J-EOLE
18-19 Octobre 2012

Haute disponibilité sur EOLE
Sphynx
ARV

Haute disponibilité

Pacemaker/Corosync

Gestionnaire de haute disponibilité

Corosync

- Cluster : deux machines ou plus

Pacemaker

- Démarrer les ressources du cluster
- Arrêter les ressources du cluster
- Superviser les ressources du cluster

Haute disponibilité

« Eolisation » de Pacemaker

Paquet eole-pacemaker

- Cluster : deux machines (maître/esclave ou actif/passif)

  Une interface réseau dédiée au dialogue inter node

Groupe de ressources ou primitives nommé VIPCluster :

- VIP : adresses IP virtuelles
- Services : /etc/init.d/service_script (compatible LSB)

Ping : test de ping

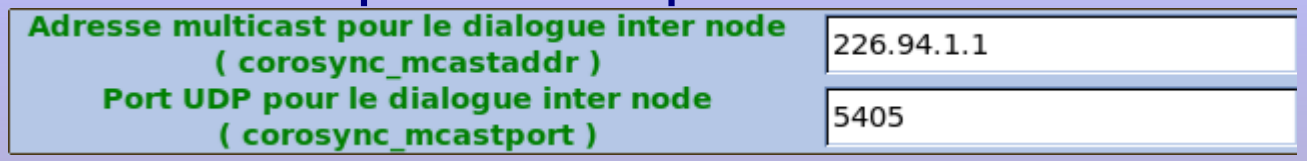
Fichiers ou répertoires à synchroniser

Haute disponibilité

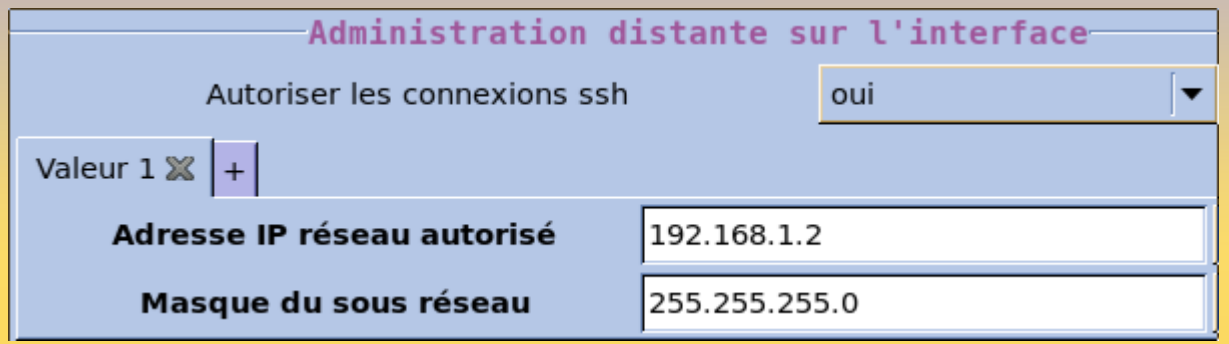
Configuration des nodes du cluster

Sur l'interface dédiée :

- Ouverture du port UDP pour la communication des nodes



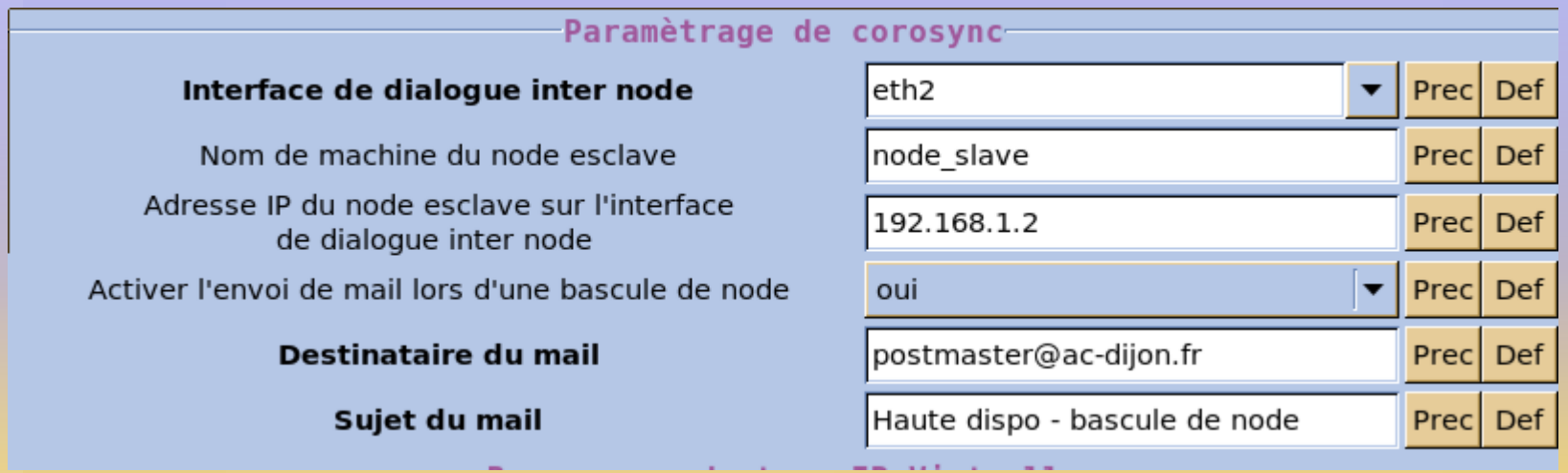
- Sur chaque node, autoriser la communication ssh pour la synchronisation des fichiers



Haute disponibilité

Configuration du maître

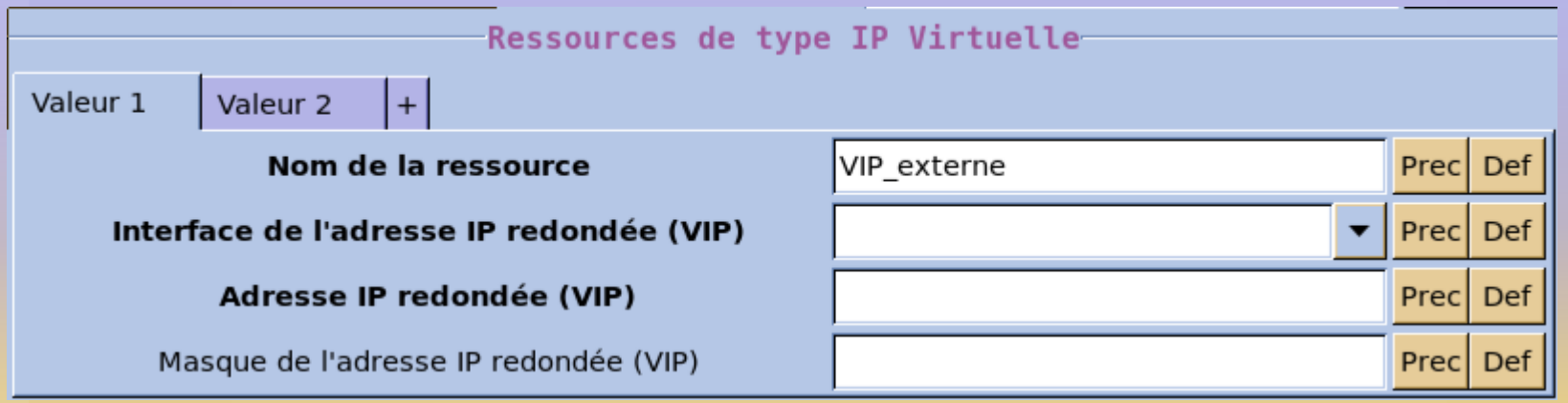
- Déclaration du node esclave
- Activation ou non de l'envoi de mail



