

INSTITUTO FEDERAL Ceará

Nome: Ana Vitória Cabral Duarte

Nome: Lara Ingrid Lima Moraes

Nome: Edvaldo de Oliveira Sousa

Avaliação 4

Apache

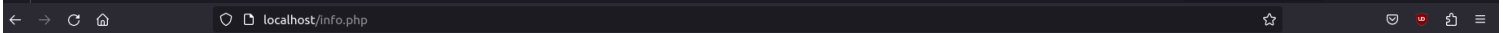
The screenshot shows a web browser window displaying the Apache2 Ubuntu Default Page. The browser's address bar shows the URL 192.168.122.1. The page has a header with the Apache logo and the text "Apache2 Ubuntu Default Page". Below the header, there is a red banner that says "It works!". The main content area contains a paragraph explaining that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It also mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Below this, there is a section titled "Configuration Overview" which explains that Ubuntu's Apache2 default configuration is different from the upstream default configuration and is split into several files optimized for interaction with Ubuntu tools. It also mentions that the configuration layout for an Apache2 web server installation on Ubuntu systems is as follows: /etc/apache2/. The configuration files are listed as follows: /etc/apache2/, /etc/apache2.conf, /etc/ports.conf, /etc/mods-enabled/, /etc/*.load, /etc/*.conf, /etc/conf-enabled/, /etc/*.conf, /etc/sites-enabled/, and /etc/*.conf. Below the list, there is a bulleted list of configuration details: apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server. ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime. Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively. They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2disite, a2enconf, a2disconf. See their respective man pages for detailed information. The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.

Banco de Dados – MariaDB

```
redes@redes2-pc07: ~  
Configurando mariadb-client-core-10.3 (1:10.3.38-0ubuntu0.20.04.1) ...  
Configurando libfcgi-perl (0.79-1) ...  
Configurando libterm-readkey-perl (2.38-1build1) ...  
Configurando libdbi-perl:amd64 (1.643-1ubuntu0.1) ...  
Configurando libfcgi-fast-perl (1:2.15-1) ...  
Configurando mariadb-client-10.3 (1:10.3.38-0ubuntu0.20.04.1) ...  
Configurando libdbd-mysql-perl:amd64 (4.050-3ubuntu0.2) ...  
Configurando mariadb-server-10.3 (1:10.3.38-0ubuntu0.20.04.1) ...  
Created symlink /etc/systemd/system/mysql.service → /lib/systemd/system/mariadb.service.  
Created symlink /etc/systemd/system/mysqld.service → /lib/systemd/system/mariadb.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /lib/systemd/system/mariadb.service.  
Configurando mariadb-client (1:10.3.38-0ubuntu0.20.04.1) ...  
Configurando mariadb-server (1:10.3.38-0ubuntu0.20.04.1) ...  
A processar 'triggers' para systemd (245.4-4ubuntu3.22) ...  
A processar 'triggers' para man-db (2.9.1-1) ...  
A processar 'triggers' para libc-bin (2.31-0ubuntu9.7) ...  
redes@redes2-pc07:~$ systemctl status mariadb  
● mariadb.service - MariaDB 10.3.38 database server  
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor prese  
   Active: active (running) since Thu 2023-09-14 21:03:52 -03; 1min 59s ago  
     Docs: man:mysqld(8)  
           https://mariadb.com/kb/en/library/systemd/  
   Main PID: 15287 (mysqld)  
     Status: "Taking your SQL requests now..."  
    Tasks: 31 (limit: 17791)  
   Memory: 63.3M  
   CGroup: /system.slice/mariadb.service  
           └─15287 /usr/sbin/mysqld  
  
redes@redes2-pc07:~$ sudo systemctl start mariadb  
redes@redes2-pc07:~$ mariadb --version  
mariadb Ver 15.1 Distrib 10.3.38-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2  
redes@redes2-pc07:~$ sudo mysql_secure_installation  
  
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!  
  
In order to log into MariaDB to secure it, we'll need the current  
password for the root user. If you've just installed MariaDB, and  
you haven't set the root password yet, the password will be blank,  
so you should just press enter here.  
  
Enter current password for root (enter for none):  
OK, successfully used password, moving on...  
  
Setting the root password ensures that nobody can log into the MariaDB  
root user without the proper authorisation.  
  
Set root password? [Y/n] y  
New password:  
Re-enter new password:  
Password updated successfully!  
Reloading privilege tables:
```

```
redes@redes2-pc07: ~  
you haven't set the root password yet, the password will be blank,  
so you should just press enter here.  
  
Enter current password for root (enter for none):  
OK, successfully used password, moving on...  
  
Setting the root password ensures that nobody can log into the MariaDB  
root user without the proper authorisation.  
  
Set root password? [Y/n] y  
New password:  
Re-enter new password:  
Password updated successfully!  
Reloading privilege tables..  
... Success!  
  
By default, a MariaDB installation has an anonymous user, allowing anyone  
to log into MariaDB without having to have a user account created for  
them. This is intended only for testing, and to make the installation  
go a bit smoother. You should remove them before moving into a  
production environment.  
  
Remove anonymous users? [Y/n] y  
... Success!  
  
Normally, root should only be allowed to connect from 'localhost'. This  
ensures that someone cannot guess at the root password from the network.  
  
Disallow root login remotely? [Y/n]  
... Success!  
  
By default, MariaDB comes with a database named 'test' that anyone can  
access. This is also intended only for testing, and should be removed  
before moving into a production environment.  
  
Remove test database and access to it? [Y/n]  
- Dropping test database...  
... Success!  
- Removing privileges on test database...  
... Success!  
  
Reloading the privilege tables will ensure that all changes made so far  
will take effect immediately.  
  
Reload privilege tables now? [Y/n]  
... Success!  
  
Cleaning up...  
  
All done! If you've completed all of the above steps, your MariaDB  
installation should now be secure.  
  
Thanks for using MariaDB!
```

