

***DOCUMENTAÇÃO DESAFIO ANALISTA DE INFRAESTRUTURA***

**Autor: Eng. Marcus Vinicius dos Santos**

INTRODUÇÃO .....	3
O QUE FOI UTILIZADO PARA O DESENVOLVIMENTO: .....	3
Instalação dos Componentes.....	4
APLICAÇÃO WEB/PHP (SCRIPT 01_WEB_PHP.sh).....	4
SERVIDOR LDAP (SCRIPT 02_SERVIDORLDAP.sh,).....	9
PHPLDAPADMIN (03_PHPLDAPADMIN.sh,).....	12
ZABBIX (04_zabbix.sh) .....	15
SEGURANÇA (05_SEGURANÇA) .....	21
Configurando WordPress para uso da base de dados LDAP .....	22
PROXY REVERSO .....	26

## INTRODUÇÃO

Este é um modelo básico de documentação sobre a solução do desafio proposto.

Considere o desafio como um aprendizado, pois nunca tive o contato tão profundo com Linux no quesito profissional, porém com muito esforço e pesquisas consegui desenvolver o desafio proposto com alguns diferenciais atendidos feitos.

Desafio proposto:

- *Aplicação WEB/PHP na versões mais atuais. Poderá trabalhar com aplicações prontas como qualquer CMS padrão de mercado, porém o diferencial será integrar uma base ldap local como autenticação primária do mesmo;*
- *Monitoramento proativo de aplicação, banco de dados e sistema operacional;*
- *Base ldap para autenticação primária da solução de monitoramento e web.*

*Diferencial: Aplicação para gerenciamento WEB da base LDAP;*

- *Segurança:*
  - a) *Política padrão DROP para as chains INPUT, FORWARD e OUTPUT;*
  - b) *Stateful;*
  - c) *Apenas http/https disponíveis;*
  - d) *Diferencial: ssh via port knocking e/ou vpn;*

## O QUE FOI UTILIZADO PARA O DESENVOLVIMENTO:

- Uma VM (utilizando VMware Workstation 15 Player) rodando sistema CENTOS7 na versão Servidor com GUI.
- Como aplicação WEB/PHP, como sugerido foi utilizado o WORDPRESS
- Active Directory Integration / LDAP Integration como intermediário da integração da base LDAP com a Aplicação WEB/PHP.
- Banco de dados MYSQL/ MariaDB
- Servidor Apache 2.4.6
- PHP 5.6 (Devido alguns bugs que estavam ocorrendo)
- Servidor OpenLdap na sua última versão
- PHPLdapAdmin para Gerenciamento web da base LDAP.
- ZABBIX para monitoramento do Sistema e Banco de Dados.

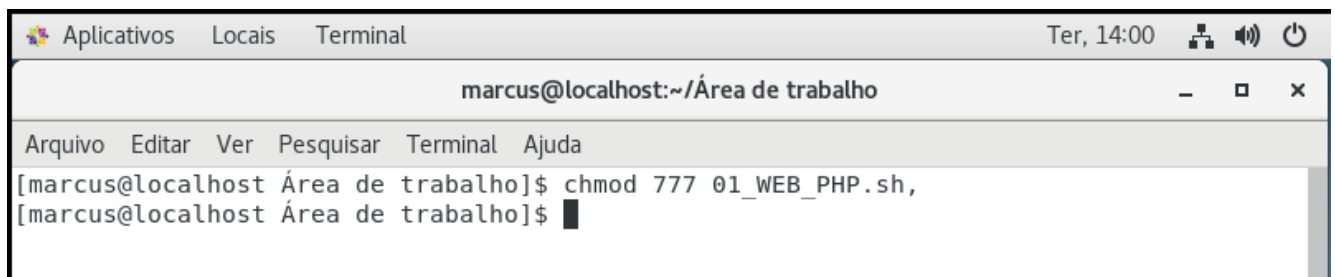
## Instalação dos Componentes

Para instalação dos componentes necessário para replicar a solução vão ser utilizados scripts separados para cada parte da solução, eles foram organizados da seguinte maneira:

1. 01\_WEB\_PHP.sh, (Onde será Instalado Apache, PHP, MariaDB, WORDPRESS além de fazer um update no **yum** )
2. 02\_SERVIDORLDAP.sh, (Onde será instalado o Servidor LDAP e criação da Base de testes da aplicação)
3. 03\_PHPLDAPADMIN.sh, (Onde será instalado o PHPLDAPADMIN para gerenciamento da Base LDAP)
4. 04\_zabbix.sh, (Onde será criada BD do Zabbix, Instalação e configuração)
5. 05\_SEGURANÇA (Script para aplicar as regras de Seguranças propostas, Usando **IPTABLES** e **firewall-cmd**)
6. 06\_PROXY (Script para configuração do proxy reverso)

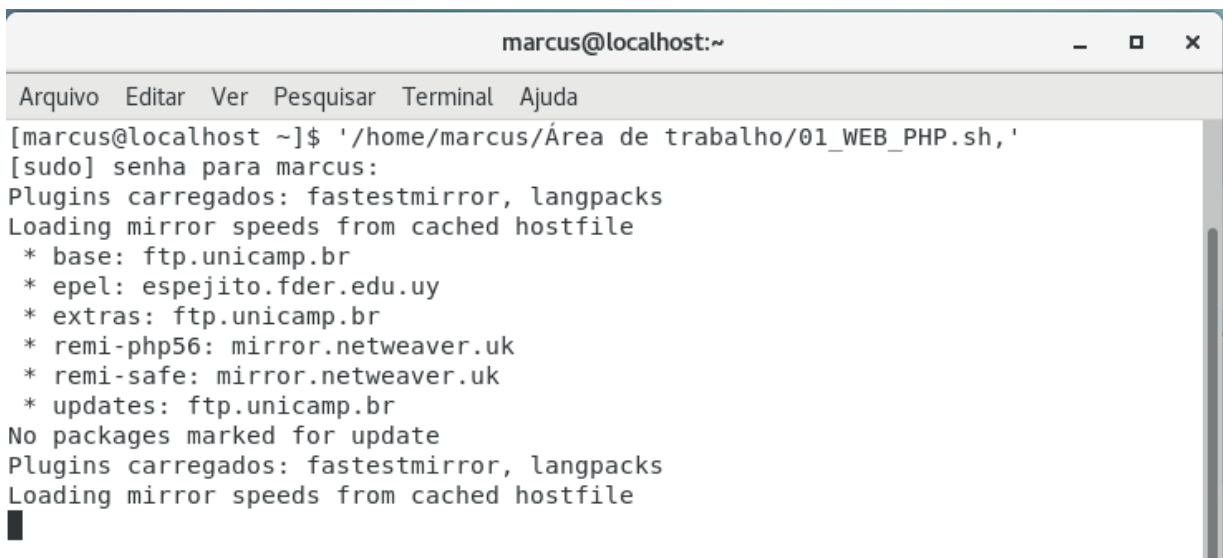
## APLICAÇÃO WEB/PHP (SCRIPT 01\_WEB\_PHP.sh)

Antes de iniciar devemos aplicar as permissões aos scripts conforme exemplo abaixo:

A terminal window titled 'marcus@localhost:~/Área de trabalho' with a menu bar (Arquivo, Editar, Ver, Pesquisar, Terminal, Ajuda). The terminal shows the command 'chmod 777 01\_WEB\_PHP.sh,' being executed, followed by a new prompt line.

```
marcus@localhost:~/Área de trabalho
Arquivo Editar Ver Pesquisar Terminal Ajuda
[marcus@localhost Área de trabalho]$ chmod 777 01_WEB_PHP.sh,
[marcus@localhost Área de trabalho]$
```

Logo após podemos executar o primeiro script.

A terminal window titled 'marcus@localhost:~' with a menu bar (Arquivo, Editar, Ver, Pesquisar, Terminal, Ajuda). The terminal shows the execution of the script '/home/marcus/Área de trabalho/01\_WEB\_PHP.sh,' which prompts for a password and then displays the output of a yum update command.

