Installation et mise en œuvre du module Zéphir

EOLE 2.5.2

création : Mai 2015 Version : révision : Avril 2018

EOLE 2.5.2

Version : révision : Avril 2018

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

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 Zéphir

Le module Zéphir propose une solution normalisée pour faciliter le **déploiement**, la **surveillance** et la **maintenance** des modules EOLE.

Ce module permet une gestion centralisée des serveurs EOLE tout en autorisant certaines divergences de configuration.

Parmi d'autres fonctionnalités le module Zéphir permet :

- Gestion centralisée des configurations
  - Adaptations sous forme de variantes
  - Gestion par groupes
  - Préparation de la migration
- Surveillance des serveurs inscrits
  - État du système et des services
  - Alertes par courrier électronique
- Envoi de fichiers et exécution d'actions à distance.
- Fonctions spécifiques à certains modules : ARV, Seshat,...

1. Qu'est ce que le module Zéphir ?

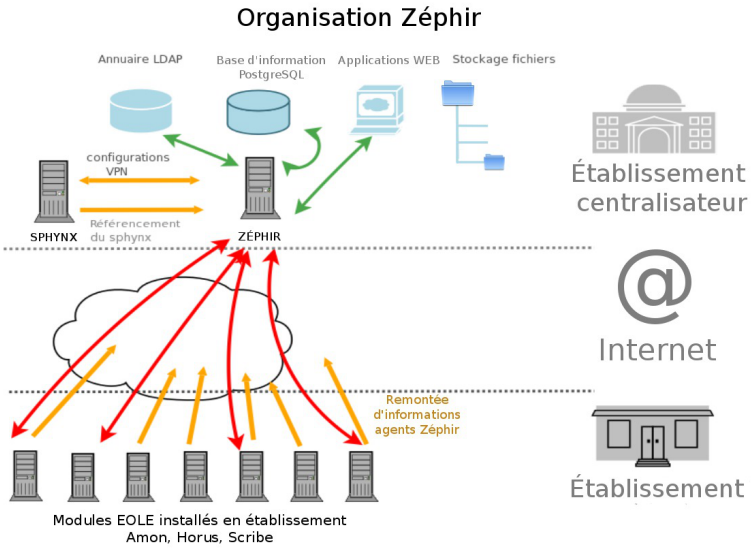
Le module Zéphir permet de déployer et gérer un parc de serveurs. Il héberge une base de données des établissements et des serveurs installés dans ces établissements. Cette base de données peut être pré--initialisée à partir du fichier national des établissements. L'ensemble constitue un inventaire de votre parc matériel.

Le module permet la gestion des différentes configurations serveur.

Il prend en charge :

- la génération des configurations serveurs (création du dictionnaire) ;
- le stockage de ces configurations ;
- la distribution de ces configurations sur les serveurs à travers le réseau ;
- la mise à jour des configurations avec une gestion des différentes versions et un historique des modifications effectuées.

Le module Zéphir permet également la surveillance des serveurs déployés en établissements. Il permet la remontée d'alertes à intervalles réguliers et le lancement d'actions à distance.



Organisation du module Zéphir

Principales fonctionnalités

- gestion centralisée des configurations ;
- travail sur des groupes de serveurs ;
- possibilité de spécialiser un module en variante ;
- aide à l'installation des serveurs clients ;
- actions à distance sur les clients ;
- surveillance des serveurs ;
- actions automatiques des agents ;
- possibilité de changer l'adresse IP du module Zéphir ;
- création d'actions personnalisées ;
- sauvegarde de fichiers dans une variante ;
- gestion des serveurs de mise à jour ;
- gestion centralisée d'identifiants pour les ENT.

2. À qui s'adresse ce module ?

Le module Zéphir s'adresse aux **administrateurs** et aux **équipes d'intervention** des réseaux informatiques académiques ou de toute autre structure (collectivités territoriales) ayant en charge l'installation, la configuration et le suivi de parcs de serveurs.

Le module Zéphir peut travailler par profils (rôles) ce qui permet des vues et des actions différentes sur les différents serveurs gérés.

Le module permet d'administrer et de surveiller plusieurs centaines de serveurs.

3. Les services Zéphir

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 Zéphir

- *PostgreSQL* : base de donnée relationnelle pour le stockage des informations du serveur ;
- *OpenLDAP* : service d'annuaire utilisé pour l'authentification des utilisateurs (annuaire local ou externe) ;
- *Ulog* : stockage des logs ;
- *Zephir-Web* : application web pour gérer les serveurs EOLE déployés.

4. Structure des conteneurs

Le module Zéphir s'installe par défaut en mode non conteneur[p.231].

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 sert à la surveillance et à la gestion à distance des modules EOLE.

La puissance de la machine est dépendante du nombre de serveurs à gérer.

Le cache des configurations étant activé par défaut, la mémoire RAM doit être privilégiée, elle dépend du nombre de serveurs à administrer. Il est recommandé d'avoir 4 Go pour environ 400/500 serveurs et au moins 8 Go au delà.

Les fonctionnalités du module demandent une bonne bande passante.

Le module héberge une base de donnée, il est souhaitable de favoriser une machine physique si le nombre de clients est important.

L'espace disque n'est pas la ressource la plus critique, par contre lors d'un partitionnement manuel il faut privilégier la partition `/var` qui contient le plus de données :

- les configurations et les fichiers personnalisés des serveurs ;
- la base de données ;
- les statistiques des serveurs ;
- les logs.

Un module Zéphir qui gère 600 serveurs utilise 20 Go d'espace disque dont une partition `/var` de plus de 7 Go. 8 Go de mémoire RAM sont nécessaire.

Le module Zéphir doit être accessible par les clients en SSH[p.235].

6. Les différences entre les versions 2.3 et 2.5

Le module Zéphir est un portage fonctionnel du module Zéphir 2.3.

Dans cette version, Zéphir prend en charge les modules EOLE dans les versions 2.3, 2.4 et 2.5.

Le module comporte quelques évolutions mineures :

- la gestion des thèmes a été améliorée ;
- ajout d'un délai pour lancer certaines actions (le délai est pris en compte après la prochaine connexion du client).

Pour la gestion des modules 2.4 et 2.5 :

- nouveau mode de gestion des dictionnaires ;
- l'édition de la configuration d'un module dans l'application web Zéphir se fait maintenant au travers de la nouvelle interface de configuration du module (intégration de la version gen_config 2.4/2.5).

Les versions 2.5 du module Zéphir ne prennent pas en charge les modules 2.6. D'une manière générale le serveur Zéphir ne gère pas de versions supérieures à lui-même. Si cette fonctionnalité existait dans la version 2.3 elle n'est pas possible a implémenter dans Zéphir 2.5 car des changements dans Creole et un changement de version de Tiramisu sur les versions EOLE 2.6 ne le permettent pas.

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.231] ;
- Backbone.js[p.230] et Marionette[p.232] ;
- Tiramisu[p.235].

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.235].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML[p.236] 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.

Paquet dédié pour le service PostgreSQL d'EOLE

Un paquet nommé `eole-postgresql` est nouvellement dédié pour gérer PostgreSQL.

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**.

2.5.2.1

Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI[p.236].

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 Zéphir

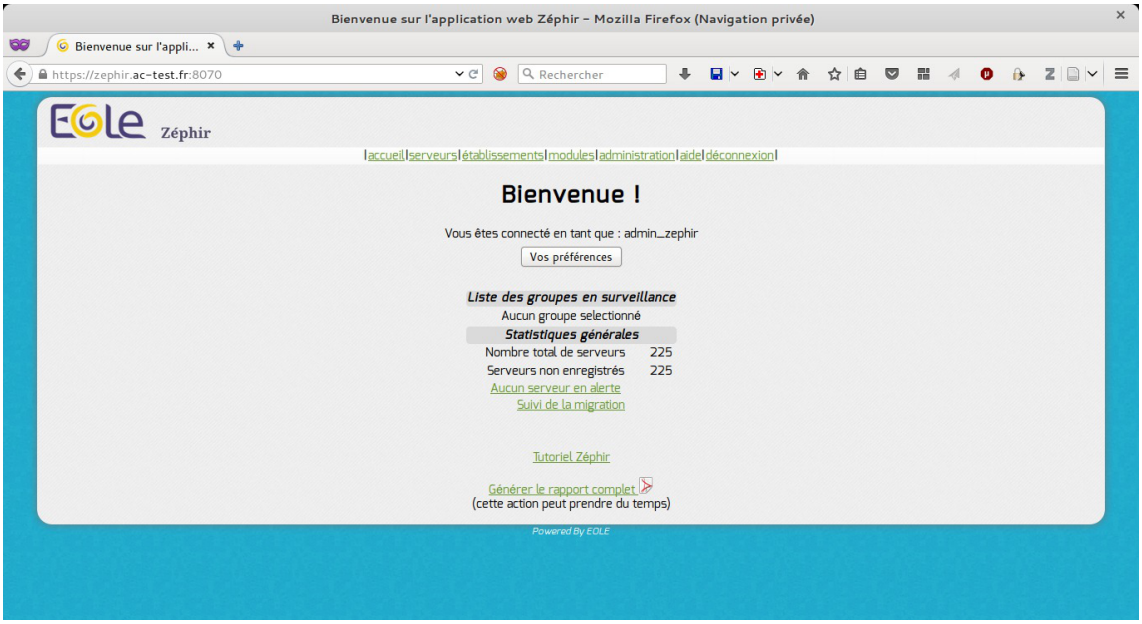
Pour jouer son rôle, le module Zéphir repose sur plusieurs projets libres : PostgreSQL, Twisted Matrix, OpenLDAP, ...

Le module Zéphir est constituée :

- d'une interface web ;
- d'un backend XMLRPC ;
- d'une base de donnée ;
- de clients installés sur l'ensemble du parc EOLE (agents Zéphir).

Les clients se connectent par l'intermédiaire des agents au serveur Zéphir à intervalle régulier via les protocoles SSH, UUCP et XMLRPC. À chaque connexion des clients, divers statistiques sont remontées auprès du serveur Zéphir. Les commandes et/ou transferts de fichier en attente sont également exécutées.

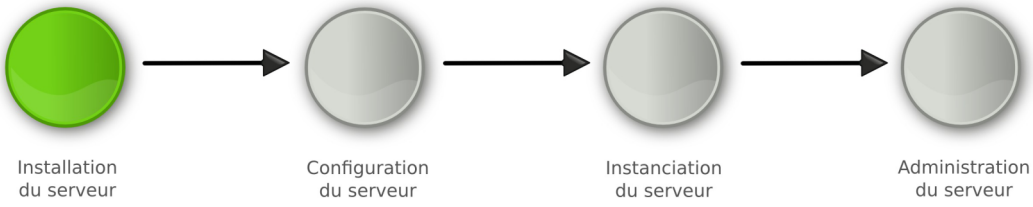
L'interface web Zéphir permet de gérer les serveurs surveillés.



Chapitre 3

Installation du module Zéphir

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.232] 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 Zéphir, la mise à jour n'est pas obligatoire mais fortement recommandée.

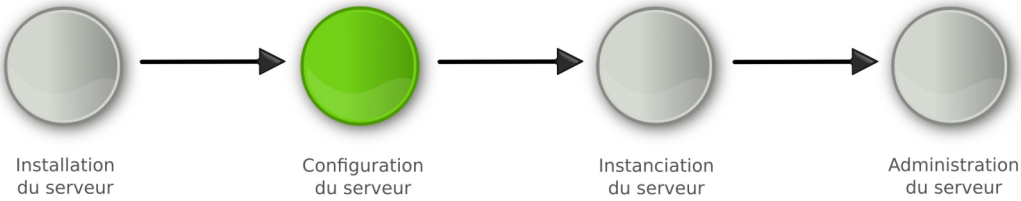
Mise à jour du module

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

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 Zéphir



Configuration

Les généralités sur la configuration **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 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.

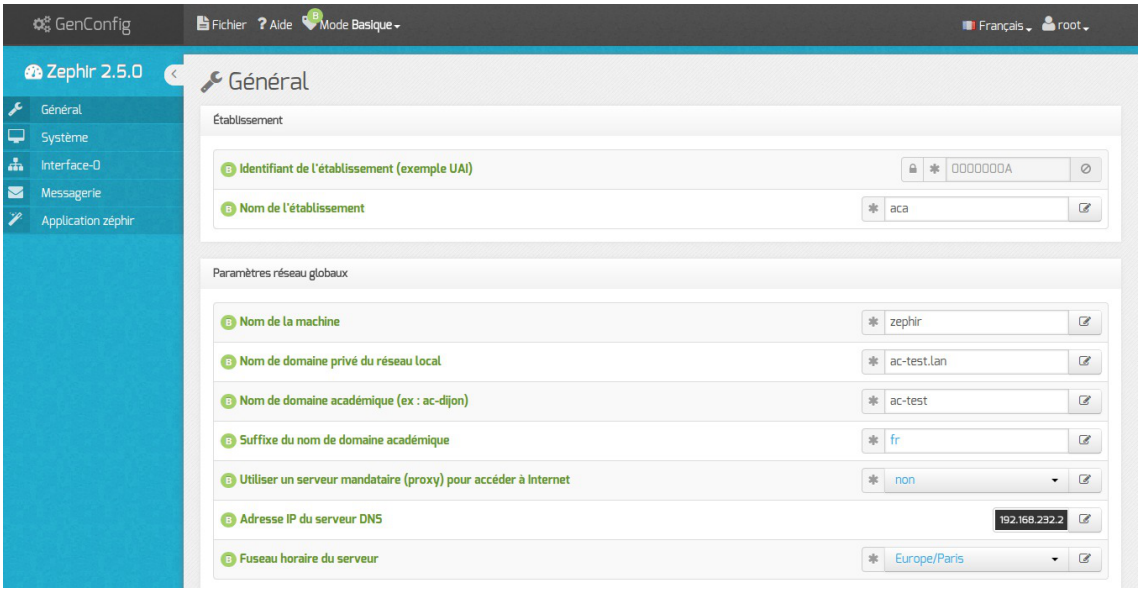
  Suivant les modules, le nombre de paramètres à renseigner est plus ou moins important.

  Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid[p.235], e2guardian[p.231], etc.

1. Configuration en mode basique

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

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

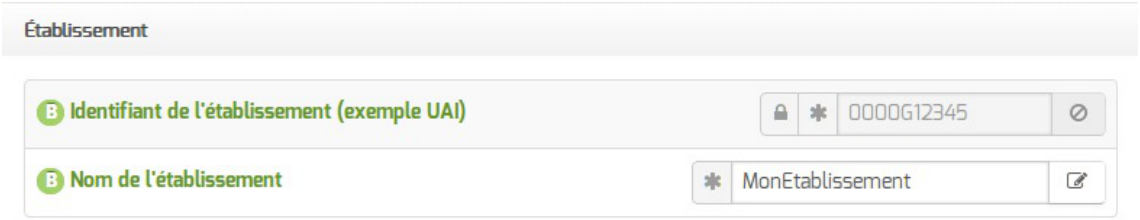


Vue générale de l'interface de configuration du module

1.1. Onglet Général

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

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

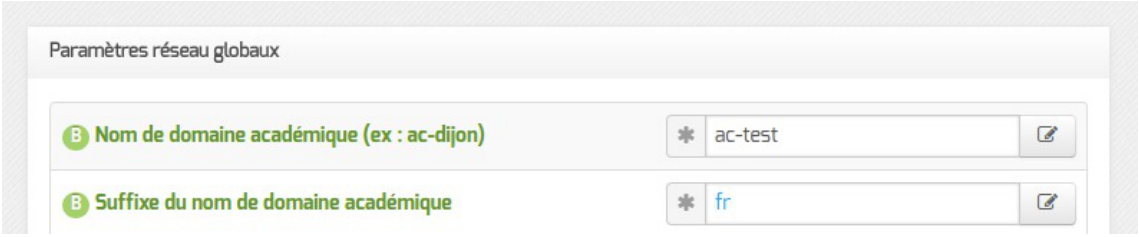
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

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

Sur les modules fournissant un annuaire LDAP[p.232] 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`.

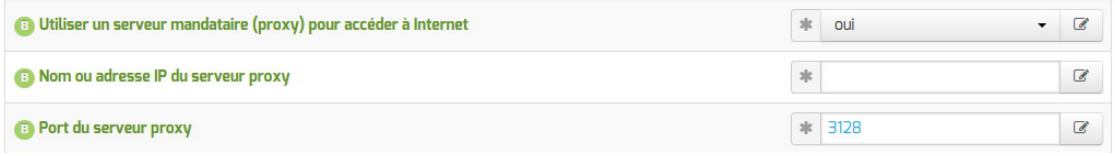
C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

> 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.

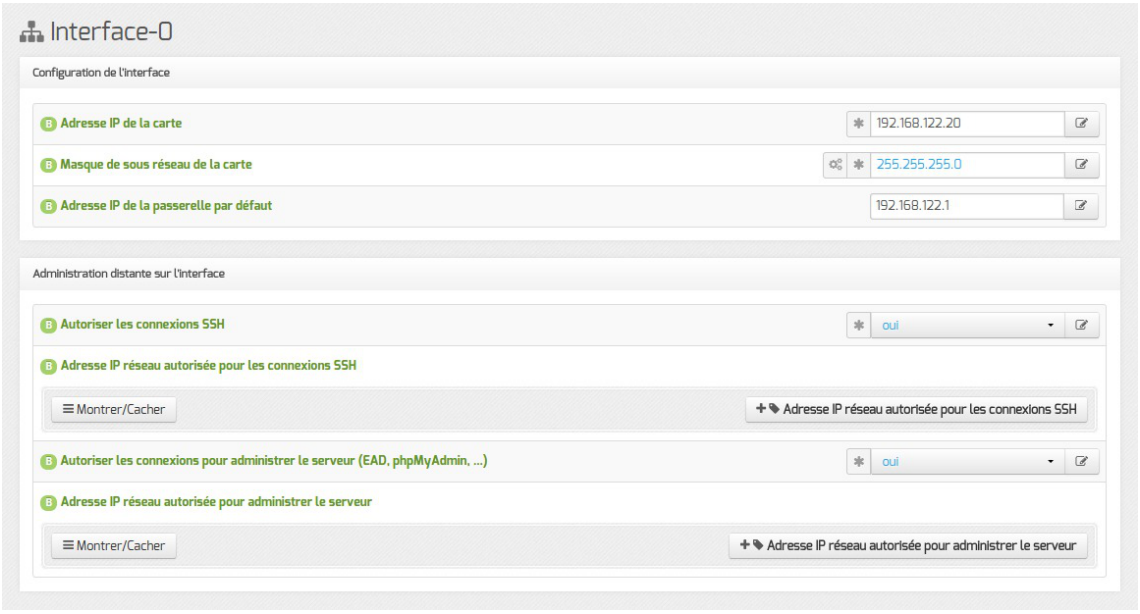
DNS et fuseau horaire

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.231].

