Asterisk : Installation

est un PBX (Private Branch Exchange) est un système de gestion téléphonique sous double licence **GNU GPLv2 et propriétaire**.
Il permet, entre autres, la messagerie vocale, les files d'attentes, les agents d'appels, les musiques d'attentes et les mises en garde d'appels, la distribution des appels.
Il est possible également d'ajouter l'utilisation des conférences par le biais de l'installation de modules supplémentaires.

Je vais vous montrer comment j'installe Asterisk à partir des dépôts sur Centos et parce que je ne suis pas expert en VOIP, mais je me débrouille avec l'interface FreePBX, je vous monterai aussi l'installation de FreePBX.

Installation de centos

D'abord, récupérer l'image ISO de CentOS 6
Pas besoin de dessin, installé CentOS
Pourquoi installer ça sur CentOS, car vous avez des modules commerciaux que vous pourrez rajouter.
Personnellement, je ne me suis jamais servi de ces modules.
URL: dépôt centos pour la netinstall (à entrer dans le menu d'installation)
http://mirror.centos.org/centos-6/6/os/ et i386 ou x86_64

Installation d'asterisk

Votre serveur Centos est prêt, nous allons mettre les dépôts en place. On va ajouter dans les dépôts de notre installation, des dépôts supplémentaires FreePBX, Asterisk et digium

schmooze commercial

Cela, représente les addons de FreePBX

```
vim /etc/yum.repos.d/schmooze-commercial.repo
```

Ajouté cela

```
#Schmooze Commercial Packages
[schmooze-commercial]
name=schmooze-commercial
mirrorlist=http://mirrorlist.schmoozecom.net/?release=$releasever&arch=$basearch&repo=schmooze-commercial
#baseurl=http://yum.schmoozecom.net/schmooze-commercial/$releasever/arch=$basearch/
gpgcheck=0
enabled=1
```

Récupérer le reste digium et asterisk, placer les fichiers dans `/etc/yum.repos.d`.

Si cela est bien fait vous devez obtenir ceux-ci :
Résultat d'une commande `ls -l` dans le répertoire `/etc/yum.repos.d`

```
 -rw-r--r--. 1 root root  208 14 nov.  11:47 centos-asterisk-10.repo
 -rw-r--r--. 1 root root  238 14 nov.  11:47 centos-asterisk-11-
certified.repo
 -rw-r--r--  1 root root  208 20 nov.  15:20 centos-asterisk-11.repo
 -rw-r--r--. 1 root root  208 11 nov.  15:01 centos-asterisk-12.repo
 -rw-r--r--. 1 root root  238 14 nov.  11:47 centos-asterisk-13-
certified.repo
 -rw-r--r--. 1 root root  208 11 nov.  15:01 centos-asterisk-13.repo
 -rw-r--r--. 1 root root  424 11 nov.  15:01 centos-asterisk.repo
 -rw-r--r--. 1 root root 1991 23 oct.  13:41 CentOS-Base.repo
 -rw-r--r--. 1 root root  647 23 oct.  13:41 CentOS-Debuginfo.repo
 -rw-r--r--. 1 root root  198 14 nov.  11:48 centos-digium-10.repo
 -rw-r--r--. 1 root root  228 14 nov.  11:48 centos-digium-11-certified.repo
 -rw-r--r--  1 root root  198 20 nov.  15:20 centos-digium-11.repo
 -rw-r--r--. 1 root root  198 11 nov.  15:01 centos-digium-12.repo
 -rw-r--r--. 1 root root  228 14 nov.  11:48 centos-digium-13-certified.repo
 -rw-r--r--. 1 root root  198 11 nov.  15:01 centos-digium-13.repo
 -rw-r--r--. 1 root root  408 11 nov.  15:01 centos-digium.repo
 -rw-r--r--. 1 root root  289 23 oct.  13:41 CentOS-fasttrack.repo
 -rw-r--r--. 1 root root  630 23 oct.  13:41 CentOS-Media.repo
 -rw-r--r--. 1 root root 5394 23 oct.  13:41 CentOS-Vault.repo
 -rw-r--r--. 1 root root  287 14 janv.  2013 schmooze-commercial.repo
```

Après, on met à jour le cache

```
 yum makecache
```

Puis, on peut installer Asterisk version 11:

installation d'asterisk 11

```
 yum install asterisk asterisk-configs asterisk-odbc asterisk-doc asterisk-
res_digium_phone asterisk-sounds-core-en-ulaw asterisk-sounds-core-fr-ulaw
asterisk-sounds-core-fr-alaw asterisk-sounds-core-fr-g722 asterisk-sounds-
core-fr-gsm asterisk-sounds-moh-opsound-ulaw --enablerepo=asterisk-11
```

si vous voulez la dernière version au lieu de mettre `–enablerepo=asterisk-11` mettre `–enablerepo=asterisk-13`

Les versions de FreePBX ne sont pas toutes compatible avec les dernières versions de FreePBX gardez ce tableau en tête :

FreePBX Version	status	Asterisk Version
2.11	Stable	* 1.8 * 10 * 11
12.0	Stable	* 1.8 * 10 * 11 * 12
13	Pre-alpha	* 10 * 11 * 12 * 13

Désactivé le lancement du service asterisk

```
chkconfig --del asterisk
```

Puis, on installe DAHDI (Digium Asterisk Hardware Device Interface) qui est un composant lié à Asterisk pour gérer la communication entre Asterisk et les différents types de cartes physiques que vous pouvez connecter à votre serveur.

```
yum install dahdi-linux dahdi-tools libpri
```

Installation de FreePBX

FreePBX est une interface web open source GUI (graphical user interface) qui permet de contrôler et administré Asterisk.