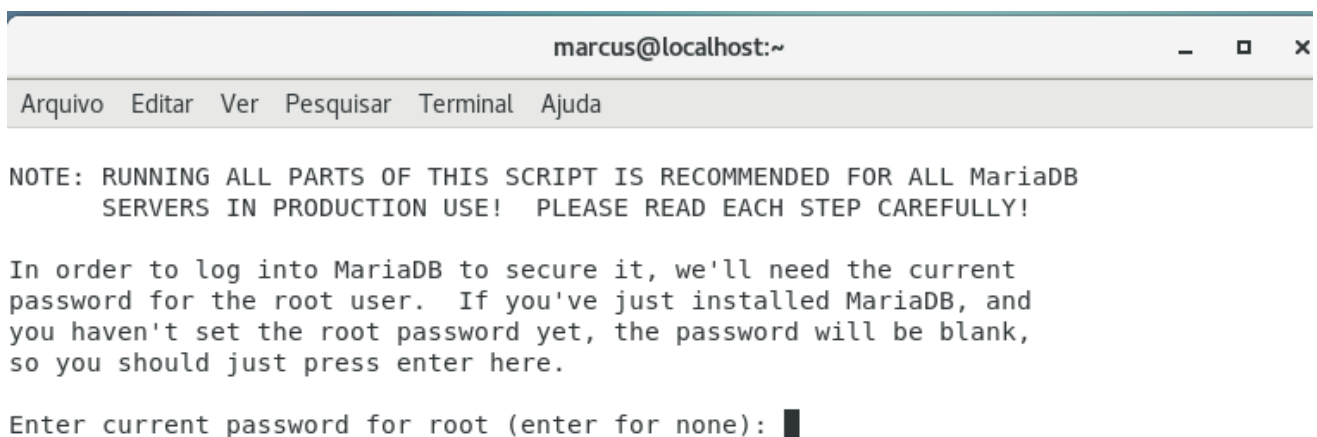
```
marcus@localhost:~
Arquivo Editar Ver Pesquisar Terminal Ajuda
[marcus@localhost ~]$ '/home/marcus/Área de trabalho/01_WEB_PHP.sh,'
[sudo] senha para marcus:
Plugins carregados: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: ftp.unicamp.br
* epel: espejito.fder.edu.uy
* extras: ftp.unicamp.br
* remi-php56: mirror.netweaver.uk
* remi-safe: mirror.netweaver.uk
* updates: ftp.unicamp.br
No packages marked for update
Plugins carregados: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
```

Ao aparecer a seguinte nota:

**“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.:*

Apenas pressionamos **ENTER**.

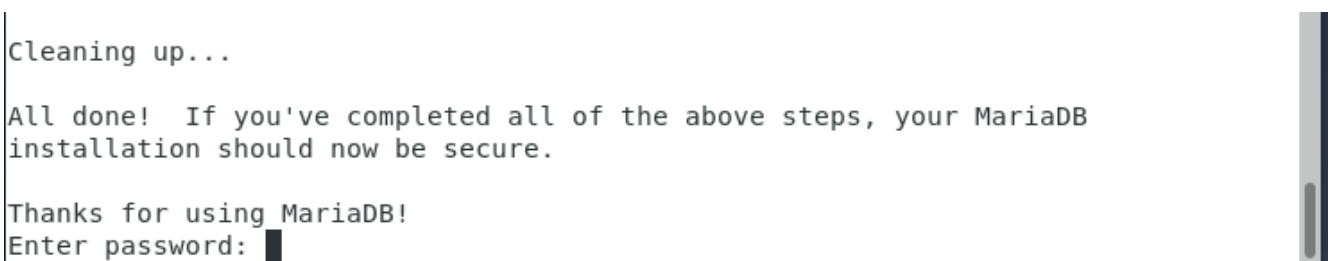


```
marcus@localhost:~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
  
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB  
SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!  
  
In order to log into MariaDB to secure it, we'll need the current  
password for the 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):
```

E responda as perguntas da seguinte maneira:

1. Set root password? **[Y/n] n**
2. Remove anonymous users? **[Y/n] y**
3. Disallow root login remotely? **[Y/n] y**
4. Remove test database and access to it? **[Y/n] y**
5. Reload privilege tables now? **[Y/n] y**

Ao final ele vai solicitar senha do BD, bastar pressionar **ENTER** e criar BD para o WORDPRESS.



```
Cleaning up...  
  
All done!  If you've completed all of the above steps, your MariaDB  
installation should now be secure.  
  
Thanks for using MariaDB!  
Enter password:
```

BD Criado:

```
CREATE DATABASE db_analista;  
GRANT ALL PRIVILEGES on db_analista.* to 'marcus'@'localhost'  
identified by '123';  
FLUSH PRIVILEGES;
```

E ao final utilizar comando “exit”

Ao dar exit ele vai prosseguir com a Instalação do WORDPRESS, automaticamente fazendo Download, configurando permissões.

Após Download e instalação é gerado o arquivo de configuração da base de dados que aparecerá pelo editor NANO para ser modificado.

Altere as seguintes linhas conforme banco criado anteriormente.

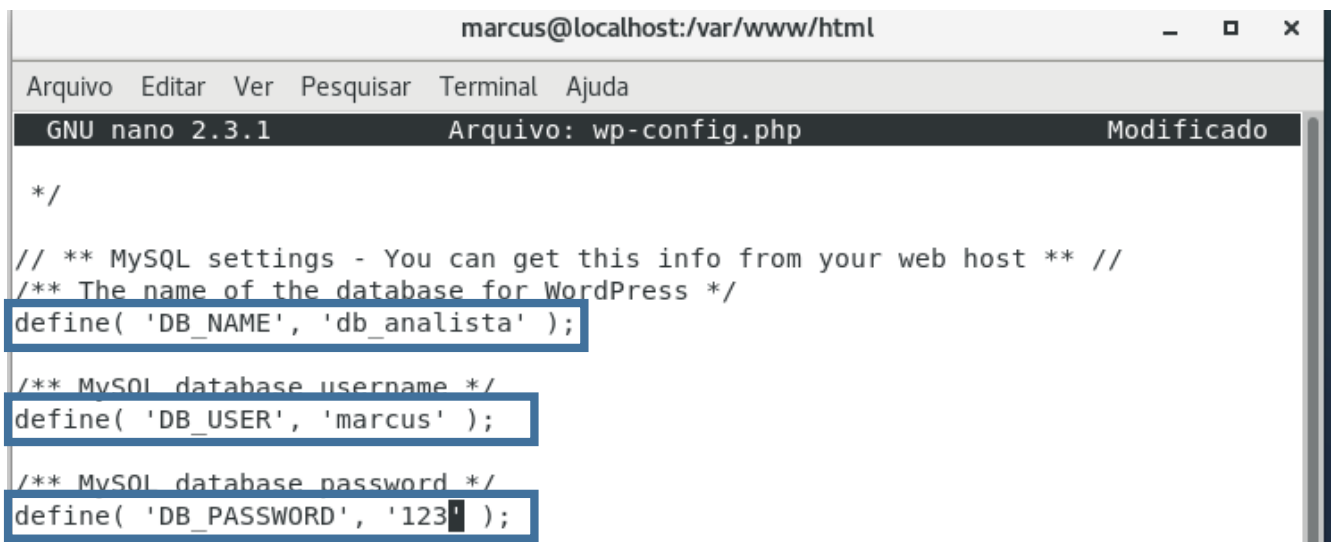
```
define( 'DB_NAME', 'db_analista' );
```

```
/** MySQL database username */
```

```
define( 'DB_USER', 'marcus' );
```

```
/** MySQL database password */
```

```
define( 'DB_PASSWORD', '123' );
```



```
marcus@localhost:/var/www/html
Arquivo Editar Ver Pesquisar Terminal Ajuda
GNU nano 2.3.1 Arquivo: wp-config.php Modificado

*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'db_analista' );

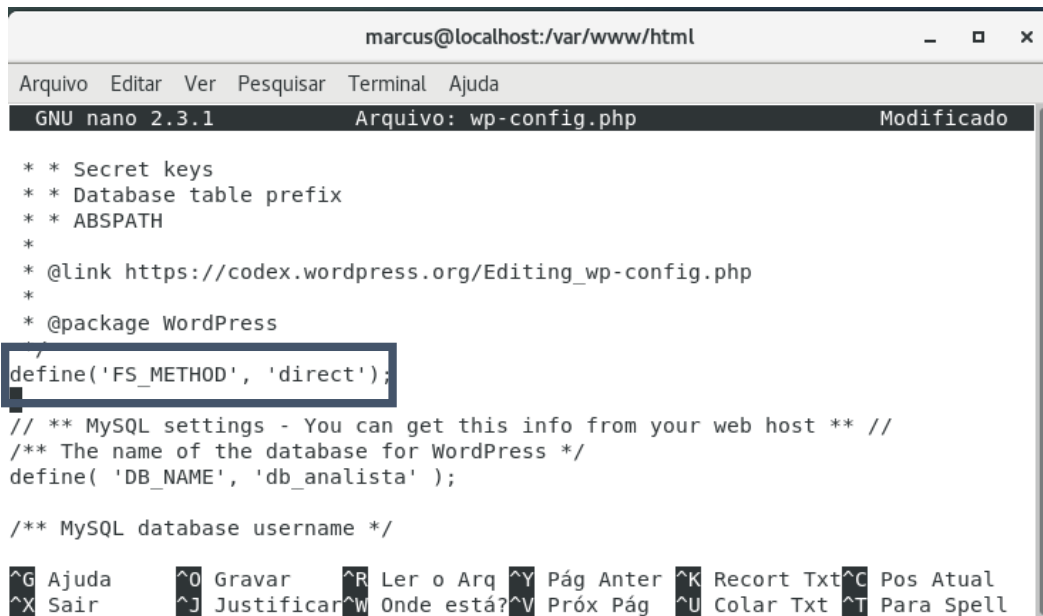
/** MySQL database username */
define( 'DB_USER', 'marcus' );

/** MySQL database password */
define( 'DB_PASSWORD', '123' );
```

