



ASTERISK FRANCE

www.asterisk-france.net

Interconnexion de serveurs Asterisk avec IAX

MINI HowTo

Interconnexion de serveurs Asterisk avec IAX

www.asterisk-france.net

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 1 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |

1.0. Table des matières

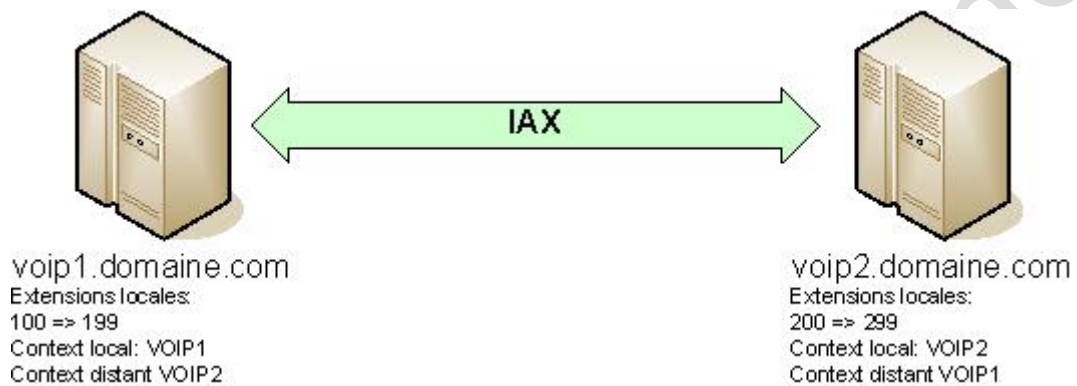
| | |
|--|----|
| 1.0. Table des matières | 2 |
| 2.0. Préface | 3 |
| 3.0. Prés-requis | 3 |
| 4.0. Sécurité de l'authentification | 4 |
| 5.0. Création d'un mot de passe crypté en md5..... | 5 |
| 6.0. Génération de clés RSA..... | 6 |
| 7.0. Configuration des paramètres IAX sur chaque serveur..... | 9 |
| 7.1. Configuration du fichier iax.conf pour le serveur voip1.domaine.com | 12 |
| 7.2. Configuration du fichier iax.conf pour le serveur voip2.domaine.com | 12 |
| 8.0. Configuration du "dialplan" dans le fichier <i>extensions.conf</i> | 13 |
| 8.1. Définition du "dialplan" pour les appels entrants. | 13 |
| 8.2. Définition du "dialplan" pour les appels sortants. | 14 |
| 9.0. Vérification des liens IAX avec la console d'Asterisk..... | 15 |
| 9.1. Connexion à la console d'Asterisk..... | 15 |
| 9.2. Vérification de l'état des liens IAX | 15 |
| 9.3. Affichage des informations d'un lien IAX en cours d'utilisation | 16 |
| 9.4. Affichage des statistiques d'un lien IAX en cours d'utilisation..... | 16 |
| 10.0. Remerciements | 17 |
| 11.0. Annexes | 17 |
| 11.1. Bibliographie | 17 |
| 11.1.1. Sites Internet | 17 |
| 11.1.2. Livres..... | 17 |
| 11.2. Listes des commandes IAX de la console d'Asterisk (en anglais) | 18 |

| | | | | |
|---------------------|--------------|---|--|---------------|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | | Page 2 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch | |



2.0. Préface

Cette procédure vous permettra de connecté les "dialplan" de plusieurs serveurs Asterisk



Dès qu'un utilisateur du serveur voip1 composera un numéro entre 200 et 299 Il sera directement redirigé vers le serveur voip2 via le protocole IAX

Dès qu'un utilisateur du serveur voip2 composera un numéro entre 100 et 199 Il sera directement redirigé vers le serveur voip1 via le protocole IAX.

Note:

Je tiens à préciser que la version actuelle de IAX est la version 2 (IAX2). Par conséquent nous emploierons le terme IAX dans notre document.

3.0. Prés-requis

- Minimum deux serveurs Asterisk déjà configuré
- Le port TCP/IP 4569 doit être redirigé sur chacun des serveurs ASTERISK
- Des connaissances sur l'édition des fichiers sous Linux
- Un accès "root" sur les serveurs Asterisk
- Openssl installé
- Savoir configurer son "Dialplan" dans Asterisk

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 3 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



4.0. Sécurité de l'authentification

Le protocole IAX permet 3 types de mots de passe pour l'authentification des clients / serveurs

Il n'est pas possible de crypter les données transmises via le protocole IAX, seul l'authentification permet plusieurs types de mots de passes plus ou moins sécurisés.

- **Plain text**

Cette méthode est déconseillée, car les mots de passe sont écrits en clair dans les fichiers de configuration.