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

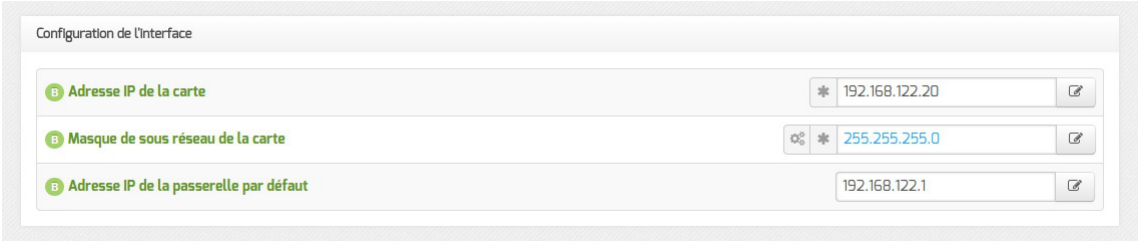
1.2. Onglet Interface-0

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



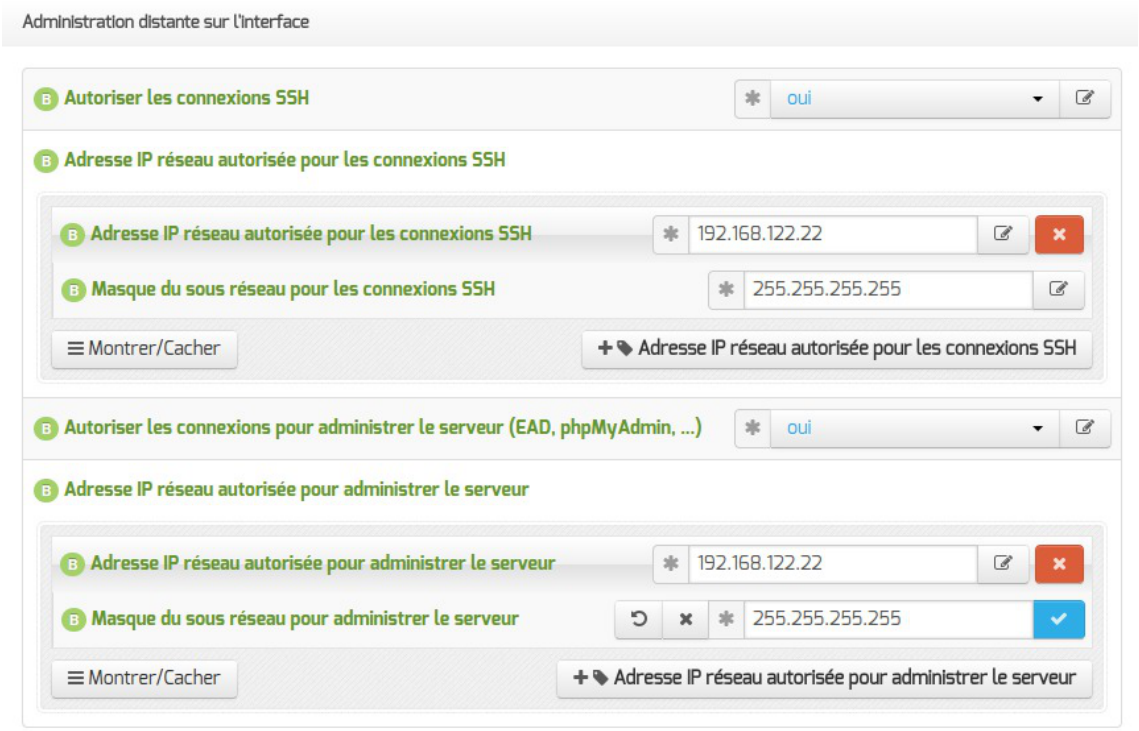
Vue de l'onglet Interface-n

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

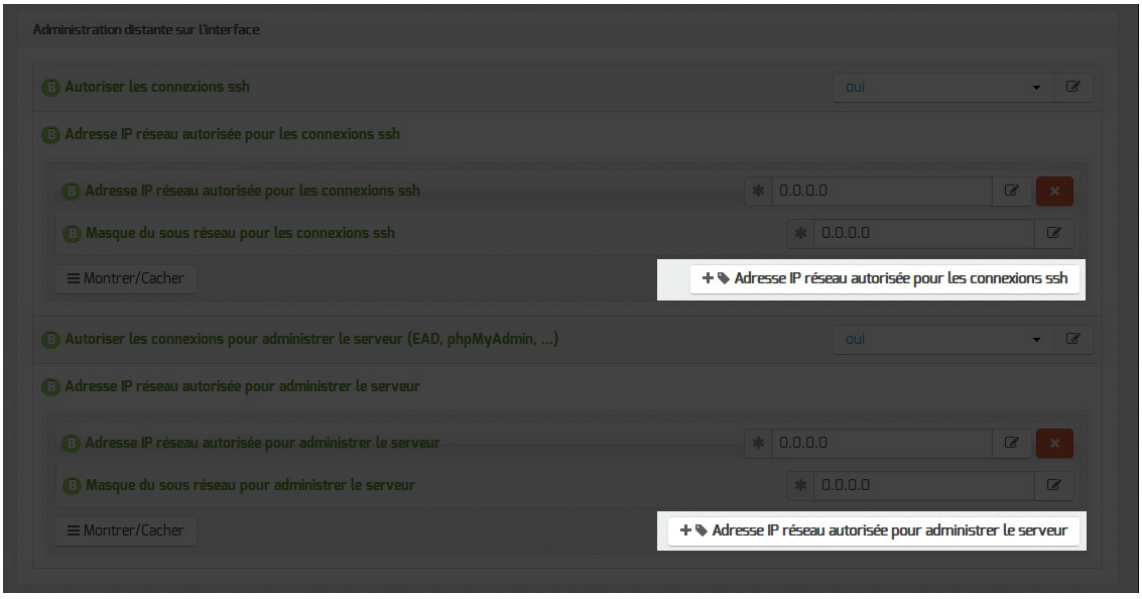


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.235] 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 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.

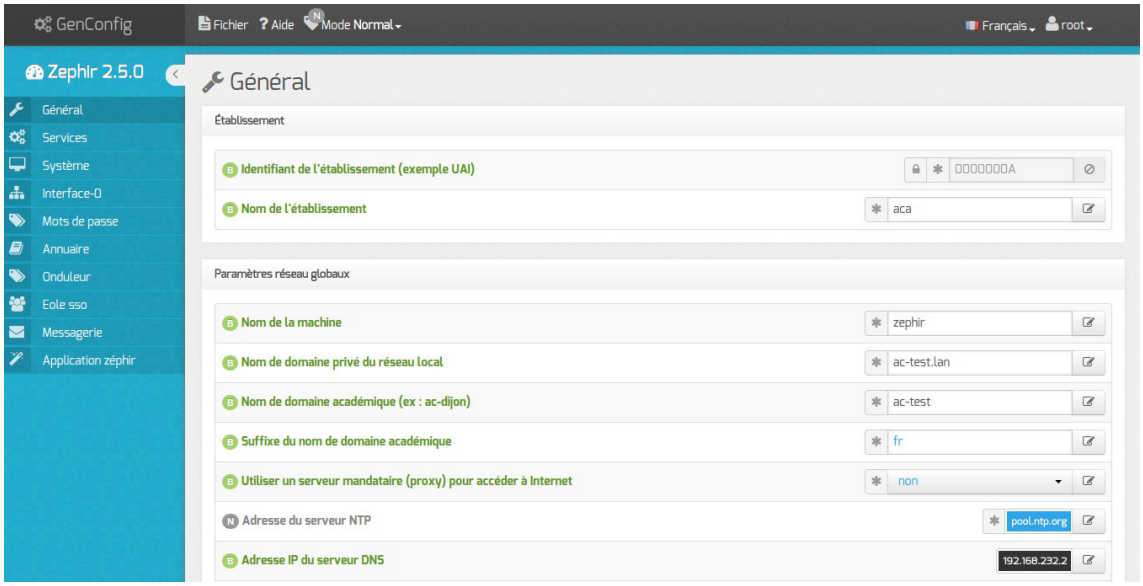
2. Configuration en mode normal

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 Zéphir :

- `Général` ;
- `Services` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Annuaire` ;
- `Onduleur` * ;
- `Eole sso` * ;
- `Messagerie` ;
- `Application zéphir`.

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

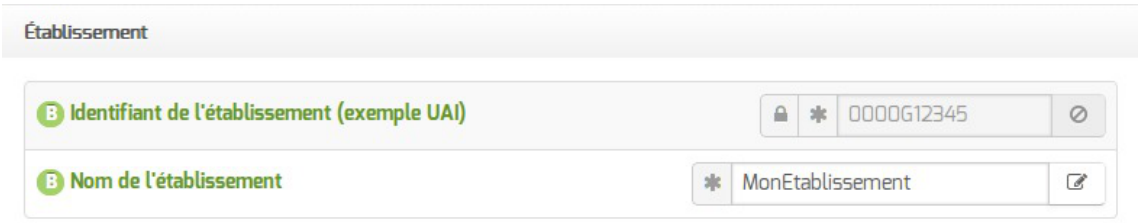
Par défaut, le module Zéphir est livré avec un annuaire LDAP local qui sert à enregistrer des utilisateurs et leur mot de passe.

Il est cependant possible de spécifier un annuaire distant lors de la configuration du module (par exemple : l'annuaire d'un module Horus, l'annuaire d'un module Scribe, ou encore un annuaire académique). Vous pourrez alors vous connecter avec un compte de l'annuaire utilisé.

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.232] 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.

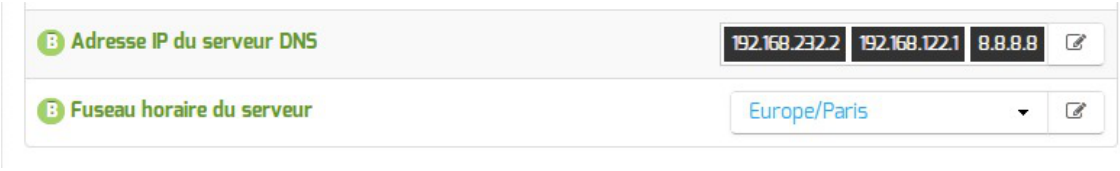
Proxy

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.

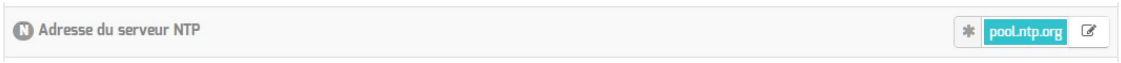
DNS et fuseau horaire



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.231].

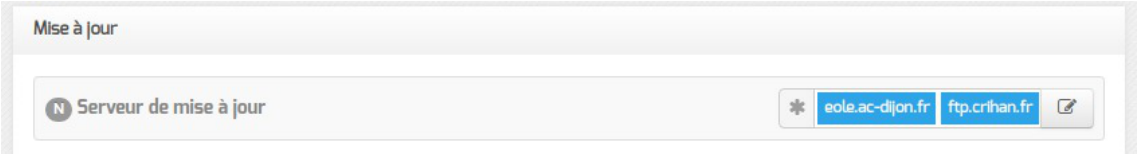
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.233]. 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...

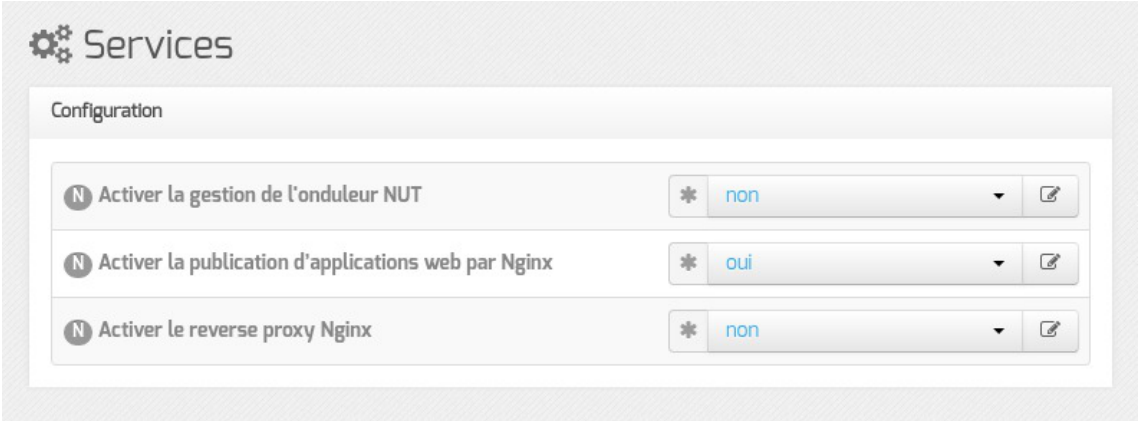
> Les différents types de mises à jour

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.

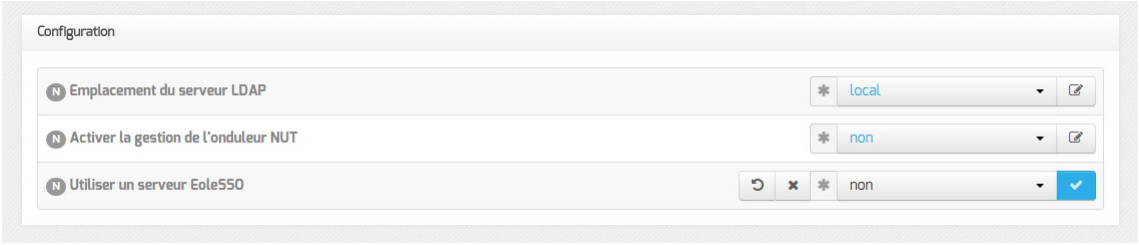
> Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un onglet de configuration propre au service.



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.233].

En mode normal l'onglet `Services` contient un peu plus de services activables ou désactivables.



Vue de l'onglet Services en mode normal

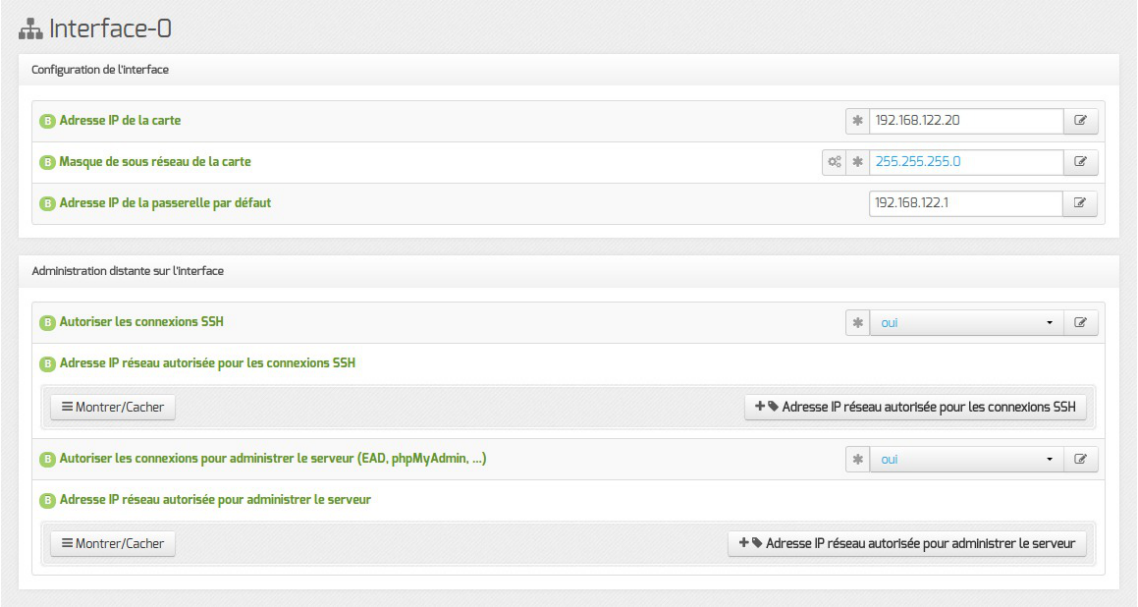
Les services disponibles propres au module Zéphir en mode normal sont les suivants :

- le serveur LDAP ;
- le service d'authentification unique EoleSSO.

Il est possible de positionner ces 2 services à `local` ou `distant`.

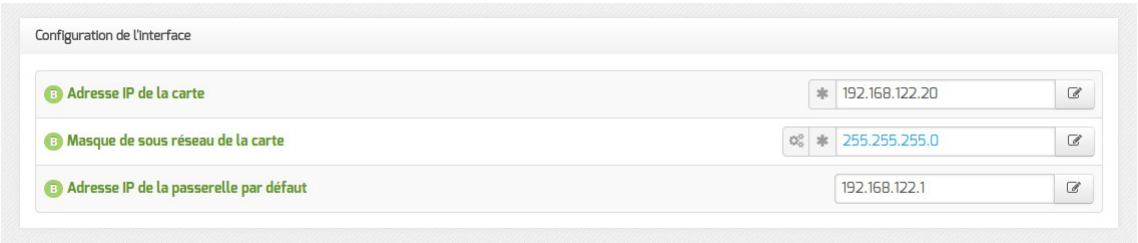
2.3. Onglet Interface-0

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.

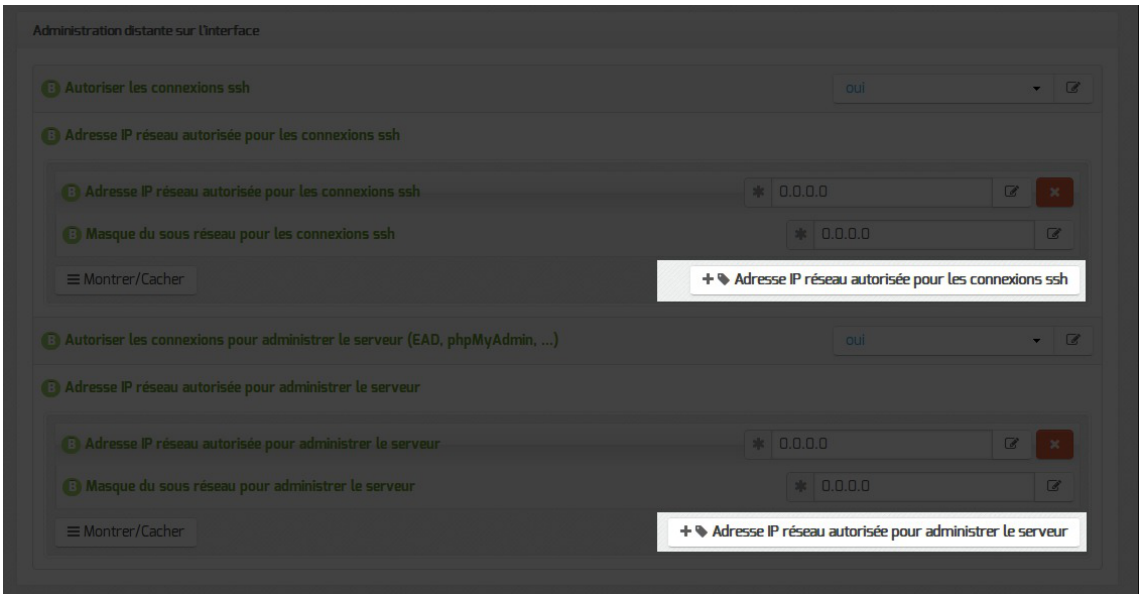
Administration à distance

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.235] 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…`.

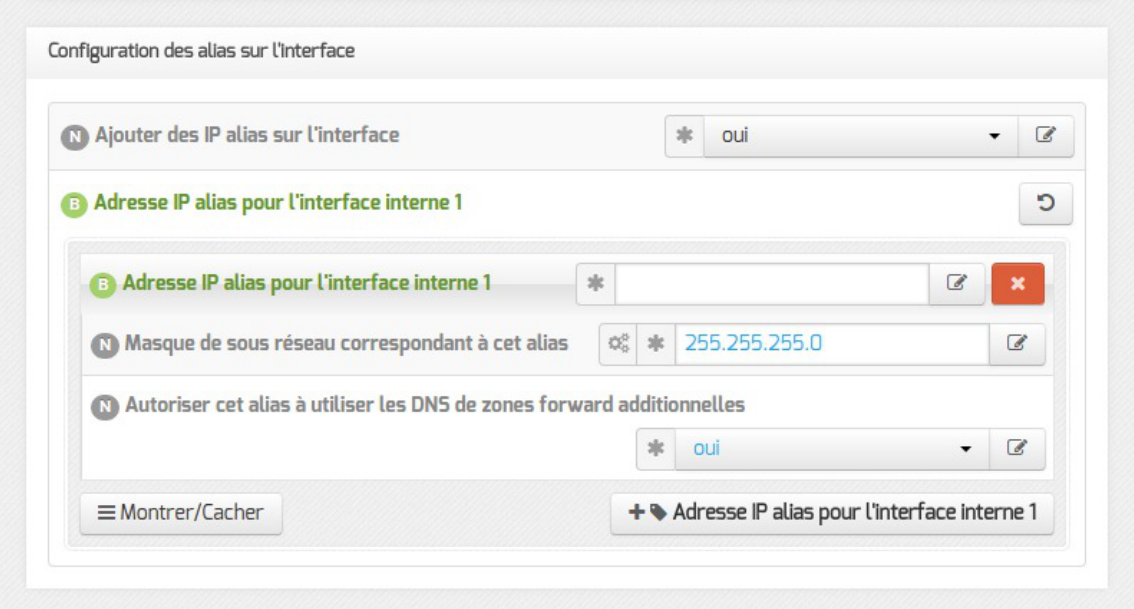
Le masque réseau d'une station isolée est `255.255.255.255`.

