

Sommaire

| | |
|--|----------|
| Serveur de messagerie instantanée Jabber..... | 1 |
| Introduction :..... | 1 |
| Matériel requis :..... | 1 |
| Installation à partir des sources :..... | 2 |
| Configuration :..... | 3 |
| Installation simplifiée :..... | 5 |
| Démarrage/Arrêt du serveur :..... | 5 |
| Passerelles :..... | 6 |
| Intranet :..... | 7 |

Serveur de messagerie instantanée Jabber

Serveur de messagerie instantanée Jabber
par Laurent DUBETTIER–GRENIER
Installation d'un serveur de messagerie instantanée Jabber

Introduction :

Cet article est une variante de l'article original paru dans le numéro 25 (Août 2003), du magazine Planète–Linux.

Jabber est un protocole de communication XML développé sous l'égide de la Jabber Software Foundation. Un protocole, c'est un "langage" particulier permettant à des ordinateurs de communiquer entre eux... Jabber est plus particulièrement développé pour la messagerie instantanée, et c'est un protocole libre (licence GPL/JOSL). Comme ses principaux concurrents privés (AIM, ICQ, MSN, Yahoo), il permet de connaître et de faire connaître votre état de présence sur le réseau Internet et d'envoyer ou de recevoir des messages instantanément. Si vous n'êtes pas connecté, vos messages sont stockés et distribués dès que vous revenez en ligne.

L'intérêt de Jabber ? il y en a plusieurs. Le protocole Jabber est libre, public, ouvert et basé sur un langage connu (XML), gage de pérennité et de développement futur. Il est et restera non payant. Il permet donc de créer des serveurs extensibles (ajout d'une brique au serveur), décentralisés (création de son propre serveur) et sûr (sans espion logiciel, avec cryptage SSL). Il n'est par contre pas nativement multi-protocole, mais des passerelles vers les autres services de messagerie instantanée existent, à installer en complément du serveur de base.

Outre le serveur de messagerie instantanée Jabber, il existe de nombreux autres serveurs utilisant le protocole Jabber. WPJabber est une alternative libre à Jabber, tandis que le site <http://www.jabber.com> diffuse un des nombreux serveurs sous licence payante et propriétaire. Un bref comparatif des serveurs existant est disponible [ici](#). Le choix est donc vaste et devrait permettre de couvrir vos besoins : de Windows à Solaris, en passant par OS X, intégrable avec une base de données MySQL, Oracle ou LDAP, vous trouverez forcément une version publique ou commerciale du serveur Jabber qui vous conviendra.

Enfin, pour se connecter à votre serveur, une multitude de clients existent, en licence libre ou propriétaire : on peut citer Gabber, Gaim et Psi sous Linux, Exodus sous Windows.

L'article qui suit devrait vous permettre d'installer un serveur de messagerie instantanée Jabber (version 1.4.2), soit à partir des sources, soit à partir des paquetages rpm, sur un serveur Mandrake 9.1. Mais le principe est identique pour toute distribution. Le hostname du serveur sera jabber.masociete.com et l'adresse IP 192.168.0.1.

Matériel requis :

Le matériel requis dépend du nombre de personnes qui vont se connecter à votre serveur : un système Linux équipé d'un processeur de type Pentium avec 512 Mo de Ram peut supporter de 100 à 1000 utilisateurs, avec un taux de charge maximum de 50%. La bande passante nécessaire est de 15 bits par seconde par utilisateur connecté... Attention, sans recompilation, Linux n'accepte pas plus de 1024 connexions simultanées...

Installation à partir des sources :

Se logger comme root.

Récupérer la source du serveur Jabberd à l'adresse suivante :
<http://jabberd.jabberstudio.org/downloads/jabber-1.4.2.tar.gz>
et la copier dans le répertoire /usr/local

Décompresser le fichier source :

```
# tar zxvf jabber-1.4.2.tar.gz  
Renommer le répertoire jabber-1.4.2 :
```

```
# mv jabber-1.4.2 jabber  
Récupérer le code source de openssl (openssl-0.9.7b.tar.gz) à l'adresse suivante : http://www.openssl.org. Et  
la copier dans le répertoire /usr/local. Décompresser le fichier source :
```

```
# tar zxvf openssl-0.9.7b.tar.gz  
Renommer le répertoire openssl-0.9.7b :
```

```
# mv openssl-0.9.7b ssl  
Changer de répertoire :
```

```
cd ssl  
Compiler openssl (Perl5 doit notamment être installé) :
```

```
# ./config  
# make  
# make test  
# make install  
Changer de répertoire :
```

```
cd /usr/local/jabber  
Installer le serveur jabber, avec prise en charge du cryptage de la connexion ssl :
```

```
$ ./configure --enable-ssl 1>sortie.txt 2>&1  
Vérifier que ssl a bien été pris en compte. Les premières lignes du fichier sortie.txt doivent contenir :
```

```
Running Jabber Configure  
Searching for SSL... Found.
```

