Installation de Webdev 22 sous linux sur un serveur OVH – Version 2

Table des matières

Table des matières

[Accès au sytème OVH management 4](#_Toc37921299)

[Accès au système SSH IP 51.254.00.00 Port 4622 4](#_Toc37921300)

[Modification du Port SSH en Port 4622 4](#_Toc37921301)

[Add new user bve (Xxxxxxxxxxxxxxxxxxxxx) 5](#_Toc37921302)

[Desactiver la possibilité de se connecter avec root 5](#_Toc37921303)

[Mise en place de Fail2Ban 5](#_Toc37921304)

[Mise en place du firewall 6](#_Toc37921305)

[Install Webmin 7](#_Toc37921306)

[Accès Webmin 7](#_Toc37921307)

[Add sudo users without password 7](#_Toc37921308)

[Install Apache 7](#_Toc37921309)

[Activer ssl / https sur apache https://doc.ubuntu-fr.org/tutoriel/securiser\_apache2\_avec\_ssl 8](#_Toc37921310)

[https://ssl-config.mozilla.org/#server=apache&server-version=2.4.39&config=modern 8](#_Toc37921311)

[Activation du module mod\_headers (Forcer HTTPS avec Strict Transport Security (HSTS)) 8](#_Toc37921312)

[Génération d’un certificat avec Certbot (qui génère un certificat letsencrypt) 8](#_Toc37921313)

[Ajout de la repository 9](#_Toc37921314)

[Fin de l’installation de certbot 9](#_Toc37921315)

[Générer le certificat avec Certbot 9](#_Toc37921316)

[Renouverler le Certificat avec Certbot 9](#_Toc37921317)

[Commande permettant de voir si le certificat est OK 9](#_Toc37921318)

[Activation / Desactivation d’un site 9](#_Toc37921319)

[Desactivation 9](#_Toc37921320)

[Activation 9](#_Toc37921321)

[Activation d’un module 10](#_Toc37921322)

[Debug après le redémarrage d’apache 10](#_Toc37921323)

[Création du site 10](#_Toc37921324)

[Association du domaine à un domaine (www.prmonline.ch) 10](#_Toc37921325)

[Commander le nouveau domaine 10](#_Toc37921326)

[Créer une entrée dans le DNS pour lier le domaine au serveur VPS 10](#_Toc37921327)

[Ajouter une entrée DNS de type « A » 11](#_Toc37921328)

[Attendre pendant 1h que le DNS soit synchronisé 11](#_Toc37921329)

[Créer le site www.prmplaner.ch 11](#_Toc37921330)

[Activation du site 12](#_Toc37921331)

[Générer le certificat www.prmonline.ch avec Certbot 12](#_Toc37921332)

[Vérification de la qualité du certificat 13](#_Toc37921333)

[Créer le site www.prmonline.com avec https 13](#_Toc37921334)

[Activer le site https://www.prmonline.com sous apache 13](#_Toc37921335)

[Installation de mySQL / mariadb 13](#_Toc37921336)

[Installation du package 13](#_Toc37921337)

[Vérification du service 14](#_Toc37921338)

[Création du fichier libmysqlclient.so (Lien symbolic) 14](#_Toc37921339)

[Change the MySQL configuration file 14](#_Toc37921340)

[Création de l’utilisateur CRMmedic 14](#_Toc37921341)

[Change le paramètre bin-address 15](#_Toc37921342)

[Mysql crmmedic database permission 15](#_Toc37921343)

[Change the port 3306 to 43306 15](#_Toc37921344)

[Vérification du n° de port 43306 16](#_Toc37921345)

[Activation du port 16](#_Toc37921346)

[Installation de vsftpd (Facultative) 16](#_Toc37921347)

[Editer "/etc/vsftpd.conf". 17](#_Toc37921348)

[Change the ftp port (4621) 17](#_Toc37921349)

[Connaître les ports ouverts 17](#_Toc37921350)

[Activer le port sur le firewall 17](#_Toc37921351)

[Configure sftp 18](#_Toc37921352)

[Validation du résultat 20](#_Toc37921353)

[Suppression de vsftpd 20](#_Toc37921354)

[Installation de webdev 20](#_Toc37921355)

[Ouverture du fichier d’aide à l’installation en PDF 20](#_Toc37921356)

[Installation des modules complémentaires 20](#_Toc37921357)

[Installation des fonts 21](#_Toc37921358)

[Installation de libstdc++ 21](#_Toc37921359)

[Installation du mode CGI-Apache 21](#_Toc37921360)

[Apache activation du module ssl 21](#_Toc37921361)

[Apache disable “isolation tmp apache” 21](#_Toc37921362)

[Installation de WebDev 22 proprement dite 22](#_Toc37921363)

[Clé d’installation 22](#_Toc37921364)

[Redémarrage de l’application Webdev 22 22](#_Toc37921365)

[Vérification de l’installation 23](#_Toc37921366)

[Mise à jour de la version de Webdev 23](#_Toc37921367)

[Validation de la version 23](#_Toc37921368)

[Créer les comptes WebDev 23](#_Toc37921369)

[Création de l’utilisateur « dev » 24](#_Toc37921370)

[Création des répertoires 24](#_Toc37921371)

[Installation de MYSQL pour Webdev 24](#_Toc37921372)

[Modification des paramêtres MYSQL dans l’application webdev 24](#_Toc37921373)

[Ajout du port 43306 dans la connexion 24](#_Toc37921374)

[Déploiement d’une application 25](#_Toc37921375)

[Paramêtres de deploiement 27](#_Toc37921376)

[Paramêtres du site 29](#_Toc37921377)

[HFSQL – Installation 29](#_Toc37921378)

[Download the Installation 29](#_Toc37921379)

[Extract to a Windows Folder 29](#_Toc37921380)

[Procedure d’installation 29](#_Toc37921381)

[Ouverture d’une règle dans le Firewall 31](#_Toc37921382)

[Troubleshooting 31](#_Toc37921383)

[Redémarrer le server 31](#_Toc37921384)

# Accès au sytème OVH management

<https://www.ovh.com/manager/>

ID : vbxxxxxx-ovh

PWD : xxxxxxxxxxxxxxxxxxxxx

# Accès au système SSH IP 51.254.00.00 Port 4622

PARAMETRES D'ACCES:  
L'adresse IPv4 du VPS est : 51.254.00.00  
L'adresse IPv6 du VPS est : 2001:41d0:401:3100:0000:0000:0000:1008  
  
Le nom du VPS est : vps724346.ovh.net  
  
Le compte administrateur suivant a été configuré sur le VPS :

**Nom d'utilisateur : root  
Mot de passe :      Xxxxxxxxxxxxxxxxxxxxx**

# Modification du Port SSH en Port 4622

vi /etc/ssh/sshd\_config

# $OpenBSD: sshd\_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file. See

# sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

**Port 4622**

/etc/init.d/ssh restart

# Add new user bve (Xxxxxxxxxxxxxxxxxxxxx)

root@vps724346:~# **adduser bve**

PWD: Xxxxxxxxxxxxxxxxxxxxx

Adding user `bve' ...