Antes de salvar aproveitamos para adicionar a seguinte linha ao arquivo de configuração

```
define( 'FS_METHOD', 'direct' );
```

Assim na hora que formos instalar os plug-ins ele não solicitara um servidor ftp.



```
marcus@localhost:/var/www/html
Arquivo Editar Ver Pesquisar Terminal Ajuda
GNU nano 2.3.1 Arquivo: wp-config.php Modificado


* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/
define('FS_METHOD', 'direct');
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'db_analista' );

/** MySQL database username */

^G Ajuda    ^O Gravar   ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair     ^J Justificar ^W Onde está? ^V Próx Pág  ^U Colar Txt  ^T Para Spell
```

Após salvo, ele prosseguirá com a liberação dos serviços http e https no firewall, utilizando o firewall-cmd. Em seguida vamos proceder à configuração do WordPress propriamente dita. Para isso basta colocar no browser [http://<IP\\_maquina\\_wordpress>](http://<IP_maquina_wordpress>).

*(Nota: Se vos aparecer a informação “Forbidden You don’t have permission to access / on this server.” insiram no terminal o seguinte comando: setenforce 0)*



## Welcome

---

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

## Information needed

---

Please provide the following information. Don't worry, you can always change these settings later.

**Site Title**

**Username**

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods and the @ symbol.

**Password, twice**  
A password will be automatically generated for you if you leave this blank.

Strength indicator

Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! \* ? \$ % ^ & .

**Your E-mail**

Double-check your email address before continuing.

**Privacy**

☒ Allow search engines to index this site.

Install WordPress

Após configurar basta fazer Login assim podemos prosseguir com o próximo script.



## SERVIDOR LDAP (SCRIPT 02\_SERVIDORLDAP.sh,)

Agora vamos ao Segundo Script (02\_SERVIDORLDAP.SH), Onde ele vai prosseguir com a instalação do servidor ldap e configuração do mesmo.

```
marcus@localhost: /var/www/html
```

Arquivo	Editar	Ver	Pesquisar	Terminal	Ajuda
---------	--------	-----	-----------	----------	-------

```
* remi-safe: remi.xpg.com.br
* updates: ftp.unicamp.br
No packages marked for update
Plugins carregados: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: ftp.unicamp.br
* epel: espejito.fder.edu.uy
* extras: ftp.unicamp.br
* remi-php56: remi.xpg.com.br
* remi-safe: remi.xpg.com.br
* updates: ftp.unicamp.br
O pacote openssl-2.4.44-21.el7_6.x86_64 já está instalado em sua última versão
Resolvendo dependências
--> Executando verificação da transação
--> 0 pacote compat-openssl.x86_64 1:2.3.43-5.el7 será instalado
--> 0 pacote openssl-clients.x86_64 0:2.4.44-21.el7_6 será instalado
--> 0 pacote openssl-devel.x86_64 0:2.4.44-21.el7_6 será instalado
--> Processando dependência: cyrus-sasl-devel(x86-64) para o pacote: openssl-devel-2.4.44-21.el7_6.x86_64
--> 0 pacote openssl-servers.x86_64 0:2.4.44-21.el7_6 será instalado
--> 0 pacote openssl-servers-ssl.x86_64 0:2.4.44-21.el7_6 será instalado
--> Processando dependência: libodbc.so.2()(64bit) para o pacote: openssl-servers-ssl-2.4.44-21.el7_6.x86_64
--> Executando verificação da transação
--> 0 pacote cyrus-sasl-devel.x86_64 0:2.1.26-23.el7 será instalado
--> 0 pacote unixODBC.x86_64 0:2.3.1-14.el7 será instalado
```

Após Instalar os Pacotes necessários e ativar os serviços ele vai gerar uma chave ssh para a configuração do ldap.

```
slappasswd -h {SSHA} -s 123 (123 é a senha que escolhi para o servidor)
```

chave gerada:

{SSHA}3P8a5fy0H2VNWgrCm5+fUctt3w+NbzvI  
COPIAR CHAVE GERADA

Após copiar a chave será gerado arquivo de configuração. onde deverá ser da seguinte forma

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=marcus,dc=analista
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=marcus,dc=marcus,dc=analista
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: SENHA GERADA
```

Nesse caso substituir conforme necessário, no exemplo foi criado o seguinte “base”  
`cn=marcus.dc=marcus.dc=analista com a senha 123`

Ao salva e sair será gerado outro arquivo  
Onde nesse será gerada a estrutura da base

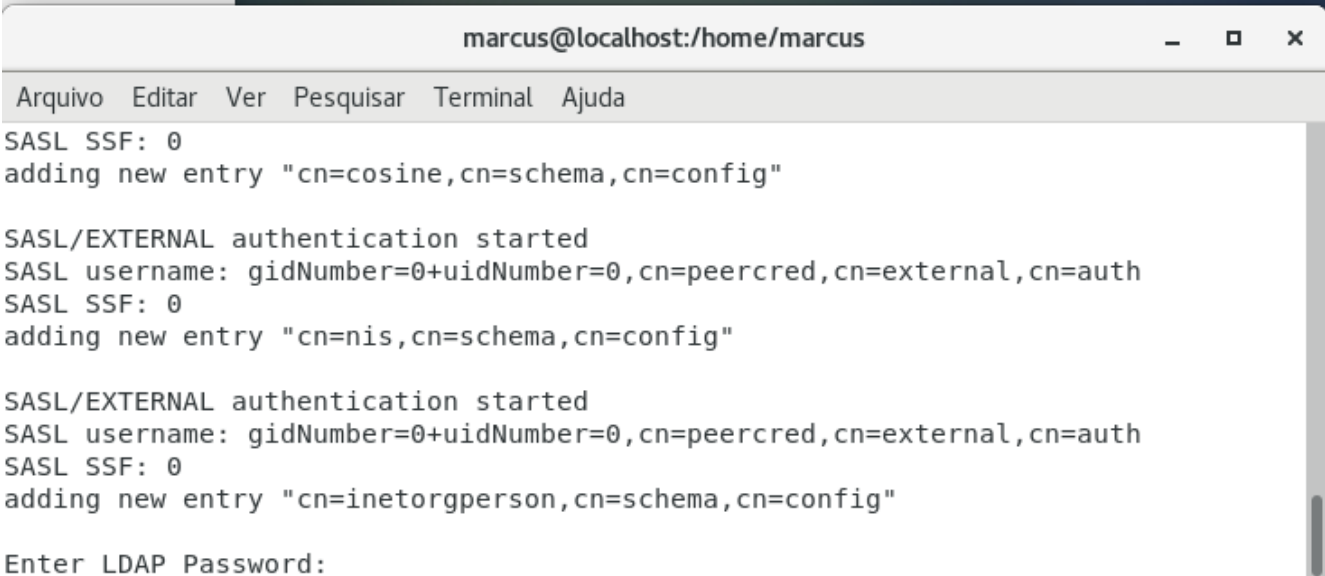
```
dn: dc=marcus,dc=analista
dc: marcus
objectClass: top
objectClass: domain
```

```
dn: cn=marcus ,dc=marcus,dc=analista
objectClass: organizationalRole
cn: marcus
description: LDAP GERENTE
```

```
dn: ou=users,dc=marcus,dc=analista
objectClass: organizationalUnit
ou: Users
```

