

ARQUIVOS DE LOG

Por Sediane Carmem Lunardi Hernandez

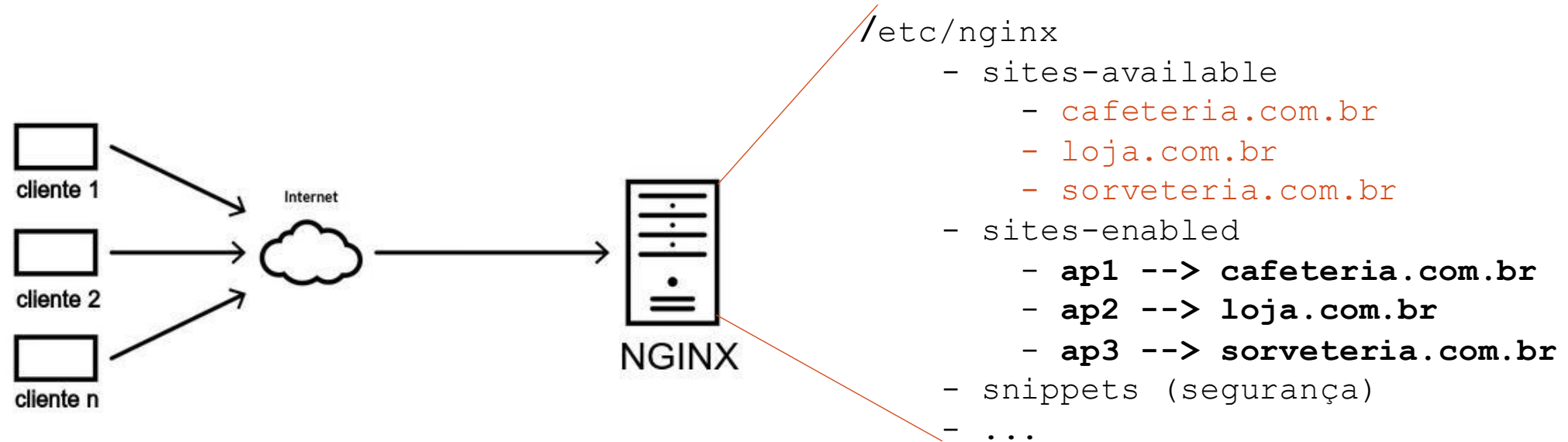
1

AGENDA

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

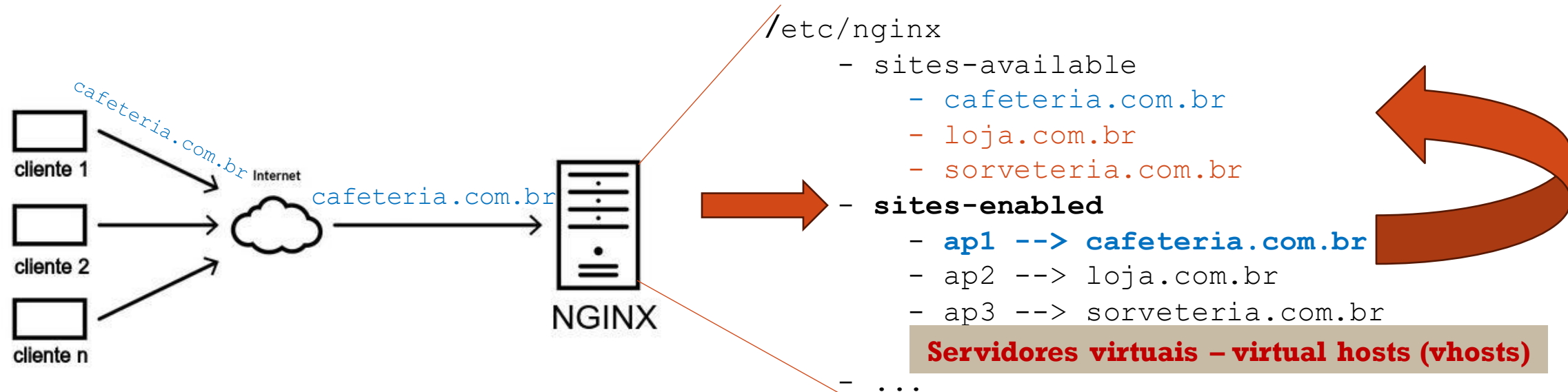
SERVIDOR WEB NGINX

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

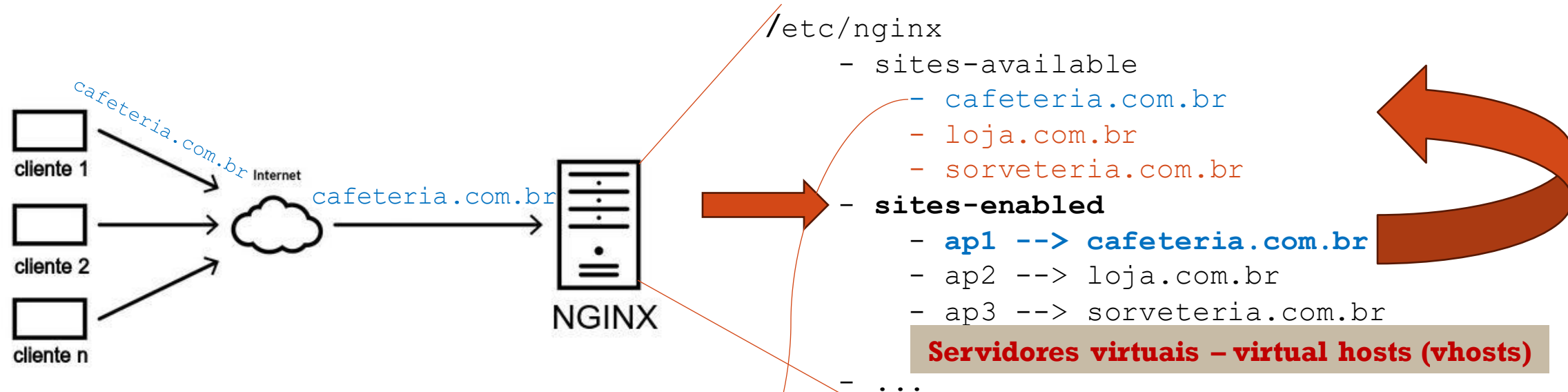


Servidores virtuais – virtual hosts (vhosts)

SERVIDOR WEB NGINX (CONT.)



SERVIDOR WEB NGINX (CONT.)



```
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 / =404;
    }
}
```

SERVIDOR WEB NGINX (CONT.)

```
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;
    }
}
```

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