Adding new group `bve' (1001) ...

Adding new user `bve' (1001) with group `bve' ...

Creating home directory `/home/bve' ...

Copying files from `/etc/skel' ...

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Changing the user information for bve

# Desactiver la possibilité de se connecter avec root

Vi /etc/ssh/sshd\_config

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

# override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis

#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

**PermitRootLogin no**

Redémarage du service

**/etc/init.d/ssh restart**

# Mise en place de Fail2Ban

apt-get install fail2ban

Une fois le paquet installé, il faut modifier le fichier de configuration de ce dernier pour l’adapter à la vôtre. Avant toute modification, il est recommandé d’effectuer une sauvegarde du fichier de configuration en tapant la commande suivante :

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup

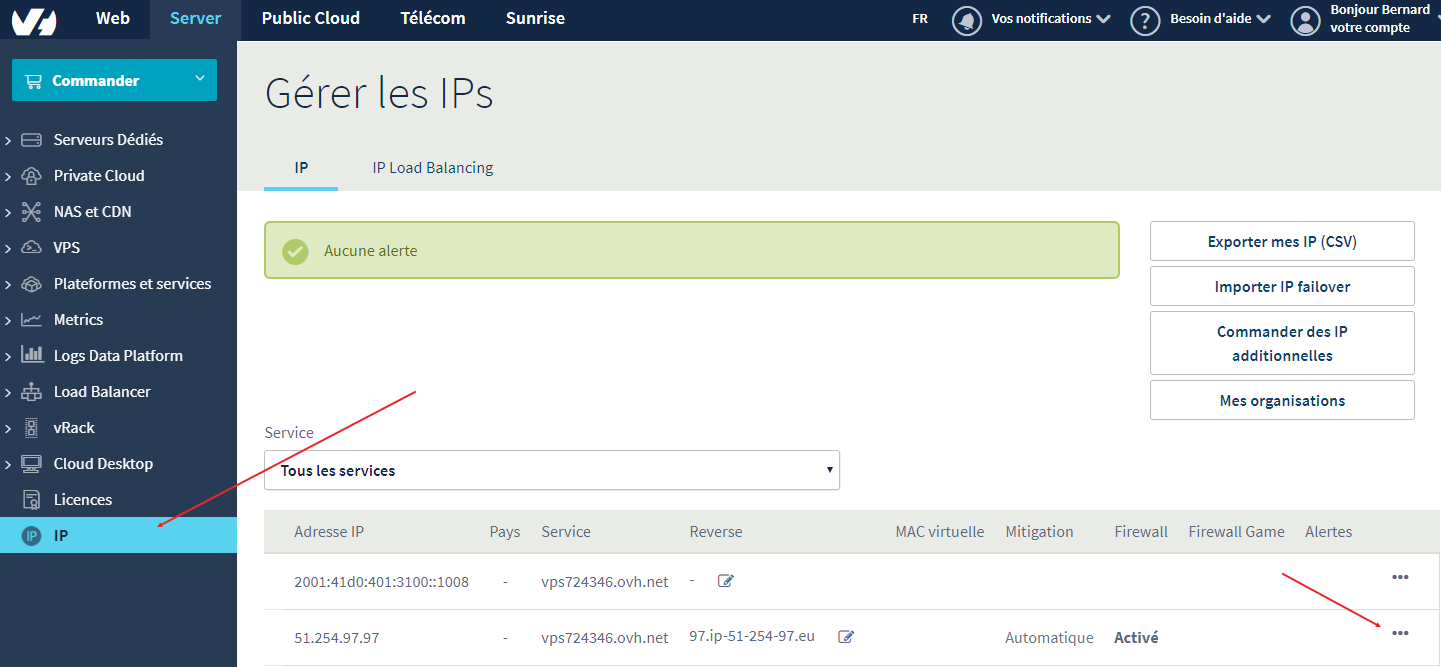
Apportez ensuite vos modifications sur le fichier :

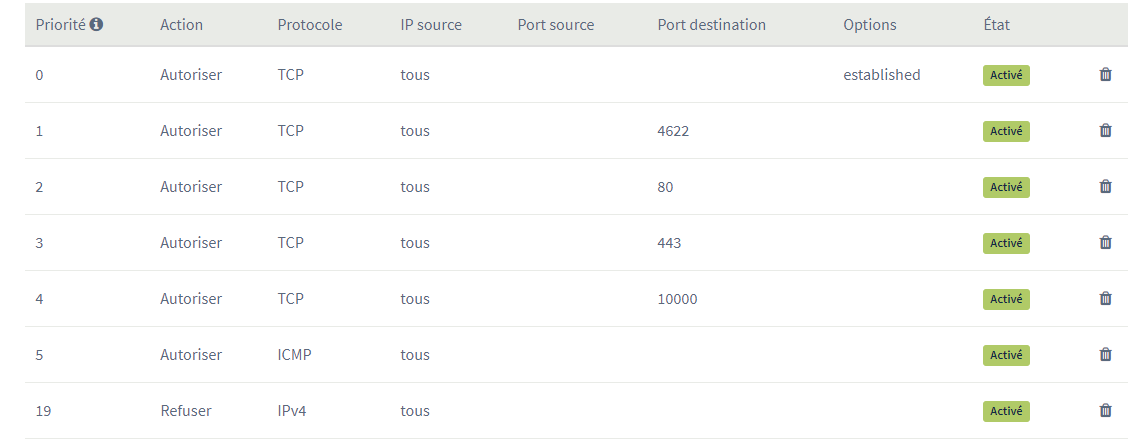
nano /etc/fail2ban/jail.conf

Une fois ces modifications terminées, redémarrez le service à l’aide de la commande suivante :

