Installation et mise en œuvre du module Sphynx

EOLE 2.5.2

création : Octobre 2015 Version : révision : Avril 2018

EOLE 2.5.2

Version : révision : Avril 2018

Date : création : Octobre 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Il est développé par le Pôle national de compétences Logiciels Libres du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information de l'académie de Dijon (DSI).

Pour toute information concernant ce projet vous pouvez nous joindre :

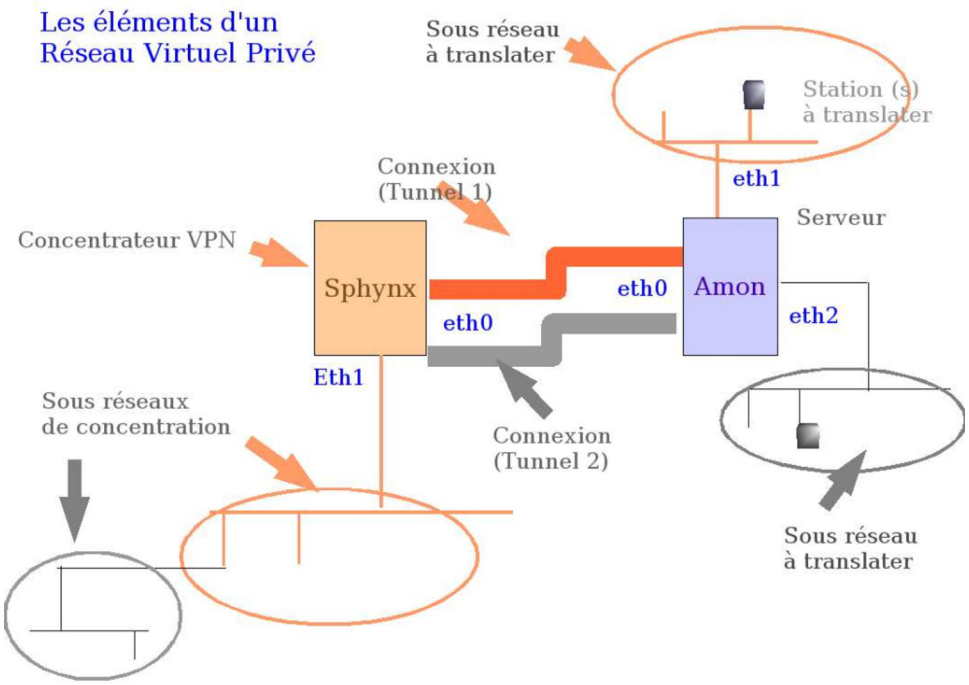
- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : http://eole.orion.education.fr

Table des matières

Chapitre 1

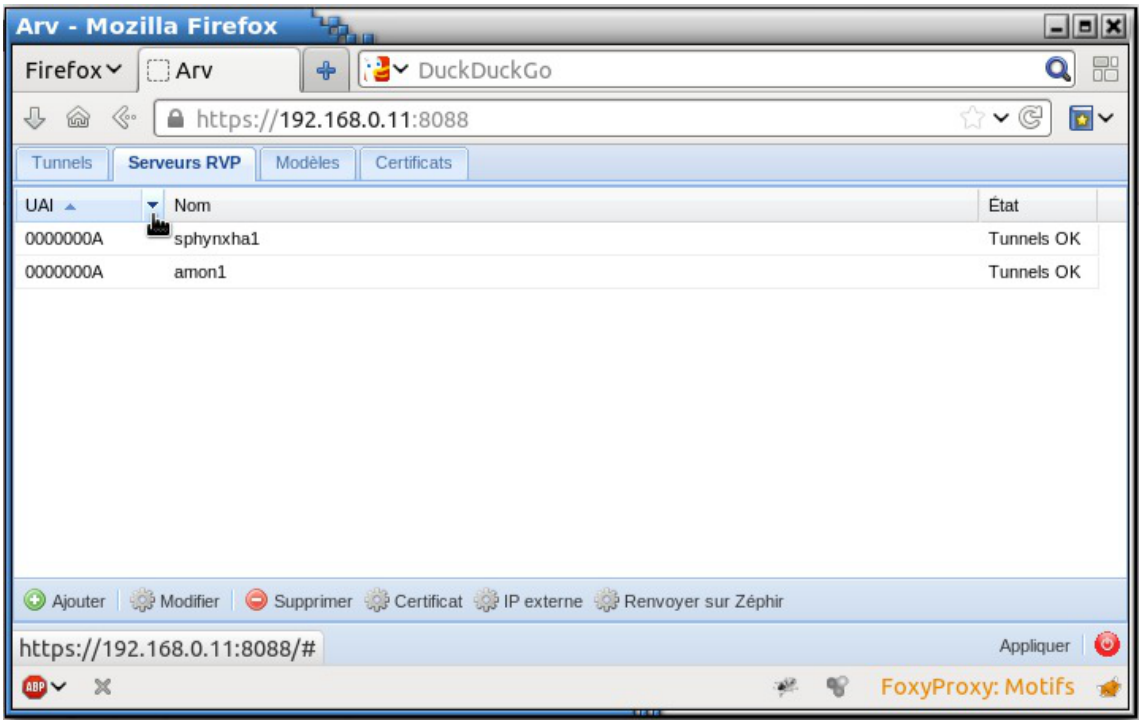
Introduction au module Sphynx

Le serveur Sphynx est un concentrateur de Réseaux Virtuels Privés (RVP[p.185] ou VPN). Il permet de relier des stations, des sous-réseaux, ou des réseaux entre eux, au travers d'Internet et ce de manière sécurisée. Le serveur Sphynx fait partie des éléments constitutifs du réseau AGRIATES[p.178].



Les éléments d'un réseau virtuel privé

L'outil ARV[p.179], pré-configuré dans le module Sphynx, permet de construire un modèle de configuration RVP. Il permet de générer des configurations RVP pour strongSwan[p.186].



1. Qu'est ce que Sphynx ?

Sphynx est un concentrateur de Réseau Virtuel Privé (RVP[p.185]). Il vous permet de relier en réseau vos serveurs pour former un RVP entre le module pare-feu Amon des établissements distants et le module Sphynx en entrée de votre réseau académique.

Principales fonctionnalités

- possibilité de travailler avec des certificats auto-signés ou signés par une PKI[p.184] externe simultanément ;
- le concentrateur académique Sphynx comprend un pare-feu pour se protéger des attaques ;
- communications chiffrées entre les réseaux des établissements et le réseau académique ;
- préparation des configurations établissement sur le serveur Sphynx grâce à l'outil ARV[p.185] ;
- mise à jour opérée sur le serveur Sphynx au moyen des outils livrés dans la distribution.

2. À qui s'adresse ce module ?

Le concentrateur de Réseaux virtuels privés Sphynx s'adresse à toutes les structures souhaitant prolonger leur réseau au travers d'Internet. Le RVP pourra alors être monté entre :

- deux modules Sphynx ;
- un module Sphynx et un module Amon ;
- entre un module Sphynx et un serveur gérant IPsec[p.183].

3. Les services Sphynx

Chaque module EOLE est constitué d'un ensemble de services.

Chacun de ces services peut évoluer indépendamment des autres et fait l'objet d'une actualisation ou d'une intégration par l'intermédiaire des procédures de mise à jour. Ce qui permet d'ajouter de nouvelles fonctionnalités ou d'améliorer la sécurité.

Services communs à tous les modules

- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;
- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO* : gestion de l'authentification centralisée ;
- *Exim4* : serveur de messagerie ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Sphynx

- *Iptables* : filtrage d'adresses IP ;
- *Strongswan* : version libre d'IPSec. Permet la création de réseaux virtuels privés ;
- *ARV* : interface d'administration des réseaux virtuels (VPN) ;
- *Pacemaker* : haute disponibilité ;
- *Quagga* : routage dynamique.

4. Structure des conteneurs

Le module Scribe s'installe par défaut en mode non conteneur[p.180].

La mise en œuvre du mode conteneur pour ce module est possible mais ne fait pas l'objet d'une procédure de qualification.

5. Pré-requis

Le module Sphynx nécessite une machine pourvue de 2 cartes réseau.

Une troisième carte est obligatoire pour l'activation de la haute disponibilité[p.182].

Le module n'utilise que très peu de ressources.

La compatibilité est assurée par strongSwan

Actuellement toutes les versions maintenues du module Sphynx fonctionnent avec toutes les versions maintenues du module Amon et inversement.

La compatibilité du module Sphynx avec les versions du module Amon est dépendante de la compatibilité des versions de strongSwan[p.186] entre elles. Pour le moment, les versions divergent peu.

Pour vérifier cette compatibilité, il est possible de relever les différentes versions de strongSwan intégrées sur les serveurs concernés et de se rendre sur le site du projet strongSwan : https://strongswan.org/.

6. Les différences entre les versions 2.4 et 2.5

Le module Sphynx n'est disponible qu'à partir de la version 2.5.2 d'EOLE.

La nouvelle version du module reproduit les mêmes fonctionnalités (iso-fonctionnel) que la version 2.4. La version 2.5 est basée sur une nouvelle version LTS d'Ubuntu.

Noyau

Cette nouvelle version d'Ubuntu implique également un changement de version du noyau avec de nouvelles prises en charge matériel. Les modules EOLE 2.5 utilisent par défaut le noyau le plus récent de la distribution Ubuntu.

Mise à jour

Sur EOLE 2.5, il n'existe plus qu'un seul niveau de mise à jour, le concept de mise à jour minimale et complète a été supprimé.

Les mises à jour sont automatiques mais peuvent se faire manuellement avec la commande `Maj-Auto`.

Passage à une nouvelle version

L'ajout de nouvelles fonctionnalités entraîne une nouvelle version d'EOLE (2.5.n). Le passage d'une version mineure à une autre est manuel et volontaire.

La commande `Maj-Release` permet de passer à une version mineure plus récente.

Le passage à une nouvelle version d'Ubuntu entraîne une nouvelle version d'EOLE (2.n.n). Le passage d'une version majeure à une autre est manuel et volontaire.

La commande `Upgrade-Auto` permet de passer à une version majeure supérieure.

Commandes

Les commandes `instance`, `reconfigure` et `Maj-Auto` ainsi que la gestion des services ont été réécrites. La commande `diagnose` a été enrichie.

Il n'est plus nécessaire de spécifier le nom du fichier à utiliser pour les commandes `instance` et `reconfigure`.

Un fichier `config.eol.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui-ci permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

Interface de configuration du module

L'interface de configuration du module est basée sur de nouvelles technologies :

- Flask[p.182] ;
- Backbone.js[p.180] et Marionette[p.183] ;
- Tiramisu[p.186].

Elle peut être rendue disponible au travers d'un navigateur web.

Il n'est plus nécessaire de spécifier le nom du fichier à utiliser avec les commandes `gen_config` et `instance`.

Règles pare-feu

La gestion des règles pare-feu ne se fait plus par fichiers `.fw`. Les règles sont maintenant définies dans des dictionnaires XML Creole.

Les flux réseau ne sont plus bloqués en interne (entre le maître et les conteneurs et entre conteneurs).

Tâches planifiées

Sur les modules EOLE, les tâches planifiées (comme par exemple les mises à jour) sont gérées par `eole-schedule`.

En version 2.5, `eole-schedule` est géré depuis Tiramisu[p.186].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML[p.187] Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

Mode conteneur

Pour les modules en mode conteneur il n'est plus possible de personnaliser le réseau des conteneurs avec l'option `-n`.

Pour passer un module en mode conteneur le paquet à installer est `eole-lxc-controller`.

Le mode conteneur utilise dorénavant le service `apt-cacher` pour mettre en cache les paquets Debian. Le service est installé sur le maître et est utilisé par le maître et les conteneurs LXC.

La nouvelle version LXC sur Ubuntu 14.04 entraîne une simplification de la gestion des conteneurs

Changement dans le PATH des commandes

Beaucoup de commandes n'ont plus besoin du chemin absolu pour être exécutées.

Répertoire d'installation du logiciel Nginx

Le répertoire d'installation du logiciel nginx n'est plus `/usr/share/nginx/www/` mais `/usr/share/nginx/html/`

Suppression de la base matériels

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Logiciel de sauvegarde

Sur les modules 2.5 le logiciel Bareos remplace le logiciel Bacula.

La sauvegarde

La sauvegarde EOLE 2.5 permet de faire des sauvegardes déportées sur un module tiers ou sur un autre serveur équipé de la même version de Bareos.

2.5.1

Choix du type de partitionnement à l'installation

Lors de l'installation d'EOLE avec une version supérieure ou égale à 2.5.1, une fenêtre propose de choisir entre un partitionnement manuel ou automatique, ce choix est également proposé sur Eolebase.

2.5.2

Mot de passe au 1er redémarrage après installation

Une fois le système redémarré, comme indiqué par le prompt, vous pouvez ouvrir une session en

console, mais aussi par SSH, avec l'utilisateur **root** et le **mot de passe aléatoire** qui est **affiché**.

Haute disponibilité

La configuration de la haute disponibilité a été simplifiée, des variables spécifiques à ce module ont été ajoutées pour permettre un calcul automatique des variables Pacemaker.

Mode VPN

Le mode VPN database n'est plus supporté et n'est plus disponible sur le module Sphynx. Un serveur Sphynx en mode fichier plat continuera à communiquer avec des serveurs distants configurés en mode database. La transition pourra se faire progressivement.

2.5.2.1

Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI[p.187].

7. Errata 2.5.n

Il n'y a plus qu'un seul niveau de mise à jour qui comportera uniquement les « bugs » critiques et les correctifs de sécurité. Les mises à jour automatiques ne contiennent pas de changement fonctionnel.

Les modifications et ajouts de fonctionnalités font l'objet d'une nouvelle version fonctionnelle (2.X.Y) et la mise à niveau s'effectue avec une procédure automatique distincte de la mise à jour ordinaire.

Quand une correction nécessite une modification sur les template et/ou les dictionnaires, elle n'est pas intégrée aux versions fonctionnelles déjà diffusées en stable afin de préserver l'intégrité des patch effectués par chacun d'entre vous.

Une page d'errata recense des problèmes affectant chacune des versions EOLE 2.5.x. Les dysfonctionnement connus sont corrigés d'une version à une autre d'EOLE.

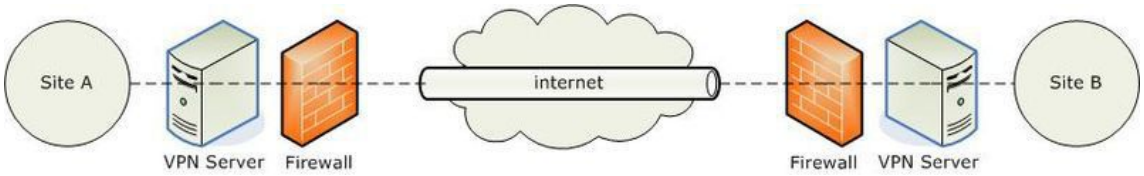
http://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Errata25

Le tableau contient les informations permettant d'appliquer manuellement les correctifs aux versions antérieures à la colonne `Corrigé à partir de`, vous permettant ainsi de les intégrer à vos patch existants si besoin.

Chapitre 2
Fonctionnement du module Sphynx

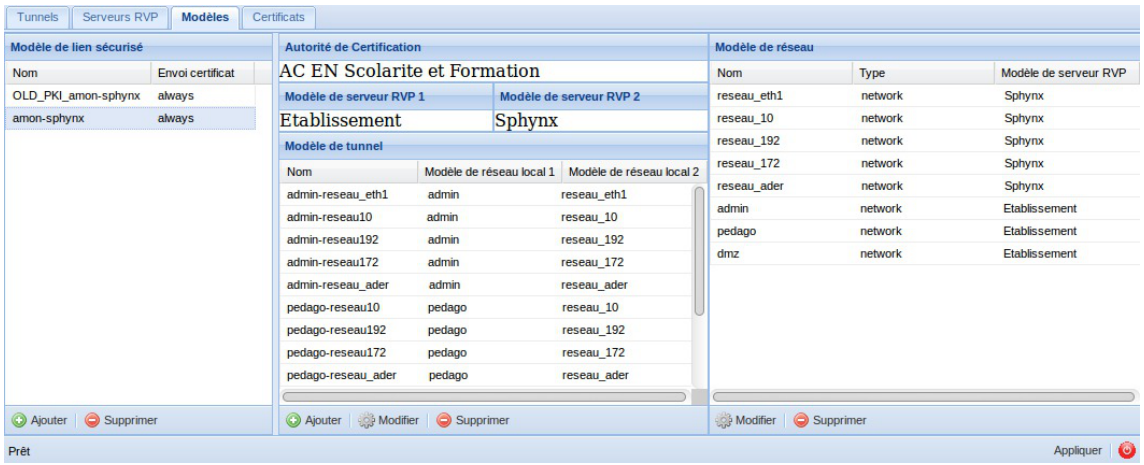
Pour jouer son rôle de concentrateur RVP, le module Sphynx repose sur des projets libres : ARV, iptables, strongSwan, Pacemaker, Corosync[p.181] et Quagga. La haute disponibilité[p.182] et routage dynamique sont activables.

Le concentrateur utilise iptables et strongSwan pour sécuriser et chiffrer les flux réseaux entre plusieurs sites.



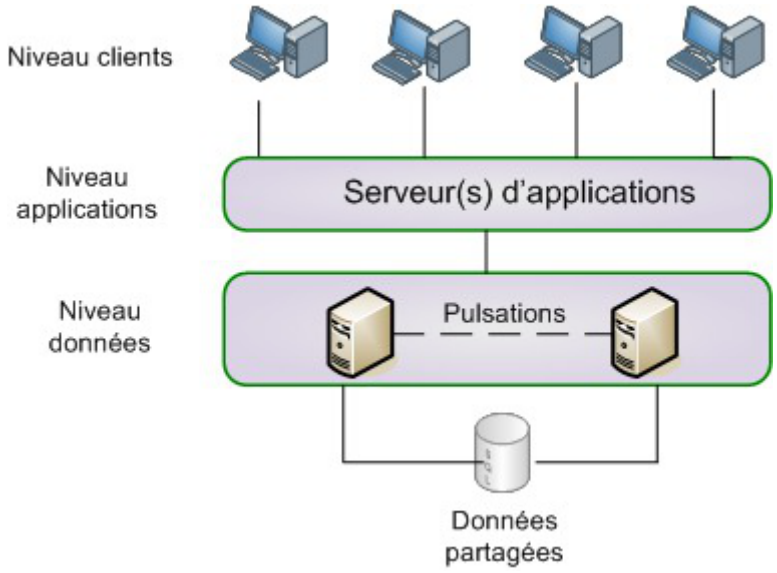
Œuvre placée dans le domaine public par Philippe Belet

Le logiciel ARV permet de modéliser et de générer les configurations IPsec pour strongSwan.



Fenêtre principale d'ARV avec l'onglet Modèles

La haute disponibilité est basée sur l'utilisation des logiciels Pacemaker et Corosync.



Représentation d'un cluster sous licence Creative Commons by-sa

Ce service crée une grappe (cluster[p.180]) de deux serveurs en mode maître/esclave (actif/passif). En cas de panne (tunnel indisponible, passerelle injoignable, serveur hors service) un basculement[p.180] (fail-over) s'opère vers le serveur passif. Le rôle actif/passif change d'un serveur à l'autre lors d'un basculement.

Le routage dynamique avec Quagga permet d'éviter de renseigner l'origine d'un paquet IP dans une trame réseau. Cela permet de ne pas remplir les tables de routage sur des routeurs supportant ce protocole. L'utilisation du routage dynamique a des avantages et des inconvénients :

- avantages
  - maintenance réduite ;
  - modularité et flexibilité accrue.
- désavantages
  - consomme de la bande passante ;
  - la diffusion automatique de message sur le réseau peut constituer un problème de sécurité ;
  - le traitement des messages réseau et le calcul des meilleures routes à emprunter représentent une consommation de CPU et de RAM supplémentaire.

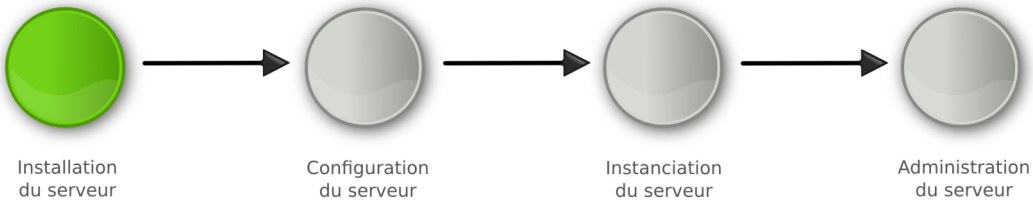
Pour en savoir plus sur les avantages et désavantages des routage statique et dynamique :

http://www.it-connect.fr/routage-statique-et-routage-dynamique/

Chapitre 3

Installation du module Sphynx

La première des quatre phases



Installation

L'installation du module **n'est pas détaillée** dans cette documentation, veuillez vous reporter à la documentation EOLE 2.5, commune aux différents modules, à la documentation sur la mise en œuvre d'un module ou à la documentation complète du module.

- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.182] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (https://pcll.ac-dijon.fr/eole/). Tous les modules installables depuis cette unique image ISO.

  Au démarrage, choisir le module à installer parmi ceux disponibles. Cette phase s'effectue sans aucune question, elle installe les paquets nécessaires, et gère la reconnaissance matérielle des éléments du serveur.

  En cas d'utilisation des conteneurs, il est nécessaire de lancer la commande `gen_conteneurs` lorsque l'installation est terminé et que le serveur a redémarré.

Après l'installation du module Sphynx, la mise à jour n'est pas obligatoire mais fortement recommandée.

Mise à jour

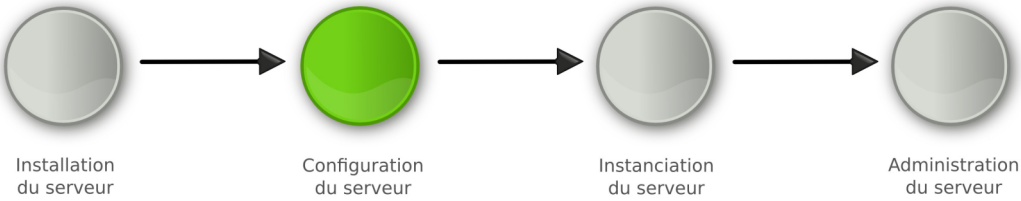
Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto` .

Mise à jour dans le cas d'un module en mode conteneur

Le mode conteneur utilise dorénavant le service `apt-cacher` pour mettre en cache les paquets Debian. Le service est installé sur le maître et est utilisé par le maître et les conteneurs LXC.

Chapitre 4

Configuration du module Sphynx



Configuration

Les généralités sur la configuration **ne sont pas traitées** dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module.

- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config`.

  Cet outil permet de renseigner et de stocker en un seul fichier (`config.eol`) tous les paramètres nécessaires à l'utilisation du serveur dans son environnement (l'adresse IP de la carte eth0 est un exemple de paramètre à renseigner). Ce fichier sera utilisé lors de la phase d'instanciation.

  Suivant les modules, le nombre de paramètres à renseigner est plus ou moins important.

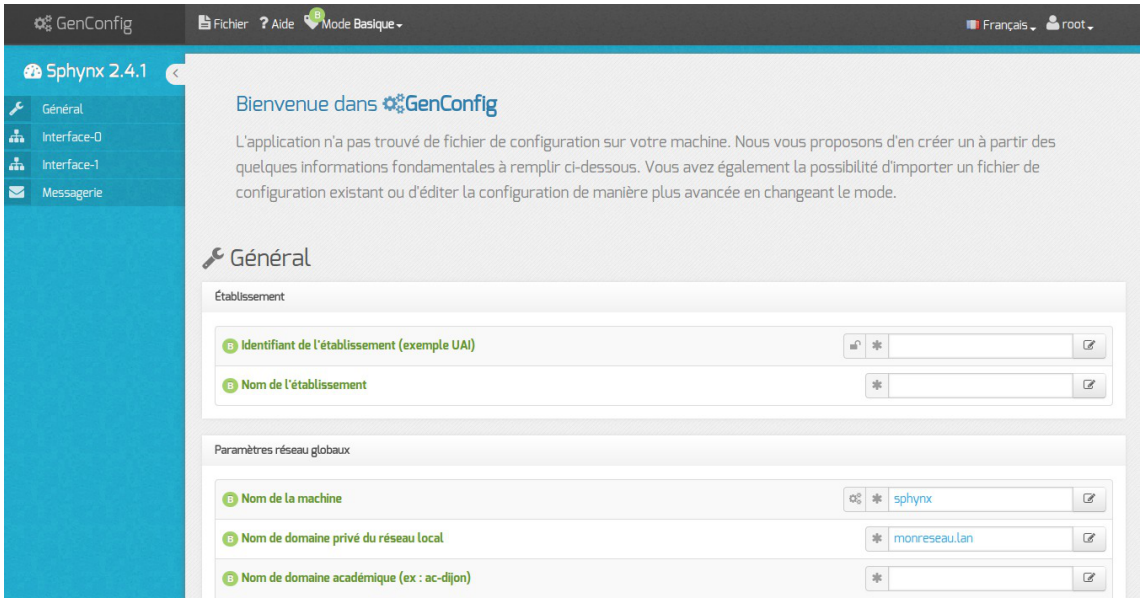
  Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid[p.186], e2guardian[p.181], etc.

1. Configuration en mode basique

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Sphynx :

- `Général` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Messagerie` ;
- `Vpn-pki`.

#fixme capture d'écran

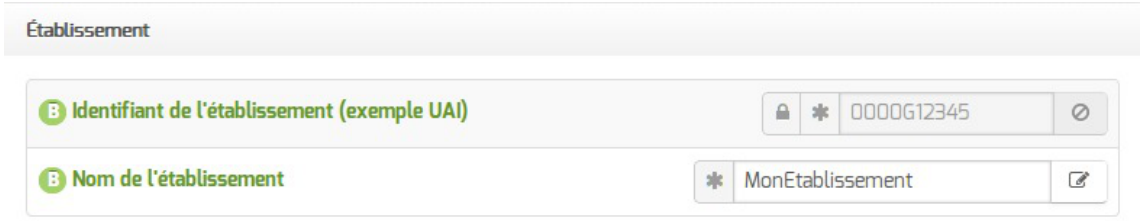


Vue générale de l'interface de configuration du module

1.1. Onglet Général

Présentation des différents paramètres de l'onglet `Général`.

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

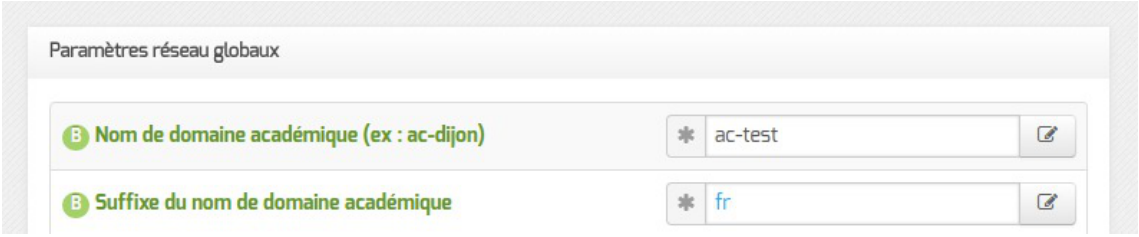
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.183] local, ces variables sont utilisées pour créer l'arborescence.

Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux



En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

> Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.
>
> Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

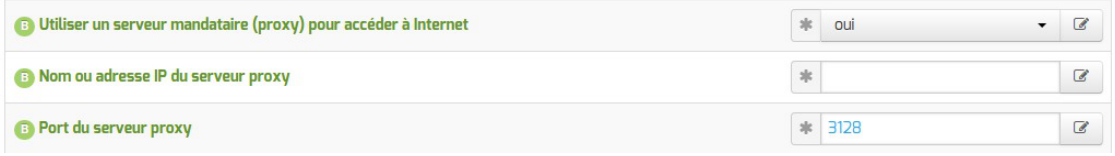
C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

> Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

> L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.



Il devient alors possible de saisir la configuration du serveur proxy :

- nom de domaine ou adresse IP du serveur proxy ;

- le port du proxy.

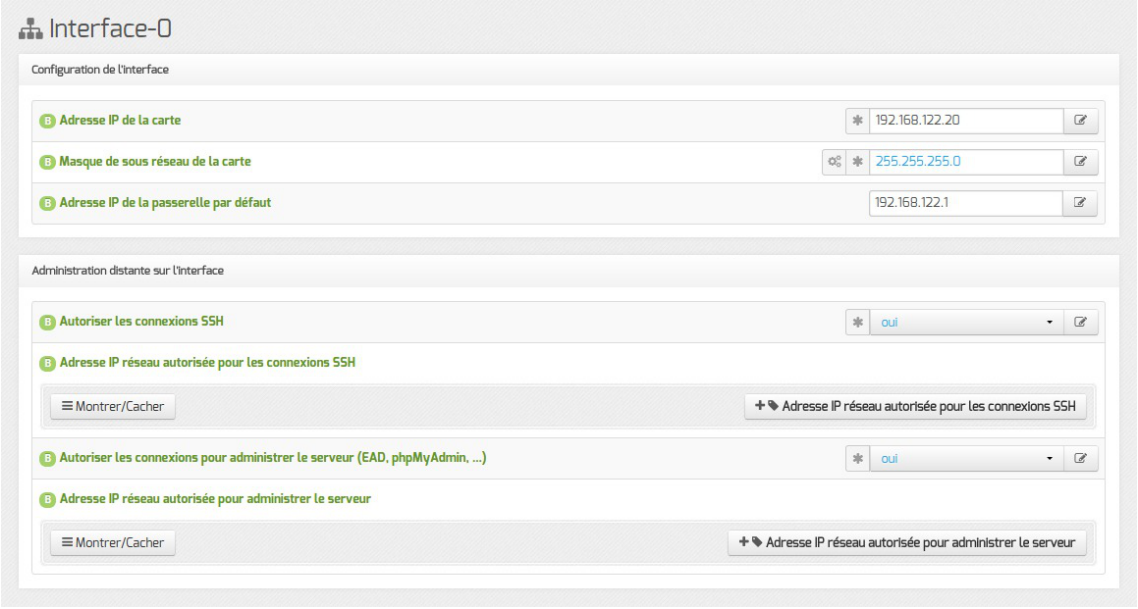
DNS et fuseau horaire

La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.181].

La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

1.2. Onglet Interface-0

Présentation des différents paramètres de l'onglet `Interface-0`.

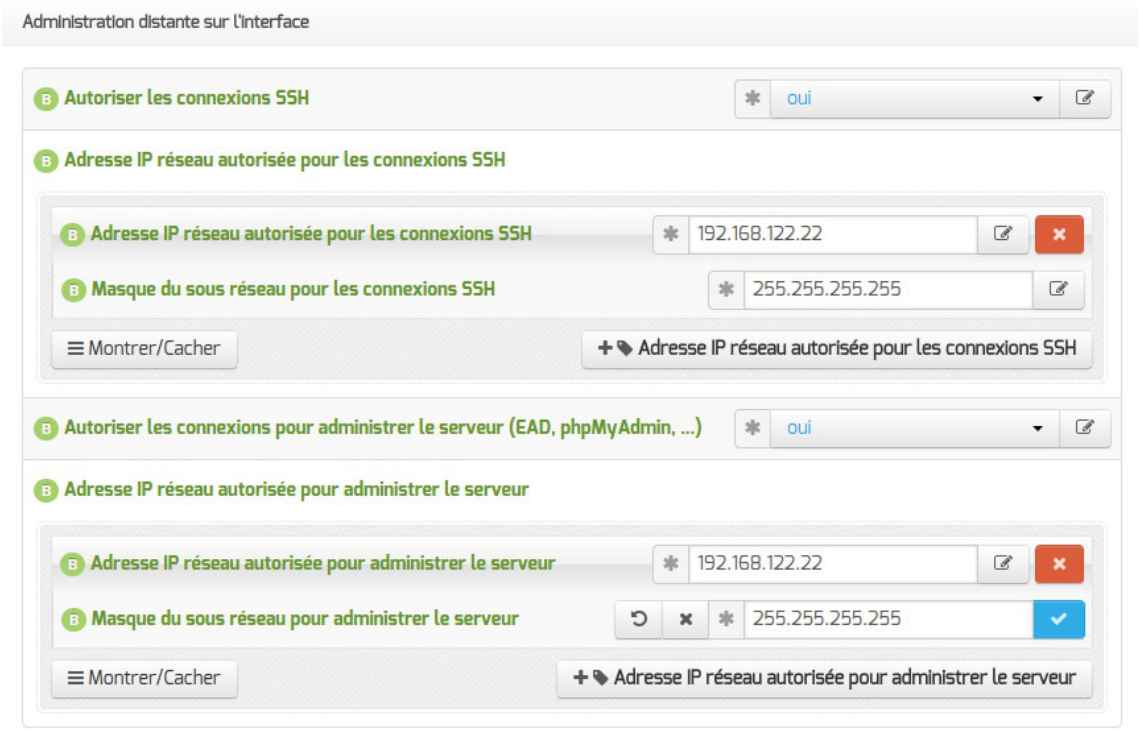


Vue de l'onglet Interface-n

Configuration de l'interface

L'interface 0 nécessite un adressage statique, il faut renseigner l'adresse IP, le masque et la passerelle.

Administration à distance

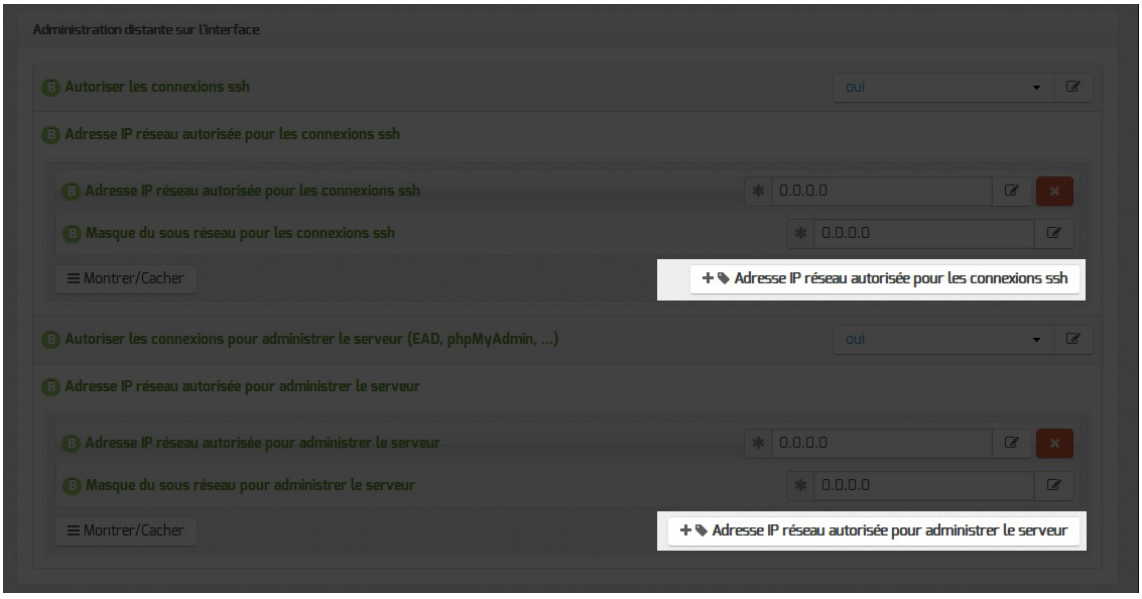


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

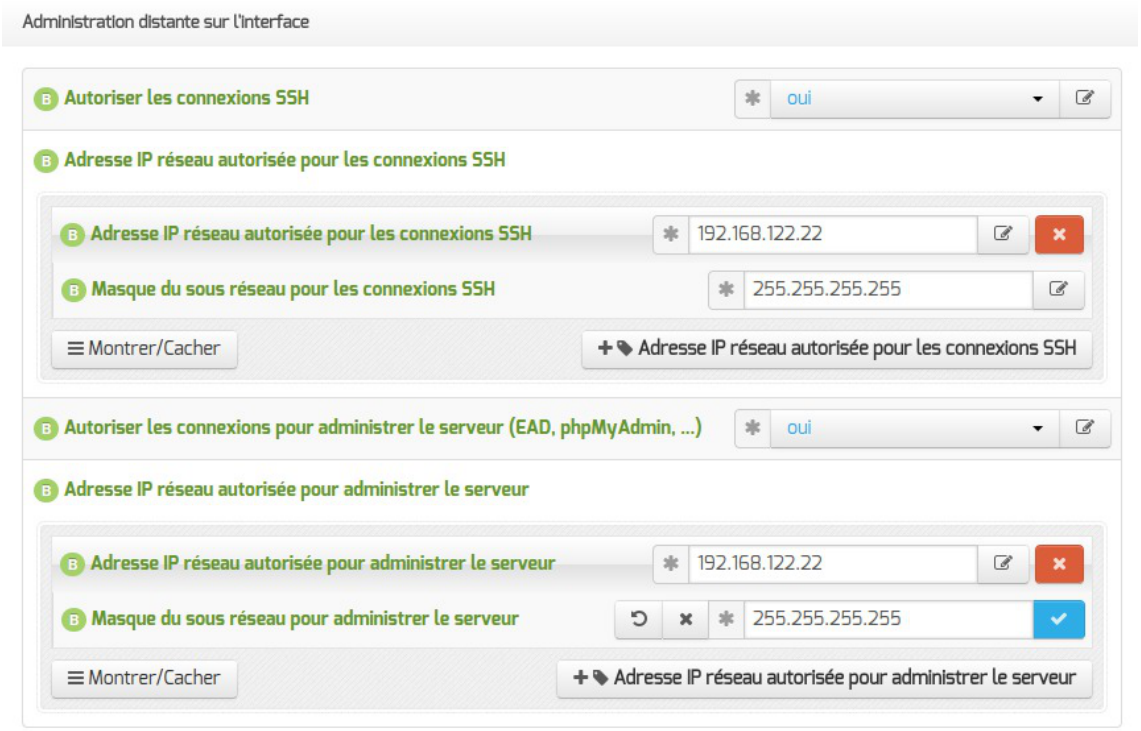
1.3. Onglet Interface-1

Seuls les flux réseaux ayant des connexions VPN déclarées provenant de cette interface seront autorisés à sortir vers eth0 de manière chiffrée.

Configuration de l'interface

L'interface nécessite un adressage statique, il faut renseigner l'adresse IP et le masque de sous réseau.

Administration à distance

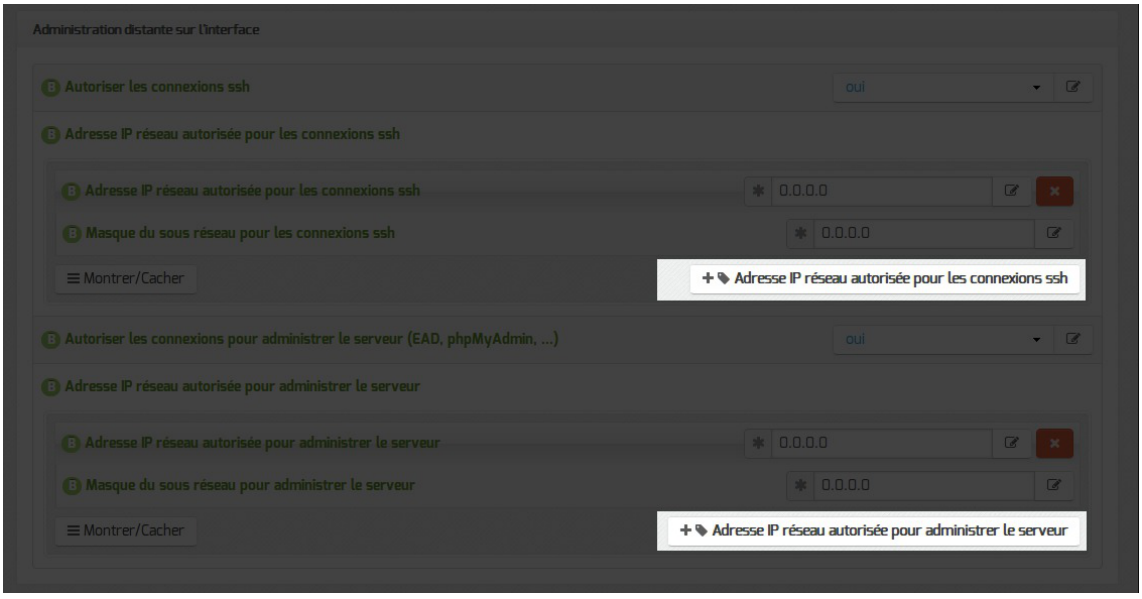


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

1.4. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-` ;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

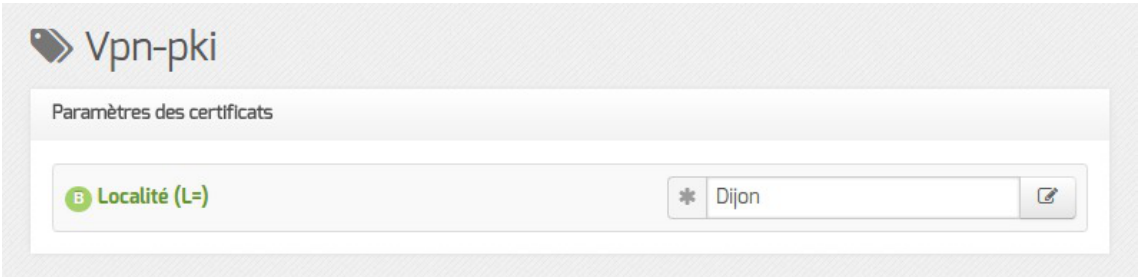
> Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

> Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.
>
> Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.

1.5. Onglet Vpn-pki



Avec la nouvelle PKI PNCN[p.185] il est nécessaire de saisir la localité.

2. Configuration en mode normal

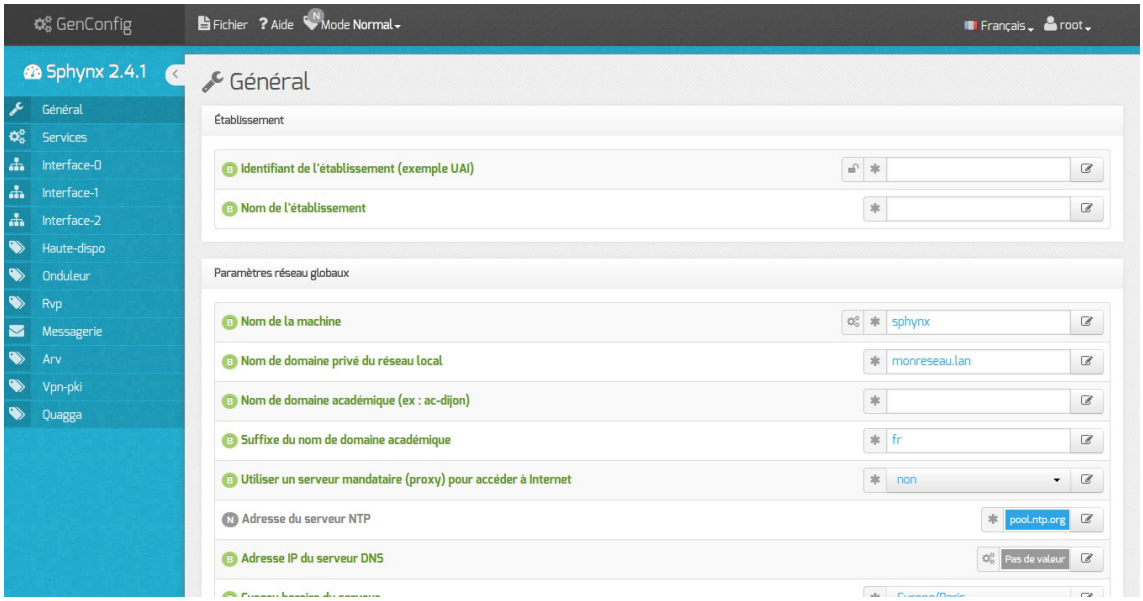
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode normal de l'interface de configuration du module.

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Sphynx :

- `Général` ;
- `Services` ;

- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Interface-2` (configuration de l'interface réseau) * ;
- `Haute-dispo` * ;
- `Onduleur` * ;
- `Messagerie` ;
- `Arv` ;
- `Vpn-pki` ;
- `Quagga` *.

Certains des onglets ne sont disponibles qu'après activation du service dans l'onglet `Services` et sont marqués avec une * dans la liste ci-dessus.

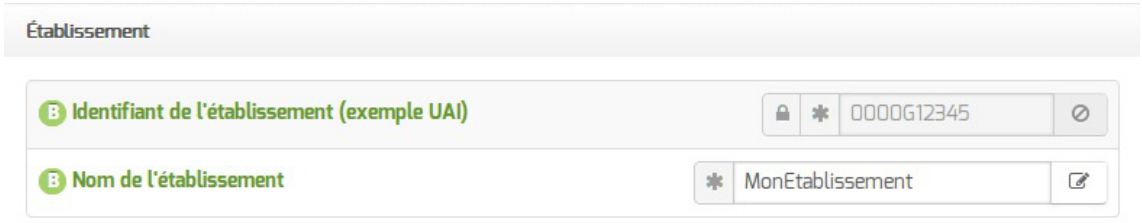


Vue générale de l'interface de configuration du module

2.1. Onglet Général

Présentation des différents paramètres de l'onglet `Général`.

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.183] local, ces variables sont utilisées pour créer l'arborescence.

Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux

En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

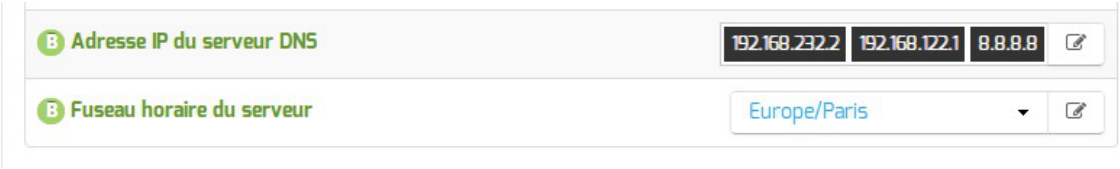
Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Il devient alors possible de saisir la configuration du serveur proxy :

- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.

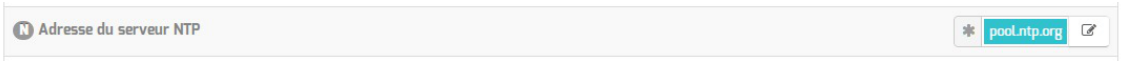
DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.181].

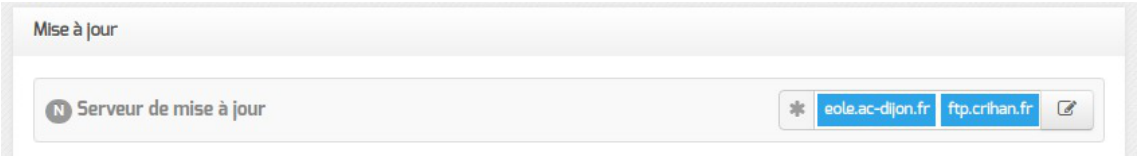
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.184]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour



Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Voir aussi...

> Les différents types de mises à jour

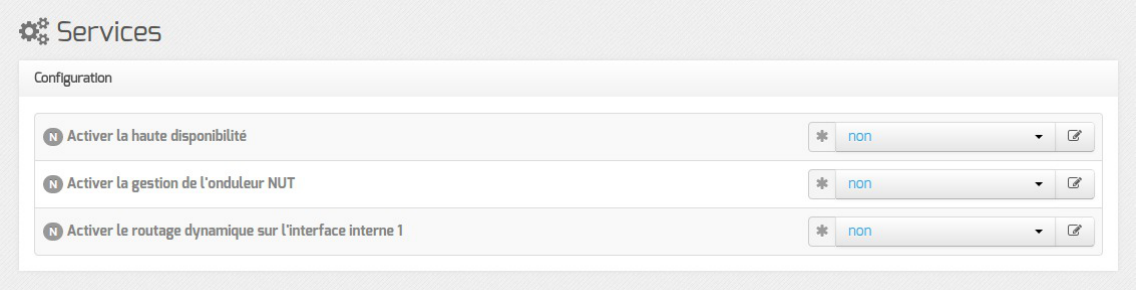
2.2. Onglet Services

L'onglet `Services` permet d'activer et de désactiver une partie des services proposés par le module.

Suivant le module installé et le mode utilisé pour la configuration, la liste des services activables ou désactivables est très différente.

Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un onglet de configuration propre au service.

En mode normal la liste des services activables ou désactivables est courte.



Vue de l'onglet Services du module Sphynx en mode normal

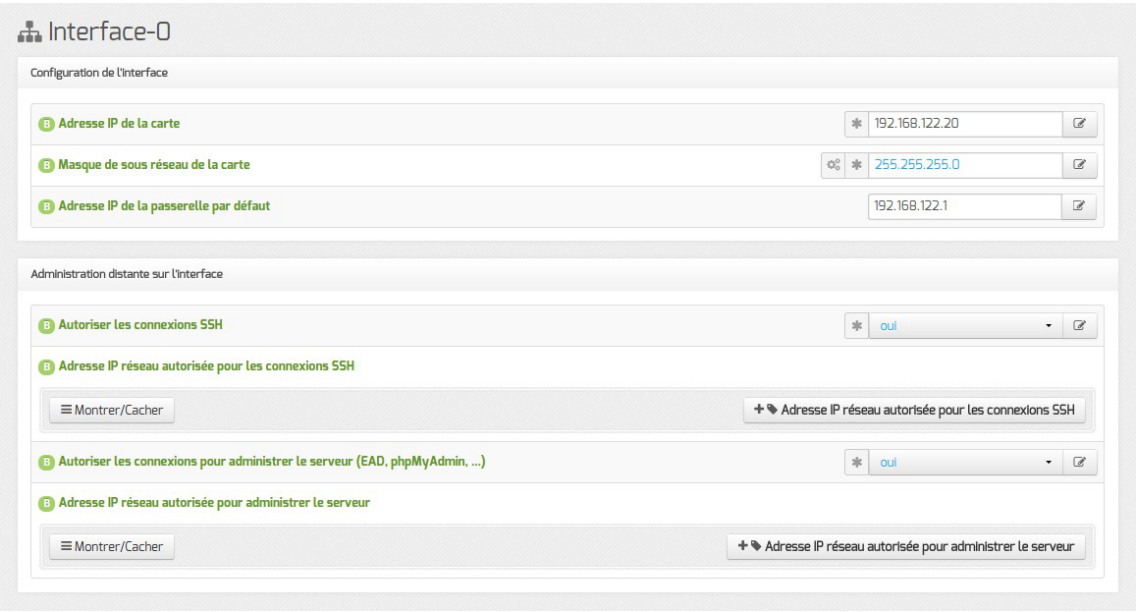
Le service de gestion des onduleurs est commun à tous les modules.

Les services de base propres au module Sphynx sont les suivants :

- la haute disponibilité ;
- le routage dynamique avec le logiciel Quagga[p.185].

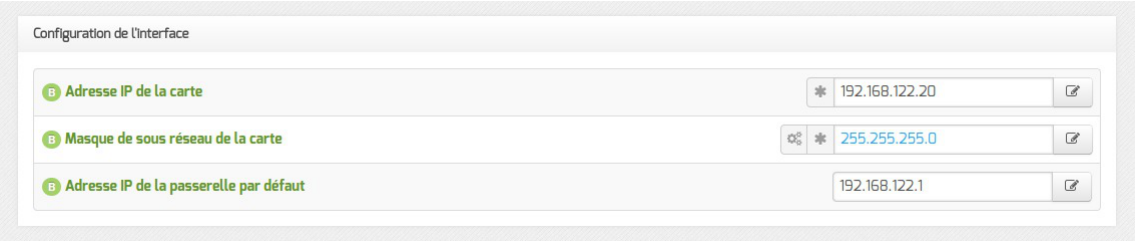
2.3. Onglet Interface-0

Présentation des différents paramètres de l'onglet `Interface-0`.