SERVIDOR WEB NGINX (CONT.)

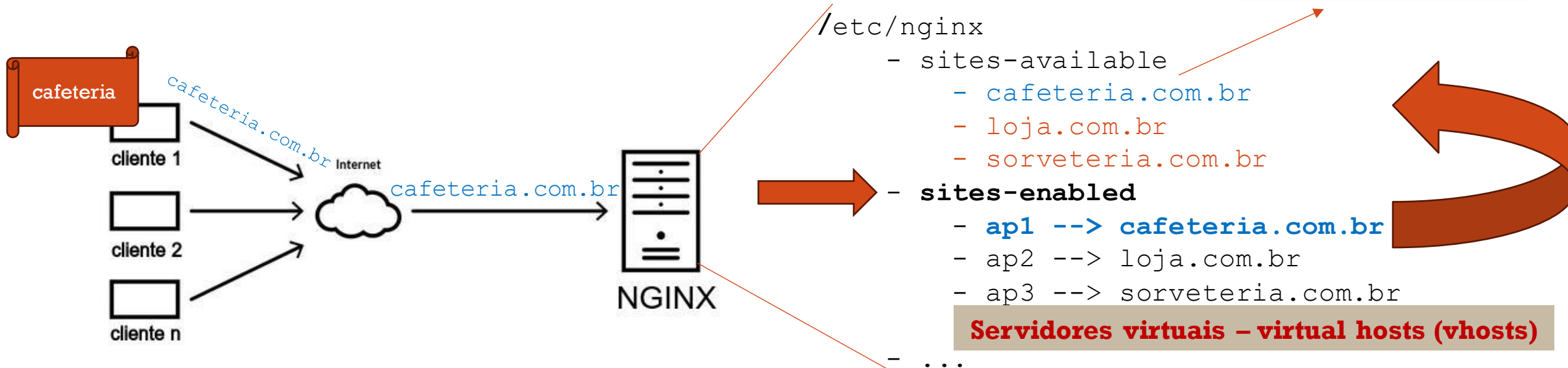
Acessa
/var/www/cafeteria.com.br/
html e envia ao usuário a
página index.html

```
user@user@nginx:~$ cat /etc/nginx/sites-available/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;
    # raíz onde se encontram os documentos que deverão ser servidos 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 amparelhar erros e ações 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 raíz especificada
    # se não achar mostra erro 404 not found (página não encontrada default do NGINX)
    location / {
        try_files $uri $uri/ =404;
    }
}
```