PHP



PHP Version 7.4.3-4ubuntu2.19

System	Linux redes2-pc07 5.15.0-83-generic #92~20.04.1-Ubuntu SMP Mon Aug 21 14:00:49 UTC 2023 x86_64
Build Date	Jun 27 2023 15:49:59
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-fli.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-imagick.ini, /etc/php/7.4/apache2/conf.d/20-imap.ini, /etc/php/7.4/apache2/conf.d/20-intl.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-soap.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

```
PS C:\Users\sousa\.ssh> ls
```

```
    Diretório: C:\Users\sousa\.ssh
```

Mode	LastWriteTime		Length	Name
----	-----		-----	----
-a----	28/08/2023	20:52	1610	chave_privada-1.ppk
-a----	24/08/2023	15:57	1610	chave_privada.ppk
-a----	28/08/2023	20:52	477	chave_publica-1.pub
-a----	24/08/2023	15:57	477	chave_publica.pub
-a----	24/08/2023	16:23	175	known_hosts

```
PS C:\Users\sousa\.ssh> pscp .\chave_publica-1.pub grupo1@192.168.0.7:/home/grupo1/.ssh
```

```
The host key is not cached for this server:
```

```
 192.168.0.7 (port 22)
```

```
You have no guarantee that the server is the computer you  
think it is.
```

```
The server's ssh-ed25519 key fingerprint is:
```

```
ssh-ed25519 255 SHA256:/ClesaQBBBr2poMq7OCxJ3cgpHKPd0tAqe2RszWxeGA0
```

```
If you trust this host, enter "y" to add the key to PSCP's  
cache and carry on connecting.
```

```
If you want to carry on connecting just once, without adding  
the key to the cache, enter "n".
```

```
If you do not trust this host, press Return to abandon the  
connection.
```

```
Store key in cache? (y/n, Return cancels connection, i for more info) yes
```

```
grupo1@192.168.0.7's password:
```

```
chave_publica-1.pub | 0 kB | 0.5 kB/s | ETA: 00:00:00 | 100%
```

```
PS C:\Users\sousa\.ssh> █
```

grupo1@anavitorialaraedvaldo: ~

```
PS C:\Users\sousa\.ssh> ssh grupo1@192.168.0.7
The authenticity of host '192.168.0.7 (192.168.0.7)' can't be established.
ECDSA key fingerprint is SHA256:xC8Y411ENuKtwsY7U4j0zv6wwYvZQNqQyGxRrNkmfCg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.7' (ECDSA) to the list of known hosts.
grupo1@192.168.0.7's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-79-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of ter 29 ago 2023 00:06:36 UTC

System load:  0.0068359375      Processes:            114
Usage of /:   49.9% of 11.21GB   Users logged in:     1
Memory usage: 5%               IPv4 address for enp0s3: 192.168.0.7
Swap usage:   0%

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Manutenção de Segurança Expandida para Applications não está ativa.

78 as atualizações podem ser aplicadas imediatamente.
Para ver as actualizações adicionais corre o comando: apt list --upgradable

Ativar ESM Apps para poder receber possíveis futuras atualizações de segurança.
Consulte https://ubuntu.com/esm ou execute: sudo pro status

Last login: Mon Aug 28 23:36:45 2023
grupo1@anavitorialaraedvaldo: $
```


grupo1@anavitorialaraedvaldo: ~

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.7' (ECDSA) to the list of known hosts.
grupo1@192.168.0.7's password:

Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-79-generic x86_64)

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

System information as of ter 29 ago 2023 00:06:36 UTC

System load:	0.0068359375	Processes:	114
Usage of /:	49.9% of 11.21GB	Users logged in:	1
Memory usage:	5%	IPv4 address for enp0s3:	192.168.0.7
Swap usage:	0%		

* Introducing Expanded Security Maintenance for Applications.
Receive updates to over 25,000 software packages with your
Ubuntu Pro subscription. Free for personal use.

<https://ubuntu.com/pro>

Manutenção de Segurança Expandida para Applications não está ativa.

78 as atualizações podem ser aplicadas imediatamente.

Para ver as actualizações adicionais corre o comando: `apt list --upgradable`

Ativar ESM Apps para poder receber possiveis futuras atualizações de segurança.
Consulte <https://ubuntu.com/esm> ou execute: `sudo pro status`

Last login: Mon Aug 28 23:36:45 2023

grupo1@anavitorialaraedvaldo: \$ `ls -la .ssh`

total 20

drwx-----	2	grupo1	grupo1	4096	ago 29 00:04	
drwxr-x---	4	grupo1	grupo1	4096	ago 24 20:00	
-rw-----	1	grupo1	grupo1	477	ago 24 19:59	authorized_keys
-rw-rw-r--	1	grupo1	grupo1	477	ago 29 00:04	chave_publica-1.pub
-rw-rw-r--	1	grupo1	grupo1	477	ago 24 20:12	chave_publica.pub

grupo1@anavitorialaraedvaldo: \$