D'abord, désactiver (Security-Enhanced Linux), abrégé SELinux, est un module de sécurité LSM (Linux security module), qui permet de définir une politique de contrôle d'accès obligatoire aux éléments d'un système issu de Linux.

```
vim /etc/selinux/config
```

Puis modifier la ligne SELINUX comme cela :

```
SELINUX=disabled
```

Et redémarrer le serveur pour que la modification prenne effet

```
reboot
```

Installons FreePBX

```
yum install freepbx
```

Installation du module digium

```
yum install php-digium_register
```

Installé le module `digium addon` dans le portail freepbx admin>module admin.
Activation des modules commerciales

```
yum install php-5.3-zend-guard-loader sysadmin fail2ban incron ImageMagick
```

**Sécurité **: Utilisez des mots de passe long (plus de 30 caractères) pour le mot de passe root, L'interface web FreePBX, tous les trunks et toutes les extensions.
Changer le Mot de passe FreePBX Web : admin → Administrateurs, créer un nouvel utilisateur avec un nom autre que “admin” avec tous les privilèges.
Supprimer l'utilisateur “admin”.
Si vous oubliez votre mot de passe administrateur, vous pouvez désactiver l'utilisation de mots de passe temporairement en tapant la commande suivante à partir de l'invite de commande:

```
amportal admin auth_none
```

Puis accéder à l'interface web et de changer le mot de passe admin.
Lorsque vous êtes prêt à nouveau, tapez à l'invite de commande:

```
amportal admin auth_database
```

La protection contre les robots, fail2ban a normalement le bon fichier de configuration à l'installation, si ce n'est pas le cas.
Éditer, le fichier `jail.local` dans `/etc/fail2ban` comme cela:

```
vim /etc/fail2ban/jail.local
```

On y insère ce qui suit

```
[DEFAULT]
ignoreip = 127.0.0.1
bantime = 1800
findtime = 600
maxretry = 8
backend = auto
[asterisk-iptables]
enabled  = true
filter = asterisk-security
action   = iptables-allports[name=SIP, protocol=all]
                   sendmail[name=SIP, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/asterisk/fail2ban

[pbx-gui]
enabled  = true
filter   = freepbx
action   = iptables-allports[name=PBX-GUI, protocol=all]
```

```
            sendmail[name=PBX-GUI, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/asterisk/freepbx_security.log

[ssh-iptables]
enabled  = true
filter   = sshd
action   = iptables-allports[name=SSH, port=ssh, protocol=tcp]
              sendmail[name=SSH, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/secure

[apache-tcpwrapper]
enabled  = true
filter   = apache-auth
action    =  iptables-allports[name=apache-auth,  port=http,
protocol=tcp]
            sendmail[name=apache-auth, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/httpd/error_log

[vsftpd-iptables]
enabled  = true
filter   = vsftpd
action   = iptables-allports[name=FTP, port=ftp, protocol=tcp]
              sendmail[name=FTP, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/vsftpd.log

[apache-badbots]
enabled  = true
filter   = apache-badbots
action   = iptables-allports[name=BadBots, port="http,https"]
            sendmail[name=BadBots, dest=email@domaine.com,
sender=email@domaine.com]
logpath  = /var/log/httpd/*access_log

[recidive]
enabled  = true
filter   = recidive
logpath  = /var/log/fail2ban.log*
action   = iptables-allports[name=recidive, protocol=all]
             sendmail[name=recidive, dest=email@domaine.com,
sender=email@domaine.com]
bantime  = 604800  ; 1 week
findtime = 86400   ; 1 day
maxretry = 20
```

purge des règles IPTABLES

En effet dans centos, il y a des règles IPTABLES qui sont mises par défaut, qu'il vaut mieux supprimer, pour éviter certain désagrément ne pas s’inquiéter pour fail2ban.

```
/etc/init.d/iptables stop
iptables-save > /etc/sysconfig/iptables
```

sécurisation du service SSH

Modifier le fichier `sshd_config` dans `/etc/ssh/`

```
vim /etc/ssh/sshd_config
```

Changer le port par défaut :

```
Port 2222
```

Utiliser la seconde version de SSH

```
Protocol 2
```

Modifier les lignes comme dans l'exemple ci-dessous, pour interdire le login root et les logins sans mot de passe :

```
PermitRootLogin no
PermitEmptyPasswords no
```

Dans le fichier à la fin ajouter `AllowUsers` pour limiter le nombre de login.

```
AllowUsers <LOGIN>
```

redémarrer le service

```
/etc/init.d/ssh restart
```

redémarrer les services http, asterisk et dahdi

```
amportal chown
amportal restart
/etc/init.d/httpd restart
```

mettre à jours les ad-dons dans le terminal

```
amportal a ma update framework
```

Maintenant vous pouvez administrer votre IPBX directement sur FREEPBX

```
http://<ip de votre IPBX>
```

Sources : wiki.freepbx.org wiki.asterisk.org