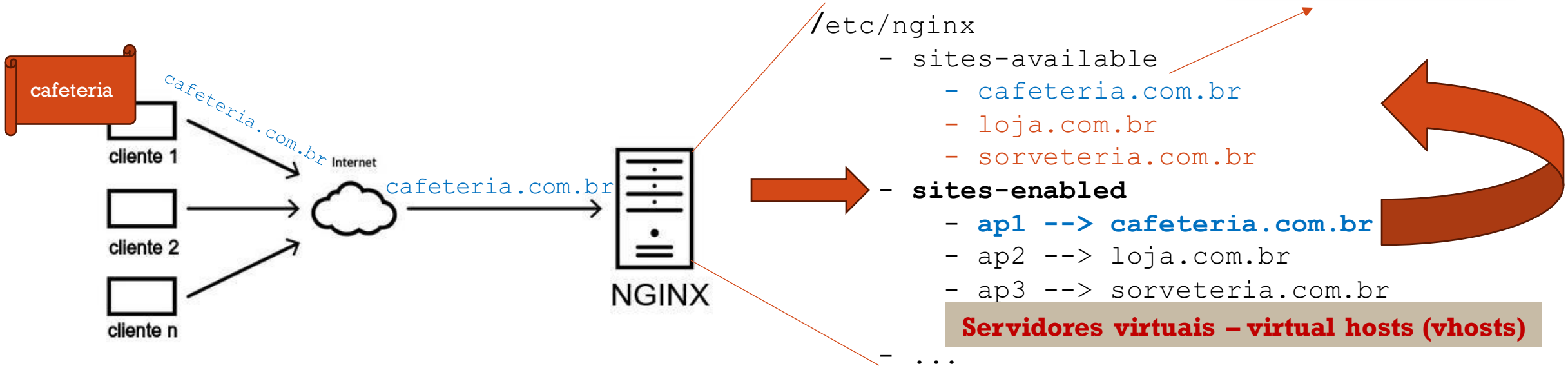
SERVIDOR WEB NGINX (CONT.)



Acessa /var/www/cafeteria.com.br/html e envia ao usuário a página index.html

SERVIDOR WEB NGINX (CONT.)

Acessa /var/www/cafeteria.com.br/html e envia ao usuário a página index.html



LOGS NO LINUX UBUNTU

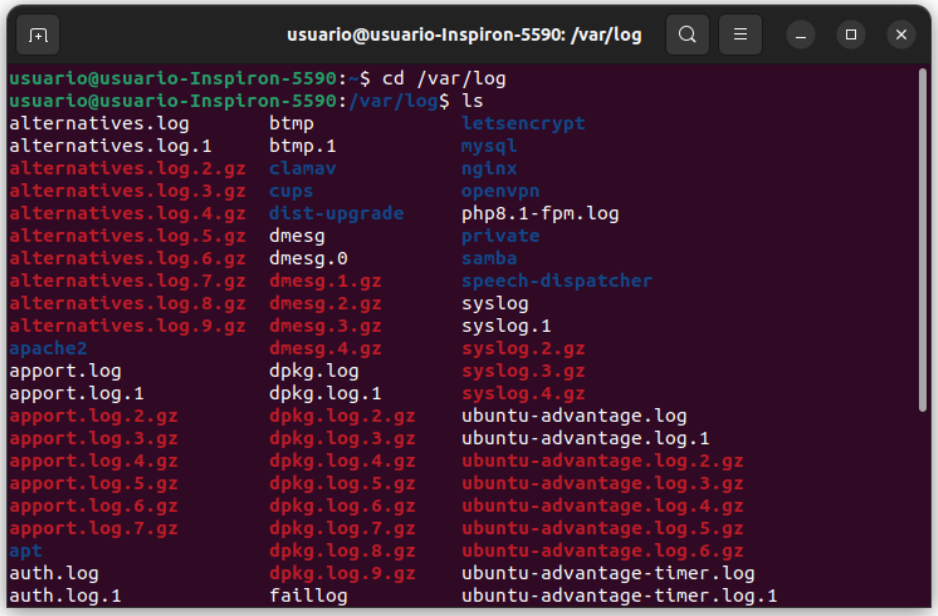
- No Linux, as atividades dos programas são registradas em arquivos de log
  - Normalmente se localizam em `/var/log`