- **MD5**

Les mots de passe sont écrits cryptés à l'aide de la méthode MD5 dans les fichiers de configurations, donc difficilement décryptables (difficile mais pas impossible)

- **RSA**

L'authentification RSA utilise deux clés partagées, une clé publique ainsi qu'une clé privée

Dans ce document nous n'utiliserons que l'authentification RSA

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 4 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



5.0. Création d'un mot de passe crypté en md5

Il suffit d'utiliser les commandes "echo" et "md5sum" pour encrypter un mot de passe en md5.

```
echo -n "<user>:<realm>:<secret>" | md5sum
```

<user> => le nom d'utilisateur

<realm> => asterisk

<secret> => le mots de passe en claire

Exemple:

```
echo -n "nom_utilisateur:asterisk:mots_de_passe" | md5sum
```

Cette commande retourne simplement le mot de passe crypter en md5 (ne pas récupérer le "-" à la fin ☺)

Il suffira de la recopier dans le fichier "iax.conf"

```
1cd57e42c215f05e06c5b5b0ec683575
```

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 5 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



6.0. Génération de clés RSA

Pour générer des clés de cryptage RSA, ASTERISK nous fournit un utilitaire: "astgenkey".

Les clés RSA doivent se trouver dans le répertoire `/var/lib/asterisk/keys`. L'utilitaire "astgenkey" génère deux clés, une clé publique à mettre sur le(s) poste(s) client(s) et une clé privée à garder sur le serveur.

Note:

Il est important que la clé privée ne soit accessible que par Asterisk, car si quelqu'un arrive à prendre cette clé il pourra décrypter la clé plus facilement.

Pour générer une clé il suffit de se déplacer dans le répertoire de stockage des clés d'Asterisk et de lancer l'application "astgenkey"

```
cd /var/lib/asterisk/keys
```

Lorsque nous lançons astgenkey nous mettons le paramètre '-n' car par défaut "astgenkey" demande une "passphrase" à chaque démarrage d'Asterisk. Avec le paramètre '-n' il enregistre la clé sans "passphrase"

```
astgenkey -n
```

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 6 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



This script generates an RSA private and public key pair in PEM format for use by Asterisk. You will be asked to enter a passcode for your key multiple times. Please enter the same code each time. The resulting files will need to be moved to /var/lib/asterisk/keys if you want to use them, and any private keys (.key files) will need to be initialized at runtime either by running Asterisk with the '-i' option, or with the 'init keys' command once Asterisk is running.

Press ENTER to continue or ^C to cancel.

Appuyez sur <ENTER> et tapez le nom de la clé que vous voulez créer (test_iax" dans notre exemple.

```
Enter key name: test_iax
```

Une fois les clés générées il affiche le résultat:

```
Generating SSL key 'test_iax':
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
writing RSA key
Key creation successful.
Public key: test_iax.pub
Private key: test_iax.key
```

La clé .pub est la clé publique et la clé .key et la clé privée.

Pour transférer la clé publique sur notre serveur "client" il suffit juste de la copier dans le répertoire /var/lib/asterisk/keys

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 7 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



ASTERISK FRANCE

www.asterisk-france.net

Interconnexion de serveurs Asterisk avec IAX

MINI HowTo

Note:

Etant donné que dans notre exemple nous allons créer une interconnexion bidirectionnelle, il faudra générer 2 paires de clés de nom différent sur les deux serveurs.

Ensuite il faudra copier la clé publique de chaque machine sur le serveur opposé dans le répertoire `/var/lib/asterisk/keys`

www.asterisk-france.net

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 8 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



7.0. Configuration des paramètres IAX sur chaque serveur

La configuration des paramètres IAX se fait dans le fichier *iax.conf* se trouvant dans le répertoire */etc/asterisk/*

Sur chaque serveur nous allons configurer un utilisateur IAX qui servira à l'authentification avec le serveur opposé.

Explication des paramètres utilisés pour configurer les utilisateurs IAX

[VOIP1] et [VOIP2]

Le nom d'utilisateur utilisé dans le fichier *extensions.conf* pour créer le "dialplan" est écrit entre crochet "[...]"

type=

Avec les comptes SIP ou IAX il existe trois sortes d'utilisateurs

- **peer**

Pour désigner un utilisateur qui pourra s'authentifier que vers un autre serveur

- **user**

Pour désigné un utilisateur qui pourra être authentifié que depuis un autre serveur ou téléphone compatible IAX

- **friend**

Un utilisateur qui pourra être authentifié vers ou depuis un autre serveur

Dans notre cas nous allons créer un utilisateur de type "friend" se qui nous permettra de configurer qu'un seul utilisateur par serveur

En général les comptes de type "user" ou "peer" ne sont utilisé que pour les liens mono directionnels

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 9 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



host=

Le paramètre `host` désigne l'adresse IP ou le nom de domaine de l'utilisateur distant, ce qui permet de s'authentifier vers le serveur opposé.