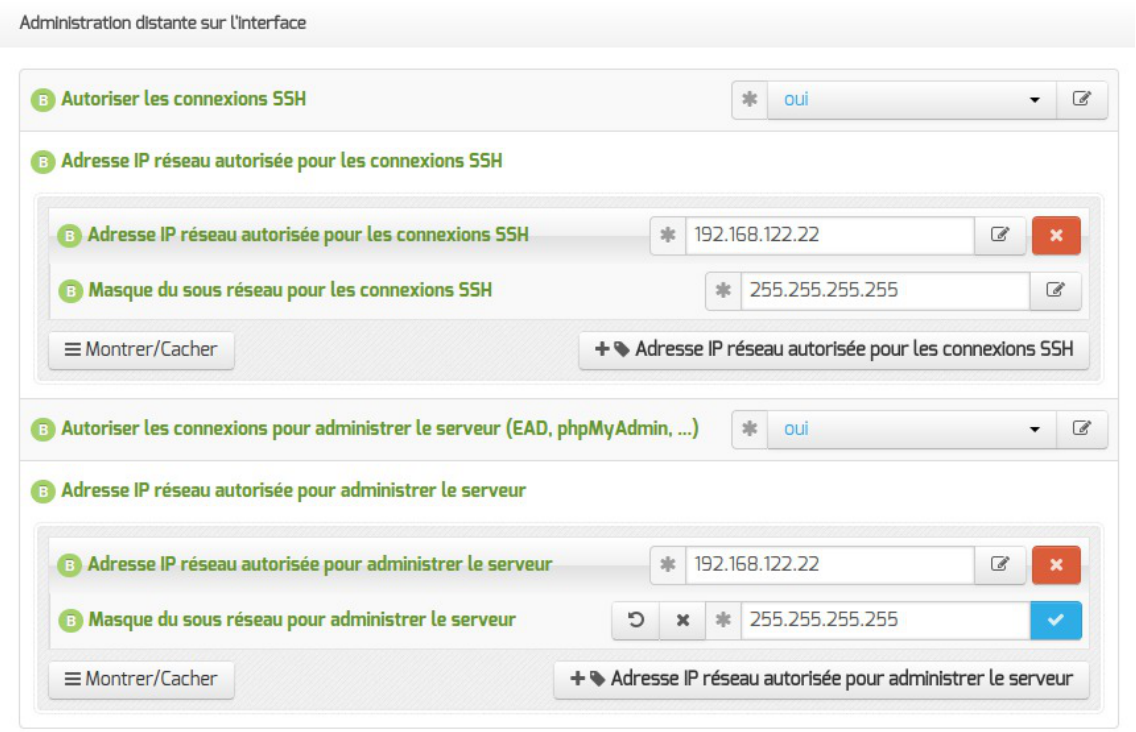
Vue de l'onglet Interface-n

Configuration de l'interface



L'interface 0 nécessite un adressage statique, il faut renseigner l'adresse IP, le masque et la passerelle.

Administration à distance

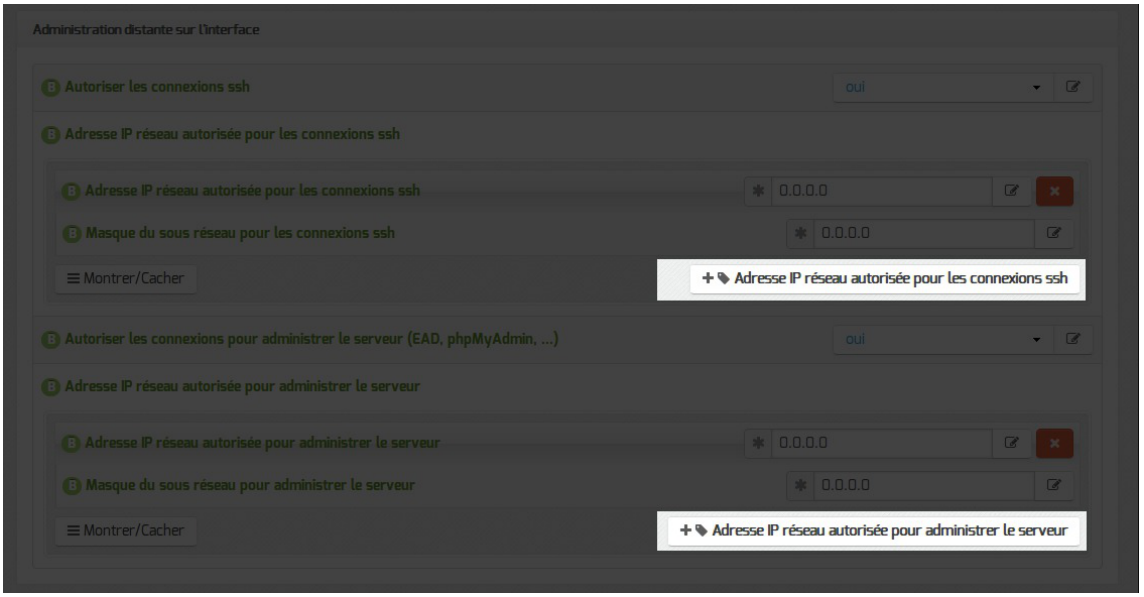


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

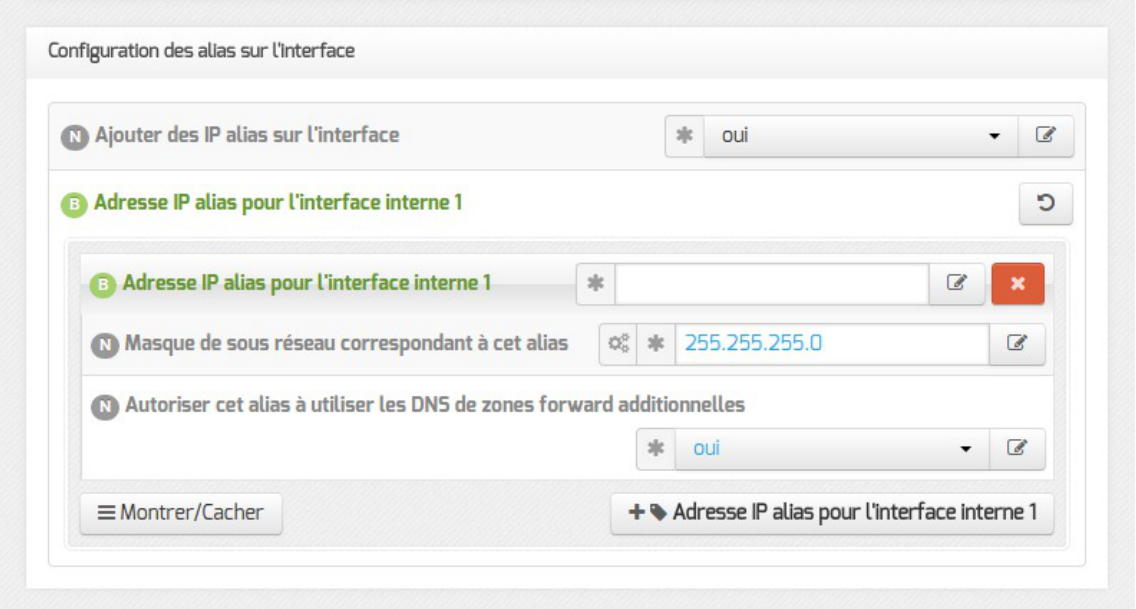
Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



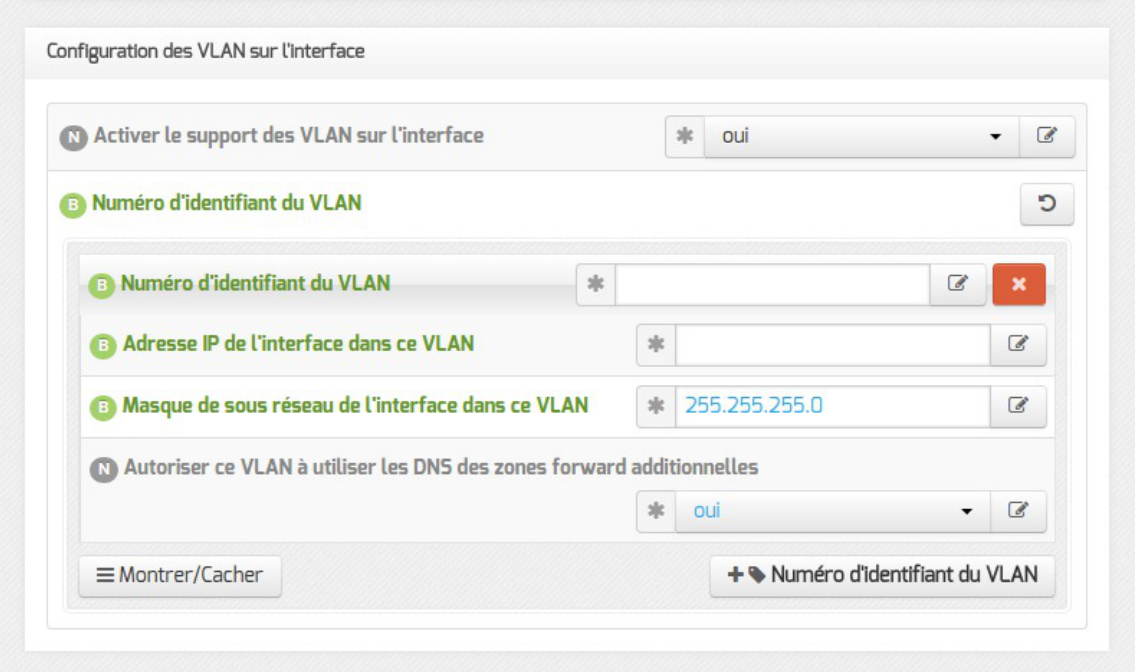
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

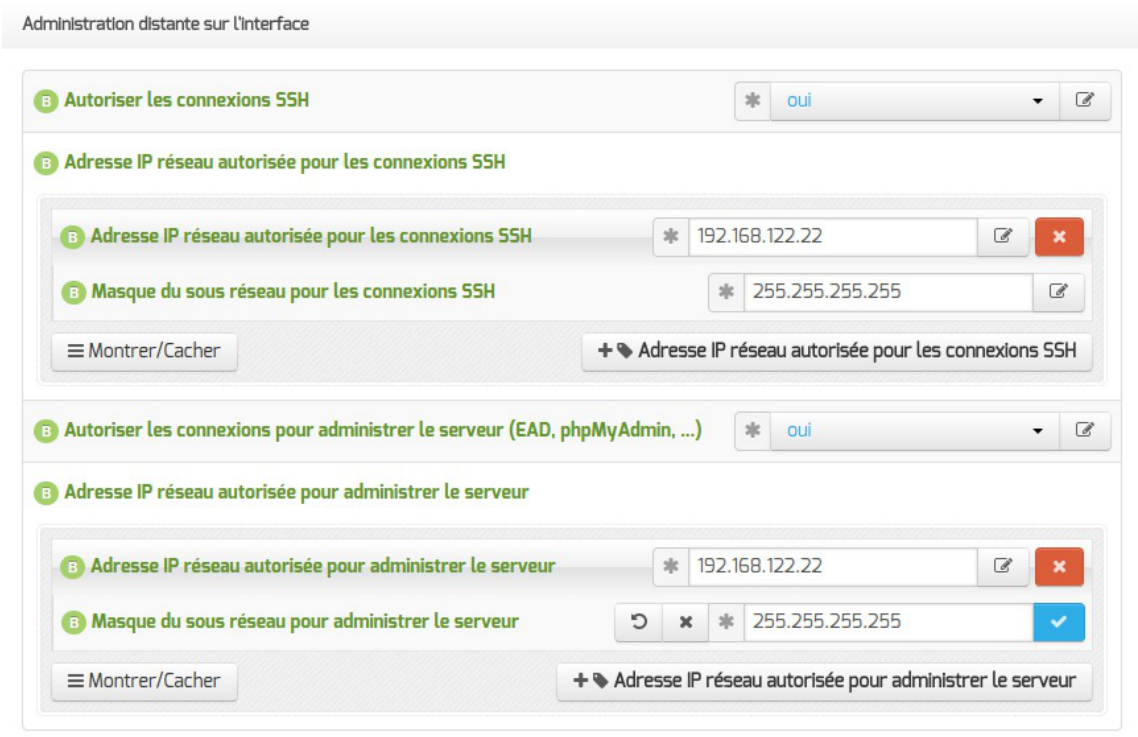
2.4. Onglet Interface-1

Seuls les flux réseaux ayant des connexions VPN déclarées provenant de cette interface seront autorisés à sortir vers eth0 de manière chiffrée.

Configuration de l'interface

L'interface nécessite un adressage statique, il faut renseigner l'adresse IP et le masque de sous réseau.

Administration à distance

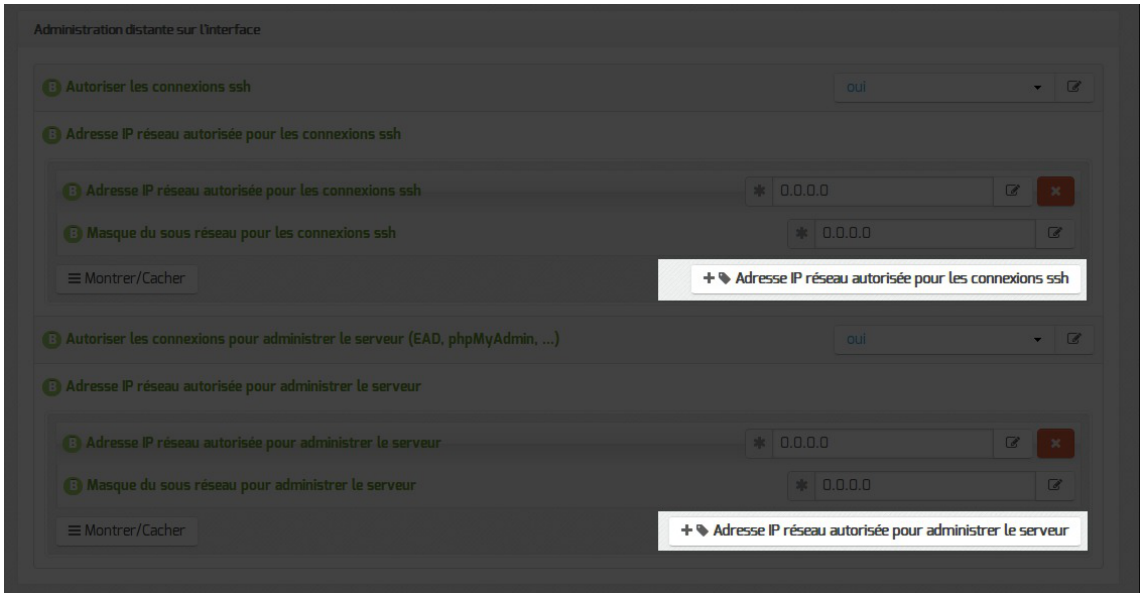


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

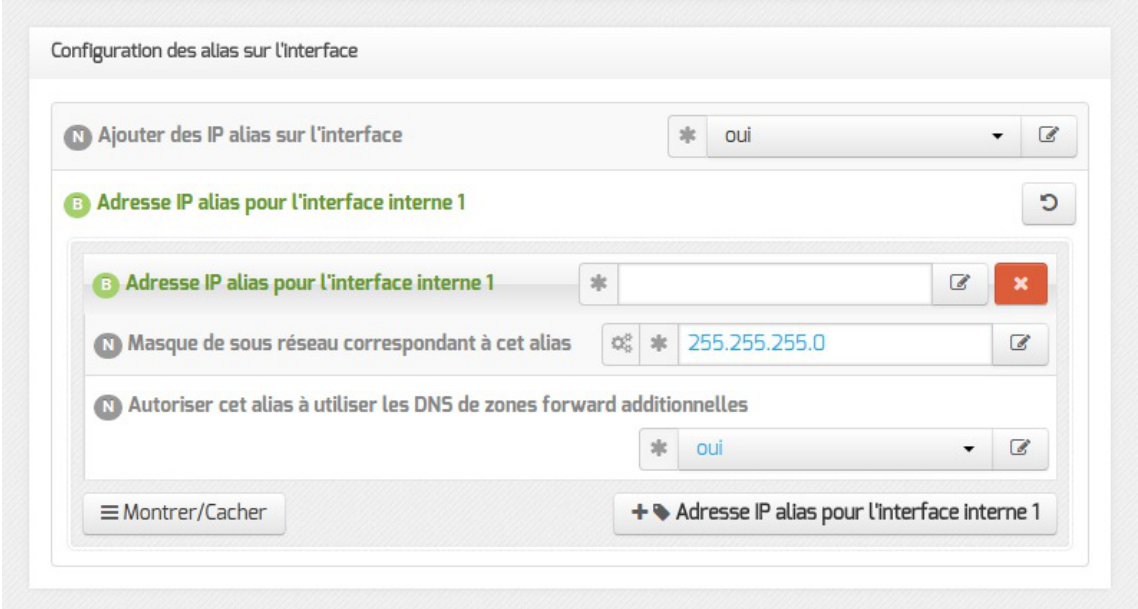
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



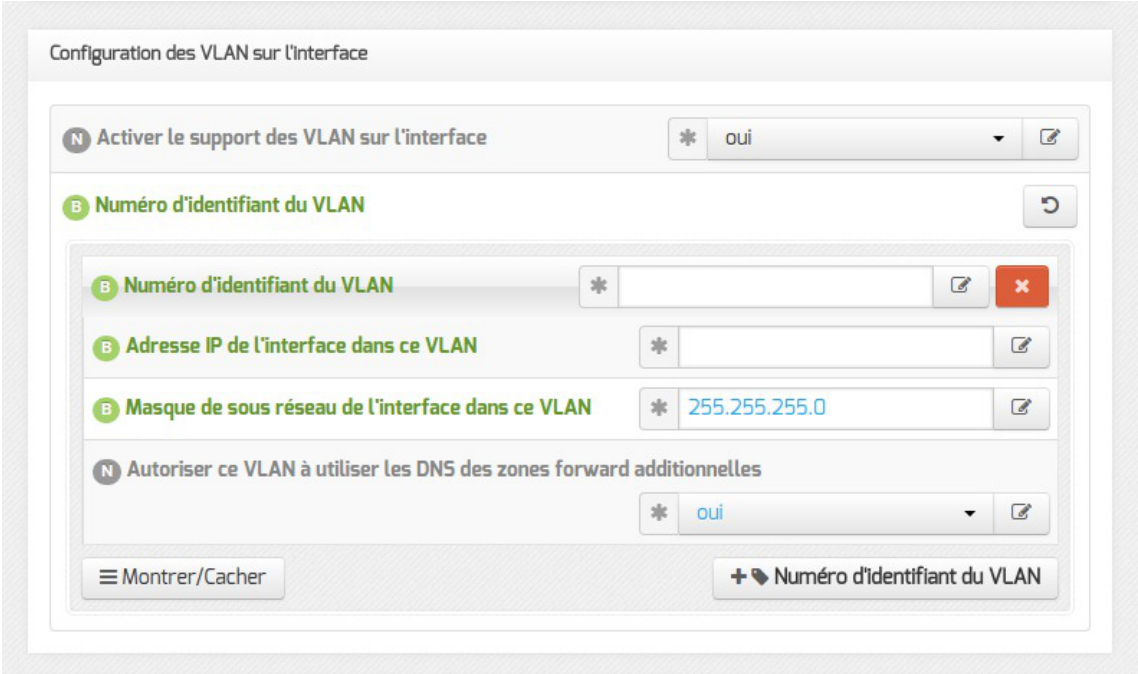
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

2.5. Onglet Interface-2

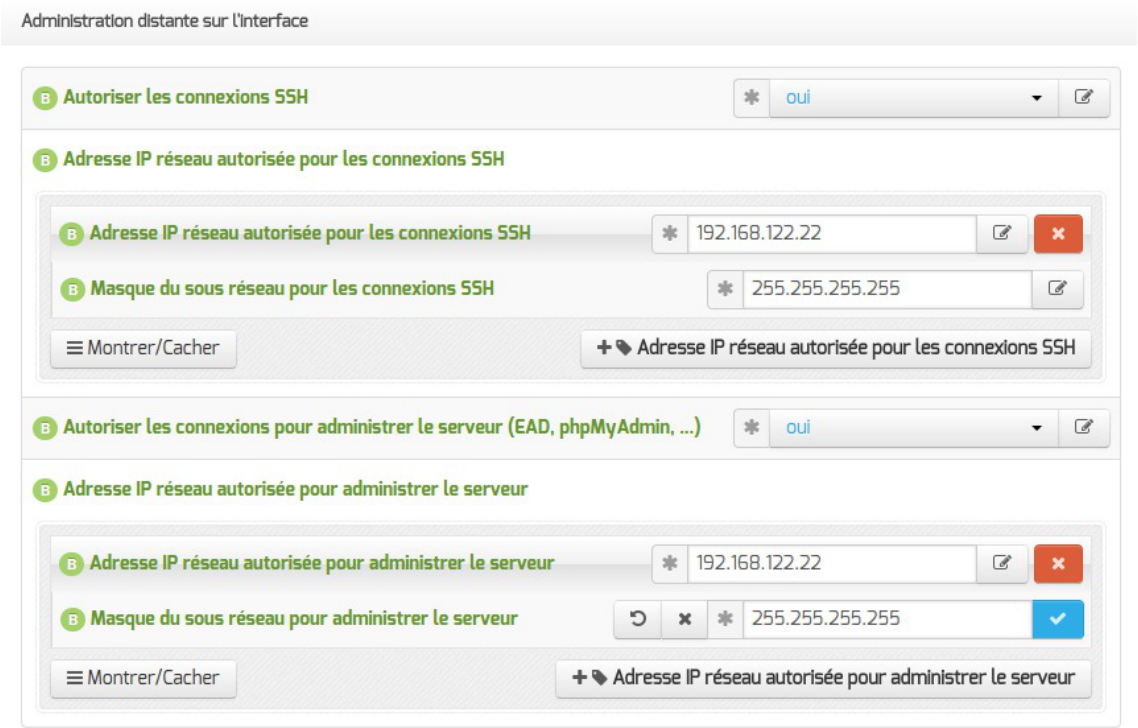
Cette interface est dédiée au dialogue (en multicast[p.183]) entre les nœuds du cluster, aussi onglet `Interface-2` n'est disponible qu'après l'activation de la Haute disponibilité dans l'onglet `Services`.

Il est préférable de réaliser des liaisons physiques directes entre les nœuds.

Configuration de l'interface

L'interface nécessite un adressage statique, il faut renseigner l'adresse IP et le masque de sous réseau.

Administration à distance



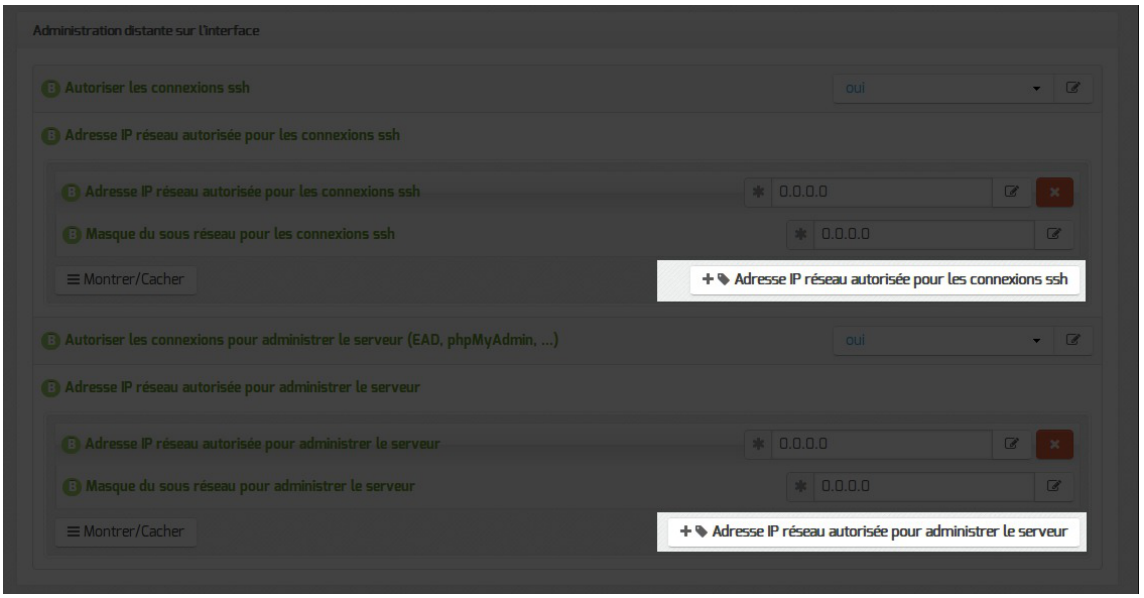
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP

ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

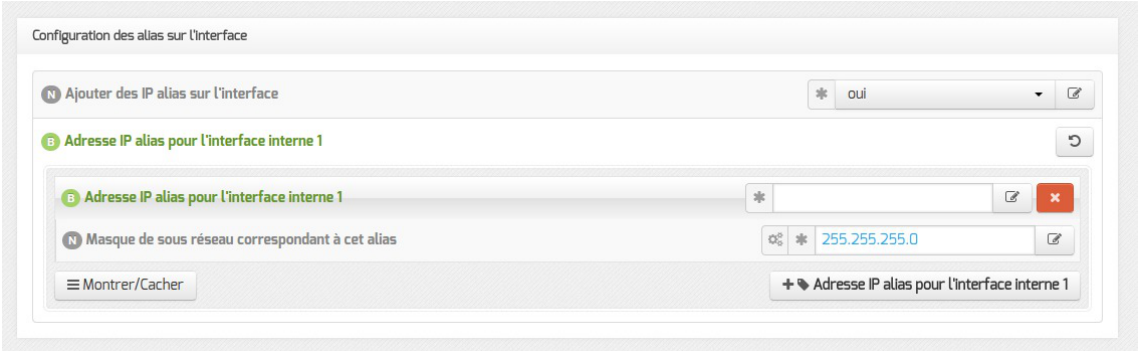
Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

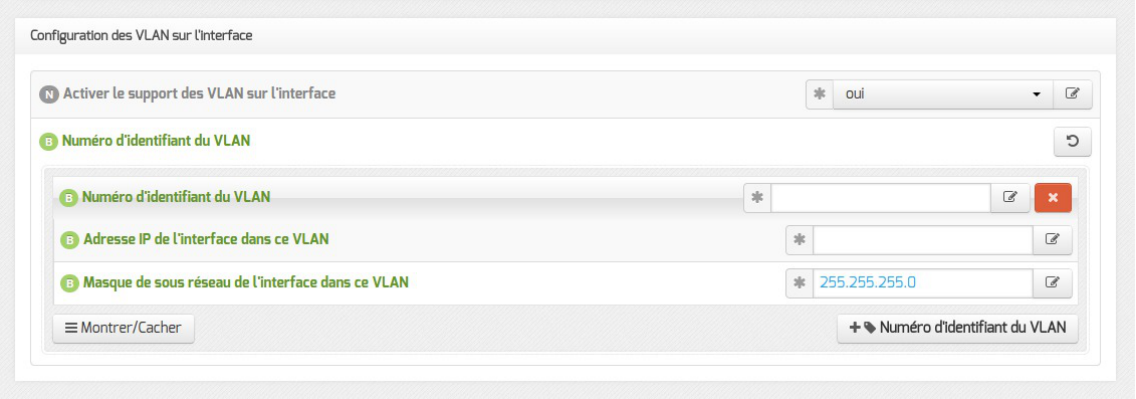
EOLE supporte les alias sur les cartes réseaux. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

Voir aussi...

> Mettre en place un cluster haute disponibilité [p.104]

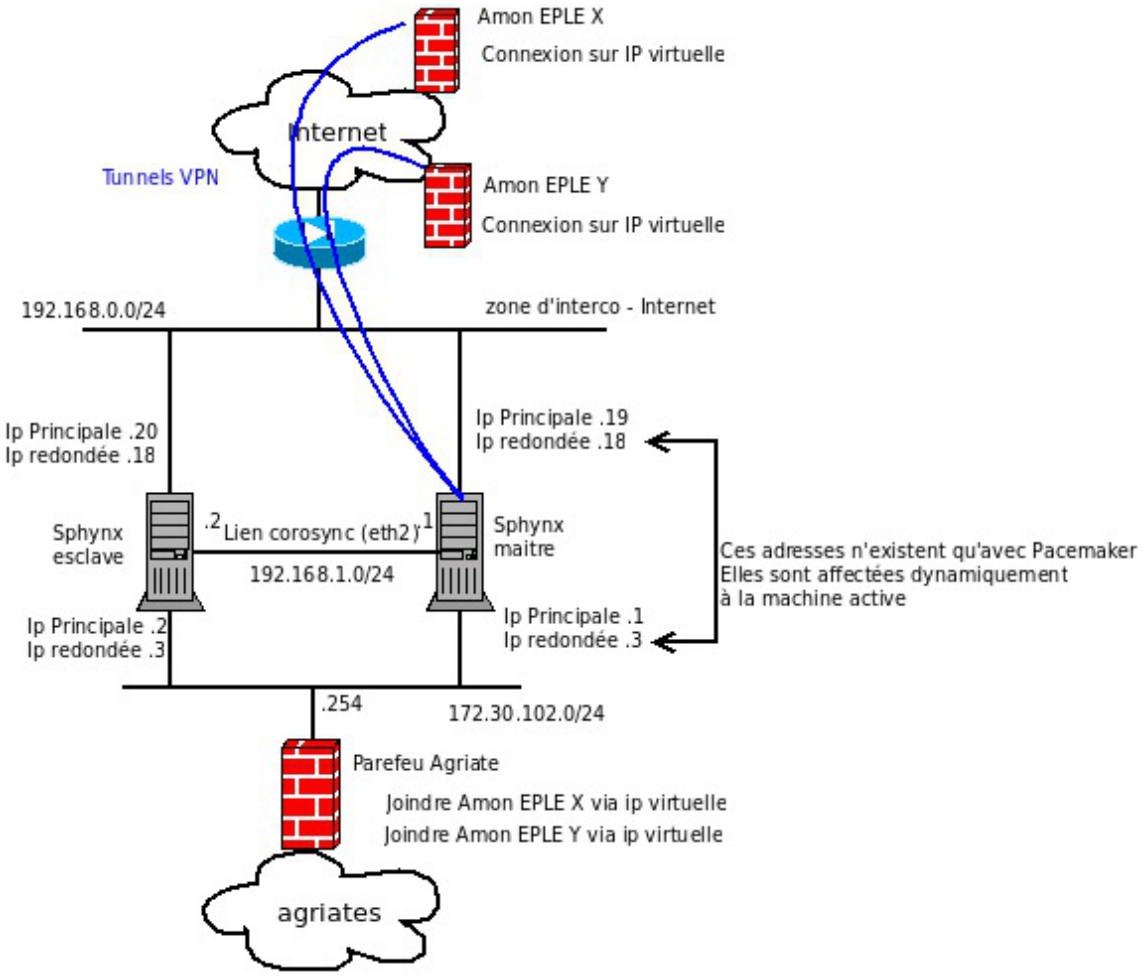
2.6. Onglet Haute-dispo : Configuration de la haute disponibilité

EOLE propose un service de haute disponibilité dont le rôle principal est de garantir la disponibilité d'un service et son bon fonctionnement.

Il est possible, depuis l'interface de configuration du module, d'activer ou non ce service.

Il est préférable de réaliser des liaisons physiques directes entre les nœuds.

Le dialogue entre les nœuds du cluster s'effectue en multicast[p.183].



La génération de la configuration se fait à l'aide du script `appliquer_hautedispo`.

Pacemaker permet de faire un cluster[p.180] de machines en Haute disponibilité[p.182], dans notre cas l'implémentation du logiciel permet un cluster de deux machines (maître/esclave ou actif/passif). Chaque machine est un nœud du cluster.

Il est recommandé d'utiliser une interface réseau dédiée pour le dialogue inter nœud.

Activer le service de haute disponibilité

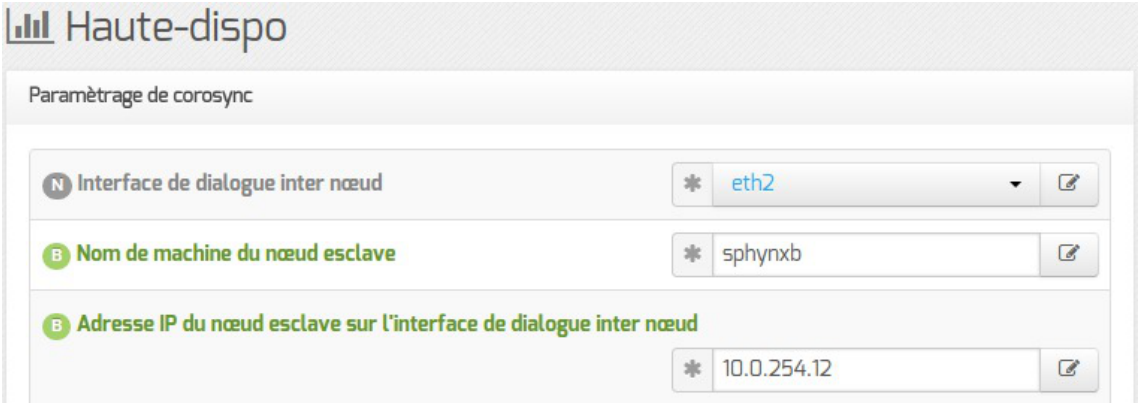
Pour activer le service de haute disponibilité il faut se rendre dans l'onglet `Services` et passer la variable `Activer la haute disponibilité` à `maitre` ou `esclave` selon ce que vous souhaitez mettre en place.

Vue de l'onglet Services

Il faut ensuite paramétrer le service de haute disponibilité dans l'onglet `Haute-dispo`.

La haute disponibilité en temps que maître

Paramétrage de corosync



Sur le module Sphynx l'interface `Interface de dialogue inter nœud` est prédéfinie sur `eth2`.

Il n'est pas nécessaire de changer cette valeur.

Sur Eolebase on peut choisir une interface dédiée au dialogue inter nœud.

Le `Nom de machine du nœud maitre` doit contenir le `Nom de la machine` configuré renseigné sur le nœud esclave.

`Adresse IP du nœud esclave sur l'interface de dialogue inter nœud` permet de saisir l'adresse IP du nœud esclave.

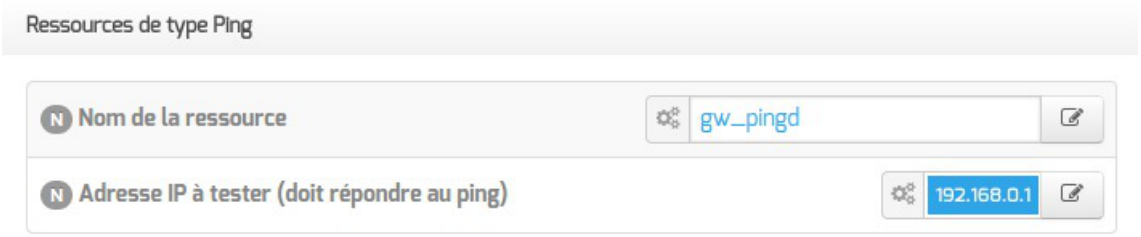
> Le `Nom de machine du nœud esclave` et l'`Adresse IP du nœud esclave sur l'interface de dialogue inter nœud` permettent de renseigner le fichier `hosts` du module.

`Activer l'envoi de courrier électronique lors d'une bascule de nœud` permet de recevoir une alerte lorsque les ressources sont basculées d'un nœud à l'autre.

Le `Nom de la ressource mail` est pré-définie et peut être modifié, il apparaît dans les logs et à l'exécution des commandes `crm` et `crm_mon`.

Le champ `Destinataire du courrier électrique` est pré-rempli par la valeur `Adresse électronique recevant les courriers électroniques à destination du compte root` défini dans l'onglet `Messagerie`. Cette valeur, au format adresse électronique, peut être changée si les alertes doivent être envoyées à une autre personne. Il est également possible de choisir le sujet du courrier électronique dans le champ `Sujet du courrier électronique`.

Ressources de type Ping

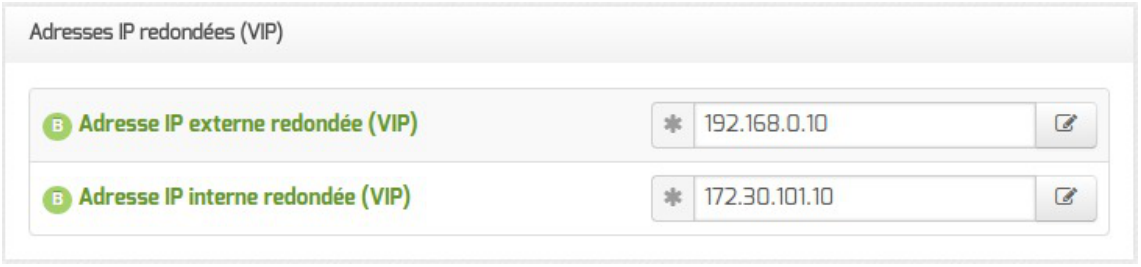


Le `Nom de la ressource` apparaît dans les logs et les commandes `crm` et `crm mon`.

Sur le module Sphynx la valeur `Nom de la ressource` est pré-définie et ne doit surtout pas être modifiée.

Sur Eolebase ce champ peut contenir le nom de votre choix sans espace et sans caractères spéciaux.

Adresses IP redondées (VIP)

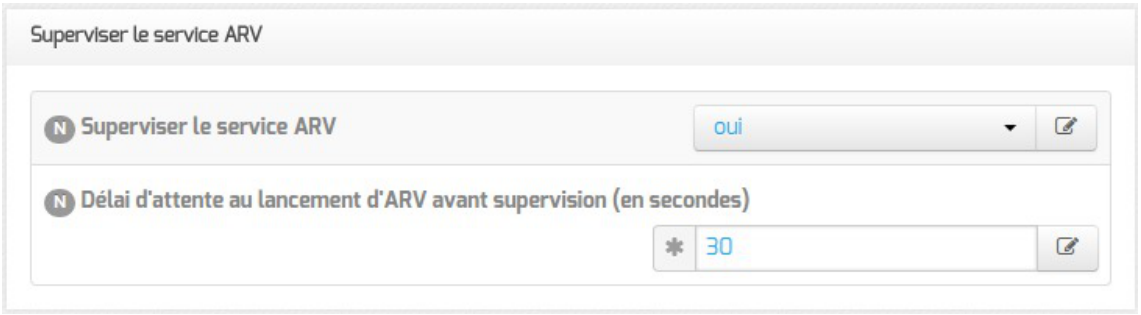


Les adresses IP redondées sont des ressources de type IP virtuelle et permettent à un cluster d'être accessible via cette adresse sur l'un des deux nœuds. Si l'un des nœuds n'est plus accessible, l'autre prend le relais avec cette même adresse IP.

`Adresse IP externe redondée (VIP)` correspond à l'adresse IP virtuelle de l'interface `eth0`.

`Adresse IP interne redondée (VIP)` correspond à l'adresse IP virtuelle de l'interface `eth1`.

Superviser le service ARV



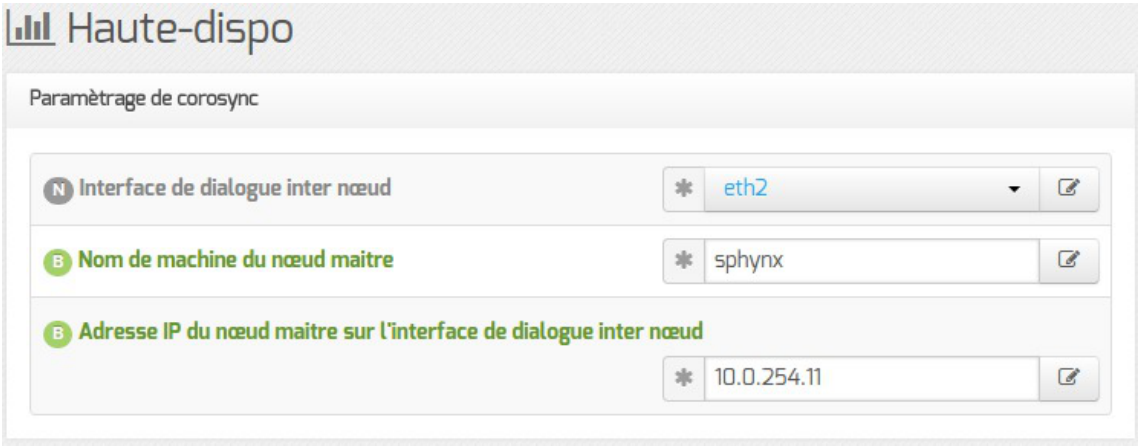
Par défaut la supervision du service ARV est activé.

Le service ARV met un certain temps à se lancer suivant la vélocité de la machine, le délai d'attente permet de différer la supervision du service. Il est également possible de désactiver complétement la supervision en passant `Superviser le service ARV` à `non`.

Sur le module Sphynx la synchronisation des fichiers de configuration sur le nœud esclave est forcée et ne peut pas être modifiée. Elle est visible uniquement en mode Debug.

La haute disponibilité en temps qu'esclave

Paramétrage de corosync



Sur le module Sphynx l'interface `Interface de dialogue inter nœud` est prédéfinie sur `eth2`.

Il n'est pas nécessaire de changer cette valeur.

Le `Nom de machine du nœud maitre` doit contenir le `Nom de la machine` configuré renseigné sur le nœud maître.

`Adresse IP du nœud maitre sur l'interface de dialogue inter node` permet de saisir l'adresse IP du nœud maître.

Le `Nom de machine du nœud maitre` et l'`Adresse IP du nœud maitre sur l'interface de dialogue inter nœud` permettent de renseigner le fichier `hosts` du module.

2.7. Onglet Onduleur

Sur chaque module EOLE, il est possible de configurer votre onduleur.

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.184]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

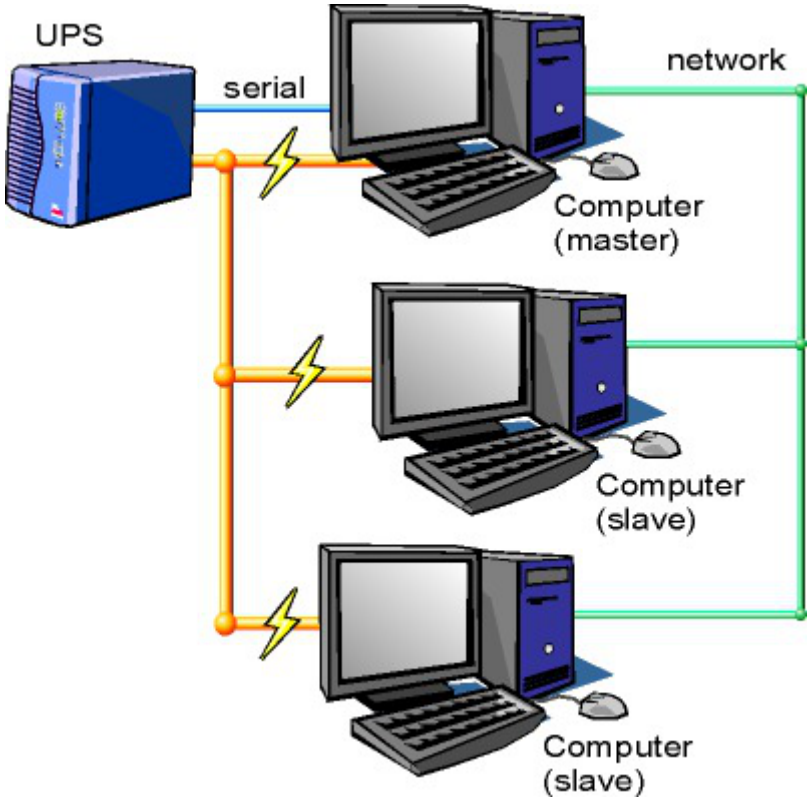


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

http://www.networkupstools.org/stable-hcl.html

Pour connaître la version de NUT qui est installée sur le module :

```
# apt-cache policy nut
```

ou encore :

```
# apt-show-versions nut
```

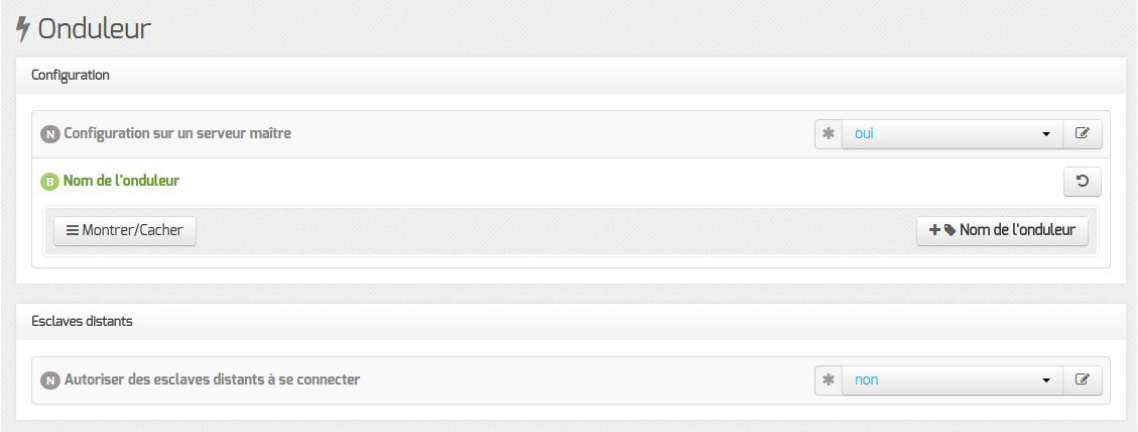
Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

http://www.networkupstools.org/source/2.7/new-2.7.1.txt

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

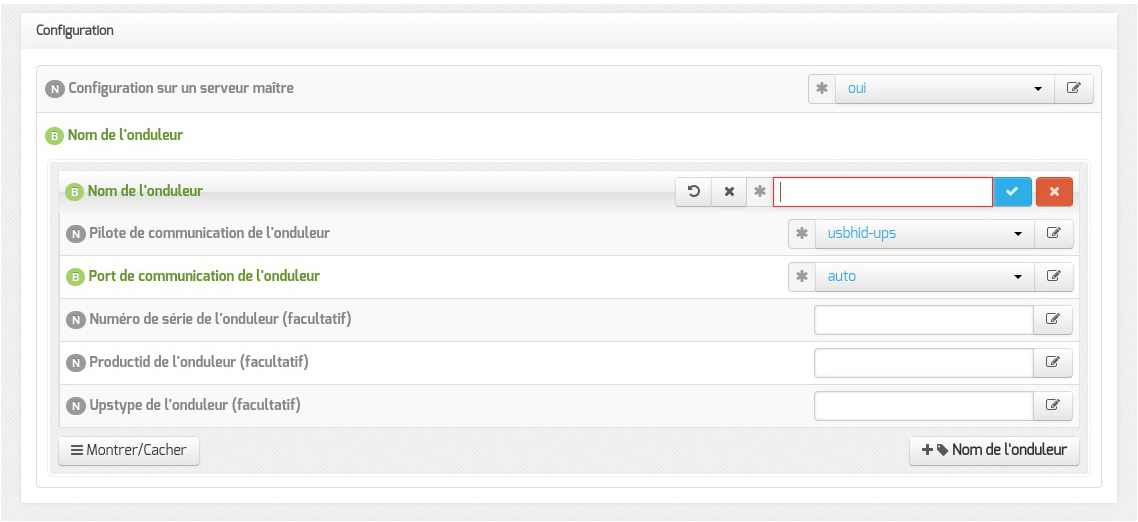
http://www.networkupstools.org/source/2.7/new-2.7.3.txt

L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.



Si l'onduleur est branché directement sur le module il faut laisser la variable `Configuration sur un serveur maître` à `oui`, cliquer sur le bouton `+ Nom de l'onduleur` et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître



Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ `Nom pour l'onduleur`.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante `Pilote de communication de l'onduleur` et éventuellement préciser le `Port de communication` si l'onduleur n'est pas USB.

Les champs `Numéro de série de l'onduleur`, `Productid de l'onduleur` et `Upstype de l'onduleur` sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un

onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost|grep <nom variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;

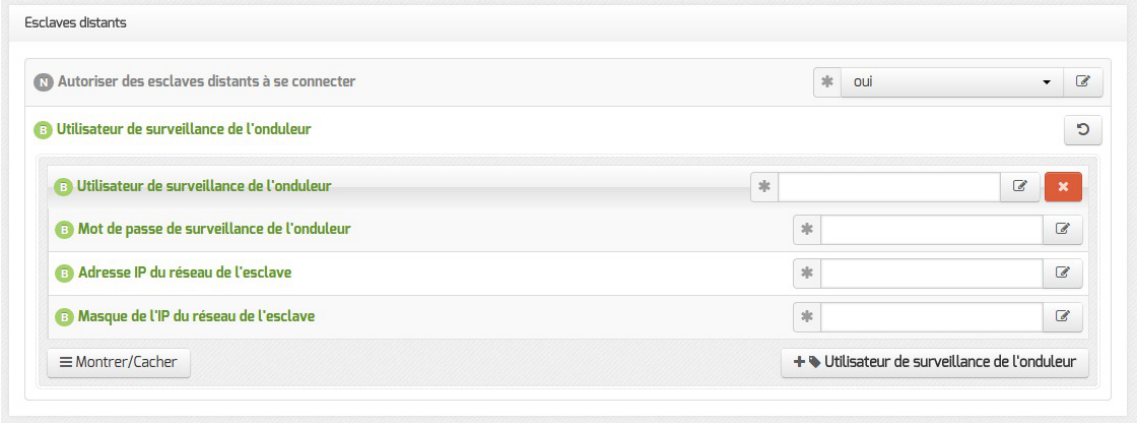
- Port de communication de l'onduleur : `auto`.

La majorité des onduleurs USB sont détectés automatiquement.

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave a se connecter avec cet utilisateur.



Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Chaque utilisateur doit avoir un nom différent.

Les noms `root` et `localmonitor` sont réservés.

Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf`

> ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il est possible de configurer le ou les serveurs esclaves.

Pour configurer le module en tant qu'esclave, il faut activer le service dans l'onglet `Services` puis, dans l'onglet `Onduleur`, passer la variable `Configuration sur un serveur maître` à `non`.

Il faut ensuite saisir les paramètres de connexion à l'hôte distant :

- le `Nom de l'onduleur distant` (valeur renseignée sur le serveur maître) ;
- l'`Hôte gérant l'onduleur` (adresse IP ou nom d'hôte du serveur maître) ;
- l'`Utilisateur de l'hôte distant` (nom d'utilisateur de surveillance créé sur le serveur maître) ;
- le `Mot de passe de l'hôte distant` (mot de passe de l'utilisateur de surveillance créé sur le serveur maître).

Exemple de configuration

Sur le serveur maître :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto` ;
- Utilisateur de surveillance de l'onduleur : `scribe` ;
- Mot de passe de surveillance de l'onduleur : `99JJUE2EZOAI2IZI10IIZ93I187UZ8` ;
- Adresse IP du réseau de l'esclave : `192.168.30.20` ;
- Masque de l'IP du réseau de l'esclave : `255.255.255.255`.

Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;

- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

2.8. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-` ;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

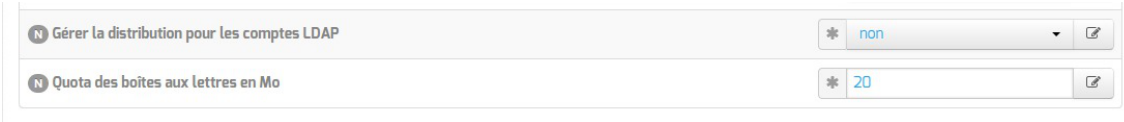
Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.

En mode normal il est possible de configurer le nom de l'émetteur des messages pour le compte `root`.

Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.



Passer `Gérer la distribution pour les comptes LDAP` à `oui` active les transports LDAP pour la distribution des courriers électroniques, la distribution des courriers locaux est forcée ainsi ils ne sont pas mis en queue et supprimés une semaine plus tard.

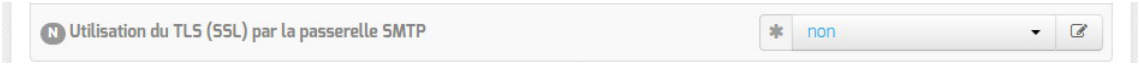
Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.

Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.