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.



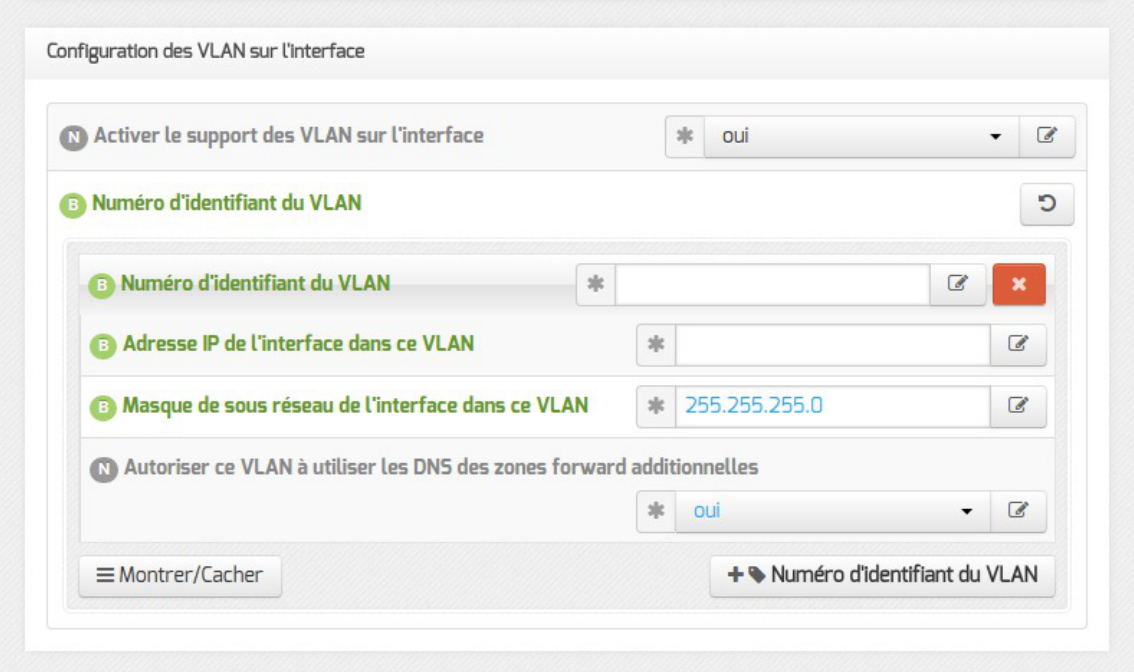
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

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.



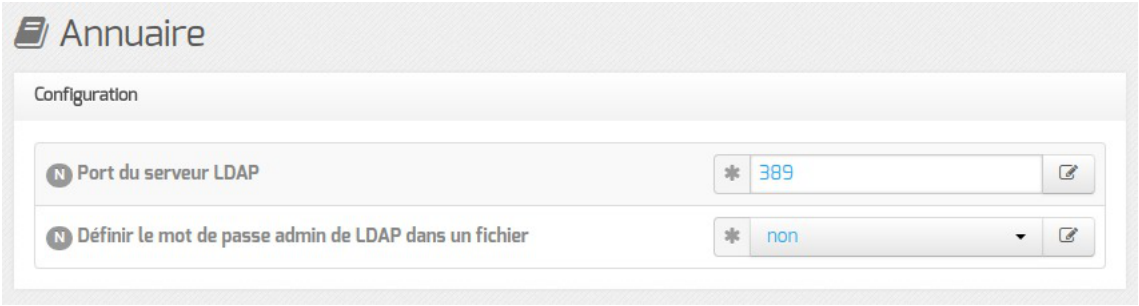
Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`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 Annuaire

Sur le module Zéphir l'annuaire est par défaut configuré comme étant local. Il est possible d'utiliser un annuaire distant en se rendant dans l'onglet `Services` et en passant la variable `Emplacement du serveur LDAP` à `distant`.

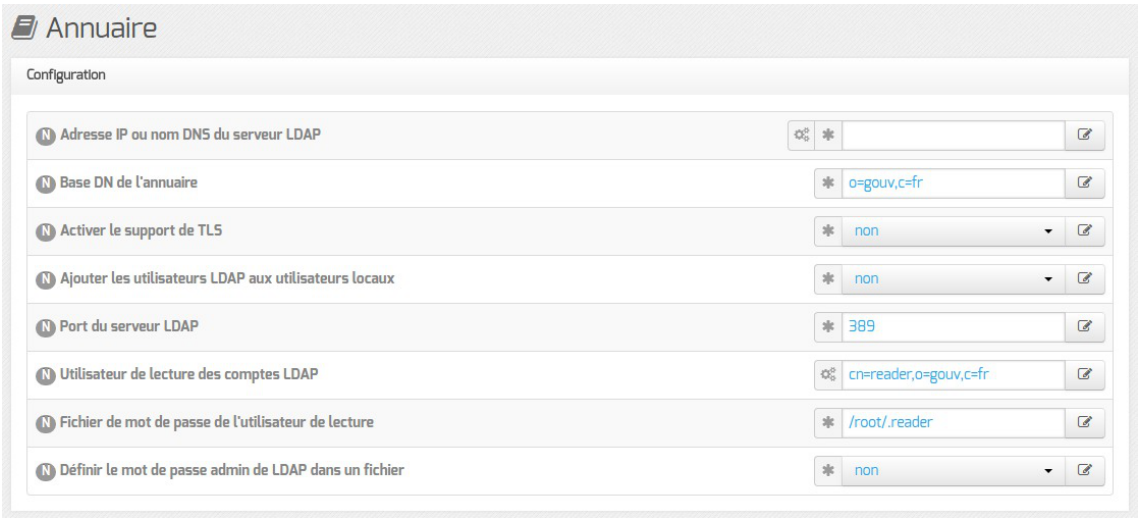
Annuaire LDAP local



Lorsque l'annuaire est configuré comme étant local, l'onglet propose 5 paramètres :

- `Base DN de l'annuaire` : définit le chemin de base pour la recherche dans l'annuaire LDAP
- `Activer le support de TLS` : permet de gérer le chiffrement TLS[p.236] des échanges ;
- `Port du serveur LDAP` : permet de changer le port d'écoute du serveur LDAP ;
- `Définir le mot de passe admin de LDAP dans un fichier` : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire dans le fichier `/root/.writer` ;
- `Administrateur principal de l'application (login LDAP)` : compte LDAP de l'administrateur du serveur Zéphir. Cet utilisateur privilégié permet l'attribuer des droits aux autres utilisateurs.

Annuaire LDAP distant



Lorsque l'annuaire est configuré comme étant distant, l'onglet propose 8 paramètres :

- `Adresse IP ou nom DNS du serveur LDAP` : adresse du serveur LDAP distant ;
- `Base DN de l'annuaire` : définit le chemin de base pour la recherche dans l'annuaire LDAP
- `Activer le support de TLS` : permet de gérer le chiffrement TLS[p.236] des échanges ;
- `Port du serveur LDAP` : permet de changer le port d'écoute du serveur LDAP ;
- `Utilisateur de lecture des comptes LDAP` : définit l'utilisateur ayant les droits de lecture, `cn=reader,o=gouv,c=fr` par défaut ;
- `Fichier de mot de passe de l'utilisateur de lecture` : le mot de passe de l'utilisateur qui a les droits de lecture sur l'annuaire distant doit être placé dans le fichier indiqué dans ce champ, /root/.reader par défaut ;
- `Définir le mot de passe admin de LDAP dans un fichier` : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire distant dans le fichier /root/.writer ;
- `Administrateur principal de l'application (login LDAP)` : compte LDAP de l'administrateur du serveur Zéphir. Cet utilisateur privilégié permet l'attribuer des droits aux autres utilisateurs.

2.5. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.233]. 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.

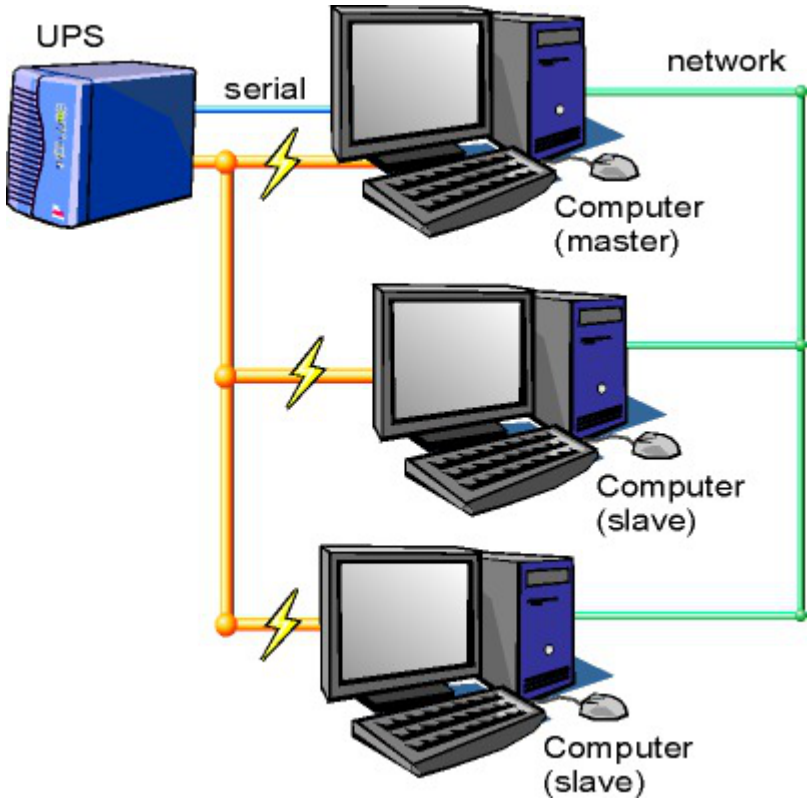


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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`

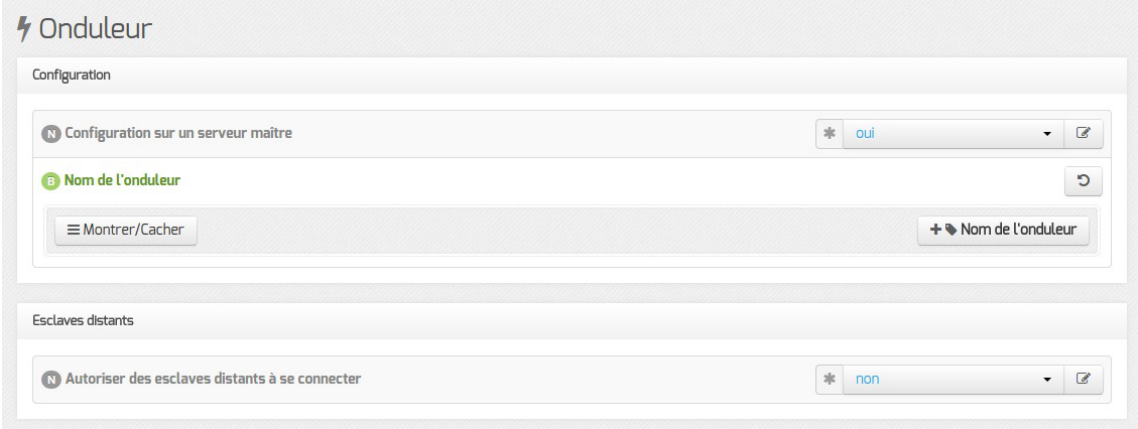
Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

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 :

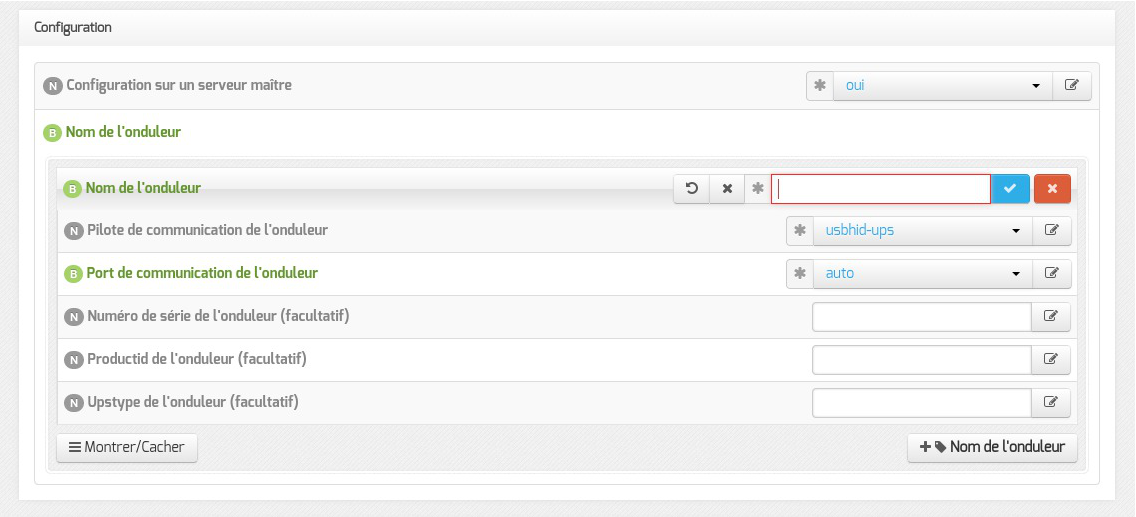
http://www.networkupstools.org/source/2.7/new-2.7.3.txt

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 :

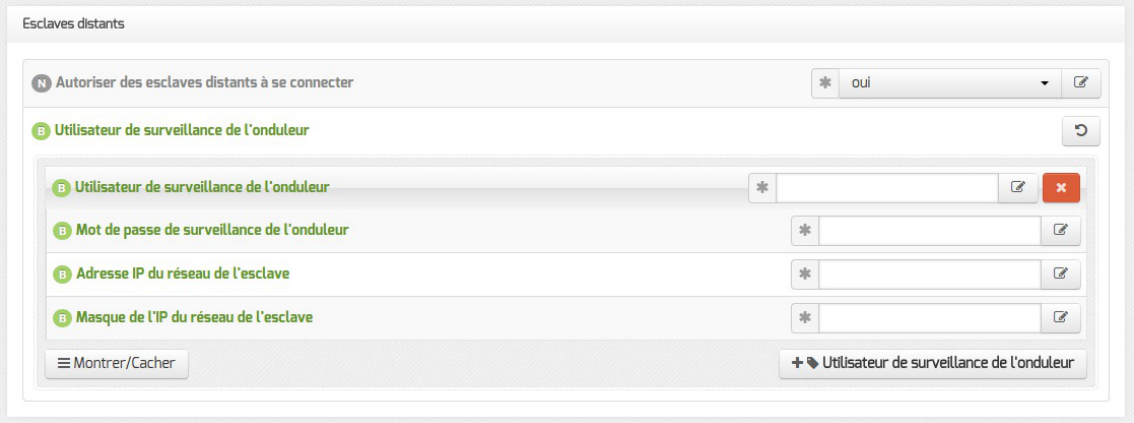
- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

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`.

2.6. Onglet Eole sso : Configuration du service SSO pour l'authentification unique

Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

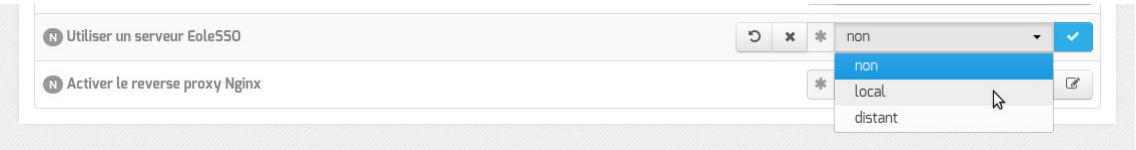
Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier

de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.

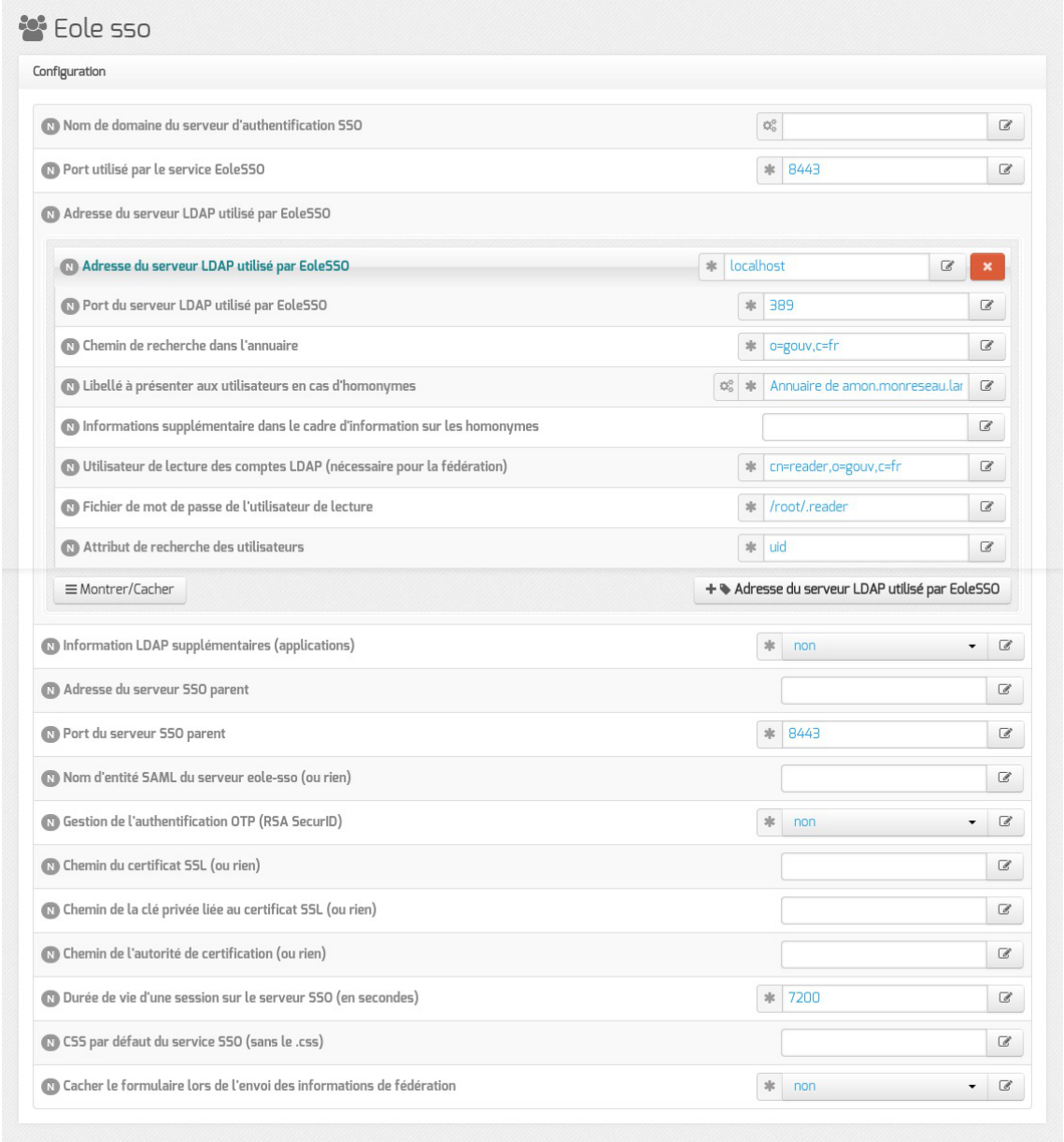


La variable `Utiliser un serveur EoleSSO` permet :

- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

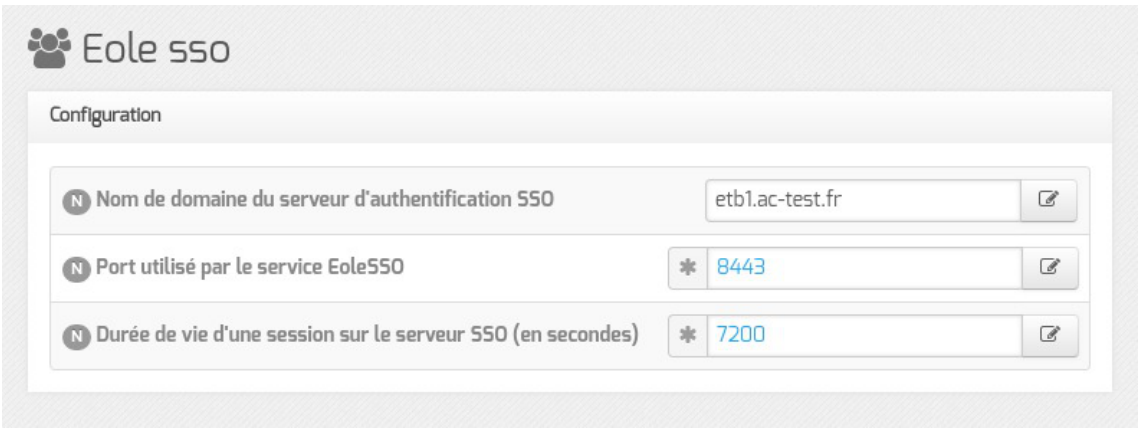
Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



Configuration d'un serveur EoleSSO distant

Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Par défaut le serveur communique sur le port `8443`. Il est conseillé de laisser cette valeur par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le changer également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP pour authentifier les utilisateurs et récupérer leurs attributs.

Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.233] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : `cn=reader,o=gouv,c=fr`
- fichier de mot de passe : `/root/.reader`

Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire

- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

Passer la variable `Information LDAP supplémentaires (applications)` à `oui` permet de configurer pour chaque annuaire LDAP déclaré des attributs supplémentaires qui seront utilisés par les applications web (DN racine de l'arbre utilisateurs, DN racine de l'arbre groupes, Champ 'nom d'affichage' de l'utilisateur, Champ 'mail' de l'utilisateur, Champ 'fonction' de l'utilisateur, Champ 'categorie' de l'utilisateur, Champ 'rne' de l'utilisateur, Champ 'fredurne' de l'utilisateur…).

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré comme serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.237] en HTTPS, sur le port défini pour le serveur EoleSSO).

Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).

Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.235] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est '`configurables`', et indique que les utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier `/usr/share/sso/securid_users/securid_users.ini`).
- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères

uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.232] du serveur et sont utilisés par défaut.

Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.235] (version 2).

`Nom d'entité SAML du serveur eole-sso (ou rien)` : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Autres options

`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet*.

Voir aussi...

> Gestion des sources d'authentification multiples

2.7. 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

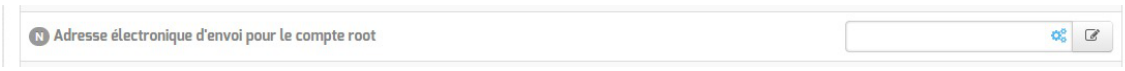
Les paramètres communs à renseigner sont les suivants :

- `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.

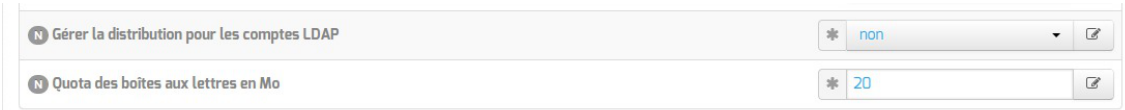
Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.



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.

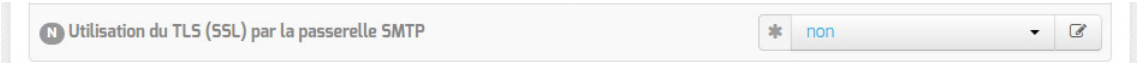
Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

Relai des messages

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

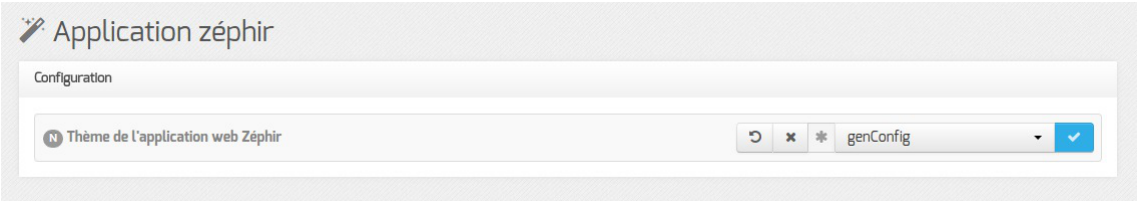
Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.

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.236] pour l'envoi de message. Si la passerelle SMTP[p.235] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.235] (port 25) ou non (port 465).

2.8. Onglet Application zéphir



Le thème de l'application web Zéphir est paramétrable, le thème par défaut est `genConfig`.

Il est possible de créer son propre thème à partir d'un thème existant présent dans `/usr/share/zephir/web/themes/` :

- choisir depuis l'interface de configuration du module un thème à partir duquel partir ;
- reconfigurer le serveur à l'aide de la commande `reconfigure` ;
- éditer le fichier `/usr/share/zephir/web/css/style.css` ;

- placer les images dans `/usr/share/zephir/web/images/` ;
- placer les fonts dans `/usr/share/zephir/web/fonts/` ;
- créer un répertoire pour le nouveau thème :
  `# mkdir /usr/share/zephir/web/themes/monTheme`
- copier le tout dans `/usr/share/zephir/web/themes/monTheme` :
  `# cp -Rp /usr/share/zephir/web/css /usr/share/zephir/web/themes/monTheme/`
  `# cp -Rp /usr/share/zephir/web/fonts /usr/share/zephir/web/themes/monTheme/`
  `# cp -Rp /usr/share/zephir/web/images /usr/share/zephir/web/themes/monTheme/`
- choisir depuis l'interface de configuration du module le nouveau thème ;
- reconfigurer le serveur à l'aide de la commande `reconfigure`.

Le fichier `colors.ini` n'est plus utilisé pour changer l'apparence de l'application web Zéphir.

3. Configuration en mode expert

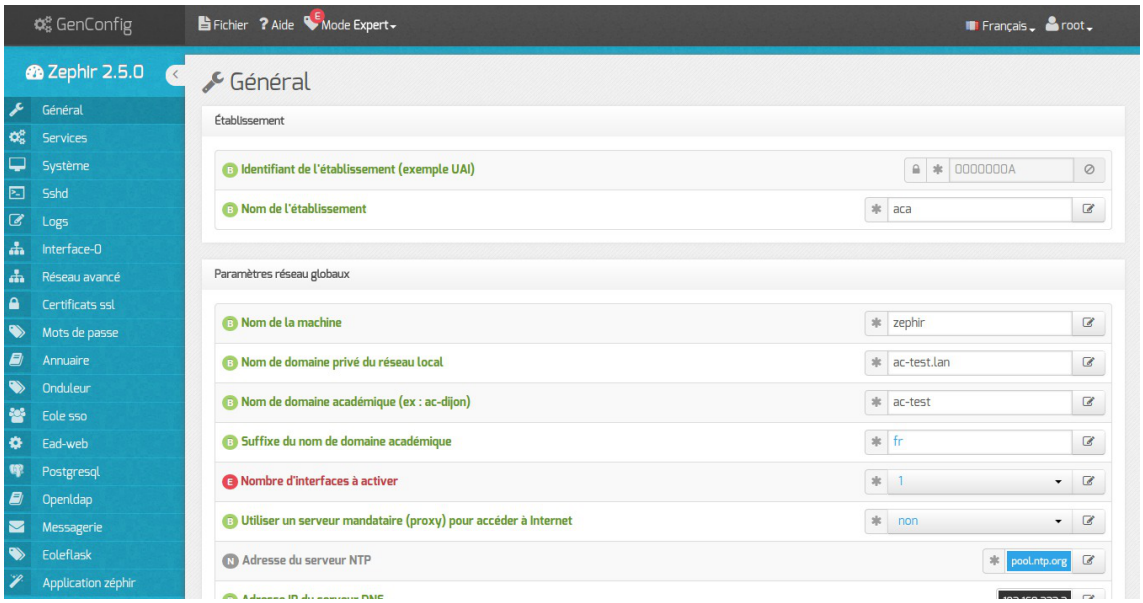
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode expert de l'interface de configuration du module.

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

- `Général` ;
- `Services` ;
- `Système` ;
- `Sshd` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-n` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificat ssl` ;
- `Annuaire` ;
- `Onduleur` * ;
- `Eole sso` * ;
- `Ead-web` ;
- `Postgresql` ;

- Openldap * ;
- Messagerie ;
- Eoleflask ;
- Application zéphir.

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

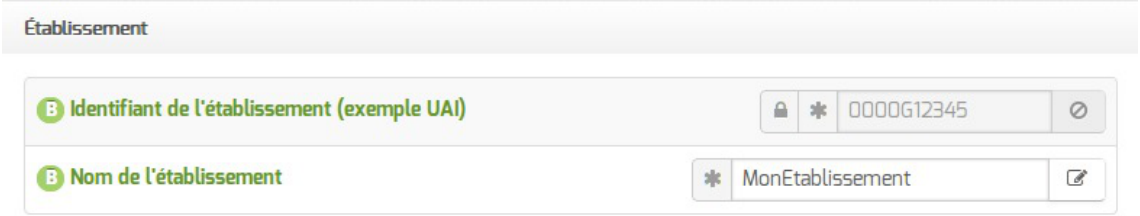
Par défaut, le module Zéphir est livré avec un annuaire LDAP local qui sert à enregistrer des utilisateurs et leur mot de passe.

Il est cependant possible de spécifier un annuaire distant lors de la configuration du module (par exemple : l'annuaire d'un module Horus, l'annuaire d'un module Scribe, ou encore un annuaire académique). Vous pourrez alors vous connecter avec un compte de l'annuaire utilisé.

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.232] 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`.

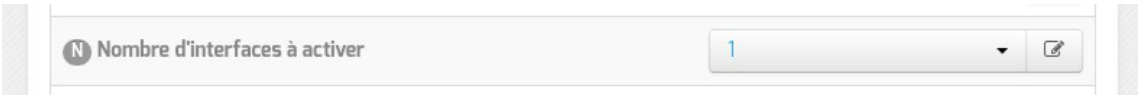
C'est ce nom qui configurera le serveur DNS (sur un module Amon par exemple) comme zone de résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

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.

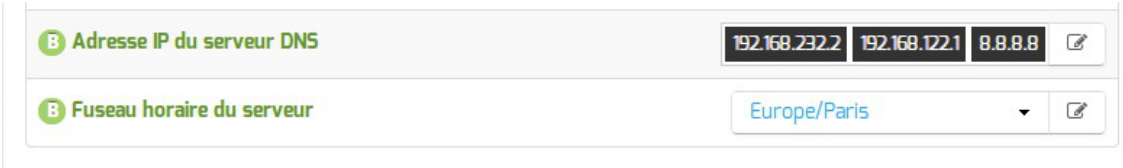
Proxy

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.

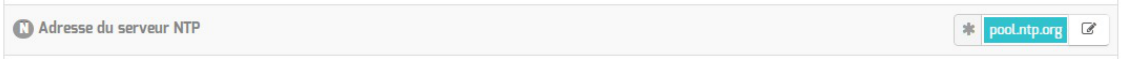
DNS et fuseau horaire



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.231].

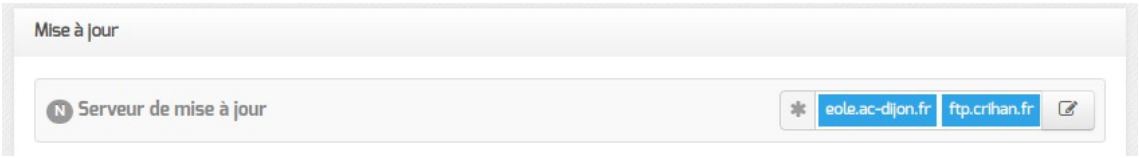
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.233]. 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...

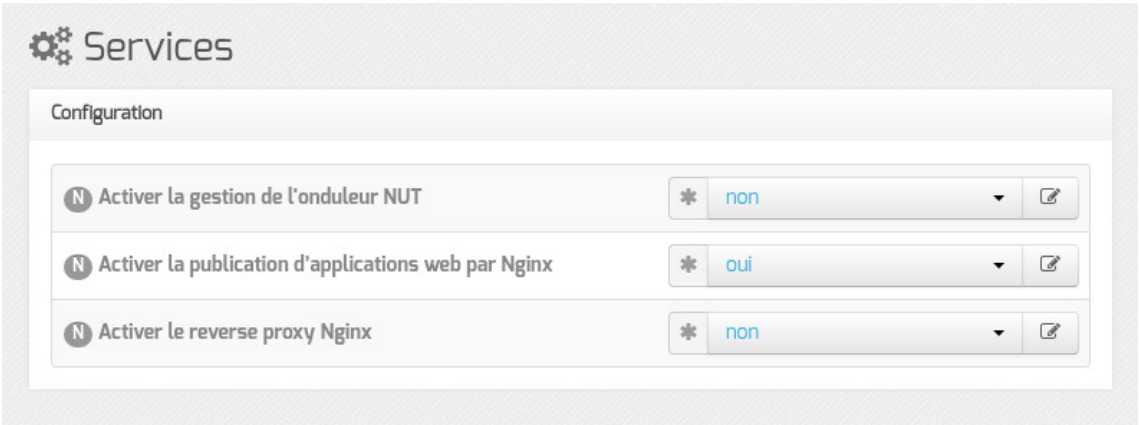
> Les différents types de mises à jour

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.



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.233].

En mode normal l'onglet `Services` contient un peu plus de services activables ou désactivables.

Vue de l'onglet Services en mode normal

Les services disponibles propres au module Zéphir en mode normal sont les suivants :

- le serveur LDAP ;
- le service d'authentification unique EoleSSO.

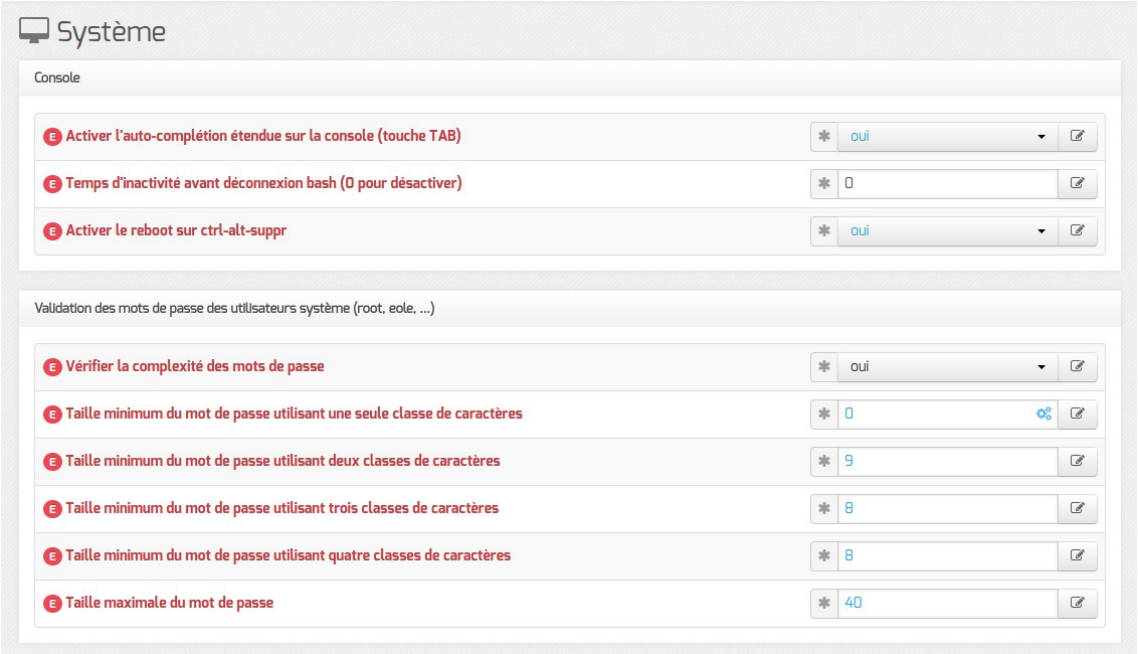
Il est possible de positionner ces 2 services à `local` ou `distant`.

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

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

Le seul service propre au module Zéphir est l'application web Zéphir, il est activé par défaut.

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 :

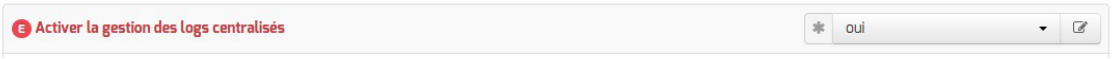
```
Permission denied (publickey).
```

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

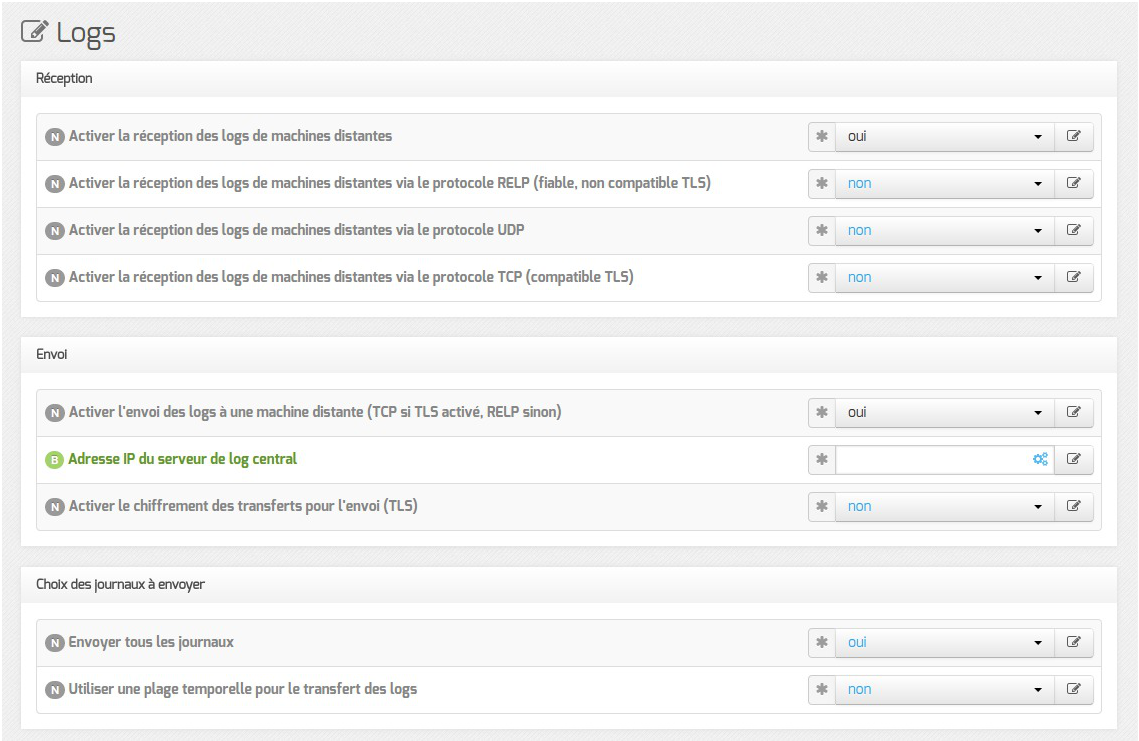
3.5. Onglet Logs : Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.237]. 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.



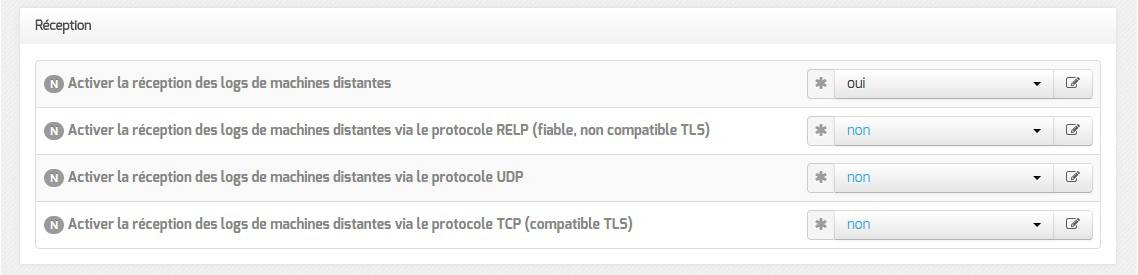
Vue de l'onglet Logs

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.235] ou RELP[p.234]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.236]) ;
- 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.230].