```
dn: ou=Group,dc=marcus,dc=analista
objectClass: organizationalUnit
ou: Group
```

Ao salvar e sair ele vai pedir a senha da base que foi configurada nesse caso na geração da chave como 123.



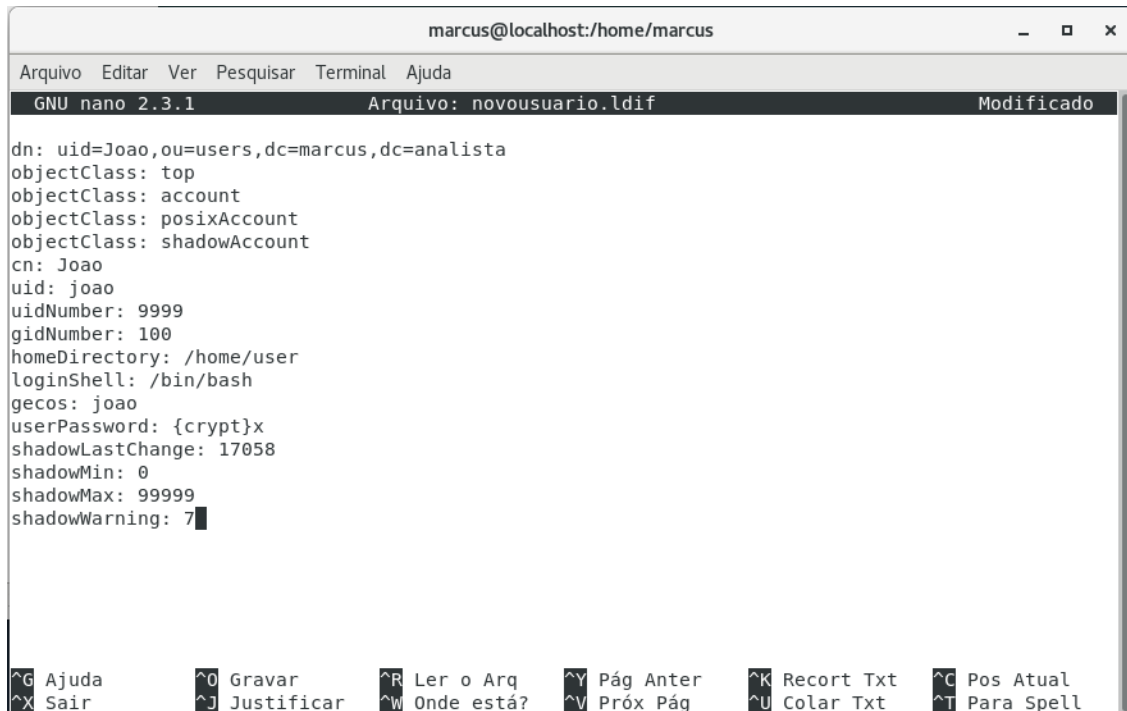
```
marcus@localhost:/home/marcus
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"

Enter LDAP Password:
```

Logo em seguida como teste, será criado arquivo para adicionar um usuário a estrutura criada



```
marcus@localhost:/home/marcus
Arquivo Editar Ver Pesquisar Terminal Ajuda
GNU nano 2.3.1      Arquivo: novousuario.ldif      Modificado

dn: uid=Joao,ou=users,dc=marcus,dc=analista
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: Joao
uid: joao
uidNumber: 9999
gidNumber: 100
homeDirectory: /home/user
loginShell: /bin/bash
gecos: joao
userPassword: {crypt}x
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7

^G Ajuda      ^O Gravar      ^R Ler o Arq  ^Y Pág Anter  ^K Recort Txt  ^C Pos Atual
^X Sair      ^J Justificar  ^W Onde está? ^V Próx Pág   ^U Colar Txt   ^T Para Spell
```

Basta salvar e ele sair e novamente será solicitada a senha da base, basta inserir e novo usuário será adicionado a estrutura. E prosseguirá com a configuração do LDAP ao final seraexecutado um teste para verificar se localiza novo usuário na base LDAP.

```
[root@localhost marcus]# ldapsearch -x cn=Joao -b dc=marcus,dc=analista
# extended LDIF
#
# LDAPv3
# base <dc=marcus,dc=analista> with scope subtree
# filter: cn=Joao
# requesting: ALL
#
# Joao, users, marcus.analista
dn: uid=Joao,ou=users,dc=marcus,dc=analista
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: Joao
uid: joao
uidNumber: 9999
gidNumber: 100
homeDirectory: /home/user
loginShell: /bin/bash
gecos: joao
userPassword:: e2NyeXB0fXg=
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

## PHPLDAPADMIN (03\_PHPLDAPADMIN.sh,)

Agora será instalado o gerenciador WEB para administrar base LDAP pelo script 03\_PHPLDAPADMIN.sh,

```
Resolvendo dependências
--> Executando verificação da transação
---> O pacote phpldapadmin.noarch 0:1.2.3-10.el7 será instalado
--> Resolução de dependências finalizada
```

Dependências resolvidas

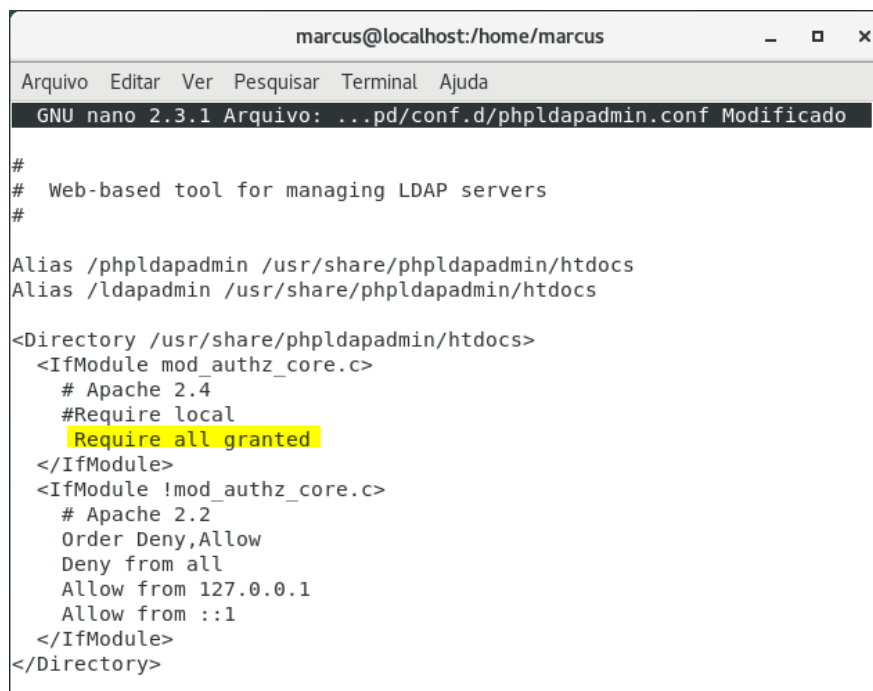
Package	Arq.	Versão	Repo	Tam.
Instalando:				
phpldapadmin	noarch	1.2.3-10.el7	epel	796 k

Resumo da transação

Instalar 1 Package

```
Tamanho total do download: 796 k
Tamanho depois de instalado: 2.4 M
Downloading packages:
phpldapadmin-1.2.3-10.el7.noarch. 0% [ ] 0.0 B/s | 0 B --:--:-- ETA
```

Após ser instalado ele vai gerar arquivo para configuração, primeiro arquivo do apache onde vamos comentar a linha # Require local e adicionar a Require all granted conforme abaixo:



```
marcus@localhost:/home/marcus
Arquivo Editar Ver Pesquisar Terminal Ajuda
GNU nano 2.3.1 Arquivo: ...pd/conf.d/phpldapadmin.conf Modificado

#
# Web-based tool for managing LDAP servers
#

Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
Alias /ldapadmin /usr/share/phpldapadmin/htdocs

<Directory /usr/share/phpldapadmin/htdocs>
  <IfModule mod_authz_core.c>
    # Apache 2.4
    #Require local
    Require all granted
  </IfModule>
  <IfModule !mod_authz_core.c>
    # Apache 2.2
    Order Deny,Allow
    Deny from all
    Allow from 127.0.0.1
    Allow from ::1
  </IfModule>
</Directory>
```

Bastando agora após modificado salvar e sair para prosseguir com script.