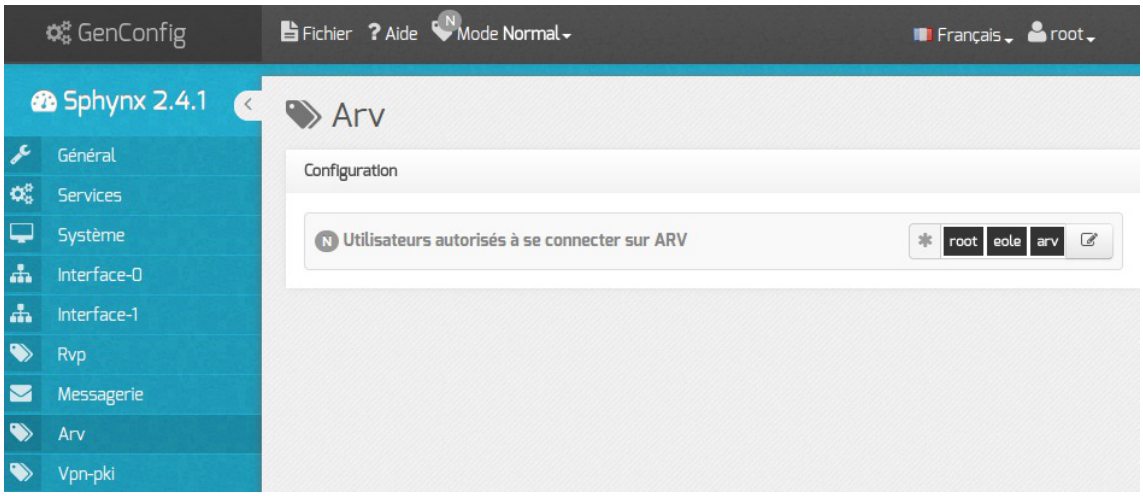
`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.187] pour l'envoi de message. Si la passerelle SMTP[p.186] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.186] (port 25) ou non (port 465).

2.9. Onglet Arv : Configuration du logiciel ARV

ARV est une application qui permet de construire des modèles et de générer des configurations RVP[p.185] pour strongSwan[p.186] [http://www.strongswan.org/ -].

Les utilisateurs autorisés à se connecter sur ARV peuvent être des comptes systèmes locaux et des comptes Zéphir.

Pour qu'un compte puisse avoir accès à ARV, il faut impérativement les déclarer dans l'interface de configuration du module.



Gestion des utilisateurs autorisés à se connecter sur ARV

Les comptes Zéphir doivent avoir les droits en `Lecture` et `Configuration vpn`.

Voir aussi...

L'application ARV [p.111]

2.10. Onglet Vpn-pki

Sphynx fonctionne aussi bien avec des certificats auto-signés qu'en mode certificats signés pour le réseau AGRIATES[p.178].

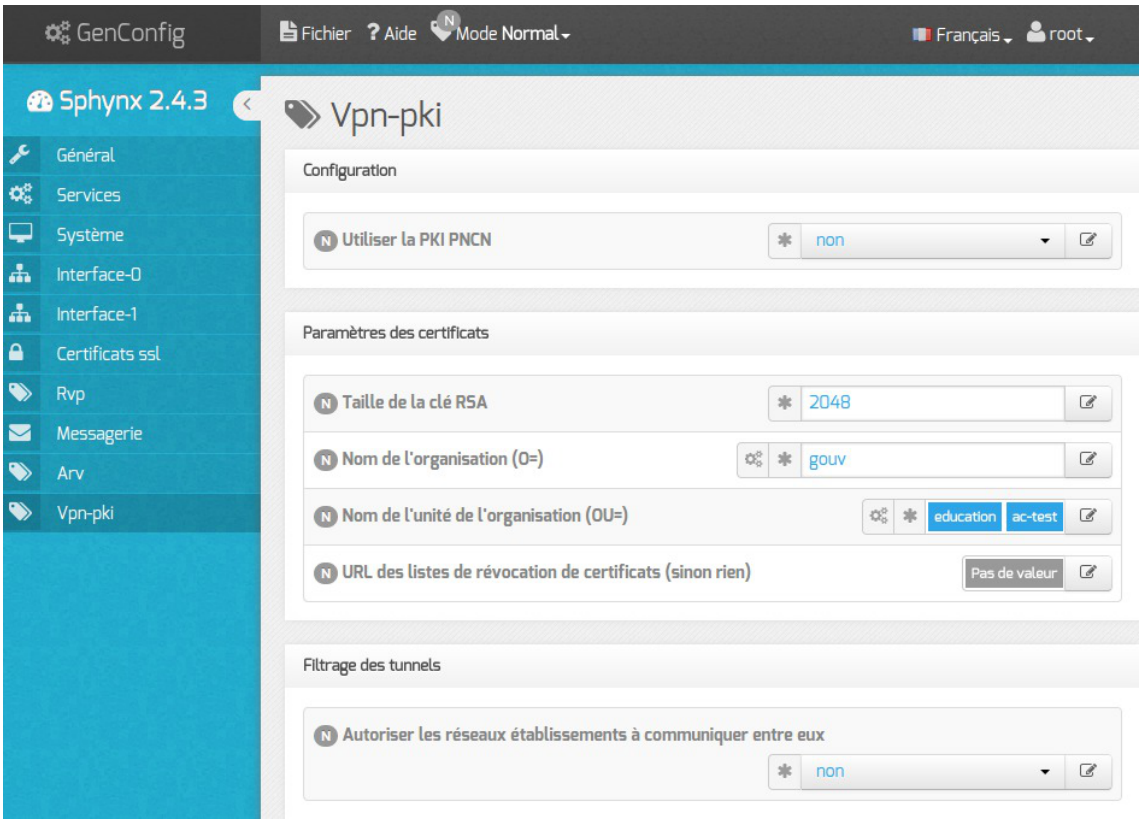
Par défaut, l'instanciation du module Sphynx génère une base ARV minimale avec uniquement les modèles de serveur `sphynx` et `etablissement`.

Un script nommé `init_sphynx` permet de générer une base ARV adaptée au réseau AGRIATES.

Il est possible d'utiliser la nouvelle PKI PNCN[p.185] ou l'ancienne PKI RACINE AGRIATES.

Les tunnels VPN sont actuellement basés sur la PKI RACINE AGRIATES mais la nouvelle PKI PNCN va prochainement la remplacer. La configuration OpenSSL préparée par le module pour effectuer les requêtes auprès de l'IGC est conditionnée par la variable `Utiliser la PKI PNCN`.

Utilisation de l'ancienne PKI RACINE AGRIATES

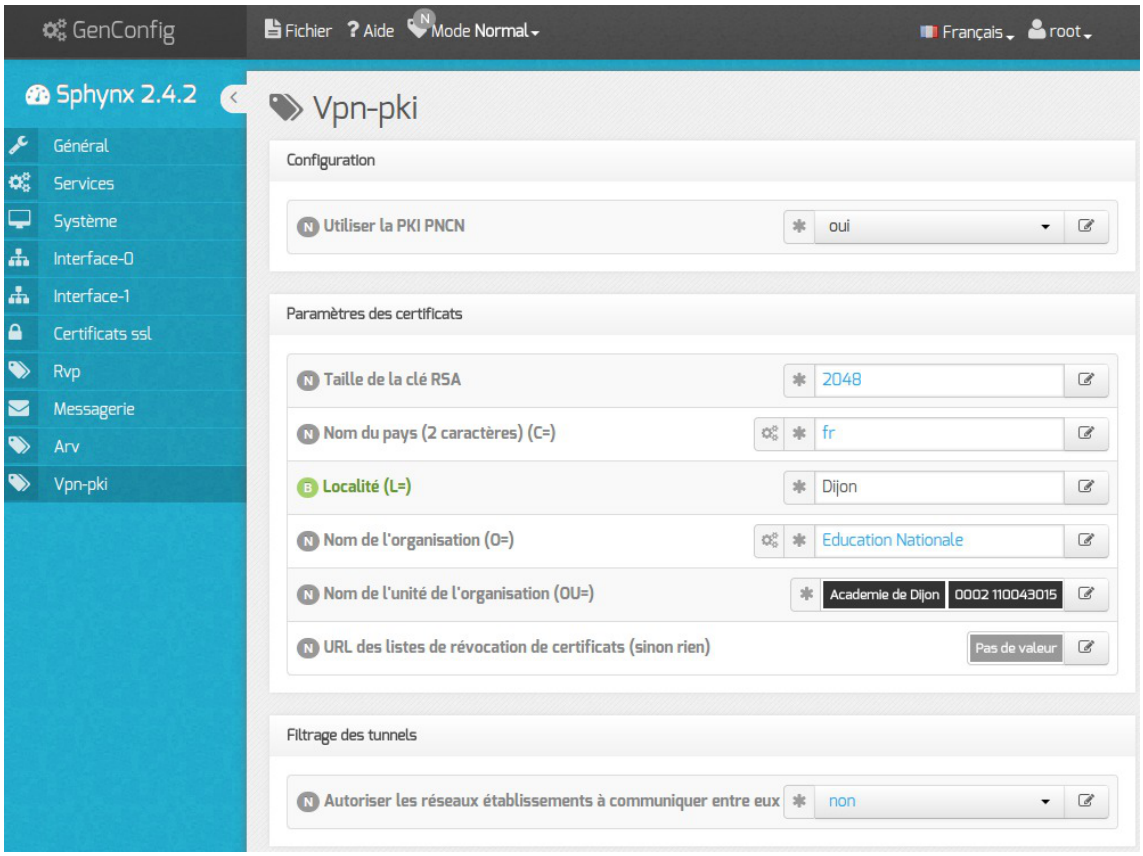


Configuration du VPN sur Sphynx

- `Taille de la clé RSA` : champ pré-rempli et obligatoire ;
- `Nom de l'organisation` : champ pré-rempli et obligatoire ;
- `Nom de l'unité de l'organisation` : champ pré-rempli et obligatoire ;
- `URL des listes de révocation des certificats` : les URL de révocation fournies par l'IGC sont à placer ici, cette variable est optionnelle car ces URL sont dorénavant intégrées aux certificats.

Utilisation de la nouvelle PKI PNCN

Pour utiliser la nouvelle PKI PNCN[p.185] il faut passer la variable `Utiliser la PKI PNCN` à `oui`. Un champ supplémentaire concernant la localité est à remplir obligatoirement.



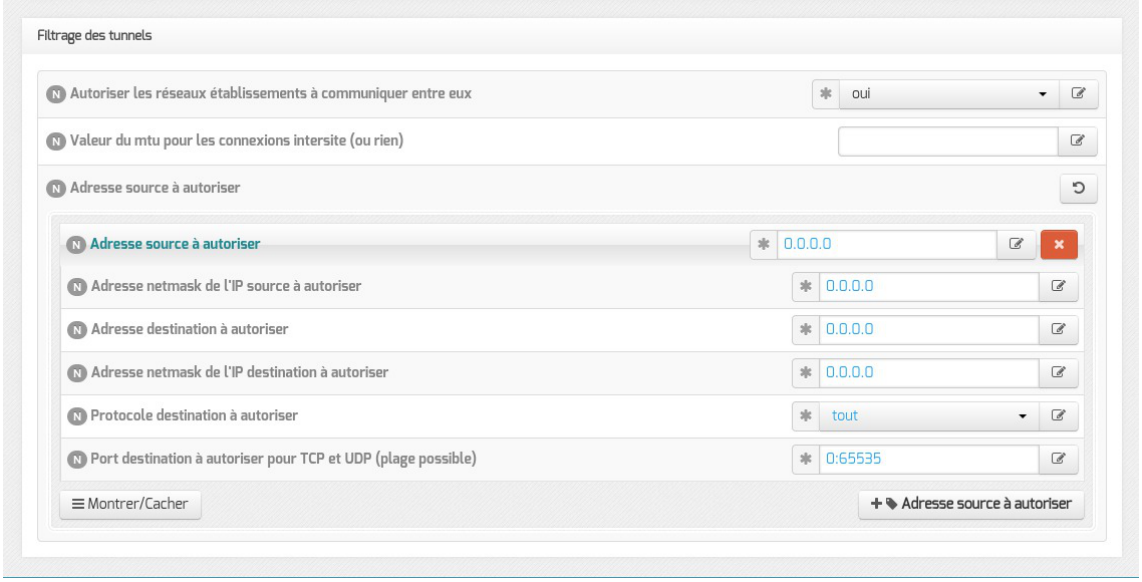
- `Taille de la clé RSA` : champ pré-rempli et obligatoire ;
- `Localité` : champ obligatoire ;
- `Nom de l'organisation` : champ pré-rempli et obligatoire ;
- `Nom de l'unité de l'organisation` : champ et obligatoire ;

  Il est impératif de respecter l'ordre des OU : *Academie de nomAcademie - 0002 110043015*

  Vous trouverez plus de détails sur le site du pôle PNCN à l'adresses suivante :
  - https://pole.pncn.education.gouv.fr/content/demande-dun-certificat-scolarité-et-formation
- `URL des listes de révocation des certificat`s : les URL de révocation fournies par l'IGC sont à placer ici, cette variable est optionnelle car ces URL sont dorénavant intégrées aux certificats.

Filtrage des tunnels

Il est possible d'autoriser les communications entre deux serveurs Amon en passant par le concentrateur Sphynx, il faut pour cela renseigner les différentes adresses réseaux à filtrer.



Parmi les paramètres il faut spécifier le réseau source, le réseau destination, le protocole ainsi que les ports autorisés à communiquer entre eux.

2.11. Onglet Quagga : Configuration du routage dynamique

Le routage dynamique peut être activé afin de ne pas avoir à gérer les routes statiques sur le serveur. Dans l'onglet service il faut passer `Activer le routage dynamique sur l'interface interne 1` à `oui`. Cela va activer le logiciel Quagga[p.185] sur l'interface eth1.

Onglet Services

Un nouvel onglet dans l'interface de configuration du module permet de choisir le protocole à utiliser et d'autoriser des réseaux à ajouter des routes.

Onglet Quagga

3. Configuration en mode expert

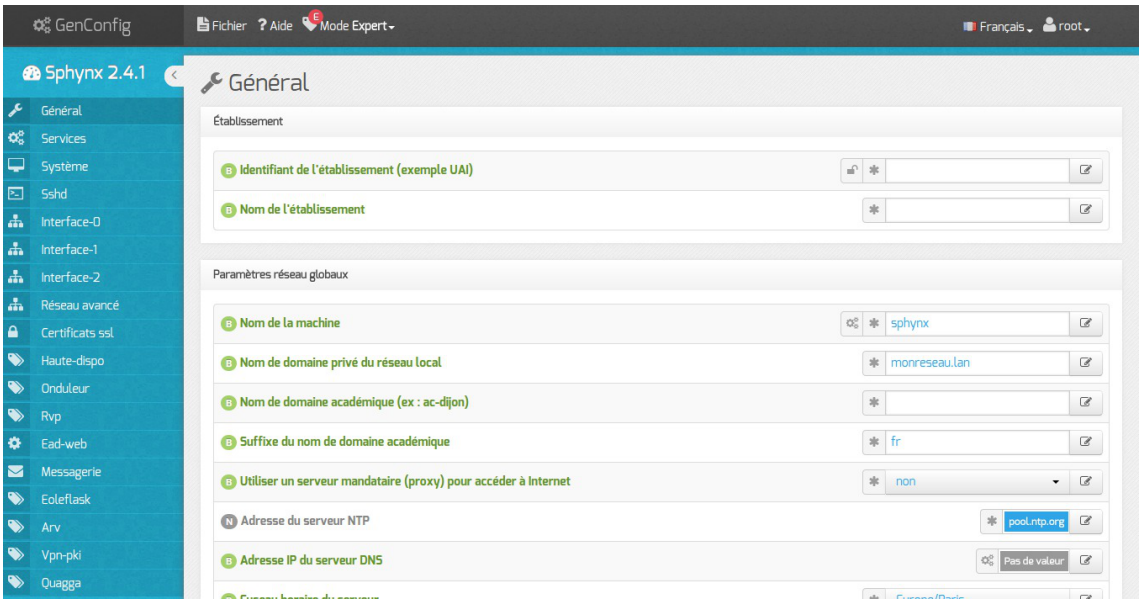
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode expert de l'interface de configuration du module.

Dans l'interface de configuration du module voici les onglets propres à la configuration du module Sphynx :

- Général ;
- Services ;
- Système ;
- Sshd ;
- Logs * ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-1 (configuration de l'interface réseau) ;
- Interface-2 (configuration de l'interface réseau) * ;
- Réseau avancé ;
- Certificat ssl ;
- Haute-dispo * ;
- Onduleur * ;
- Rvp ;
- Ead-web ;
- Messagerie ;
- Eoleflask ;
- Arv ;
- Vpn-pki ;

- Quagga *.

Certains des onglets ne sont disponibles qu'après activation du service dans l'onglet Services et sont marqués avec une * dans la liste ci-dessus.

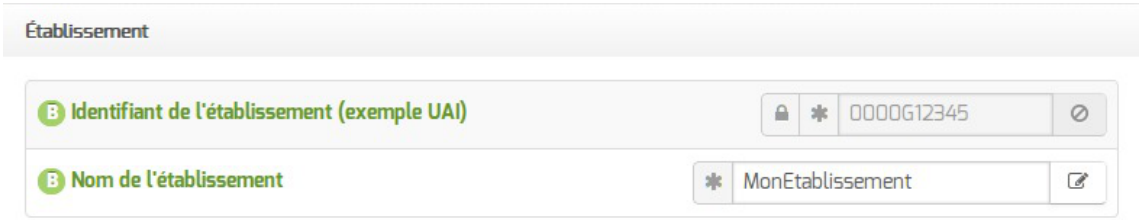


Vue générale de l'interface de configuration du module

3.1. Onglet Général

Présentation des différents paramètres de l'onglet Général.

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

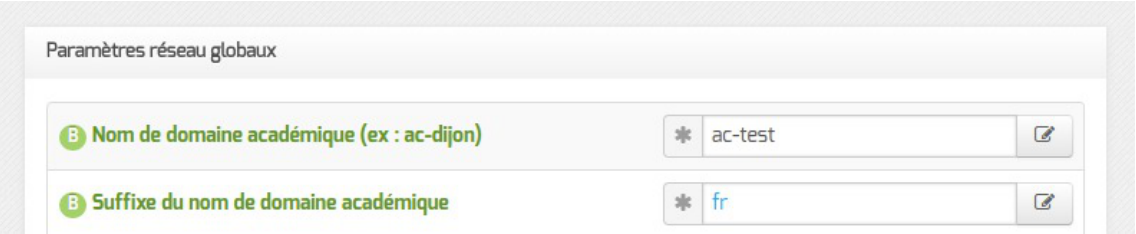
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.183] local, ces variables sont utilisées pour créer l'arborescence.

Il est déconseillé de modifier ces informations après l'instanciation du serveur sur les modules utilisant un serveur LDAP local.

Paramètres réseau globaux



En premier lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

Le `Nom de la machine` est laissé à l'appréciation de l'administrateur.

Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

Le `Nom de domaine privé du réseau local` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

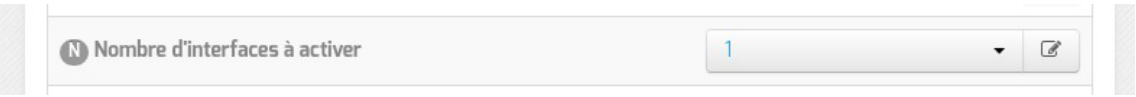
C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.

L'usage d'un domaine de premier niveau utilisé sur Internet n'est pas recommandé, car il existe un risque de collision entre le domaine privé et le domaine public.

Nombre d'interfaces

Un module EOLE peut avoir de 1 à 5 cartes réseau.



Suivant le module installé, un nombre d'interface est pré-paramétré. Il est possible d'en ajouter en sélectionnant la valeur du nombre total d'interfaces souhaitées dans le menu déroulant. Cela ajoute autant d'onglet `Interface-n` que le nombre d'interfaces à activer choisi.

Il est possible en fonction du module que la configuration ne permette pas toujours de choisir le nombre d'interfaces et que l'ensemble des paramétrages ne soit pas proposé.

Proxy

Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Il devient alors possible de saisir la configuration du serveur proxy :

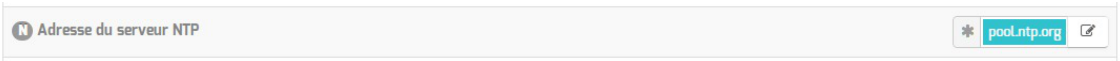
- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.

DNS et fuseau horaire

La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.181].

La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.184]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Il est possible de définir d'autres adresses pour le serveur de mise à jour Ubuntu que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Voir aussi...

> Les différents types de mises à jour

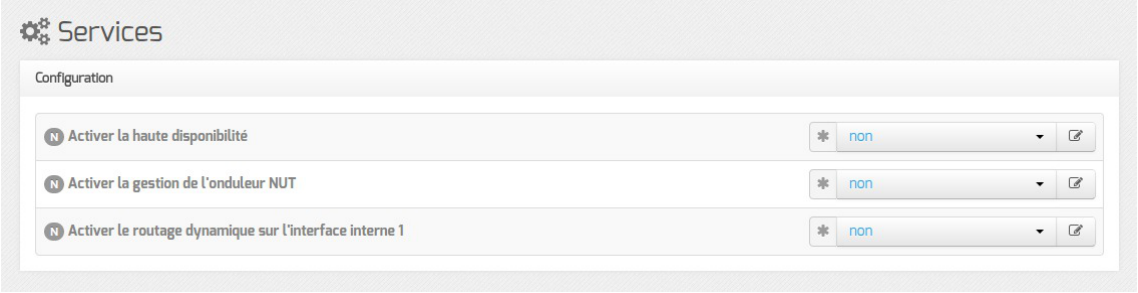
3.2. Onglet Services

L'onglet Services permet d'activer et de désactiver une partie des services proposés par le module.

Suivant le module installé et le mode utilisé pour la configuration la liste des services activables ou désactivables est très différente.

> Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un onglet de configuration propre au service.

En mode normal la liste des services activables ou désactivables est courte.



Vue de l'onglet Services du module Sphynx en mode normal

Le service de gestion des onduleurs est commun à tous les modules.

Les services de base propres au module Sphynx sont les suivants :

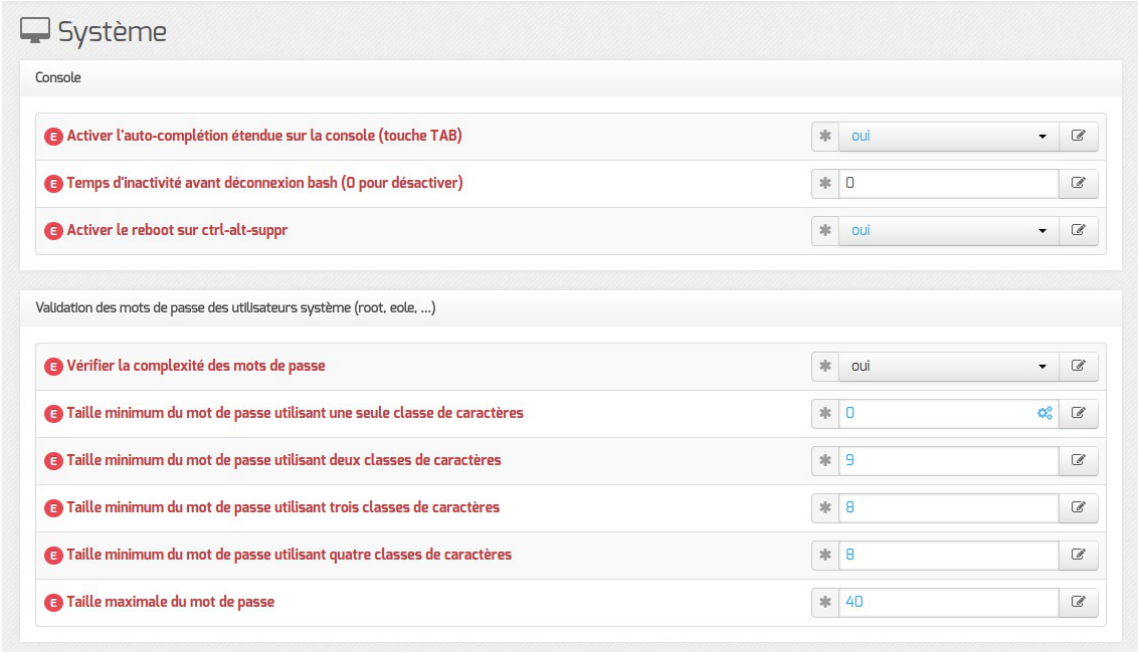
- la haute disponibilité ;
- le routage dynamique avec le logiciel Quagga[p.185].

En mode expert les services de base communs à tous les modules sont :

- gestion des logs centralisés ;
- interface web de l'EAD.

En mode expert il n'y a aucun service propre au module Sphynx.

3.3. Onglet Système



Les paramètres de l'onglet `Système` permettent de régler le comportement de la console et de déterminer le niveau de complexité requis pour les mots de passe des utilisateurs système.

Paramétrage de la console

- `Activer l'auto-complétion étendue sur la console` : l'auto-complétion facilite l'utilisation de la ligne de commande mais peut ralentir son affichage, elle est activée par défaut ;
- `Temps d'inactivité avant déconnexion bash` : si aucune activité n'est constatée sur la console utilisateur pendant cette durée (en secondes), sa session est automatiquement coupée, avec le message : `attente de données expirée : déconnexion automatique`. La valeur `0` permet de désactiver cette fonctionnalité ;
- `Activer le reboot sur ctrl-alt-suppr` : si cette variable est passée à `non`, la séquence `ctrl - alt - suppr` est désactivée et affiche le message suivant `Control-Alt-Delete - séquence désactivée`.

Optimisations système

- `Poids relatif de l'utilisation de la swap par rapport à la mémoire vive` : Le swappiness est un paramètre du noyau Linux permettant de définir avec quelle sensibilité il va écrire dans la swap si la quantité de RAM à utiliser devient trop importante. Le système accepte des valeurs comprises entre 0 et 100. La valeur `0` empêchera au maximum le système d'utiliser la

partition d'échange.

- `Activer le service de génération de nombres aléatoires rng-tools` : Le démon `rngd` agit comme une passerelle entre un vrai générateur de nombres aléatoires, matériel (TRNG), tel que ceux que l'on peut trouver dans les puces Intel/AMD/VIA et le pseudo-générateur de nombres aléatoires du noyau (PRNG).

Sur les serveurs virtualisés, le service `rngd` ne sera généralement pas fonctionnel et affichera, au démarrage, un message du type :

`erreur Starting Hardware RNG entropy gatherer daemon: (failed)`

Validation des mots de passe

EOLE propose un système de vérification des mots de passe évolué pour les utilisateurs système.

Un paramétrage a été mis par défaut, mais il est possible d'affiner les paramètres proposés.

La question `Vérifier la complexité des mots de passe` permet d'activer ou de désactiver la validation des mots de passe.

Si la vérification de la complexité des mots de passe est activée, celle-ci peut être régler plus finement à l'aide des paramètres suivants :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` ;
- `Taille minimum du mot de passe utilisant deux classes de caractères` ;
- `Taille minimum du mot de passe utilisant trois classes de caractères` ;
- `Taille minimum du mot de passe utilisant quatre classes de caractères` ;
- `Taille maximale du mot de passe`.

Plus d'informations sur le site du projet : http://www.openwall.com/passwdqc/

Ce paramétrage ne concerne que les comptes locaux. Les utilisateurs LDAP ne sont pas soumis aux mêmes restrictions.

Voir aussi...

Les mots de passe

3.4. Onglet Sshd : Gestion SSH avancée

Les paramètres disponibles dans cet onglet permettent d'affiner la configuration des accès SSH au serveur et viennent en complément des variables définissant les autorisations d'administration à distance saisies au niveau de chacune des interfaces (onglets `Interface-n`).

Ils permettent :

- d'interdire à l'utilisateur `root` de se connecter ;
- de n'autoriser que les connexions par clef RSA ;
- de déclarer des groupes Unix supplémentaires autorisés à se connecter en SSH au serveur.

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant :

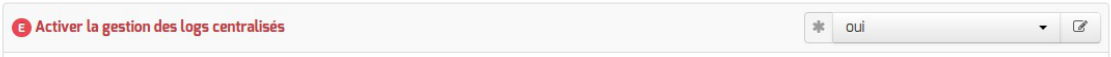
`Permission denied (publickey).`

Par défaut les groupes Unix autorisés sont `root` et `adm`.

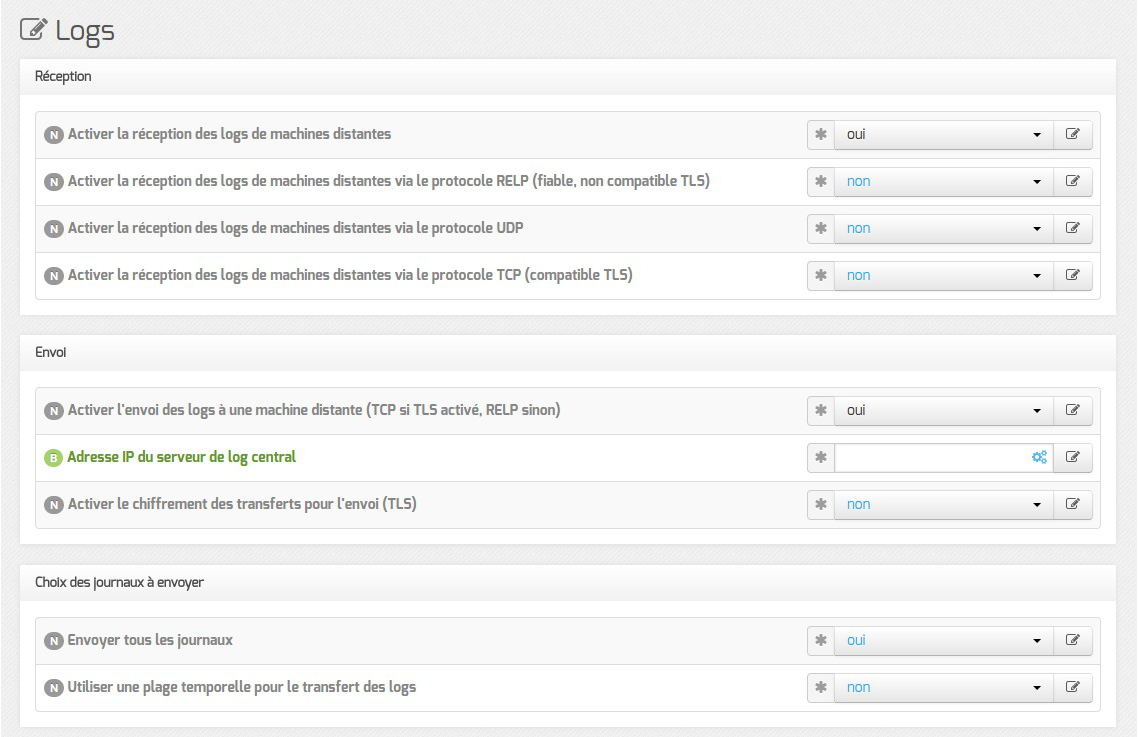
3.5. Onglet Logs : Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.187]. Cela rend possible un transfert croisé des journaux ou une centralisation.

Le support des logs centralisés peut être activé dans l'onglet `Service` en mode expert.



Cette activation affiche un nouvel onglet nommé `Logs` dans l'interface de configuration du module.



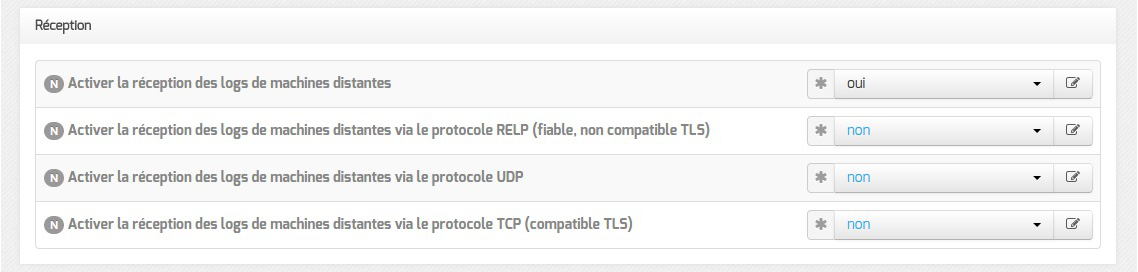
Vue de l'onglet Logs

Les options de cet onglet sont réparties en plusieurs sections :

- la configuration de la réception des logs permet de spécifier les protocoles de communication entre des machines distantes émettrices identifiées par leur adresse IP et le poste configuré ;
- la configuration de l'envoi des logs permet de spécifier l'adresse de la machine distante réceptrice. Le protocole (TCP[p.186] ou RELP[p.185]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.187]) ;
- la configuration des journaux à envoyer permet de sélectionner les journaux à envoyer ainsi que l'heure de début et de fin de transfert.

Réception des journaux

Si la réception des journaux est activée (`Activer la réception des logs de machines distantes` à `oui`), il faut activer au moins l'un des 3 protocoles de réception : RELP, UDP et TLS over TCP.



L'activation des protocoles ouvre les ports adéquats sur le module.

Pour les clients EOLE, l'envoi de journaux avec le protocole TCP n'est possible que si le TLS est activé.

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.179].

Envoi des journaux

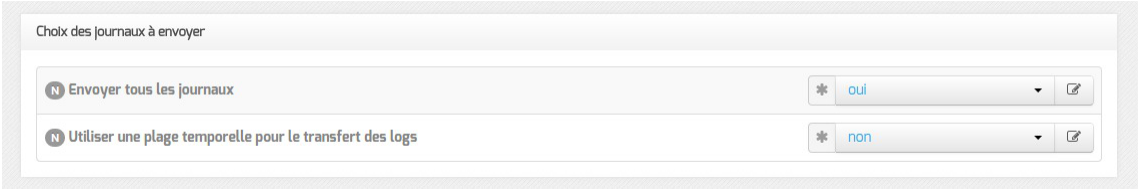
L'activation de l'envoi des journaux (`Activer l'envoi des logs à une machine distante` à `oui`) nécessite la saisie de l'adresse IP du serveur centralisateur de journaux.

Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.179].

Choix des journaux à envoyer

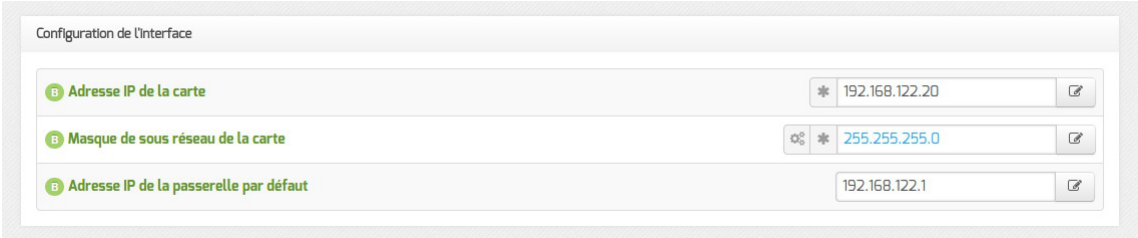
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



Il est également possible d'envoyer les journaux en temps réel ou en différé. L'heure de début et de fin (plage temporelle) de transfert des journaux est également paramétrable.

3.6. Onglet Interface-0

Configuration de l'interface



L'interface 0 nécessite un adressage statique, il faut renseigner l'adresse IP, le masque et la passerelle.

En mode expert quelques variables supplémentaires sont disponibles.

Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

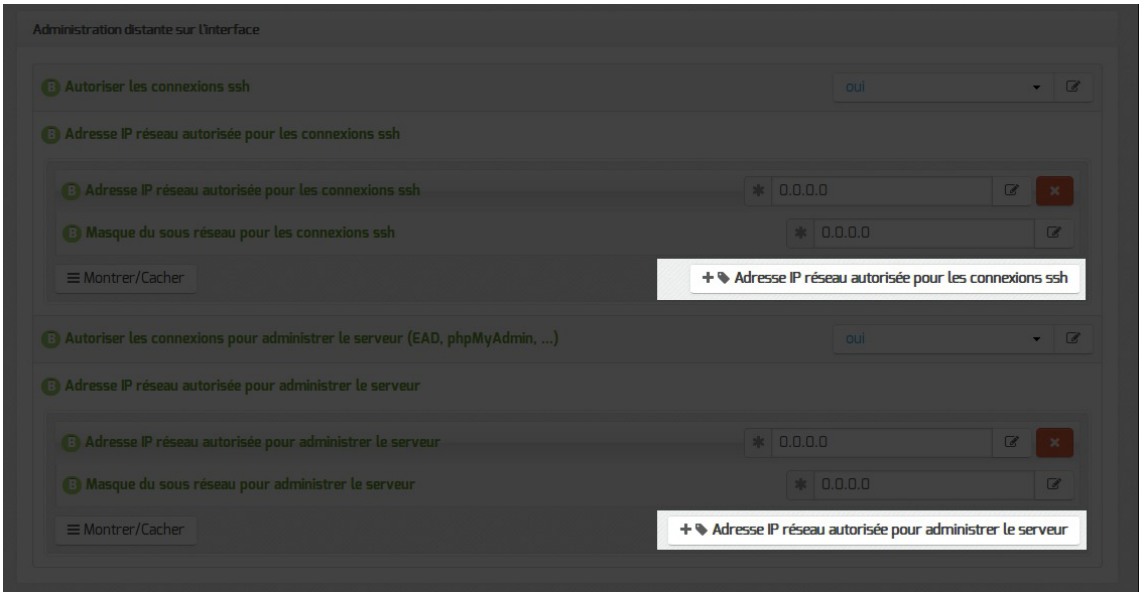
Administration à distance

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

Le masque réseau d'une station isolée est `255.255.255.255`.

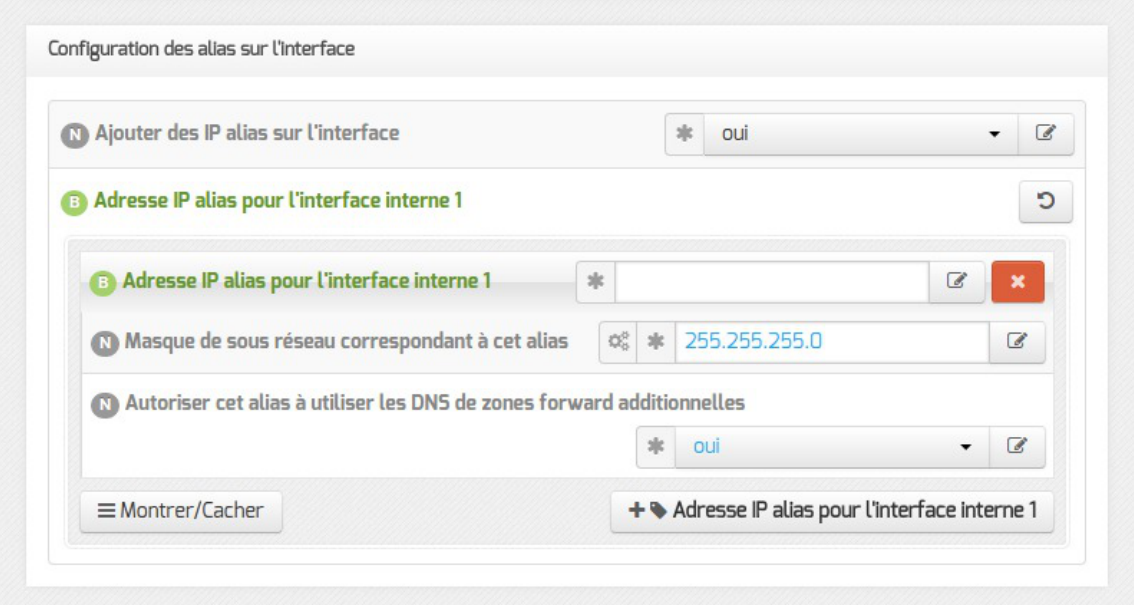
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



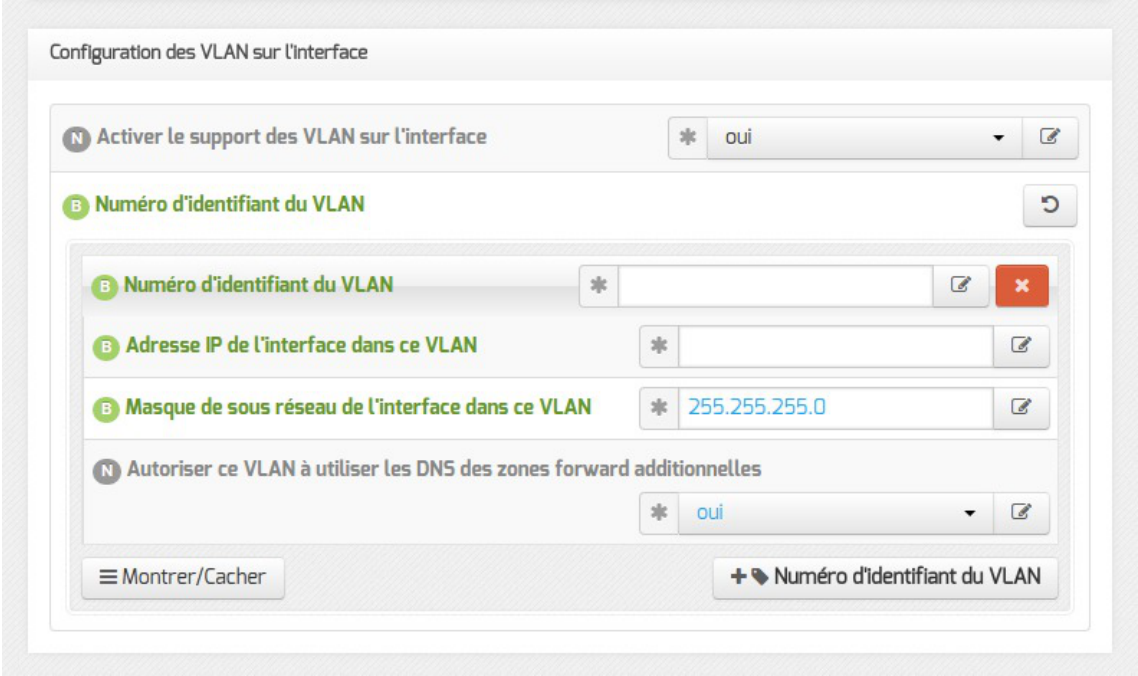
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

`Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

3.7. Onglet Interface-1

Seuls les flux réseaux ayant des connexions VPN déclarées provenant de cette interface seront autorisés à sortir vers eth0 de manière chiffrée.

Configuration de l'interface

L'interface nécessite un adressage statique, il faut renseigner l'adresse IP et le masque de sous réseau.

En mode expert quelques variables supplémentaires sont disponibles.

Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

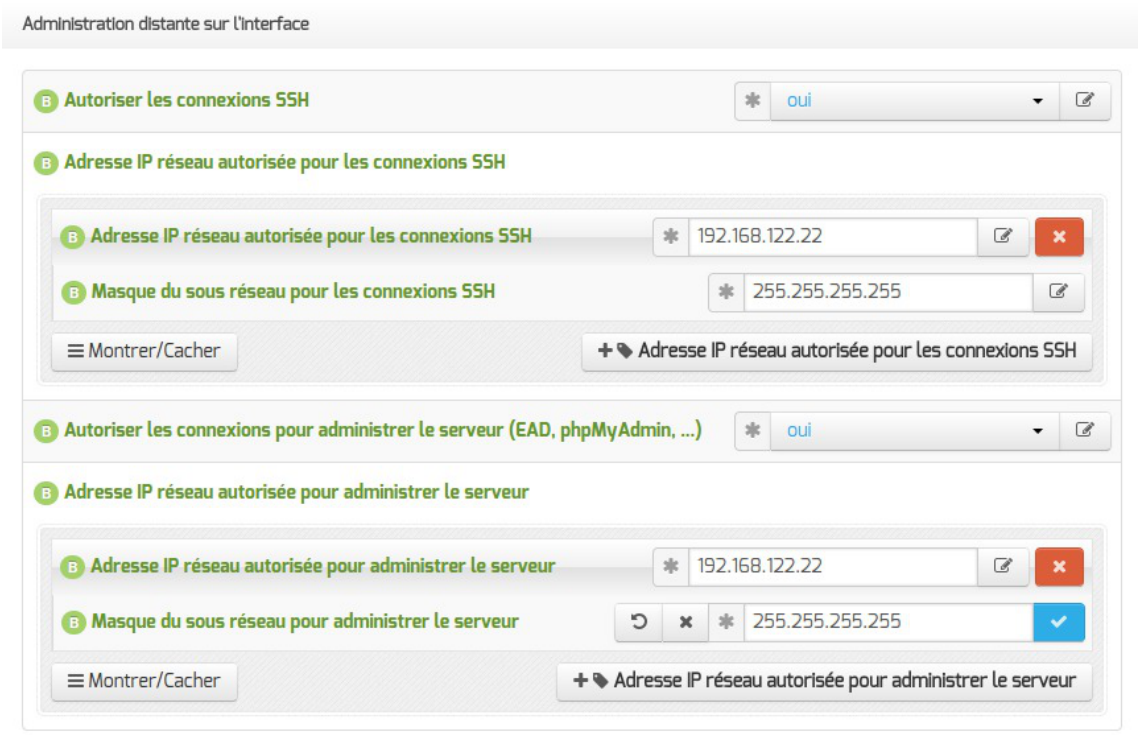
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseaux, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

Administration à distance

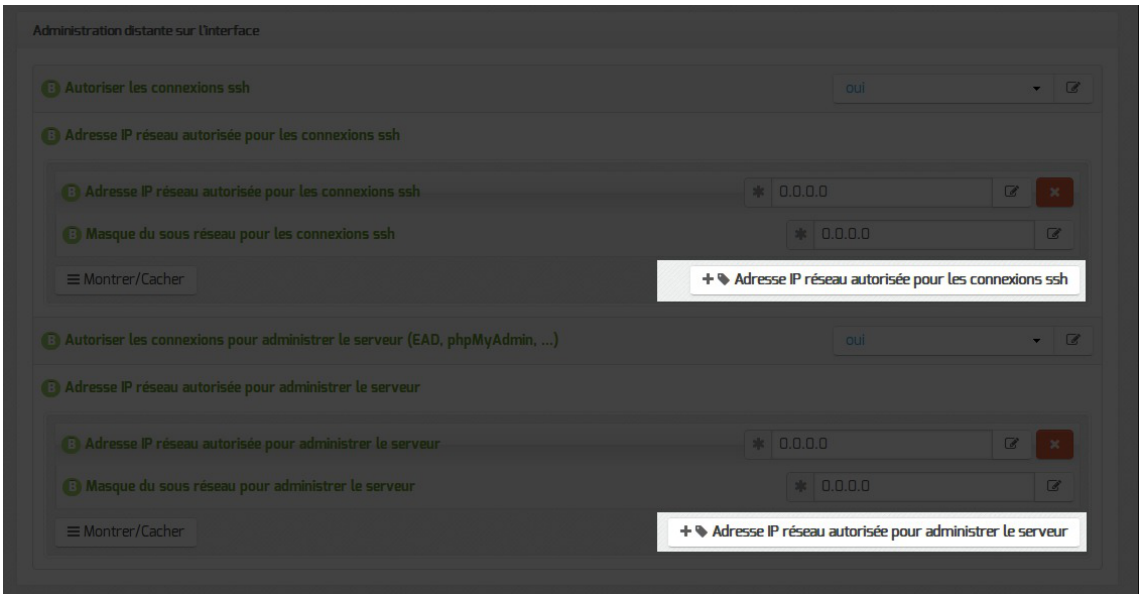


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

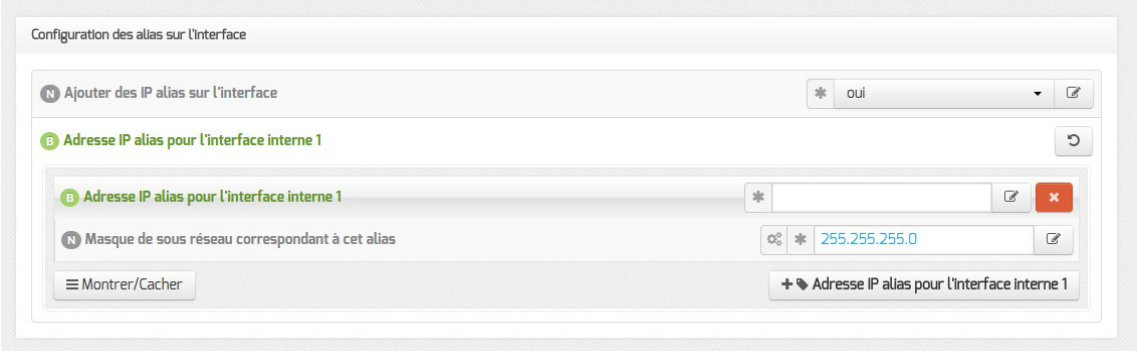
Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

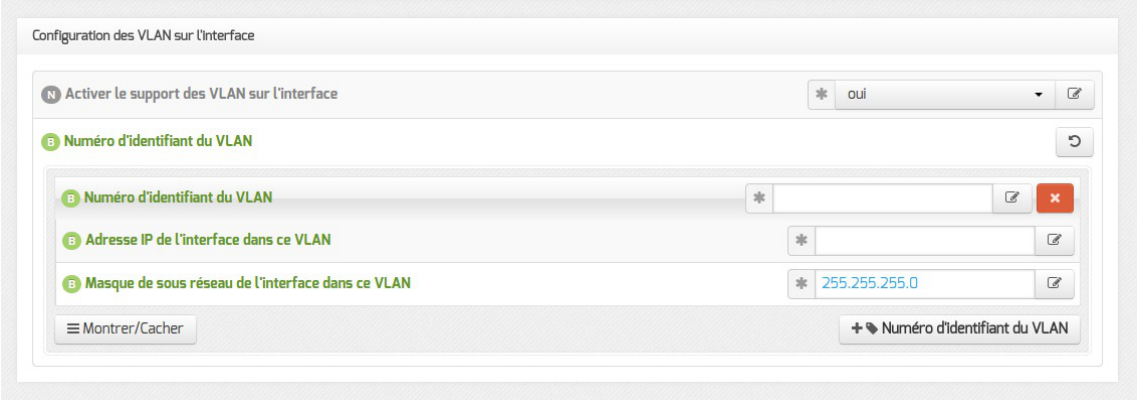
EOLE supporte les alias sur les cartes réseaux. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



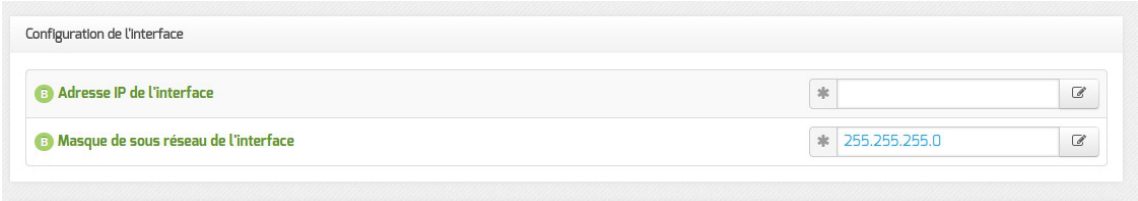
Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

3.8. Onglet Interface-2

Cette interface est dédiée au dialogue (en multicast[p.183]) entre les nœuds du cluster, aussi onglet `Interface-2` n'est disponible qu'après l'activation de la Haute disponibilité dans l'onglet `Services`.

Il est préférable de réaliser des liaisons physiques directes entre les nœuds.

Configuration de l'interface



L'interface nécessite un adressage statique, il faut renseigner l'adresse IP et le masque de sous réseau.

En mode expert quelques variables supplémentaires sont disponibles.

Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.

Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.