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.230].

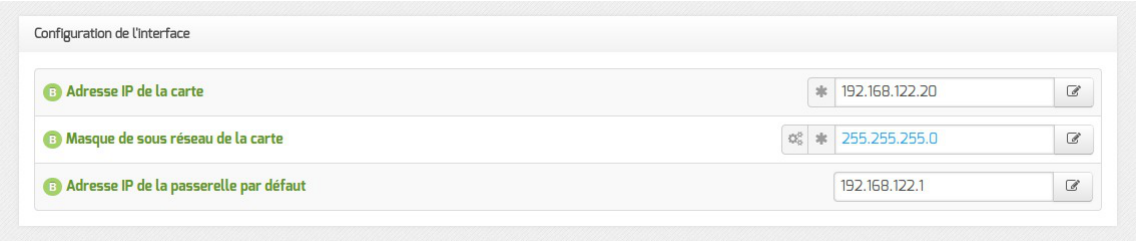
Choix des journaux à envoyer

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`.

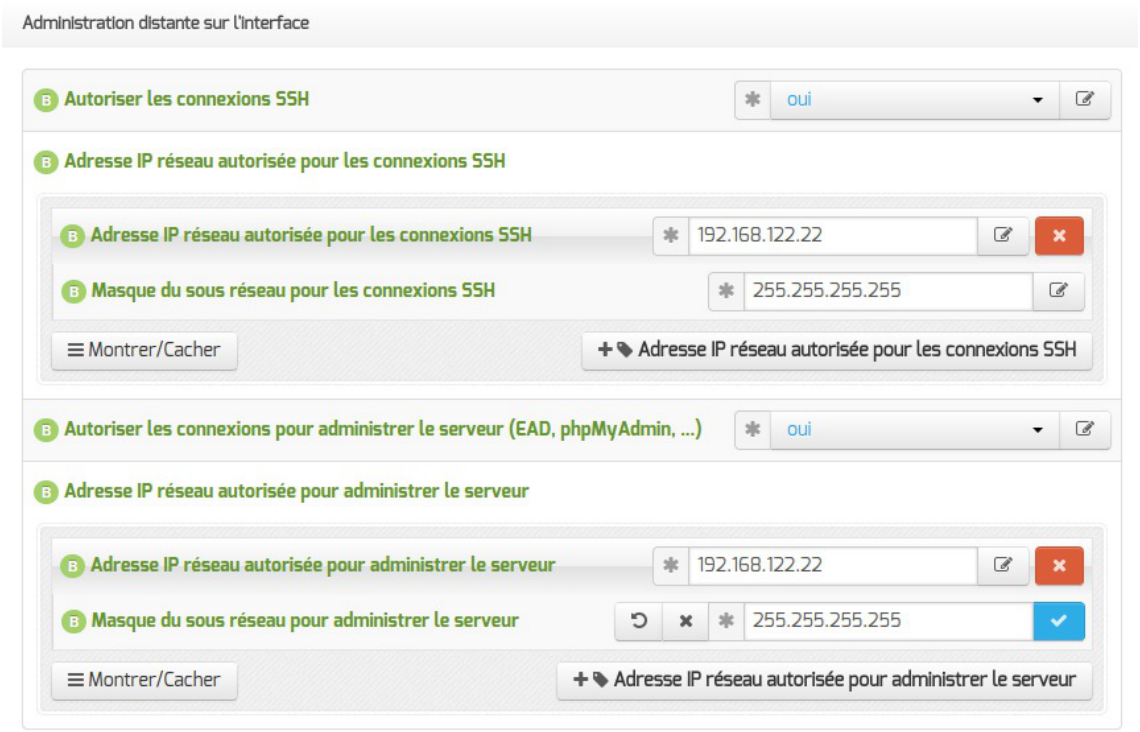
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

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

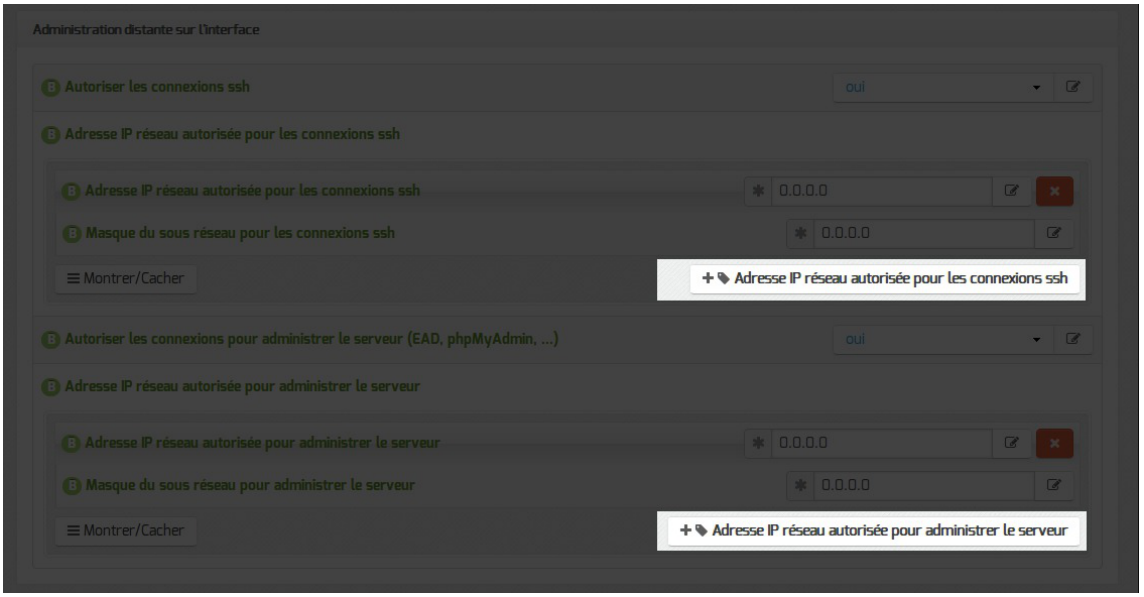


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.235] 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`.

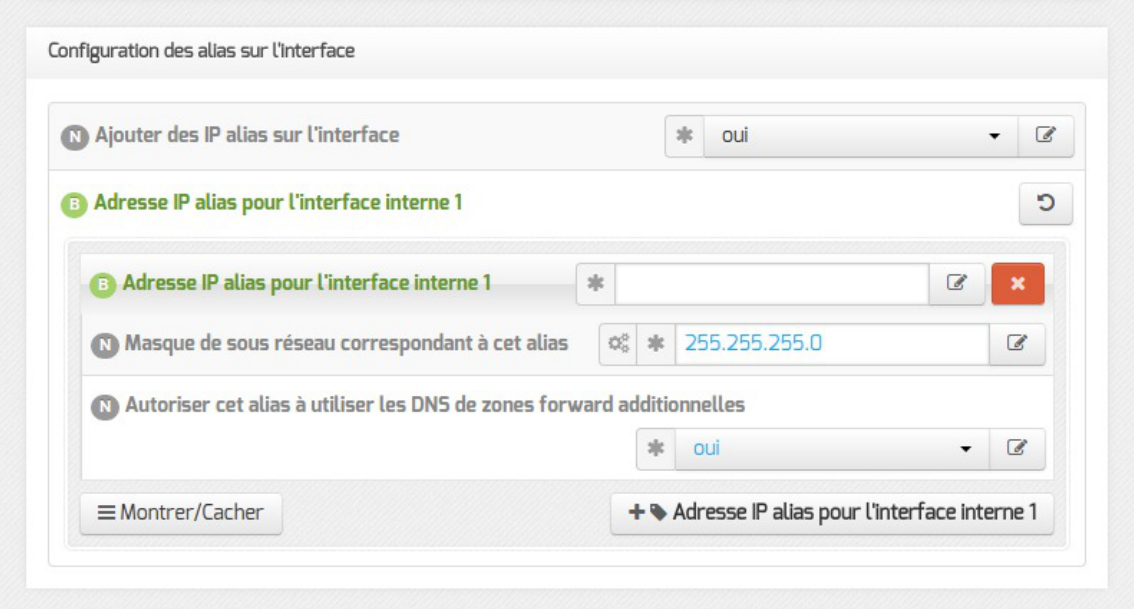
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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.



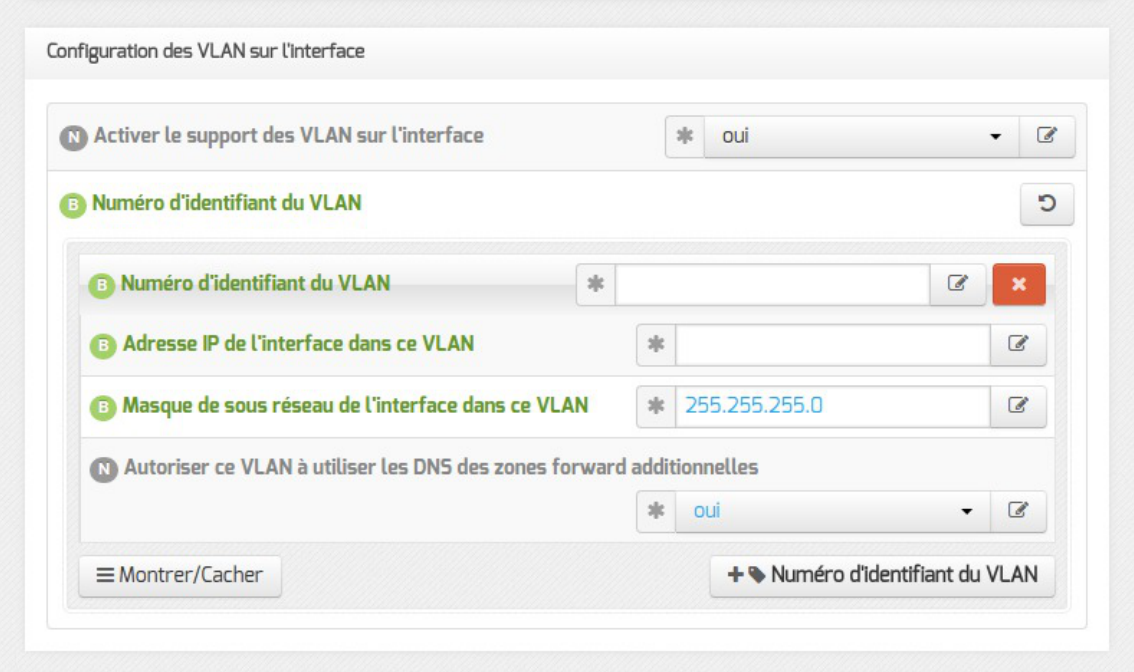
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

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-n

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

Le nombre d'interfaces activées se définit en mode expert dans l'onglet `Général` de l'interface de configuration du module.

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.

Configuration de l'interface

Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau.

Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

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`.

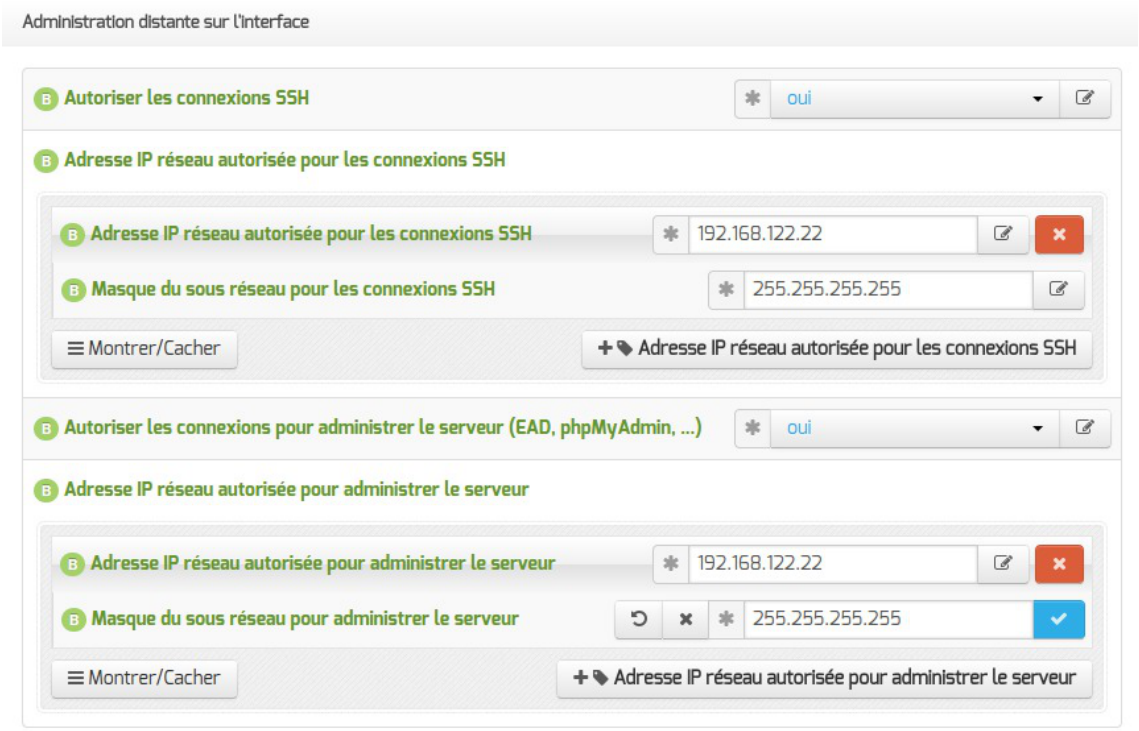
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

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

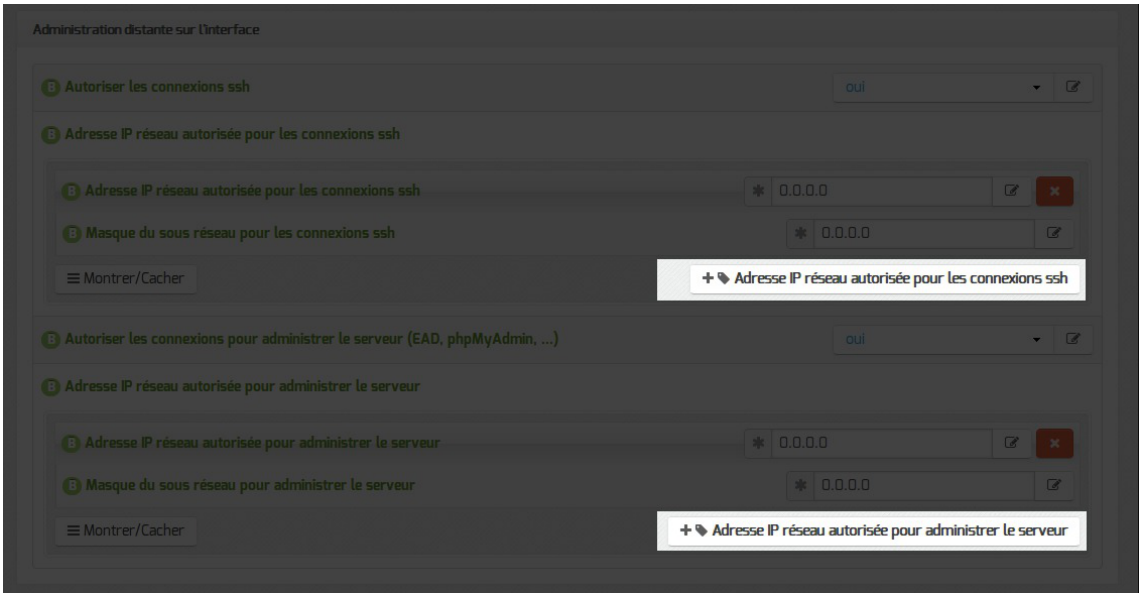


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.235] 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

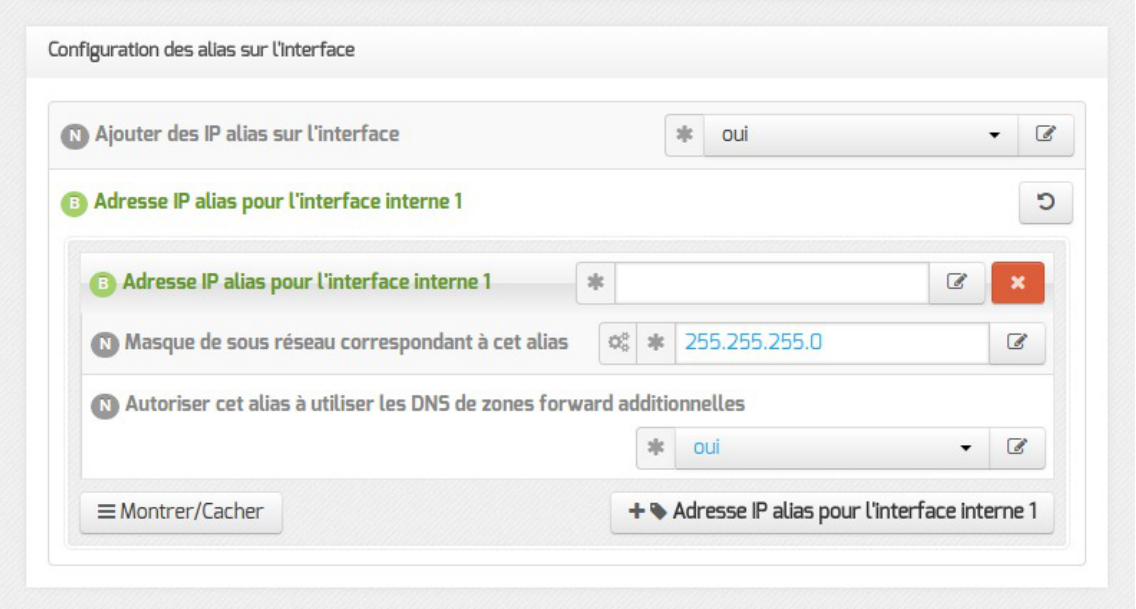
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

> 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.



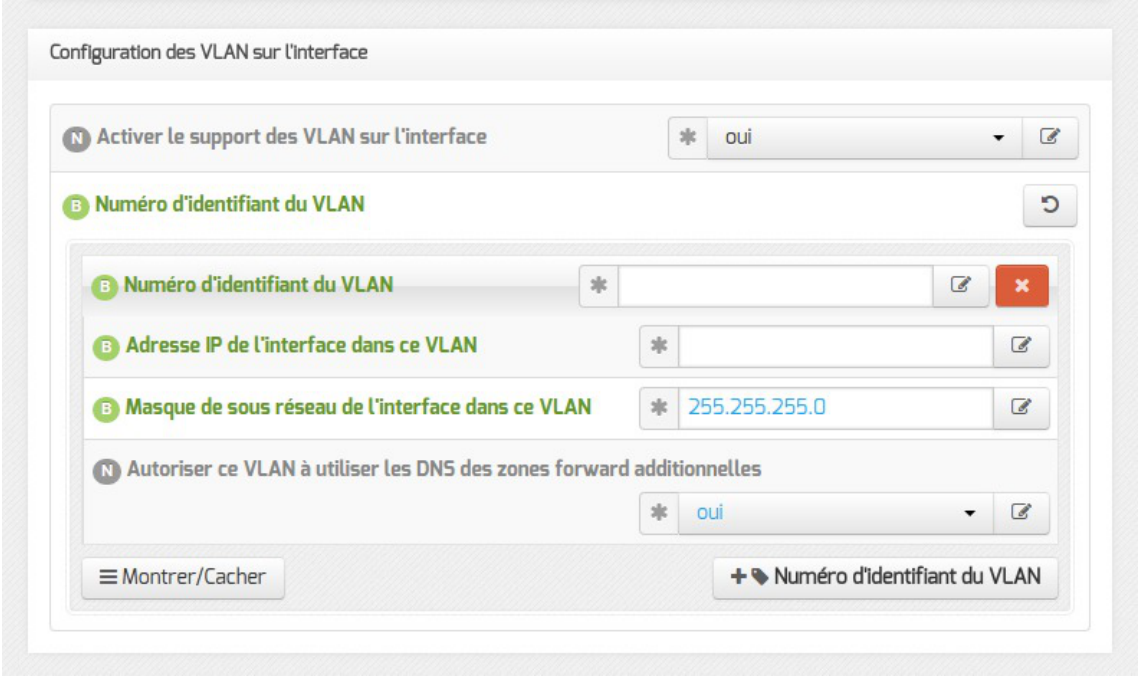
Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

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.