Onde agora vai abrir segundo documento porem pelo editor VIM onde esse disponibiliza recurso de sabermos qual linha estamos no documento assim facilitando na configuração baixo:

Vamos alterar as seguintes linhas:

**Linha 291** (“Adicionar nome do Nosso Servidor”)

```
/* A convenient name that will appear in the tree viewer and throughout  
   phpLDAPAdmin to identify this LDAP server to users. */  
$servers->setValue('server','name','Gerenciador LDAP Server');
```

**Linha 332** (“Vamos deixar valor padrão do login na base assim não precisamos digita-lo toda vez que queremos acessa-la”)

```
// $servers->setValue('login','bind_id','');  
$servers->setValue('login','bind_id','cn=marcus,dc=marcus,dc=analista');  
  
-- INSERÇÃO --
```

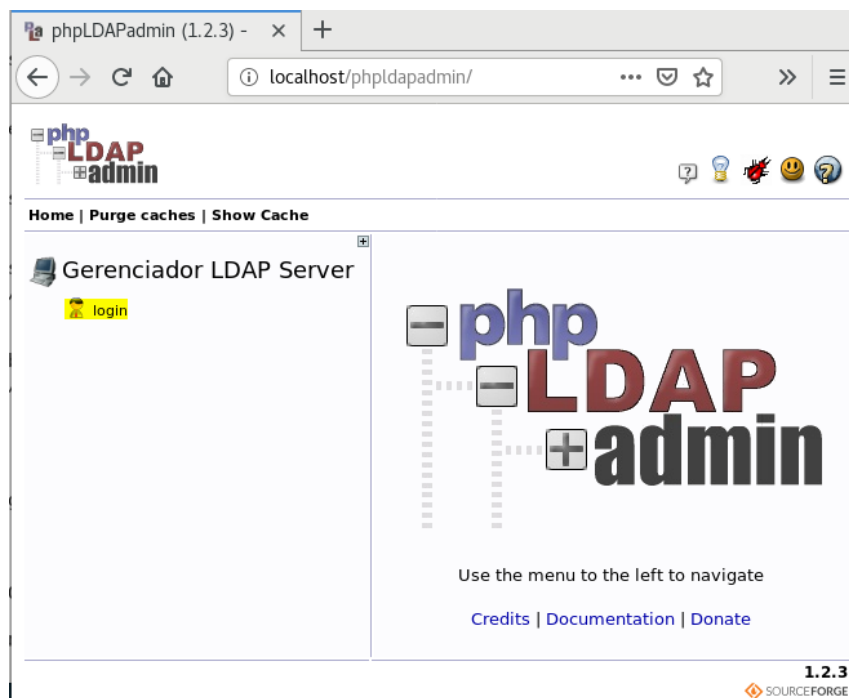
332,70

Agora basta descometa a **linha 397** e **comentar a 398**

```
$servers->setValue('login','attr','dn');  
//$servers->setValue('login','attr','uid');
```

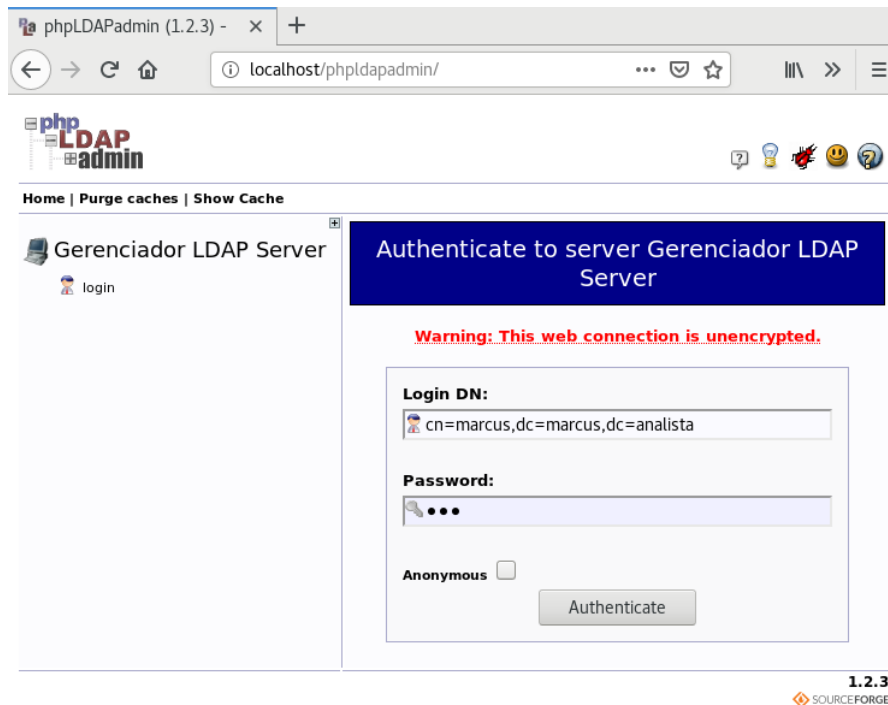
Bastando agora salvar e sair assim concluindo a instalação do PHPLDAPADMIN

Para acessar basta acessar: <http://localhost/phpldapadmin>

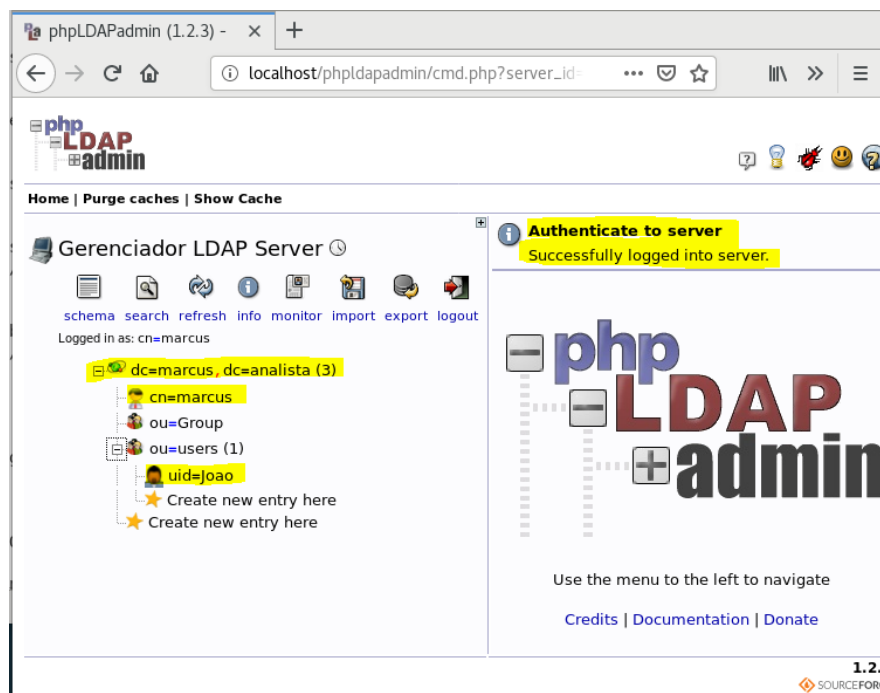


Vamos em Login e testamos o funcionamento do PhpLdapAdmin.

Login: Base Criada, senha:123 criada no momento da criação da chave



Clica para se Autenticar, e verificamos que a base está conforme criamos.



## ZABBIX (04\_zabbix.sh)

Esse script cuidara da parte do sistema Zabbix que ser utilizado para monitoramento da maquia e banco de dados. Primeiro devemos criar um BD para o Zabbix, assim logo que iniciamos o script será aberto tela para criar o BD.

```
[root@localhost marcus]# '/home/marcus/Área de trabalho/04_zabbix.sh,'
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.64-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

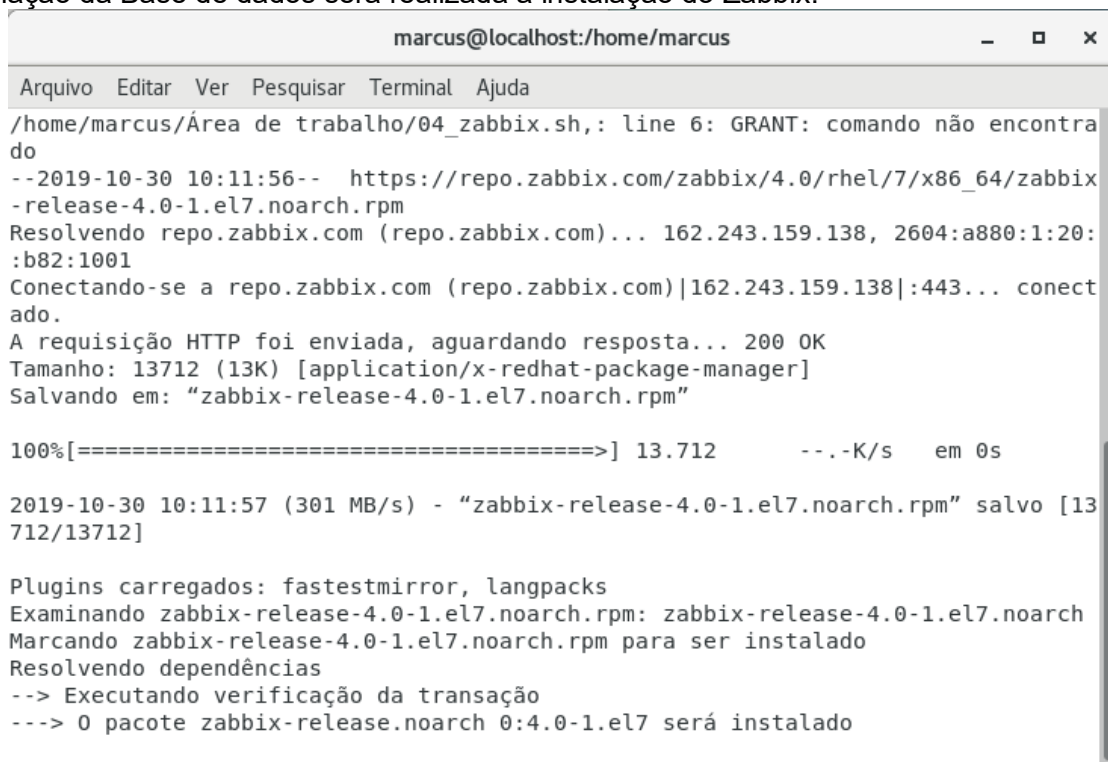
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> █
```

