

Watchdog v2.x

Manuel d'installation



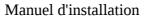




Table des matières

1Pré-requis à l'installation sous « Mandriva »	
1.1Création du user sur « Server »	
1.2Création du user sur « Client »	
1.3Installation du server MySQL	
1.4Installation du TTS Espeak	
1.5Installation de MbrOLA	
1.6Création de l'autorité de certification et du certificat server	
2Installation « from scratch »	8
2.1Installation des paquetages	8
2.2Compilation des sources	
3Installation « from RPMs »	
4Préparation d'un nouveau client	10
5Lancement du logiciel serveur	
6Lancement du logiciel client	
7Liens/Contacts	





1 Pré-requis à l'installation sous « Mandriva »

Ce chapitre décrit le processus à suivre pour installer, préparer et configurer les logiciels détaillés ci dessus selon deux méthodes :

- From Scratch : Compilation des sources
- From RPMs : Installation directement packagée.

Nous considérons qu'une machine « Server » est installée avec la dernière version disponible de « Mandriva », et correctement configurée, notamment concernant les déclarations des dépots RPM.

1.1 Conventions

- Les caractères de style « gras » sont les commandes/informations que l'administrateur doit entrer au clavier. Les commandes sont à passer telles que décrites dans ce document. Les informations sont à adapter aux besoins et désirs de l'administrateur.
- Les caractères de style « root@Server » sont les réponses ou attente des machines ou postes de travail.
- Les mots de passe utilisés en clair dans ce document sont à remplacer par des mots de passe robustes choisis par l'administrateur.





1.2 Création du user sur « Server »

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

```
[root@Server ~]# useradd -m -r -d /var/WatchdogHome watchdog
[root@Server ~]# passwd watchdog
```

Entrez alors le nouveau mot de passe de connexion de l'utilisateur « watchdog ».

1.3 Création du user sur « Client »

L'installation utilise une configuration pour un user « watchdoguser ». Bien sûr, n'importe quel utilisateur standard de la machine pourra être utilisé en lieu en place.

Sur la machine « Client », lancez en tant que « root », les commandes suivantes :

```
[root@Client root]# useradd watchdoguser
[root@Client root]# passwd watchdoguser
```

Entrez alors le nouveau mot de passe de connexion de l'utilisateur « watchdoguser ».





1.4 Installation du server MySQL

Par défaut, le serveur de base de données est installé sur la même machine que le serveur Watchdog. Il peut cependant être déporté sur n'importe quelle autre machine.

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

```
[root@Server ~]# urpmi mysql
[root@Server ~]# /etc/init.d/mysqld start
[root@Server ~]# /usr/bin/mysql_secure_installation
Enter current password for root (enter for none): (enter)
Set root password? [Y/n] Y
New password: changeit
Re-enter new password : changeit
Remove anonymous users? [Y/n] Y
Disallow root login remotely? [Y/n] Y
Remove test database and access to it? [Y/n] Y
Reload privilege tables now? [Y/n] Y
[root@Server ~]# /usr/bin/mysqladmin -u root -p create WatchdogDB
Enter password: changeit
[root@Server ~]# mysql -u root -p WatchdogDB
Enter password: changeit
Welcome to the MySQL monitor. Commands end with; or \g.
mysql> CREATE USER 'watchdog' IDENTIFIED BY 'seb';
```





Sébastien LEFEVRE Bruno LEFEVRE

Query OK, 0 rows affected (0.00 sec)

mysql> GRANT CREATE, SELECT, INSERT, UPDATE, DELETE, EVENT ON WatchdogDB.* TO
'watchdog';

mysql> exit





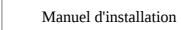
1.5 Installation du TTS Espeak

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

[root@Server ~]# urpmi espeak

Répetez l'opérations sur la machine « Cliente ».







1.6 Installation de MbrOLA

Attention, ce logiciel de synthèse vocale n'est pas sous licence GPL. Les sources et binaires ne sont donc pas fournies par « Watchdog », et vous devrez vous même allez les chercher sur le site internet dédié.

Allez sur le site http://tcts.fpms.ac.be/synthesis/ et télécharger les binaires et les voix françaises fr1 à fr7.

Copiez, sur la machine « Server », en tant que « watchdog », les fichiers « frX » dans le répertoire HOME. Puis adaptez les droits des fichiers en conséquence

[watchdog@Server ~] \$ chmod -R 755 fr*

Copiez, sur la machine « Server », en tant que « root », le fichier binaire MBROLA-i386 dans le répertoire « /usr/local/bin », et adaptez les droits en conséquence

[root@Server /usr/local/bin]# chmod 755 mbrola-linux-i386

Répetez l'opération sur la machine « Client », en utilisant le répertoire ~/.watchdog pour stocker les fichiers « frx »





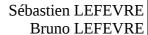
1.7 Création de l'autorité de certification et du certificat server

L'outil nécessite une autorité de certification pour signer les certificats de chiffrements et d'authentification. Si vous n'en disposez pas, voici une méthode pour en créer une.