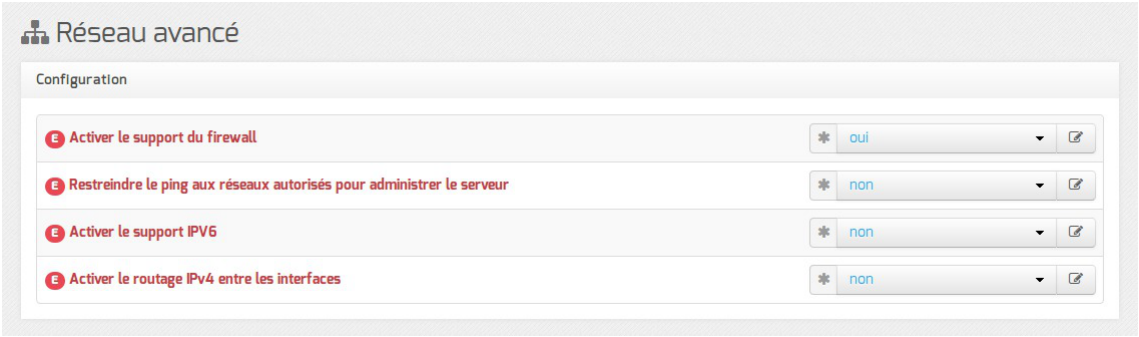
Pour cela, il faut activer son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

`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`.

3.8. Onglet Réseau avancé

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

Configuration IP



Le support du pare-feu peut être désactivé en passant `Activer le support du firewall` à `non`.

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).

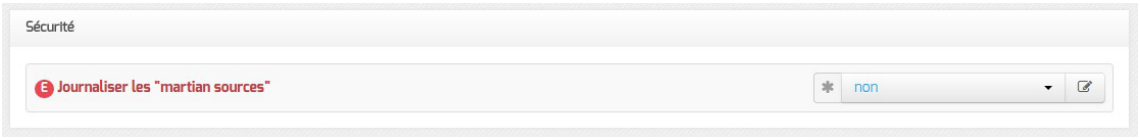
Le support de l'IPv6[p.232] peut être activé en passant la variable `Activer le support IPv6` à `oui` mais sa prise en charge ne se sera faite qu'au niveau du noyau.

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`)

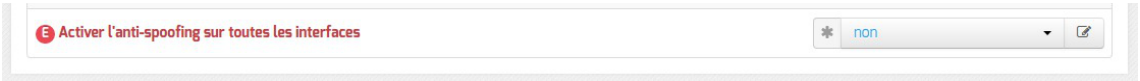
L'activation du support IPv6 entraîne l'apparition de la variable : `Activer le routage IPv6 entre les interfaces`.

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



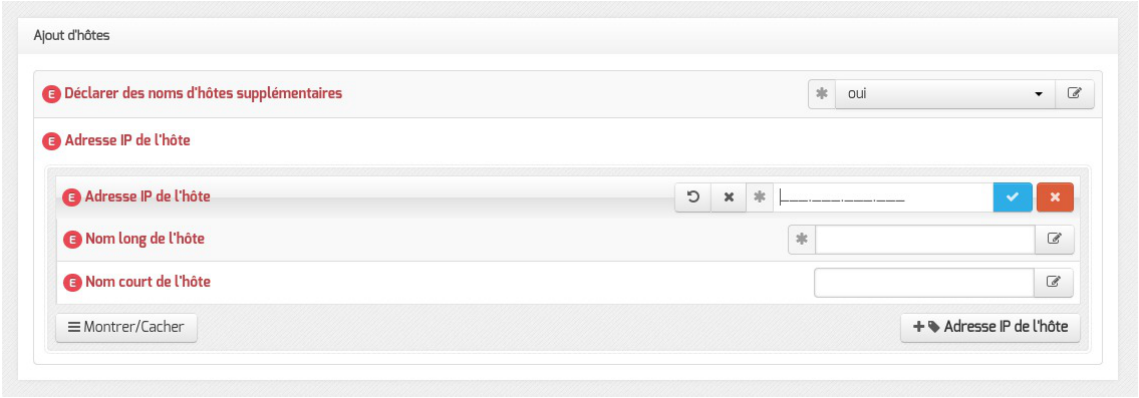
Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.230] 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`.

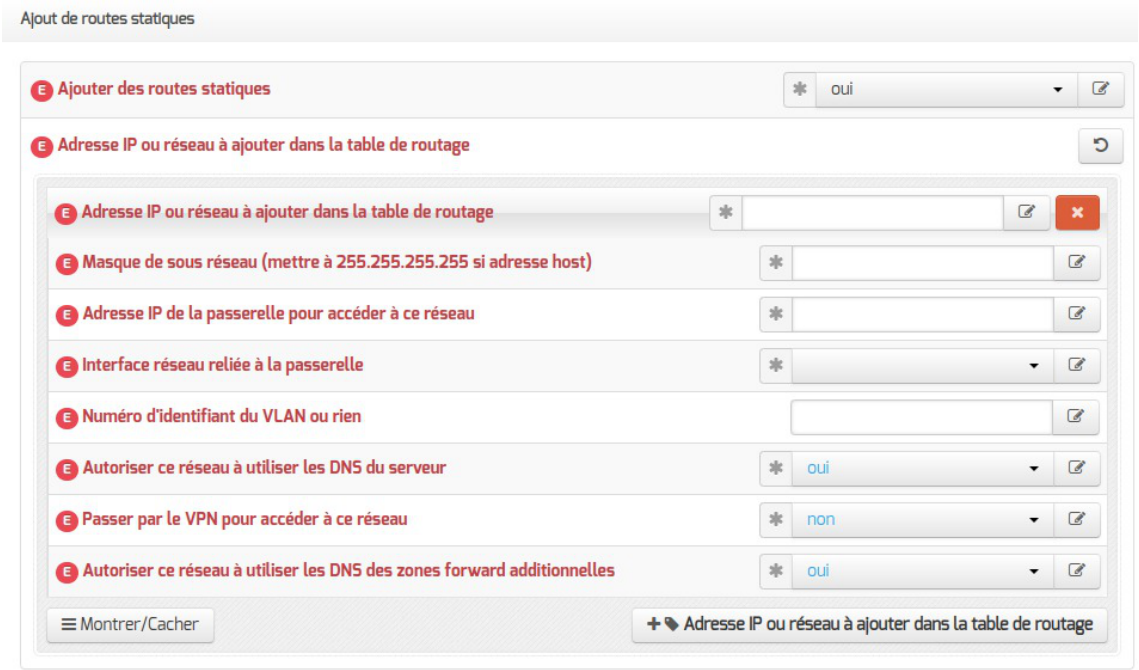
Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte`.

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.230] 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.233] (/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.232] 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.233] pour l'interface externe.

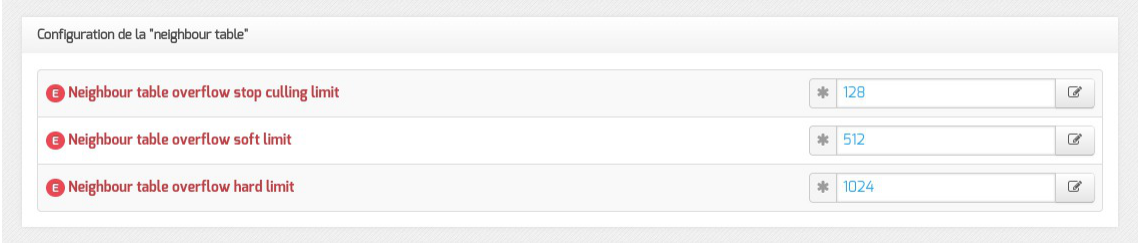
Si le champ n'est pas renseigné, la valeur par défaut est utilisée (1500 octets pour un réseau de type Ethernet).

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.

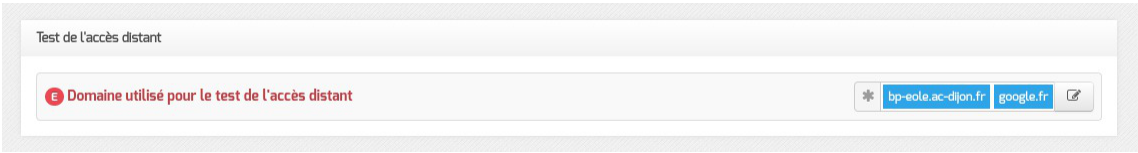
Configuration de la "neighbour table"



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

3.9. 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/`

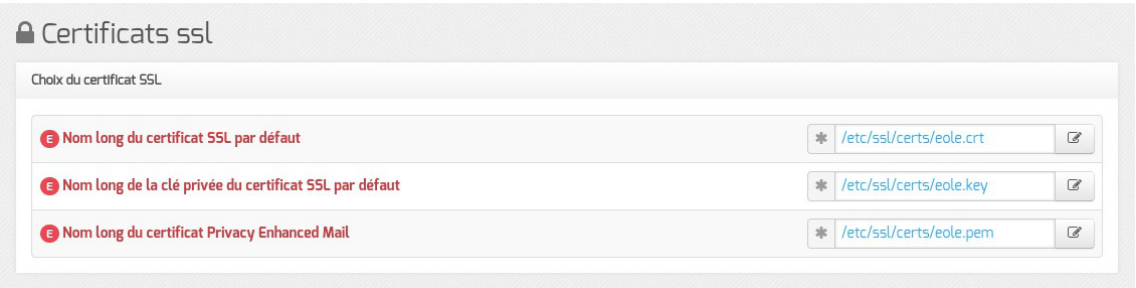
Détermination du nom de serveur (commonName) dans le certificat

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.

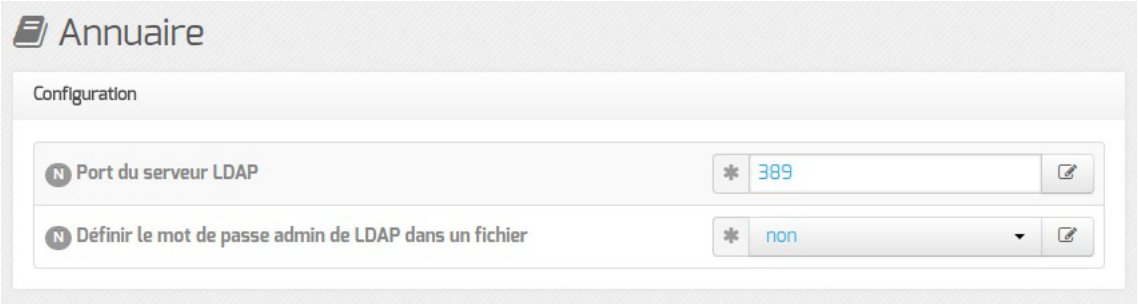
Certificats intermédiaires

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

3.10. Onglet Annuaire

Sur le module Zéphir l'annuaire est par défaut configuré comme étant local. Il est possible d'utiliser un annuaire distant en se rendant dans l'onglet Services et en passant la variable Emplacement du serveur LDAP à distant.

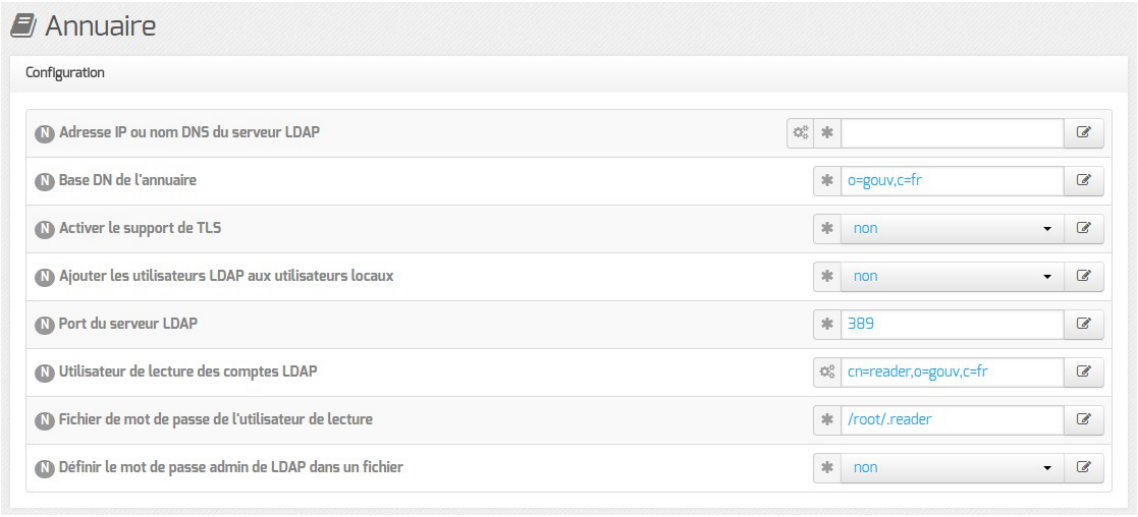
Annuaire LDAP local



Lorsque l'annuaire est configuré comme étant local, l'onglet propose 5 paramètres :

- Base DN de l'annuaire : définit le chemin de base pour la recherche dans l'annuaire LDAP
- Activer le support de TLS : permet de gérer le chiffrement TLS[p.236] des échanges ;
- Port du serveur LDAP : permet de changer le port d'écoute du serveur LDAP ;
- Définir le mot de passe admin de LDAP dans un fichier : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire dans le fichier /root/.writer ;
- Administrateur principal de l'application (login LDAP) : compte LDAP de l'administrateur du serveur Zéphir. Cet utilisateur privilégié permet l'attribuer des droits aux autres utilisateurs.

Annuaire LDAP distant



Lorsque l'annuaire est configuré comme étant distant, l'onglet propose 8 paramètres :

- Adresse IP ou nom DNS du serveur LDAP : adresse du serveur LDAP distant ;

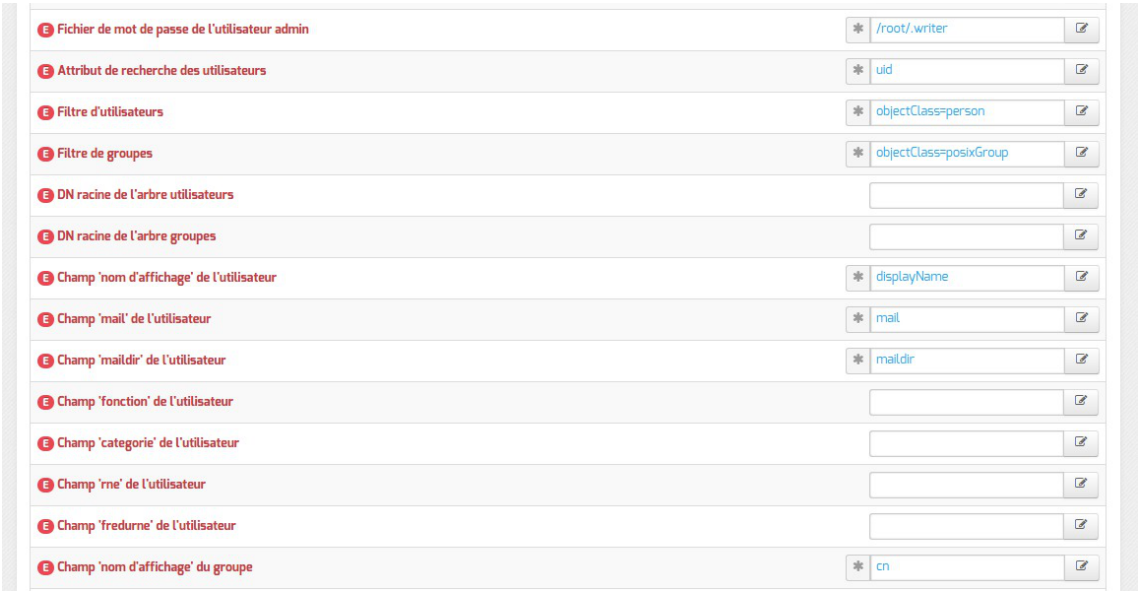
- `Base DN de l'annuaire` : définit le chemin de base pour la recherche dans l'annuaire LDAP
- `Activer le support de TLS` : permet de gérer le chiffrement TLS[p.236] des échanges ;
- `Port du serveur LDAP` : permet de changer le port d'écoute du serveur LDAP ;
- `Utilisateur de lecture des comptes LDAP` : définit l'utilisateur ayant les droits de lecture, `cn=reader,o=gouv,c=fr` par défaut ;
- `Fichier de mot de passe de l'utilisateur de lecture` : le mot de passe de l'utilisateur qui a les droits de lecture sur l'annuaire distant doit être placé dans le fichier indiqué dans ce champ, `/root/.reader` par défaut ;
- `Définir le mot de passe admin de LDAP dans un fichier` : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire distant dans le fichier `/root/.writer` ;
- `Administrateur principal de l'application (login LDAP)` : compte LDAP de l'administrateur du serveur Zéphir. Cet utilisateur privilégié permet l'attribuer des droits aux autres utilisateurs.

Mode expert

Le paramétrage du serveur LDAP local se fait dans l'onglet Openldap.

Mode expert

Les variables du mode expert pour l'annuaire sont identiques qu'il soit distant ou local, elles permettent de modifier finement le comportement de l'annuaire.



La variable `Fichier de mot de passe de l'utilisateur admin` permet de modifier le fichier par défaut contenant le mot de passe de l'administrateur de l'annuaire.

L'attribut de recherche par défaut peut également être modifié.

Les filtres, les DN racine et les attributs LDAP renvoyés par l'annuaire peuvent être personnalisés.

Le paramétrage d'un serveur LDAP local se fait dans l'onglet `Openldap`.

Voir aussi...

Onglet Openldap : Configuration du serveur LDAP local [p.85]

3.11. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.233]. 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.