No caso foi criado seguinte BD:

```
CREATE DATABASE zabbix CHARACTER SET utf8 collate utf8_bin;
GRANT ALL ON zabbix.* TO 'zabbix'@'localhost' IDENTIFIED BY '123';
```

Após criação da Base de dados será realizada a instalação do Zabbix.



```
marcus@localhost:/home/marcus
Arquivo Editar Ver Pesquisar Terminal Ajuda
/home/marcus/Área de trabalho/04_zabbix.sh,: line 6: GRANT: comando não encontra
do
--2019-10-30 10:11:56-- https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix
-release-4.0-1.el7.noarch.rpm
Resolvendo repo.zabbix.com (repo.zabbix.com)... 162.243.159.138, 2604:a880:1:20:
:b82:1001
Conectando-se a repo.zabbix.com (repo.zabbix.com)|162.243.159.138|:443... conect
ado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 13712 (13K) [application/x-redhat-package-manager]
Salvando em: "zabbix-release-4.0-1.el7.noarch.rpm"

100%[=====>] 13.712 --.-K/s em 0s

2019-10-30 10:11:57 (301 MB/s) - "zabbix-release-4.0-1.el7.noarch.rpm" salvo [13
712/13712]

Plugins carregados: fastestmirror, langpacks
Examinando zabbix-release-4.0-1.el7.noarch.rpm: zabbix-release-4.0-1.el7.noarch
Marcando zabbix-release-4.0-1.el7.noarch.rpm para ser instalado
Resolvendo dependências
--> Executando verificação da transação
---> 0 pacote zabbix-release.noarch 0:4.0-1.el7 será instalado
```

Após concluir esse procedimento sera aberto arquivo de configuração onde apenas vamos alterar o campo **# php\_value date.timezone Europe/Riga** (tirando do comentário e alterar a região) ficando assim:

```
marcus@localhost
Arquivo Editar Ver Pesquisar Terminal Ajuda
Alias /zabbix /usr/share/zabbix

<Directory "/usr/share/zabbix">
  Options FollowSymLinks
  AllowOverride None
  Require all granted

  <IfModule mod_php5.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_vars 10000
    php_value always_populate_raw_post_data -1
    php_value date.timezone America/Manaus
  </IfModule>
</Directory>
```

Após essa configuração de TimeZone será aberto outro documento onde vamos adicionar a senha do BD criado, Vamos localizar a linha `#DBPassword=` onde vamos tira-la do comentário e altera-la com a nossa senha.

```
marcus@localhost:/home/marcus
Arquivo Editar Ver Pesquisar Terminal Ajuda
GNU nano 2.3.1 Arquivo: /etc/zabbix/zabbix_server.conf Modificado

#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=123

### Option: DBSocket
# Path to MySQL socket.
#
# Mandatory: no

^G Ajuda ^O Gravar ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair ^J Justificar ^W Onde está? ^V Próx Pág ^U Colar Txt ^T Para Spell
```

Após salvar e fechar ela vai concluir a instalação, e verificar status, porem sistema bloqueou de rodar, então ele automaticamente aplica as alterações de sistema e executa o servidor novamente e adiciona ao firewall.

Porém ainda precisamos configurar Zabbix para monitorar os recursos da máquina para isso entrado em `localhost/zabbix`.





Basta Clicar em NEXT STEP

Nessa próxima tela será mostrado se toda configuração inicial está correta, se estiver damos um NEXT

**ZABBIX**

Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

## Check of pre-requisites

	Current value	Required	
PHP version	5.6.40	5.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	America/Manaus		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

Back Next step

Então agora configuramos conforme nossa base de dados anterior e avançamos.



Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

### Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

Database type	<input type="text" value="MySQL"/>
Database host	<input type="text" value="localhost"/>
Database port	<input type="text" value="0"/> 0 - use default port
Database name	<input type="text" value="zabbix"/>
User	<input type="text" value="zabbix"/>
Password	<input type="password" value="..."/>

Back

Next step

Configuramos então IP do servidor, e nome se quiser e avançamos.



Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

### Zabbix server details


Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).

Host	<input type="text" value="localhost"/>
Port	<input type="text" value="10051"/>
Name	<input type="text"/>

Back

Next step

Será mostrada uma tela de confirmação conferimos e avançamos.



Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

### Pre-installation summary


Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Database type	MySQL
Database server	localhost
Database port	default
Database name	zabbix
Database user	zabbix
Database password	***
Zabbix server	localhost
Zabbix server port	10051
Zabbix server name	

Back

Next step

Basta agora finalizar.



Welcome

Check of pre-requisites

Configure DB connection

Zabbix server details

Pre-installation summary

Install

### Install

**Congratulations! You have successfully installed Zabbix frontend.**

Configuration file "/etc/zabbix/web/zabbix.conf.php" created.

Back


Finish

## Analista de Infraestrutura – Eng. Marcus Vinicius dos Santos

Basta realizar login e configurar painéis conforme necessário.

Usuário padrão: Admin

Senha Padrão: zabbix



Username

Admin

Password


••••••

☒ Remember me for 30 days

Sign in

or [sign in as guest](#)

E pronto sistema Zabbix está funcionando.

 Monitoring Inventory Reports Configuration Administration

Dashboard Problems Overview Web Latest data Graphs Screens Maps Discovery Services

Global view Edit dashboard

All dashboards / Global view


System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	85	1 / 0 / 84
Number of items (enabled/disabled/not supported)	92	86 / 0 / 6
Number of triggers (enabled/disabled [problem/ok])	50	50 / 0 / 0 / 50]
Number of users (online)	2	1

Problems by severity

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
No data found.						

Local



## **SEGURANÇA (05\_SEGURANÇA)**

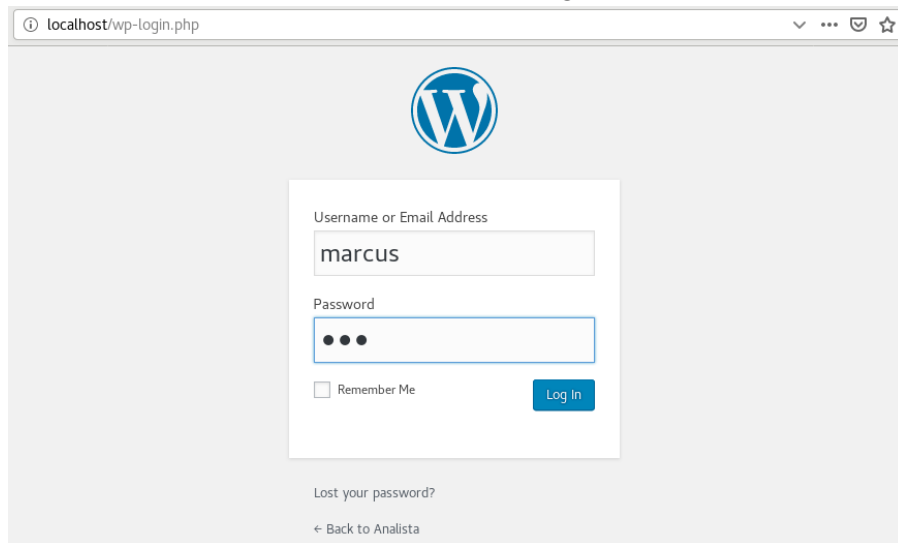
Esse Script tratara da parte da segurança do servidor ele adota como política padrão a estrutura DROP.