L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

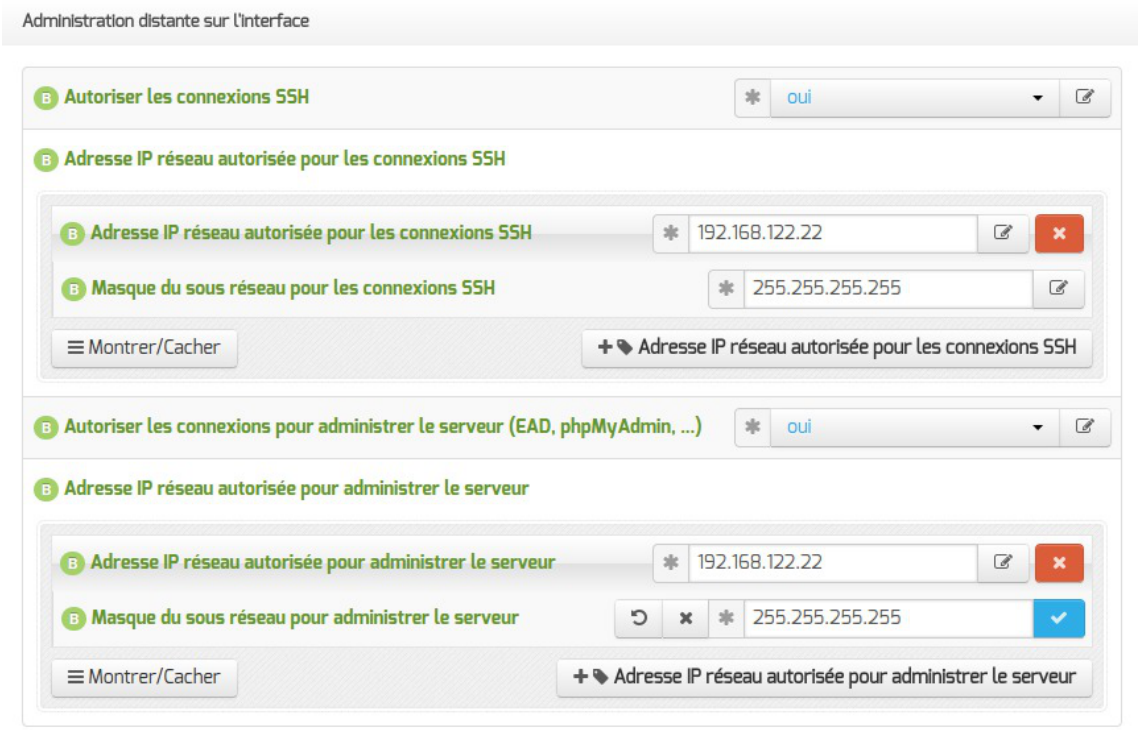
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseaux, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet).

Administration à distance



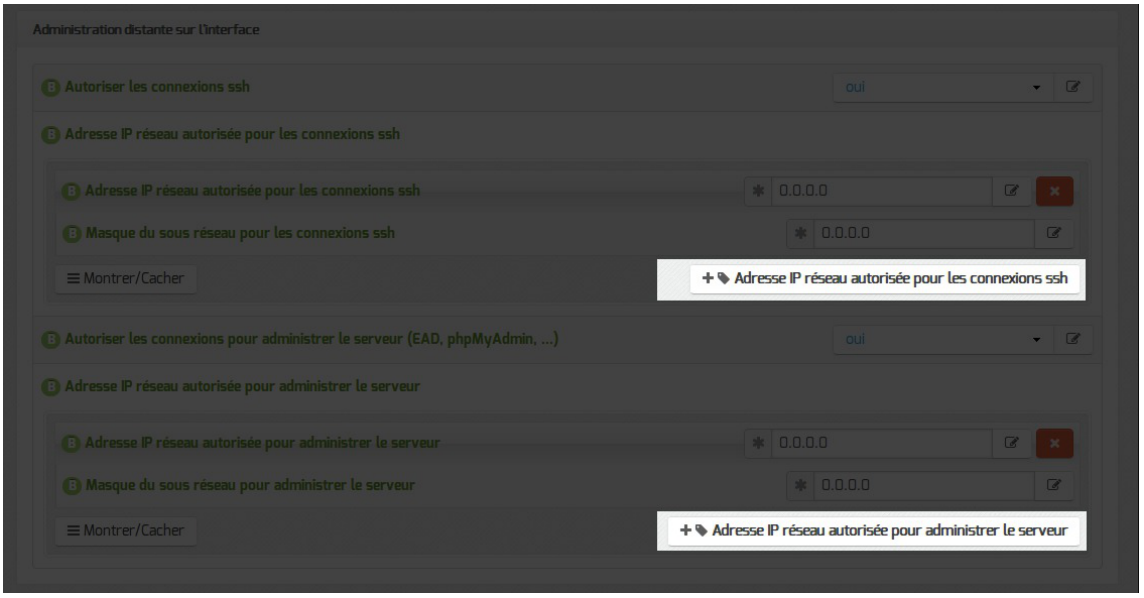
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.186] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS,

ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.



Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour…`.

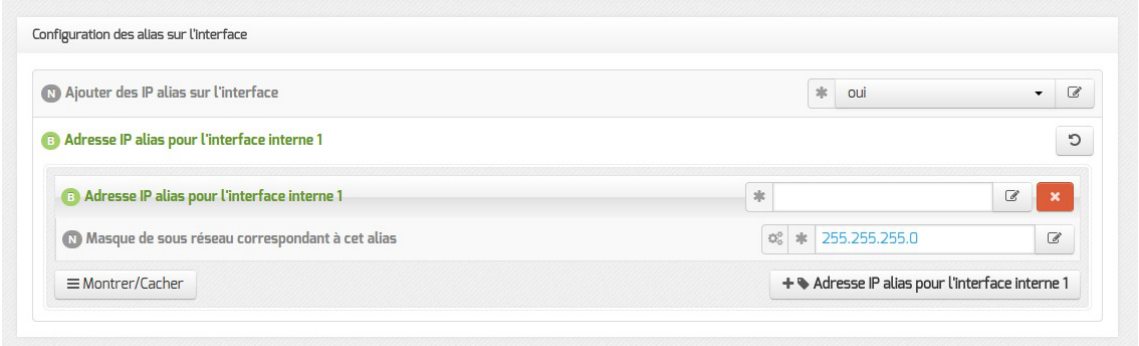
Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

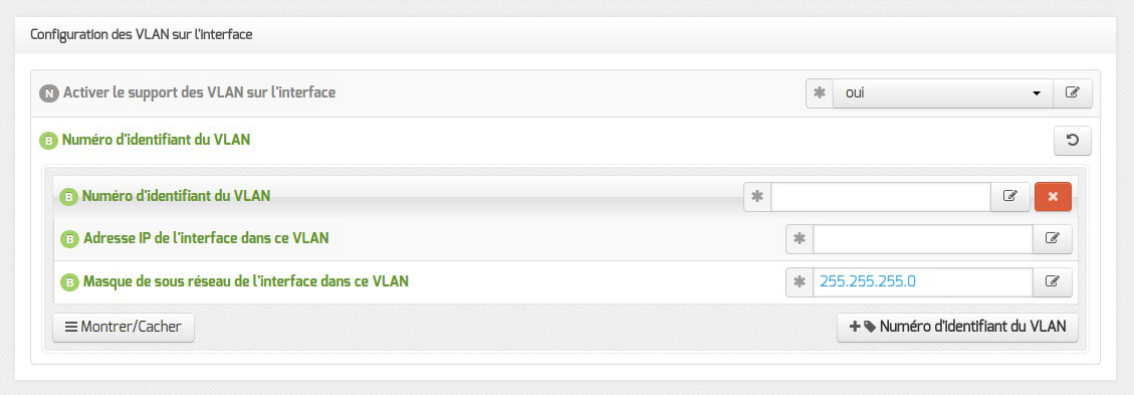
EOLE supporte les alias sur les cartes réseaux. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

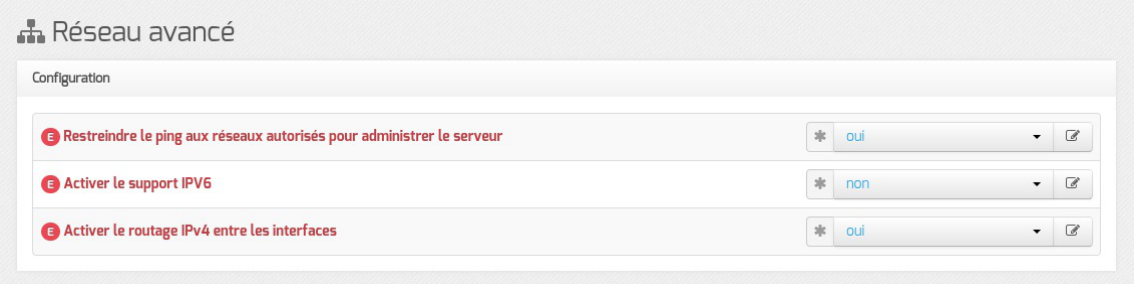
Voir aussi...

> Mettre en place un cluster haute disponibilité [p.104]

3.9. Onglet Réseau avancé

Présentation des différents paramètres de l'onglet `Réseau avancé` accessible en mode expert.

Configuration IP



La valeur par défaut de la variable `Restreindre le ping aux réseaux autorisés pour administrer le serveur` est à `oui` par défaut mais cette restriction peut être levée en passant la variable à `non`.

Sur les modules disposant de la fonctionnalité serveur de fichiers comme Scribe et Horus, cette restriction est déjà levée puisque la variable est par défaut à `non`.

Il est recommandé de laisser la variable `Restreindre le ping aux réseaux autorisés pour administrer le serveur` à `non` sur les serveurs disposant de la fonctionnalité serveur de fichiers, principalement pour que les postes clients puissent fonctionner correctement.

La variable `Activer le support IPv6` est par défaut à `non` et est utilisée pour désactiver explicitement le support de l'IPv6 dans la configuration de certains logiciels (BIND, Proftpd).

Le support de l'IPv6[p.183] peut être activé en passant la variable `Activer le support IPv6` à `oui` mais sa prise en charge ne se sera faite qu'au niveau du noyau.

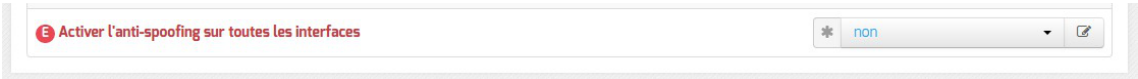
Si la variable `Activer le routage IPv4 entre les interfaces` est à `oui`, alors le routage IPv4 est activé au niveau du noyau (`/proc/sys/net/ipv4/ip_forward` passe à `1`)

L'activation du support IPv6 entraîne l'apparition de la variable : `Activer le routage IPv6 entre les interfaces`.

Si cette dernière est à `oui` le routage IPv6 est activé au niveau du noyau (`/proc/sys/net/ipv6/conf/all/forwarding` passe à `1`).

Sécurité

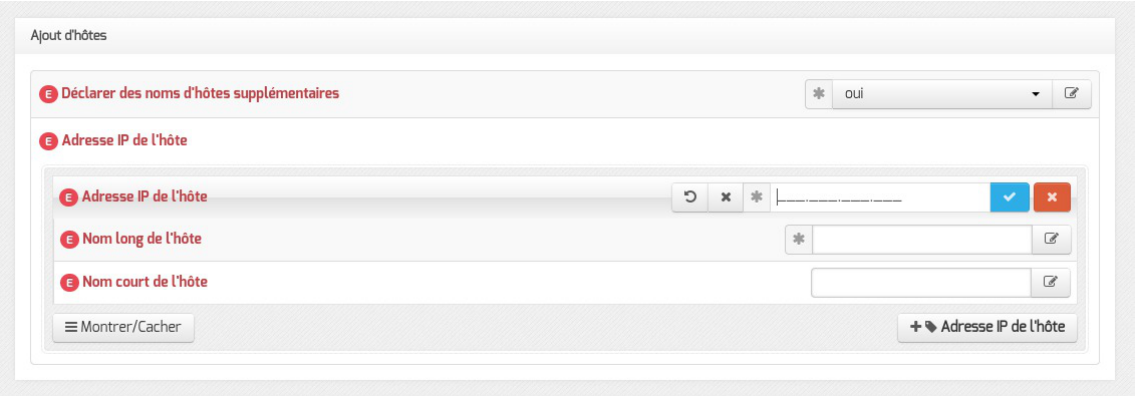
Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.179] est activé sur l'interface-0 des modules EOLE.

Sur les serveurs ayant 2 interfaces réseau ou plus d'activées (cas par défaut pour Amon et Sphynx), il est possible de demander l'activation de l'anti-spoofing sur les autres interfaces en passant la variable `Activer l'anti-spoofing sur toutes les interfaces` à `oui`.

Ajout d'hôtes



Passer la variable `Déclarer des noms d'hôtes supplémentaires` à `oui`, permet de déclarer des noms d'hôtes qui seront ajoutés au fichier `/etc/hosts`.

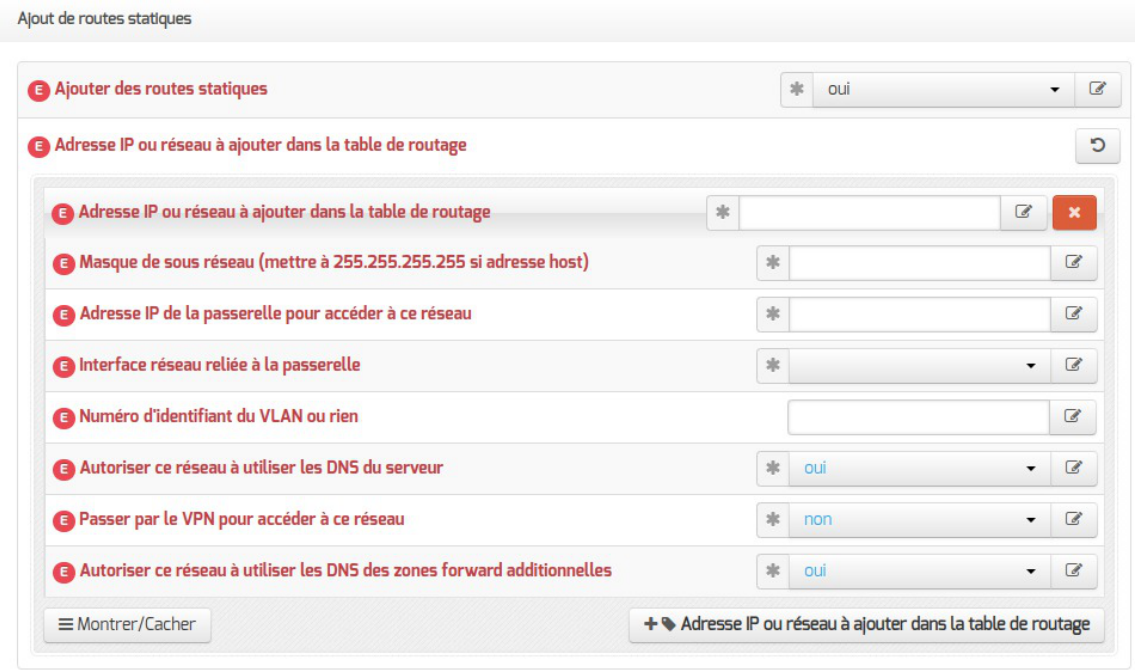
Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte`.

Le champ `Nom court de l'hôte` est optionnel.

Sur les serveurs EOLE faisant office de serveur DNS, comme les modules Amon et AmonEcole, pour que le logiciel BIND[p.180] puisse résoudre un nom, il faut que le suffixe DNS de ce nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

Si ce n'est pas le cas, il faut déclarer un `Nom de domaine local supplémentaire` dans l'onglet `Zones-dns` pour permettre au serveur de résoudre ce nom d'hôte.

Ajout de routes statiques



Ce bloc de paramètres permet d'ajouter, manuellement, des routes afin d'accéder à des adresses ou à des plages d'adresses par un chemin différent de celui par défaut (défini par le routeur par défaut).

Après avoir passé la variable `Ajouter des routes statiques` à `oui` il faut ajouter les paramètres suivants :

- `Adresse IP ou réseau à ajouter dans la table de routage` : permet de définir l'adresse de sous-réseau (ou l'adresse de l'hôte) vers lequel le routage doit s'effectuer ;
- `Masque de sous réseau` : permet de définir le masque du réseau défini ci-dessus (s'il s'agit d'une machine seule, il faut mettre l'adresse du masque à 255.255.255.255) ;
- `Adresse IP de la passerelle pour accéder à ce réseau` : permet de renseigner l'adresse de la passerelle permettant d'accéder au sous-réseau ou à l'hôte défini ci-dessus ;
- `Interface réseau reliée à la passerelle` : permet d'associer la route à une interface donnée. Ce champ, de type liste déroulante, comporte un certain nombre d'interfaces pré-définies. Il est possible d'en ajouter une en tapant son nom (par exemple : `ppp0`) ;
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Configuration du MTU

La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.183] (/proc/sys/net/ipv4/ip_no_pmtu_disc).

Cette option est à `non` par défaut (ip_no_pmtu_disc=0) ce qui est le fonctionnement normal.

Cela peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP[p.182] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTU discovery est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Si vous rencontrez des problèmes d'accès à certains sites (notamment messagerie ou site intranet via le VPN, Gmail ou Gmail Apps), vous pouvez passer ce paramètre à `oui` (ip_no_pmtu_disc=1).

Il est possible de forcer une valeur de MTU[p.183] pour l'interface externe.

Si le champ n'est pas renseigné, la valeur par défaut est utilisée (1500 octets pour un réseau de type Ethernet).

Si l'interface est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le premier champ : `Valeur du MTU pour l'interface eth0`.

Si l'interface est de type PPPoE et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le second champ : `Valeur du MTU pour l'interface ppp0`.

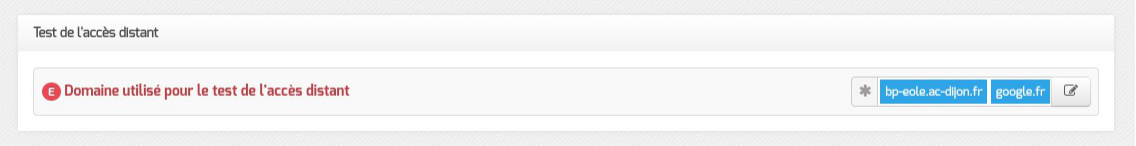
Les commandes `ping`, `ip route` et `tracepath` sont utilisées pour ajuster les valeurs.

Configuration de la "neighbour table"

Les variables `ipv4 neigh default gc thresh1`, `ipv4 neigh default gc thresh2` et `ipv4 neigh default gc thresh3` servent à gérer la façon dont la table ARP évolue :

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;
- **gc_thresh2** : seuil qui, s'il est dépassé depuis un certain temps (5 secondes par défaut), déclenche le recyclage des entrées de la table qui ne sont plus utilisées ;
- **gc_thresh3** : seuil au-delà duquel le recyclage est immédiatement déclenché pour contenir la taille de la table.

Test de l'accès distant



Cette variable permet de définir le ou les domaines qui sont utilisés lorsque le module EOLE a besoin de tester son accès à Internet.

En pratique, seul l'accès au premier domaine déclaré est testé sauf dans le cas où il n'est pas accessible.

Les domaines définis sont utilisés dans les outils `diagnose` et dans l'agent Zéphir.

Voir aussi...

Résoudre des dysfonctionnements liés au MTU [p.150]

3.10. Onglet Certificats ssl : gestion des certificats SSL

La gestion des certificats a été standardisée pour faciliter leur mise en œuvre.

Ils sont désormais gérés par l'intermédiaire des outils Creole.

Certificats par défaut

Un certain nombre de certificats sont mis en place lors de la mise en œuvre d'un module EOLE :

- `/etc/ssl/certs/ca_local.crt` : autorité de certification propre au serveur (certificats auto-signés) ;
- `/etc/ssl/private/ca.key` : clef privée de la CA ci-dessus ;
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un certificat ;
- `/etc/ssl/certs/eole.crt` : certificat serveur généré par la CA locale, il est utilisé par les applications (apache, ead2, eole-sso, ...) ;
- `/etc/ssl/certs/eole.key` : clé du certificat serveur ci-dessus.

Après génération de la CA locale, un fichier `/etc/ssl/certs/ca.crt` est créé qui regroupe les certificats suivants :

- `ca_local.crt` ;
- `ACInfraEducation.pem` ;
- tout certificat présent dans le répertoire `/etc/ssl/local_ca/`

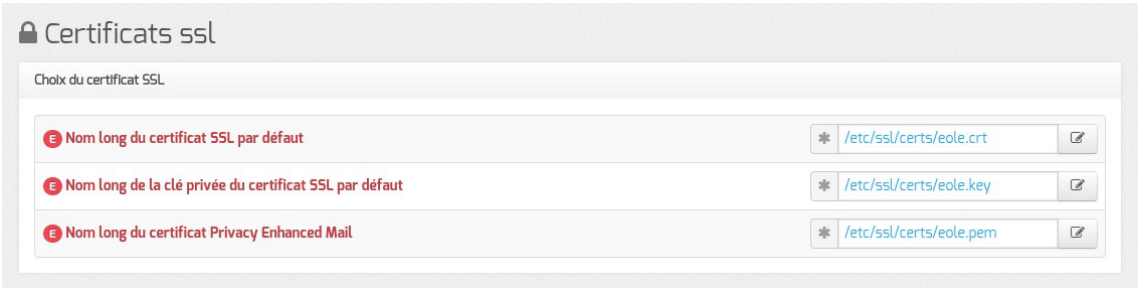
Détermination du nom de serveur (commonName) dans le certificat

Le nom du sujet auquel le certificat s'applique est déterminé de la façon suivante (important pour éviter les avertissements dans les navigateurs) :

- si la variable `ssl server name` est définie dans l'interface de configuration du module (onglet `Certifs ssl` -> `Nom DNS du serveur`), elle est utilisée comme nom de serveur dans les certificats ;
- sinon, si un nom de domaine académique est renseigné, le nom sera : `nom machine.numero etab.nom domaine academique` (exemple : `amon monetab.0210001A.mon dom acad.fr`) ;
- le cas échéant, on utilise : `nom machine.numero etab.debut(nom academie).min(ssl country name)` (exemple : `amon monetab.0210001A.ac-dijon.fr`).

Mise en place d'un certificat particulier

Pour que les services d'un module EOLE utilisent un certificat particulier (par exemple, certificat signé par une autorité tierce), il faut modifier deux variables dans l'onglet `Certificats ssl` de l'interface de configuration du module.



- `Nom long du certificat SSL par défaut` (server_cert) : chemin d'un certificat au format PEM à utiliser pour les services ;

- `Nom long de la clé privée du certificat SSL par défaut` (server_key) : chemin de la clé privée correspondante (éventuellement dans le même fichier).

Dans le cas d'un certificat signé par une autorité externe, copier le certificat de la CA en question dans `/etc/ssl/local_ca/` pour qu'il soit pris en compte automatiquement (non nécessaire pour les certificats de l'IGC nationale).

Le répertoire `/etc/ssl/certs/` accueille le fichier de certificat issu de la CA interne ainsi que la clé privée correspondant au certificat.

Il faut déclarer les bons chemins dans l'interface de configuration du module.

Pour appliquer les modifications, utilisez la commande `reconfigure`.

Si les certificats configurés ne sont pas trouvés, ils sont générés à partir de la CA locale.

Le répertoire `/etc/ssl/local_ca/` n'accueille que des certificats CA.

Création de nouveaux certificats

Le script `/usr/share/creole/gen_certif.py` permet de générer rapidement un nouveau certificat SSL.

Génération d'un certificat avec gen_certif.py

```
root@eole:~#          /usr/share/creole/gen_certif.py          -fc
/etc/ssl/certs/test.crt
Generation du certificat machine
* Certificat /etc/ssl/certs/test.crt généré
```

Obtention d'un certificat signé par l'IGC de l'Éducation nationale

Étapes à suivre :

1. récupérer la requête du certificat située dans le répertoire `/etc/ssl/req/` : `eole.p10` ;
2. se connecter sur l'interface web de demande des certificats et suivre la procédure ;
3. récupérer le certificat depuis l'interface (copier/coller dans un fichier) ;
4. copier le fichier dans le répertoire `/etc/ssl/certs/`.

Seuls les ISR/OSR des académies sont accrédités pour effectuer les demandes.

Certificats intermédiaires

En attendant que la prise en compte des certificats intermédiaires soit automatisée pour l'ensemble des services de base (fixme #13362 [https://dev-eole.ac-dijon.fr/issues/13362]), les manipulations nécessaires pour éviter des avertissements dans les navigateurs sont documentées dans la page wiki suivante : https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Gestion_certificats

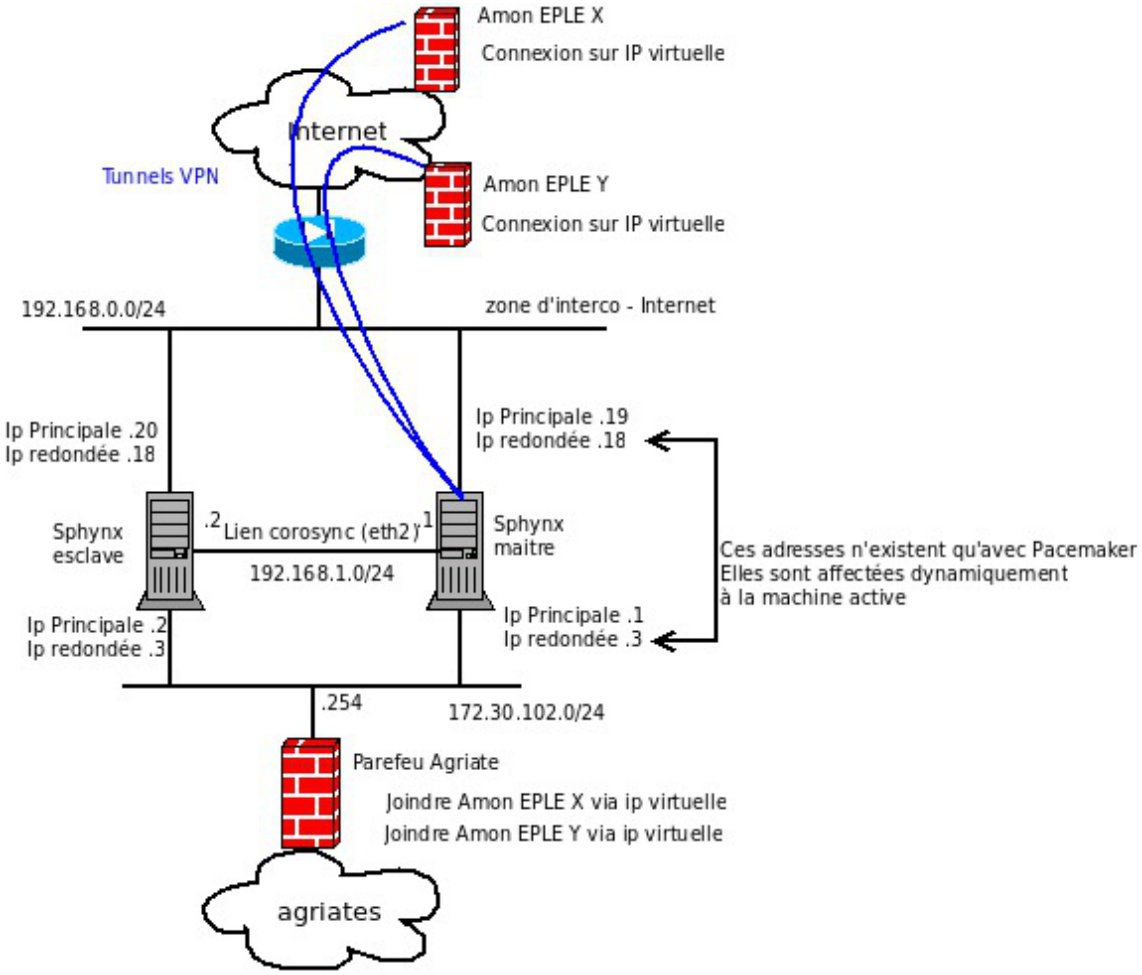
3.11. Onglet Haute-dispo : Configuration de la haute disponibilité

EOLE propose un service de haute disponibilité dont le rôle principal est de garantir la disponibilité d'un service et son bon fonctionnement.

Il est possible, depuis l'interface de configuration du module, d'activer ou non ce service.

Il est préférable de réaliser des liaisons physiques directes entre les nœuds.

Le dialogue entre les nœuds du cluster s'effectue en multicast[p.183].



La génération de la configuration se fait à l'aide du script `appliquer_hautedispo`.

Pacemaker permet de faire un cluster[p.180] de machines en Haute disponibilité[p.182], dans notre cas l'implémentation du logiciel permet un cluster de deux machines (maître/esclave ou actif/passif). Chaque machine est un nœud du cluster.

Il est recommandé d'utiliser une interface réseau dédiée pour le dialogue inter nœud.

Activer le service de haute disponibilité

Pour activer le service de haute disponibilité il faut se rendre dans l'onglet `Services` et passer la variable `Activer la haute disponibilité` à `maitre` ou `esclave` selon ce que vous souhaitez mettre

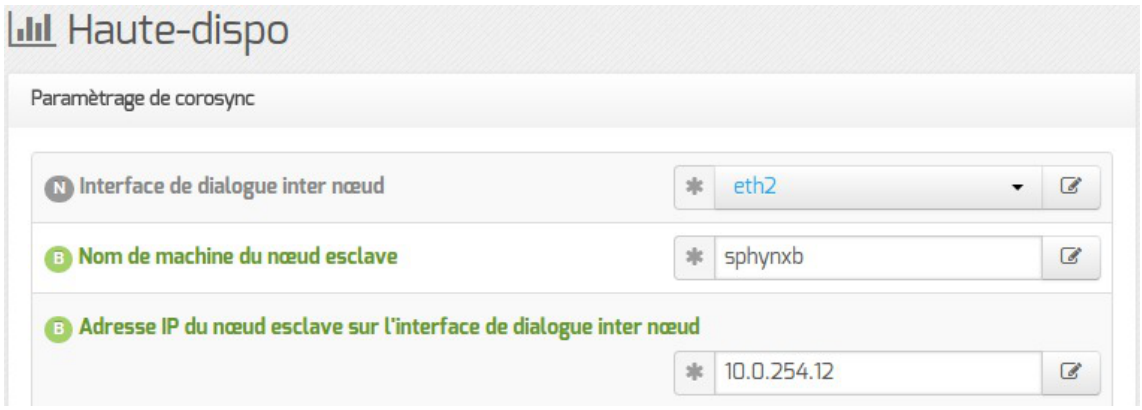
en place.

Vue de l'onglet Services

Il faut ensuite paramétrer le service de haute disponibilité dans l'onglet `Haute-dispo`.

La haute disponibilité en temps que maître

Paramétrage de corosync



Sur le module Sphynx l'interface `Interface de dialogue inter nœud` est prédéfinie sur `eth2`.

Il n'est pas nécessaire de changer cette valeur.

Sur Eolebase on peut choisir une interface dédiée au dialogue inter nœud.

Le `Nom de machine du nœud maitre` doit contenir le `Nom de la machine` configuré renseigné sur le nœud esclave.

`Adresse IP du nœud esclave sur l'interface de dialogue inter nœud` permet de saisir l'adresse IP du nœud esclave.

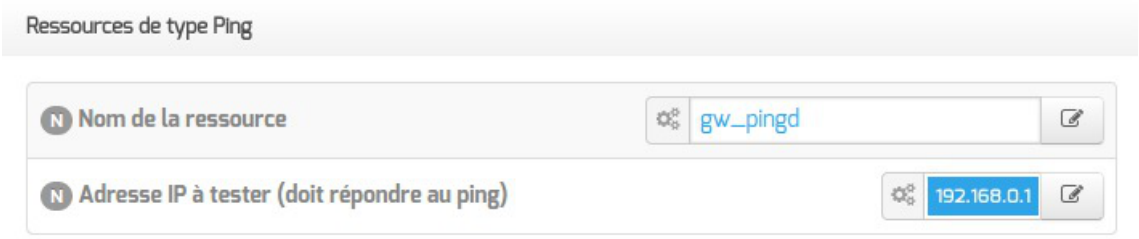
> Le `Nom de machine du nœud esclave` et l'`Adresse IP du nœud esclave sur l'interface de dialogue inter nœud` permettent de renseigner le fichier `hosts` du module.

`Activer l'envoi de courrier électronique lors d'une bascule de nœud` permet de recevoir une alerte lorsque les ressources sont basculées d'un nœud à l'autre.

Le `Nom de la ressource mail` est pré-définie et peut être modifié, il apparaît dans les logs et à l'exécution des commandes `crm` et `crm mon`.

Le champ `Destinataire du courrier électrique` est pré-rempli par la valeur `Adresse électronique recevant les courriers électroniques à destination du compte root` défini dans l'onglet `Messagerie`. Cette valeur, au format adresse électronique, peut être changée si les alertes doivent être envoyées à une autre personne. Il est également possible de choisir le sujet du courrier électronique dans le champ `Sujet du courrier électronique`.

Ressources de type Ping

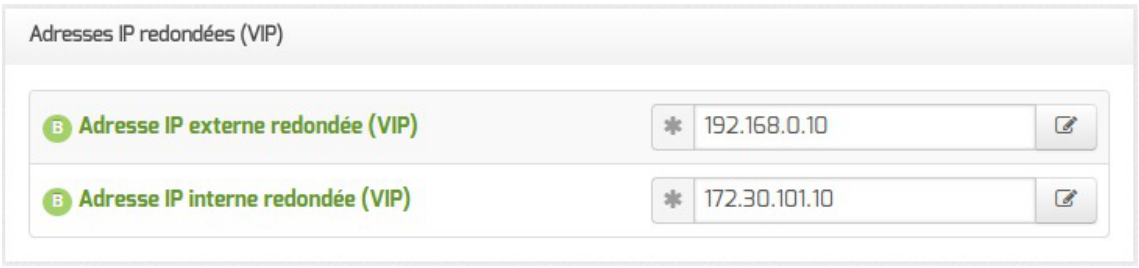


Le `Nom de la ressource` apparaît dans les logs et les commandes `crm` et `crm mon`.

Sur le module Sphynx la valeur `Nom de la ressource` est pré-définie et ne doit surtout pas être modifiée.

Sur Eolebase ce champ peut contenir le nom de votre choix sans espace et sans caractères spéciaux.

Adresses IP redondées (VIP)

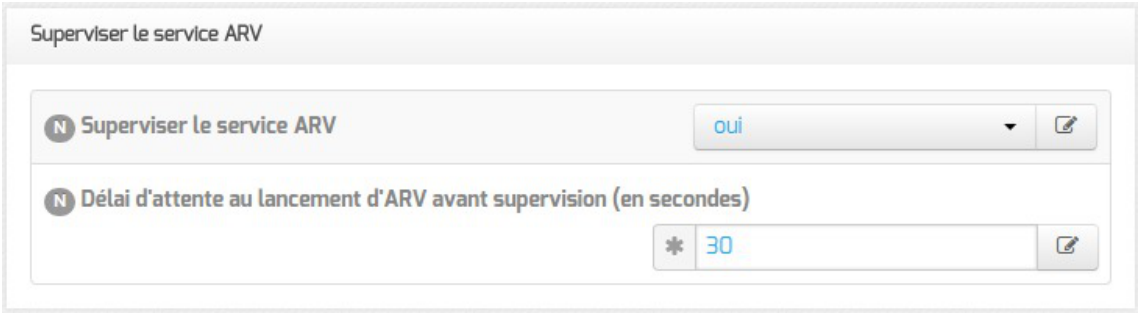


Les adresses IP redondées sont des ressources de type IP virtuelle et permettent à un cluster d'être accessible via cette adresse sur l'un des deux nœuds. Si l'un des nœuds n'est plus accessible, l'autre prend le relais avec cette même adresse IP.

`Adresse IP externe redondée (VIP)` correspond à l'adresse IP virtuelle de l'interface `eth0`.

`Adresse IP interne redondée (VIP)` correspond à l'adresse IP virtuelle de l'interface `eth1`.

Superviser le service ARV



Par défaut la supervision du service ARV est activé.

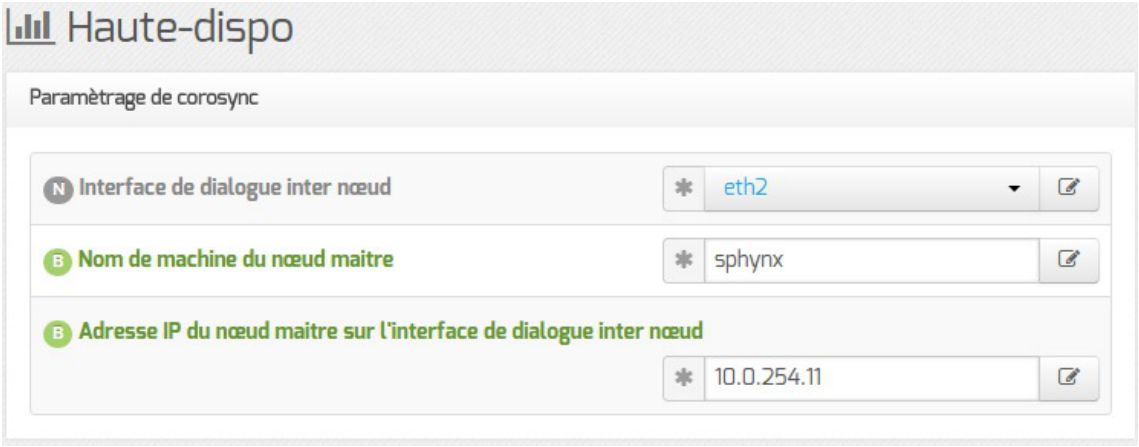
Le service ARV met un certain temps à se lancer suivant la vélocité de la machine, le délai d'attente permet de différer la supervision du service. Il est également possible de désactiver complétement la supervision en passant `Superviser le service ARV` à `non`.

Sur le module Sphynx la synchronisation des fichiers de configuration sur le nœud esclave est forcée et ne peut pas être modifiée. Elle est visible uniquement en mode Debug.

En mode expert l'adresse et le port multicast dédiés au dialogue inter nœuds peuvent être changés pour éviter un éventuel conflit avec un adressage déjà utilisé.

La haute disponibilité en temps qu'esclave

Paramétrage de corosync



Sur le module Sphynx l'interface `Interface de dialogue inter nœud` est prédéfinie sur `eth2`.

Il n'est pas nécessaire de changer cette valeur.

Le `Nom de machine du nœud maitre` doit contenir le `Nom de la machine` configuré renseigné sur le nœud maître.

`Adresse IP du nœud maitre sur l'interface de dialogue inter node` permet de saisir l'adresse IP du nœud maître.

> Le `Nom de machine du nœud maitre` et l'`Adresse IP du nœud maitre sur l'interface de dialogue inter nœud` permettent de renseigner le fichier `hosts` du module.

En mode expert l'adresse et le port multicast dédiés au dialogue inter nœuds peuvent être changés pour éviter un éventuel conflit avec un adressage déjà utilisé.

3.12. Onglet Onduleur

Sur chaque module EOLE, il est possible de configurer votre onduleur.

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.184]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

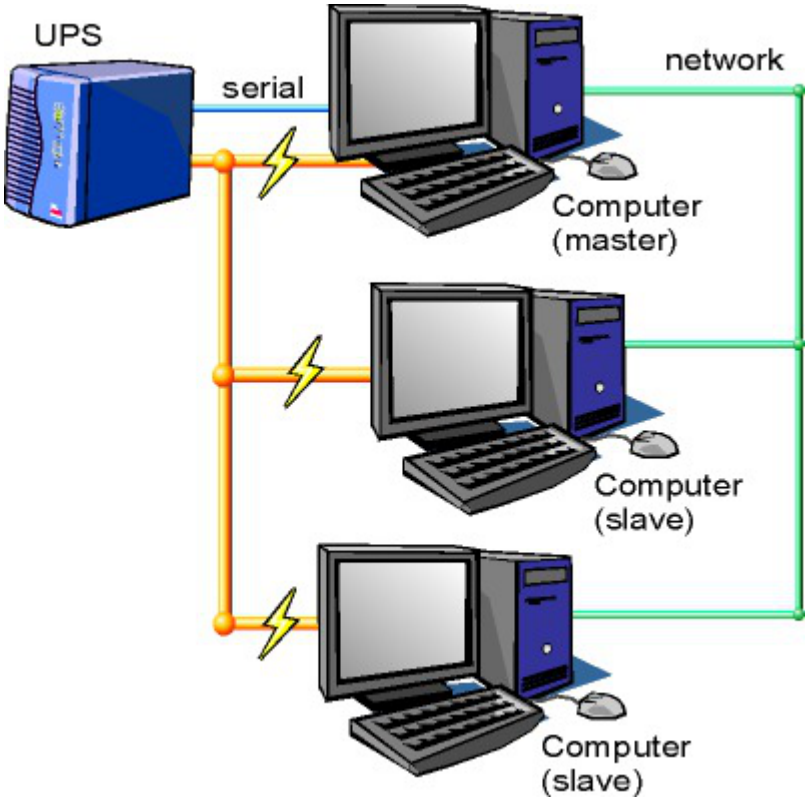


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

http://www.networkupstools.org/stable-hcl.html

Pour connaître la version de NUT qui est installée sur le module :

```
# apt-cache policy nut
```

ou encore :

```
# apt-show-versions nut
```

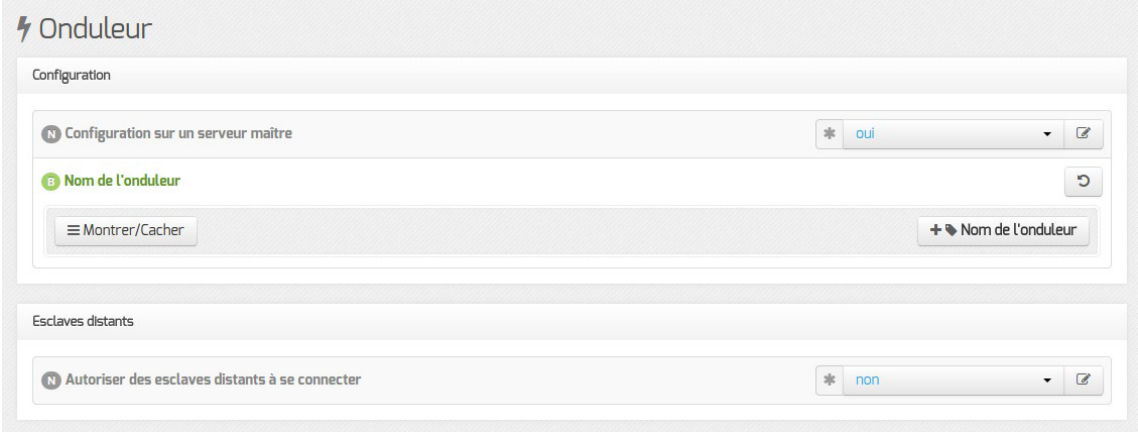
Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

http://www.networkupstools.org/source/2.7/new-2.7.1.txt

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

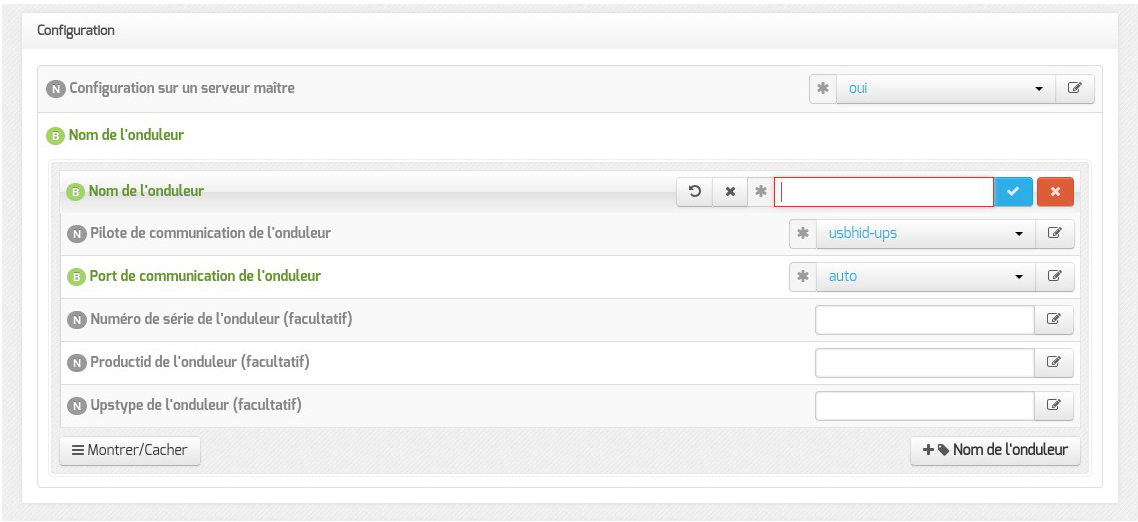
http://www.networkupstools.org/source/2.7/new-2.7.3.txt

L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.



Si l'onduleur est branché directement sur le module il faut laisser la variable `Configuration sur un serveur maître` à `oui`, cliquer sur le bouton `+ Nom de l'onduleur` et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître



Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ `Nom pour l'onduleur`.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante `Pilote de communication de l'onduleur` et éventuellement préciser le `Port de communication` si l'onduleur n'est pas USB.

Les champs `Numéro de série de l'onduleur`, `Productid de l'onduleur` et `Upstype de l'onduleur` sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

> Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un

onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost|grep <nom variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;

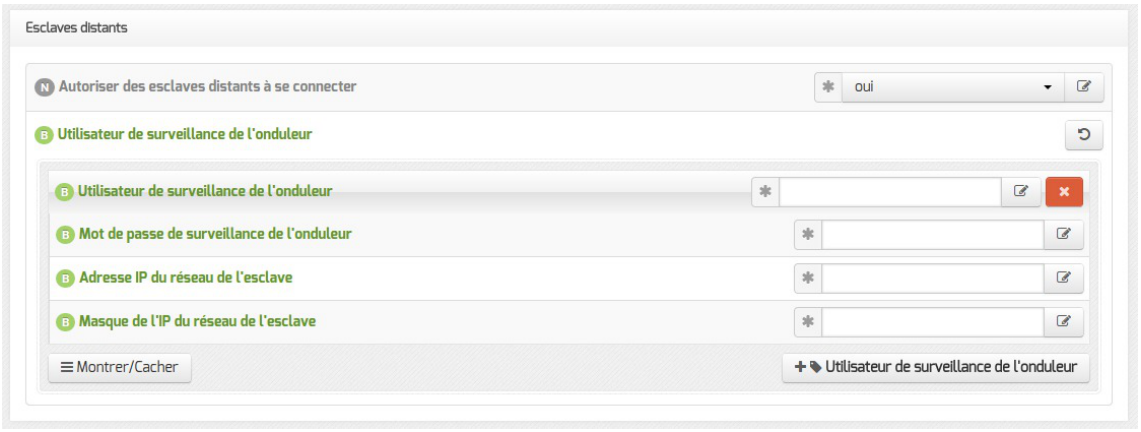
- Port de communication de l'onduleur : `auto`.

La majorité des onduleurs USB sont détectés automatiquement.

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave a se connecter avec cet utilisateur.



Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

Chaque utilisateur doit avoir un nom différent.

Les noms `root` et `localmonitor` sont réservés.

Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf`

> ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il est possible de configurer le ou les serveurs esclaves.

Pour configurer le module en tant qu'esclave, il faut activer le service dans l'onglet `Services` puis, dans l'onglet `Onduleur`, passer la variable `Configuration sur un serveur maître` à `non`.

Il faut ensuite saisir les paramètres de connexion à l'hôte distant :

- le `Nom de l'onduleur distant` (valeur renseignée sur le serveur maître) ;
- l'`Hôte gérant l'onduleur` (adresse IP ou nom d'hôte du serveur maître) ;
- l'`Utilisateur de l'hôte distant` (nom d'utilisateur de surveillance créé sur le serveur maître) ;
- le `Mot de passe de l'hôte distant` (mot de passe de l'utilisateur de surveillance créé sur le serveur maître).

Exemple de configuration

Sur le serveur maître :

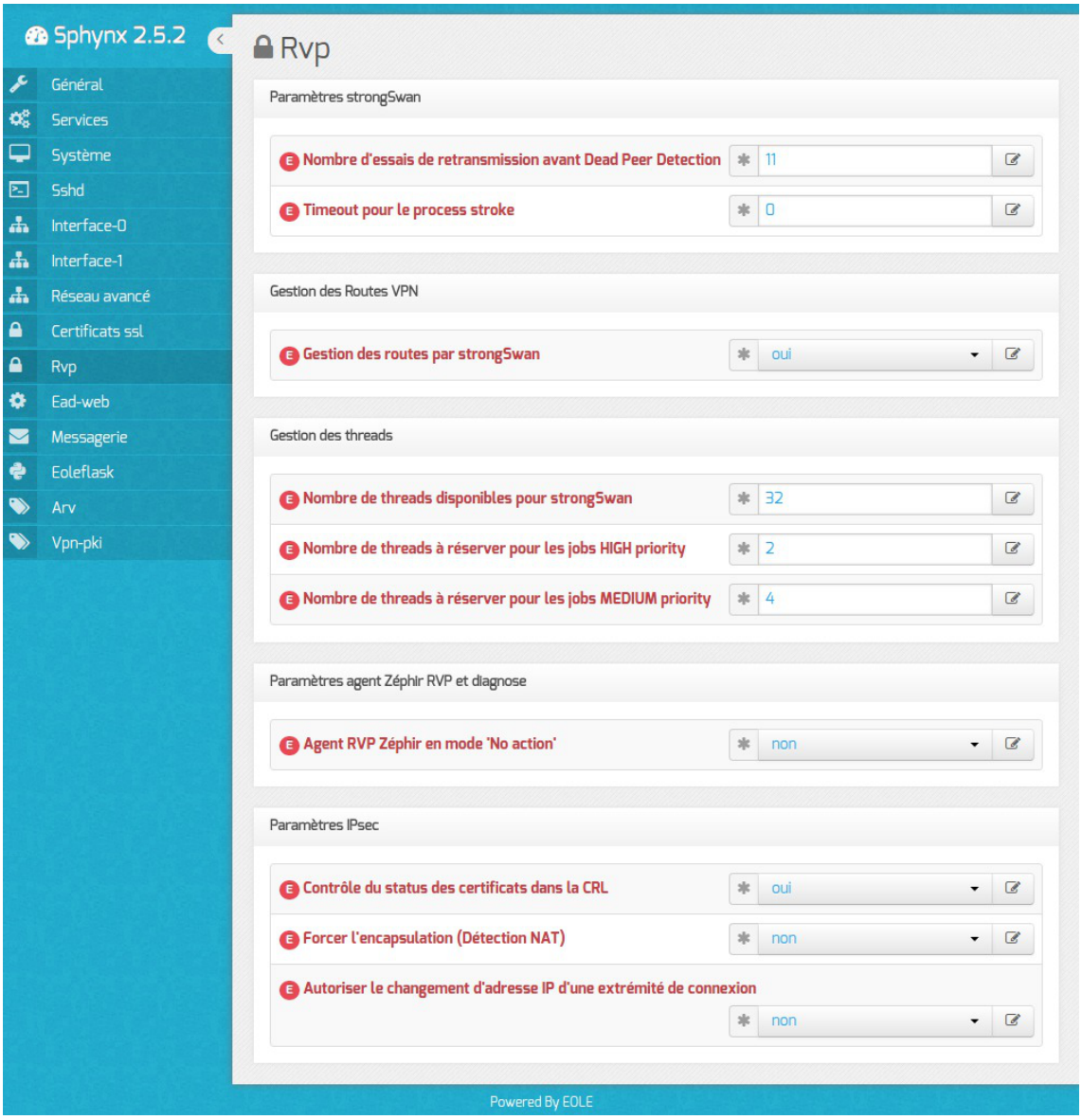
- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto` ;
- Utilisateur de surveillance de l'onduleur : `scribe` ;
- Mot de passe de surveillance de l'onduleur : `99JJUE2EZOAI2IZI10IIZ93I187UZ8` ;
- Adresse IP du réseau de l'esclave : `192.168.30.20` ;
- Masque de l'IP du réseau de l'esclave : `255.255.255.255`.

Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;

- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

3.13. Onglet Rvp : Mettre en place le réseau virtuel privé



Onglet Rvp mode Expert

Sphynx-ARV et Sphynx distant

Un module Sphynx peut être dédié ou non à la gestion des configurations RVP :

- un module Sphynx dédié à la gestion des configurations RVP avec ARV est appelé **Sphynx-ARV** ;
- un module Sphynx dont la configuration RVP est gérée par un autre module (Sphynx-ARV) est appelé **Sphynx distant**.

Sur un serveur **Sphynx distant** la mise en place du RVP se fera comme sur un serveur Amon.

Configuration des tunnels

Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.2 du module Sphynx. La configuration des tunnels s'effectue d'office en mode fichier plat.

Un serveur Sphynx en mode fichier plat continuera à communiquer avec des serveurs distants configurés en mode database. La transition pourra se faire progressivement.

À l'occasion de la mise en place d'un nouveau tunnel avec un serveur Amon ou Sphynx dans une version d'EOLE inférieur à 2.5, il faudra impérativement configurer le serveur distant en mode database à non.