Nous pouvons aussi mettre `host=dynamic` dans le cas où on ne connaît pas l'adresse du serveur distant, mais dans ce cas l'utilisateur distant devra s'authentifier vers notre serveur.

En cas d'utilisation d'un nom de domaine mis à jour dynamiquement comme `dyndns.org` il faudra modifier le fichier `dnsmgr.conf` pour qu'Asterisk vérifie les entrées DNS du serveur distant à intervalles réguliers.

Définition du type d'authentification

Voir chapitre 4.0.

Lorsque nous utilisons une clé partagée de type RSA

- **auth=rsa**
- **inkey**=clés publiques distantes
- **outkey**=clé privée locale

Lorsque nous utilisons un mot de passe de type MD5

- **username**= nom d'utilisateur
- **md5secret**= mot de passe crypté en MD5

Lorsque nous utilisons un mot de passe de type "plain text"

- **username**= nom d'utilisateur
- **secret**= mot de passe non crypté

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 10 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |

**context=**

Défini le contexte dans lequel les appels distants arrivent

trunk=

Le paramètre trunk défini si nous voulons créer un "trunk" avec le serveur distant

Un "trunk" est une façon de limiter la bande passante utilisée par le protocole IAX vers un serveur distant.

Si vous avez 10 communications IAX simultanées vers le même serveur avec le protocole Ulaw, le total de bande passante ne sera pas 10 X 64Kb/s. En effet, le trunk va permettre de regrouper les paquets tcp pour consommer moins de bande passante

qualify=

Le paramètre qualify=yes ou qualify=<millisecondes> permet de savoir si le serveur distant est toujours joignable.

Par défaut Asterisk envoie des requêtes ping toutes les 2000ms pour savoir si le serveur distant répond.

Se paramètres permet aussi à certaines applications de gestion d'Asterisk de savoir si le lien est connecté ou mort

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 11 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



7.1. Configuration du fichier iax.conf pour le serveur voip1.domaine.com

```
[VOIP2]
type=friend
host=voip2.domaine.com
auth=rsa
inkey=voip1
outkey=voip2
context=FROM_VOIP2
qualify=yes
trunk=yes
```

7.2. Configuration du fichier iax.conf pour le serveur voip2.domaine.com

```
[VOIP1]
type=friend
host=voip1.domaine.com
auth=rsa
inkey=voip2
outkey=voip1
context=FROM_VOIP1
qualify=yes
trunk=yes
```

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 12 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



8.0. Configuration du "dialplan" dans le fichier *extensions.conf*

Nous allons configurer le dialplan de chaque serveur Asterisk pour que les appels passent d'un serveur à l'autre.

8.1. Définition du "dialplan" pour les appels entrants.

Dans les fichiers de configuration *iax.conf* au chapitre 7 nous avons défini le contexte pour les appels entrants depuis l'autre serveur.

Nous devons créer le même contexte dans le fichier *extensions.conf*

Exemple pour le "dialplan" du serveur *voip1.domaine.com*:

```
[FROM_VOIP2]
include => VOIP1
```

```
[VOIP1]
exten => 1XX,1,Dial(${EXTEN}) ; notre context local
```

Exemple pour le "dialplan" du serveur *voip2.domaine.com*:

```
[FROM_VOIP1]
include => VOIP2
```

```
[VOIP2]
exten => 2XX,1,Dial(${EXTEN}) ; notre context local
```

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 13 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



8.2. Définition du "dialplan" pour les appels sortants.

Pour configurer les appels sortants nous allons simplement créer une extension qui inclut toutes les extensions qui se trouve sur le serveur opposé.

Nous allons passer le protocole IAX2 ainsi que l'utilisateur IAX à la commande Dial.

Exemple pour le "dialplan" du serveur voip1.domaine.com:

```
[FROM_VOIP2]
include => VOIP1

[VOIP1]
exten => 1XX,1,Dial(${EXTEN}) ; notre context local

exten => 2XX,1,Dial(IAX2/VOIP2/${EXTEN})
```

Exemple pour le "dialplan" du serveur voip2.domaine.com:

```
[FROM_VOIP1]
include => VOIP2

[VOIP2]
exten => 2XX,1,Dial(${EXTEN}) ; notre context local

exten => 1XX,1,Dial(IAX2/VOIP1/${EXTEN})
```

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 14 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