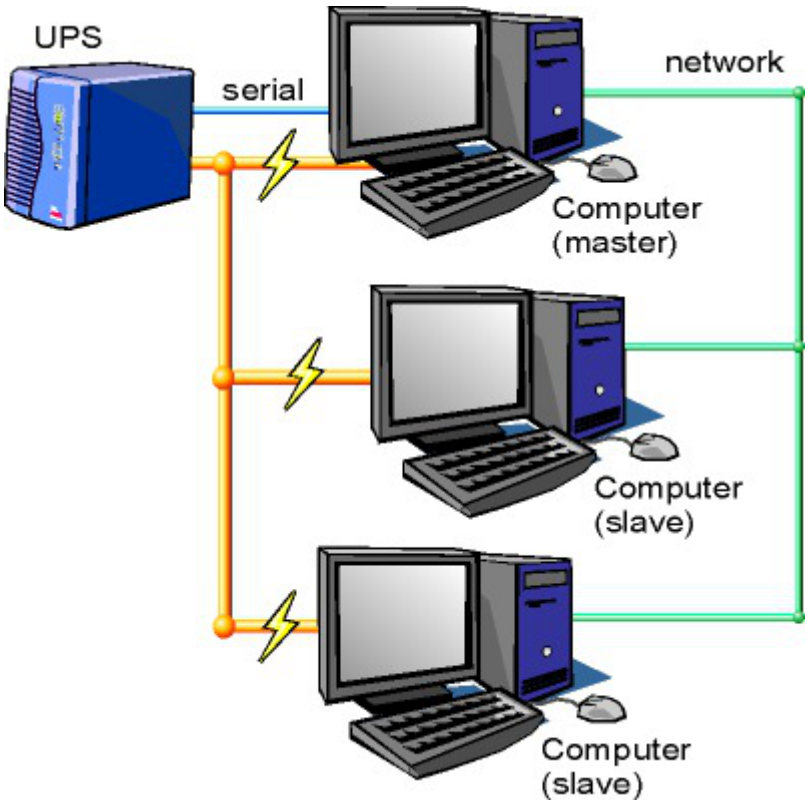


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

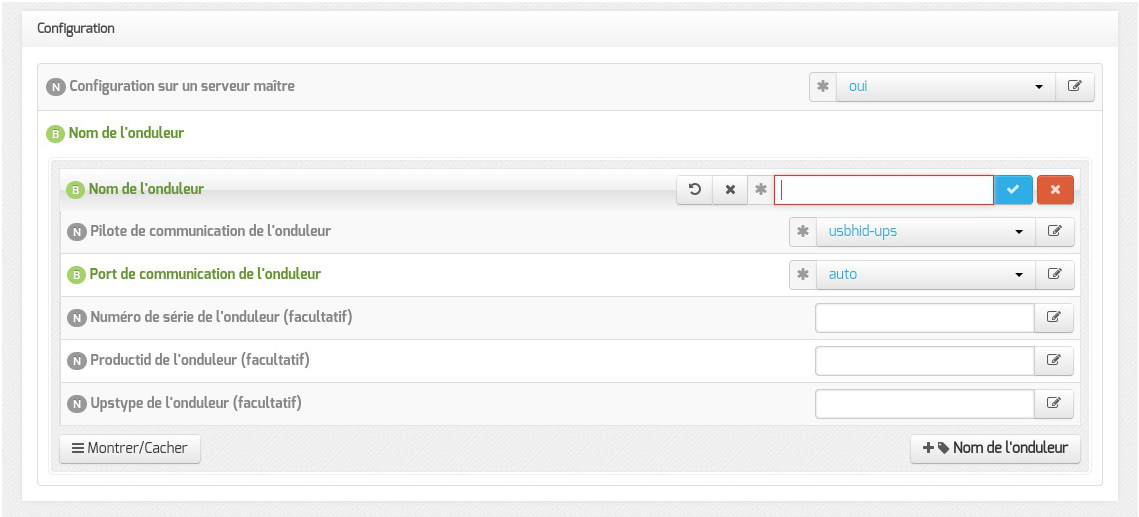
```
# apt-cache policy nut
```

> 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 :

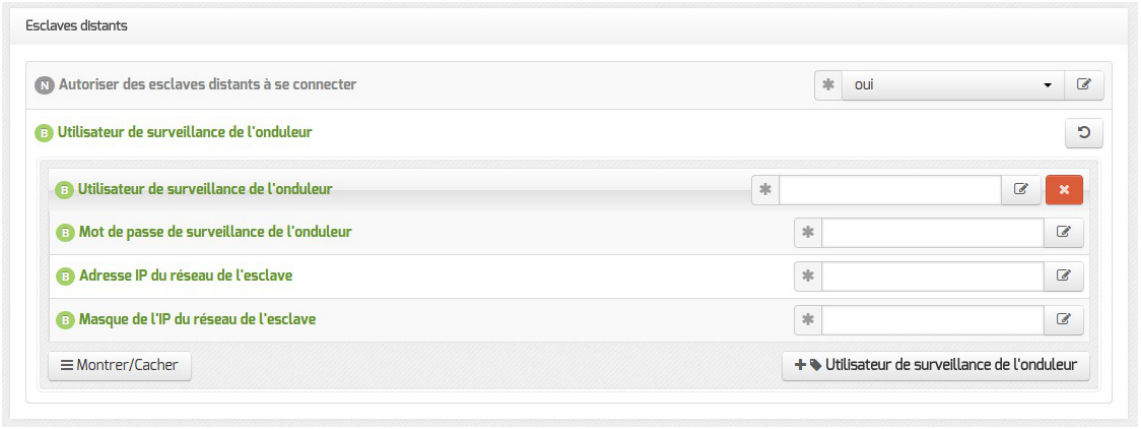
- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

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`.

3.12. Onglet Eole sso : Configuration du service SSO pour l'authentification unique

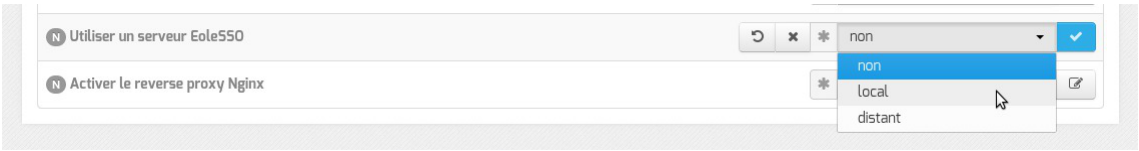
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.

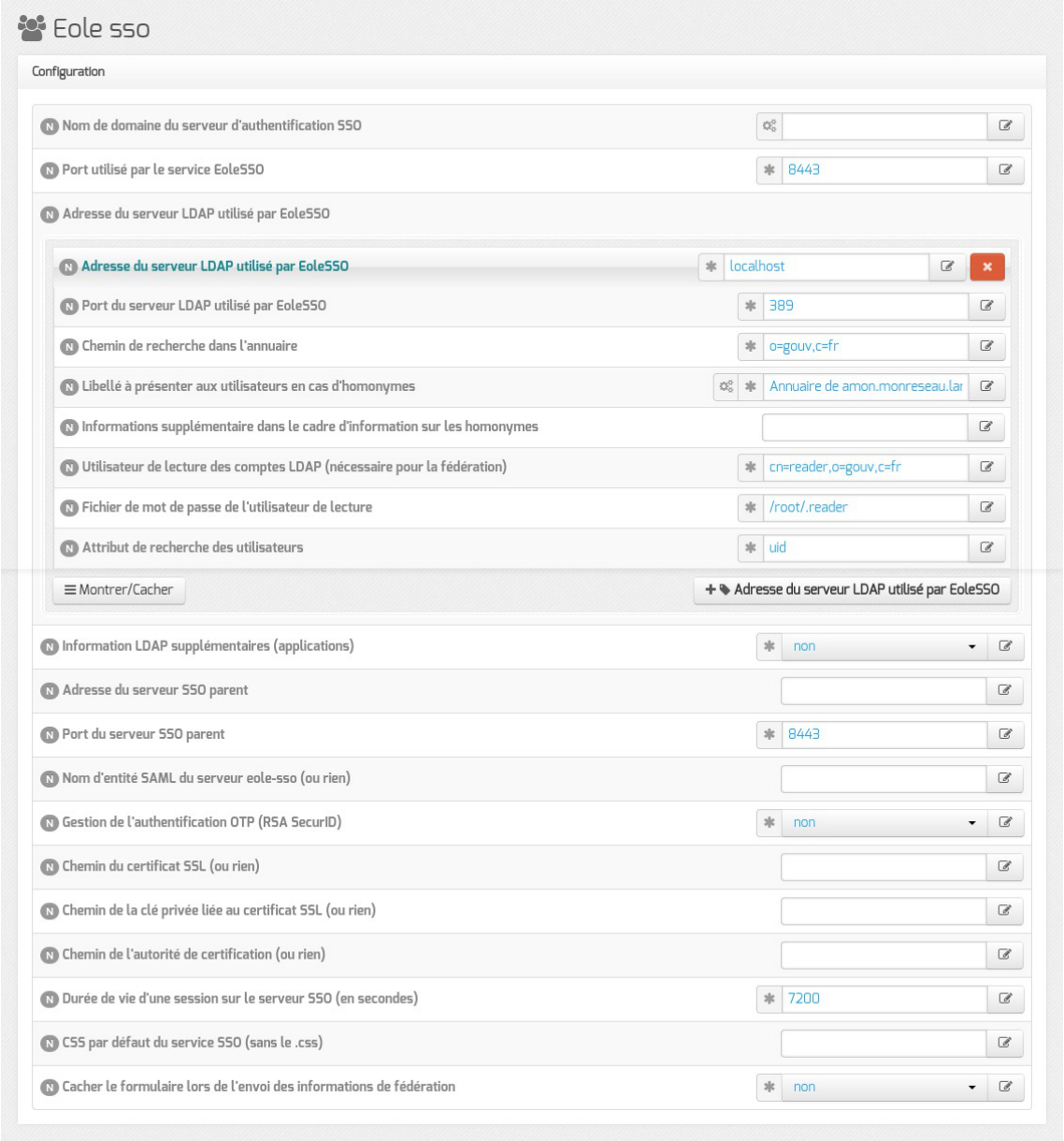


La variable `Utiliser un serveur EoleSSO` permet :

- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

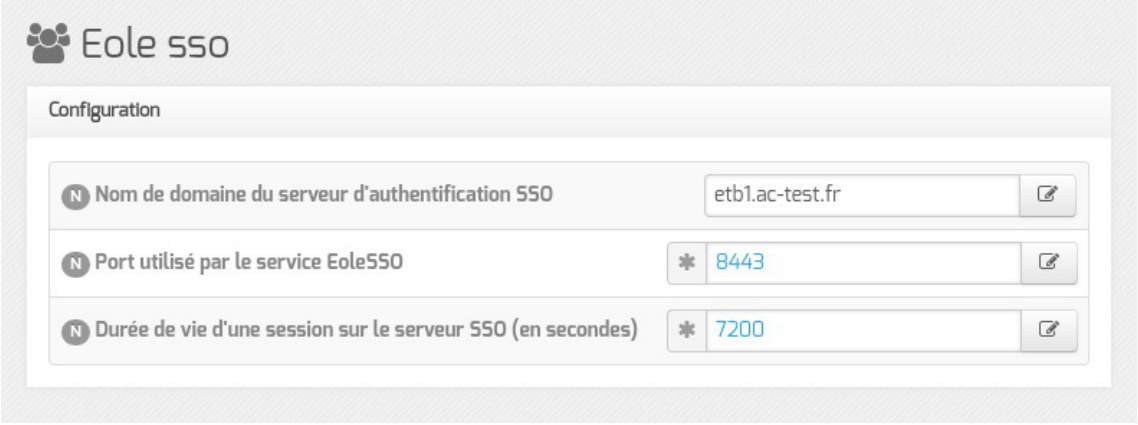
Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



Configuration d'un serveur EoleSSO distant

Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Par défaut le serveur communique sur le port `8443`. Il est conseillé de laisser cette valeur par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le changer également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP pour authentifier les utilisateurs et récupérer leurs attributs.

Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre Gestion des sources d'authentifications multiples) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.233] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : `cn=reader,o=gouv,c=fr`
- fichier de mot de passe : `/root/.reader`

Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire

- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

Passer la variable `Information LDAP supplémentaires (applications)` à `oui` permet de configurer pour chaque annuaire LDAP déclaré des attributs supplémentaires qui seront utilisés par les applications web (DN racine de l'arbre utilisateurs, DN racine de l'arbre groupes, Champ 'nom d'affichage' de l'utilisateur, Champ 'mail' de l'utilisateur, Champ 'fonction' de l'utilisateur, Champ 'categorie' de l'utilisateur, Champ 'rne' de l'utilisateur, Champ 'fredurne' de l'utilisateur…).

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré comme serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.237] en HTTPS, sur le port défini pour le serveur EoleSSO).

Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).

Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.235] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est '`configurables`', et indique que les utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier `/usr/share/sso/securid_users/securid_users.ini`).
- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères

uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.232] du serveur et sont utilisés par défaut.

Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.235] (version 2).

`Nom d'entité SAML du serveur eole-sso (ou rien)` : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Autres options

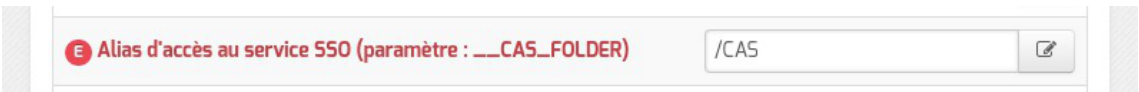
`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

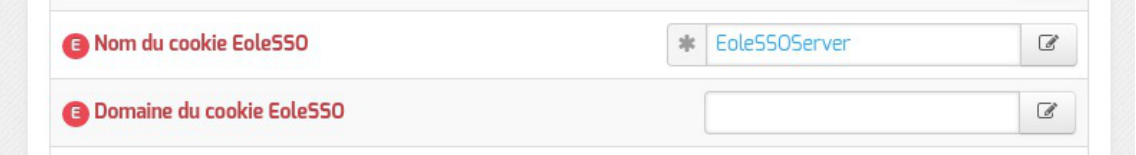
Configuration en mode expert

Options générales

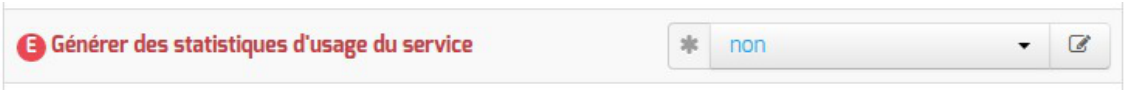
En mode expert plusieurs nouvelles variables sont disponibles :



- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP ou keycloak.



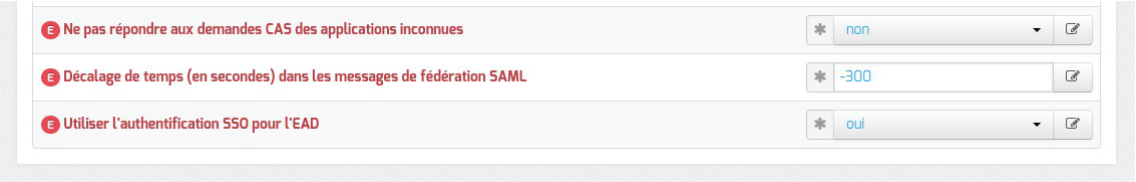
- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.



- `Générer des statistiques d'usage du service` est à `non` par défaut.

  Si ce paramètre est à oui, eole-sso va générer des statistiques sur l'usage du service (consommation mémoire, nombre de session, ...). Ces statistiques sont générées par la librairie python prometheus-client. Elles peuvent être intégrées à un outil tel que Grafana, et sont disponible sur l'URL suivante : https://<adresse_serveur>:8443/metric [https://<adresse_serveur>:8443/metrics] .

- `Activer la balise meta viewport (CSS responsive)` permet d'inclure la balise HTML meta `viewport` dans les pages de l'application (avec content="width=device-width, initial-scale=1"). Elle est à activer en cas d'utilisation d'une feuille de style CSS responsive.



- `Ne pas répondre aux demandes CAS des applications inconnues` est à `non` par défaut

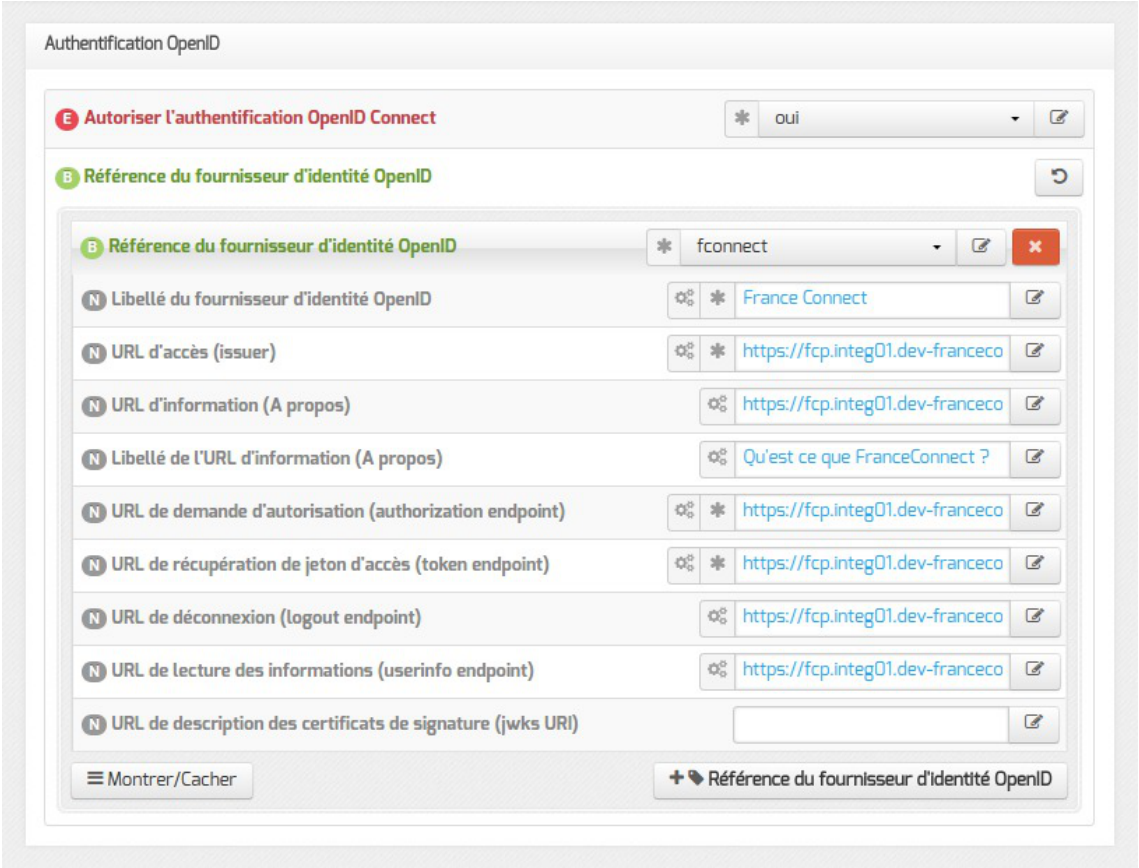
  Si ce paramètre est à `oui`, seules les applications renseignées dans les fichiers d'applications (`/usr/share/sso/app_filters/*_apps.ini`) sont autorisées à recevoir des réponses du serveur en mode CAS. Si il est à non, le filtre par défaut leur sera appliqué ;

- `Décalage de temps (en secondes) dans les messages de fédération SAML` est à `-300` secondes par défaut

  Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;

- `Utiliser l'authentification SSO pour l'EAD` est à `oui` par défaut. Le passer à `non` permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Configuration d'authentification OpenID Connect



- `Autoriser l'authentification OpenID Connect` est à `non` par défaut

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;
  - `/usr/share/sso/interface/images/logo-<libelle>.png` : logo du fournisseur qui sera affiché sur la page d'association de comptes.
- `Libellé du fournisseur d'identité OpenID` : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- `URL d'accès (issuer)` : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- `URL de demande d'autorisation (authorization endpoint)` : URL permettant au client d'initier le processus d'authentification ;
- `URL de récupération de jeton d'accès (token endpoint)` : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- `URL de déconnexion (logout endpoint)` : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- `URL de lecture des informations (userinfo endpoint)` : URL permettant de

récupérer les informations de l'utilisateur à l'aide du jeton fourni ;

- `URL de description des certificats de signature (jwks URI)` : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

Définition de l'identifiant client (Client ID) et clé secrète (Client secret)

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le `nom_fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Voir aussi...

Gestion des sources d'authentification multiples

Compatibilité OpenID Connnect

3.13. 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`.

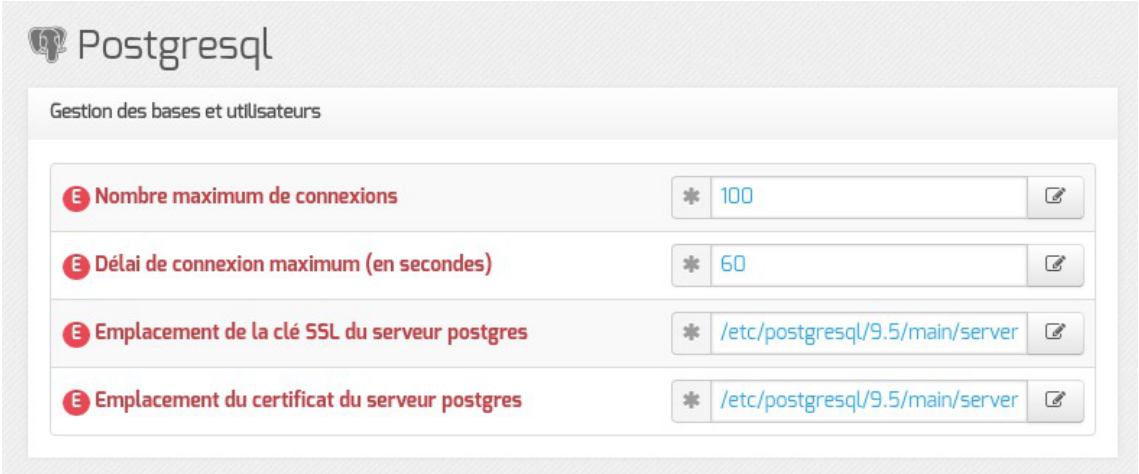
Si la variable est passée à `oui`, le port proposé pour accéder à l'EAD depuis l'extérieur est par défaut 4203.

Voir aussi...