Apenas em seguida vai liberando os serviços necessários como http e https em *Stateful* e adição de portas para o restante dos componentes instalados, ainda bloqueia alguns itens como ping ao servidor e proteções diversas contra portscanners, ping of death, ataques DoS. E bloqueando qualquer outra coisa que não foi especificada no Script.

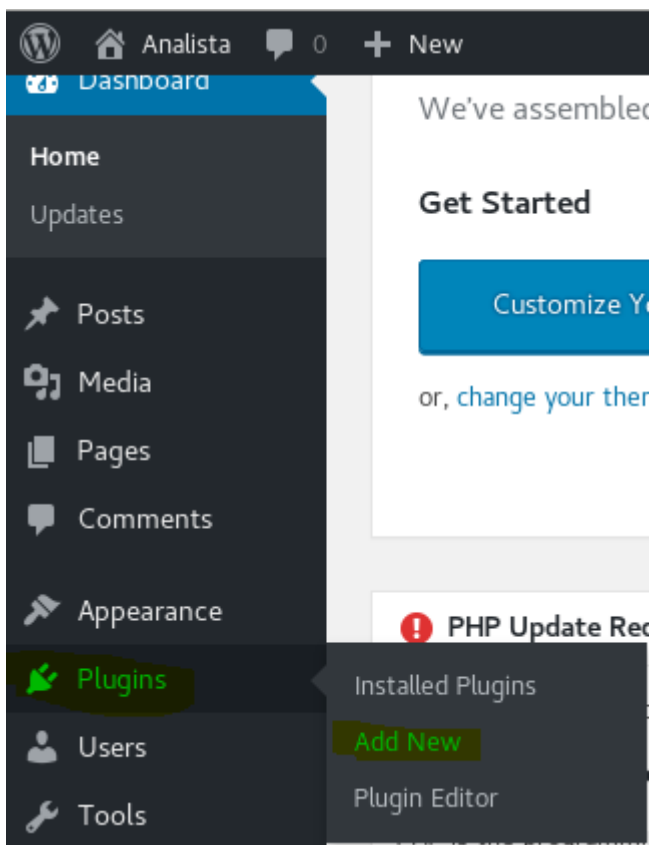
```
Warning: ALREADY_ENABLED: 10051:tcp
success
Warning: ALREADY_ENABLED: 10050:tcp
success
success
Warning: ALREADY_ENABLED: http
success
Warning: ALREADY_ENABLED: https
success
Warning: ALREADY_ENABLED: ldap
success
- - - - -
```

## Configurando WordPress para uso da base de dados LDAP

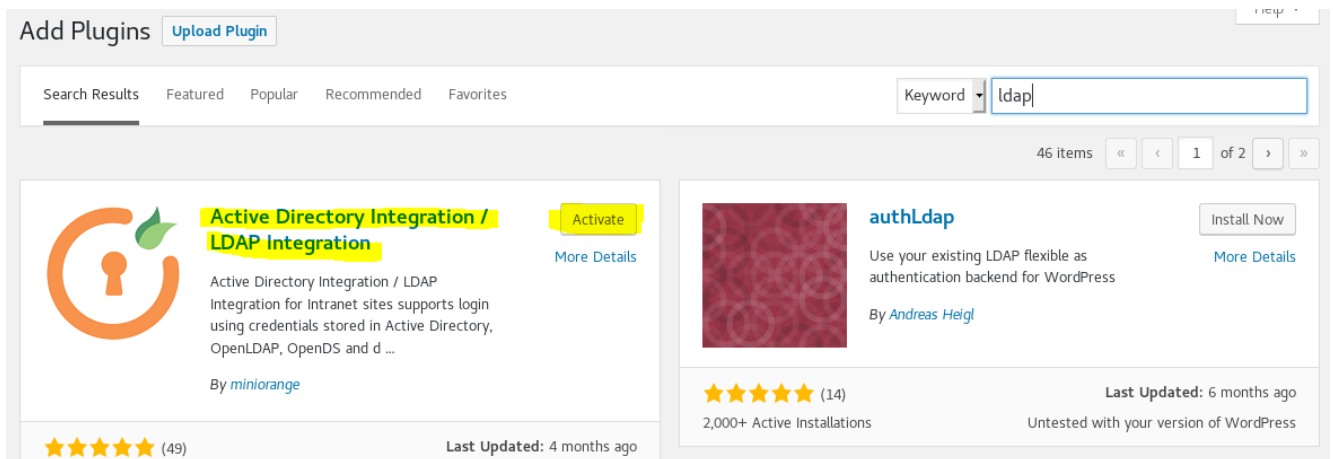
Primeiro devemos entrar como administrador do WORDPRESS



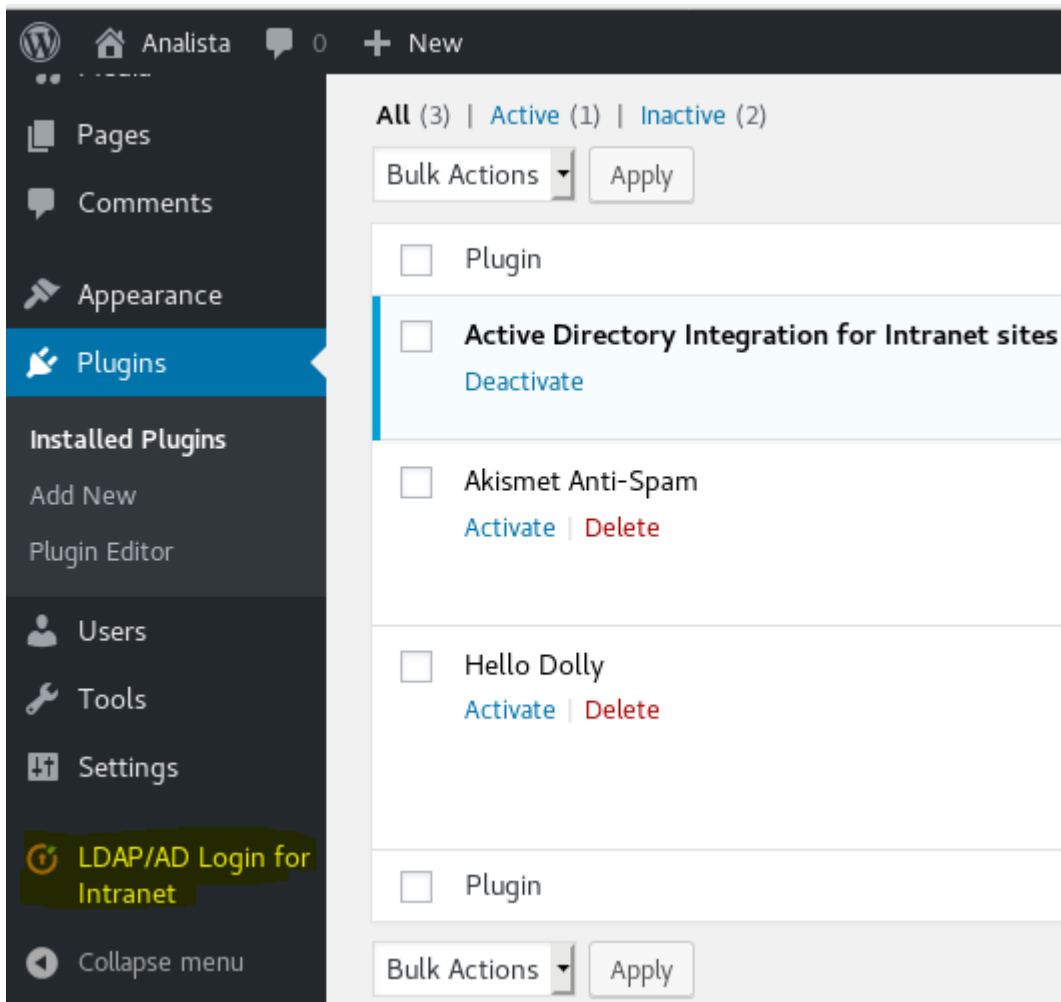
Após entrar, vamos em Plugins e add New



Na barra de pesquisas digitamos LDAP e buscamos pelo Plugin Active Directory Integration/LDAP Integration, e instalamos e ativamos o mesmo.