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`)

```
usuario@usuario-Inspiron-5590: /var/log
usuario@usuario-Inspiron-5590:~$ cd /var/log
usuario@usuario-Inspiron-5590:/var/log$ ls
alternatives.log      bttmp      letsencrypt
alternatives.log.1    bttmp.1    mysql
alternatives.log.2.gz clamav      nginx
alternatives.log.3.gz cups        openvpn
alternatives.log.4.gz dist-upgrade php8.1-fpm.log
alternatives.log.5.gz dmesg      private
alternatives.log.6.gz dmesg.0    samba
alternatives.log.7.gz dmesg.1.gz speech-dispatcher
alternatives.log.8.gz dmesg.2.gz syslog
alternatives.log.9.gz dmesg.3.gz syslog.1
apache2              dmesg.4.gz syslog.2.gz
apport.log           dpkg.log   syslog.3.gz
apport.log.1         dpkg.log.1 syslog.4.gz
apport.log.2.gz      dpkg.log.2.gz ubuntu-advantage.log
apport.log.3.gz      dpkg.log.3.gz ubuntu-advantage.log.1
apport.log.4.gz      dpkg.log.4.gz ubuntu-advantage.log.2.gz
apport.log.5.gz      dpkg.log.5.gz ubuntu-advantage.log.3.gz
apport.log.6.gz      dpkg.log.6.gz ubuntu-advantage.log.4.gz
apport.log.7.gz      dpkg.log.7.gz ubuntu-advantage.log.5.gz
apt                 dpkg.log.8.gz ubuntu-advantage.log.6.gz
auth.log            dpkg.log.9.gz ubuntu-advantage-timer.log
auth.log.1          faillog    ubuntu-advantage-timer.log.1
```

```
usuario@usuario-Inspiron-5590: /var/log
boot.log              hp          ubuntu-advantage-timer.log.5.gz
boot.log.1           installer  ubuntu-advantage-timer.log.6.gz
boot.log.2           journal    ufw.log
boot.log.3           kern.log   ufw.log.1
boot.log.4           kern.log.1 ufw.log.2.gz
boot.log.5           kern.log.2.gz ufw.log.3.gz
boot.log.6           kern.log.3.gz ufw.log.4.gz
boot.log.7           kern.log.4.gz unattended-upgrades
bootstrap.log        lastlog    wtmp
usuario@usuario-Inspiron-5590:/var/log$ ls -la *.log
-rw-r--r-- 1 root root 1664 nov 5 16:51 alternatives.log
-rw-r----- 1 root adm 3263 nov 4 23:52 apport.log
-rw-r----- 1 syslog adm 119115 nov 5 19:17 auth.log
-rw----- 1 root root 86047 nov 5 16:51 boot.log
-rw-r--r-- 1 root root 108494 ago 9 2022 bootstrap.log
-rw-r--r-- 1 root root 0 nov 1 08:27 dpkg.log