Haute disponibilité

Configuration du maître

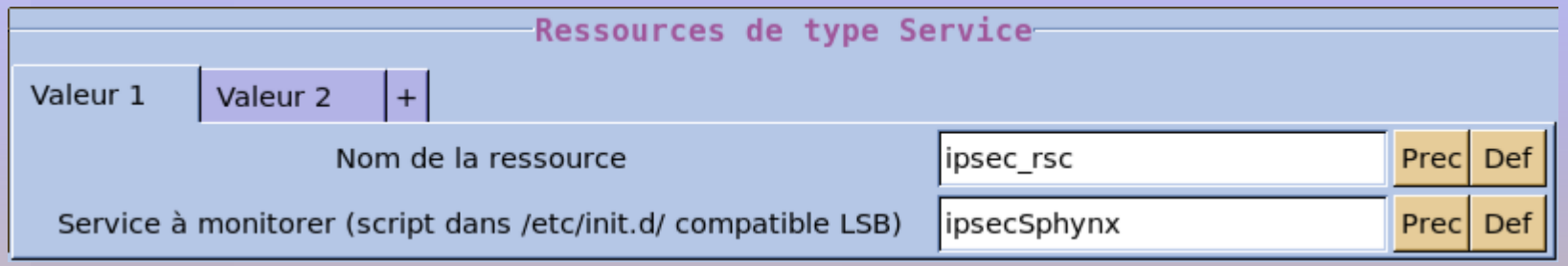
- Paramétrage des VIP



Haute disponibilité

Configuration du maître

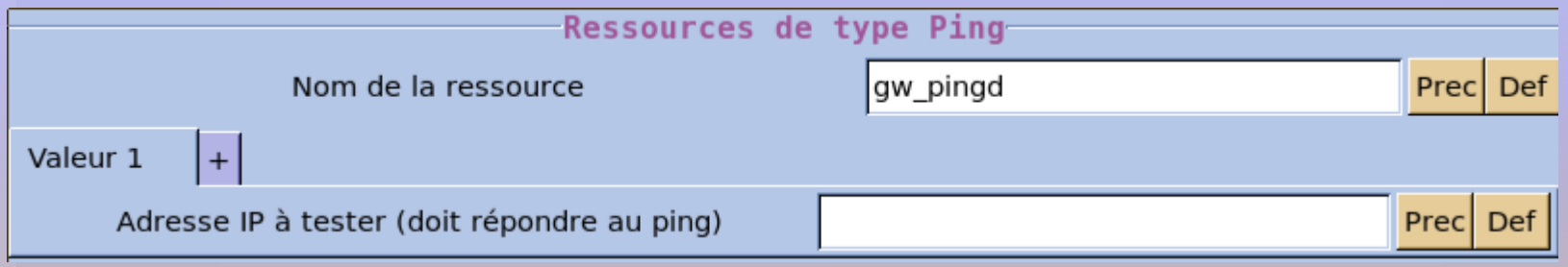
- Paramétrage des services à superviser



Haute disponibilité

Configuration du maître

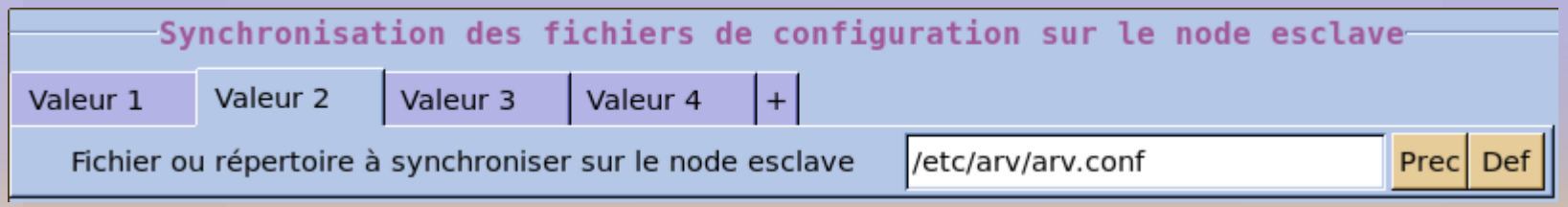
- Test des machines distances à atteindre



Haute disponibilité

Configuration du maître

- Fichiers ou répertoires à synchroniser avec le node esclave par le script /usr/share/eole/synchro-nodes.sh



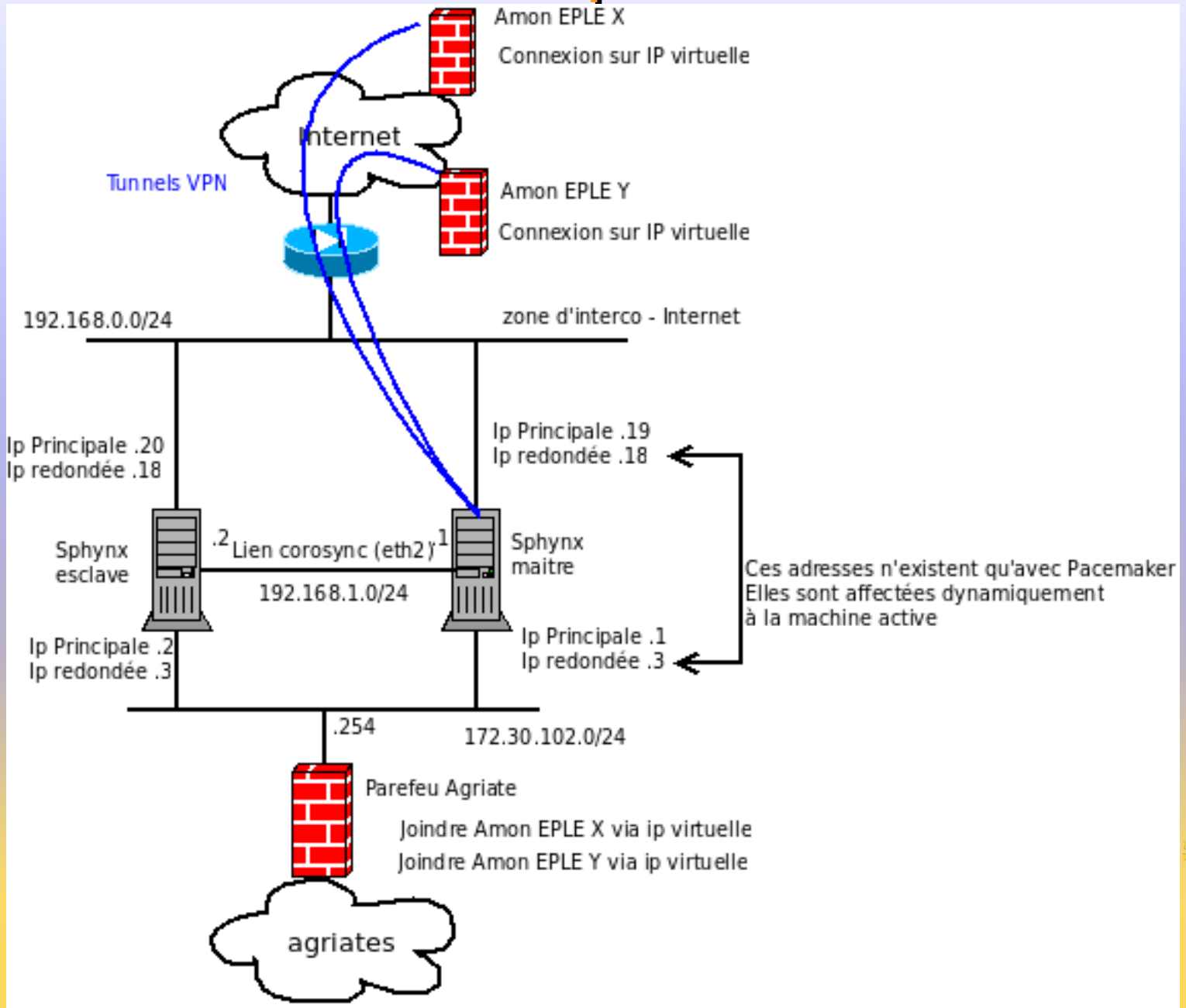
Haute disponibilité

Configuration de l'esclave

- Déclaration du node maître

Aucune ressource n'est déclarée sur la machine esclave

Haute disponibilité



Haute disponibilité

Mise en place sur Sphynx

Paramètrage de corosync

Interface de dialogue inter node	eth2
Nom de machine du node esclave	sphynxtestha2
Adresse IP du node esclave sur l'interface de dialogue inter node	192.168.1.2
Activer l'envoi de mail lors d'une bascule de node	oui
Destinataire du mail	barco@ac-dijon.fr
Sujet du mail	Haute dispo - bascule de node

Paramètrage de corosync

Interface de dialogue inter node	eth2
Nom de machine du node maitre	sphynxtestha1
Adresse IP du node maitre sur l'interface de dialogue inter node	192.168.1.1

Haute disponibilité

Mise en place sur Sphynx

- On redonde eth0 et eth1

Ressources de type IP Virtuelle

Valeur 1	Valeur 2	+

Nom de la ressource	VIP_externe
Interface de l'adresse IP redondée (VIP)	eth0
Adresse IP redondée (VIP)	192.168.0.18
Masque de l'adresse IP redondée (VIP)	255.255.255.0