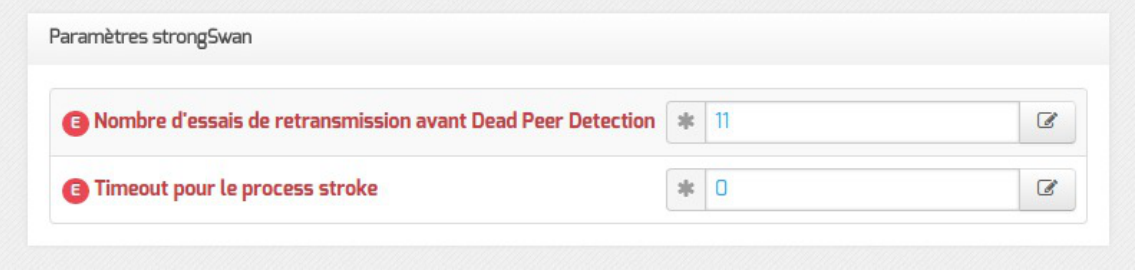
Paramètres propres au mode expert

Le mode Expert permet de personnaliser le fonctionnement de strongSwan.

`Forcer l'encapsulation (Détection NAT)`, si la valeur est à `oui`, cela force la socket UDP/4500 pour l'établissement des connexions. Si la valeur est à `non`, le socket est fixé à UDP/500 sauf s'il y a détection de NAT (UDP/4500).

`Autoriser le changement d'adresse IP d'une extrémité de connexion` (MOBIKE IKEv2 extension - RFC 4555) permet à une extrémité de changer d'adresse IP pour une connexion donnée. Dans ce cas, la connexion se fera toujours sur UDP/4500.

Paramètres strongSwan



`Nombre d'essais de retransmission avant Dead Peer Detection` indique à strongSwan le nombre d'essais de reconnexion avant l'abandon.

`Timeout pour le process stroke` permet de fixer le nombre de millisecondes avant l'arrêt forcé de processus qui se seraient figés.

La variable `Configuration des tunnels en mode database` n'est plus disponible dans la version 2.5 d'EOLE, ce mode a été supprimé au profit du mode fichier plat.

Gestion des Routes VPN

Onglet Rvp mode Expert

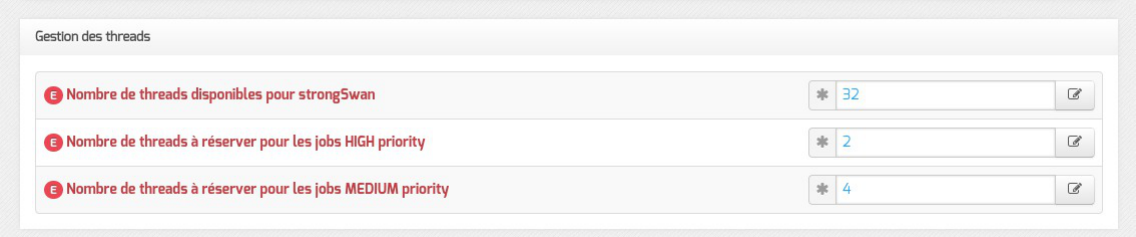
`Gestion des routes par strongSwan` permet si la valeur est passée à `non` de faire gérer la mise en place des routes concernant les tunnels par un script.

Exemple, dans notre cas et sur le module Amon uniquement :

`/etc/ipsec.d/ipsec_updown`

`Forcer l'adresse IP source de l'interface` permet de forcer l'adresse IP que le serveur utilisera pour entrer dans les tunnels. Cette option est utilisée sur les serveur Amon afin d'éviter qu'ils utilisent aléatoirement l'adresse IP de l'une de ses interfaces lorsqu'ils passent dans un tunnel.

Gestion des threads



`Nombre de threads disponibles pour strongSwan` permet d'allouer un nombre de fils d'exécution maximum pour ses différentes tâches. Une valeur trop petite peut entraîner des mises en file d'attente importantes.

`Nombre de threads à réserver pour les jobs HIGH priority` réserve une nombre de fils d'exécution minimum pour les tâches HIGH priority (`ipsec stroke` et DPD). La valeur `1` ou `2` maximum est idéale.

`Nombre de threads à réserver pour les jobs MEDIUM priority` réserve une nombre de fils d'exécution minimum pour les tâches MEDIUM priority (Initialisation de connexion entre autres).

Paramètres agent Zéphir RVP et diagnose

Onglet Rvp mode Expert

`Agent rvp Zéphir en mode 'No action'` permettait sur les versions strictement inférieures à EOLE 2.4.2 de paramétrer l'agent RVP pour ne rien faire en cas de détection de tunnels défectueux (pas de coupure/relance des tunnels).

Cette variable est sans effet depuis la version EOLE 2.4.2.

Paramètres IPsec

Onglet Rvp mode Expert

Active ou non la vérification de la validité d'un certificat dans la liste de révocation (CRL[p.181]).

Application de la configuration et gestion du RVP

Application de la configuration RVP sur un module Sphynx-ARV

L'application de la configuration RVP se fait au moment de leur génération avec l'application ARV.

Activation du RVP sur un module Sphynx distant

Pour activer un RVP sur un module Sphynx distant déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Au lancement de la commande `active_rvp init`, le choix `1.Manuel` ou `2.Zéphir` est proposé.

- Le choix 1 permet de prendre en compte la configuration RVP présente sur une clé USB.
- Le choix 2 active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un utilisateur et mot de passe Zéphir et l'identifiant Zéphir du serveur Sphynx.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine.

Les tunnels déjà mis en place sur un module Sphynx distant ne sont pas coupés lors de l'utilisation de la commande `active_rvp init`.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

3.14. Onglet Ead-web : EAD et proxy inverse

Si l'interface web de l'EAD est activée sur le module (onglet `Services`), les paramètres de l'onglet `Ead-web` permettent de régler le port d'accès à l'interface EAD depuis l'extérieur si un proxy inverse est utilisé.

Par défaut l'utilisation d'un proxy inverse pour accéder à l'EAD est à `non`.

Si la variable est passée à `oui`, le port proposé pour accéder à l'EAD depuis l'extérieur est par défaut 4203.

Voir aussi...

> Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur

3.15. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

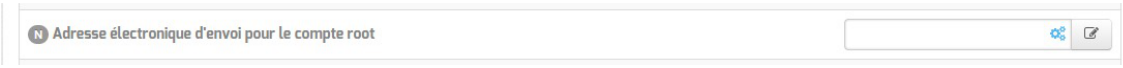
Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

> Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

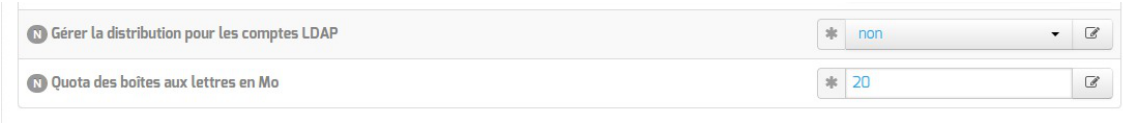
> Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.
>
> Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.



En mode normal il est possible de configurer le nom de l'émetteur des messages pour le compte `root`.

> Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.



Passer `Gérer la distribution pour les comptes LDAP` à `oui` active les transports LDAP pour la distribution des courriers électroniques, la distribution des courriers locaux est forcée ainsi ils ne sont pas mis en queue et supprimés une semaine plus tard.

Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

En mode expert il est possible d'écraser l'entêtes des courriers électroniques.

La réécriture des adresses doit prendre en compte la distinction entre l'enveloppe SMTP (« MAIL FROM » et « RCPT TO ») et les en-têtes des messages (« From: », « Reply-To:», « To: », « Cc: », « Bcc: »).

Les adresses électroniques systèmes ont par défaut une des formes suivante :

- `user@%%domaine messagerie etab` si l'expéditeur ne précise pas le nom de domaine, par exemple :

  ```
  root@internet:~# echo "Test" | mail -s "Test mail from shell" -r root root
  ```

- `user@%%nom machine.%%domaine messagerie etab` pour le maître si l'expéditeur utilise la configuration définie dans `/etc/mailname`
- `user@%%conteneur.%%nom machine.%%domaine messagerie etab` pour les conteneurs[p. 180] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

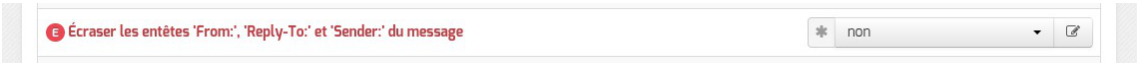
Si la valeur de `%%nom domaine local` est différente de la valeur de `%%domaine messagerie etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

- `user@%%nom machine.%%domaine messagerie etab` pour le maître
- `user@%%conteneur.%%nom machine.%%domaine messagerie etab` pour les conteneurs

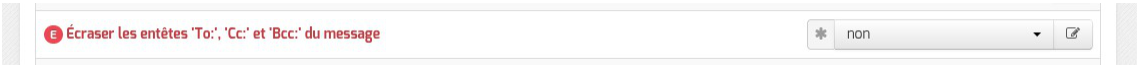
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

Les adresses expéditeurs et destinataires systèmes sont ensuite réécrites selon les tableaux suivants en fonction de variables expertes :

- `system_mail_from_for_headers` : écraser les en-têtes « From: », « Reply-To: » et « Sender: » du message, par défaut à `non`



- `system_mail_to_for_headers` : écraser les en-têtes « To: », « Cc: » et « Bcc: » du message, par défaut à `non`



Réécriture de l'expéditeur :

	system_mail_from_for_headers = non	system_mail_from_for_headers = oui
MAIL FROM	system_mail_from	system_mail_from
From :	user@conteneur.machine.domaine	system_mail_from
Reply-To :	user@conteneur.machine.domaine	system_mail_from
Sender :	user@conteneur.machine.domaine	system_mail_from

Réécriture du destinataire :

	system_mail_to_for_headers = non	system_mail_to_for_headers = oui
RCPT TO	system_mail_to	system_mail_to
To :	user@conteneur.machine.domaine	system_mail_to
Cc :	user@conteneur.machine.domaine	system_mail_to
Bcc :	user@conteneur.machine.domaine	system_mail_to

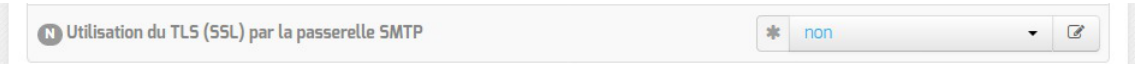
Par défaut la distribution des messages se fait en local, ce qui permet d'avoir un domaine local et un domaine privé.

Dans ce cas il est possible d'agir sur le quota des boîtes et sur le pourcentage d'occupation, qui entraîne un message électronique d'avertissement.

Relai des messages

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

> Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.
>
> Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.187] pour l'envoi de message. Si la passerelle SMTP[p.186] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.186] (port 25) ou non (port 465).

Par défaut le relai des messages n'est pas activé sur les modules sauf sur le module Seshat. Si la variable est passée à oui, elle active les listes d'adresses IP autorisées à utiliser ce serveur comme relai de messagerie et la liste des noms de domaines autorisés à être relayés par ce serveur.

Le TLS est activé par défaut pour les clients.

Dans la rubrique Configuration experte plusieurs paramètres peuvent être modifiés.

- `FQDN utilisé par Exim`
  Personnalisation du nom de domaine complètement qualifié utilisé par Exim dans le protocole SMTP.

C'est utile pour les vérifications anti-spam des MX externes

Les valeurs possibles sont :

- automatique : laisser Exim décider ;
- nom_machine.domaine_messagerie_etab : utiliser le nom de la machine complété par le nom de domaine de la messagerie établissement ;
- nom_machine.nom_domaine_local : utiliser le nom de la machine complété par le nom de domaine local.

- `Domaine utilisé pour qualifier les adresses`

  Nom de domaine ajouté aux adresses :

  - nom de domaine local ;
  - domaine privé de messagerie établissement ;
  - domaine public de messagerie établissement.

- `Envoyer les logs à rsyslog`

  Permet de désactiver l'envoi des logs.

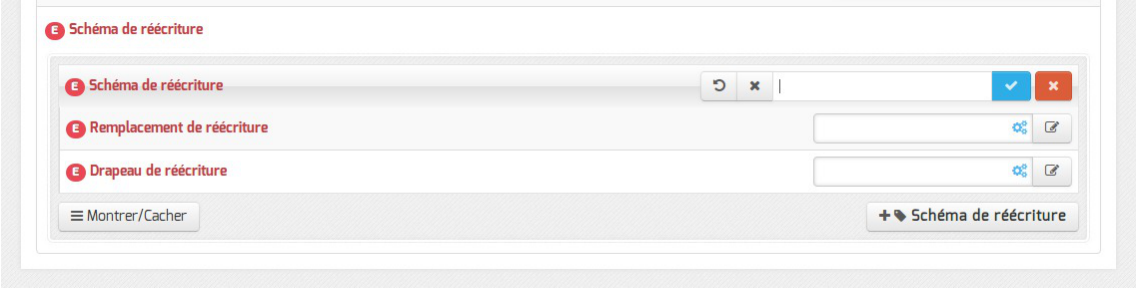
- `Dupliquer les logs dans des fichiers`

  Dupliquer les logs dans des fichiers gérés directement par Exim. Si vous envoyez les logs à syslog, vous pouvez conserver la gestion des fichiers traditionnelle d'Exim. Ces fichiers étant gérés directement par Exim, ils se trouveront dans le conteneur du service.

- `Activer les règles de réécriture étendue`

  Permettre de définir des règles de réécriture personnalisées. Si non, seuls les courriers électroniques en `localhost` sont réécrits avec le `nom domain local`.

  http://exim.org/exim-html-current/doc/html/spec_html/ch31.html.

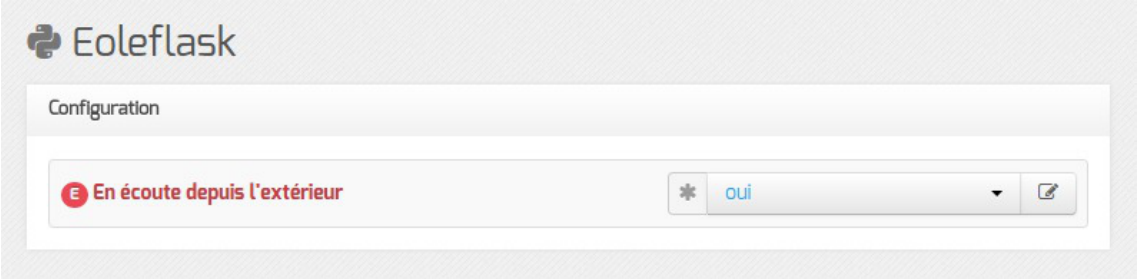


Les trois variables à saisir sont :

- Modèle de correspondance des adresses courriers électroniques à réécrire : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID151
- Valeur de remplacement des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID152
- Drapeau contrôlant la réécriture des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID153

3.16. Onglet Eoleflask

Dans cet onglet se trouvent les options concernant le service Eoleflask et les options des applications reposant sur ce service.



Passer la variable `En écoute depuis l'extérieur` à `oui` permet d'accéder à l'interface de configuration du module depuis un poste client.

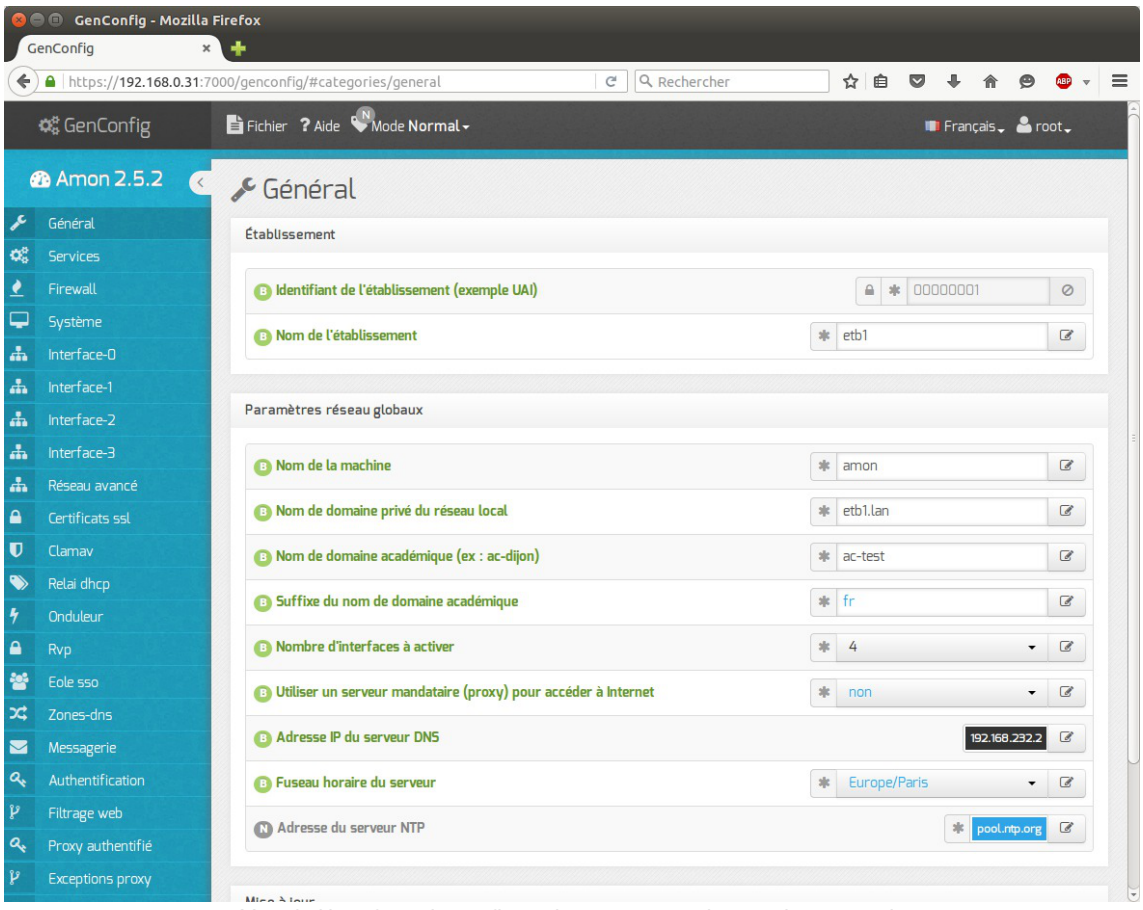
Accès distant

Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

`https://<adresse_serveur>:7000/genconfig/`

Ne pas oublier d'utiliser le protocole HTTPS et de préciser le numéro de port 7000.

Il faut ensuite valider les certificats pour pouvoir accéder à l'interface.



Vue de l'interface de configuration au travers d'un navigateur web

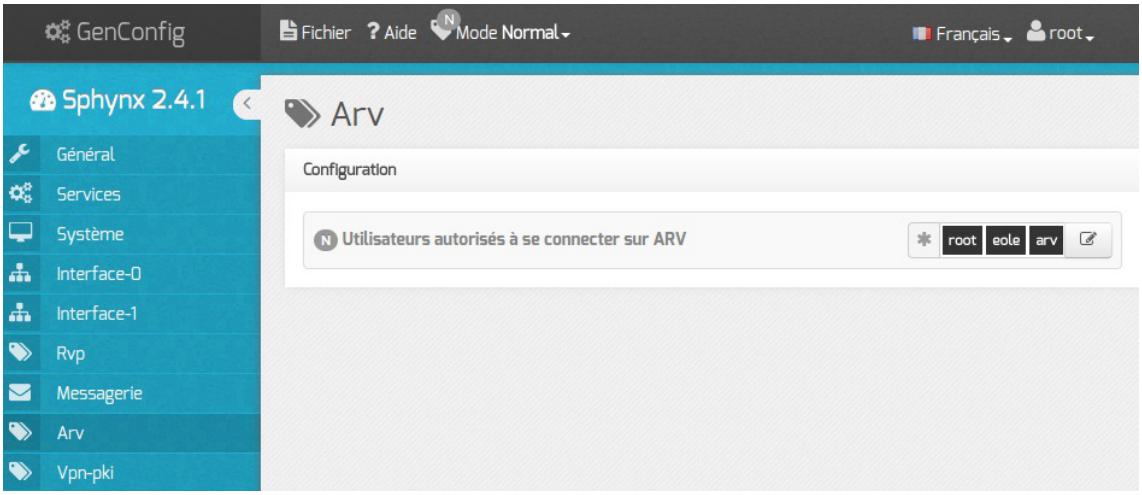
Pour autoriser l'accès distant à une ou plusieurs adresses IP il faut le déclarer explicitement dans l'onglet `Interface-n` de l'interface de configuration du module en passant la variable `Autoriser les connexions SSH` à `oui`.

3.17. Onglet Arv : Configuration du logiciel ARV

ARV est une application qui permet de construire des modèles et de générer des configurations RVP[p.185] pour strongSwan[p.186] [http://www.strongswan.org/ -] .

Les utilisateurs autorisés à se connecter sur ARV peuvent être des comptes systèmes locaux et des comptes Zéphir.

Pour qu'un compte puisse avoir accès à ARV, il faut impérativement les déclarer dans l'interface de configuration du module.



Gestion des utilisateurs autorisés à se connecter sur ARV

Les comptes Zéphir doivent avoir les droits en `Lecture` et `Configuration vpn`.

Voir aussi...

L'application ARV [p.111]

3.18. Onglet Vpn-pki

Sphynx fonctionne aussi bien avec des certificats auto-signés qu'en mode certificats signés pour le réseau AGRIATES[p.178].

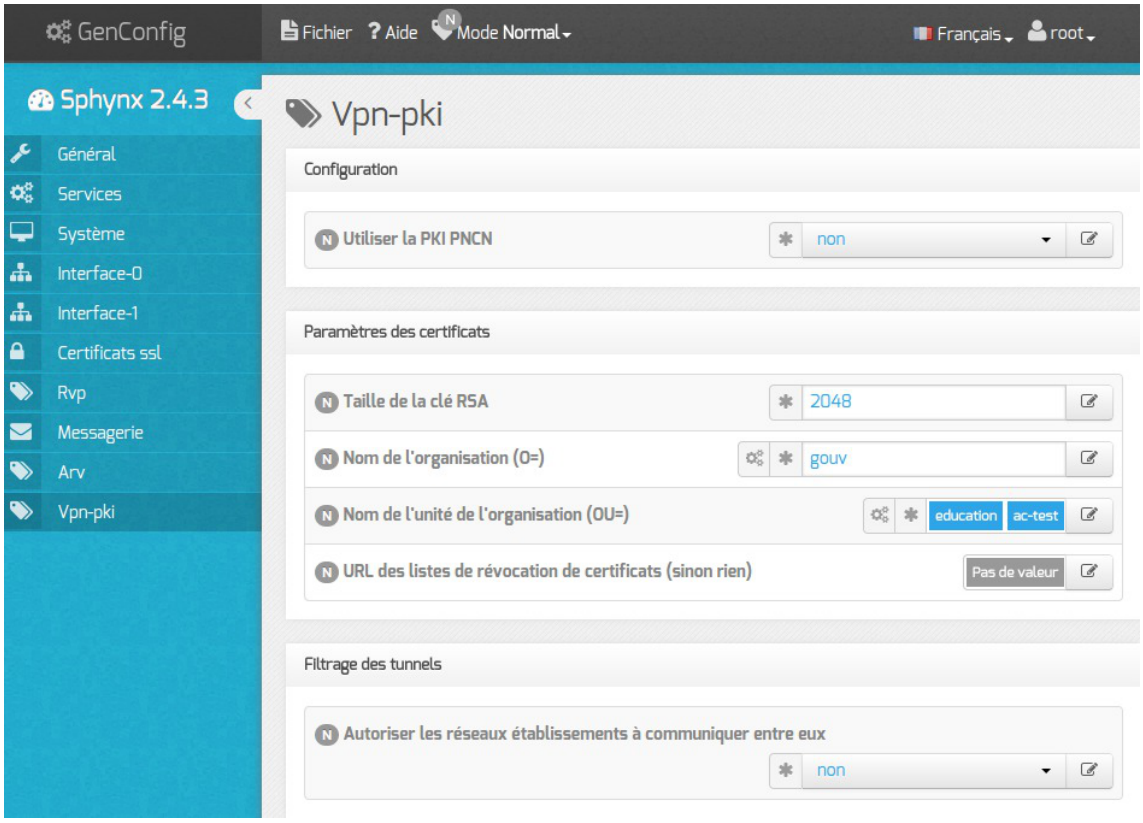
Par défaut, l'instanciation du module Sphynx génère une base ARV minimale avec uniquement les modèles de serveur `sphynx` et `etablissement`.

Un script nommé `init_sphynx` permet de générer une base ARV adaptée au réseau AGRIATES.

Il est possible d'utiliser la nouvelle PKI PNCN[p.185] ou l'ancienne PKI RACINE AGRIATES.

Les tunnels VPN sont actuellement basés sur la PKI RACINE AGRIATES mais la nouvelle PKI PNCN va prochainement la remplacer. La configuration OpenSSL préparée par le module pour effectuer les requêtes auprès de l'IGC est conditionnée par la variable `Utiliser la PKI PNCN`.

Utilisation de l'ancienne PKI RACINE AGRIATES

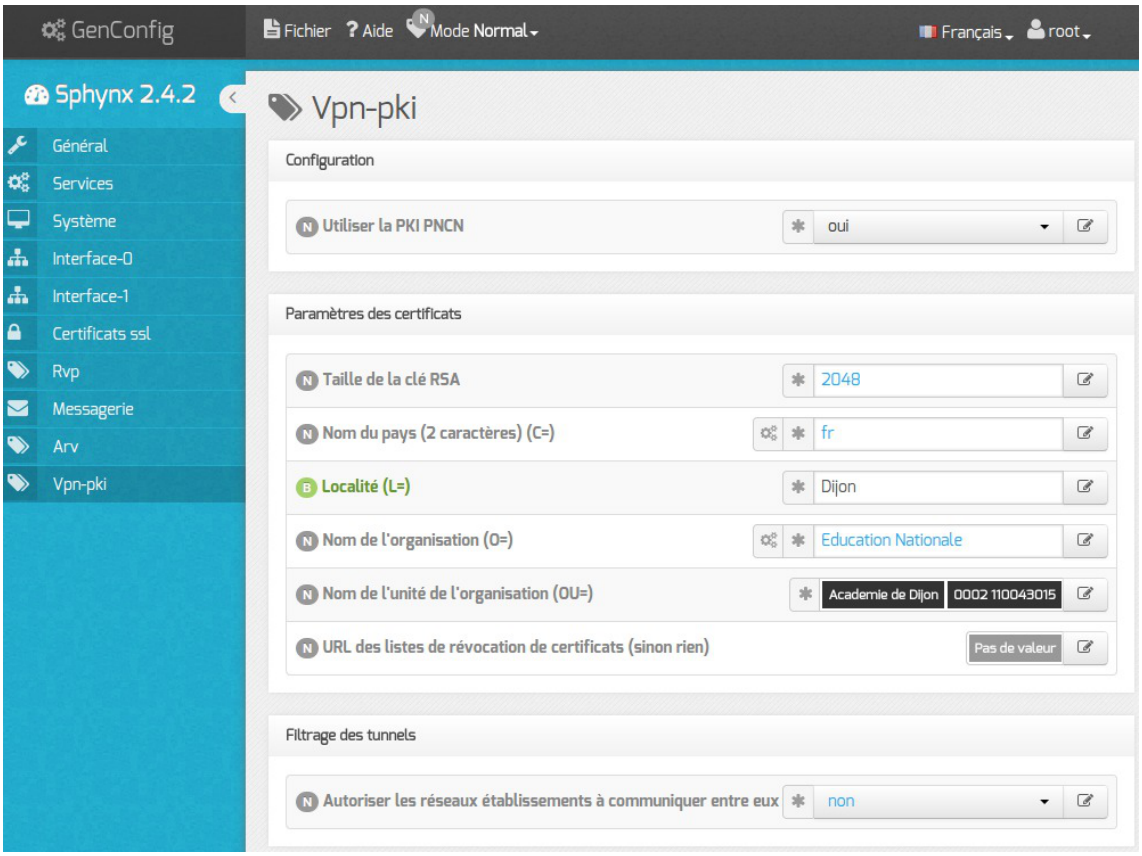


Configuration du VPN sur Sphynx

- `Taille de la clé RSA` : champ pré-rempli et obligatoire ;
- `Nom de l'organisation` : champ pré-rempli et obligatoire ;
- `Nom de l'unité de l'organisation` : champ pré-rempli et obligatoire ;
- `URL des listes de révocation des certificats` : les URL de révocation fournies par l'IGC sont à placer ici, cette variable est optionnelle car ces URL sont dorénavant intégrées aux certificats.

Utilisation de la nouvelle PKI PNCN

Pour utiliser la nouvelle PKI PNCN[p.185] il faut passer la variable `Utiliser la PKI PNCN` à `oui`. Un champ supplémentaire concernant la localité est à remplir obligatoirement.



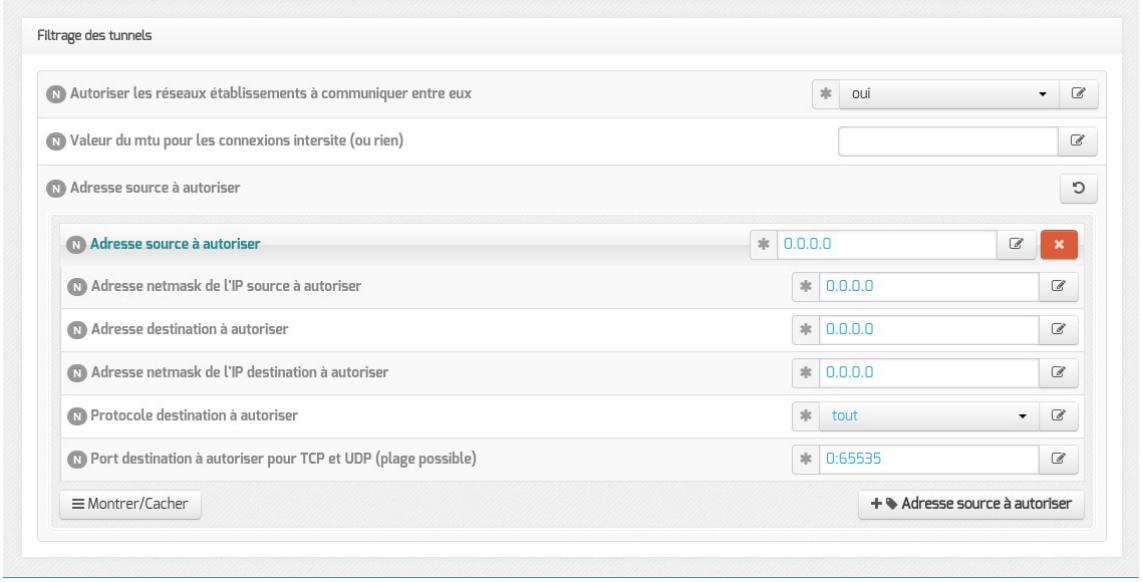
- `Taille de la clé RSA` : champ pré-rempli et obligatoire ;
- `Localité` : champ obligatoire ;
- `Nom de l'organisation` : champ pré-rempli et obligatoire ;
- `Nom de l'unité de l'organisation` : champ et obligatoire ;

  Il est impératif de respecter l'ordre des OU : *Academie de nomAcademie - 0002 110043015*

  Vous trouverez plus de détails sur le site du pôle PNCN à l'adresses suivante :
  - https://pole.pncn.education.gouv.fr/content/demande-dun-certificat-scolarité-et-formation
- `URL des listes de révocation des certificats` : les URL de révocation fournies par l'IGC sont à placer ici, cette variable est optionnelle car ces URL sont dorénavant intégrées aux certificats.

Filtrage des tunnels

Il est possible d'autoriser les communications entre deux serveurs Amon en passant par le concentrateur Sphynx, il faut pour cela renseigner les différentes adresses réseaux à filtrer.



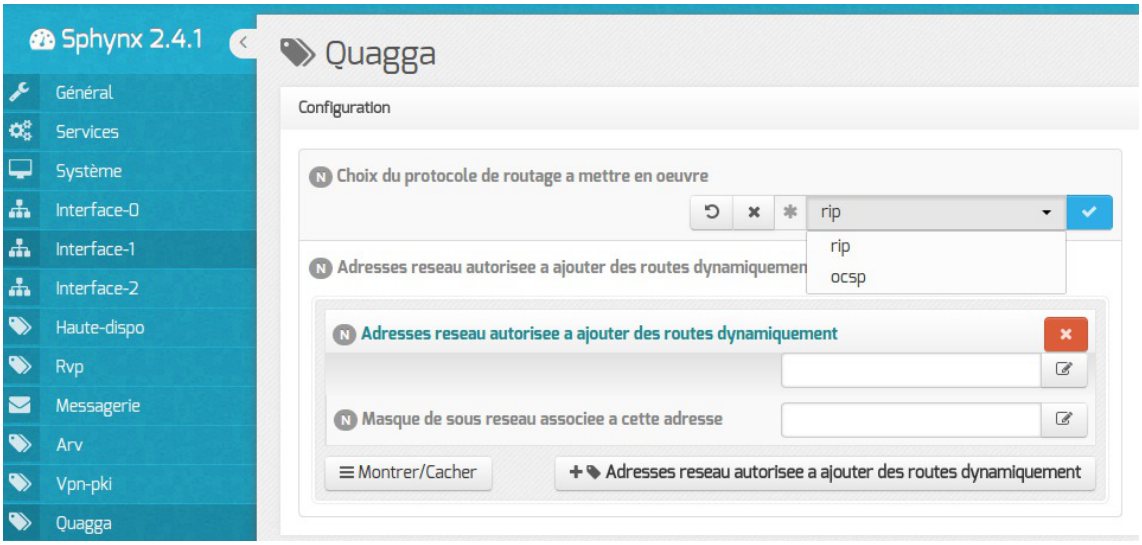
Parmi les paramètres il faut spécifier le réseau source, le réseau destination, le protocole ainsi que les ports autorisés à communiquer entre eux.

3.19. Onglet Quagga : Configuration du routage dynamique

Le routage dynamique peut être activé afin de ne pas avoir à gérer les routes statiques sur le serveur. Dans l'onglet service il faut passer `Activer le routage dynamique sur l'interface interne 1` à `oui`. Cela va activer le logiciel Quagga[p.185] sur l'interface eth1.

Onglet Services

Un nouvel onglet dans l'interface de configuration du module permet de choisir le protocole à utiliser et d'autoriser des réseaux à ajouter des routes.



Onglet Quagga

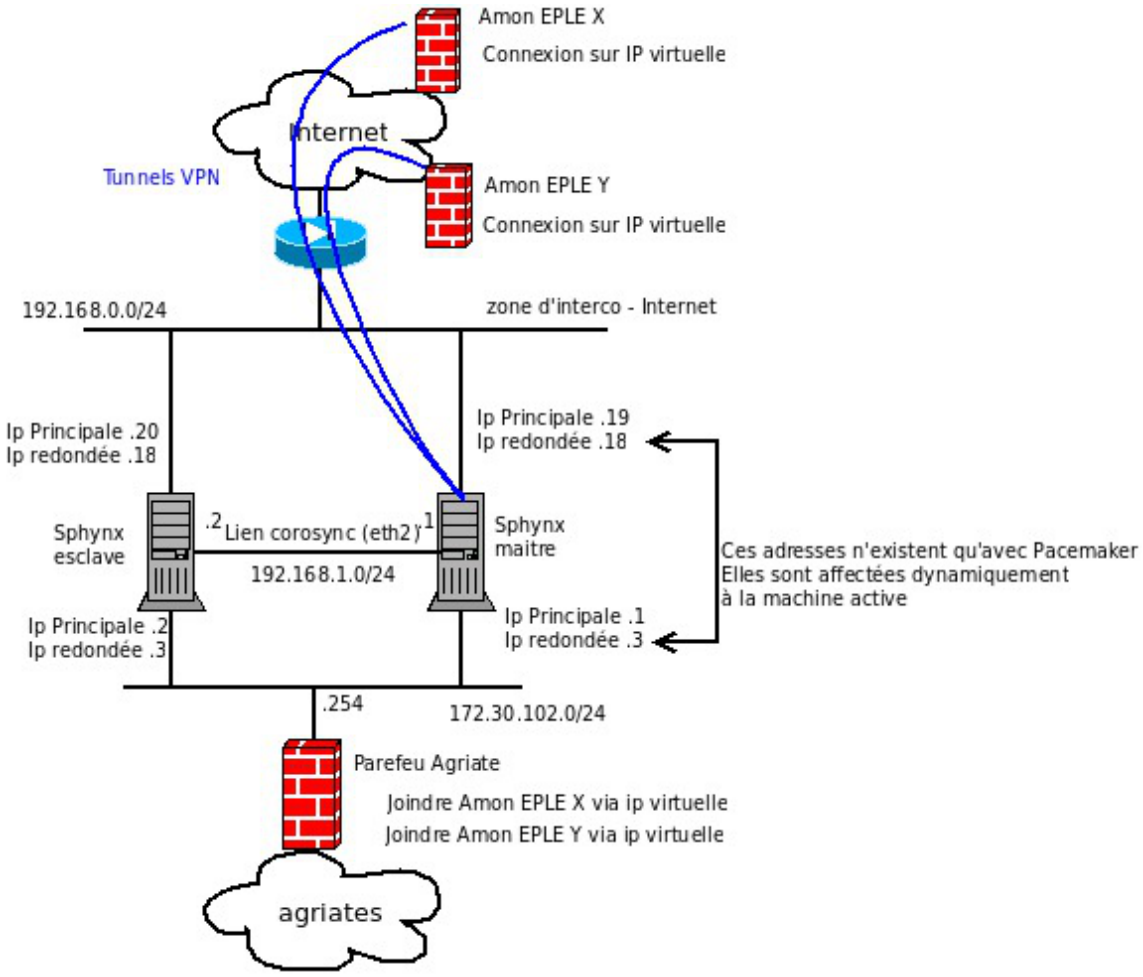
4. Mettre en place un cluster haute disponibilité

EOLE propose un service de haute disponibilité dont le rôle principal est de garantir la disponibilité d'un service et son bon fonctionnement.

Il est possible, depuis l'interface de configuration du module, d'activer ou non ce service.

Il est préférable de réaliser des liaisons physiques directes entre les nœuds.

Le dialogue entre les nœuds du cluster s'effectue en multicast[p.183].



La génération de la configuration se fait à l'aide du script `appliquer_hautedispo`.

Pacemaker permet de faire un cluster[p.180] de machines en Haute disponibilité[p.182], dans notre cas l'implémentation du logiciel permet un cluster de deux machines (maître/esclave ou actif/passif). Chaque machine est un nœud du cluster.

Il est recommandé d'utiliser une interface réseau dédiée pour le dialogue inter nœud.

Installer et configurer un module Sphynx qui sera la machine maître.

Installer et configurer un module Sphynx qui sera la machine esclave.

Sur le serveur Sphynx maître, exécuter l'instance à l'aide de la commande :

```
# instance
```

À la question `Voulez vous synchroniser les nœuds ?` il ne faut rien saisir et passer l'autre machine.

Sur le serveur Sphynx esclave, exécuter l'instance à l'aide de la commande :

```
# instance
```

À la question `Voulez vous synchroniser les nœuds ?` répondre `oui` (les deux serveurs Sphynx doivent pouvoir communiquer en SSH).

Au moment de l'envoi de la clé RSA sur le serveur Sphynx, saisir le mot de passe de l'utilisateur `root` du serveur Sphynx maître.

À la question `Voulez vous attendre le script synchro-nodes.sh soit exécuté sur le nœud maître ?` il ne faut rien saisir et passer l'autre machine.

Sur le serveur Sphynx maître, à la question `Voulez vous synchroniser les nœuds ?`, toujours en attente, il faut répondre `oui`.

Au moment de l'envoi de la clé RSA sur le serveur Sphynx esclave, saisir le mot de passe de l'utilisateur `root` du serveur Sphynx esclave.

Terminer la procédure d'instanciation en répondant aux 2 autres questions.

Si vous êtes connecté en SSH avec la fonctionnalité transfert d'agent[p.178] (option par défaut de la commande `ssh`) et que la clé privée a été copiée sur le serveur distant, la phrase secrète n'est pas demandée.

Sur le serveur Sphynx esclave, à la question `Voulez vous attendre le script synchro-nodes.sh soit executé sur le nœud maître ?`, toujours en attente, il faut répondre `oui`.

Terminer la procédure d'instanciation en répondant aux 2 autres questions.

Sur le serveur Sphynx esclave, exécuter la commande diagnose :

```
# diagnose
```

Les compte rendus sont à `OK`.

Sur le serveur Sphynx maître, exécuter la commande diagnose :

```
# diagnose
```

Les compte rendus sont à `OK`.

Sur le serveur Sphynx maître, afficher le contenu du fichier `/etc/ha.d/.rsc_list` :

```
# cat /etc/ha.d/.rsc_list
```

Les ressources suivantes de type service sont présentes :

```
ipsec_rsc
arv_rsc
```

Sur le serveur Sphynx esclave, afficher le contenu du fichier `/etc/ha.d/.rsc_list` :

```
# cat /etc/ha.d/.rsc_list
```

Les ressources suivantes de type service sont présentes :

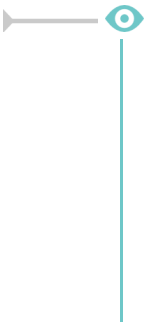
```
ipsec_rsc
arv_rsc
```

Sur le serveur Sphynx maître :

`# crm_mon -1`

La sortie de `crm_mon` permet de visualiser l'état du cluster.

À la ligne `Online` toutes les machines actives sont visibles : le serveur Sphynx maître et le serveur Sphynx esclave.



Ressources démarrées sur le serveur Sphynx maître :

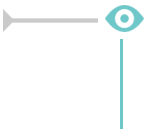
`VIP_externe`

`VIP_interne`

`VIP_src_addr`

`ipsec_rsc`

`arv_rsc`



Ressources démarrées sur les 2 nœuds :

`gw_pingd_clone`

La commande `crm_mon` permet d'afficher l'état du cluster, l'option `-1 –one-shot` affiche l'état à un seul instant et quitte.Il est également possible d'utiliser la commande `crm status`. Cette commande peut aussi bien être utilisé dans l'interface de configuration du cluster.

Voir aussi...

Onglet Haute-dispo : Configuration de la haute disponibilité

Commandes de gestion du cluster [p.158]

5. Scripts de configuration complémentaires

Initialisation de la base ARV

Après instanciation et enregistrement sur le serveur Zéphir, il est possible de régénérer la base ARV du serveur Sphynx avec un script nommé `init_sphynx`. Celui-ci permet de générer une base ARV contenant un modèle adapté au réseau AGRIATES, la base contient :

- un modèle de connexion VPN basé sur l'autorité de certification défini dans l'onglet `Vpn-pki` de l'interface de configuration du module ;
- le(s) certificat(s) CA de la chaîne de certification (contenus dans le fichier au format PKCS7 [p.184] fourni par l'IGC, , Toulouse dans notre cas) ;
- la ou les CRL [p.181] définie(s) dans l'interface de configuration du module ;
- la clé privée et le certificat du serveur Sphynx (optionnel, demandé par le script).

Les fichiers `*****.pkcs7` ou `*****.p7` et `<cléPrivéServeurSphynx>.pem` devront être copiés dans un répertoire temporaire sur le serveur et ce avant lancement du script. Le chemin sera demandé lors de l'exécution du script.

Le modèle prédéfini par le script peut être modifié dans ARV pour l'adapter à votre configuration.

Après exécution du script il est nécessaire de supprimer les fichiers copiés dans le répertoire temporaire.

Prise en compte de la PKI PNCN

Dans le cas d'un serveur fraîchement installé, la prise en compte de la PKI PNCN[p.185] se fait uniquement si cela a été spécifié dans l'onglet `Vpn-pki` de l'interface de configuration du module. Il faudra alors utiliser le script `init_sphynx`.

Le script `init_pncn` est à utiliser dans le cas d'un serveur Sphynx déjà en exploitation avec la PKI RACINE AGRIATES.
Avant d'exécuter ce script, il faut que le serveur soit reconfiguré avec la variable `Utiliser la PKI PNCN` à `oui` dans l'onglet `Vpn-pki`.
Le script `init_pncn` :

- ajoute la chaîne de certification PNCN dans la base ARV ;
- clone les modèles de connexion basés sur la PKI RACINE AGRIATES ;
- renomme les modèles de connexion RACINE AGRIATES ainsi que les modèles de tunnel liés en les préfixant par `OLD_PKI_` ;
- nomme les nouveaux modèles PNCN clonés avec les noms des anciens modèles RACINES AGRIATES.

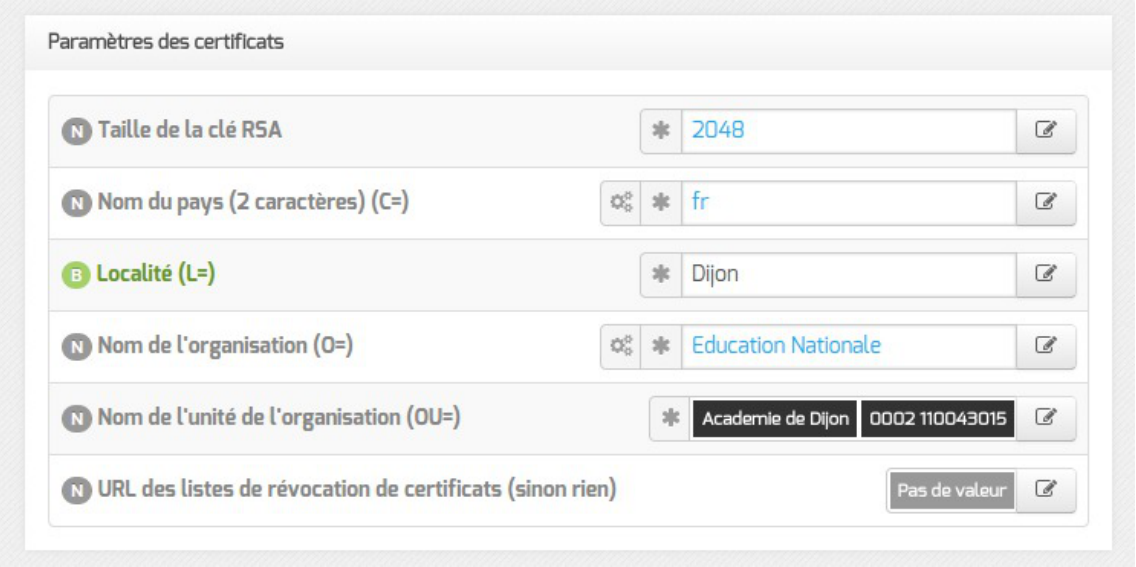
Voir aussi...

Onglet Vpn-pki [p.49]

6. Migration vers la nouvelle PKI PNCN

Procédure pour la migration d'un VPN de l'ancienne vers la nouvelle PKI PNCN[p.185] pour un serveur déjà en production :

- passer `Utiliser la PKI PNCN` à `oui` dans l'onglet `Rvp-pki` de l'interface de configuration du module ;



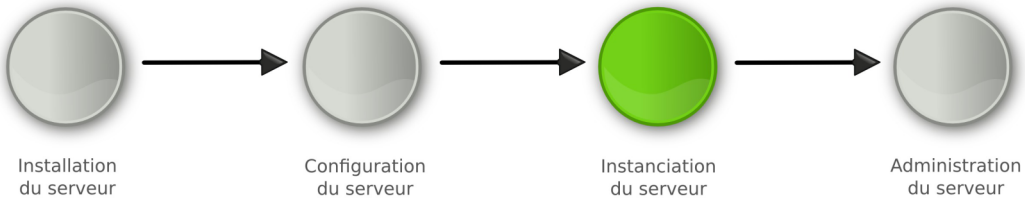
- renseigner la nouvelle variable qui concerne la `Localité` ;
- renseigner au format imposé par l'IGC de Toulouse le `Nom de l'unité de l'organisation` :
  - `Academie de nomAcademie` ;
  - `0002 110043015` ;

  Il est impératif de respecter l'ordre des OU : *Academie de nomAcademie - 0002 110043015*
  Vous trouverez plus de détails sur le site du pôle PNCN à l'adresses suivante :
  - https://pole.pncn.education.gouv.fr/content/demande-dun-certificat-scolarité-et-formation
- supprimer les URLs dans `URL des listes de révocation de certificats (sinon rien)` ;
- enregistrer et quitter l'interface de configuration du module ;
- reconfigurer le serveur à l'aide de la commande `reconfigure` ;
- exécuter le script `init_pncn`, celui-ci permet adapter la base ARV :
  - ajout des certificats de l'autorité de certification de la PNCN ;
  - renommage des modèles de connexion basés sur RACINE AGRIATES ;
  - clonage des modèles de connexion basés sur RACINE AGRIATES.
- dans ARV, chaque serveur à migrer doit avoir un certificat valide sur l'IGC PNCN ;
- dans ARV, modifier la connexion entre 2 serveurs :
  - ajouter le modèle de connexion PNCN ;
  - supprimer le lien basé sur modèle de connexion RACINE AGRIATES ;
  - supprimer le certificat AGRIATES du serveur modifié.
- appliquer les modifications (bouton `Appliquer` de l'application ARV) ;
- sur le serveur Amon modifié, exécuter les commandes :
  - `active_rvp delete`
  - `active_rvp init`

Chapitre 5

Instanciation du module

La troisième des quatre phases



Instanciation

Les généralités sur l'instanciation commune aux différents modules **ne sont pas traitées** dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module concerné.

- La **phase d'instanciation** s'effectue au moyen de la commande `instance` .

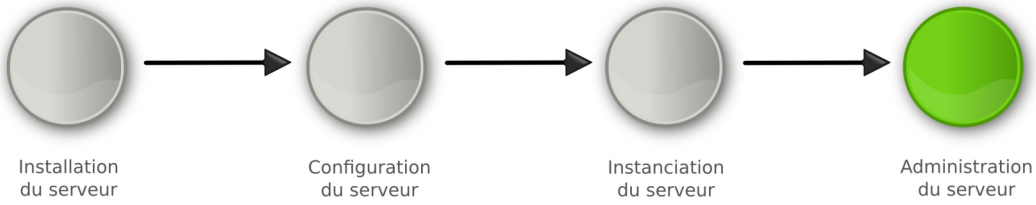
  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

  À l'issue de cette phase, le serveur est utilisable en exploitation.

  Cette phase doit être complétée par un diagnostique complet du module à l'aide de la commande `diagnose -L` .

Chapitre 6

Administration du module Sphynx



Administration

Les généralités sur l'administration et l'administration commune aux différents modules ne sont pas traités dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module.

- La **phase d'administration** correspond à l'exploitation du serveur.
  Chaque module possède des fonctionnalités propres, souvent complémentaires.
  Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

1. L'application ARV

ARV est une application qui permet de construire des modèles et de générer des configurations RVP[p.185] pour strongSwan[p.186] [http://www.strongswan.org/ -] .

Fenêtre principale d'ARV avec l'onglet Modèles

1.1. Présentation de ARV

ARV[p.179] est l'acronyme de : Administration de Réseaux Virtuels.

ARV permet de construire un modèle de configuration RVP[p.185]. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan[p.186].

http://www.strongswan.org/

ARV est pré-configuré dans le module Sphynx.

Le serveur Sphynx doit être enregistré sur Zéphir pour permettre de gérer les RVP des modules EOLE enregistrés sur Zéphir.

Un seul "Sphynx ARV" pourra gérer les RVP des modules Amon mais également d'autres "Sphynx distants".

ARV en mode certificats auto-signés ou certificats signés

Le Réseau Virtuel Privé[p.185] (RVP) est prévu pour fonctionner en mode PKI[p.184] :

- mode certificats auto signés (par CA locale) ;
- mode certificats signés (par CA externe).

Le concentrateur RVP (Sphynx) est pré-configuré pour fonctionner de cette façon.

Les connexions établies à l'aide de certificats auto signés et de certificats signés par une CA externe peuvent coexister sur ce serveur.

Le fonctionnement du concentrateur Sphynx en mode certificats signés nécessite comme pré-requis, un certificat délivré par l'Autorité de Certification (AC ou CA). Toute la gestion des certificats et des clefs nécessite une infrastructure de type RACINE[p.185] (chaque configuration établissement doit obtenir également un certificat).