Une erreur existe dans le fichier résultant platform-settings, qu'il faut corriger. Editer le fichier avec vi par exemple :

```
$ vi platform-settings  
Repérer la ligne :
```

```
CFLAGS=-I/usr/local/ssl/include/openssl -DHAVE_SSL  
Et la transformer en :
```

```
CFLAGS=-I/usr/local/ssl/include/openssl -I/usr/local/ssl/include -DHAVE_SSL  
Faire la même modification pour la ligne CCFLAGS. Taper alors :
```

\$ make

Et c'est terminé, votre serveur de messagerie instantanée est installé (enfin presque...) !

Configuration :

L'essentiel de la configuration du serveur s'effectue en intervenant sur le fichier /usr/local/jabber/jabber.xml (ou /etc/jabber/jabber.xml si vous avez utilisé un paquet Mandrake). Avant toute modification, il est judicieux de faire une copie de secours du fichier original

NB : le fichier jabber.xml étant au format XML, la mise en commentaire est réalisée en utilisant des balises : (balise fermante), comme en HTML

Ouvrir le fichier jabber.xml et modifier la ligne :

```
<host> <jabberd:cmdline flag="h">localhost</jabberd:cmdline> </host>
```

en remplaçant localhost par votre nom de domaine (jabber.masociete.com par exemple), ou par l'adresse IP de votre serveur Jabber (déconseillé). Si vous créer un serveur jabber interne, sans lien avec internet, vous pouvez commenter cette ligne :

```
<update> <jabberd:cmdline flag="h">localhost</jabberd:cmdline> </update>
```

C'est la commande permettant de contrôler automatiquement la présence de mise à jour sur le serveur jabber.org. Configurer alors le répertoire destiné à stocker les fichiers de profils des utilisateurs :

```
mkdir -p /usr/local/jabber/spool/jabber.masociete.com
```

en remplaçant jabber.masociete.com par le nom que vous avez indiqué ci-dessus à la place de localhost dans la balise <host> du fichier jabber.xml. Démarrez Jabber et tester son fonctionnement sans cryptage ssl (voir rubrique [#demarrer-arreter Démarrer/Arrêter le serveur]). Si tout fonctionne normalement, on peut passer à la suite.

Il faut maintenant créer la clé de cryptage SSL. Rester dans le répertoire /usr/local/jabber et repérer l'emplacement de l'exécutable openssl :

```
which openssl
```

Il réside normalement dans le répertoire /usr/bin/openssl. C'est ce chemin qui devra figurer dans la première ligne du fichier keygen.sh.

Créer un fichier keygen.sh :

```
$ vi keygen.sh
```

et taper le code suivant :

```
#!/bin/sh
## régler le chemin ci desous sur le chemin de openssl
OPENSSL=/usr/bin/openssl
## Génération du certificat et de la clé
$OPENSSL req -new -x509 -newkey rsa:1024 -keyout privkey.pem -out key.pem
## effacement de la phrase servant de mot de passe
$OPENSSL rsa -in privkey.pem -out privkey.pem
## Assemblage
cat privkey.pem >> key.pem
## Effacement
rm privkey.pem
```

Reseau-message-jabber

Enregistrer et rendre exécutable ce fichier :

```
chmod u+x keygen.sh
```

Exécuter ce fichier :

```
./keygen.sh
```

Répondre aux questions posées. A la fin de l'exécution, vous devez trouver dans le répertoire /usr/local/jabber un fichier key.pem. Tester alors le mode ssl :

```
openssl s_client -connect 192.168.0.1:5223
```