Ressources de type IP Virtuelle

Valeur 1	Valeur 2	+

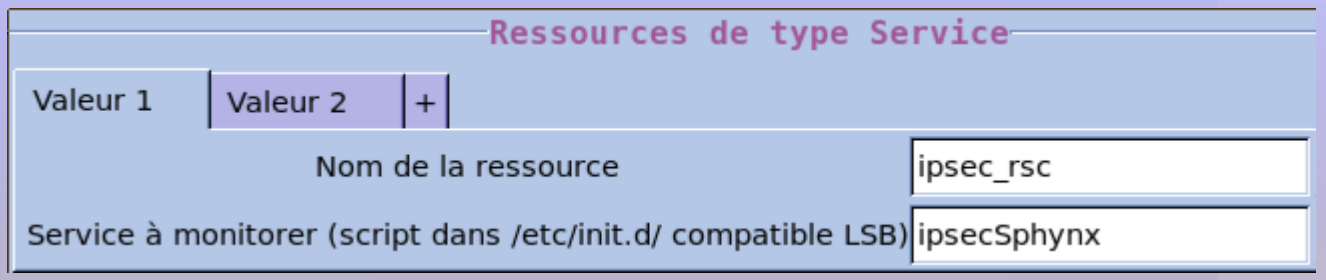
Nom de la ressource	VIP_interne
Interface de l'adresse IP redondée (VIP)	eth1
Adresse IP redondée (VIP)	172.30.102.3
Masque de l'adresse IP redondée (VIP)	255.255.255.0

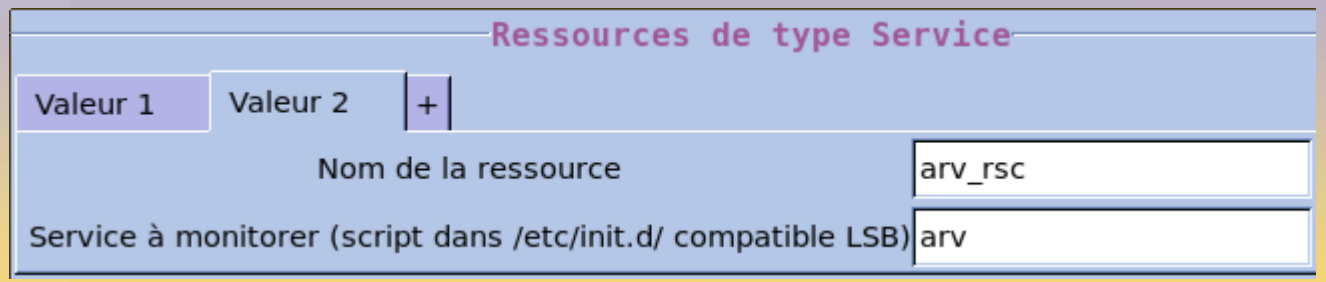
Haute disponibilité

Mise en place sur Sphynx

- On supervise ipsec et arv

Compatibilité LSB : http://www.clusterlabs.org/doc/en-US/Pacemaker/1.0/html/Pacemaker_Explained/ap-lsb.html

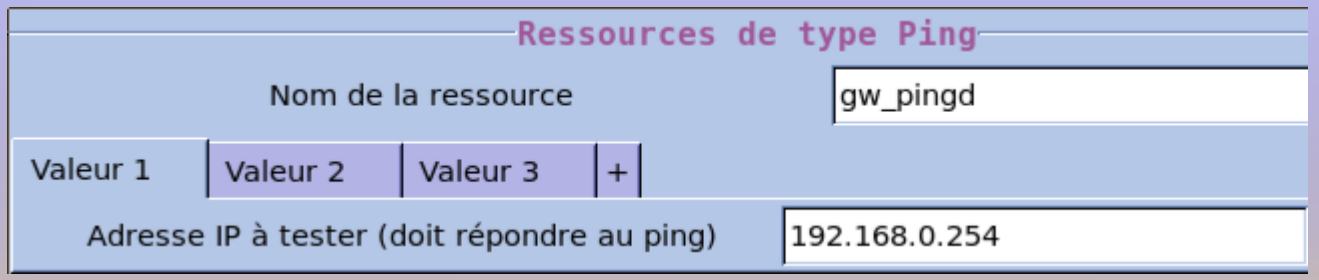




Haute disponibilité

Mise en place sur Sphynx

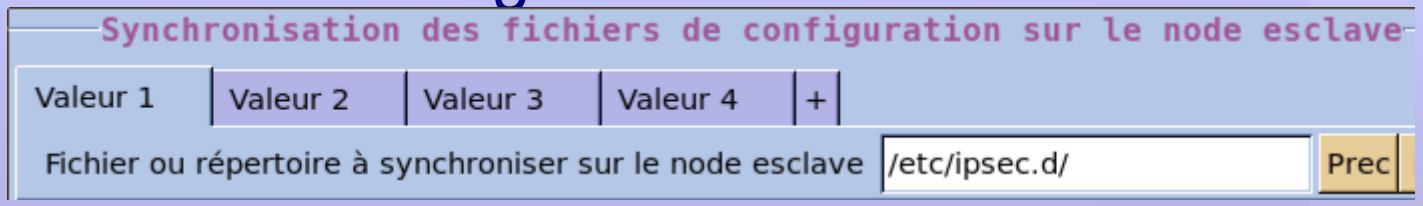
- On teste le ping sur la passerelle

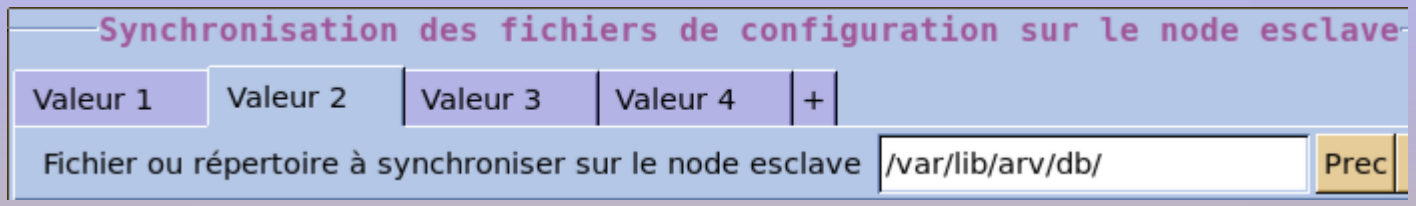


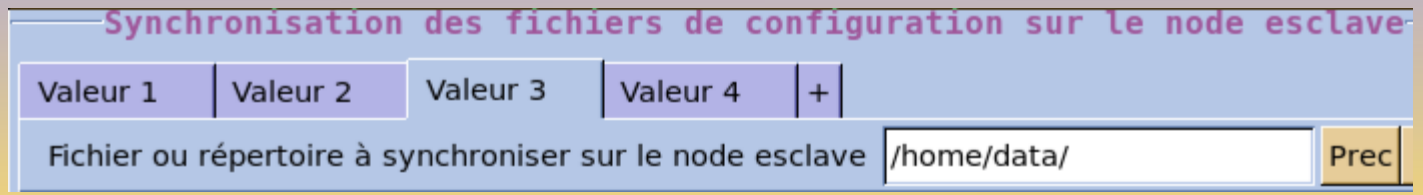
Haute disponibilité

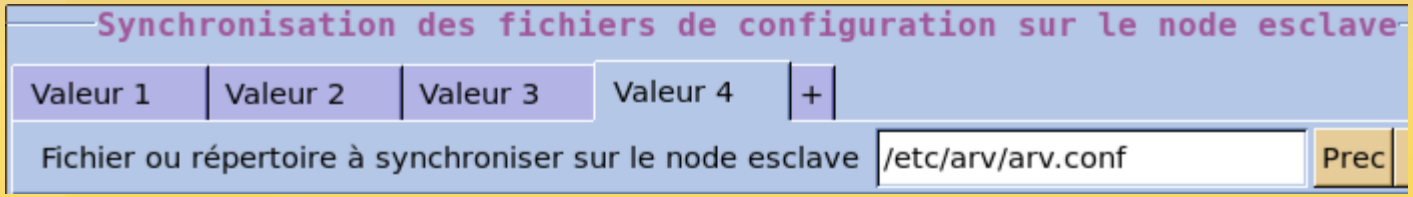
Mise en place sur Sphynx

- On synchronise arv et Strongswan









Haute disponibilité

Mise en place sur Sphynx

- Instanciation du serveur maître
- Instanciation du serveur esclave
- Lancer synchro-nodes.sh sur le serveur maître
- Lancer synchro-nodes.sh sur le serveur esclave

crm_mon : état du cluster

Haute disponibilité

« Eolisation » de Pacemaker

Evolutions :