Les éléments d'un Réseau Virtuel Privé

Un Réseau Virtuel Privé est composé de différents éléments :

- un **concentrateur RVP** :

  il permet la concentration des tunnels en provenance des établissements extérieurs (topologie en étoile) avant de les rediriger vers le sous réseau de concentration choisi ;

- le **pare-feu Amon** :

  point d'entrée dans le réseau établissement et point de sortie unique de l'établissement vers Internet (une extrémité du tunnel RVP) ;

- le **lien sécurisé** :

  lien entre un nœud de type pare-feu Amon et un concentrateur RVP, ce lien est sécurisé par des certificats SSL. Les tunnels passeront dans le lien sécurisé ;

- le **tunnel** :

  connexion au travers l'Internet permettant de relier deux réseaux locaux ;

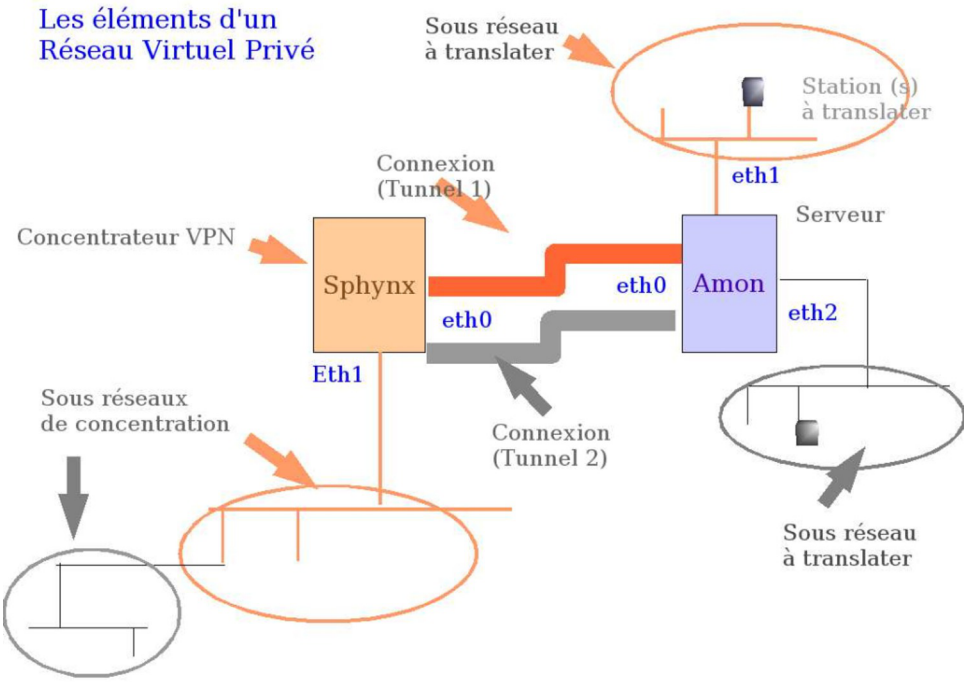
- le **réseau local** :

  situé derrière le pare-feu Amon (réseau établissement) ou derrière le concentrateur, il est composé de plusieurs sous-réseaux composés eux mêmes de stations.

La création de ce RVP permet donc de relier l'établissement à un ou plusieurs sous-réseaux des services académiques, mais également à plusieurs concentrateurs RVP et à plusieurs établissements.

Il est possible de choisir à l'intérieur de l'établissement la station, les stations du sous-réseau, le(s) sous-réseau(x) pouvant transiter au travers du tunnel ou des tunnels, et ainsi bénéficier des avantages du RVP (chiffrement des informations).

Le schéma ci-dessous récapitule de manière simple les différents composants d'un Réseau virtuel privé.



Les éléments d'un réseau virtuel privé

Serveurs impactés

Pour monter un tunnel vous devez intervenir sur les serveurs suivant : Sphynx, Amon, Zéphir (pour les utilisateurs du gestionnaire de parc). Vous devez également connaître les éléments des réseaux à relier.

C'est à dire :

- coté pare-feu Amon : la station, les sous-réseaux ou le réseau de l'établissement à translater dans le tunnel ;
- coté concentrateur : les sous-réseaux de concentration à atteindre.

Les tunnels

Le module Amon accepte de monter de 1 à n tunnels vers 1 ou n concentrateur RVP et vers 1 ou n Amon.

Avec ARV, il est possible de mélanger les modes.

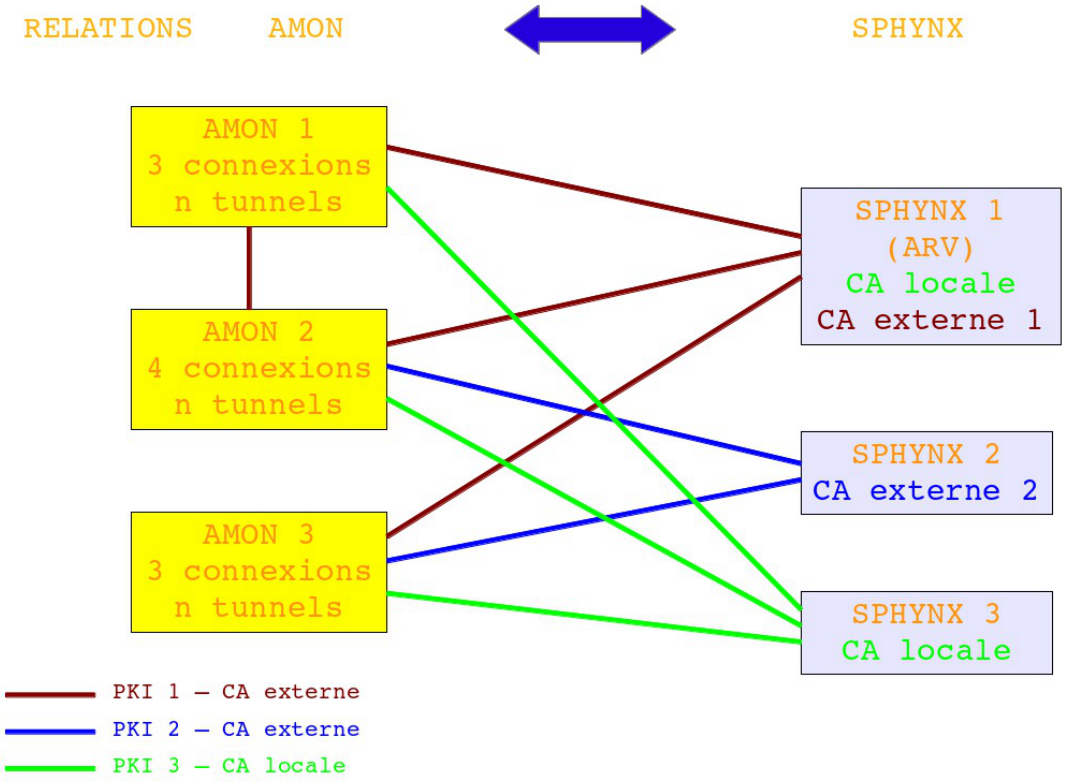
On peut donc envisager, par exemple, d'avoir dans un établissement :

- un tunnel vers un serveur Sphynx académique protégeant les flux administratifs ;

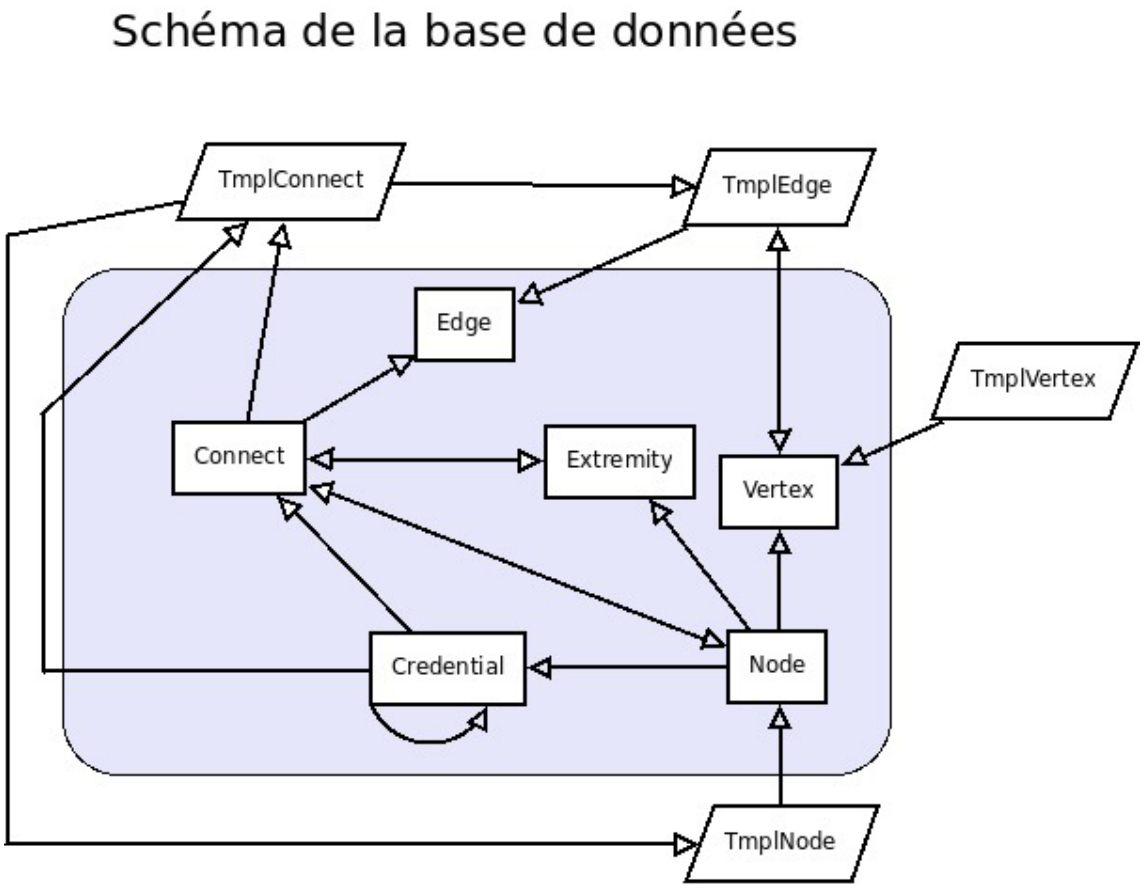
- un tunnel faisant transiter certains flux vers un autre serveur Sphynx utilisant une CA différente ;
- un tunnel vers un autre site de son établissement connecté sur internet par un Amon.

Ces trois tunnels passeront dans trois liens sécurisés différents.

Les tunnels sont montés de façon permanente, une vérification automatique depuis l'extrémité établissement est mise en place. Elle permet de remonter le tunnel en cas de problème.

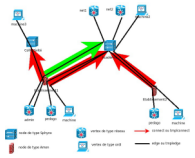


Les modèles

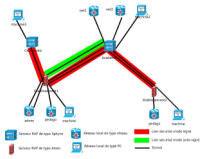


ARV est composé de deux vues :

- la vue abstraite, appelée modèle ;



- la vue concrète, avec les pare-feu Amon, les concentrateurs RVP, les liens sécurisés et les tunnels.



Un modèle est un squelette de réseau virtuel. Il permet de schématiser les relations entre les réseaux locaux de chaque serveur (Amon--concentrateur RVP et Amon--Amon). Chaque tunnel final sera basé sur ce modèle.

1.2. Présentation de l'interface

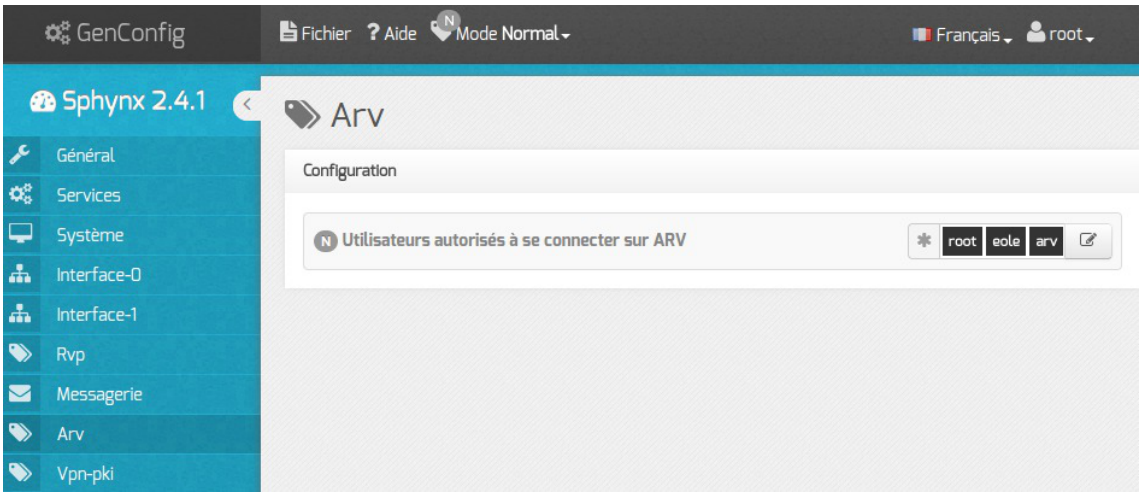
L'interface d'ARV est accessible via un navigateur web à l'adresse : `https://<IP Sphynx>:8088`

Elle nécessite une authentification.

Fenêtre d'authentification d'ARV

Les utilisateurs autorisés à se connecter sur ARV peuvent être des comptes systèmes locaux et des comptes Zéphir.

Pour qu'un compte puisse avoir accès à ARV, il faut impérativement les déclarer dans l'interface de configuration du module.



Gestion des utilisateurs autorisés à se connecter sur ARV

L'utilisation d'un compte Zéphir permet :

- de gérer les tunnels ;
- d'importer de Zéphir les serveurs de type Amon (Amon, AmonEcole, AmonHorus) et Sphynx enregistrés ;
- de générer les configurations RVP des tunnels modélisés sous forme d'archive ;
- d'envoyer sur le module Zéphir les archives RVP des serveurs ajoutés par importation.

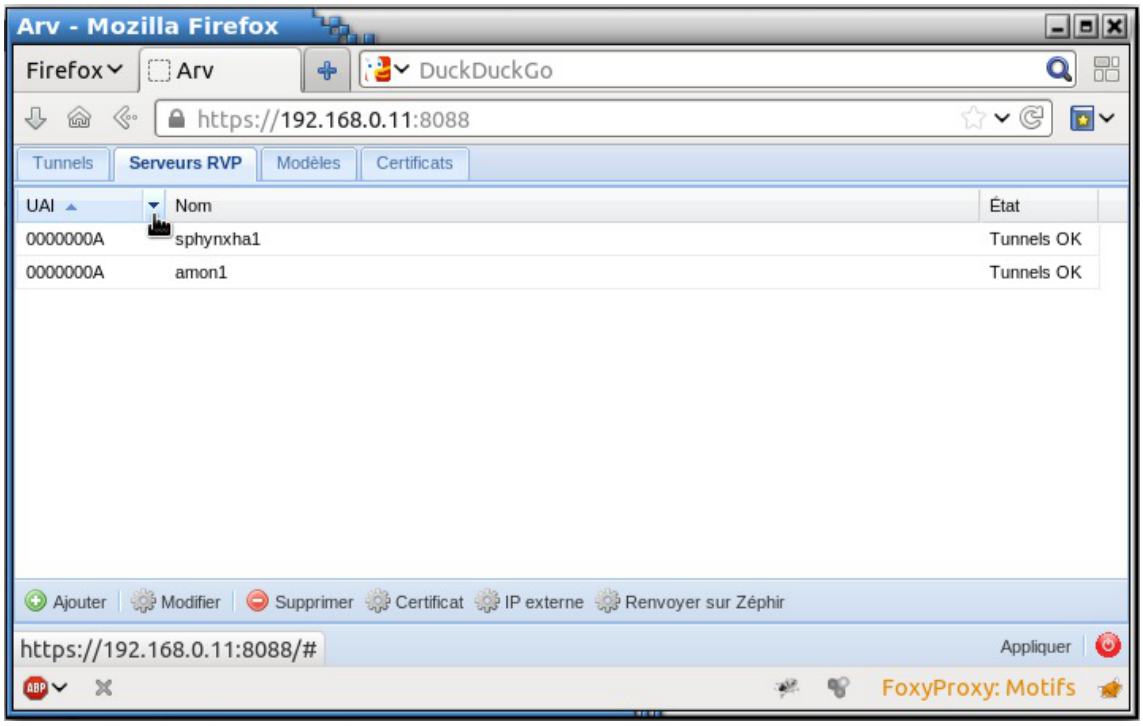
L'utilisation des comptes locaux (`root` et `eole` par défaut) permet :

- de gérer les tunnels ;
- de générer les configurations RVP des tunnels modélisés sous forme d'archive.

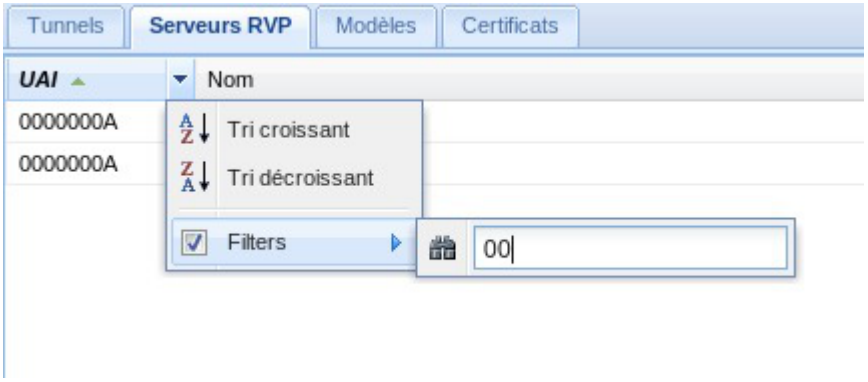
Les comptes Zéphir doivent avoir les droits en `Lecture` et `Configuration vpn`.

Sur certaines colonnes de l'application il est possible de trier ou de filtrer l'affichage.

Pour accéder à ces fonctionnalités il faut positionner le pointeur à la droite du titre de la colonne, une icône flèche en bas apparaît.



Un clique sur la flèche affiche les options de tri et éventuellement de filtrage.



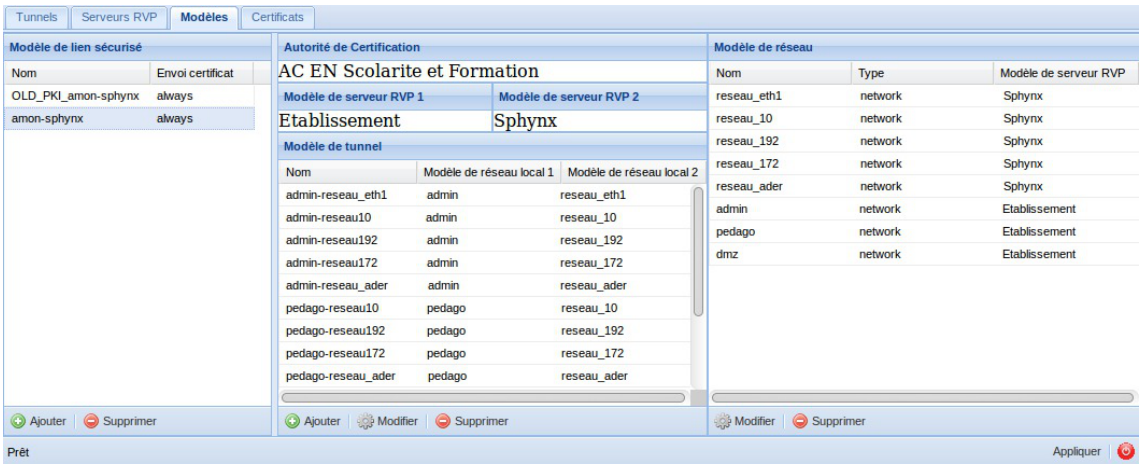
La déconnexion se fait en cliquant sur le bouton rouge en bas à droite dans l'application.

Bouton de déconnexion d'ARV

1.3. Modèles ARV

Ajout/Modification/Suppression d'un modèle de lien sécurisé

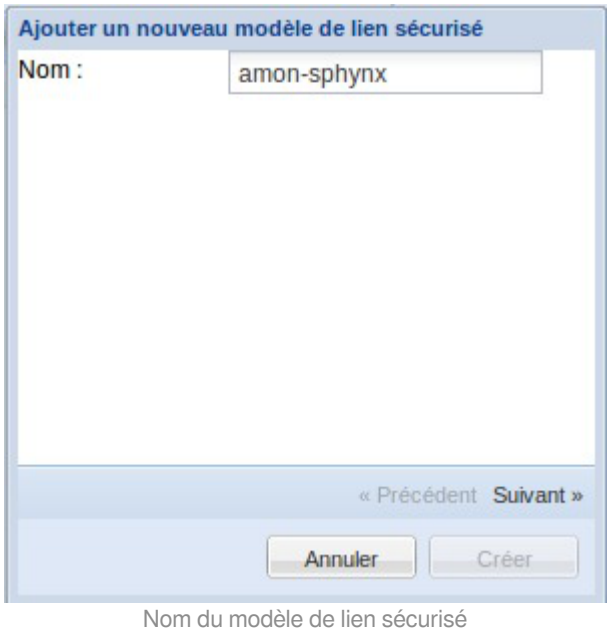
Pour ajouter, modifier ou supprimer un modèle de lien sécurisé, se rendre dans l'onglet `modèles` de la fenêtre principale de l'application web.



Fenêtre principale d'ARV avec l'onglet Modèles

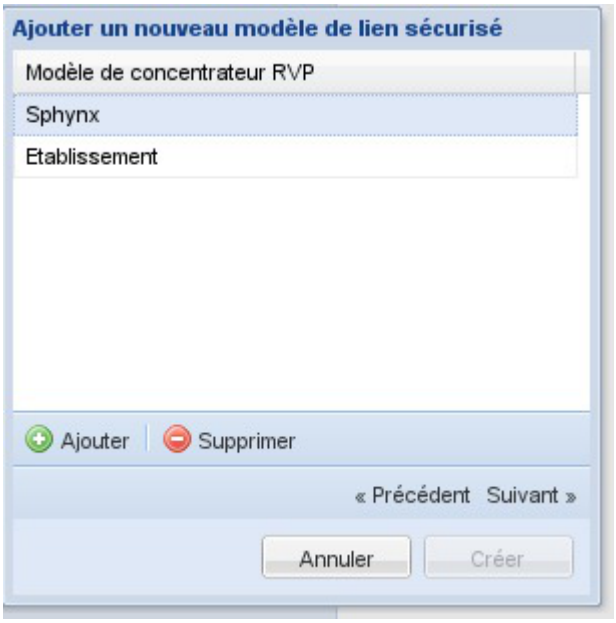
- Pour créer un nouveau modèle de lien sécurisé, cliquer sur le bouton `Ajouter` dans la colonne `modèle de lien sécurisé`.
- Pour modifier un modèle de lien sécurisé, il faut sélectionner le modèle voulu dans la colonne `modèle de lien sécurisé`. Vous pouvez ensuite `Ajouter` / `Modifier` / `Supprimer` des modèles de tunnel.
- Pour supprimer un modèle de lien, sélectionner le modèle voulu et cliquer sur le bouton `Supprimer` dans la colonne `modèle de lien sécurisé`. Ce modèle ne peut être supprimé que si il n'est plus utilisé.

Pour ajouter en modèle de lien sécurisé, commencer par lui donner un nom.



Nom du modèle de lien sécurisé

Choisir ensuite un modèle de serveur RVP source.



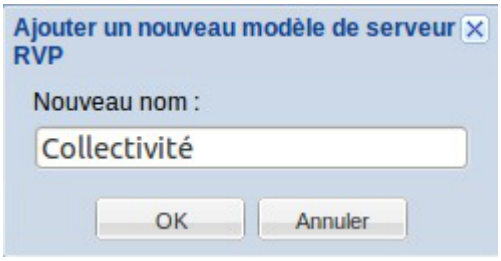
Modèle de concentrateur RVP source

Et le modèle de serveur RVP de destination.

Modèle de concentrateur RVP destination

Notez qu'il est possible de construire des modèles de lien sécurisé de tout type (Etablissement-Sphynx, Etablissement-Etablissement, Sphynx-Sphynx).

Si vous voulez ajouter un modèle de serveur RVP, par exemple une collectivité locale, cliquer sur le bouton Ajouter et spécifier un nom.



Ajout d'un nouveau modèle de concentrateur RVP

Enfin, choisir l'autorité de certification et choisir si le certificat est envoyé ou non via le protocole IPsec.

Sélection de l'autorité de certification pour le modèle de lien sécurisé

Et cliquer sur Créer pour ajouter le modèle.

Le protocole IKEv2 ne supporte la fragmentation des paquets réseaux, ne jamais envoyer le certificat via le protocole IPsec permet de réduire la taille des paquets.

Ajout/Modification/Suppression d'un modèle de tunnel

Pour ajouter, modifier ou supprimer un modèle de tunnel, se rendre dans l'onglet modèles de la fenêtre principale de l'application web,et choisir un modèle de lien sécurisé.

- Pour ajouter un modèle de tunnel, cliquer sur le bouton Ajouter de la colonne Modèle de tunnel.
- Pour modifier un modèle de tunnel, il faut sélectionner le modèle voulu dans la colonne Modèle de tunnel et cliquer sur Modifier dans cette même colonne.

C'est ici qu'il sera possible d'Ajouter/Modifier/Supprimer des modèles de réseaux locaux.

- Pour supprimer un modèle de tunnel, il faut sélectionner le modèle voulu dans la colonne Modèle de tunnel et cliquer sur Supprimer dans cette même colonne. Ce modèle ne peut être supprimé que si il n'est plus utilisé.

La suppression d'un modèle de tunnel entraîne également la suppression des modèles de réseaux locaux non utilisés.

Pour ajouter un modèle de tunnel, commencer par lui donner un nom. C'est ce nom qui apparaîtra comme `child` lié à une `connexion` à l'exécution de la commande `ipsec statusall`.

Création d'un modèle de tunnel

Choisir, les modèles de réseaux locaux correspondants à chaque extrémité du tunnel et cliquer sur Créer.

Ajout/Modification/Suppression d'un modèle de réseau local

Un réseau local correspond à un nom et un type.

Il existe trois types de réseaux locaux :

- `IP` : adresse IP d'une machine isolée ;
- `réseau` : adresse réseau et adresse masque du réseau ;
- `plage` : plage d'adresses IP correspondant à des adresses de machines.

Pour pouvoir ajouter, modifier ou supprimer un modèle de réseau local, il faut ajouter ou modifier un modèle de tunnel.

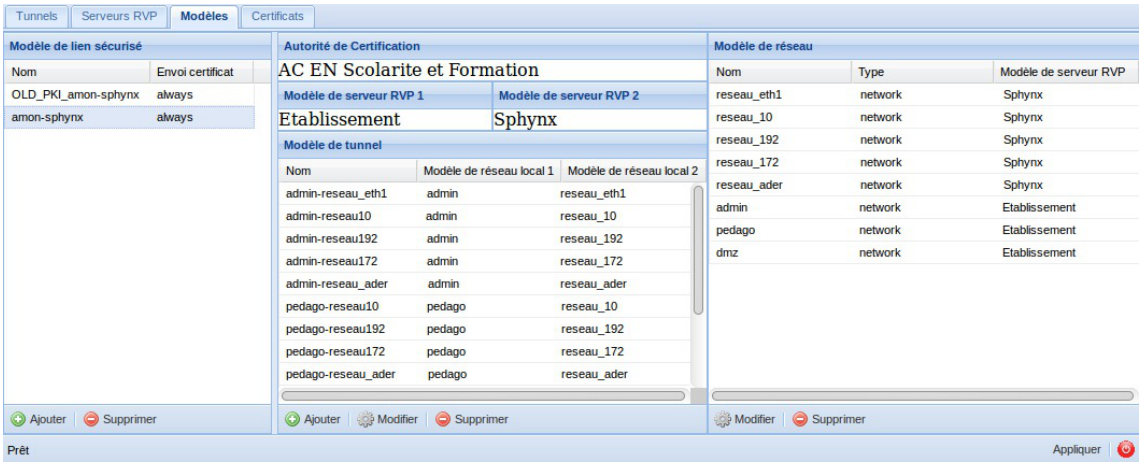
Création d'un modèle de tunnel

La modification d'un modèle de réseau local ne modifie pas les tunnels déjà créés.

- Pour ajouter un modèle de réseau local, cliquer sur le bouton Ajouter de la fenêtre d'ajout/modification de modèle de tunnel.
- Pour modifier un modèle de réseau local, il faut sélectionner le modèle voulu dans une des listes déroulantes et cliquer sur le bouton Modifier de la fenêtre d'ajout/modification de modèle de tunnel.
- Pour supprimer un modèle de réseau local, il faut sélectionner le modèle voulu dans une des listes déroulantes et cliquer sur le bouton Suppr. de la fenêtre d'ajout/modification de modèle de tunnel.Ce modèle ne peut être supprimé que si il n'est plus utilisé.

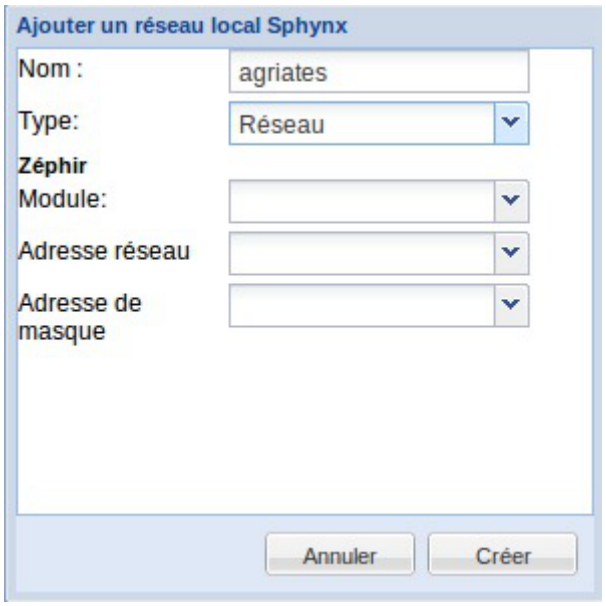
Il est également possible de modifier / supprimer les modèles de réseau dans la colonne de

droite de l'onglet Modèle.



Fenêtre principale d'ARV avec l'onglet Modèles

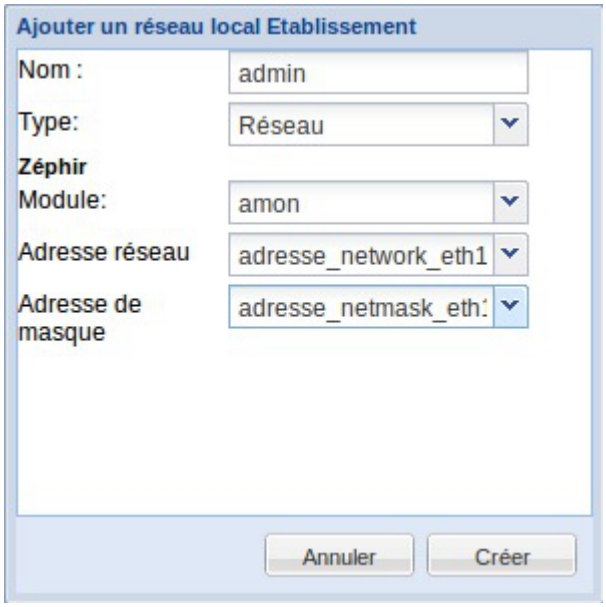
Pour ajouter un modèle de réseau local, commencer par lui donner un nom.



Création du modèle de réseau local net1

Pour faciliter la saisie des paramètres réseau, il est possible d'utiliser le serveur Zéphir.

Pour cela, indiquer le nom du module et les variables Creole correspondantes.



Création du modèle de réseau local Scribe

Il est possible d'utiliser des variables multivaluées qui peuvent être :

- sans index :
  - L'ensemble des valeurs de la variable multivaluée sera traité
  - Un tunnel sera créé pour chaque réseau de la liste

  Syntaxe : `adresse_network_vlan_eth1`
- avec index (`[n]`) :
  - Seule la valeur correspondant à l'index sera traitée
  - Un seul tunnel sera créé

  Syntaxe :

  `adresse_network_vlan_eth1[0]` et `adresse_netmask_vlan_eth1[0]` pour le premier vlan déclaré sur eth1 ;

  `adresse_network_vlan_eth1[1]` et `adresse_netmask_vlan_eth1[1]` pour le deuxième vlan déclaré sur eth1 ;

  [...]

  ou

  `alias_network_eth2[0]` et `alias_netmask_eth2[0]` pour le premier alias déclaré sur eth2 ;

  `alias_network_eth2[1]` et `alias_netmask_eth2[1]` pour le deuxième alias déclaré sur eth2 ;

  [...]

Si le modèle de réseau ne correspond pas à des variables Creole, il faut ne pas spécifier le nom du module et les adresses.

On peut toutefois spécifier des adresses IP si elles sont identiques sur tous les serveurs.

Puis cliquer sur `Créer`.

Si des modèles de sous réseau sont ajoutés, les valeurs correspondantes ne sont pas appliquées dans les serveurs RVP déjà existants dans la base ARV. Il faudra explicitement

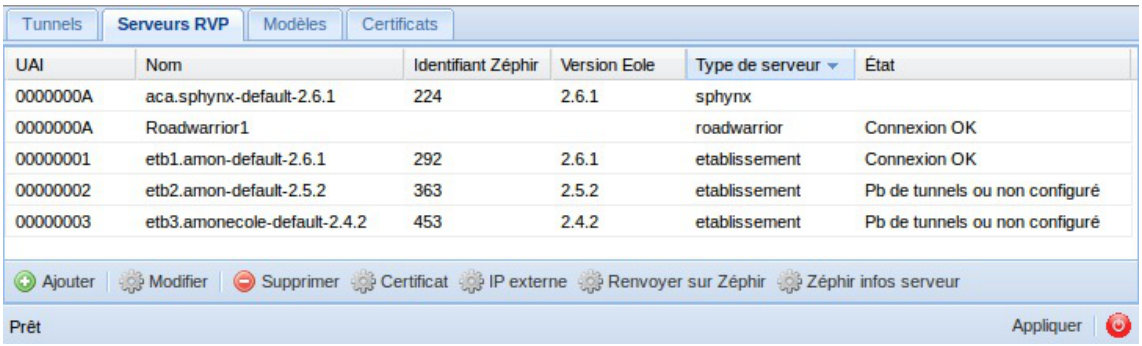
modifier chaque serveur dans l'onglet `Serveurs RVP` :

- sélectionner un serveur ;
- cliquer sur `Modifier` ;
- cliquer sur `Recharger les valeurs du modèle`.

Ce principe a été choisi pour pouvoir garder le contrôle des modifications.

1.4. Création d'un serveur RVP

La création d'un serveur est possible dans l'onglet Serveurs RVP.



Gestion des serveurs RVP

Selon le mode de connexion (compte Zéphir ou compte local) les informations présentes dans l'onglet varient. Avec le compte Zéphir l'identifiant Zéphir et la version d'EOLE apparaissent.

Pour créer un nouveau serveur RVP, il faut cliquer sur le bouton `Ajouter` dans l'onglet `Serveurs RVP`.

Il est possible de créer des serveurs RVP manuellement ou, si le serveur est enregistré sur le serveur Zéphir, de récupérer les informations depuis la base de données Zéphir.

Les renseignements d'un serveur RVP sont très importants et doivent être complétés en plusieurs étapes :

- Vérifier et renseigner les réseaux locaux utilisés, y compris sur Sphynx, ils ne sont pas tous renseignés automatiquement.
- Ajouter les certificats nécessaires à l'établissement des tunnels (auto-signés et signés par l'AC de Toulouse).
- Ajouter les adresses IP externes utilisées (y compris sur Sphynx).

La modification et la suppression d'un serveur RVP se fait en sélectionnant un serveur et en cliquant sur les boutons correspondants à l'action voulue.

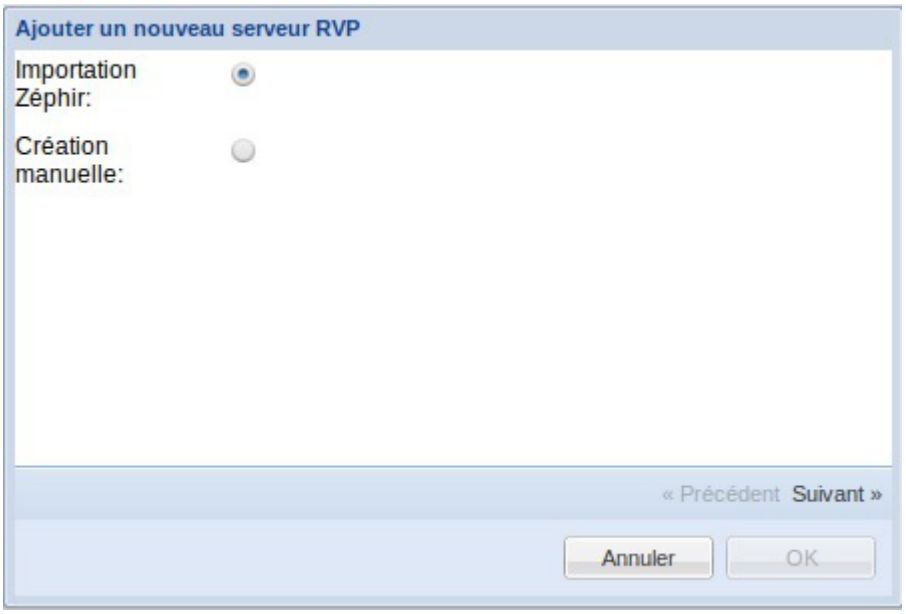
Toujours selon le mode de connexion (compte Zéphir ou compte local) les boutons `Renvoyer sur Zéphir` et `Zéphir infos serveur` sont disponibles ou grisés.

`Renvoyer sur Zéphir` permet de renvoyer une archive VPN déjà générée vers le serveur Zéphir.

`Zéphir infos serveur` permet de synchroniser l'identifiant Zéphir et la version d'EOLE d'un serveur créé manuellement. L'UAI et le nom dans ARV doivent correspondre à l'UAI et au libellé présent sur Zéphir.

1.4.1. Création manuelle d'un serveur RVP

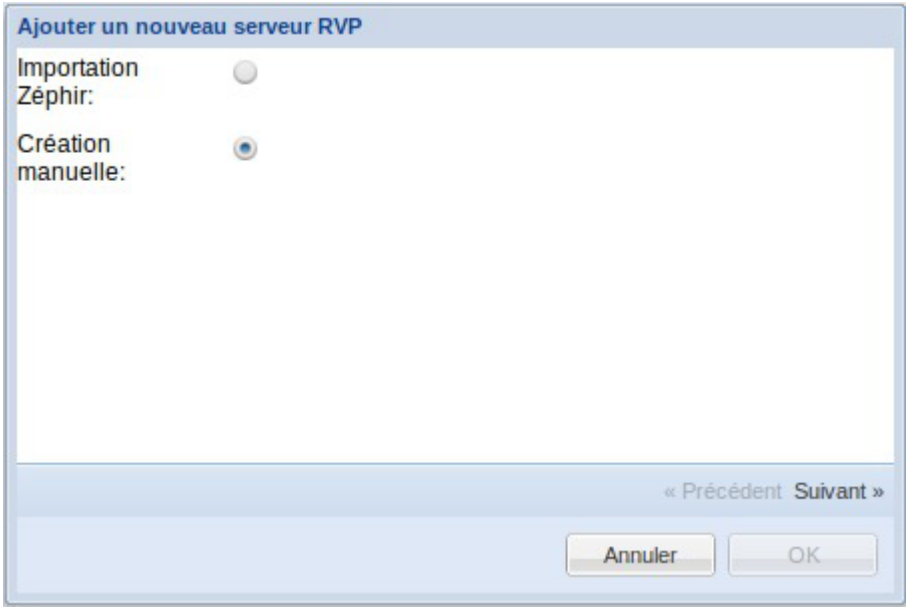
Dans le cas de la création manuelle du serveur RVP, il faut renseigner un nom, un identifiant (UAI, ex-RNE) et le type. Il existe deux types prédéfinis : Etablissement et Sphynx.



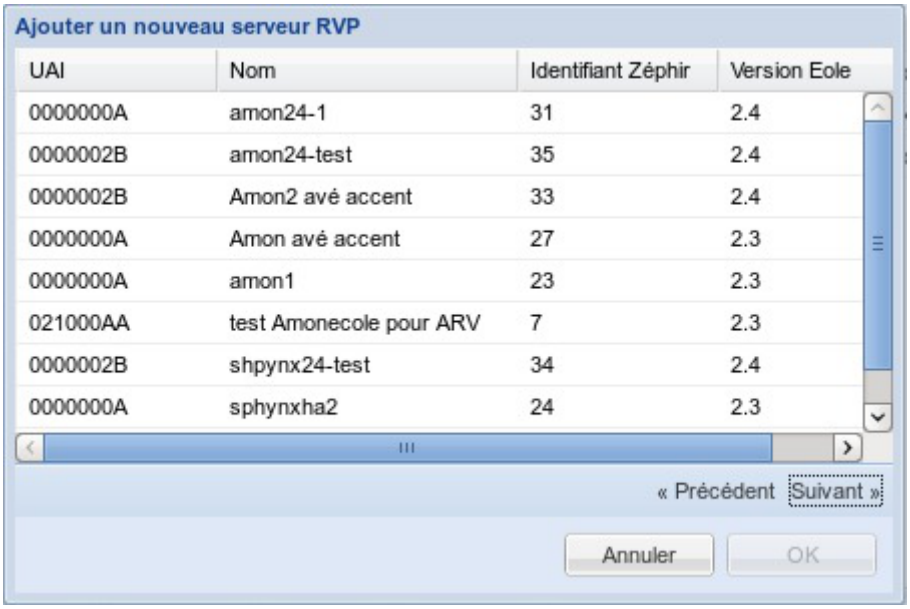
Configuration du concentrateur RVP manuelle

1.4.2. Création d'un serveur RVP par importation de Zéphir

Si ARV peut se connecter au serveur Zéphir, il est possible de rapatrier la liste des serveurs non présents dans ARV depuis la base de données Zéphir. Il suffit alors de sélectionner l'établissement à rapatrier.



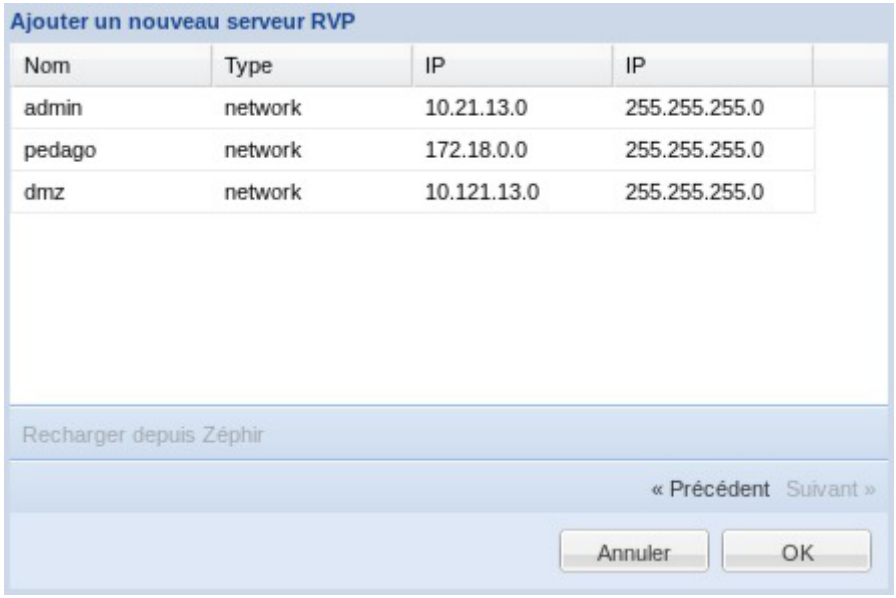
Ajouter un nouveau serveur RVP depuis Zéphir



Sélectionner un nouveau serveur RVP depuis Zéphir

Les valeurs correspondant aux variables indiquées dans le modèle de réseau local de l'établissement sont récupérées automatiquement sur Zéphir ainsi que l'identifiant Zéphir et la version d'EOLE.

Il sera possible de modifier un serveur RVP et de recharger les valeurs des variables depuis Zéphir.

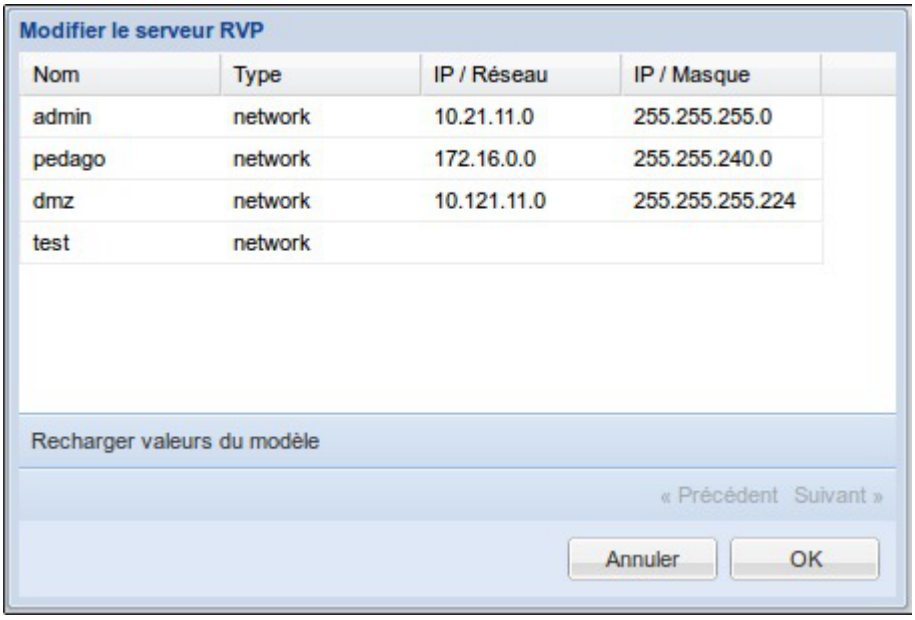


Les réseaux locaux sont automatiquement remplis en fonction du modèle défini

1.4.3. Création des réseaux locaux

Une fois le paramétrage du serveur RVP spécifié (par la méthode manuelle), il faut éventuellement renseigner les IP des réseaux locaux.

La liste des modèles de réseaux locaux est disponible dans la boite de dialogue suivante :



Spécification des IP des réseaux locaux du serveur RVP si le modèle de réseau local ne fait pas référence à des variables

Dans le cas où les réseaux locaux ne font pas référence à des variables Creole, il faut saisir les adresses IP manuellement.

Les adresses IP peuvent rester vides.

Un réseau non renseigné et non utilisé n'est pas bloquant.

Un réseau non renseigné utilisé dans un tunnel ne provoquera pas d'erreur dans ARV à la génération des bases ni de plantage de strongSwan. Le tunnel ne se montera pas et l'agent Zéphir du module Amon indiquera une erreur.

- Pour un modèle de type Réseau, la première colonne IP correspond à l'adresse réseau, la deuxième colonne correspond au masque de sous-réseau ;
- Pour un modèle de type Plage, la première colonne IP correspond à l'adresse du début de la plage, et la deuxième colonne correspond à l'adresse de fin de la plage ;
- Pour un modèle de type IP, la première colonne IP correspond à l'adresse de la machine, ne rien spécifier dans la deuxième colonne.

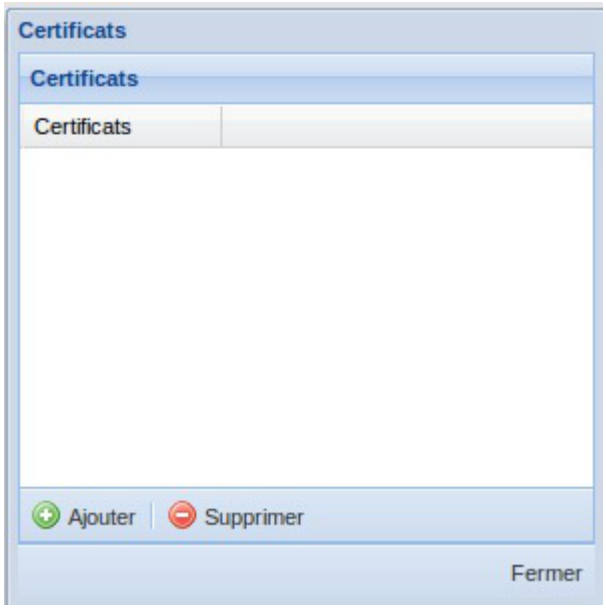
Dans le cas de la méthode Zéphir, les adresses IP correspondant au modèle trouvées dans la base de données sont affichées. Ces adresses IP peuvent être modifiées à la création du réseau local. Si l'adresse IP est mise à jour dans Zéphir, la modification ne sera pas synchronisée avec ARV. Il est possible de les resynchroniser en cliquant sur `Recharger valeurs du modèle`.

1.4.4. Ajout des certificats

Il est nécessaire d'ajouter des certificats au serveur RVP.

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur Certificat puis sur Ajouter



Ajouter des certificats

Trois possibilités :

- vous possédez déjà les fichiers **clé privée** et **certificat** pour le serveur RVP, il faut ◉ Importer un certificat ;
- vous possédez un fichier au format PKCS12[p.184] qui contient le certificat et la clé privée, il faut ◉ Importer un fichier PKCS12 ;
- vous ne possédez pas de certificat pour le serveur RVP, il faut ◉ Générer un nouveau certificat

Importer un certificat

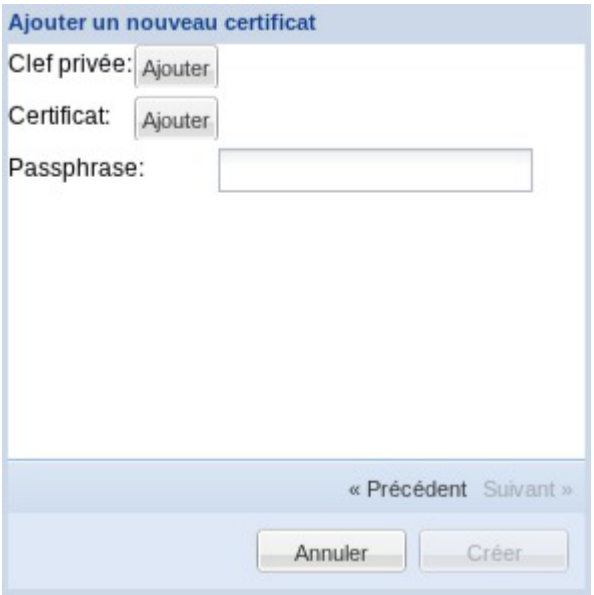
Importer un certificat

Pour importer un certificat, il faut ajouter la clé privée et le certificat du serveur signé par la CA (fichier avec l'extension `.pkcs7` ou `.p7`).

Le champ `Passphrase:` correspond au mot de passe qui protège la clé privée. Il n'est pas enregistré dans la base. Il permet d'extraire de la clé privée des informations nécessaires à la configuration.

Si il s'agit d'un certificat importé sur le serveur Sphynx-ARV, il servira à déchiffrer sa clé privée pour permettre l'activation du VPN.

Le mot de passe (phrase secrète) de la clé privée sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.



Importer une clé privée et un certificat un signé par la CA

Importer un fichier PKCS12

Cocher la case ◉ Importer un fichier PKCS12 pour insérer les fichiers certificat et clé privée dans la base ARV.

Importer un certificat PKCS12

Il reste à ajouter le fichier au format PKCS12 contenant le certificat ou toute la chaîne et la clé privée (fichier avec l'extension `.pkcs12` ou `.p12`).

Le mot de passe PKCS12 est celui qui a été utilisé pour générer le fichier PKCS12. Il permet d'extraire les certificats et la clé privée de ce fichier.des informations nécessaires à la configuration et de déchiffrer la clé privée du module Sphynx.

Le mot de passe permet de chiffrer la clé privée. Il sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.

Importer un certificat PKCS12 - Formulaire rempli

Générer un nouveau certificat

Cocher la case ◉ Générer un nouveau certificat pour utiliser des certificats autosignés ou créer un fichier de requête de certificat à fournir à une IGC.