en remplaçant 192.168.0.1 par l'adresse ip de votre serveur. Vous devez recevoir une réponse du type :

```
CONNECTED(00000003)
```

```
depth=0 /C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email address
```

```
verify error:num=18:self signed certificate
```

```
verify return:1
```

```
depth=0 /C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email address
```

```
verify return:1
```

```
-----
```

```
Certificate chain
```

```
0 s:/C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email address
```

```
i:/C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email address
```

```
-----
```

```
Server certificate
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIDdDCCAt2gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBI TELMAkGA1UEBhMCVVMx
EDAObgNVBAgTB0FyaXpvbmExEDAOBgNVBAcTB1Bob2VuaXgxETAPBgNVBAoTTCERJ
TEExJR0FGMQ8wDQYDVQQLEwZKYWJiZXIxFzAVBgNVBAMTDkNocmlzIE1jRG9uYWxk
MRkwFwYJKoZIhvcNAQkBFgpwaHgtamFiYmVyMB4XDTAxMDYwNjAxNTMwNloXDTAx
MDcwNjAxNTMwNlowgYkxCzAJBgNVBAYTAiVTMRAwDgYDVQQIEwdBcml6b25hMRAw
DgYDVQQHEwdQaG9lbml4MREwDwYDVQQKEwhESUxMSUdBRjEPMA0GA1UECxMGSmFi
YmVyMRcwFQYDVQQDEw5DaHJpcyBNY0RvbmFsZDEZMBCGCSqGSIb3DQEJARYKcGh4
LWphYmJlcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArybyosgyf9VNpPZc
+nU6yKdfAsOSpBu/n/MkChis5POuLkXo62WEoiYuDYF6bmd6XYaVC7ZwIteCwTiv
OqdErh4u82E2qeArN0j9eq6EX+MMrYBSkv2nzwabNkkWPCS9VaOsVWx+kvRw598p
ACyANf52liFhfDGISIoTIBOn+ysCAwEAaAOb6TCB5jAdBgNVHQ4EFgQUv9mxa1Yj
o7Um9ZK0OSW0phiG23AwgbYGA1UdIwSBrijCBq4AUv9mxa1Yjo7Um9ZK0OSW0phiG
23ChgY+kgYwwgYkxCzAJBgNVBAYTAiVTMRAwDgYDVQQIEwdBcml6b25hMRAwDgYD
VQQHEwdQaG9lbml4MREwDwYDVQQKEwhESUxMSUdBRjEPMA0GA1UECxMGSmFiYmVy
MRcwFQYDVQQDEw5DaHJpcyBNY0RvbmFsZDEZMBCGCSqGSIb3DQEJARYKcGh4LWph
YmJlcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArybyosgyf9VNpPZc+nU6y
KdfAsOSpBu/n/MkChis5POuLkXo62WEoiYuDYF6bmd6XYaVC7ZwIteCwTivOqdErh
4u82E2qeArN0j9eq6EX+MMrYBSkv2nzwabNkkWPCS9VaOsVWx+kvRw598pKoQY9OK
bV4NnkxDM8lxCjvIvGvrbvnr
```

```
-----END CERTIFICATE-----
```

```
subject=/C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email address
```

```
issuer=/C=FR/ST=FRANCE/L=Departement/O=organization/OU=Jabber/CN=contact name/Email=email
```

Configuration :

Reseau-message-jabber

address

No client certificate CA names sent

SSL handshake has read 1042 bytes and written 320 bytes

New, TLSv1/SSLv3, Cipher is DES-CBC3-SHA

Server public key is 1024 bit

SSL-Session:

Protocol : TLSv1

Cipher : DES-CBC3-SHA

Session-ID: A23C1FB04F635EC09F92CBD722DAB8BB1503B54D4A0E9C61B3708CB33D6ED372

Session-ID-ctx:

Master-Key:

C8C25C17D5B4312E1440DBC956FF5738829C50E16E8E704010B84B1A8D33C405995D8B7FB02E06988890C7E

Key-Arg : None

Start Time: 991792771

Timeout : 300 (sec)

Verify return code: 0 (ok)

Ouvrir le fichier /usr/local/jabber/jabber.xml et valider la prise en charge du mode SSL en repérant la ligne :

```
<ip port='5222'/>
```

et en ajoutant la ligne suivante à la suite :

```
<ssl port='5223'>192.168.0.1</ssl>
```

De même, repérer la ligne :

```
<ssl> /usr/local/jabber/key.pem </ssl>
```

Redémarrez le serveur et tester avec cryptage ssl (voir rubrique [#demarrer-arreter Démarrer/Arrêter le serveur]).

Installation simplifiée :

Si compiler les sources vous paraît trop compliqué, sous Mandrake 9.1 et KDE 3.1, il suffit d'utiliser l'interface graphique (Configuration / Paquetages / Installer des logiciels). Le paquetage actuel est jabber-1.4.2a-6mdk.i586.rpm. Le fichier principal de configuration est alors /etc/jabber/jabber.xml. Les seules modifications à effectuer sont celles indiquées ci-dessus concernant ce fichier. La clé SSL est générée automatiquement.