- Active/Active
- Drbd : ressource de partage de fichiers

http://www.clusterlabs.org/

http://binbash.fr/2011/09/19/des-clusters-avec-pacemaker/

Haute disponibilité

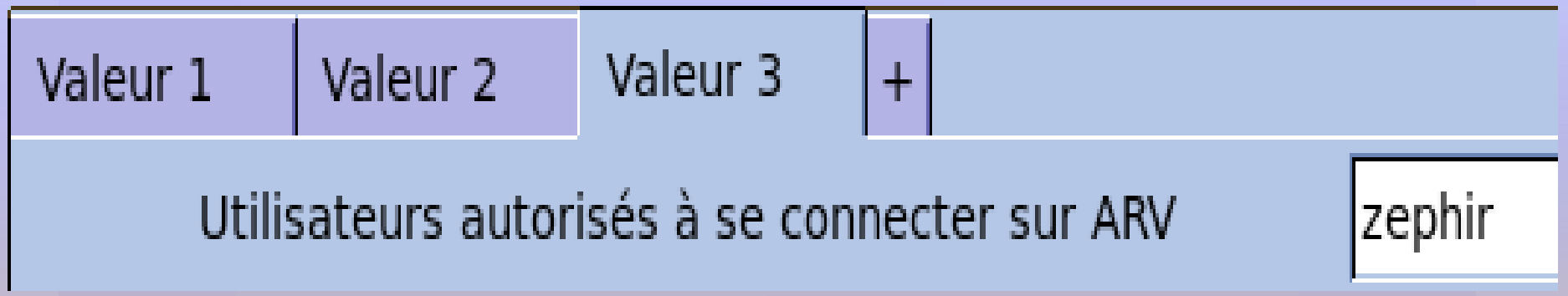
« Eolisation » de Pacemaker

QUESTIONS

Sphynx

Sphynx

Configuration



Sphynx

Sphynx

Configuration

Paramètres des certificats

Taille de la clé RSA	2048
Nom du pays (2 caractères) (C=)	fr
Nom de l'organisation (O=)	gouv

Valeur 1 | Valeur 2 | +

Nom de l'unité de l'organisation (OU=)	ac-dijon

Valeur 1 | Valeur 2 | +

URL des listes de révocation de certificats (sinon rien)	http://crl1.igc.education.fr/agriates.crl

Sphynx

Sphynx

Configuration

Filtrage des tunnels

Autoriser les réseaux établissements à communiquer entre eux	oui
Valeur du mtu pour les connexions intersite (ou rien)	

Valeur 1 +

Adresse source à autoriser	10.21.11.0
Adresse netmask de l'IP source à autoriser	255.255.255.0
Adresse destination à autoriser	10.21.12.0
Adresse netmask de l'IP destination à autoriser	255.255.255.0
Protocole destination à autoriser	tout

Sphynx

Sphynx

Configuration

Choix du protocole de routage a mettre en oeuvre	ocsp rip
Valeur 1 ■ +	
Adresses reseau autorisee a ajouter des routes dynamiquement	172.30.102.0
Masque de sous reseau associee a cette adresse	255.255.255.0