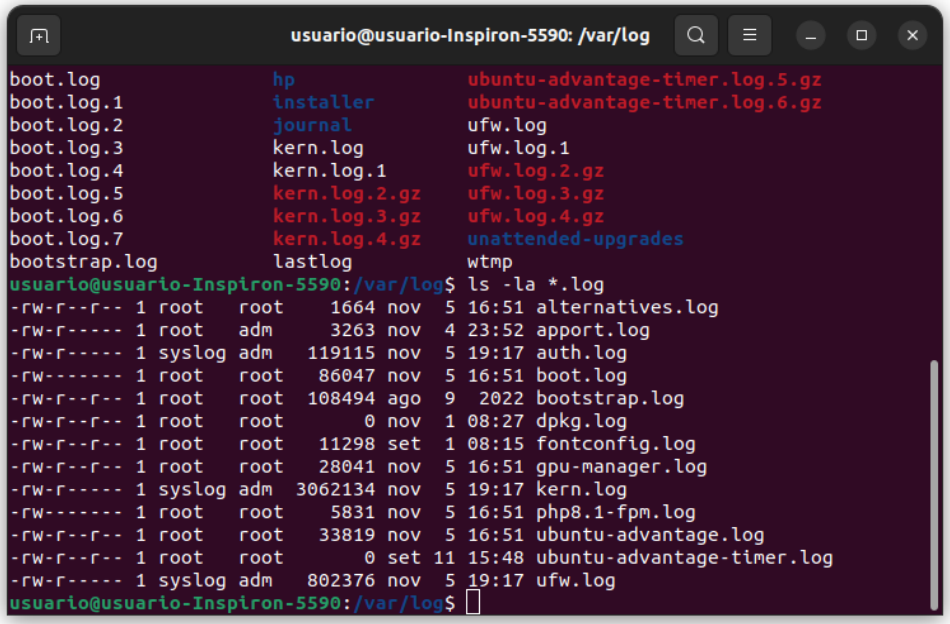
- Arquivos de log contém:
  - data
  - hora
  - mensagem emitida pelo programa (violações do sistema, mensagens de erro, alerta, entre outros eventos)
  - outros campos

  - Alguns programas como o NGINX e o Apache criam diversos arquivos de log e por este motivo são organizados em sub-diretórios em `/var/log`

ATIVIDADE

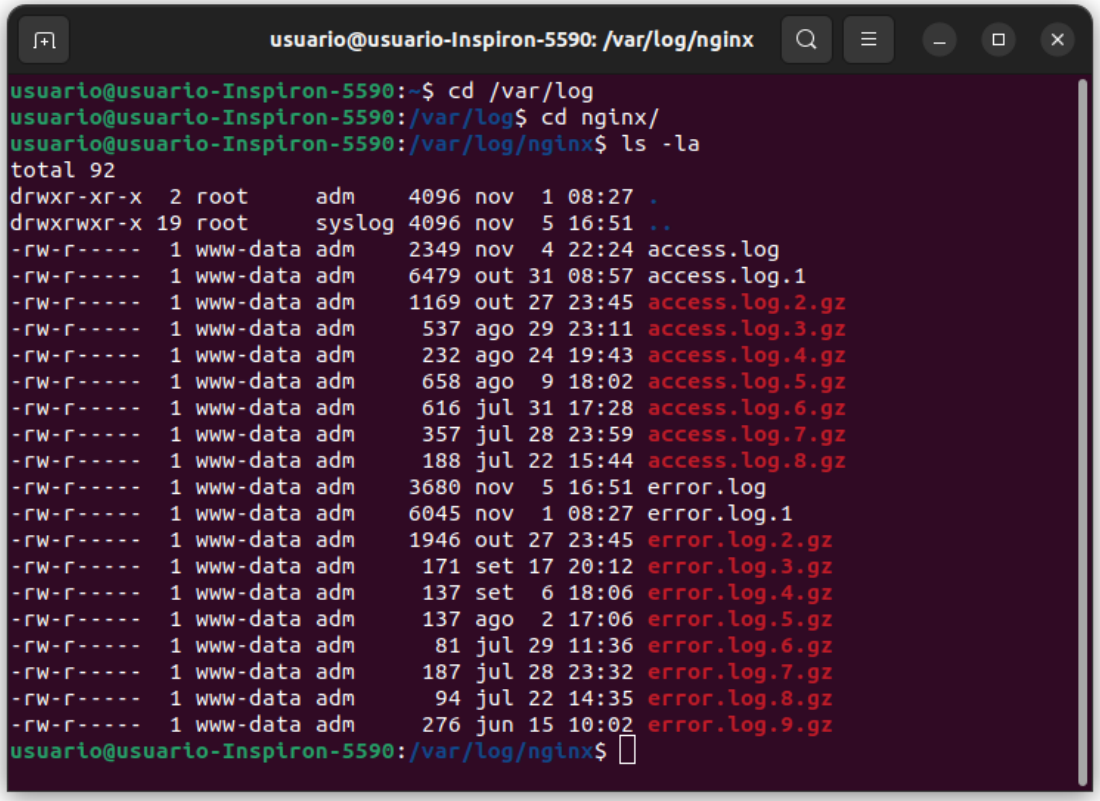
- Utilizando o terminal do Linux vá até ao diretório `/var/log` e verifique os arquivos de log (arquivos com a extensão .log)





ATIVIDADE (CONT.)