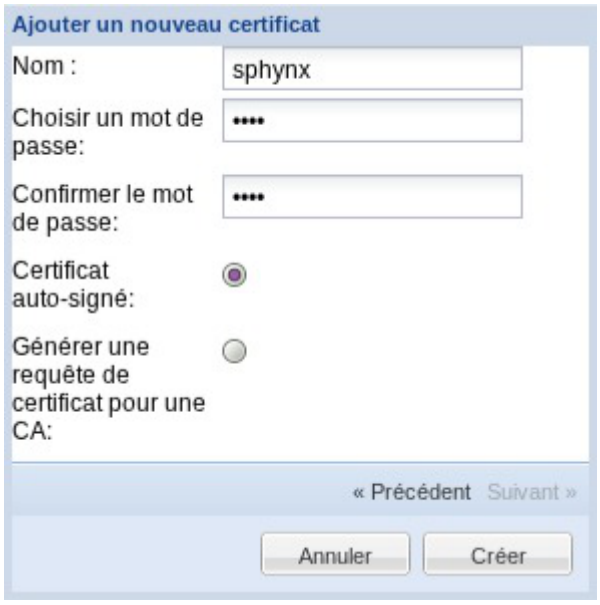
Générer un certificat autosigné ou importer les fichiers

Vous pouvez générer :

◉ Certificat auto-signé ;

◉ Générer une requête de certificat pour une CA externe.

Le fonctionnement en mode certificats auto-signés est un mode PKI mais avec une AC[p.180] (ou CA[p.180]) locale (sur Sphynx-ARV) qui signe le certificat généré.



Générer un certificat autosigné

Pour plus d'information sur l'option ◉ Générer une requête de certificat pour une CA externe il faut se référer à la partie de la documentation qui concerne la requête de certificat auprès de le l'IGC.

Voir aussi...

Requête de certificat auprès de l'IGC [p.132]

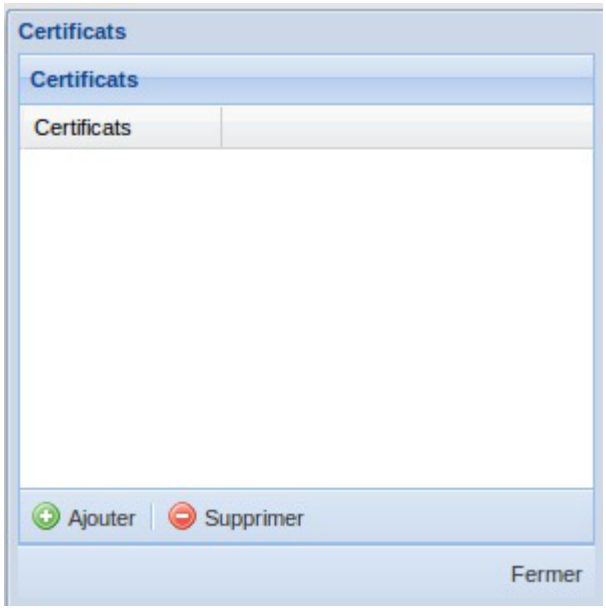
1.4.5. Requête de certificat auprès de l'IGC

Générer une requête de certificat pour une CA[p.180] génère une archive contenant la requête à envoyer à l'IGC[p.184].

Il faut se rendre dans l'onglet Serveurs RVP, sélectionner un serveur et enfin cliquer en bas sur le bouton Certificat.

Ce bouton permet d'ajouter des certificats au serveur RVP

Une fenêtre surgissante s'ouvre, cliquer alors sur le bouton Ajouter.



Ajouter des certificats

Choisir alors ◉ Générer un nouveau certificat et cliquer le bouton Suivant.

Générer un certificat autosigné ou importer les fichiers

Remplir les différents champs et sélectionner ◉ Générer une requête de certificat pour une CA .

La valeur du champ `Nom` est utilisée telle quelle dans le CN[p.180] du certificat.

Dans le cas où la PKI PNCN est utilisée, que la valeur du champ `Nom` soit saisie avec ou sans suffixe DNS, le CN sera forcé avec le suffixe saisi dans les paramètres de l'onglet `Général` de l'interface de configuration du module.

Exemples avec un suffixe ac-test.fr

Nom saisi	CN généré
certif	certif.ac-test.fr
certif.ac-test.fr	certif.ac-test.fr
certif.ac-test.fr.toto	certif.ac-test.fr.toto.ac-test.fr

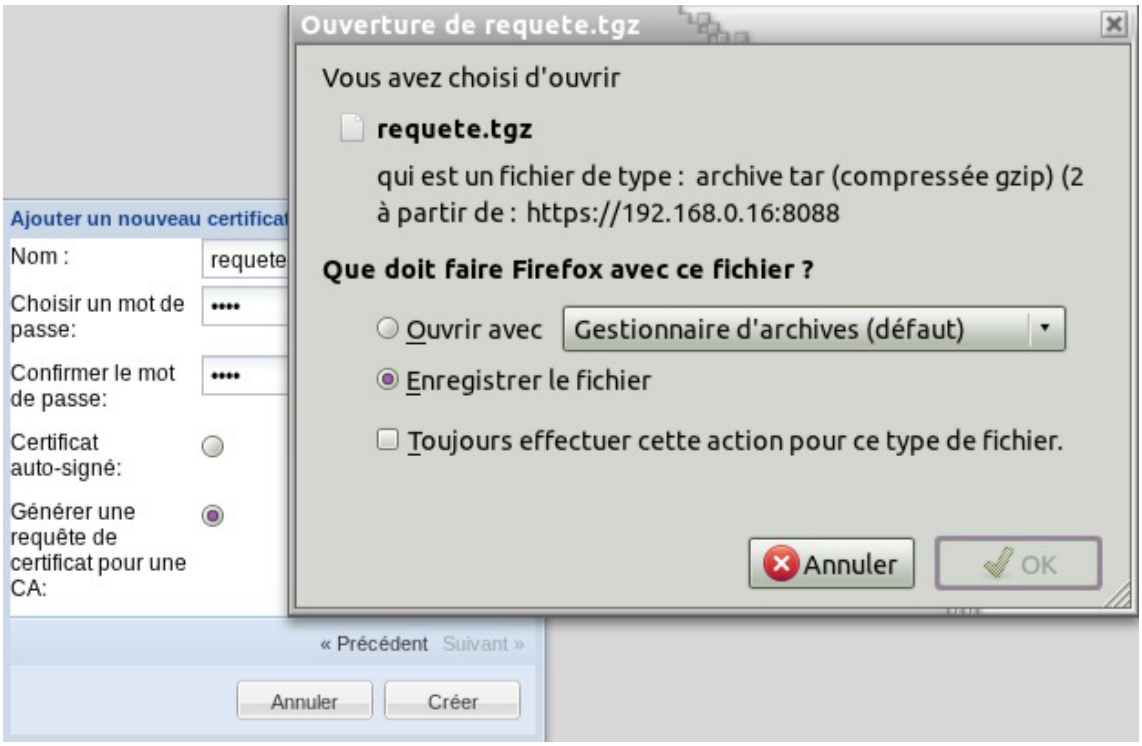
Valider en cliquant sur `Créer`.

Pensez à mémoriser le mot de passe (phrase secrète).

Le navigateur vous propose de télécharger une archive.

Elle contient la requête ainsi que la clé privée qui est associée au futur certificat signé par la CA.

Conserver précieusement cette archive, elle vous sera nécessaire pour un renouvellement de certificat.



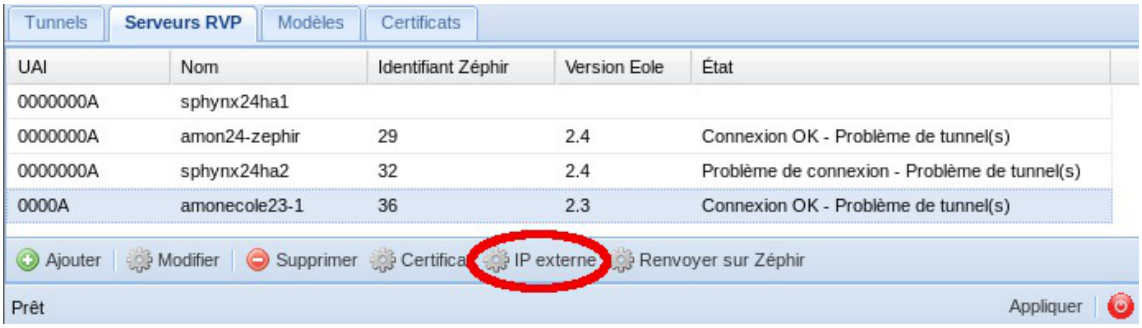
Requête de certificat à envoyer à l'IGC

Seul le fichier portant l'extension `.p10` est à envoyer à l'IGC après l'avoir extrait de l'archive.

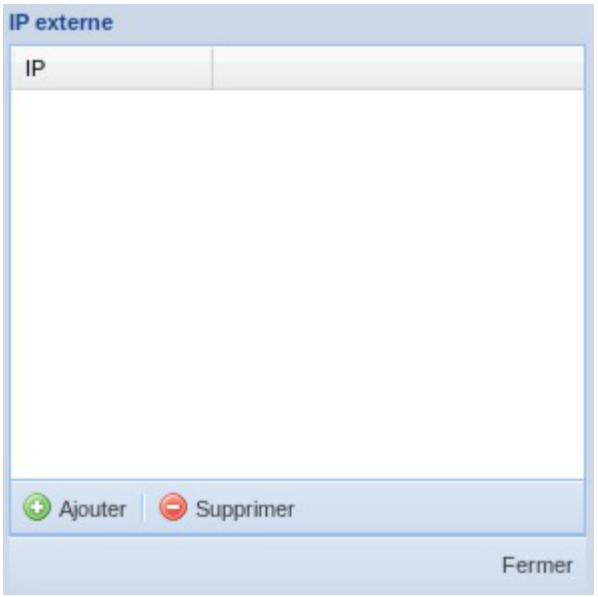
Il faudra par la suite importer la clé privée de cette archive ainsi que le certificat signé et renvoyé par l'IGC.

1.4.6. IP externes des serveurs RVP

Il est nécessaire de renseigner l'IP externe d'un serveur RVP.



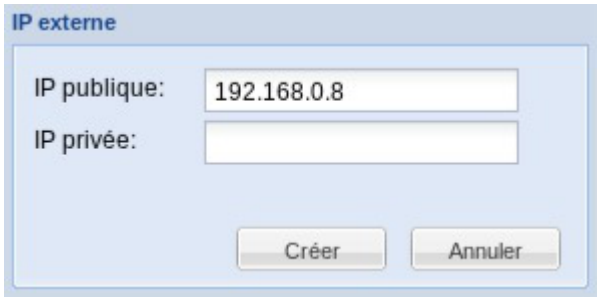
Il est possible de renseigner plusieurs IP externes (si IP aliasing).



L'IP publique est obligatoire. Elle concerne l'interface extérieure du module Amon.

Si le routeur est en bridge, il faut spécifier l'adresse IP attribuée à eth0 dans la zone `IP publique` et rien dans la zone `IP privée`.

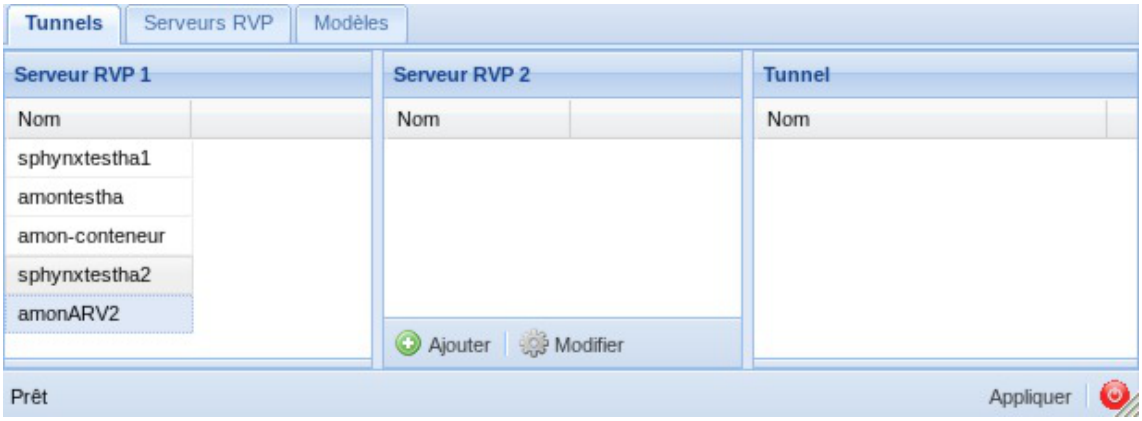
Si votre routeur est en NAT, dans la zone `IP publique`, il faut spécifier l'adresse IP extérieure du routeur et dans la zone `IP privée`, l'adresse IP eth0 d'Amon.



1.5. Création des tunnels

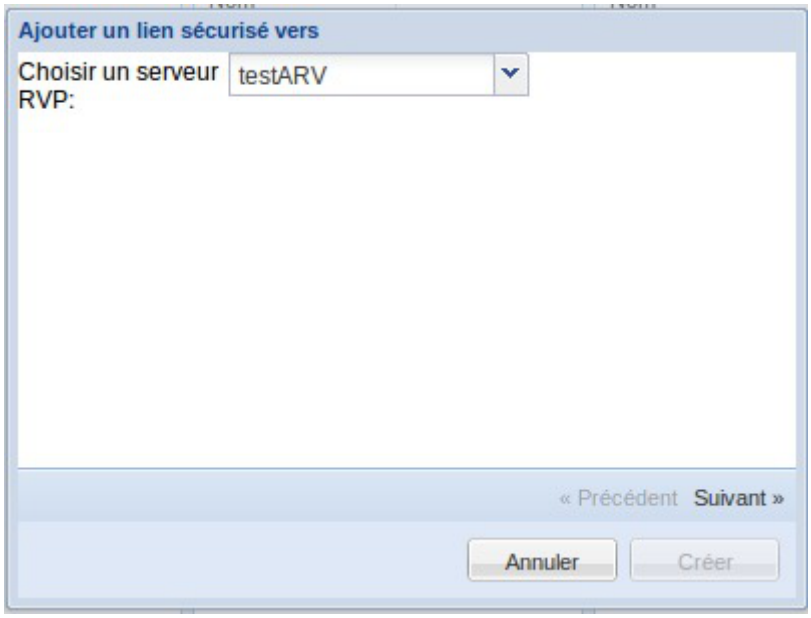
Création du lien sécurisé

La création de tunnels est possible entre deux serveurs RVP de même modèle (entre deux modules Amon ou deux modules Sphynx). La création des tunnels se fait dans l'onglet `Tunnels` de la fenêtre principale de l'application web.



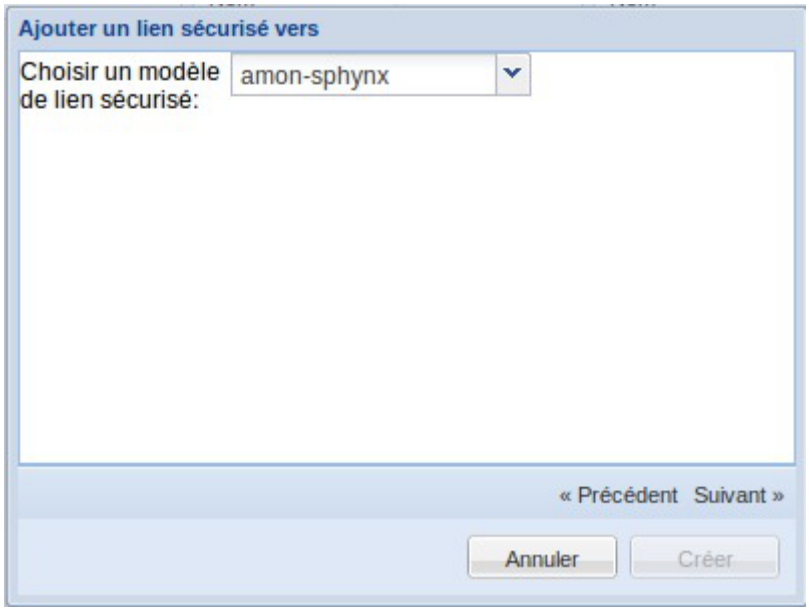
Fenêtre principale d'ARV avec l'onglet Tunnels

Pour pouvoir ajouter un tunnel entre deux réseaux locaux, il faut déjà créer un lien sécurisé entre deux serveurs RVP. Commencer par sélectionner le serveur RVP 1. Puis cliquer sur le bouton `Ajouter` de la colonne `Serveur RVP 2`. Choisir ensuite le serveur RVP 2 dans le menu déroulant suivant :



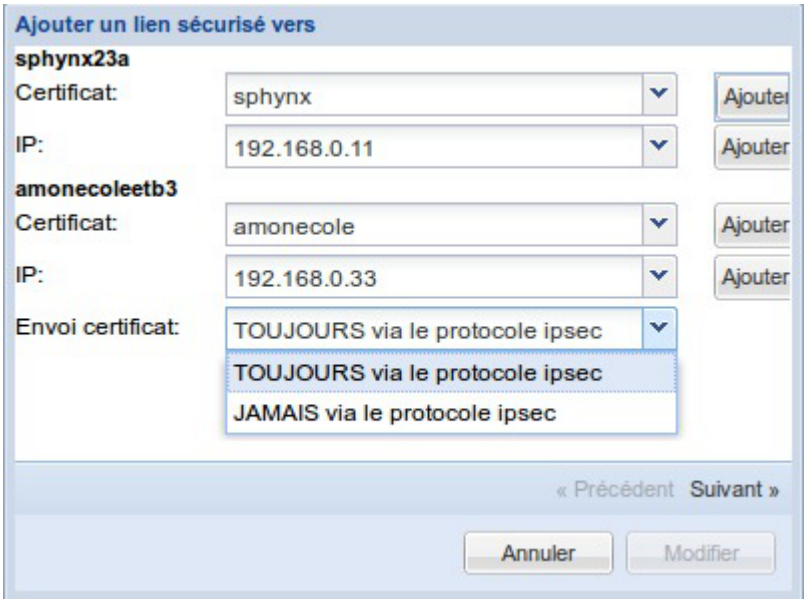
Choix du concentrateur RVP pour le lien sécurisé

Une fois les deux serveurs RVP sélectionnés, choisir le modèle de lien sécurisé voulu :



Choix du modèle de lien sécurisé

Puis choisir les IP et les certificats des deux serveurs RVP et la méthode d'envoi des certificats :



Choix des IP et certificats du lien sécurisé

Si besoin, ajouter l'IP et/ou un certificat d'un des deux serveurs RVP.

L'IP publique est obligatoire. Elle concerne à l'interface extérieure d'Amon (eth0).

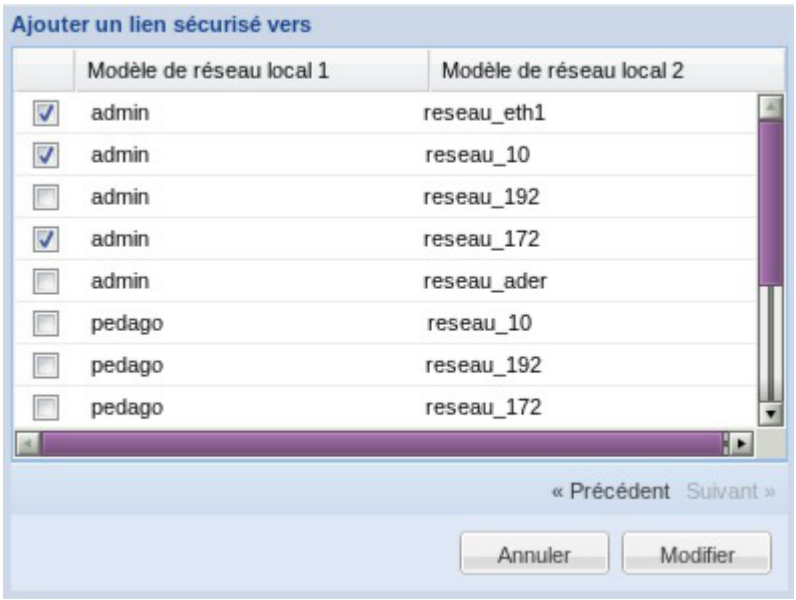
Si le routeur est en bridge, il faut spécifier l'adresse IP attribuée à eth0 dans la zone IP publique et rien dans la zone IP privée.

Si votre routeur est en NAT, dans la zone IP publique, il faut spécifier l'adresse IP extérieure du routeur et dans la zone IP privée, l'adresse IP eth0 d'Amon.

La méthode d'envoi du certificat pour la connexion choisi est celle du modèle utilisée. Il est possible de choisir une méthode différente pour chaque connexion.

Le protocole IKEv2 ne supporte la fragmentation des paquets réseaux, ne jamais envoyer le certificat via le protocole IPsec permet de réduire la taille des paquets.

Une fois le lien sécurisé paramétré, cocher les tunnels voulus (prédéfinis dans les modèles de liens et de tunnels).



Choix des tunnels

Gestion des translations

Si un réseau local possède le même adressage sur plusieurs Amon, il ne faut pas créer de tunnel mais utiliser un tunnel existant pour effectuer une translation. ARV n'implémente pas les translations dans un tunnel. Il faudra modifier le modèle ERA.

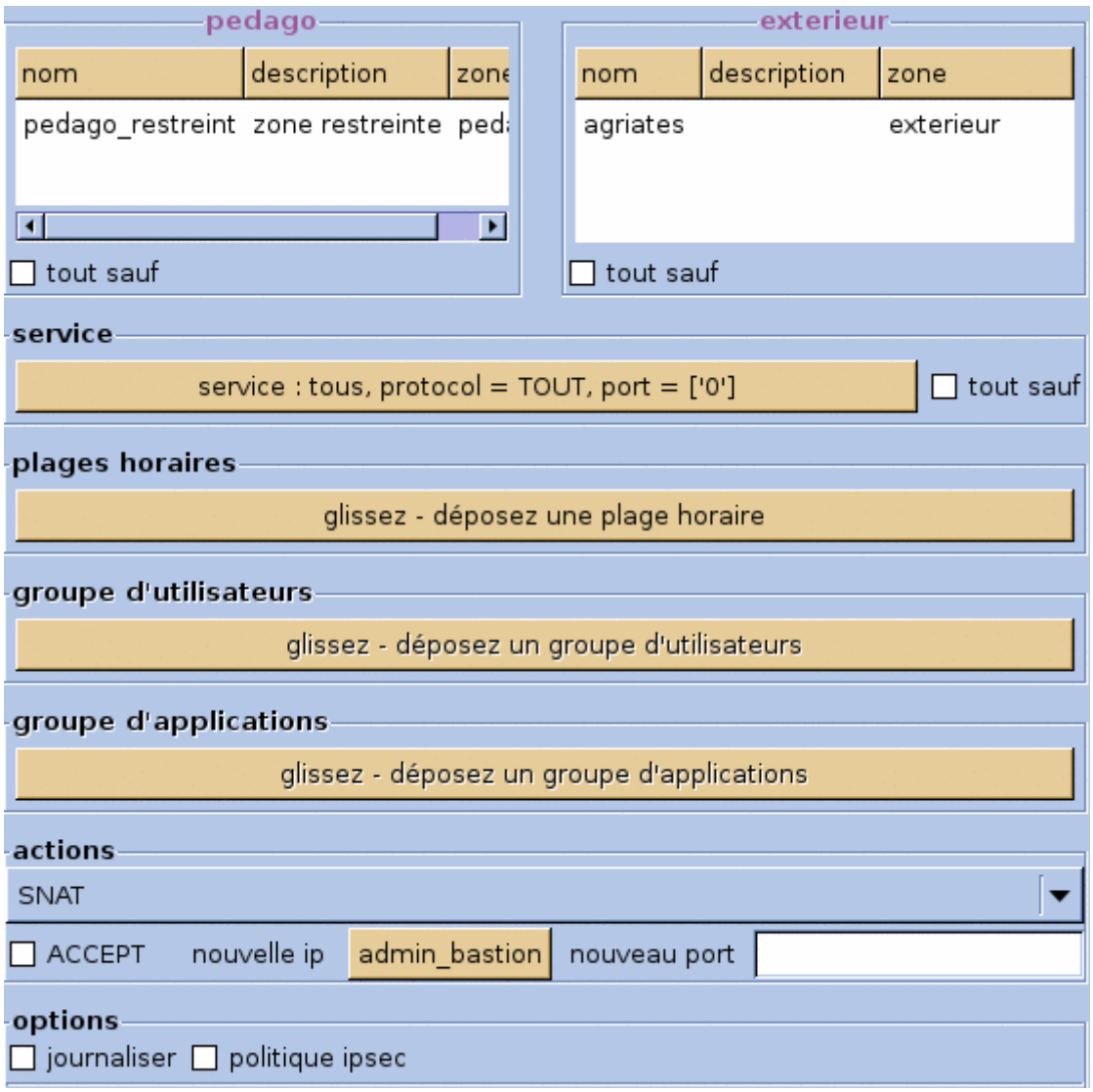
Par exemple :

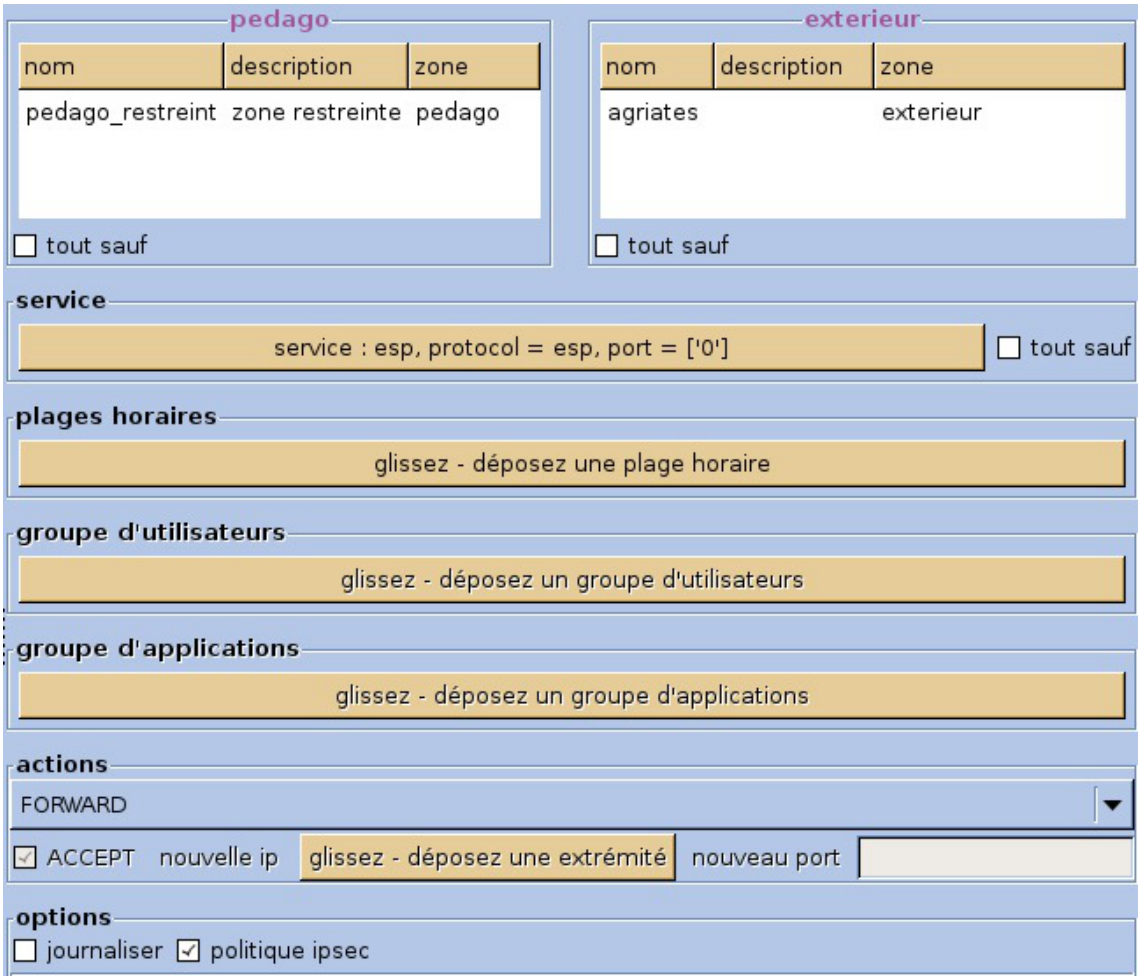
Si le réseau de l'interface eth2 est en 172.16.0.0/24 dans tous les établissements. Il sera impossible coté Sphynx d'établir des routes pour le même sous réseau vers plusieurs Amon. Il faudra donc translater ce réseau depuis l'Amon vers un tunnel existant.

On considère que le réseau eth1 (admin) est unique pour chaque Amon.

Il faut ensuite créer dans la zone `exterieur` les sous réseaux correspondant à l'intranet académique.

Les directives à ajouter dans ERA seront de ce type :





Il faudra ajouter autant de fois ces 2 directives que de réseaux de destination.

Ajout/Suppression d'un tunnel ou suppression de lien sécurisé

Pour supprimer ou modifier (ajout/suppression de tunnels) un lien sécurisé entre deux serveurs RVP, sélectionner le serveur RVP 1 et le serveur RVP 2 et cliquer sur `Modifier` dans la colonne `Serveur RVP 2` puis :

- Modification (ajout/suppression de tunnels) : Sélectionner le lien sécurisé à modifier et cliquer sur `Modifier`, cliquer sur `Suivant` et sélectionner ou désélectionner le/les tunnel(s).
- Suppression : Sélectionner le lien sécurisé à supprimer et cliquer sur `Supprimer`.

1.6. Génération des configurations IPsec

Opérations effectuées sur ARV

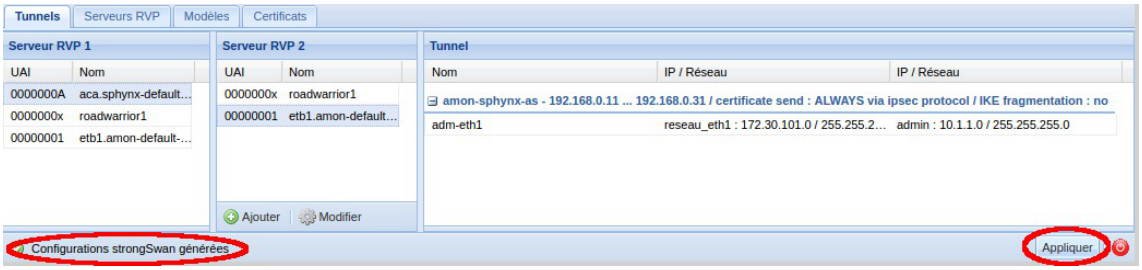
La génération des configurations IPsec pour strongSwan se fait en cliquant sur le bouton `Appliquer` en bas à droite de la fenêtre.

Quand les configurations strongSwan sont générées, la mention `Bases de données créées` ou `Configurations strongSwan générées` (selon le paramétrage du mode choisi dans l'onglet Rvp) s'affiche en bas à gauche de la fenêtre.

La configuration strongSwan du serveur Sphynx ARV est automatiquement mise à jour.

Les configurations strongSwan archivées des modules Amon et des modules Sphynx distants sont placées dans `/home/data/vpn/RNE/nom_serveur.tar.gz`.

Si on est connecté dans ARV avec un utilisateur Zéphir, les archives (Amon et Sphynx distants) sont également envoyées sur le module Zéphir.



Génération des configurations IPsec pour strongSwan

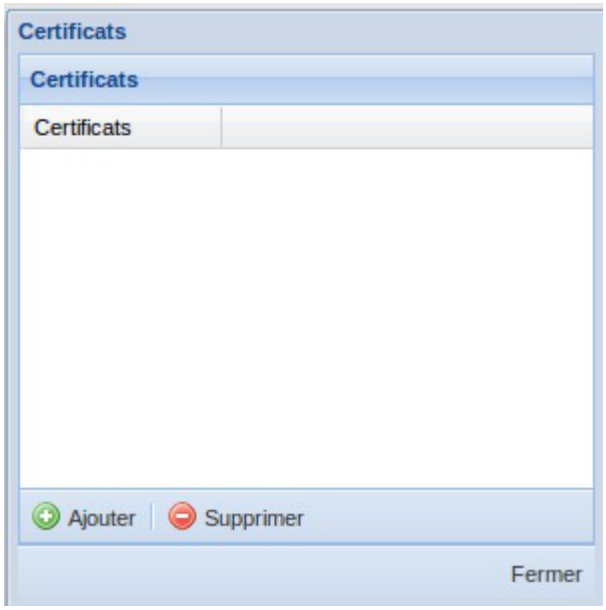
1.7. Gestion des certificats

1.7.1. Ajout des certificats

Il est nécessaire d'ajouter des certificats au serveur RVP.

Ce bouton permet d'ajouter des certificats au serveur RVP

Sélectionner le serveur RVP, cliquer sur `Certificat` puis sur `Ajouter`



Ajouter des certificats

Trois possibilités :

- vous possédez déjà les fichiers **clé privée** et **certificat** pour le serveur RVP, il faut ◉ Importer un certificat ;
- vous possédez un fichier au format PKCS12[p.184] qui contient le certificat et la clé privée, il faut ◉ Importer un fichier PKCS12 ;
- vous ne possédez pas de certificat pour le serveur RVP, il faut ◉ Générer un nouveau certificat

Importer un certificat

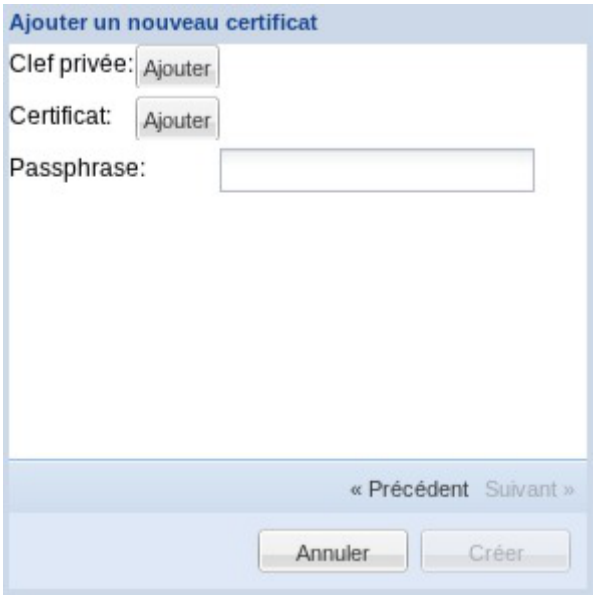
Importer un certificat

Pour importer un certificat, il faut ajouter la clé privée et le certificat du serveur signé par la CA (fichier avec l'extension .pkcs7 ou .p7).

Le champ Passphrase: correspond au mot de passe qui protège la clé privée. Il n'est pas enregistré dans la base. Il permet d'extraire de la clé privée des informations nécessaires à la configuration.

Si il s'agit d'un certificat importé sur le serveur Sphynx-ARV, il servira à déchiffrer sa clé privée pour permettre l'activation du VPN.

Le mot de passe (phrase secrète) de la clé privée sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.



Importer une clé privée et un certificat un signé par la CA

Importer un fichier PKCS12

Cocher la case ◉ Importer un fichier PKCS12 pour insérer les fichiers certificat et clé privée dans la base ARV.

Importer un certificat PKCS12

Il reste à ajouter le fichier au format PKCS12 contenant le certificat ou toute la chaîne et la clé privée (fichier avec l'extension `.pkcs12` ou `.p12`).

Le mot de passe PKCS12 est celui qui a été utilisé pour générer le fichier PKCS12. Il permet d'extraire les certificats et la clé privée de ce fichier.des informations nécessaires à la configuration et de déchiffrer la clé privée du module Sphynx.

Le mot de passe permet de chiffrer la clé privée. Il sera redemandé lors de l'activation du RVP sur un module Amon ou un module Sphynx distant pour son déchiffrement.

Importer un certificat PKCS12 - Formulaire rempli

Générer un nouveau certificat

Cocher la case ◉ Générer un nouveau certificat pour utiliser des certificats autosignés ou créer un fichier de requête de certificat à fournir à une IGC.

Générer un certificat autosigné ou importer les fichiers

Vous pouvez générer :

◉ Certificat auto-signé ;

◉ Générer une requête de certificat pour une CA externe.

Le fonctionnement en mode certificats auto-signés est un mode PKI mais avec une AC[p.180] (ou CA[p.180]) locale (sur Sphynx-ARV) qui signe le certificat généré.

Générer un certificat autosigné

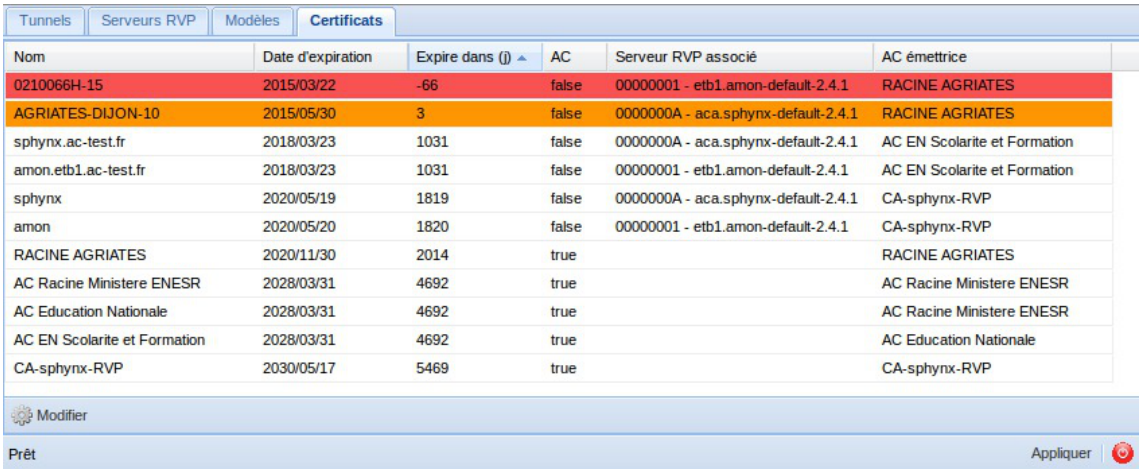
Pour plus d'information sur l'option ◉ Générer une requête de certificat pour une CA externe il faut se référer à la partie de la documentation qui concerne la requête de certificat auprès de le l'IGC.

Voir aussi...

> Requête de certificat auprès de l'IGC [p.132]

1.7.2. Durée de vie d'un certificat

Les certificats sont utilisés par les serveurs Sphynx et Amon. Ces certificats délivrés par l'AC (Autorité de Certification) ont une durée de vie fixée à 5 ans pour les certificats RACINE[p.185]-AGRIATES[p.178].



Lorsqu'un certificat arrive en fin de vie, il est dit expiré et apparaît en rouge dans l'onglet `Certificats`.

Dans les 45 jours précédents son arrivée à expiration, il apparaît en orange.

La colonne `Serveur RVP associé` permet de savoir si un certificat est bien associé à un serveur RVP. Si ce n'est pas le cas, il s'agit d'une anomalie et le certificat peut être supprimé.

> Les certificats de type CA (colonne CA à `true`) n'auront jamais de serveur RVP associé. Il ne doivent pas être supprimés.

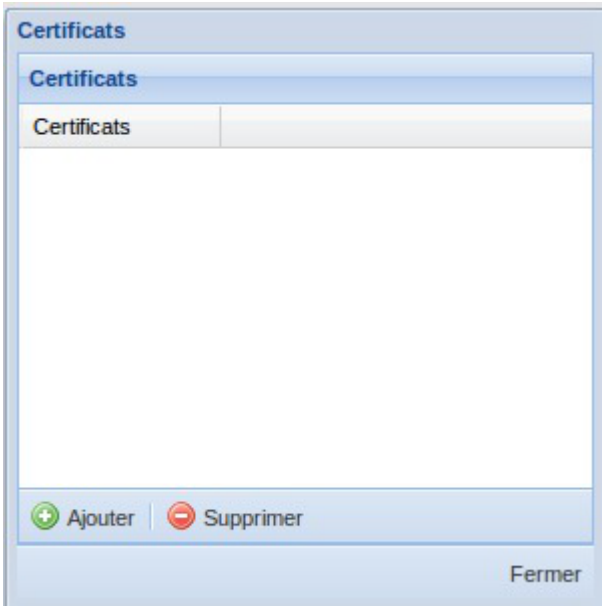
1.7.3. Requête de certificat auprès de l'IGC

Générer une requête de certificat pour une CA[p.180] génère une archive contenant la requête à envoyer à l'IGC[p.184].

Il faut se rendre dans l'onglet Serveurs RVP, sélectionner un serveur et enfin cliquer en bas sur le bouton Certificat.

Ce bouton permet d'ajouter des certificats au serveur RVP

Une fenêtre surgissante s'ouvre, cliquer alors sur le bouton Ajouter.



Ajouter des certificats

Choisir alors ◉ Générer un nouveau certificat et cliquer le bouton Suivant.

Générer un certificat autosigné ou importer les fichiers

Remplir les différents champs et sélectionner ◉ Générer une requête de certificat pour une CA .

La valeur du champ `Nom` est utilisée telle quelle dans le CN[p.180] du certificat.

Dans le cas où la PKI PNCN est utilisée, que la valeur du champ `Nom` soit saisie avec ou sans suffixe DNS, le CN sera forcé avec le suffixe saisi dans les paramètres de l'onglet `Général` de l'interface de configuration du module.

Exemples avec un suffixe ac-test.fr

Nom saisi	CN généré
certif	certif.ac-test.fr
certif.ac-test.fr	certif.ac-test.fr
certif.ac-test.fr.toto	certif.ac-test.fr.toto.ac-test.fr

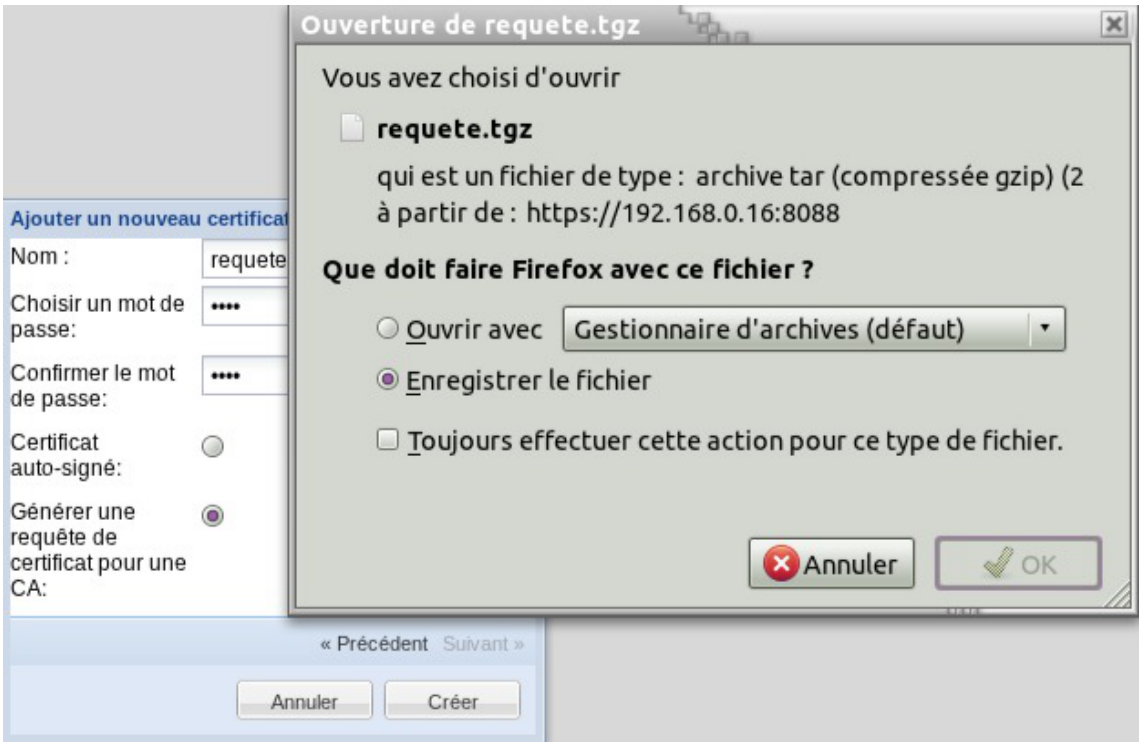
Valider en cliquant sur `Créer`.

Pensez à mémoriser le mot de passe (phrase secrète).

Le navigateur vous propose de télécharger une archive.

Elle contient la requête ainsi que la clé privée qui est associée au futur certificat signé par la CA.

Conserver précieusement cette archive, elle vous sera nécessaire pour un renouvellement de certificat.



Requête de certificat à envoyer à l'IGC

Seul le fichier portant l'extension `.p10` est à envoyer à l'IGC après l'avoir extrait de l'archive.

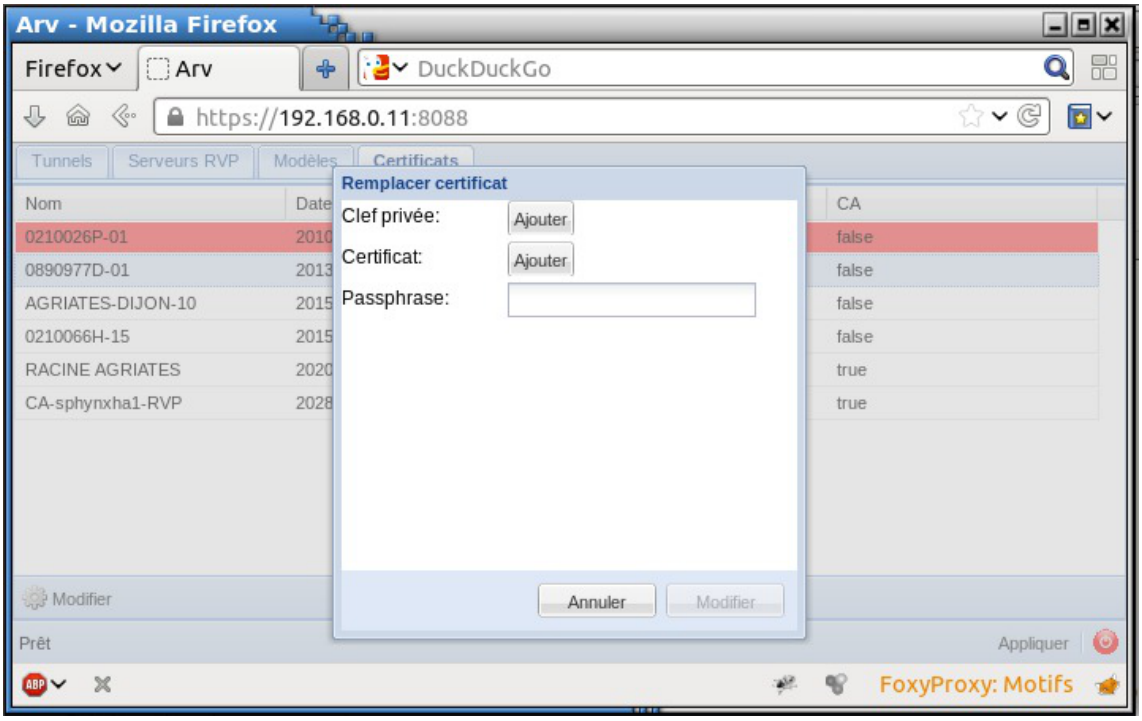
Il faudra par la suite importer la clé privée de cette archive ainsi que le certificat signé et renvoyé par l'IGC.

1.7.4. Prolongation d'un certificat existant

Pour prolonger la durée de vie du certificat il faut envoyer le fichier .p10 conservé dans l'archive de la requête précédente à l'IGC.

Une fois le certificat récupéré il faut le mettre à jour dans ARV.

Dans l'onglet `Certificats`, sélectionner le certificat concerné et cliquer sur le bouton `Modifier`



Dans la fenêtre surgissante :

- cliquer sur le bouton `Ajouter` de la ligne `Certificat` et choisir le nouveau fichier .pkcs7 renvoyé par l'IGC ;
- saisir le mot de passe dans le champs `Passphrase` ;
- cliquer sur `Modifier`.

La clé privé est conservée et le certificat est prolongé.

> N'oubliez pas de refaire les configurations strongSwan dans ARV en cliquant sur le bouton `Appliquer`.

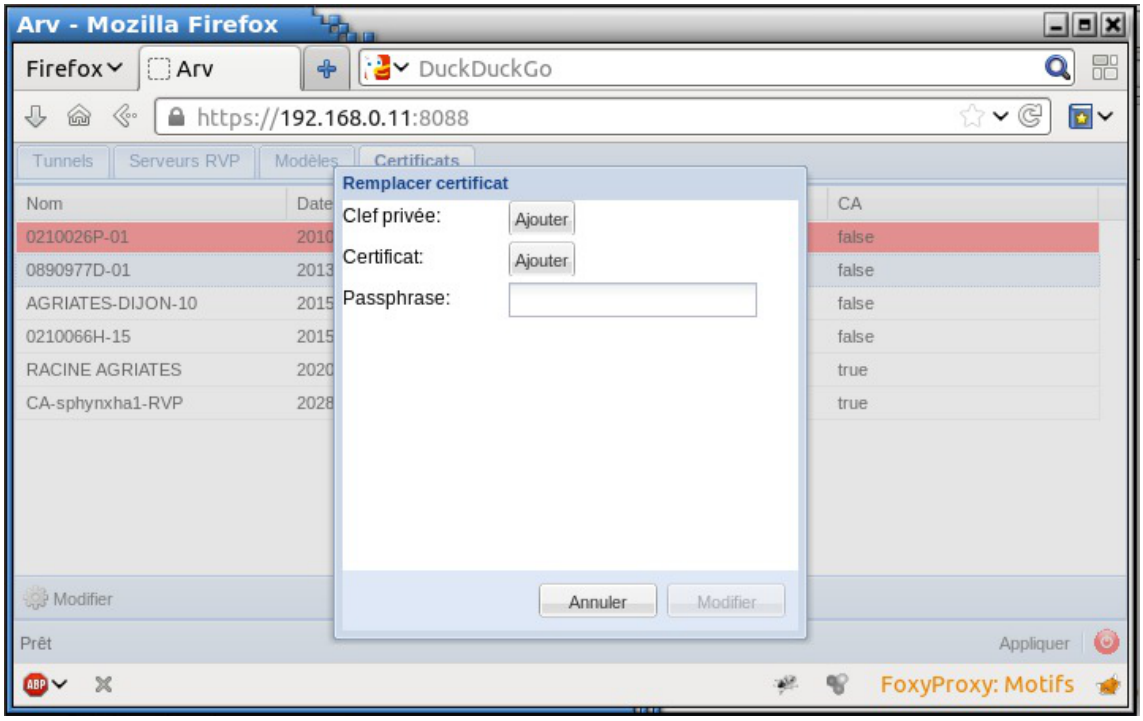
1.7.5. Remplacement d'un certificat existant

Pour remplacer un certificat il faut préalablement avoir fait une requête à l'IGC.

Dans l'archive issue de la requête à l'IGC se trouve la clé privée qu'il faut extraire.

Une fois le certificat récupéré auprès de l'IGC il faut mettre à jour dans ARV, le certificat et la clé privée.

Dans l'onglet `Certificats`, sélectionner le certificat concerné et cliquer sur le bouton `Modifier`.



Dans la fenêtre surgissante :

- cliquer sur le bouton `Ajouter` de la ligne Clef privée et choisir le fichier .pem extrait de l'archive ;
- cliquer sur le bouton `Ajouter` de la ligne `Certificat` et choisir le nouveau fichier .pkcs7 renvoyé par l'IGC ;
- saisir le mot de passe dans le champs `Passphrase` ;
- cliquer sur `Modifier`.

Le certificat et la clé privé sont remplacés.

N'oubliez pas de refaire les configurations strongSwan dans ARV en cliquant sur le bouton `Appliquer`.

2. Gestion des tunnels : RVP

Sphynx-ARV et Sphynx distant

Un module Sphynx peut être dédié ou non à la gestion des configurations RVP :

- un module Sphynx dédié à la gestion des configurations RVP avec ARV est appelé **Sphynx-ARV** ;
- un module Sphynx dont la configuration RVP est gérée par un autre module (Sphynx-ARV) est appelé **Sphynx distant**.

Sur un serveur **Sphynx distant** la mise en place du RVP se fera comme sur un serveur Amon.

Pré-requis

Le réseau virtuel privé (RVP)[p.185] est activé au moment de la configuration et de l'instanciation du

module.

Le mode de configuration de strongSwan (database ou fichier plat) doit être le même que sur le serveur ARV qui a généré la configuration IPsec.

ARV[p.179] permet de gérer les RVP de plusieurs serveurs Sphynx. Un serveur Sphynx autre que le serveur Sphynx-ARV sera appelé Sphynx distant. Sur un serveur de ce type, la mise en place du RVP se fera comme sur un serveur Amon.