/etc/init.d/fail2ban restart

# Mise en place du firewall





# Install Webmin

Ajouter la repository dans le serveur

Vi /etc/apt/sources.list

Ajouter la ligne suivante

deb http://download.webmin.com/download/repository sarge contrib

Acquisition de la clé

wget <http://www.webmin.com/jcameron-key.asc>

sudo apt-key add jcameron-key.asc

Mise à jour de la repository

sudo apt update

sudo apt install webmin

## Accès Webmin

https://vps724346.ovh.net:10000

# Add sudo users without password

On ajoute l’utilisateur bve au groupe admin

usermod -a -G admin be

visudo

et ajouter la ligne suivante :

# User privilege specification

root ALL=(ALL:ALL) ALL

**bve ALL=(ALL) NOPASSWD:ALL**

… ensuite on peut exécuter les commandes sudo xy

# Install Apache

sudo apt-get install apache2

Test de la connection

<http://vps724346.ovh.net/>

Les commandes de base pour piloter Apache

/etc/apache2/apache2.conf

/etc/apache2/ports.conf

/etc/apache2/sites-available

/etc/apache2/sites-enabled

sudo systemctl stop apache2.service

sudo systemctl start apache2.service

sudo systemctl restart apache2.service

sudo systemctl reload apache2.service

## Activer ssl / https sur apache <https://doc.ubuntu-fr.org/tutoriel/securiser_apache2_avec_ssl>

Pour Générer de configurations propres

## <https://ssl-config.mozilla.org/#server=apache&server-version=2.4.39&config=modern>

**sudo a2enmod ssl**

bve@vps724346:~$ sudo a2enmod ssl

Considering dependency setenvif for ssl:

Module setenvif already enabled

Considering dependency mime for ssl:

Module mime already enabled

Considering dependency socache\_shmcb for ssl:

Enabling module socache\_shmcb.

Enabling module ssl.

See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.

To activate the new configuration, you need to run:

**sudo systemctl restart apache2**

Test l’activation du module

**apache2ctl -M | grep ssl**

## Activation du module mod\_headers (Forcer HTTPS avec Strict Transport Security (HSTS))

LoadModule headers\_module modules/mod\_headers.so

sudo a2enmod headers

## Génération d’un certificat avec Certbot (qui génère un certificat letsencrypt)

### Ajout de la repository

sudo apt update

sudo apt install software-properties-common

sudo add-apt-repository ppa:certbot/certbot

sudo apt update

### Fin de l’installation de certbot

sudo apt install certbot

## Générer le certificat avec Certbot

sudo certbot certonly --webroot -w /var/www/example -d example.com -d www.example.com

## Renouverler le Certificat avec Certbot

sudo certbot certonly --webroot -w /home/dev/site/gestionpatient/GESTIONPATIENT\_WEB --renew-by-default -d prmonline.ch -d [www.prmonline.ch](http://www.prmonline.ch)

## Commande permettant de voir si le certificat est OK

sudo certbot certificates

#Si la date est ok, ne pas oublier de redémarrer Apache

sudo systemctl stop apache2.service

sudo systemctl start apache2.service

sudo systemctl restart apache2.service

sudo systemctl reload apache2.service

Si la date est ok, ne pas oublier de redémarrer Apache

/etc/letsencrypt/csr/0000\_csr-certbot.pem

/etc/letsencrypt/keys/0000\_key-certbot.pem

## Activation / Desactivation d’un site

### Desactivation

sudo a2dissite example.com.conf

### Activation

sudo a2ensite example.com.conf

systemctl reload apache2

### Activation d’un module

sudo a2enmod php5

### Debug après le redémarrage d’apache

systemctl status apache2.service

## Création du site

sudo cp -p default-ssl.conf 001-default-ssl.conf

Multiple identities can be used for authentication:

# Association du domaine à un domaine (www.prmonline.ch)

## Commander le nouveau domaine



## Créer une entrée dans le DNS pour lier le domaine au serveur VPS



## Ajouter une entrée DNS de type « A »



Suppression de l’entrée qui redirige vers les mails

Suppression de entrée “A” prmonline.ch qui renvoie vers 213.186.33.5

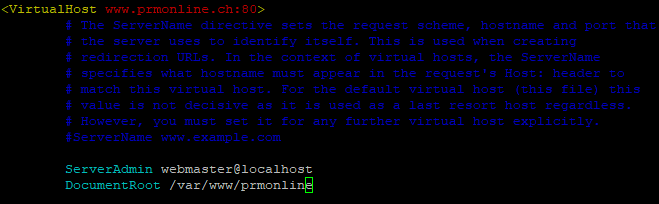
 

## Attendre pendant 1h que le DNS soit synchronisé

# Créer le site www.prmplaner.ch

cd /etc/apache2/sites-available

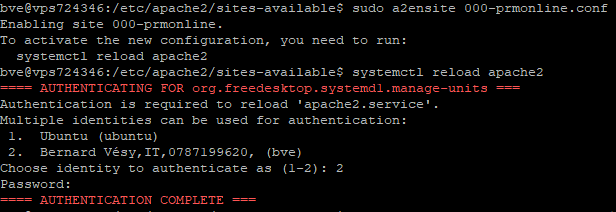
sudo mkdir /var/www/prmonline

sudo cp -p 000-default.conf 000-prmonline.conf  
  


## Activation du site

sudo a2ensite 000-prmonline.conf

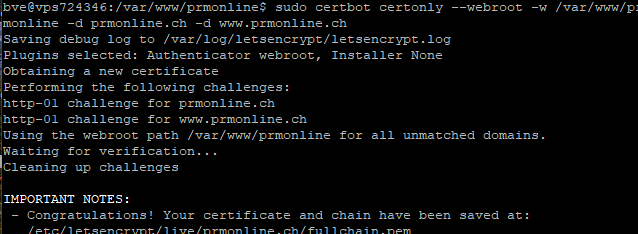
systemctl reload apache2



## Générer le certificat www.prmonline.ch avec Certbot

cd /var/www/prmonline

sudo certbot certonly --webroot -w /var/www/prmonline -d prmonline.ch -d [www.prmonline.ch](http://www.prmonline.ch)