Sur la machine « Server », lancez en tant que « watchdog », les commandes suivantes :

```
[watchdog@Server ~]$ openssl req -newkey rsa:2048 -nodes -x509 -days 3650
-keyout cakey.pem -out cacert.pem
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) [Default Province]: IDF
Locality Name (eg, city) [Default City]: CROSNE
Organization Name (eg, company) [Default Company Ltd]:WatchdogTest
Organizational Unit Name (eg, section) []:
Common Name (eq, your name or your server's hostname) []: WatchdogTest CA
Email Address []:
[watchdog@Server ~] $ openssl req -newkey rsa:2048 -nodes -days 3650 -keyout
serveurkey.pem -out serveurcert.req
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) [Default Province]: CROSNE
Locality Name (eg, city) [Default City]: CROSNE
Organization Name (eq, company) [Default Company Ltd]:WatchdogTest
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Certificat test serveur
Watchdog
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```







An optional company name []:

```
[watchdog@Server ~]$ mkdir newcerts
[watchdog@Server ~]$ touch index.txt
[watchdog@Server ~]$ echo "01" > serial
[watchdog@Server ~]$ openssl ca -config /usr/share/Watchdog/openssl.cnf -in serveurcert.req -out serveursigne.pem
...
Certificate is to be certified until Feb 8 16:31:43 2021 GMT (3650 days)
Sign the certificate? [y/n]: Y

1 out of 1 certificate requests certified, commit? [y/n] Y
Write out database with 1 new entries
Data Base Updated
[watchdog@Server ~]$
```





2 Installation « from scratch »

2.1 Installation des paquetages

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

```
[root@Server ~]# urpmi autoconf automake make libtool
[root@Server ~]# urpmi bison flex

[root@Server ~]# urpmi gcc gcc-c++
[root@Server ~]# urpmi glib2-devel libgnomeui2-devel
[root@Server ~]# urpmi gtksourceview-devel
[root@Server ~]# urpmi goocanvas-devel
[root@Server ~]# urpmi nut-devel mysql-devel
[root@Server ~]# urpmi gnokii-devel
[root@Server ~]# urpmi gtkdatabox-devel ungif4-devel
[root@Server ~]# urpmi liblirc-devel libcurl-devel libgif-devel
```



2.2 Compilation des sources

La procédure d'installation et compilation des sources est la même pour la machine « Server » et la machine « Client ».

Connectez vous à la machine « Server », en tant que user « watchdog ».

Télécharger les sources du logiciel, en SVN, et installer le logiciel via les commandes suivantes :

[watchdog@Server ~] \$ svn co svn://seblef.dyndns.org/branches-2.x/ SRC

[watchdog@Server ~] \$ cd SRC

[watchdog@Server ~] \$ aclocal; libtoolize; autoheader; autoconf; automake --add-

missing

[watchdog@Server ~]\$./configure

[watchdog@Server ~]\$ su

Password: (entrez le mot de passe root)

[root@Server WatchdogHome]# make install

[root@Server WatchdogHome]# exit

Répétez la procédure sur la machine « Client ».



2.3 Définition du schéma de base de données

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

[root@Server ~]# mysql -u root -p WatchdogDB
Enter password: changeit
Welcome to the MySQL monitor. Commands end with ; or \g.
mysql> source init_db.sql
mysql> exit



3 Installation « from RPMs »

Télécharger les RPMs du logiciel « common » et « server », et sur la machine « Server », lancez en tant que « root », les commandes suivantes:

```
[root@Server ~]# urpmi Watchdog-common-2.6.xx-1.i586.rpm
[root@Server ~]# urpmi Watchdog-server-2.6.xx-1.i586.rpm
```

Remplacer le « x » par le numéro de version en cours.

Au besoin, complétez par les commandes suivantes :

```
[root@Server ~]# urpmi Watchdog-server-tellstick-2.6.xx-1.i586.rpm
[root@Server ~]# urpmi Watchdog-server-lirc-2.6.xx-1.i586.rpm
```

Télécharger les RPMs du logiciel « client », et sur la machine « Client », lancez en tant que « root », les commandes suivantes:

```
[root@Client ~]# urpmi Watchdog-common-2.6.xx-1.i586.rpm
[root@Client ~]# urpmi Watchdog-client-2.6.xx-1.i586.rpm
```

3.1 Définition du schéma de base de données

Sur la machine « Server », lancez en tant que « root », les commandes suivantes:

```
[root@Server ~]# mysql -u root -p WatchdogDB
Enter password: changeit
Welcome to the MySQL monitor. Commands end with ; or \g.
mysql> source /usr/share/Watchdog/init_db.sql
4  mysql> exit
```





5 Préparation d'un nouveau client

Sur la machine « Client », lancez en tant que « watchdoguser », les commandes suivantes :

[watchdoguser@Client ~]\$ mkdir .watchdog; cd .watchdog
[watchdoguser@Client .watchdog]\$ openssl req -newkey rsa:2048 -nodes -days 3650
-keyout clientkey.pem -out clientcert.req

Déplacer le fichier « clientcert.req » sur la machine « Server », dans le répertoire home de l'utilisateur « watchdog ».

[watchdoguser@Client .watchdog]\$ scp clientcert.req watchdog@Server:
watchdog@Server's password:
clientcert.req 100% 1001 1.0KB/s 00:00

Sur la machine « Server », lancez en tant que « watchdog », les commandes suivantes :

[watchdog@Server ~]\$ openssl ca -config /usr/share/Watchdog/openssl.cnf -in clientcert.req -out clientsigne.pem

Certificate is to be certified until Feb $8\ 17:53:01\ 2021\ GMT\ (3650\ days)$ Sign the certificate? [y/n]:Y

1 out of 1 certificate requests certified, commit? [y/n]Y
Write out database with 1 new entries
Data Base Updated

Déplacer le fichier « clientsigne.pem » sur la machine « Client », dans le répertoire « .watchdog » de l'utilisateur « watchdoguser ».

[watchdog@localhost ~]\$ scp clientsigne.pem watchdoguser@Client:.watchdog/





Sébastien LEFEVRE Bruno LEFEVRE

 $watch dog user @Client's \ password:\\$

clientsigne.pem 100% 4427 4.3KB/s 00:00

Faites de même avec le certificat de l'autorité de certification.

[watchdog@localhost ~]\$ scp cacert.pem watchdoguser@Client:.watchdog/
watchdoguser@Client's password:

cacert.pem 100% 4427 4.3KB/s 00:00





6 Configuration du logicier « Server »

Sur la machine « Server », editez en tant que « root » le fichier de configuration « /etc/watchdogd.conf » en y précisant vos paramètres personnels :

[root@Server ~]# vi /etc/watchdogd.conf

[DEBUG]

debug_SIGNAUX = true

debug DB = true

debug CONFIG = true

debug USER = true

debug_CRYPT0 = true

 $debug_INF0 = true$

debug_SERVEUR = true

debug_CDG = true

debug NETWORK = true

debug_ARCHIVE = true

debug_CONNEXION = true

 $debug_DLS = true$

debug_MODBUS = true

debug_ADMIN = true

 $debug_RS485 = true$

 $debug_ONDULEUR = true$

debug SMS = true

debug_AUDI0 = true

debug CAMERA = true

debug_COURBE = true

debug_TELLSTICK = true

debug_LIRC = true

debug_ASTERISK = true





[GLOBAL]

home = /var/WatchdogHome

db_host = localhost

db_port = 3306

db_database = WatchdogDB
db_password = changeit
db_username = Watchdog

[SERVER]

taille_clef_dh = 64

min_serveur = 1

 $max_serveur = 2$

max inactivite = 86400

[RS485]

port_rs485 = /dev/watchdog_RS485

[SMS]

smsbox_user = smboxuser

smsbox_passwd = smsboxpasswd

 $sms_telephone = 0123456789$

 $min_m = 9000$

 $max_m = 9099$

[TELLSTICK]

 $min_a = 1$

 $max_a = 10$

[ASTERISK]

min m = 9100

 $max_m = 9199$





Sébastien LEFEVRE Bruno LEFEVRE

Remplacez les arguments par défaut par vos propres paramètres





7 Lancement du logiciel serveur

Lors du tout premier lancement, sur la machine « Server », lancez en tant que « watchdog », les commandes suivantes :

[watchdog@Server ~]\$ Watchdogd --initrsa

Sur la machine « Server », lancez en tant que « watchdog », les commandes suivantes :

[watchdog@Server ~]\$ Watchdogd

Puis configurer un mot de passe administrateur Watchdog :

[watchdog@Server ~]\$ WatchdogdAdmin

-- WatchdogdAdmin v2.6.1163

Watchdogd 2.6.xx on server

#Watchdogd*CLI> setrootpasswd changerootpasswdWatchdog

#Watchdogd*CLI> quit

[watchdog@Server ~]\$





8 Lancement du logiciel client

Sur la machine « Client », lancez en tant que « watchdoguser », la commande suivante :

[watchdoguser@Client ~]\$ Watchdog-client





9 Liens/Contacts

Les différentes personnes ayant contribué au projet sont :

- Bruno LEFEVRE < bruno LEFEVRE < <a href="mailto:bruno.lefevre1953@gmailto:bruno.lefevr
 - Architecture Technique, Module de contrôle/commande, Logistique, Programmation D.L.S, Beta-testeur Watchdog.
- Sébastien LEFEVRE < lefevre.seb@gmail.com >
 - Développeur, Programmation D.L.S, Bêta-testeur Watchdog

Les sources du logiciel peuvent être téléchargées sur les sites internets suivants :

Format Web : http://seblef.dyndns.org/

Format RPM : http://seblef.dyndns.org/

Format SVN: svn://seblef.dyndns.org/branches-2.x/