- Procure o diretório do NGINX e acesse o mesmo
  - Verifique os arquivos com a extensão .log




```
usuario@usuario-Inspiron-5590:/var/log/nginx$ ls -la *.log
-rw-r----- 1 www-data adm 2349 nov  4 22:24 access.log
-rw-r----- 1 www-data adm 3680 nov  5 16:51 error.log
```

ATIVIDADE (CONT.)

- Mostre o conteúdo dos arquivos (**`cat nome_arquivo.log`**)
  - `access.log`
  - `error.log`

- Verifique nesses arquivos se o formato é igual ao que a teoria mostra (data, hora, mensagem e outras informações)

PERGUNTAS

Sobre o arquivo de log **access.log**:

1. Você observou que as vezes aparece o domínio solicitado e as vezes não?
2. Você observou que esse é um log de todos os domínios que você criou para o NGINX servir?
3. Por que criamos em alguns domínios arquivos de log e erro (/var/www/????)?

Sobre o arquivo de log **error.log**:

a) Observe que ele não apresenta que acesso gerou o erro?

RESPOSTA

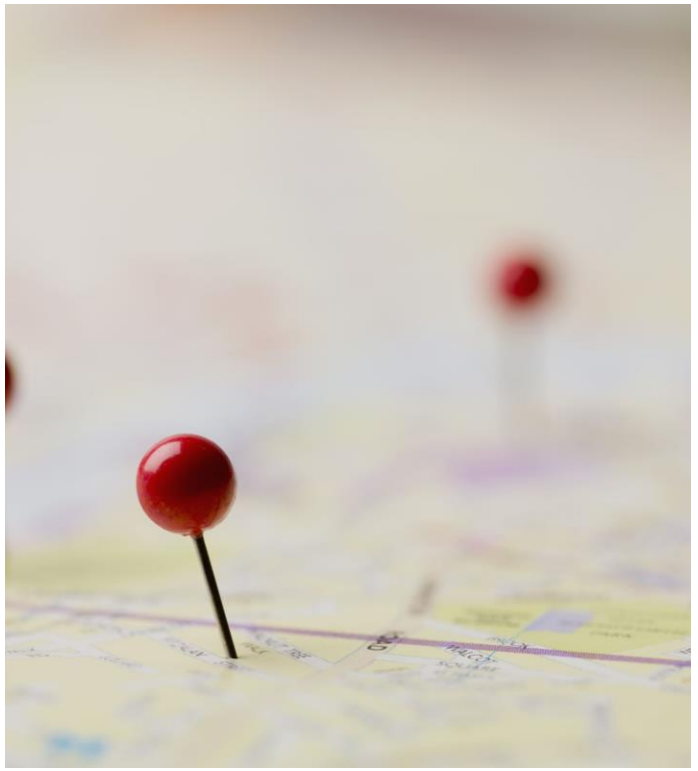
- **Pergunta 3:** para melhor organização e contabilização
  - Achar erros fica mais fácil
  - Contabilizar acessos é mais prático

MÃOS A OBRA:

- Vamos brincar com os arquivos de log?
  - Vá até /var/log/nginx
  - Baixe do Moodle os arquivos de logs disponibilizados

ALGUNS TESTES COM O ARQUIVO DE LOGS

1. Mostrar o número de acessos aos domínios servidos pelo NGINX (somente os que apresentarem GET).
2. Contar o número de acessos aos domínios servidos pelo NGINX (somente os que apresentarem GET).
3. Procurar pelo método POST no arquivo access.log.
4. Contar quantos métodos POST foram encontrados no arquivo access.log.
5. Mostrar os 5 primeiros acessos.
6. Mostrar os 5 últimos acessos.
7. Mostrar o número de acessos ao domínio cafeteria.com.br.
8. Contar o número de acessos ao domínio cafeteria.com.br.
9. Contar quantas códigos de status 404 (*page not found*) foram encontrados.



ALGUNS TESTES COM O ARQUIVO DE LOGS

10. Mostrar e depois contar o número de acessos aos domínios servidos pelo NGINX (somente os que apresentarem GET) dos seguintes domínios:
    a) cafeteria.com.br
    b) sorveteria.com.br
    c) livraria.com.br
    d) shopping.com.br
    e) loja.com.br

11. Considerando os domínio acima
    a) verificar se eles tiveram acesso https.
    b) contar quantas códigos de status 404 (page not found) foram encontrados.

REFERÊNCIAS

https://www.guiafoca.org/guiaonline/avancado/ch06.html