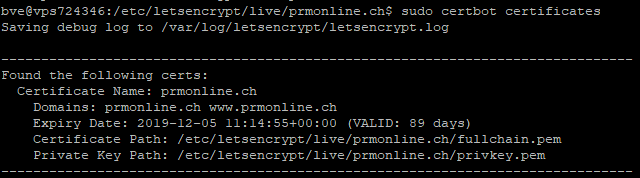


cd /etc/letsencrypt/live/prmonline.ch



## Vérification de la qualité du certificat

sudo certbot certificates



Found the following certs:

Certificate Name: prmonline.ch

Domains: prmonline.ch www.prmonline.ch

Expiry Date: 2019-12-05 11:14:55+00:00 (VALID: 89 days)

Certificate Path: /etc/letsencrypt/live/prmonline.ch/fullchain.pem

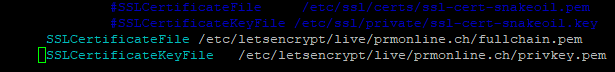
Private Key Path: /etc/letsencrypt/live/prmonline.ch/privkey.pem

## Créer le site www.prmonline.com avec https

cd /etc/apache2/sites-available

sudo cp -p default-ssl.conf 001-prmonline-ssl.conf

sudo vi 001-prmonline-ssl.conf



## Activer le site https://www.prmonline.com sous apache

cd /etc/apache2/sites-available

sudo a2ensite 001-prmonline-ssl.conf

systemctl reload apache2

# Installation de mySQL / mariadb

## Installation du package

sudo apt update

sudo apt install mariadb-server

## Vérification du service

sudo systemctl status mariadb

mysql -V

## Création du fichier libmysqlclient.so (Lien symbolic)

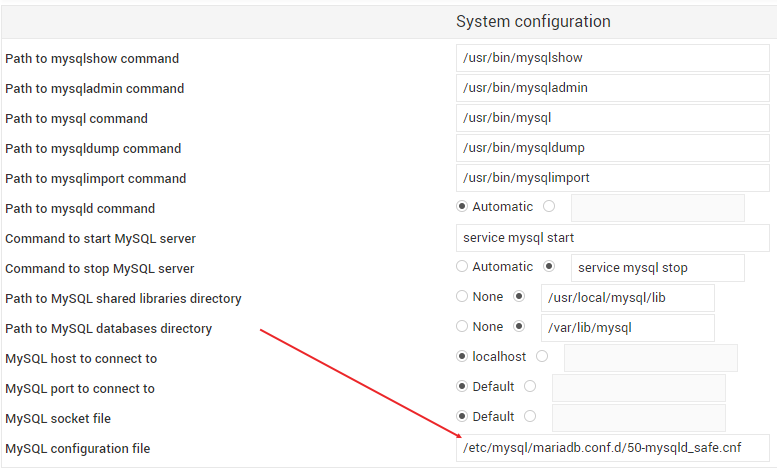
cd /usr/lib/x86\_64-linux-gnu

sudo ln -s /usr/lib/x86\_64-linux-gnu/libmysqlclient.so.20 /usr/lib/libmysqlclient.so

## Change the MySQL configuration file

Change /etc/mysql/mysql.conf.d/mysqld.cnf to

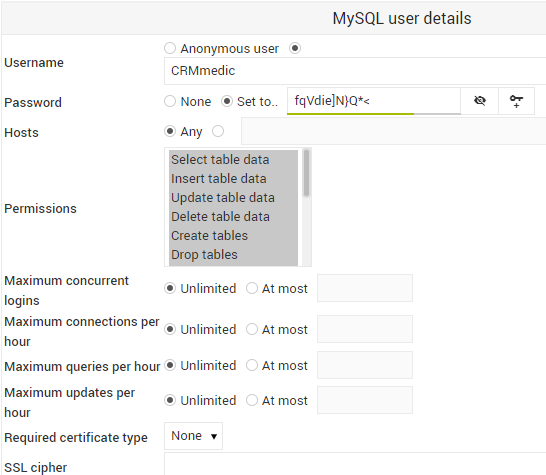
/etc/mysql/mariadb.conf.d/50-mysqld\_safe.cnf