Sphynx

Sphynx
Configuration

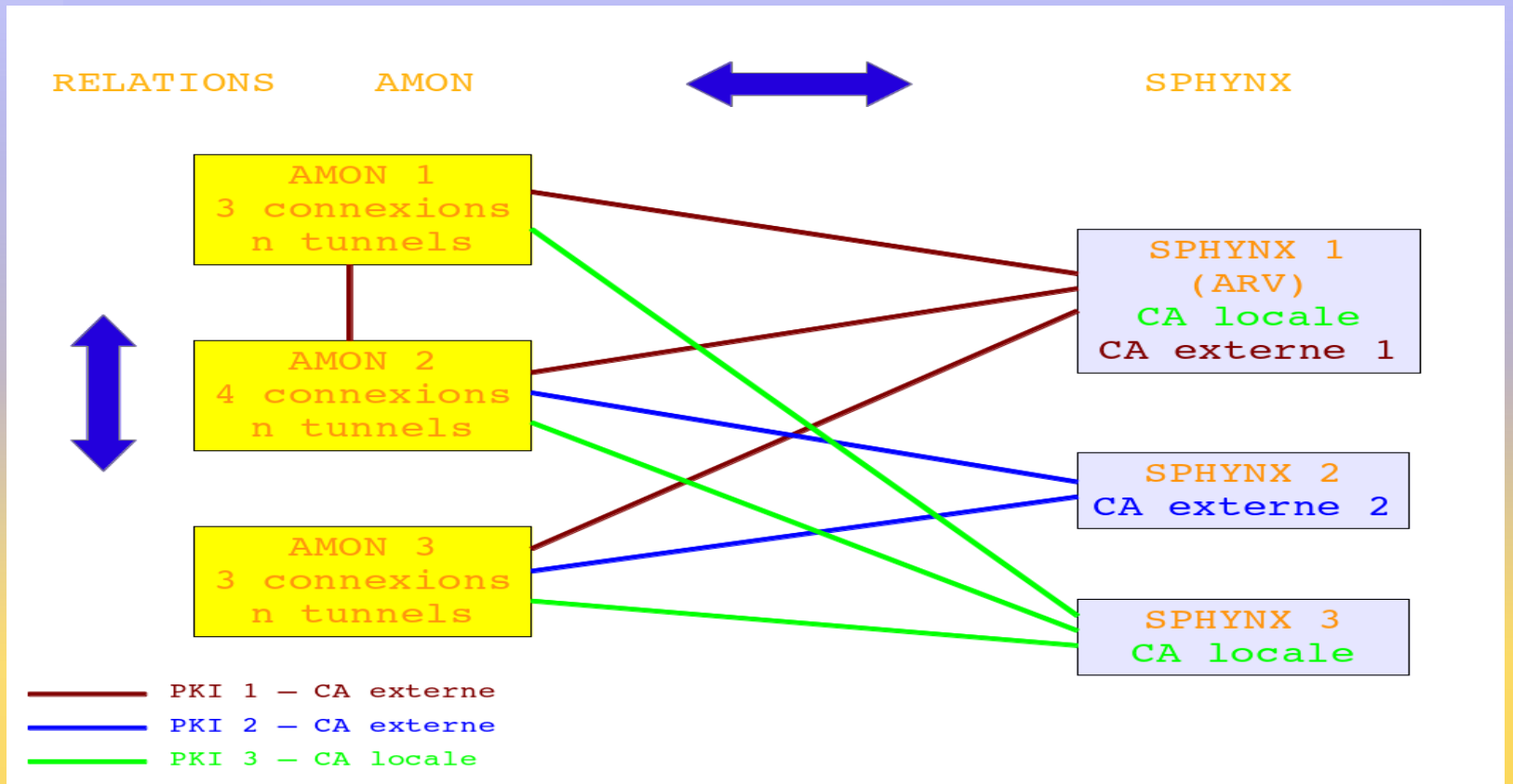
QUESTIONS

Sphynx

ARV

Administration des Réseaux Virtuels

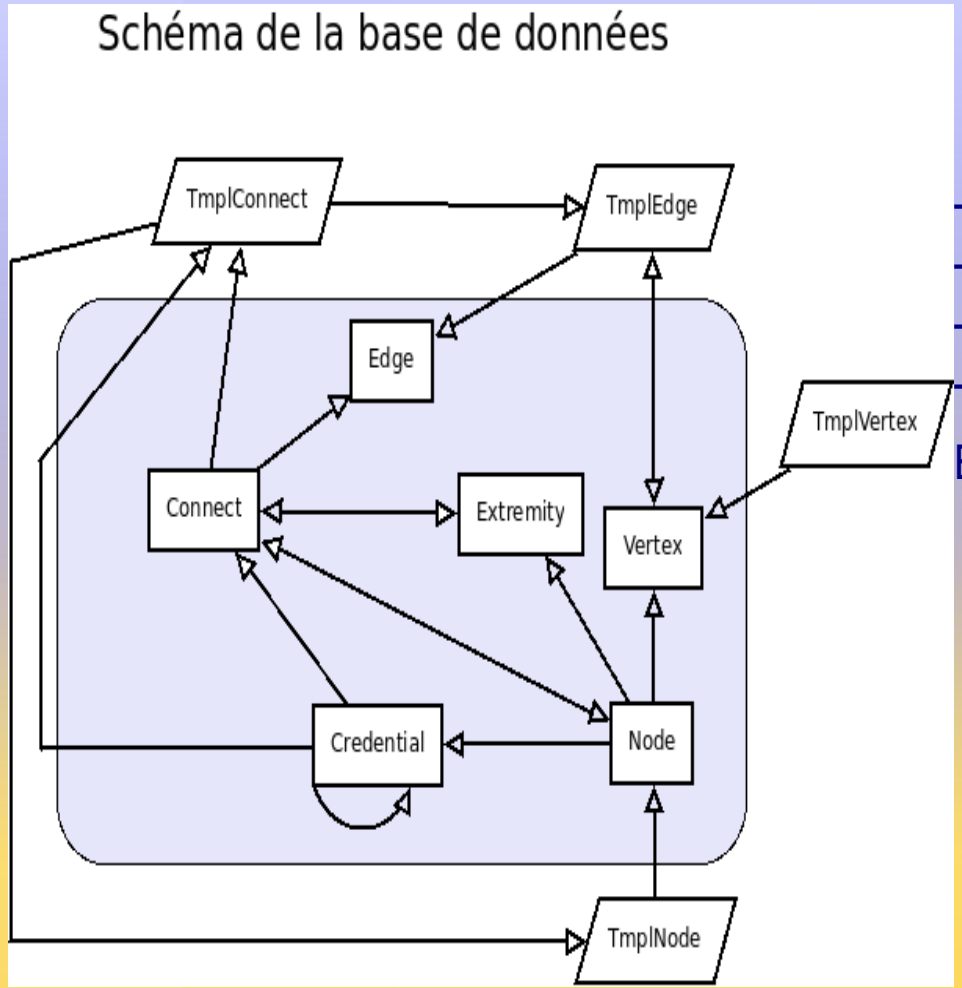
- Permet de modéliser les connexions RVP



Sphynx

ARV

Plus en détail...

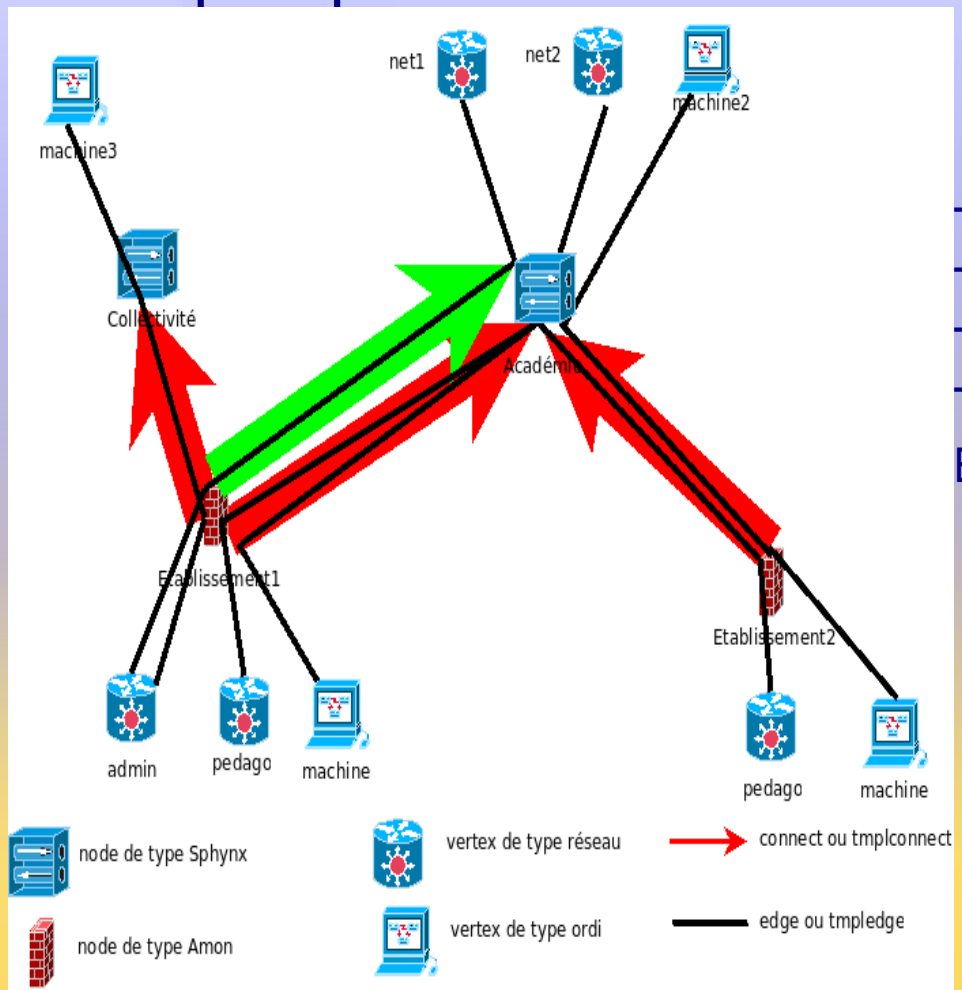


Tmplvertex / vertex : modèle / réseau local (admin)
Tmpledge/ edge : modèle / tunnel (admin-reseau172)
Tmplconnect / connect : modèle / lien sécurisé (amon-sphynx)
Tmplnode / node : modèle / serveur RVP (Amon_Clg1)
Extremity : extrémité (IP publique)

Sphynx

ARV

Un peu plus concrètement...



Tmplvertex / vertex : modèle / réseau local (admin)
Tmpledge/ edge : modèle / tunnel (admin-reseau172)
Tmplconnect / connect : modèle / lien sécurisé (Amon-Sphynx)
Tmplnode / node : modèle / serveur RVP (Amon-0000000A)
Extremity : extrémité (IP publique)

Sphynx

ARV - L'interface

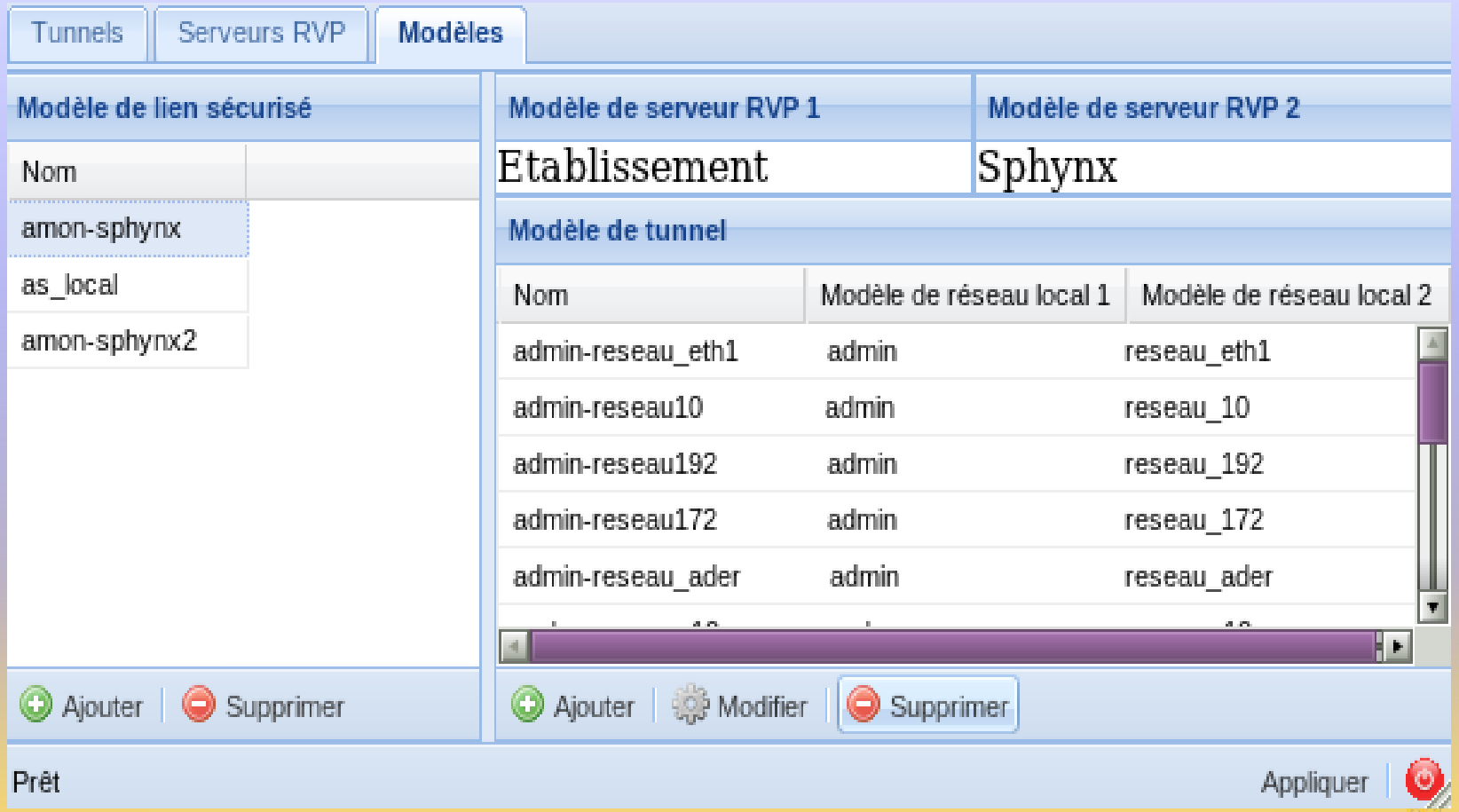
Connexion PAM ou avec utilisateur Zéphir