Démarrage/Arrêt du serveur :

Si vous avez installé Jabber depuis les sources (fichier tar.gz), pour démarrez le serveur, tapez :

```
# ./usr/local/jabberd/jabberd
```

Il y a un mode debug :

```
# ./usr/local/jabber/jabberd/jabberd -D
```

Si vous avez installé Jabber à partir du fichier rpm, pour démarrer/arrêter/redémarrer, votre serveur Jabber, tapez :

Installation simplifiée :

Reseau-message-jabber

service jabber start/stop/restart
et le mode "debug" (option -D) :

```
# service jabber stop
# /usr/sbin/jabberd -h jabber.masociete.com -c /etc/jabber/jabber.xml -B -D
Pour vérifier que le serveur Jabber est effectivement en service, tapez :
```

```
ps ax | grep jabber
Vous devez obtenir un résultat ressemblant aux deux lignes suivantes :
```

```
3052 ? S 0:00 /usr/sbin/jabberd -h jabber.masociete.com -c /etc/jabber/jabber.xml -B
> 3053 ? S 0:00 /usr/sbin/jabberd -h jabber.masociete.com -c /etc/jabber/jabber.xml -B
où jabber.masociete.com est remplacé par le hostname de votre serveur.
```

Le serveur jabber utilise les ports 5222 (connexion normale avec le client), 5223 (connexion sécurisée avec le client) et 5269 (connexion entre serveurs). En tapant :

```
netstat -an | grep -E '5222'
vous devez obtenir la ligne suivante, qui vous indique que le serveur Jabber écoute le port 5222 :
```

```
tcp 0 0 0.0.0.0:5222 0.0.0.0:* LISTEN
De même pour 5223 et 5269.
```

Pour gérer le démarrage, vous pouvez utiliser chkconfig :

```
# chkconfig --list | less # liste des services démarrés
# chkconfig --add jabber # ajouter jabber à la liste des services
# chkconfig jabber off # inhibition du démarrage automatique
# chkconfig jabber on # démarrage automatique au démarrage
```

Passerelles :

Il existe plusieurs briques additionnelles au serveur jabber de base : mu-conference (conférence multi-utilisateurs), jud (Jabber User Directory : répertoire des utilisateurs), et les passerelles pour les utilisateurs de AIM, ICQ, MSN et Yahoo.

Les paquetages sont distribués avec la Mandrake 9.1, et peuvent donc être installés facilement (Configuration / Paquetages / Installer des logiciels).

Il faut ensuite les déclarer dans le fichier jabber.xml : c'est généralement expliqué dans le fichier README du paquetage (pour savoir où il est : rpm -ql nom_du_paquetage) et le fichier jabber.xml est abondamment commenté.

L'exemple suivant s'applique au paquetage jabber-jud. Une fois le paquetage installé, il existe un fichier jud.so dans le répertoire /usr/lib/jabber/jud

Pour activer ce service, il faut insérer les lignes suivantes dans le fichier jabber.xml, dans la zone où sont défini les services :

```
<service id="jud">
<host>jud.monserveurjabber</host>
<load><jud>./jud/jud.so</jud></load>
<jud xmlns="jabber:config:jud">
<vcard>
```

Reseau-message-jabber

```
<fn>Annuaire des utilisateurs locaux</fn>
<desc>Ce service est un annuaire des utilisateurs locaux</desc>
<url></url>
</vcard>
</jud>
</service>
```

Et à la place du jud existant, qui déclare l'annuaire du serveur jabber.org (users.jabber.org), dans la zone <browse> :

```
<service type="jud" jid="jud.monserveurjabber" name="Annuaire des utilisateurs locaux">
<ns>jabber:iq:search</ns>
<ns>jabber:iq:register</ns>
</service>
```

Redémarrez jabber : le service d'annuaire devrait maintenant exister.

Depuis Gabber, il faut choisir Actions/Consultations des agents IM pour s'inscrire dans l'annuaire des utilisateurs locaux de jabber.masociete.com

Liste des extensions serveurs :

- Conférence multi-utilisateurs : <http://mu-conference.jabberstudio.org/>
- JUD (Jabber User Directory) : <http://download.jabber.org/dists/1.4/final/>
- Passerelle AIM : <http://aim-transport.jabberstudio.org/>
- Passerelle ICQ : <http://icq7-t.sourceforge.net/>
- Passerelle MSN : <http://msn-transport.jabberstudio.org/>
- Passerelle Yahoo : <http://yahoo-transport.jabberstudio.org/>

Intranet :

Pour une utilisation en Intranet, sans communication avec l'extérieur, il faut réaliser les opérations suivantes :

- Interdire la communication entre serveurs : pour cela, fermer le port 5269 du firewall de votre organisation.
- Interdire la communication avec les clients extérieurs : fermer les ports 5222 et 5223 du firewall de votre passerelle internet.
- Commenter les sections <service id="dnsrv">