## Création de l’utilisateur CRMmedic

ID: CRMmedic

PWD: xxxxxxxxxxxxxxxxxxx



## Change le paramètre bin-address

sudo vi /etc/mysql/mariadb.conf.d/50-server.cnf

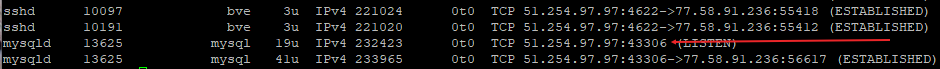
#bind-address = 127.0.0.1a

bind-address = 51.254.00.00

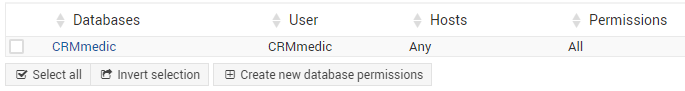
Test

Vérification que le service soit bien démarré

sudo lsof -i -P -n



## Mysql crmmedic database permission



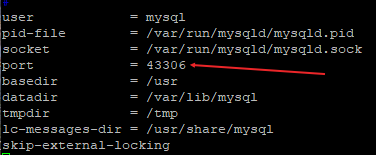
## Change the port 3306 to 43306

sudo vi /etc/mysql/mariadb.conf.d/50-server.cnf

sudo service mysql stop

sudo service mysql start

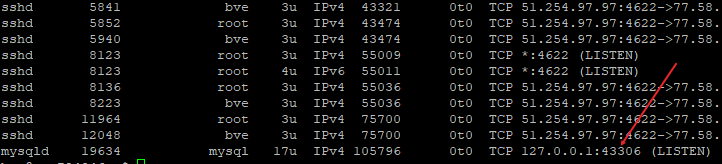
sudo service mysql status



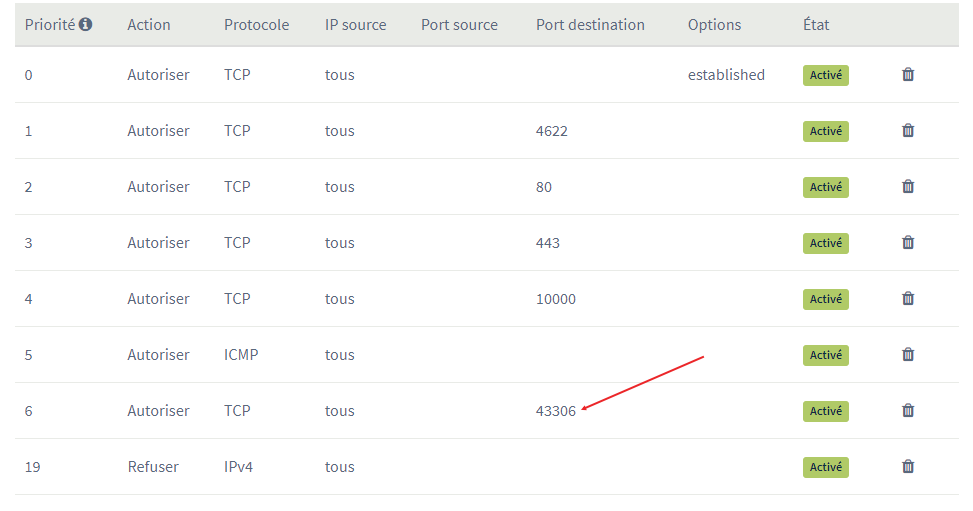
## Vérification du n° de port 43306

43306

sudo lsof -i -P -n



## Activation du port



# Installation de vsftpd (Facultative)

sudo apt-get install vsftpd

## Editer "/etc/vsftpd.conf".

sudo vi /etc/vsftpd.conf

Décommenter la ligne "local\_enable=YES" pour autoriser les logins du poste à se connecter par FTP.

Décommenter la ligne "write\_enable=YES" pour autoriser les écritures.

Décommenter la ligne "local\_umask=022

## Change the ftp port (4621)

sudo vi /etc/vsftpd.conf

add the line

listen\_port=4621

sudo systemctl stop vsftpd

sudo systemctl start vsftpd

sudo systemctl status vsftpd

## Connaître les ports ouverts

sudo lsof -i -P -n

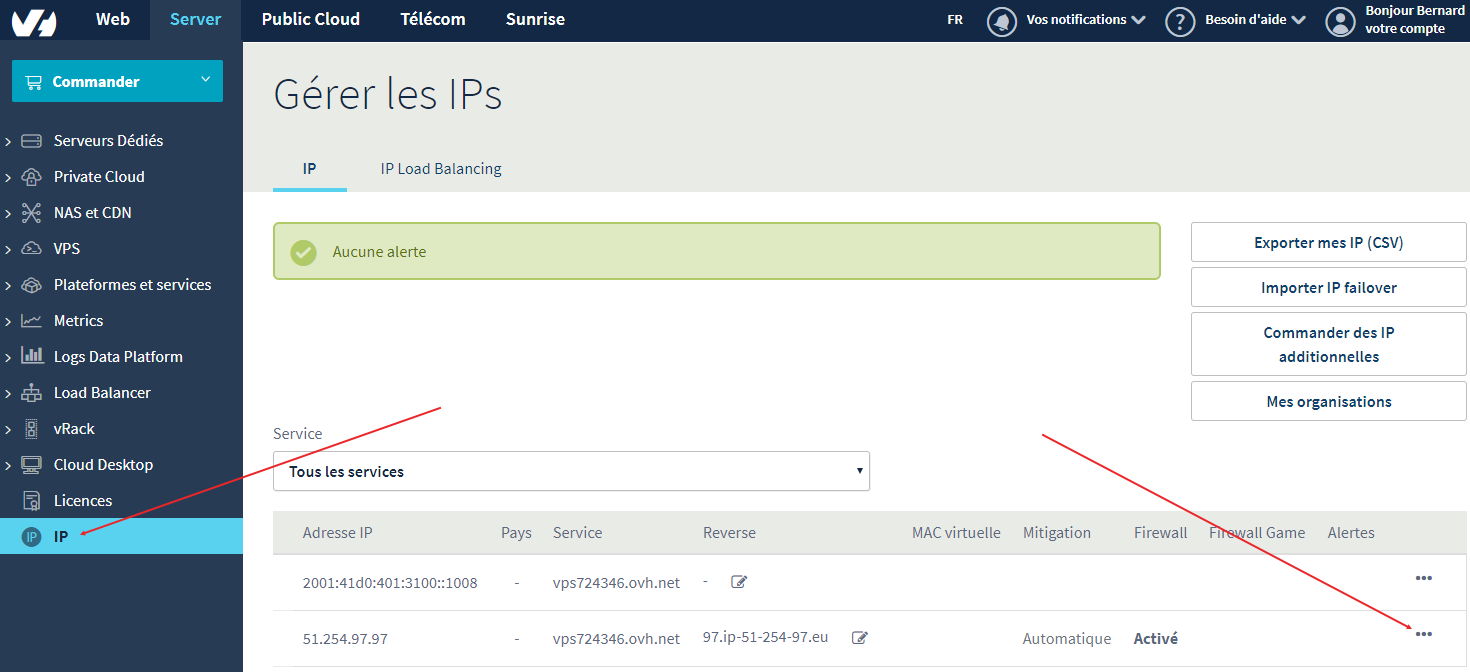
## Activer le port sur le firewall

Accès au VPS

<https://www.ovh.com/manager/>

vb1xxxxx-ovh

Xxxxxxxxxxxxxxxxxxxxxx



# Configure sftp

# $OpenBSD: sshd\_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file. See

# sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

Port 4622

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

# Ciphers and keying

#RekeyLimit default none

# Ciphers and keying

#RekeyLimit default none

# Logging

#SyslogFacility AUTH

#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

#PermitRootLogin prohibit-password

#StrictModes yes

#MaxAuthTries 6

#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized\_keys2 to be disregarded by default in future.

#AuthorizedKeysFile .ssh/authorized\_keys .ssh/authorized\_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none

#AuthorizedKeysCommand none

#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh\_known\_hosts

#HostbasedAuthentication no

# Change to yes if you don't trust ~/.ssh/known\_hosts for

# HostbasedAuthentication

#IgnoreUserKnownHosts no

# Don't read the user's ~/.rhosts and ~/.shosts files

#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!