No Menu lateral vai aparecer **LDAP/AD Login for Intranet**



Agora vamos verificar se a comunicação com a BASE LDAP para isso vamos encontra o campo \*LDAP Server e habilitar Bind anonymously (to check connection to server).

E checar o resultado

\*LDAP Server:

ldap://localhost:389

Specify the host name for the LDAP server eg: ldap://myldapserver.domain:389 , ldap://89.38.192.1:389. When using SSL, the host may have to take the form ldaps://host:636.

☒ Bind anonymously (to check connection to server).

Contact LDAP Server

Se tudo ocorrer bem e as portas estiverem liberadas aparecera a seguinte mensagem:

Successfully contacted LDAP Server. Please configure your Service Account now.

Vamos então prosseguir com os dados necessários para utilização de nossa base. primeiro configuramos o acesso a nossa base. E clicamos em Test.

\*LDAP Server:

ldap://localhost:389

Specify the host name for the LDAP server eg: ldap://myldapserver.domain:389 , ldap://89.38.192.1:389. When using SSL, the host may have to take the form ldaps://host:636.

☐ Bind anonymously (to check connection to server).

\*Service Account Username:



cn=marcus,dc=marcus,dc=analista

This service account username will be used to establish the connection.

Specify the Service Account Uername of the LDAP server in the either way as follows

Username@domainname or Distinguished Name(DN) format

\*Service Account Password:



• • •

Password for the Service Account in the LDAP Server.

Test Connection & Save

Troubleshooting



Após configuração de conexão, configuramos onde o serviço vai localizar as informações para login no exemplo ele vai localizar na base completa e verificar no atributo CN.

### LDAP User Mapping Configuration

\*Search Base(s):

*This is the LDAP Tree under which we will search for the users for authentication. If we are not able to find a user in LDAP it means they are not present in this search base or any of its sub trees. They may be present in some other .*

*Provide the distinguished name of the Search Base object. eg. cn=Users,dc=domain,dc=com.*

*Multiple Search Bases are supported in the [Premium version](#) of the plugin.*

\*Username Attribute:

*This field is important for two reasons.*

- 1. While searching for users, this is the attribute that is going to be matched to see if the user exists.*
- 2. If you want your users to login with their username or firstname.lastname or email - you need to specify those options in this field. e.g. `LDAP_ATTRIBUTE`. Replace `<LDAP_ATTRIBUTE>` with the attribute where your username is stored. Some common attributes are*

Clicamos em save Mapping, e por fim podemos testar se login esta ocorrendo de maneira correta, para testar vamos em Test Authentication e colocamos as credenciais de algum usuário da nossa base, como exemplo utilizarei o cadastro Joao feito anteriormente.

E clicamos em TEST

**OBS: CASO A SENHA NÃO ESTEJA FUNCIONANDO RODE O COMANDO TROCANDO O 123 PELA SENHA DESEJADA, APÓS ISSO AGUARDAR ATÉ A BASE SER ATUALIZADA.**

```
ldappasswd -s 123 -W -D "cn=marcus,dc=marcus,dc=analista" -x "uid=Joao,ou=users,dc=marcus,dc=analista"
```

### Test Authentication

Wordpress username is mapped to the **LDAP attribute defined in the Search Filter** attribute in LDAP. Ensure that you have an administrator user in LDAP with the same attribute value.

\*Username:

\*Password:

A seguinte mensagem vai aparecer

You have successfully configured your LDAP settings.  
You can now do either of two things.

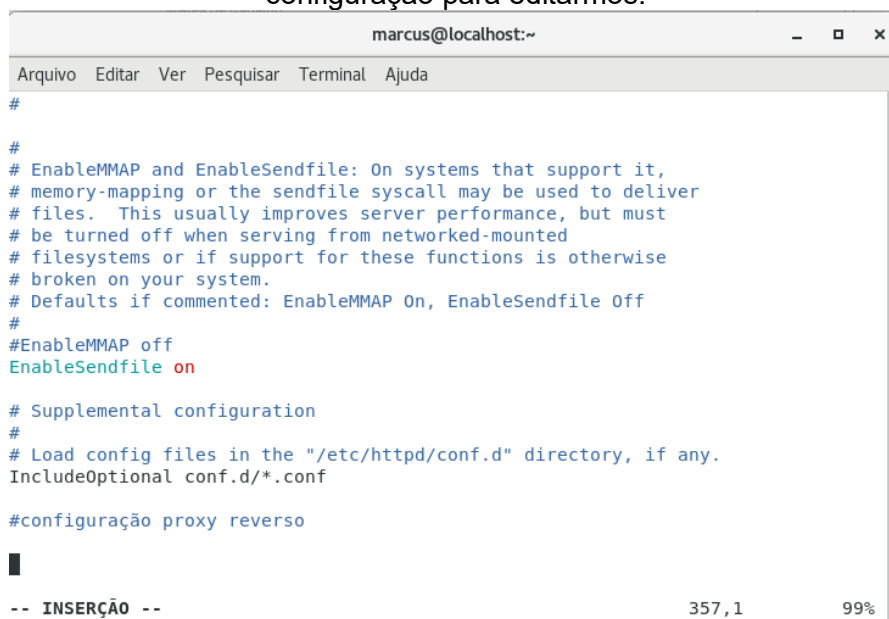
1. Enable LDAP Login at the top and then [Logout](#) from wordpress and login again with your LDAP credentials.
2. Do role mapping ([Click here](#))

Agora nosso WordPress está utilizando a Base LDAP para autenticação.

## PROXY REVERSO

Para esse Script devemos ter outra máquina que sirva como servidor proxy, para funcionar o proxy reverso utilizaremos o recurso de Virtual Host do apache

Ao Rodar o Script ele vai iniciar a instalação do módulo httpd, após isso irá abrir o arquivo de configuração para editarmos.



```
marcus@localhost:~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
#  
#  
# EnableMMAP and EnableSendfile: On systems that support it,  
# memory-mapping or the sendfile syscall may be used to deliver  
# files. This usually improves server performance, but must  
# be turned off when serving from networked-mounted  
# filesystems or if support for these functions is otherwise  
# broken on your system.  
# Defaults if commented: EnableMMAP On, EnableSendfile Off  
#  
#EnableMMAP off  
EnableSendfile on  
#  
# Supplemental configuration  
#  
# Load config files in the "/etc/httpd/conf.d" directory, if any.  
IncludeOptional conf.d/*.conf  
#configuração proxy reverso  
-- INSCRIÇÃO -- 357,1 99%
```

Então ao final desse arquivo iremos adicionar os seguintes comandos.

#módulos de proxy

LoadModule proxy\_module modules/mod\_proxy.so

LoadModule proxy\_http\_module modules/mod\_proxy\_httpd.so

#PROXY REVERSO PARA PORTA 80

<VirtualHost \*:80>

ProxyPreserveasdasdHost On

ProxyPass / <http://192.168.1.4/> #IP SERVIDOR DA APLICAÇÃO

ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO

</VirtualHost>

#PROXY REVERSO PARA POR 389 REFERENTE AO PHPLDAPADMIN

<VirtualHost \*:389>

ProxyPreserveasdasdHost On

ProxyPass / <http://192.168.1.4/> #IP SERVIDOR DA APLICAÇÃO

ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO

</VirtualHost>

#PROXYREVERSO ZABBIX

<VirtualHost \*:1051>

ProxyPreserveasdasdHost On

ProxyPass / <http://192.168.1.4/> #IP SERVIDOR DA APLICAÇÃO

ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO

</VirtualHost>

```
#configuração proxy reverso
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_httpd.so
#PROXY REVERSO PARA PORTA 80
<VirtualHost *:80>
    ProxyPreserveasdasdHost On
    ProxyPass / http://192.168.1.4/ #IP SERVIDOR DA APLICAÇÃO
    ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO
</VirtualHost>
#PROXY REVERSO PARA POR 389 REFERENTE AO PHPLDAPADMIN
<VirtualHost *:389>
    ProxyPreserveasdasdHost On
    ProxyPass / http://192.168.1.4/ #IP SERVIDOR DA APLICAÇÃO
    ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO
</VirtualHost>
#PROXYREVERSO ZABBIX
<VirtualHost *:1051>
    ProxyPreserveasdasdHost On
    ProxyPass / http://192.168.1.4/ #IP SERVIDOR DA APLICAÇÃO
    ProxyPassReverse / http://192.168.1.4 #IP SERVIDOR DA APLICAÇÃO
</VirtualHost>
```

Após editar, salvamos o arquivo e servidor apache será reiniciado.

```
[marcus@localhost ~]$ systemctl restart httpd  
[marcus@localhost ~]$
```

Pronto, o proxy reverso já está em ação.