Avantage utilisateur Zéphir :

- Importation des serveurs
- Récupération des paramètres réseau
- Envoi d'archives RVP sur Zéphir

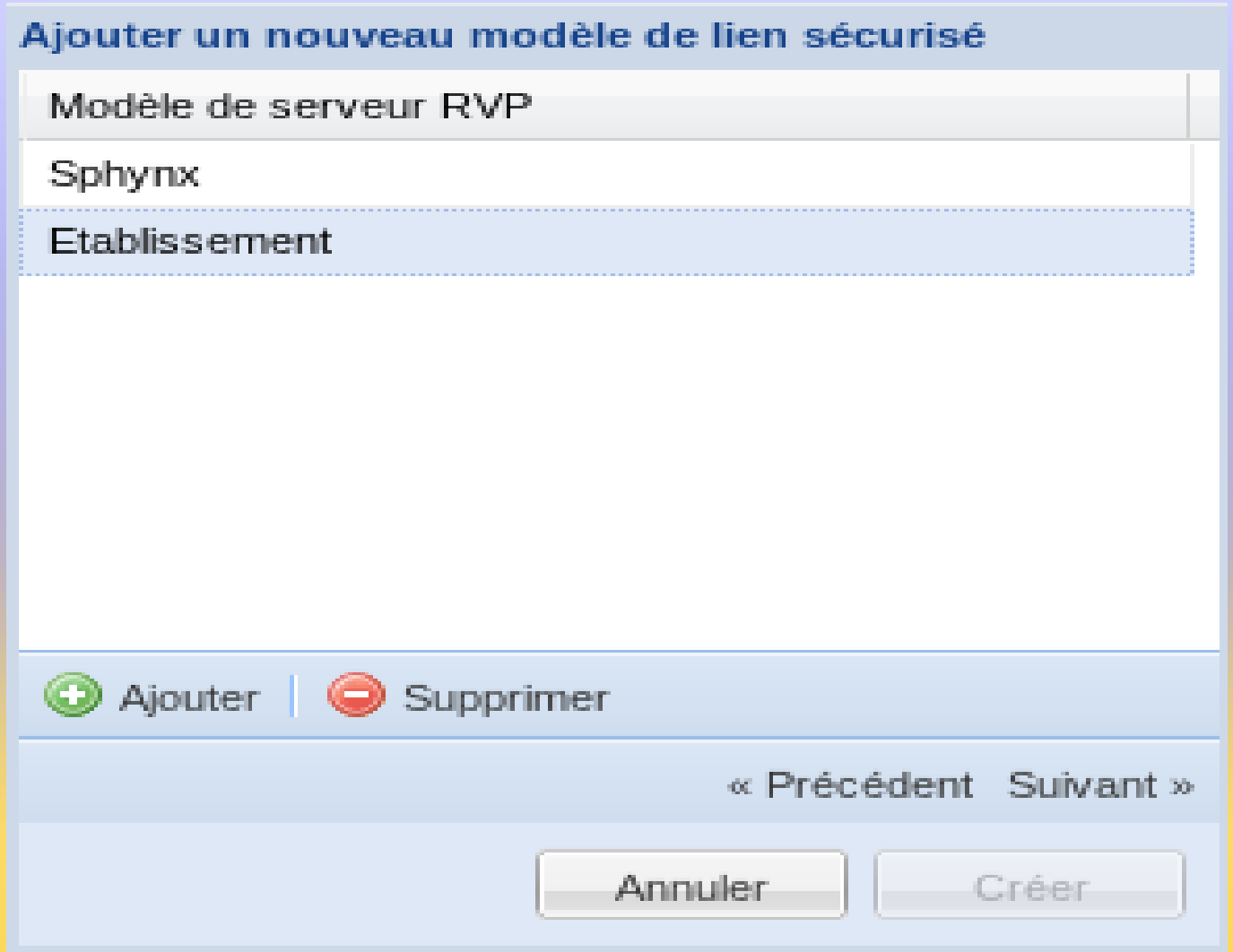
Sphynx

ARV - L'interface



Sphynx

ARV - L'interface

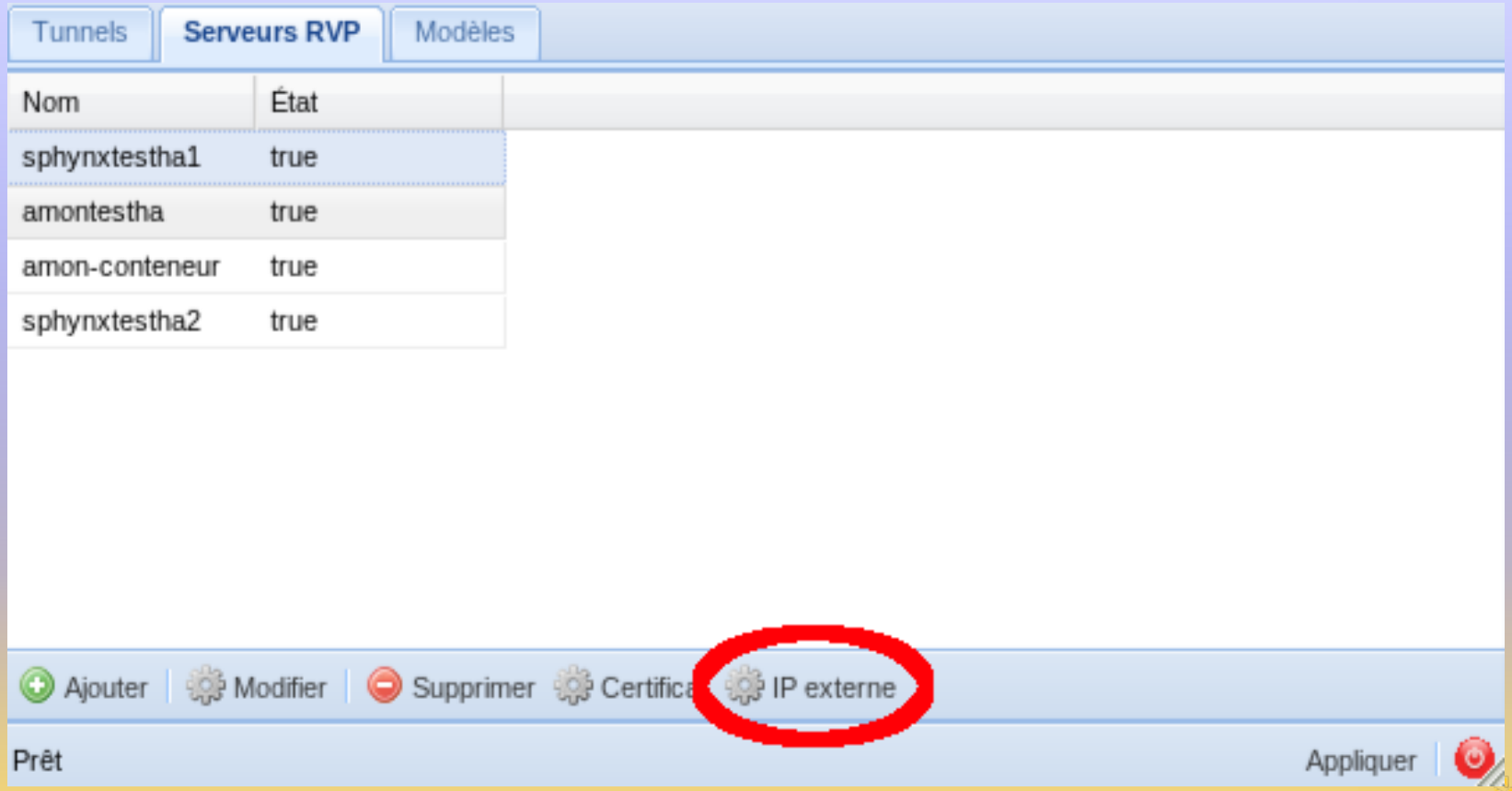


Sphynx

ARV - L'interface

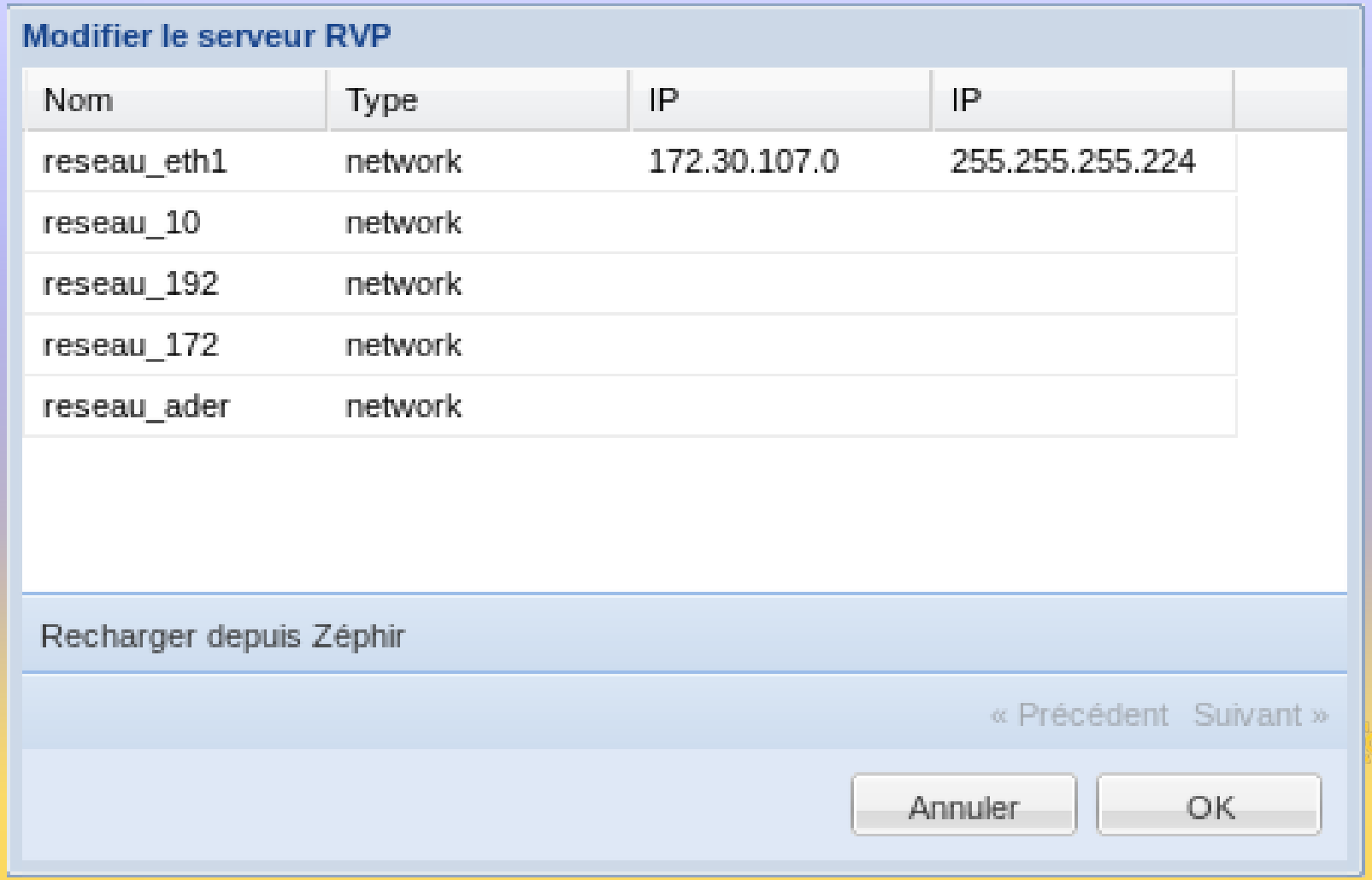
Sphynx

ARV - L'interface



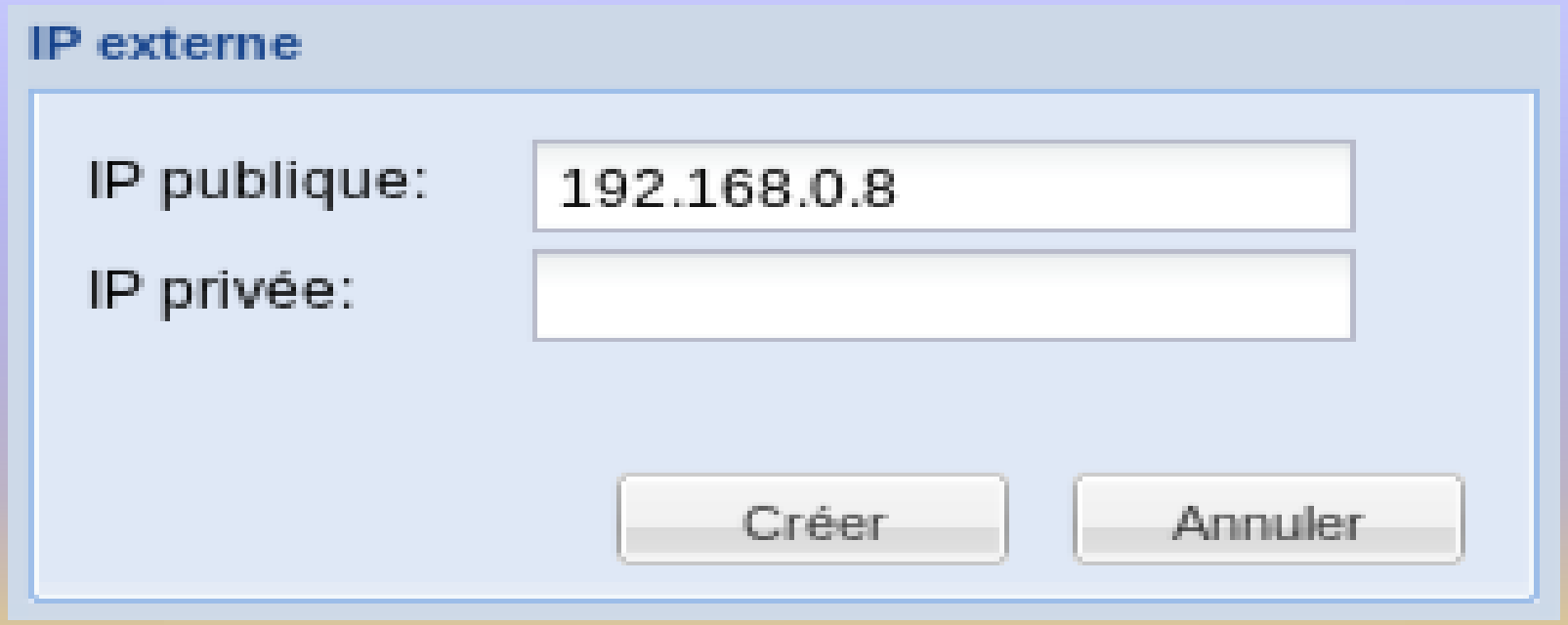
Sphynx

ARV - L'interface



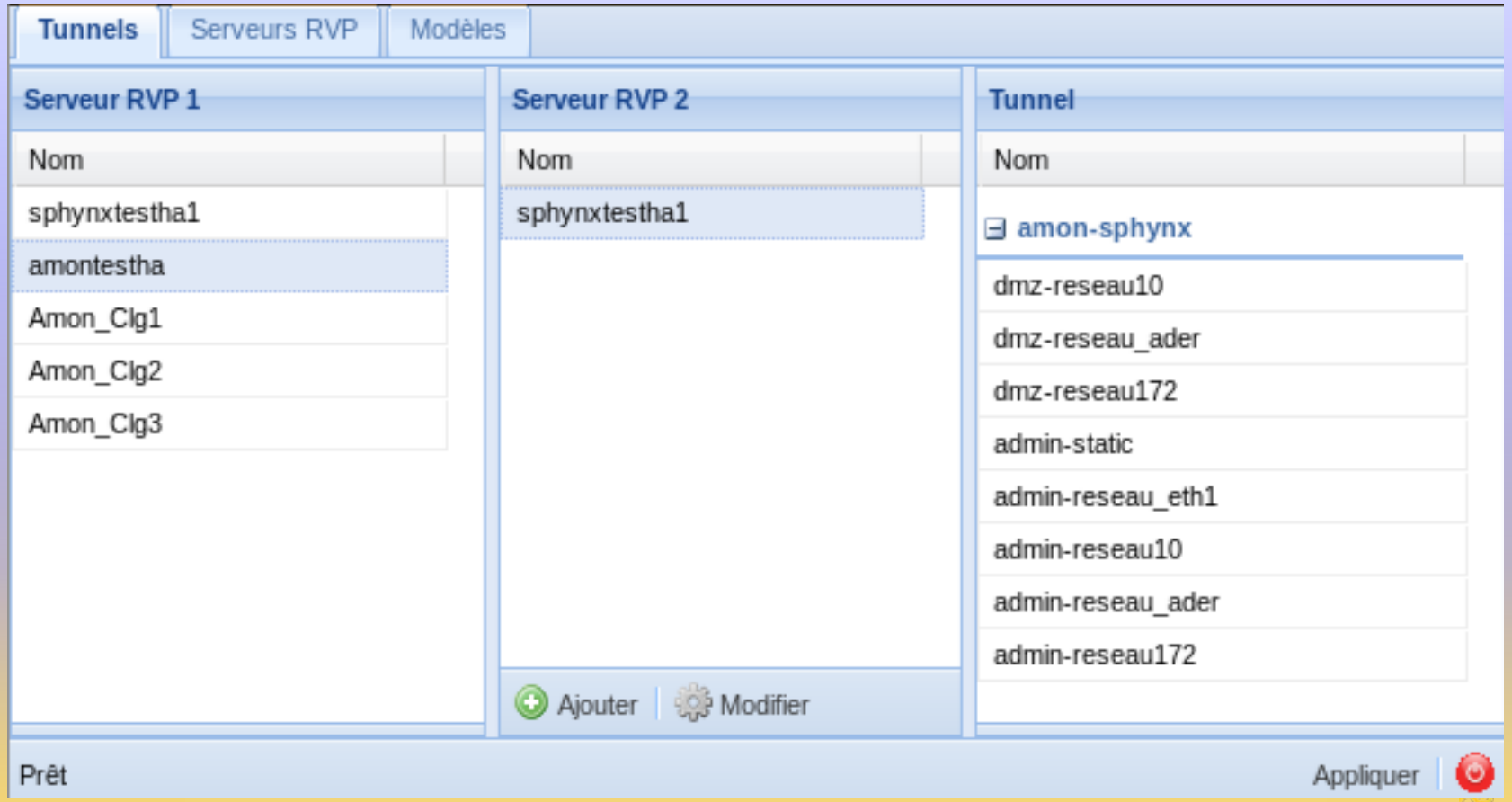
Sphynx

ARV - L'interface



Sphynx

ARV - L'interface



Sphynx

ARV – l'API

Scripter l'alimentation de la base ARV en python :

Exemple dans */usr/share/eole/init_sphynx*

Débuter le script par :

#!/usr/bin/env python

 # -- coding: UTF-8 -*-*

Ouverture de la base ARV :

from arv.db.initialize import initialize_database

initialize_database() : ouvre la base existante

initialize_database(create=True) : Crée une base vide

Sphynx

ARV – l'API

Créer une autorité de certification locale :

```
from creole import cert
from arv.db.edge import add_credential_auth
credential = open(cert.ca_file, 'r').read()
credauth = add_credential_auth(credential=credential,
local=True)
```

Ajouter l'autorité de certification de Toulouse :

```
from arv.config import CACert
ca_toulouse = add_credential_auth(credential=CACert)
```

Sphynx

ARV – l'API

Se connecter à Zéphir :

```
from arv.lib.usezephir import Zephir
zephir = Zephir(user='login', password='passwd')
sphynxmodule = zephir.get_module('sphynx')['moduleid']
amonmodule = zephir.get_module('amon')['moduleid']
```

Sphynx

ARV – l'API

Récupérer la valeur d'une variable depuis Zéphir :

```
ip_network = zephir.get_var(uai='0000000B',
                            name='Amon_Clg1',
                            var='adresse_network_eth1')