PasswordAuthentication yes

#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with

# some PAM modules and threads)

ChallengeResponseAuthentication no

# Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

# GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,

# and session processing. If this is enabled, PAM authentication will

# be allowed through the ChallengeResponseAuthentication and

# PasswordAuthentication. Depending on your PAM configuration,

# PAM authentication via ChallengeResponseAuthentication may bypass

# the setting of "PermitRootLogin without-password".

# If you just want the PAM account and session checks to run without

# PAM authentication, then enable this but set PasswordAuthentication

# and ChallengeResponseAuthentication to 'no'.

UsePAM yes

#AllowAgentForwarding yes

#AllowAgentForwarding yes

#AllowTcpForwarding yes

#GatewayPorts no

X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

#PermitTTY yes

PrintMotd no

#PrintLastLog yes

#TCPKeepAlive yes

#UseLogin no

#PermitUserEnvironment no

#Compression delayed

#ClientAliveInterval 0

#ClientAliveCountMax 3

#UseDNS no

#PidFile /var/run/sshd.pid

#MaxStartups 10:30:100

#PermitTunnel no

#ChrootDirectory none

#VersionAddendum none

#VersionAddendum none

# no default banner path

#Banner none

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

# override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis

#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

PermitRootLogin no

## Validation du résultat

sudo systemctl stop vsftpd

sudo systemctl start vsftpd

sudo systemctl status vsftpd

# Suppression de vsftpd

sudo apt-get remove vsftpd

sudo apt-get purge vsftpd

# Installation de webdev

## Ouverture du fichier d’aide à l’installation en PDF

<https://drive.google.com/drive/u/0/folders/0B7fsjyex5F2KYzhId2g3aTJ6V0E>

## Installation des modules complémentaires

sudo apt-get install libqtcore4

sudo apt-get install libqtgui4

sudo apt-get install libxft2

sudo apt-get install libc6-i386

sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl

sudo apt-get install libqt4-dev

## Installation des fonts

sudo apt-get install xfonts-utils

sudo apt-get install libfreetype6-dev

sudo apt-get install xfonts-utils

sudo apt-get install libfreetype6

## Installation de libstdc++

**sudo apt-get install ssh**

**sudo apt-get install libstdc++2.10-glibc2.2**

**sudo apt-get install libstdc++6**

**Création de deux symbolic link**

**sudo ln -s /usr/lib/x86\_64-linux-gnu/libstdc++.so.6.0.25 /usr/lib/libstdc++.so.6**

**sudo ln -s /usr/lib/x86\_64-linux-gnu/libstdc++.so.6.0.25 /usr/lib/libstdc++.so.3**

## Installation du mode CGI-Apache

**sudo a2enmod cgi**

**systemctl restart apache2**

Vérification du résultat

**systemctl status apache2**

**cd /etc/apache2/mods-enabled/**

**sudo ln -s ../mods-available/actions.conf**

**sudo ln -s ../mods-available/actions.load**

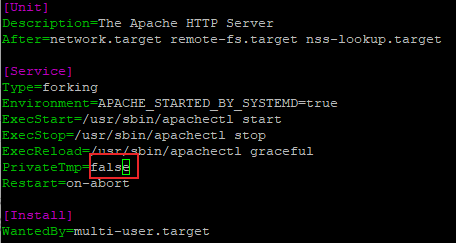
## Apache activation du module ssl

a2enmod ssl

sudo systemctl daemon-reload

sudo service apache2 start

## Apache disable “isolation tmp apache”

sudo vi /lib/systemd/system/apache2.service  
  
Passer la ligne  “PrivateTmp=true” à “PrivateTmp=false”  
  


sudo systemctl daemon-reload

sudo service apache2 start

## Installation de WebDev 22 proprement dite

cd /dump/webdev22/Linux64

chmod +x webdev\_install64

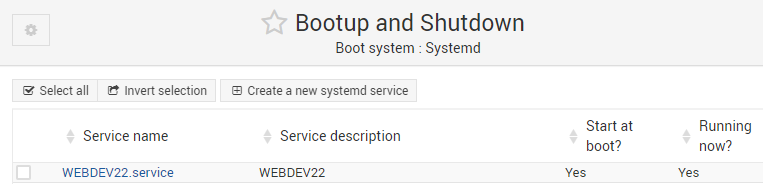
Passer en mode Root !

## Clé d’installation

N22F0122220 (clé d'installation xxxxxx)

Poursuivre le processus d’installation jusqu’à la fin

## Redémarrage de l’application Webdev 22

1. Arrêter le service Apache  
   sudo service apache2 stop
2. Arrêter le service Webdev  
   sudo service WEBDEV22 stop  
     
   Attention Webdev ne peut pas être démarré en mode superuser. L’installation à normalement créé un utilisateur «webdevadmin»
3. Redémarrer le service depuis l’interface Webmin  
     
   

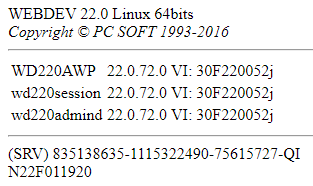
## Vérification de l’installation

http://<Adresse IP Serveur>/WD210AWP/WD210AWP/version

L’URL ci-dessous

<https://www.prmonline.ch/WD220AWP/WD220AWP/version>

Renvoie le résultat suivant :



# Mise à jour de la version de Webdev

cd /dump/webdev22/Linux64/update

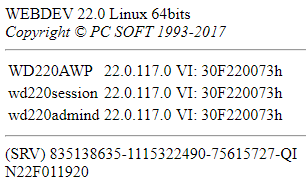
sudo unzip WB220PACKDEPLINUX64073h.zip

chmod +x webdev\_update64

./webdev\_update64

## Validation de la version

https://www.prmonline.ch/WD220AWP/WD220AWP/version



# Créer les comptes WebDev

URL importantes

<https://www.prmonline.ch/WDAdminWeb220>

id: admin

pwd: xxxxxxxxxxxxxxxxxxxxxx

<https://www.prmonline.ch/WD220AWP/WD220AWP/version>

## Création de l’utilisateur « dev »

sudo adduser dev

Ajouter les group webdevadmin

## Création des répertoires

Se connecter avec l’utilisateur « dev »