-rw-r--r-- 1 root root 11298 set 1 08:15 fontconfig.log
-rw-r--r-- 1 root root 28041 nov 5 16:51 gpu-manager.log
-rw-r----- 1 syslog adm 3062134 nov 5 19:17 kern.log
-rw----- 1 root root 5831 nov 5 16:51 php8.1-fpm.log
-rw-r--r-- 1 root root 33819 nov 5 16:51 ubuntu-advantage.log
-rw-r--r-- 1 root root 0 set 11 15:48 ubuntu-advantage-timer.log
-rw-r----- 1 syslog adm 802376 nov 5 19:17 ufw.log
usuario@usuario-Inspiron-5590:/var/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
usuario@usuario-Inspiron-5590:~$ cd /var/log
usuario@usuario-Inspiron-5590:/var/log$ cd nginx/
usuario@usuario-Inspiron-5590:/var/log/nginx$ ls -la
total 92
drwxr-xr-x  2 root    adm   4096 nov  1 08:27 .
drwxrwxr-x 19 root    syslog 4096 nov  5 16:51 ..
-rw-r----- 1 www-data adm  2349 nov  4 22:24 access.log
-rw-r----- 1 www-data adm  6479 out 31 08:57 access.log.1
-rw-r----- 1 www-data adm  1169 out 27 23:45 access.log.2.gz
-rw-r----- 1 www-data adm   537 ago 29 23:11 access.log.3.gz
-rw-r----- 1 www-data adm   232 ago 24 19:43 access.log.4.gz
-rw-r----- 1 www-data adm   658 ago  9 18:02 access.log.5.gz
-rw-r----- 1 www-data adm   616 jul 31 17:28 access.log.6.gz
-rw-r----- 1 www-data adm   357 jul 28 23:59 access.log.7.gz
-rw-r----- 1 www-data adm   188 jul 22 15:44 access.log.8.gz
-rw-r----- 1 www-data adm  3680 nov  5 16:51 error.log
-rw-r----- 1 www-data adm  6045 nov  1 08:27 error.log.1
-rw-r----- 1 www-data adm  1946 out 27 23:45 error.log.2.gz
-rw-r----- 1 www-data adm   171 set 17 20:12 error.log.3.gz
-rw-r----- 1 www-data adm   137 set  6 18:06 error.log.4.gz
-rw-r----- 1 www-data adm   137 ago  2 17:06 error.log.5.gz
-rw-r----- 1 www-data adm    81 jul 29 11:36 error.log.6.gz
-rw-r----- 1 www-data adm   187 jul 28 23:32 error.log.7.gz
-rw-r----- 1 www-data adm    94 jul 22 14:35 error.log.8.gz
-rw-r----- 1 www-data adm   276 jun 15 10:02 error.log.9.gz
usuario@usuario-Inspiron-5590:/var/log/nginx$
```

```
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



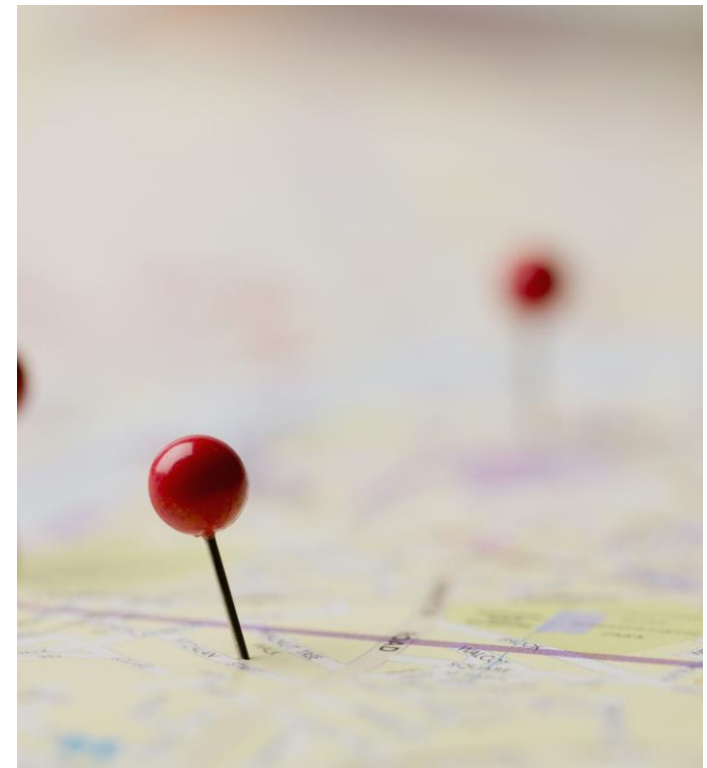


MÃOS A OBRA:

- 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>