ip_netmask = zephir.get_var(uai='0000000B',
                            name='Amon_Clg1',
                            var='adresse_netmask_eth1')
```

Sphynx

ARV – l'API

Créer un modèle de serveur RVP (tmplnode) :

```
from arv.db.node import add_tmpl_node
tmpl_sphynx = add_tmpl_node(name=u"Sphynx",
                            mimetype=u'sphynx')
tmpl_amon = add_tmpl_node(name=u"Etablissement",
                          mimetype=u'etablissement')
```

Sphynx

ARV – l'API

Créer un modèle de réseau local (tmplvertex) :

```
subnet172 = tmpl_sphynx.add_tmpl_vertex(
                                        name='reseau_172',
                                        mimetype=u'network')
subnet_admin = tmpl_amon.add_tmpl_vertex(
                    name='admin',
                    mimetype=u'network',
                    zephir_module=amonmodule,
                    zephir_var_ip1='adresse_network_eth1',
                    zephir_var_ip2='adresse_netmask_eth1')
```

Sphynx

ARV – l'API

Créer un modèle de connexion (tmplconnect) :

tmplconnect = add_tmpl_connect('amon-sphynx',
tmpl_amon,
tmpl_sphynx,
ca_toulouse)

Sphynx

ARV – l'API

Créer un modèle de tunnel (tmpledge) :

```
admin_res172 = tmplconnect.add_tmpl_edge(
                                'admin-reseau172',
                                subnet_admin,
                                subnet172)
```

Sphynx

ARV – l'API

Créer un serveur RVP (node) :

```
sphynx = tmpl_sphynx.add_node(name='Sphynx_Acad',
                              uai='0000000A')
amon = tmpl_amon.add_node(name='Amon_Clg1',
                          uai='0000000B')
sphynx_extr = sphynx.add_extremity(pub_ip='194.167....')
amon_extr = amon.add_extremity(pub_ip='194.167....')
```

Sphynx