mkdir /home/dev/

mkdir /home/dev/webserviceSOAP

mkdir /home/dev/webserviceREST

mkdir /home/dev/data

# Installation de MYSQL pour Webdev

cd /dump/webdev22/mysql

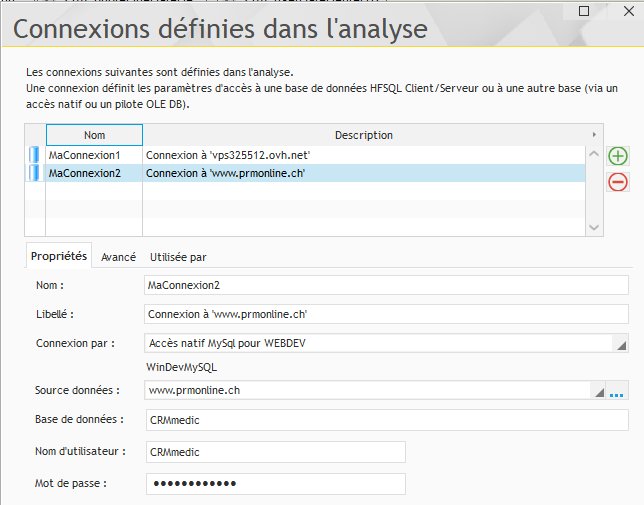
sudo chmod +x mysql\_install64

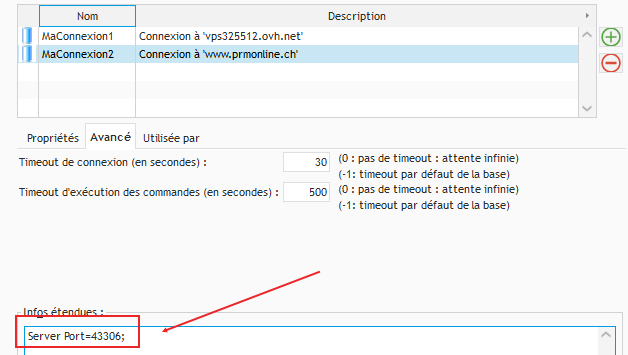
sudo ./mysql\_install



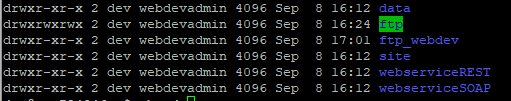
# Modification des paramêtres MYSQL dans l’application webdev

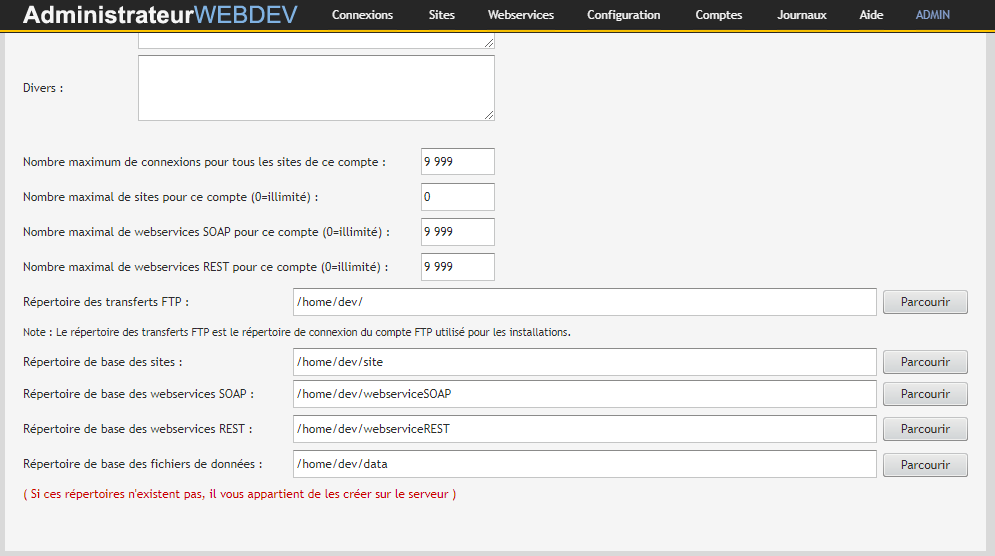
## Ajout du port 43306 dans la connexion