Activation du RVP sur un module Sphynx distant

Pour activer un RVP sur un module Sphynx distant déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Au lancement de la commande `active_rvp init`, le choix `1.Manuel` ou `2.Zéphir` est proposé.

- Le choix 1 permet de prendre en compte la configuration RVP présente sur une clé USB.
- Le choix 2 active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un utilisateur et mot de passe Zéphir et l'identifiant Zéphir du serveur Sphynx.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine.

Les tunnels déjà mis en place sur un module Sphynx distant ne sont pas coupés lors de l'utilisation de la commande `active_rvp init`.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

3. Résoudre des dysfonctionnements liés au MTU

Le PMTUd (Path MTU[p.183] discovery), activé par défaut sur les modules EOLE, est une technique permettant de déterminer, dans un réseau informatique, la taille du MTU[p.183] sur le chemin entre deux hôtes IP, afin d'éviter la fragmentation des paquets.

Cette configuration peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP[p.182] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTUd est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Il est possible de forcer la valeur du MTU pour une interface donnée dans l'onglet `Réseau avancé` de l'interface de configuration du module en mode expert.

Les commandes `ping`, `ip route` et `tracepath` sont utilisées pour ajuster les valeurs.

Utilisation de la commande `ping`

La commande `ping` permet de réaliser des tests en forçant la taille des paquets :

- ping OK avec une taille forcée à la valeur 1400 :

```
root@amon:~#  ping -M do -s 1400 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1400(1428) bytes of data.
1408 bytes from platon.ac-dijon.fr (194.167.18.17): icmp_seq=1 ttl=62 time=1.38 ms

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.380/1.380/1.380/0.000 ms
```

- ping KO avec une taille forcée à la valeur 1500 :

```
root@amon:~#  ping -M do -s 1500 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1500(1528) bytes of data.
ping: local error: Message too long, mtu=1500

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Utilisation de la commande `ip route`

La commande `ip route get to` permet de visualiser les problèmes de MTU.

```
# ip route get to 172.X.Y.Z
172.X.Y.Z dev eth0 src 10.67.V.W
cache expires 508sec mtu 1400
```

La commande `ip route flush cache` permet quant à elle de vider le cache.

Utilisation de la commande `tracepath`

La commande `tracepath` permet d'identifier où se trouvent les limitations du MTU.

```
# tracepath 172.X.Y.Z
1?: [LOCALHOST] pmtu 1500
1?: [LOCALHOST] pmtu 1438
1: 192.168.A.B 1.353ms
1: 192.168.C.D 1.972ms
2: 192.168.E.F 2.014ms
3: 192.168.G.H 1.657ms
4: 192.168.I.J 3.026ms
5: 192.168.K.L 2.543ms pmtu 1400
5: 172.M.N.O 9.930ms
6: no reply
...
```

Voir aussi...

> Onglet Réseau avancé

4. Sauvegarde et restauration

La procédure de sauvegarde/restauration peut s'effectuer sur des modules de versions différentes.
Il est possible d'utiliser cette procédure pour migrer un serveur en changeant de machine physique.
L'archive créée par la sauvegarde comprend :

- la base ARV et la configuration IPsec ;
- tous les dictionnaires et patchs ;
- le fichier de configuration `config.eol`.

Sauvegarde

Des scripts de sauvegarde et restauration des données sont intégrés au serveur Sphynx. Pour démarrer une sauvegarde, il faut exécuter la commande `sauvegarde.sh` sur le serveur. Il n'y a rien de particulier à faire dans cette procédure. Le fichier de sauvegarde créé est `'date du jour'.tar.gz`.

Les sauvegardes générées sont stockées localement dans le répertoire `/var/lib/sphynx_backups/`. Il est donc recommandé de sauvegarder ce répertoire avec un système de sauvegarde externe.

Exemple de sauvegarde

```
root@sphynx:~# sauvegarde.sh
Sauvegarde en cours, patientez ...
- base ARV + Strongswan
- clés de connexion
- configuration eole
tar: Suppression de « / » au début des noms des membres
Compression de l'archive...
Archive créée : /var/lib/sphynx_backups/17-03-2015.tar.gz
root@sphynx:~#
```

Restauration

Si la restauration a lieu sur un nouveau serveur instancié ou non, il faut copier l'archive `tar.gz` souhaitée dans le répertoire `/var/lib/sphynx_backups/` (Le créer si nécessaire).

La restauration se fait via le script `restauration.sh`. Une liste des sauvegardes présentes est affichée.
Taper en toute lettre le nom de la sauvegarde à restaurer (date de création de la sauvegarde).

Vous aurez le choix de restaurer ou non la base ARV qui permet de générer les configurations IPsec.

Une sauvegarde restaurée sur un serveur de même version restaurera toute l'archive.

Une sauvegarde restaurée sur un serveur de version différente ne restaurera pas les patchs et dictionnaires.

Attention, toutes les données modifiées depuis la sauvegarde (modifications de la base ARV, configurations IPsec) seront perdues lors de la restauration.

Exemple de restauration

```
root@sphynx:~# restauration.sh
Utilitaire de restauration sphynx
!!Attention : toutes les modifications effectuées après la sauvegarde restaurée seront perdues!! liste des sauvegardes présentes :
17-03-2015
sauvegarde à restaurer (rien pour sortir): 17-03-2015
décompression en cours...
vérification des données...
Restaurer les bases ARV et la configuration Strongswan (o/n) ?
[non] : o
- bases ARV + Strongswan
Stopping strongSwan IPsec...
* Stopping Serveur ARV: arv
* waiting for process to die [OK]
- configuration eole
Reconfigurez le serveur après la fin de la restauration
Suppression du répertoire temporaire...
Système restauré
root@sphynx:~#
```

Suivant le cas de figure, serveur instancié ou non, exécuter la commande `instance` ou `reconfigure`.

Chapitre 7

Compléments techniques

Cette partie de la documentation regroupe différentes informations complémentaires : des schémas, des informations sur les services, les ports utilisés sur chacun des modules...

1. Les services utilisés sur le module Sphynx

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP Exim.

Logiciels et services

Le paquet `eole-exim` s'appuie principalement sur le service exim4.

http://www.exim.org/

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais utilisé sur tous les modules.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur le module AmonEcole et ses variantes, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.2. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.

La gestion des onduleurs fait l'objet d'une documentation dédiée : GestionDesOnduleurs.

Logiciels et services

Le paquet `eole-nut` s'appuie sur le service upsd.

http://www.networkupstools.org/

Historique

Ce paquet est pré-installé sur tous les modules depuis la version 2.3 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.3. eole-pacemaker

Le paquet `eole-pacemaker` permet la mise en place d'un service de haute disponibilité[p.182].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync[p.181].

Historique

A la base, le service de haute disponibilité était uniquement disponible sur le module Sphynx via le service Heartbeat. Celui-ci se fait maintenant via les logiciels Corosync[p.181] et Pacemaker. Le service a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service s'installe sur le serveur maître.

1.4. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN[p.185].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.186].

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés ainsi que sur le module Sphynx.

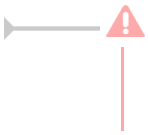
Conteneurs

Le service s'installe sur le serveur maître.

2. Ports utilisés sur le module Sphynx

Ce document donne la liste exhaustive des ports utilisés sur un module Sphynx.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.
Il est possible de lister les ports ouverts sur le serveur par la commande :
`netstat -ntulp`



En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 25/tcp : smtp (Exim4)
- 68/udp : dhclient
- 123/udp : ntpd
- 514/udp : rsyslogd (réception des journaux distants)
- 3493/tcp : nut (gestion des onduleurs)
- 4200/tcp : ead-web
- 4201/tcp : ead-server
- 4202/tcp : ead-server (transfert de fichiers)
- 5000/tcp : eoleflask/eolegenconfig (application admin)
- 7000/tcp : gen_config
- 8000/tcp : creoled
- 8090/tcp : z_stats (consultation des statistiques Zéphir locales), mise à jour automatique du client Zéphir
- 8443/tcp : EoleSSO
- 10514/tcp : rsyslogd (réception des journaux distants, protocole TCP)
- 12560/tcp : rsyslogd (réception des journaux distants, protocole RELP)

Ports spécifiques au module Sphynx

- 500/udp : charon (VPN)
- 4500/udp : charon (VPN)
- 8088/tcp : application web ARV
- Protocole `esp`

Services et numéro de ports

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

3. Commandes IPsec

Liste des principales commandes IPsec sur les modules Sphynx ou Amon :

- `ipsec statusall` renvoie la configuration d'IPsec[p.183] et l'état des connexions ;
- `ipsec status` renvoie uniquement l'état des connexions.

Monitorer l'utilisation des threads :

`worker threads: 2 of 32 idle, 5/1/2/22 working, job queue: 0/0/1/149, scheduled: 198`

Sur 32 threads disponibles,

- 2 sont en état idle ;
- 5 lancent des tâches CRITICAL priority ;
- 1 lance une tâche HIGH priority (process stroke par exemple) ;
- 2 lancent des tâches MEDIUM priority (messages IKE_SA_INIT ou CREATE_CHILD_SA) ;
- 22 lancent des tâches LOW priority .

`job queue` indique combien de tâches sont en file d'attente pour chaque priorité.

`Security Associations:`

`amon test ARV-Sphynx[3]: ESTABLISHED 18 minutes ago, 192.168.10.5[C=fr, O=gouv, OU=education, OU=ac-dijon, CN=AGRIATES-DIJON-10]...192.168.10.10[C=fr, O=gouv, OU=education, OU=ac-dijon, CN=0210066H-15]`

`amon test ARV-Sphynx[3]: IKE SPIs: b7db486b205cfb94_i 283a11782b375b7e_r*, public key reauthentication in 39 minutes`

`amon test ARV-Sphynx[3]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048`

`pedago-reseau172{27}: INSTALLED, TUNNEL, ESP SPIs: cbcb0242_i`

```
cd686778_o
 pedago-reseau172{27}:  AES_GCM_16_128,  0  bytes_i,  0  bytes_o,
rekeying_in_10_minutes
pedago-reseau172{27}: 172.16.0.0/12 === 172.16.0.0/24
 admin-reseau172{26}:  INSTALLED,  TUNNEL,  ESP  SPIs:  c058f927_i
c1f643f6_o
 admin-reseau172{26}:  AES_GCM_16_128,  0  bytes_i,  0  bytes_o,
rekeying_in_11_minutes
admin-reseau172{26}: 172.16.0.0/12 === 10.21.11.0/24
```

- `ipsec down "Security Association"` ou `"tunnel"` (les guillemets sont utiles si le nom contient des espaces)

  - `ipsec down "amon test ARV-Sphynx[3]"` arrête tous les tunnels liés à `amon test ARV-Sphynx[3]` et ferme la connexion `amon test ARV-Sphynx[3]` ;
  - `ipsec down pedago-reseau172{27}` arrête la 27ème instance du tunnel `pedago-reseau172`.

- `ipsec up "Security Association"` ou `"tunnel"` établit une connexion et tous les tunnels associés ou monte un seul tunnel

  - `ipsec up "amon test ARV-Sphynx"` établit la connexion `amon test ARV-Sphynx` et monte tous les tunnels associés ;
  - `ipsec up admin-reseau172` établit la connexion `amon test ARV-Sphynx` (car liée au tunnel) et monte le tunnel `admin-reseau172`.

4. Commandes de gestion du cluster

Voici quelques commandes Corosync.

Informations sur l'état du cluster

La commande `crm_mon` permet d'afficher l'état du cluster, l'option `-1 –one-shot` affiche l'état à un seul instant et quitte.Il est également possible d'utiliser la commande `crm status`. Cette commande peut aussi bien être utilisé dans l'interface de configuration du cluster.

Interface de configuration du cluster

Pour utiliser interface de configuration du cluster il suffit d'exécuter la commande crm :

```
# crm
crm(live)# exit
```

```
#
```

Exemple de l'utilisation de la commande status dans l'interface de configuration du cluster

```
# crm
crm(live)# status
============
Last updated: Thu Mar 26 11:49:12 2015
Last change: Thu Mar 26 11:47:22 2015 via crmd on sphynx
Stack: openais
Current DC: sphynx - partition WITHOUT quorum
Version: 1.1.6-9971ebba4494012a93c03b40a2c58ec0eb60f50c
1 Nodes configured, 2 expected votes
6 Resources configured.
============
Online: [ sphynx ]
Resource Group: VIPCluster
VIP_externe (ocf::heartbeat:IPaddr2): Started sphynx
VIP_interne (ocf::heartbeat:IPaddr2): Started sphynx
VIP_src_addr (ocf::heartbeat:IPsrcaddr): Started sphynx
ipsec_rsc (lsb:ipsecSphynx): Started sphynx
arv_rsc (lsb:arv): Started sphynx
Clone Set: gw_pingd_clone [gw_pingd]
Started: [ sphynx ]
crm(live)# exit
bye
#
```

La commande `help` liste les commandes disponibles et `exit` permet de quitter l'interface.

Action sur les postes et les ressources

Mettre un nœud en maintenance

```
# crm node standby <nom de l'hôte>
```

Les ressources de ce nœud seront migrées automatiquement sur l'autre nœud du cluster.

Sortir un nœud du mode maintenance

```
# crm node online <nom de l'hôte>
```

Reset de l'état d'un nœud du cluster

Cela peut régler le fait que des ressources ne reviennent pas sur un nœud ou que les nœuds ne se voient plus dans le cluster.

```
# crm node clearstate <nom de l'hôte>
```

Migrer une ressource vers un autre poste

`# crm resource migrate <nom ressource> <nom du poste allant accueillir la ressource>`

Annuler la migration de la ressource

```
# crm resource unmigrate <nom ressource>
```

Mettre à zéro les compteurs d'échec pour un hôte et une ressource donnés

```
# crm resource failcount <nom de la ressource> delete <nom de l'hôte>
```

Mettre à zéro l'état d'une ressource

```
# crm resource cleanup <nom de la ressource>
```

http://clusterlabs.org/wiki/Debian_Lenny_HowTo
http://doc.ubuntu-fr.org/pacemaker

5. Compléments techniques ARV

Répertoires utilisés par ARV

Le répertoire `/var/lib/arv/` contient un certain nombre d'éléments liés à ARV :

- `/var/lib/arv/CA/` contient la PKI[p.184] utilisée pour les certificats auto-signés du VPN ;
- `/var/lib/arv/db/` contient le fichier `sphynxdb.sqlite` qui est la base de données d'ARV (configuration VPN des serveurs EOLE).

Le répertoire `/var/lib/arv/nodeconf/` sert uniquement à préparer la génération des archives VPN.

Débogage du service ARV

Il est possible de passer ARV en mode debug en passant le paramètre `log level` à la valeur `debug` au lieu de `critical` dans le fichier `/etc/arv/arv.conf`.
Il faut ensuite redémarrer le service `arv`.

Les informations du service sont journalisées dans le fichier `/var/log/arv/error.log`.

Chapitre 8

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.

1. Questions fréquentes communes aux modules

Accéder aux partitions du module depuis un Live Linux

Lorsqu'on a recours à un live CD ou USB, il n'est pas possible d'accéder directement aux partitions.

```
# mkdir /media/partition
# mount /dev/sda2 /media/partition
mount: type inconnu de système de fichiers 'LVM2_member'
```

Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
# vgscan
Reading all physical volumes. This may take a while...
Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
# vgchange -a y eolebase-vg
4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
# ll /dev/mapper/
total 0
drwxr-xr-x  2 root root     160 févr.  8 11:53 ./
```

```
drwxr-xr-x 19 root root    4460 févr.  8 11:53 ../
crw-------  1 root root 10, 236 févr.  8 11:53 control
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-home ->
../dm-4
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-root ->
../dm-0
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-swap_1 ->
../dm-1
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-var -> ../dm-3
```

ou

```
# lvdisplay
  --- Logical volume ---
  LV Path                /dev/eolebase-vg/swap_1
  LV Name                swap_1
  VG Name                eolebase-vg
  LV UUID                OO47WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
  LV Write Access        read/write
  LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
  LV Status              available
  # open                 2
  LV Size                1,09 GiB
  Current LE             280
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:1
[...]
```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

Ajouter de l'espace disque à un volume LVM

Sur le nouveau périphérique physique, créer une partition de type Linux LVM (8E), avec `cfdisk` par exemple.

La nouvelle partition s'appelle par exemple `/dev/sdb1` et peut être ajoutée au volume, par exemple pour agrandir `/var`.

Après avoir créé la nouvelle partition `/dev/sdb1` il peut être nécessaire de redémarrer le serveur pour la faire prendre en compte par le système.

Démonter la partition

Pour démonter la partition

```
# umount /var
```

Créer un volume physique

Créer un volume physique avec la nouvelle partition :

```
# pvcreate /dev/sdb1
```

Quel est le groupe de volumes

Rechercher dans quel groupe de volumes (VG Name) se trouve le volume logique `/var` :

```
root@scribe:/dev/mapper# lvdisplay /dev/scribe-vg/var
  --- Logical volume ---
  LV Path                /dev/scribe-vg/var
  LV Name                var
  VG Name                scribe-vg
  LV UUID                N4dHMU-htpz-AhEI-x5Ld-EvpM-ZFJX-M3LbHD
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-01-16 19:17:09 +0100
  LV Status              available
  # open                 1
  LV Size                8,35 GiB
  Current LE             2138
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:3

root@scribe:/dev/mapper#
```

Ajouter ce volume physique au groupe de volumes contenant le volume logique `/var`, ici `scribe-vg` :

```
# vgextend scribe-vg /dev/sdb1
```

Agrandir le volume logique

Agrandir le volume logique correspondant à `/var` avec le nouvel espace libre :

```
# lvextend -l +100%FREE /dev/scribe-vg/var
# e2fsck -f /dev/scribe-vg/var
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM

Sur un serveur où une partition est saturée.

```
root@scribe:~# df -h
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
udev                          1,5G       0  1,5G   0% /dev
tmpfs                         301M     52M  250M  18% /run
/dev/mapper/scribe--vg-root   9,1G    2,6G  6,0G  30% /
tmpfs                         1,5G     28K  1,5G   1% /dev/shm
tmpfs                         5,0M       0  5,0M   0% /run/lock
tmpfs                         1,5G       0  1,5G   0% /sys/fs/cgroup
/dev/sda1                     687M    107M  531M  17% /boot
/dev/mapper/scribe--vg-tmp    1,8G    3,4M  1,7G   1% /tmp
/dev/mapper/scribe--vg-var    8,1G      8G  0,1G  99% /var
/dev/mapper/scribe--vg-home    18G    149M   18G   1% /home
tmpfs                         301M       0  301M   0% /run/user/0
root@scribe:~#
```

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.

Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

Pour démonter le périphérique :

```
root@scribe:~# umount /home
```

Si le périphérique est occupé, la commande `lsof` renvoie les programmes utilisant la partition :

```
# lsof | grep home
```

Il faut alors arrêter les services concernés puis démonter la partition.

Vérifier le support

Pour vérifier le support, lancer la commande :

```
# fsck -f /dev/mapper/scribe--vg-home
```

Diminuer la taille de la première partition

Réduire le système de fichiers :

```
# resize2fs -p /dev/scribe-vg/home 1G
```

Réduire la partition logique :

```
# lvresize -L-1G /dev/scribe-vg/home
```

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/home
```

Vérifier l'espace libéré

Pour vérifier que l'espace a bien été libéré il faut utiliser la commande `vgdisplay` :

```
# vgdisplay
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  6
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       10060 / 39,30 GiB
  Free  PE / Size       0 / 0
  VG UUID               hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3

root@scribe:~#
```

La ligne `Free PE / Size` affiche l'espace libre.

Agrandir la taille de la deuxième partition

Les agrandissements peuvent se faire à chaud, ce qui est recommandé si la partition contient les commandes.

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/var
```

Agrandir la partition logique :

```
# lvresize -L+1G /dev/scribe-vg/var
```

Étendre le système de fichiers (sans option le système de fichiers prend toute la place possible) :

```
# resize2fs  /dev/scribe-vg/var
```

Remonter le périphérique

Procéder au montage du périphérique avec la commande `mount` :

```
# mount /var/home
```

Pensez à redémarrer les services qui ont précédemment été arrêtés.

CAS Authentication failed !

Le message ***`CAS Authentication failed ! You were not authenticated.`*** *(ou* ***`Authentification CAS infructueuse ! Vous n'avez pas été authentifié(e).`*** *)* peut apparaître si des modifications ont été faites dans l'interface de configuration.

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

```
# reconfigure
```

Vous avez ajouté un nom DNS alternatif ou une adresse IP alternative sur le serveur

Il faut ajouter le nom alternatif ou l'adresse IP alternative dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet `Certifs-ssl` en mode expert il faut remplir les champs `Nom DNS alternatif du serveur` et/ou l'adresse `IP alternative du serveur`.

Le bouton `+` permet d'ajouter autant d'alternatives que vous voulez. Il faut ensuite `Valider le groupe` et enregistrer la configuration.

L'opération doit être suivie de la reconfiguration du module, cela va régénérer le certificat `/etc/ssl/certs/eole.crt`

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

`# /usr/share/creole/gen_certif.py -f` ou `# /usr/share/creole/gen_certif.py -f nom_du_certificat` pour la régénération d'un certificat en particulier.

```
# reconfigure
```

Attention, les adresses suivantes ne sont pas définies comme sujet du certificat...

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient

à jour).

`# reconfigure`

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

`# reconfigure`

Une erreur se produit lors de l'instanciation ou d'un reconfigure : "starting firewall : [...] Erreur à la génération des règles eole-firewall !! non appliquées !"

Le message suivant apparaît à l'instance ou au reconfigure après changement de valeurs dans l'interface de configuration du module :

`* starting firewall : bastion (modèle XXX) Erreur à la génération des règles eole-firewall !!`

`non appliquées !`

Vérifier la configuration des autorisations d'accès à SSH et à l'EAD sur les interfaces réseau

Cette erreur provient certainement du masque des variables d'autorisation d'accès à SSH sur l'une des interfaces réseau.

Pour autoriser une seule IP, par exemple `192.168.1.10`, le masque doit être `255.255.255.255` pour autoriser une IP particulière et non 255.255.255.0

Vérifier l'ensemble des autorisations pour l'accès SSH et pour l'accès à l'EAD.

Pour appliquer les changements il faut reconfigurer le module :

`# reconfigure`

La connexion SSH renvoie Permission denied (publickey)

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant : `Permission denied (publickey).`

Gestion des mises à jour

Pour connaître la date et l'heure des mises à jour du système il est possible de passer par l'EAD ou par un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

```
python -c "from creole import maj; print maj.get_maj_day()"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un

terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

Activation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly add
```

ou :

```
python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly del
```

ou :

```
python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

Le mot de passe par défaut ne fonctionne pas

Suite à une nouvelle installation le mot de passe par défaut ne fonctionne pas.

Le mot de passe à saisir comprend les dollars devant et derrière : `$eole&123456$`

Échec de la connexion sécurisée

Le navigateur affiche :

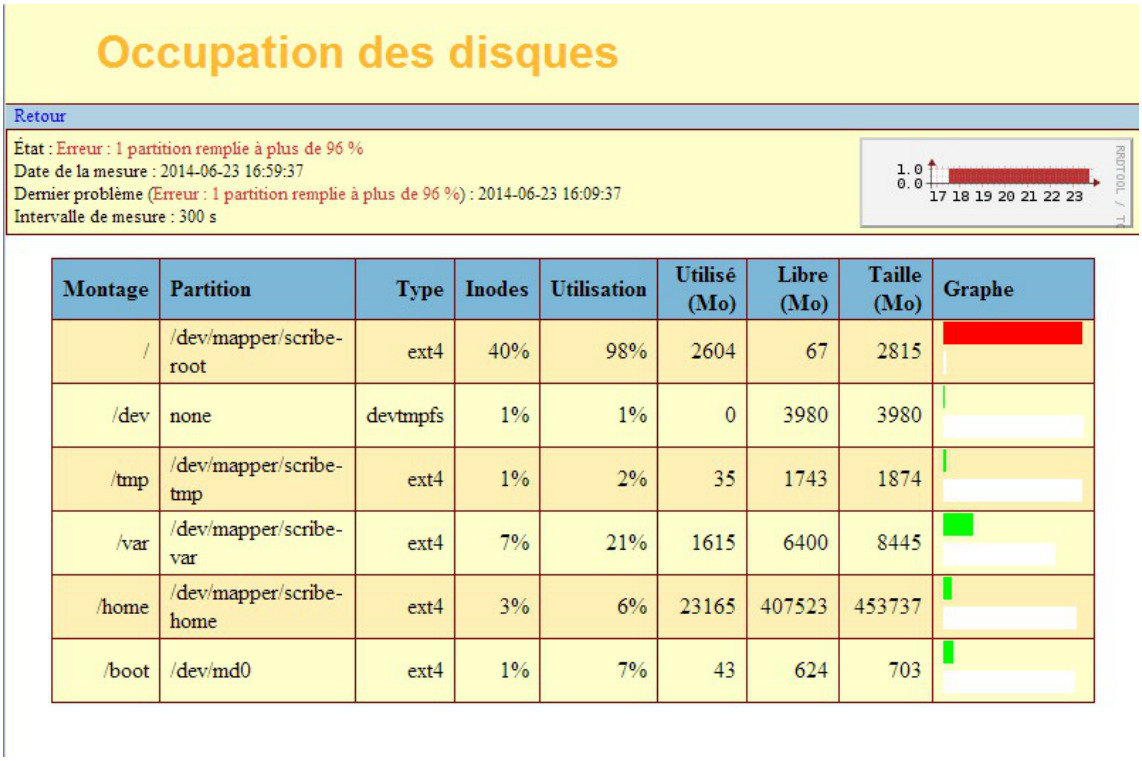
```
Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à IP:Port.

Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :

Votre certificat contient le même numéro de série qu'un autre certificat émis par l'autorité de certification. Veuillez vous procurer un nouveau certificat avec un numéro de série unique.

(Code d'erreur : sec error reused issuer and serial)
```

Les paramètres constituant un certificat ont été modifiés récemment

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une régénération des certificats a eu lieu.

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

Partition saturée



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

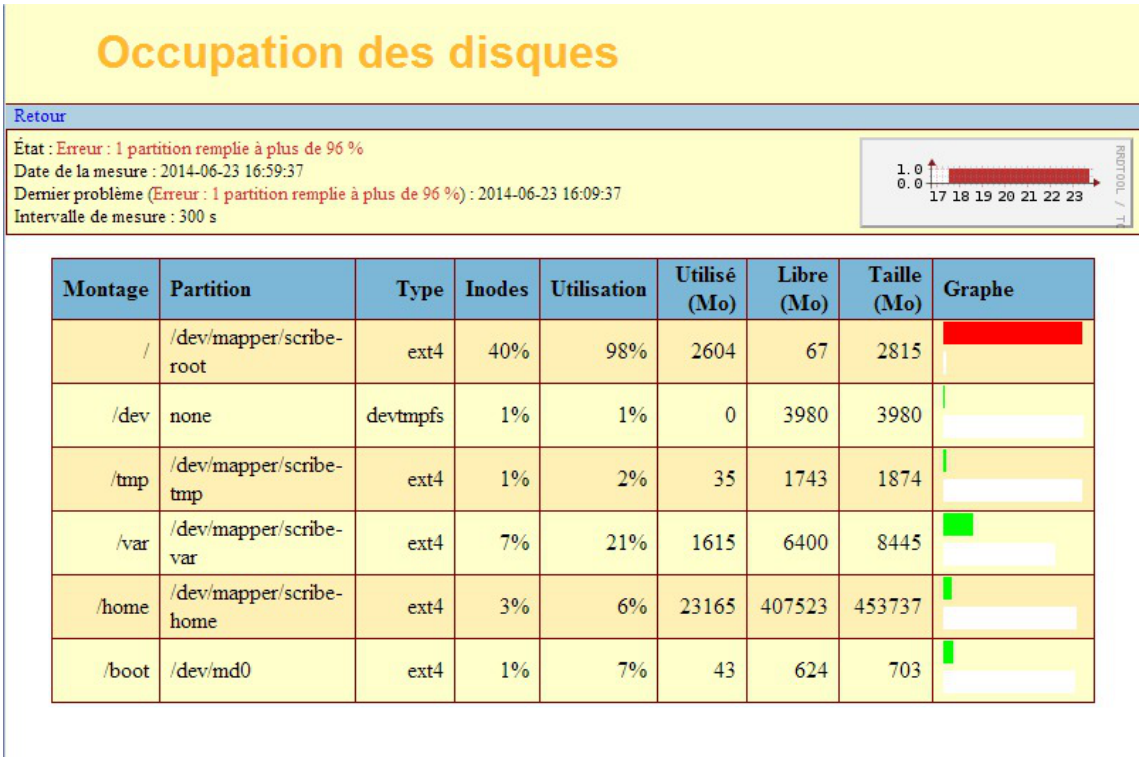
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- le manque de place disponible ;
- le manque d'inodes disponibles.

La cause de la saturation apparaît dans la page Occupation des disques, soit les inodes soit l'utilisation sont à un pourcentage élevé. La résolution du problème est différente selon le cas.

Partition / saturée



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

1.0
0.0
17 18 19 20 21 22 23
RRDTOOL / TO

Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Si la partition racine est saturée sans raison apparente et que le taux d'inodes est correct, le montage d'un répertoire avant copie a peut être échoué. La conséquence est que la copie c'est faite sur la partition racine et non sur le montage. Cela peut être le cas, par exemple, de la sauvegarde.

Il faut donc vérifier le contenu et la place occupée par les répertoires (points de montage) `/mnt`, `/mnt/sauvegardes` et `/media` :

Si le répertoire `/mnt/sauvegardes` n'est pas monté il doit être vide :

```
root@scribe:/mnt/sauvegardes# ls -la
total 8 drwxr-xr-x 2 root root 4096 mai 25 11:29 ./ drwxr-xr-x 26 root root 4096 sept. 9 21:07 ../
root@scribe:/mnt/sauvegardes#
```

Normalement le répertoire `/media` ne contient que des sous-dossiers pour le montage des partitions et ou des périphériques.

Pour vérifier l'espace occupé par ces différents répertoires :

```
root@scribe:/# du -h --max-depth=1 /media /mnt/
4,0K /media 4,0K /mnt/
```

Dans certains cas particuliers, la taille allouée à la partition `/` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM[p. 183]).

Partition /var saturée

Cette partition contient entre autres les journaux systèmes du serveur.

La commande suivante affiche l'espace occupé par chaque répertoire et les classe par taille, le plus grand nombre en dernier (sans tenir compte de l'unité) :

```
# du -smh /var/* | sort -n
```

Un service mal configuré génère une quantité importante de journaux. Si le problème n'est pas résolu la partition va de-nouveau saturer.

Dans certains cas particuliers, la taille allouée à la partition `/var` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM[p. 183]).

Partition /var saturée en inode

Un nombre important de fichiers peut être du à un service mal configuré mais peut aussi être du à un fonctionnement normal. Il faut identifier le répertoire dans lequel il y a le plus de fichier.

La commande suivante affiche le nombre de fichiers par répertoire et les classe par taille, le plus grand nombre en dernier :

```
# for i in $(find /var -type d); do f=$(ls -A $i | wc -l); echo "$f : $i"; done | sort -n
```

Selon les circonstances il faudra soit supprimer des fichiers soit agrandir la partition.

La suppression de fichier ne doit pas être effectué sans connaissances solides du système d'exploitation.

Liste d'arguments trop longue

La commande `# rm -rf /var/<rep>/*` renvoie `Liste d'arguments trop longue`.

Préférez l'utilisation d'une autre commande :

```
# find /var/<rep>/* -type f -name "*" -print0 | xargs -0 rm
```

Le démarrage reste figé à l'étape de vérification des disques

Le serveur est virtualisé avec une solution basée sur l'émulateur qemu.

Seul l'affichage est figé, la machine démarre en fait normalement et est certainement accessible par SSH. Cela vient du support de la carte graphique. Il faut forcer la carte graphique à utiliser une autre carte graphique que celle par défaut (cirrus).

Sous Proxmox, indiquez carte `VGA standard` à la place de `par défaut`.

Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.

Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :

1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet `Eoleflask`.
2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.

Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

```
https://<adresse_serveur>:7000/genconfig/
```

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.

Un fichier `config.eole.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.

S'il existe une différence entre `config.eol` et `config.eole.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Impossible de trouver la base des matériels maintenue par EOLE

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Changer le disque dur du serveur

Il est possible entre autre de faire une image avec le logiciel Clonezilla.

L'UUID[p.187] ayant naturellement changé il faut démarrer en utilisant un LiveCD et éditer l'UUID dans `/etc/fstab` du serveur.

Sources supplémentaires pour apt

Il est possible d'ajouter des sources supplémentaires pour le logiciel apt.

Pour que la solution soit pérenne il faut ajouter dans le répertoire `/etc/apt/sources.list.d/` la description de la nouvelle source dans un fichier portant l'extension `.list`

Par exemple pour avoir à disposition `SCENARIserveur` sur un module EOLE il faut ajouter le fichier `scenari.list` dans le répertoire `/etc/apt/sources.list.d/` avec le contenu suivante :

```
#scenari ppa
deb https://download.scenari.org/deb precise main
```

Il faut ensuite mettre la liste des paquets disponibles à jour avec la commande `apt-get update`.

Dysfonctionnement des agents suite à un changement d'architecture

En allant sur la page des statistiques de surveillance d'un serveur (EAD ou Application Zéphir), j'obtiens

un message du type `rrdtool.error: This RRD was created on another architecture`

Ce problème peut survenir en cas de réinstallation des données d'un serveur 32 bits sur un serveur 64 bits (ou inversement).

Une solution consiste à supprimer les fichiers de statistiques :

- Statistiques propres au serveur Zéphir

  Concerne les statistiques de Zéphir lui-même, pour les statistiques des serveurs clients, l'erreur doit être corrigée sur le client (voir cas suivant).

  ```
  # service zephir stop
  # rm -rf /var/lib/zephir/data/0/*
  # service zephir start
  ```

- Sur un module EOLE autre que Zéphir

  ```
  # service z_stats stop
  # rm -rf /usr/share/zephir/monitor/data/*
  # rm -rf /usr/share/zephir/monitor/stats/*
  # service z_stats start
  ```

Si perdre les statistiques pose problème, il est possible de convertir les fichiers `.rrd` avec l'outil rrdtool.

Depuis l'ancien serveur, pour convertir les fichiers RRD vers des fichiers XML avec la commande `dump` :

```
# rrdtool dump stats.rrd > stats.xml
```

Après les avoir transférés sur le nouveau serveur il faut les convertir en RRD avec la commande `restore` :

```
# rrdtool restore -f stats.xml stats.rrd
```

Le serveur peut maintenant lire le fichier. Vous pouvez le tester avec la commande `info` :

```
# rrdtool info stats.rrd
```

Attention, il y a un (ou plusieurs) fichier par agent.

Exemple sur un serveur Zéphir :

```
root@zephir:~# ls -l /var/lib/zephir/data/0/*/*.rrd -rw-r--r-- 1 root root 11464 août 31 14:51 /var/lib/zephir/data/0/bastion/status.rrd -rw-r--r-- 1 root root 17032 août 31 15:27 /var/lib/zephir/data/0/bilan/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/debsums/status.rrd -rw-r--r-- 1 root root 1000 août 31 14:51 /var/lib/zephir/data/0/diag/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/diskspace/status.rrd
[…]
```

Si vous voulez convertir un répertoire entier en XML, utilisez ce petit script bash :

```
# for f in *.rrd; do rrdtool dump ${f} > ${f}.xml; done
```

Source : http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite

Comment débloquer les message en file d'attente ?

Un nombre de messages apparaissent comme étant *Frozen* dans le retour de la commande `diagnose`.

```
*** Messagerie
. Courrier SMTP => Ok
. File d'attente => 1 message(s)
. Messages "Frozen" => 1 message(s)
```

Une solution consiste à récupérer les identifiants des messages :

```
root@scribe:~# exim4 -bp
10h 2.5K 1abJaX-00036S-Bu <> *** frozen ***
touser@ac-test.fr
```

Il est ensuite possible de récupérer les journaux spécifiques message par message :

```
root@scribe:~# exim4 -Mvl 1abJaX-00036S-Bu
2016-03-03 04:06:05 Received from <> R=1abJaX-00036L-8j U=Debian-exim P=local S=2525
2016-03-03 04:06:05 SMTP error from remote mail server after RCPT TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
2016-03-03 04:06:05 touser@ac-test.fr R=satellite_route T=remote_smtp: SMTP error from remote mail server after RCPT TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
*** Frozen (delivery error message)
```

Dans cet exemple, le message d'erreur est `Recipient address rejected: Access denied`, l'expéditeur n'est pas autorisé à transiter par la passerelle configurée dans l'interface de configuration du module.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
root@eole:~# rm /etc/eole/extra/schedule/config.eol
rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

Le proxy empêche les mises à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le blocage de certaines mises à jour aussi, la déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon.

```
root@scribe:~# Maj-Auto
Mise à jour le lundi 20 mars 2017 11:47:52
*** scribe 2.6.1 ***

Maj-Auto - (VERSION CANDIDATE) - Augmenter le niveau de mise à jour peut empêcher de revenir au niveau de mise à jour stable.
Voulez-vous continuer ? [oui/non]
[non] : oui
pyeole.pkg - Pas de configuration du miroir Ubuntu avec eole.ac-dijon.fr qui semble inaccessible : Impossible d'obtenir la version pour le dépôt : http://eole.ac-dijon.fr/ubuntu/dists/xenial/main/binary-amd64/Release
pyeole.pkg - Pas de configuration du miroir Ubuntu avec ftp.crihan.fr qui semble inaccessible : Impossible d'obtenir la version pour le dépôt : http://ftp.crihan.fr/ubuntu/dists/xenial/main/binary-amd64/Release
Maj-Auto - Impossible de configurer les sources APT pour Ubuntu
```

La déclaration du proxy s'effectue dans l'onglet `Général` de l'interface de configuration du module, passer `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui` et paramétrer l'adresse du proxy dans le champ `Nom ou adresse IP du serveur proxy`.

Pour effectuer les mises à jour d'un module qui n'est pas encore instancié, il faut configurer manuellement la variable d'environnement :

```
# export http_proxy=http://<adresseProxy>:<portProxy>
# Maj-Auto
```

Comment lister les services gérés par CreoleService

Il peut être utile de lister les services qui sont gérés par CreoleService.

Une astuce consiste à utiliser la commande `CreoleGet .containers.services|grep \.name=`

```
root@eolebase:~# CreoleGet .containers.services|grep \.name=
service0.name="networking"
service1.name="cron"
service10.name="exim4"
service11.name="eoleflask"
service12.name="nginx"
service13.name="ead3"
service14.name="genconfig"
service15.name="bastion"
service16.name="z_stats"
service2.name="rng-tools"
service3.name="ntp"
service4.name="nut-server"
service5.name="salt-api"
service6.name="salt-master"
service7.name="salt-minion"
service8.name="ead-server"
service9.name="ead-web"
root@eolebase:~#
```

Résoudre des dysfonctionnements liés à l'EAD

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation du fichier journal `/var/log/ead/ead-server.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```
service ead-server stop
cd /tmp
export PYTHONPATH=/usr/share
twistd -noy /usr/share/ead2/backend/eadserver.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

Si c'est le service `ead-web` qui est en erreur et que le fichier journal `/var/log/ead/ead-web.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```
service ead-web stop
cd /tmp
export PYTHONPATH=/usr/share
twistd -noy /usr/share/ead2/frontend/frontend.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

2. Questions fréquentes propres au module Sphynx

Compatibilité du module Sphynx avec les différentes versions du module Amon

Un serveur Sphynx 2.5 est-il en mesure d'établir des tunnels VPN avec des serveurs Amon 2.6 ?

Inversement, un Sphynx 2.6 est-il en mesure d'établir des tunnels VPN avec des serveurs Amon 2.7 et 2.5 ?

La compatibilité est assurée par strongSwan

Actuellement toutes les versions maintenues du module Sphynx fonctionnent avec toutes les versions maintenues du module Amon et inversement.

La compatibilité du module Sphynx avec les versions du module Amon est dépendante de la compatibilité des versions de strongSwan[p.186] entre elles. Pour le moment, les versions divergent peu.

Pour vérifier cette compatibilité, il est possible de relever les différentes versions de strongSwan intégrées sur les serveurs concernés et de se rendre sur le site du projet strongSwan : https://strongswan.org/.

Glossaire

Agent SSH *= Agent d'authentification*	Un agent stocke en mémoire les clés privées utilisées lors de l'authentification par clef publique (RSA, DSA, ECDSA) pendant toute la durée de la session. L'utilisation d'un agent, évite donc d'avoir à retaper la phrase secrète à chaque fois que l'on sollicite l'utilisation de la clé privée. L'agent se lance au début d'une session (graphique ou non) et tous les appels (fenêtres ou autres programmes) sont réalisés en tant que client du programme de l'agent SSH. Grâce à des variables d'environnement, l'agent peut être trouvé et être utilisé pour l'authentification lors de la connexion à d'autres machines en SSH. ssh-agent est l'agent d'authentification inclus dans la suite logicielle OpenSSH.

AGRIATES *= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires*	De responsabilité partagée entre les collectivités locales et les académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications Intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements. RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE. http://www.igc.education.fr/agriates/agriates.htm C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements. RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes. RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement. RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.
ANSSI *= Agence nationale de la sécurité des systèmes d'information*	Service à compétence nationale, l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale. Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Source : https://www.cert.ssi.gouv.fr/a-propos/
Anti-spoofing *= Anti-usurpation d'adresse IP*	L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.

ARV *= Administration de Réseaux Virtuels*	ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan. http://www.strongswan.org/
Autorité de Certification *= CA : Certification Authority*	AC est l'acronyme de Autorité de Certification. Une autorité de certification est une société ou un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.
Backbone.js	Backbone est une bibliothèque JavaScript avec une interface RESTful JSON et est basée sur le modèle-vue-contrôleur (MVC). Cette bibliothèque est connu pour être légère, comme sa seule dépendance avec la bibliothèque JavaScript Underscore.js. Elle est conçu pour développer des applications web d'une seule page et permet de maintenir les différentes parties d'applications Web (par exemple, les clients multiples et le serveur) synchronisée. Backbone a été créé par Jeremy Ashkenas, qui est également connu pour CoffeeScript. http://backbonejs.org/
Basculement *= fail-over*	Le basculement (en anglais, fail-over qui se traduit par passer outre à la panne) est la capacité d'un équipement à basculer automatiquement vers un réseau alternatif ou en veille. Il existe deux modes principaux de basculement : • actif/actif qui s'apparente plus à de l'équilibrage de charge (load-balancing) ; • le mode classique couramment répandu, actif/passif où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.
BIND *= Berkeley Internet Name Domain*	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet. http://www.isc.org/downloads/bind/
Cluster *= Grappe, bloc, ensemble*	Un cluster est un terme anglophone qui est utilisé pour parler de grappe ou de bloc suivant le contexte dans lequel il est utilisé : • un cluster de serveur est une grappe de serveur constituée au minimum de 2 machines qui partage des ressources communes la plupart du temps à travers le réseau ; • un cluster peut également être un bloc, un ensemble de données ou d'éléments présentant des similarités ; • un cluster peut être un système informatique composé d'unité de calcul permettant une répartition de charge et une optimisation des traitements à réaliser pour effectuer des calculs.
CN *= Common Name*	Valeur permettant d'identifier le serveur dans le certificat.

Conteneur *= LXC*	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
Corosync Cluster Engine *= Corosync*	Corosync Cluster Engine est un moteur libre de cluster. C'est un système de communication avec des fonctionnalités supplémentaires pour la mise en œuvre de la haute disponibilité dans les applications. Le projet fournit quatre fonctionnalités principales : • un groupe restreint de processus avec une garantie de synchronisation virtuelle afin de créer des machines à états répliquées ; • un simple gestionnaire de disponibilité qui redémarre les processus d'application lorsqu'ils ont échoués ; • une configuration et des statistiques stockées en base de données dans la mémoire vive permet de définir, de récupérer et de recevoir des notifications concernant les changements d'état ; • un système de notification qui se déclenche lorsque un quorum est atteint ou perdu. Sources : https://fr.wikipedia.org/wiki/Corosync_Cluster_Engine et http://clusterlabs.org/
CRL	Acronyme : Certificate Revocation List Une CRL ou Liste de Certificats Révoqués (LCR) est une liste, datée et signée par une Autorité de Certification, des numéros de série des certificats révoqués (mis en opposition) et non expirés, mise à jour périodiquement.
DNS *= Domain Name System*	Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types. L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP. Source : http://fr.wikipedia.org/wiki/Dns

e2guardian	e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie. Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian. http://e2guardian.org
Flask	Flask est un framework d'application web léger écrit en Python et basé sur le toolkit Werkzeug (une librairie Python WSGI) et sur le moteur de template Jinja2. Flask est appelé microframework parce qu'il garde un cœur simple, mais extensible. Il n'y a aucune couche d'abstraction de données, pas de formulaire de validation ou tout autre composant que des bibliothèques tierces ne traitent déjà. Cependant, Flask supporte les extensions, ce qui permet d'ajouter des fonctionnalités si elles sont mises en œuvre dans Flask lui-même. Il existe des extensions pour utiliser les objets relationnels, valider des formulaires, le téléchargement, diverses technologies d'authentification ouvertes, et plus encore. Flask est sous licence BSD. http://flask.pocoo.org/
Haute Disponibilité *= High Availability ou HA*	La haute disponibilité c'est garantir la disponibilité et le bon fonctionnement d'un service ou d'une architecture informatique. Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité : • la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle. Est alors créé un cluster de haute-disponibilité (par opposition à un cluster de calcul) : une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités ; • la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur. ITIL contient de nombreux processus de ce type. Source Wikipédia : http://fr.wikipedia.org/wiki/Haute disponibilité
ICMP *= Internet Control Message Protocol*	Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

Image ISO *= Image disque*	Une image ISO est une archive proposant la copie conforme d'un disque optique ou magnétique. L'opération de gravure de l'image ISO consiste à recopier cette structure sur un disque optique.
IPsec *= Internet Protocol Security*	IPsec est un standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques. IPsec offre des services d'authentification, de contrôle d'intégrité et de confidentialité en s'appuyant sur un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. Source Wikipédia : http://fr.wikipedia.org/wiki/Internet Protocol Security
IPv6 *= Internet Protocol version 6*	L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4. Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
LVM *= Logical Volume Management*	La gestion par volumes logiques est à la fois une méthode et un logiciel. Elle permet le découpage, la concaténation, le redimensionnement et l'utilisation des espaces de stockage. Le logiciel permet de gérer, de sécuriser et d'optimiser de manière souple les espaces de stockage sur les systèmes d'exploitation de type UNIX.
Marionette	Marionette simplifie le code applicatif Backbone grâce à des vues robustes et des solutions d'architecture. http://marionettejs.com/
MTU *= Maximum Transmission Unit*	Le MTU définit la taille maximum d'un paquet (en octets) pouvant être transmis sur le réseau sans fragmentation. Source Wikipédia : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit

multicast	Le multicast est une forme de diffusion d'un émetteur (source unique) vers un groupe de récepteurs. Les termes « diffusion multipoint » ou « diffusion de groupe » sont également employés. En multicast, chaque paquet n'est émis qu'une seule fois et sera routé vers toutes les machines du groupe de diffusion sans que le contenu ne soit dupliqué sur une quelconque ligne physique ; c'est donc le réseau qui se charge de reproduire les données. Source Wikipédia : http://fr.wikipedia.org/wiki/Multicast
NTP *= Network Time Protocol*	NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.
NUT *= Network UPS Tools*	NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments : • le démon `nut` lancé au démarrage du système ; • le démon `upsd` qui permet d'interroger l'onduleur, il est lancé sur le PC relié à l'onduleur ; • le démon `upsmon` qui permet de monitorer et lancer les commandes nécessaires sur le réseau ondulé (arrêt de machines ...) ; • différents programmes pour envoyer des commandes manuellement à l'onduleur. `upsd` peut communiquer avec plusieurs onduleurs si nécessaire. `upsmon` interroge à intervalle régulier la machine du réseau sur laquelle est lancée `upsd`.
PKCS12 *= Public Key Cryptographic Standards*	Utilisé pour signer et/ou chiffrer des messages dans le cadre d'une infrastructure à clés publiques. Sert également à la transmission de certificats. Source : http://fr.wikipedia.org/wiki/Public_Key_Cryptographic_Standards
PKCS7 *= Public Key Cryptographic Standards*	Utilisé pour signer et/ou chiffrer des messages dans le cadre d'une infrastructure à clés publiques. Sert également à la transmission de certificats. Source : http://fr.wikipedia.org/wiki/Public_Key_Cryptographic_Standards

PKI *= Public Key Infrastructure*	Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques. Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs. En résumé, ces services sont les suivants : • enregistrement des utilisateurs (ou équipement informatique) ; • génération de certificats ; • renouvellement de certificats ; • révocation de certificats ; • publication de certificats ; • publication des listes de révocation (comprenant la liste des certificats révoqués) ; • identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'ICP) ; • archivage, séquestre et recouvrement des certificats (option). Source de la définition : http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_public
PNCN *= Plateforme Nationale de Confiance Numérique*	La PNCN est la nouvelle IGC de l'Éducation nationale.
Quagga	Quagga est une suite de logiciels de routage implémentant les protocoles OSPF (v2 & v3), RIP (v1, v2 & v3), BGP (v4) et IS-IS pour les plates-formes de type Unix. http://www.nongnu.org/quagga/
RACINE *= Réseaux d'Accès et de Consolidation des INtranets de l'Éducation nationale*	Les réseaux RACINE (Réseaux d'Accès et de Consolidation des INtranets de l'Éducation nationale) sont des réseaux privés virtuels (RPV) qui ont pour objet d'offrir et garantir un environnement d'accès sécurisé aux systèmes d'information de l'Éducation nationale pour toute communauté d'utilisateurs " ayant droit " quel que soit le lieu où les utilisateurs exercent leurs activités professionnelles. http://www.igc.education.fr/IGC/IGC.htm L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE.
RELP *= Reliable Event Logging Protocol*	Reliable Event Logging Protocol ou RELP est un protocole définissant un service de journaux d'événements d'un système informatique. Il est supporté entre autres par Rsyslog.

Réseau virtuel Privé *= RVP ou VPN (Virtual Private Network) en anglais*	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.
SMTP *= Simple Mail Transfer Protocol*	SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
Squid	Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.
SSH *= Secure Shell*	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
StartTLS	Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas, par exemple des protocoles de mails IMAP et SMTP ou LDAP.
strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/
TCP *= Transmission Control Protocol*	TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport qui travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.

Tiramisu *= Outil de gestion de configuration*	À cause de l'afflux de plus en plus grand des options de configuration des serveurs EOLE (plus de 1600 au dernier recensement), il était devenu de plus en plus difficile de correctement récupérer les options et de les utiliser là où elles devaient effectivement être employées. Pour remédier à ces difficultés, l'outil Tiramisu a été développé, il est utilisé comme moteur du générateur de configuration de la version EOLE 2.4. La documentation technique du projet : http://tiramisu.labs.libre-entreprise.org Les sources du projet Tiramisu : http://labs.libre-entreprise.org/projects/tiramisu/
TLS *= Transport Layer Security*	Le TLS et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le TLS est la poursuite des développements de SSL. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
UEFI *= Unified Extensible Firmware Interface*	Le standard UEFI définit un logiciel intermédiaire entre le micrologiciel (firmware) et le système d'exploitation (OS) d'un ordinateur. Cette interface succède sur certaines cartes-mères au BIOS. Elle fait suite à EFI (Extensible Firmware Interface), conçue par Intel pour les processeurs Itanium. Source Wikipédia : https://fr.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
UUID *= Universally Unique IDentifier*	Le but des UUID est de permettre à des systèmes distribués d'identifier de façon unique une information sans coordination centrale importante. Dans ce contexte, le mot « unique » doit être pris au sens de « unicité très probable » plutôt que « garantie d'unicité ». Source : http://fr.wikipedia.org/wiki/Universal_Unique_Identifier
XML *= Extensible Markup Language*	L'Extensible Markup Language (« langage de balisage extensible » en français) est un langage informatique de balisage générique qui dérive du SGML. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG... Elle est reconnaissable par son usage des chevrons (< >) encadrant les balises. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche...) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés une application XML respecte généralement certains principes : • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. Source : http://fr.wikipedia.org/wiki/Xml

ZéphirLog	ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.