ARV – l'API

Affecter un réseau local à un serveur RVP (vertex) :

```
sphynx_172 = subnet172.add_vertex(sphynx,
                                  ip1 = '172.16.0.0',
                                  ip2 = '255.240.0.0')
amon_admin = subnet_admin.add_vertex(amon,
                                     ip1=ip_network,
                                     ip2=ip_netmask)
```

Sphynx

ARV – l'API

Affecter un certificat à un serveur RVP :

```
sphynx_cert = sphynx.import_credential(
                    private_key=decrypted_privkey_string,
                    credential=certificate_string,
                    password=key_password)
amon_cert = amon.import_credential(
                    private_key=encrypted_privkey_string,
                    credential=certificate_string,
                    password=key_password)
```

Sphynx

ARV – l'API

Appliquer un modèle de connexion à 2 serveurs (connect) :

```
amon_sph_connect = tmplconnect.add_connect(
                        tail_node=amon,
                        head_node=sphynx,
                        tail_extr=amon_extr,
                        head_extr=sphynx_extr,
                        tail_cred=amon_cert,
                        head_cred=sphynx_cert)
```

Sphynx

ARV – l'API

Appliquer un modèle de tunnel à une connexion (edge) :

admin_res172.add_edge(amon_sph_connect)

Commit de la base de données ARV :

from arv.db.initialize import commit_database
commit_database()

Sphynx

ARV – l'API

Générer la base de données Strongswan :

```
from arv.lib.dbapply import db_apply
from arv.lib.usezephir import Zephir
user = 'zephir'
password = 'eole'
zephir = Zephir(user=user, password=password)
if zephir:
    print("Login Zéphir OK")
db_apply(zephir=zephir)
```

Sphynx

ARV – l'API

QUESTIONS