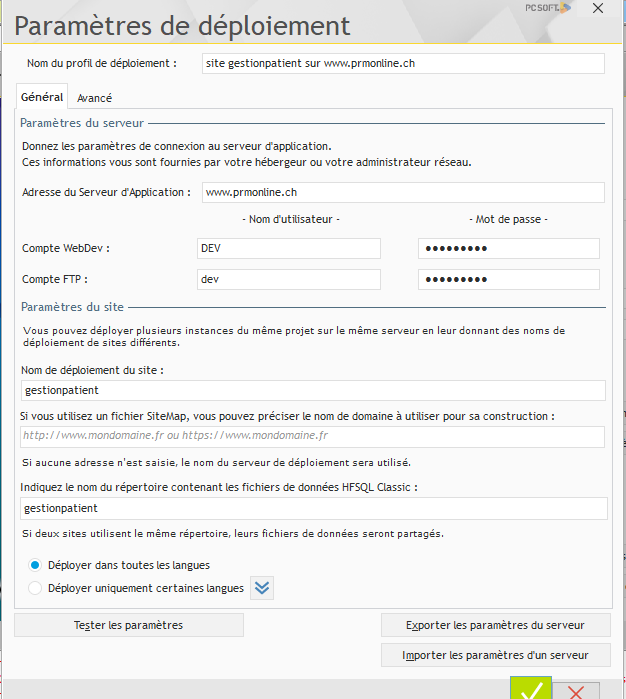


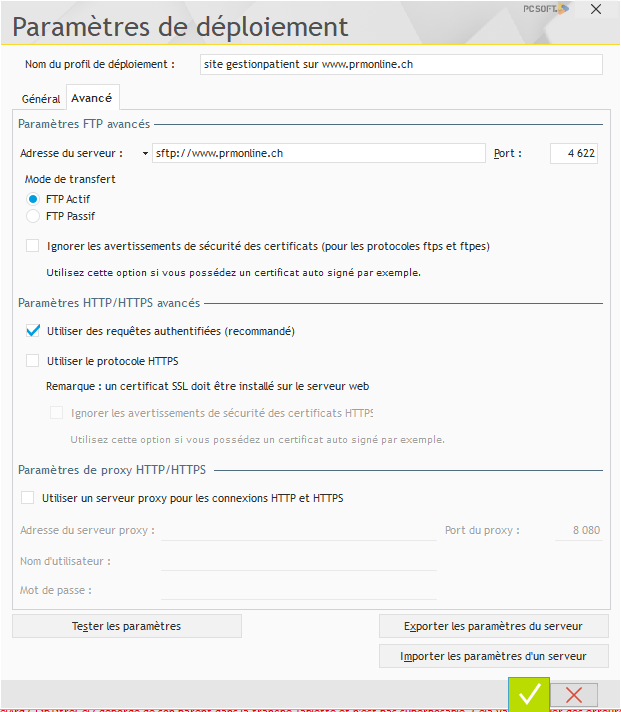
# Déploiement d’une application



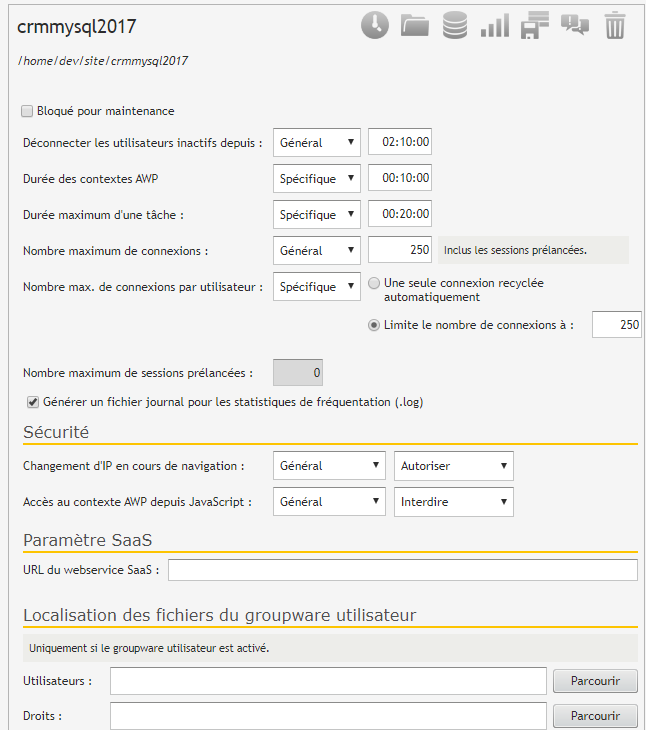


# Paramêtres de deploiement





# Paramêtres du site



# HFSQL – Installation

## Download the Installation

[PCsoft - Link](https://www.pcsoft.fr/st/telec/modules-communs-25/wx25_83h.htm?p=google025HF&gclid=Cj0KCQjwybD0BRDyARIsACyS8mvtsu7ozOVCvO1i_FJHQDcEaTxQGglhJVmsFNDX3dq26uZTu7-apCgaAsXeEALw_wcB)

## Extract to a Windows Folder

Installation Windows contient également les sources d’installation pour Linux

D:\Serveur HFSQL 25 - Installation - 083\Linux64x86

### Procedure d’installation

cd /dump

su

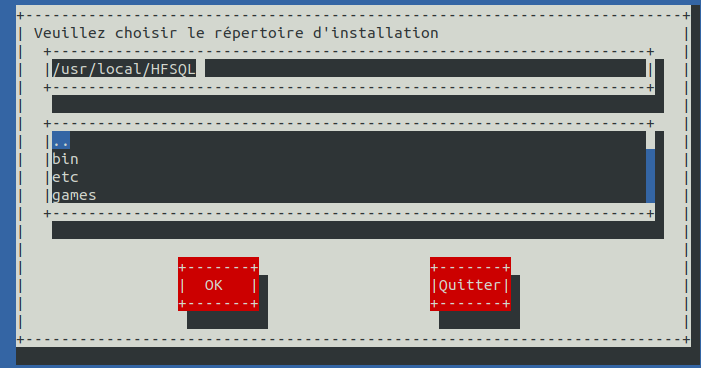
chmod +x manta\_install64

Si on a le message d’erreur **Error opening terminal: xterm-256color** il faut exécuter la commande :

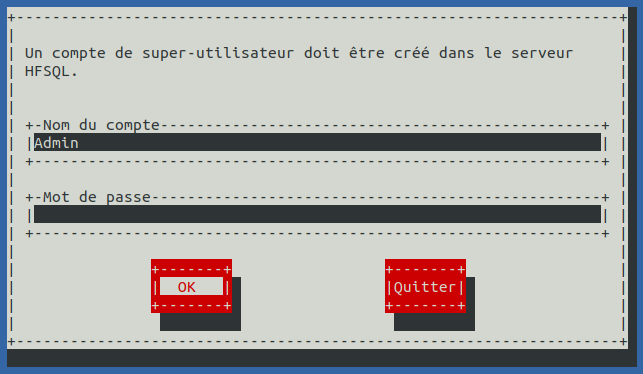
export TERM=xterm

./manta\_install64

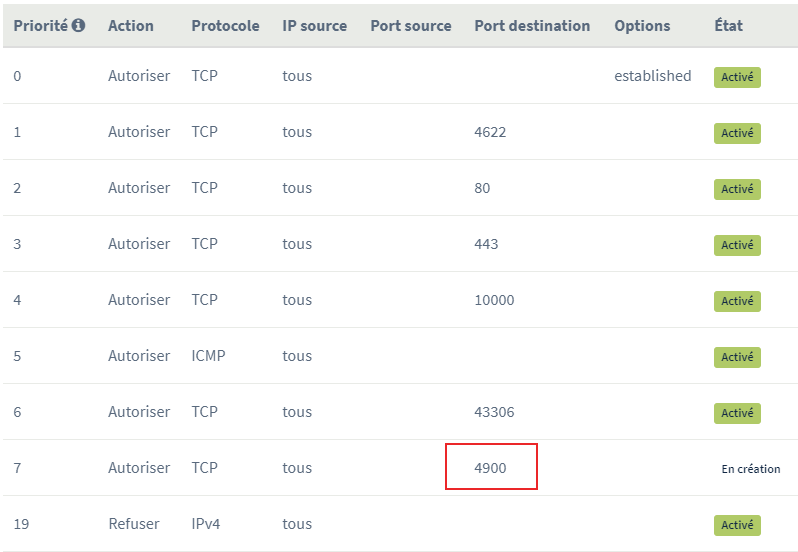








## Ouverture d’une règle dans le Firewall



# Troubleshooting

## Redémarrer le server