9.0. Vérification des liens IAX avec la console d'Asterisk

9.1. Connexion à la console d'Asterisk

```
[root@asterisk ~]# asterisk -r
```

```
Asterisk SVN-trunk-r7230, Copyright (C) 1999 - 2005 Digium.
Written by Mark Spencer markster@digium.com
=====
Connected to Asterisk SVN-trunk-r7230 currently running on mercure (pid = 16791
Verbosity is at least 2147483647
-- Remote UNIX connection
asterisk*CLI>
```

9.2. Vérification de l'état des liens IAX

```
asterisk*CLI> iax2 show peers
```

| Name/Username | Host | Mask | Port | Status |
|---|---------------|---------------------|----------|------------|
| VOIP1 | XXX.XXX.XX.XX | (S) 255.255.255.255 | 4569 (T) | OK (25 ms) |
| 1 iax2 peers [1 online, 0 offline, 0 unmonitored] | | | | |

Explication des colonnes:

Name/Username: affiche le nom de la connexion
Host: affiche l'adresse IP de l'utilisateur
(S): affiche si l'adresse IP de l'utilisateur est statique
(D): affiche si l'adresse IP de l'utilisateur est dynamique
Mask: affiche le masque de sous réseau
Port: affiche le port IAX utilisé
(T): affiche si le lien est un "trunk"
Status: affiche si le lien est OK avec les [ms] de lag
affiche UNREACHABLE si le status du lien est mort
affiche UNMONITORED si le status du lien n'est pas monitorer
ou inconnu



9.3. Affichage des informations d'un lien IAX en cours d'utilisation

```
asterisk*CLI> iax2 show channels
```

```
Channel      Peer      UsernameID (Lo/Rem)Seq (Tx/Rx)    Lag    Jitter  JitBuf Format
IAX2/VOIP1-16385 XXX.XXX.XX.XX VOIP1 16385/16385 00007/00004 00000ms -0001ms 0000ms ulaw
1 active IAX channel
```

Explications des colonnes:

Channel: identification du channel
Peer: adresse IP de l'utilisateur IAX
UsernameID: nom d'utilisateur IAX
(Lo/Rem)Seq:
(Tx/Rx): nombres de paquets envoyés
Lag: LAG du lien IAX
Jitter:
JitBuf:
Format: codec utilisé

9.4. Affichage des statistiques d'un lien IAX en cours d'utilisation

```
asterisk*CLI> iax2 show netstats
```

```
----- LOCAL ----- REMOTE -----
Channel      RTT Jit Del Lost % Drop OOO Kpkts Jit Del Lost % Drop OOO Kpkts
IAX2/VOIP1-16384 88 -1 0 -1 -1 0 -1 0 0 40 0 0 0 0 0
1 active IAX channel
```



10.0. Remerciements

Je tiens à remercier les personnes suivantes:

- Cyril Mandrilly
- Vincent Renaville

pour avoir testé ainsi que corrigé cette procédure.

11.0. Annexes

11.1. Bibliographie

11.1.1. Sites Internet

<http://www.voip-info.org/wiki/index.php?page=Asterisk+iax+rsa+auth>

11.1.2. Livres

Titre: Asterisk , The Future of Telephony
Editeur: Oreilly
Langue: anglais
ISBN: 0-596-00962-3

Titre: Bulding Telephony Systems with Asterisk
Editeur: PACKT Publishing
Langue: angais
ISBN: 1-904811-15-9

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 17 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |



11.2. Listes des commandes IAX de la console d'Asterisk (en anglais)

iax2 debug Enable IAX debugging
iax2 jb debug Enable IAX jitterbuffer debugging
iax2 no debug Disable IAX debugging
iax2 no jb debug Disable IAX jitterbuffer debugging
iax2 no trunk debug Disable IAX trunk debugging
iax2 provision Provision an IAX device
iax2 prune realtime Prune a cached realtime lookup
iax2 reload Reload IAX configuration
iax2 set jitter Sets IAX jitter buffer
iax2 show cache Display IAX cached dialplan
iax2 show channels Show active IAX channels
iax2 show firmware Show available IAX firmwares
iax2 show netstats Show active IAX channel netstats
iax2 show peer Show details on specific IAX peer
iax2 show peers Show defined IAX peers
iax2 show provisioning Show iax provisioning
iax2 show registry Show IAX registration status
iax2 show stats Display IAX statistics
iax2 show users Show defined IAX users
iax2 test losspect Set IAX2 incoming frame loss percentage
iax2 trunk debug Enable IAX trunk debugging

| | | | |
|---------------------|--------------|---|---|
| ASTERISK-FRANCE.NET | | Auteurs: Serge Carpentier Frédéric Marti | Page 18 sur 18 |
| 11.01.2006 | Version: 1.2 | Mise à jour: 15.01.2006 | Tous droits réservés. Pour toutes modifications, veuillez nous contacter. sergecarpentier@free.fr f.marti@submusic.ch |