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

3.14. Onglet Postgresql : Configuration du serveur PostgreSQL

Sur le module Zéphir, le serveur de base de données PostgreSQL est obligatoirement activé.



Vue de l'onglet Postgresql de l'interface de configuration du module

L'onglet expert `Postgresql` permet de modifier et de fixer une sélection de paramètres disponibles pour PostgreSQL :

- `Nombre maximum de connexions` : permet de définir le nombre maximum de connexions concurrentes au serveur de base de données ;
- `Délai de connexion maximum (en secondes)` : permet de définir le temps maximum pour terminer l'authentification du client ;
- `Quantité de mémoire pour les buffers partagés` : permet de définir la quantité de mémoire cache utilisée par le serveur, ce paramètre contribue le plus au gain de performance ;
- `Unité de la quantité de mémoire pour les buffers partagés` : permet de choisir l'unité kB ou MB utilisée pour le paramètre ci-dessus ;
- `Taille du cache (blocs de 8ko)` : taille de la mémoire de mise en cache, une grosse valeur aura tendance à augmenter l'utilisation des index, l'accès disque sera rendu plus rapide ;
- `Unité de la taille du cache` : permet de choisir l'unité kB ou MB utilisée pour le paramètre ci-dessus.

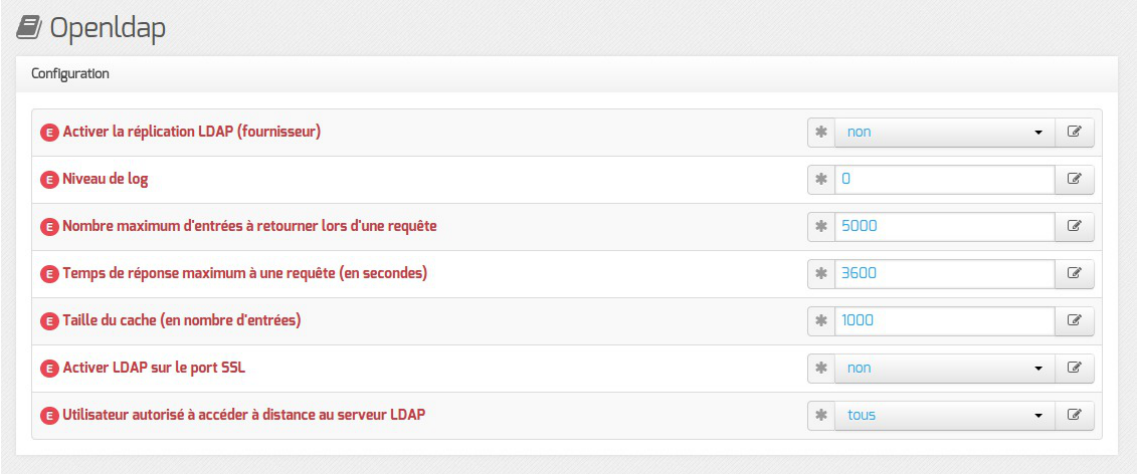
Le nom des variables Creole peut être affiché en activant le mode debug. Celles-ci portent le même nom que les paramètres du fichier `/etc/postgresql/9.3/main/postgresql.conf` mais préfixés par la chaîne `pg_`.

Pour plus d'informations, vous pouvez consulter la documentation officielle du logiciel :
http://docs.postgresqlfr.org/

3.15. Onglet Openldap : Configuration du serveur LDAP local

Sur certains modules EOLE, l'annuaire est obligatoirement configuré comme étant local :

- sur les modules faisant office de contrôleur de domaine tels que les modules Scribe, Horus et AmonEcole (et ses variantes), ou sur Seshat, l'annuaire est obligatoirement configuré comme étant local.
- sur le module Zéphir il est possible de choisir si l'annuaire est local ou distant. L'onglet expert `Openldap` n'existe que si l'annuaire est configuré comme étant local, cas par défaut.



Vue de l'onglet Openldap de l'interface de configuration du module

L'onglet expert `Openldap` permet de modifier et de fixer une sélection de paramètres disponibles dans le fichier de configuration : `/etc/ldap/slapd.conf`

Les paramètres en question se retrouvent dans le nom des variables Creole et sont généralement préfixés de la chaîne "`ldap_`".

Activer la réplication LDAP (fournisseur)

Sur les modules Scribe, Horus et AmonEcole, il est possible d'activer la réplication des données de l'annuaire local vers un annuaire distant (en général celui d'un module Seshat) avec l'option : `Activer la réplication LDAP (fournisseur)`.

A l'inverse, sur le module Seshat, l'option `Activer la réplication LDAP (client)` permet d'activer/désactiver le client de réplication LDAP.

Niveau de log

Avec `slapd` chaque niveau de log (une puissance de deux) représente la surveillance d'une fonctionnalité particulière du logiciel (exemple : le niveau 1 trace tout les appels de fonctions), les niveaux peuvent s'additionner.

Le niveau de log est à `0` par défaut.

Nombre maximum d'entrées à retourner lors d'une requête

Si le `Nombre maximum d'entrées à retourner lors d'une requête` est trop faible, il y a un risque que le résultat d'une requête LDAP retournant un nombre important d'entrées (liste de tous les élèves, par exemple) soit tronqué.

La valeur par défaut est de `5000` entrées.

Temps de réponse maximum à une requête (en secondes)

Le paramètre `Temps de réponse maximum à une requête` définit le nombre maximum de secondes le processus slapd passera pour répondre à une requête d'interrogation.

La valeur par défaut est de `3600` secondes.

Taille du cache (en nombre d'entrées)

Le paramètre `Taille du cache` définit le nombre d'entrées que le backend LDAP va conserver en mémoire.

La valeur par défaut est de `1000` entrées.

Activer LDAP sur le port SSL

Le paramètre `Activer LDAP sur le port SSL` permet de configurer *slapd* pour qu'il écoute sur le port SSL (636) en plus du port standard (389). La valeur `uniquement` n'impacte que les accès depuis l'extérieur (avec cette configuration, le port standard reste accessible pour les services qui s'exécutent sur le serveur).

Si la variable est paramétrée avec la valeur `uniquement`, certains logiciels utilisant l'interrogation LDAP tels que l'interface d'édition de règles ESU ne seront plus utilisables.

Utilisateur autorisé à accéder à distance au serveur LDAP

Le paramètre `Utilisateur autorisé à accéder à distance au serveur LDAP` permet de restreindre les accès depuis l'extérieur en fonction du compte LDAP utilisé :

- `tous` : connexion anonyme autorisée
- `authentifié` : connexion anonyme interdite
- `aucun` : aucune connexion possible

Pour plus d'informations, vous pouvez consulter la page de manuel :

```
# man slapd.conf
```

ou

http://manpages.ubuntu.com/manpages/trusty/en/man5/slapd.conf.5.html

3.16. 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 :

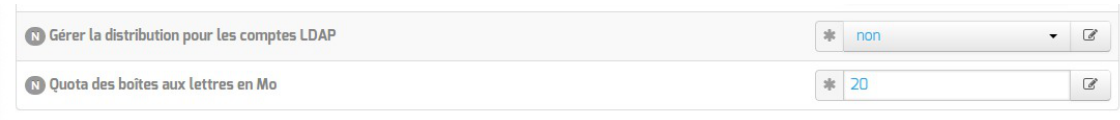
- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-` ;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer 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. 231] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

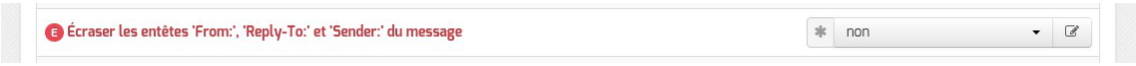
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

- `user@%%nom_machine.%%domaine_messagerie_etab` pour le maître
- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs

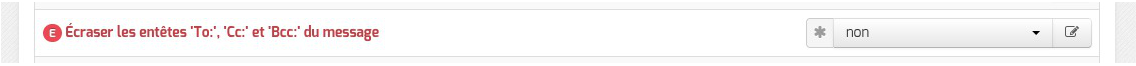
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

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`



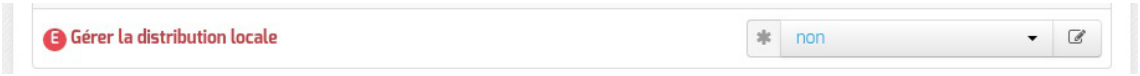
Réécriture de l'expéditeur :

	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.

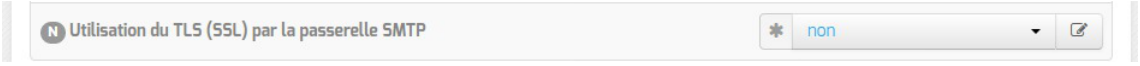


Dans ce cas il est possible d'agir sur le quota des boîtes et sur le pourcentage d'occupation, qui entraîne un message électronique d'avertissement.

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.236] pour l'envoi de message. Si la passerelle SMTP[p.235] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.235] (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 :

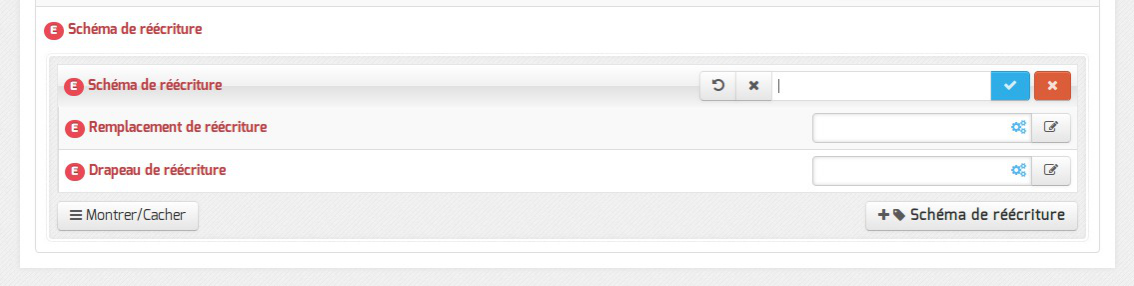
  - nom de domaine local ;
  - domaine privé de messagerie établissement ;
  - domaine public de messagerie établissement.
- `Envoyer les logs à rsyslog`

  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.

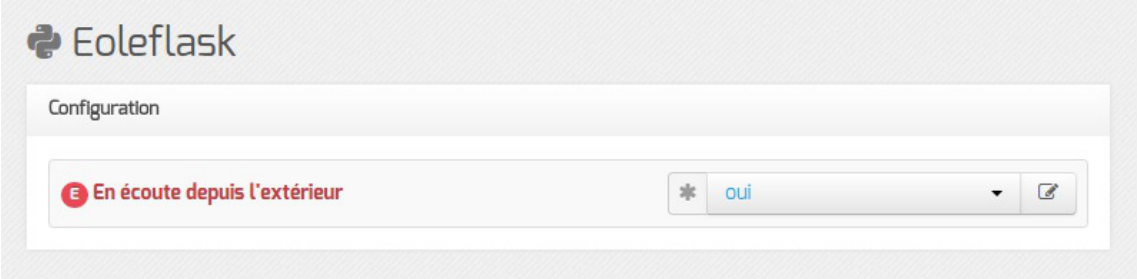


Les trois variables à saisir sont :

- 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

3.17. 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.

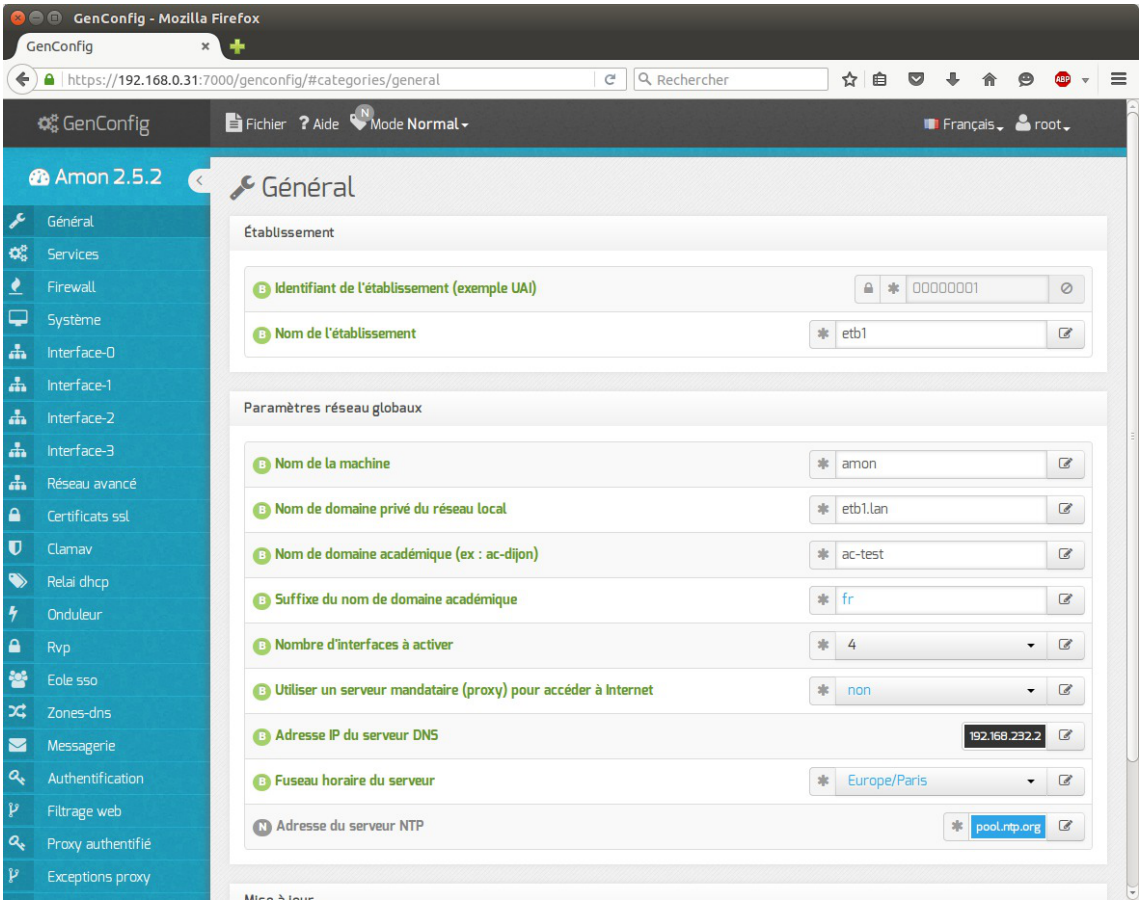
Accès distant

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.

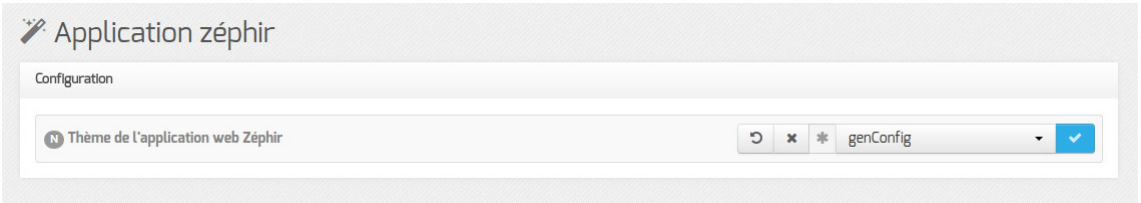
Il faut ensuite valider les certificats pour pouvoir accéder à l'interface.



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`.

3.18. Onglet Application zéphir



Le thème de l'application web Zéphir est paramétrable, le thème par défaut est `genConfig`.

Il est possible de créer son propre thème à partir d'un thème existant présent dans `/usr/share/zephir/web/themes/` :

- choisir depuis l'interface de configuration du module un thème à partir duquel partir ;
- reconfigurer le serveur à l'aide de la commande `reconfigure` ;
- éditer le fichier `/usr/share/zephir/web/css/style.css` ;
- placer les images dans `/usr/share/zephir/web/images/` ;

- placer les fonts dans `/usr/share/zephir/web/fonts/` ;
- créer un répertoire pour le nouveau thème :

  ```
  # mkdir /usr/share/zephir/web/themes/monTheme
  ```

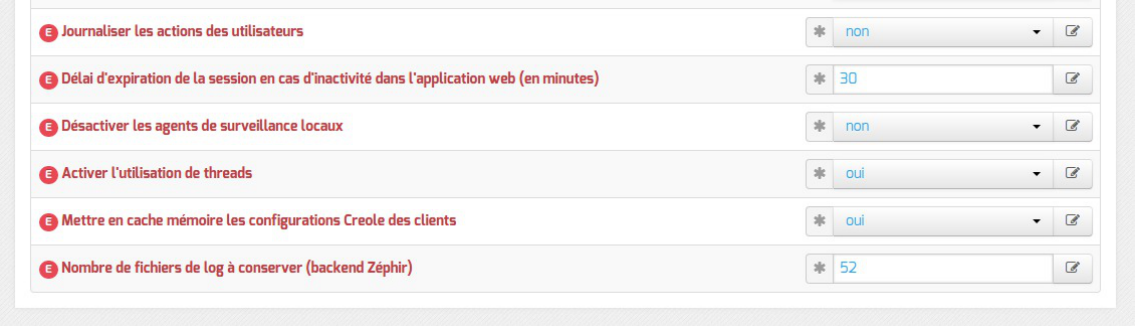
- copier le tout dans `/usr/share/zephir/web/themes/monTheme` :

  ```
  # cp -Rp /usr/share/zephir/web/css /usr/share/zephir/web/themes/monTheme/
  # cp -Rp /usr/share/zephir/web/fonts /usr/share/zephir/web/themes/monTheme/
  # cp -Rp /usr/share/zephir/web/images /usr/share/zephir/web/themes/monTheme/
  ```

- choisir depuis l'interface de configuration du module le nouveau thème ;
- reconfigurer le serveur à l'aide de la commande `reconfigure`.

Le fichier `colors.ini` n'est plus utilisé pour changer l'apparence de l'application web Zéphir.

En mode expert un certain nombre de paramètres supplémentaires permet de personnaliser le comportement du serveur Zéphir : backend et frontend.



- `Journaliser les actions des utilisateurs` : permet d'enregistrer dans les journaux (`/var/log/rsyslog/local/zephir_backend/zephir_backend.info.log`) les appels au backend effectués par les utilisateurs (appels authentifiés) ;
- `Délai d'expiration de la session en cas d'inactivité dans l'application web (en minutes)` : permet de modifier le délai en minutes au bout duquel un utilisateur inactif sera déconnecté de l'application web Zéphir ;
- `Désactiver les agents de surveillance locaux` : permet de désactiver les agents de surveillance du serveur Zéphir lui-même, cela permet dans certains cas de débloquer ou de rendre plus rapide l'application si des agents posent problème (par exemple blocage d'un test réseau, timeout sur un accès web) ;
- `Activer l'utilisation de threads` : permet, en cas d'instabilité du service, de désactiver l'utilisation de threads pour certaines fonctions du backend Zéphir ;
- `Mettre en cache mémoire les configurations Creole des clients` : permet de désactiver la mise en cache des configurations des serveurs pour utiliser moins de mémoire vive ;
- `Nombre de fichiers de log à conserver (backend Zéphir)` : permet de définir le nombre de fichiers à conserver lors de la purge hebdomadaire des journaux du service Zéphir

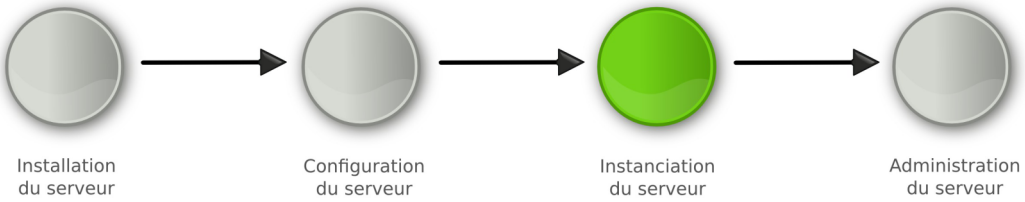
```
/var/log/rsyslog/local/zephir_backend/zephir_backend.*.log
```

Il est possible de désactiver totalement l'application web Zéphir en répondant `non` à la question `Activer l'application web Zéphir` qui apparaît dans l'onglet `Services` en mode expert.

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`.

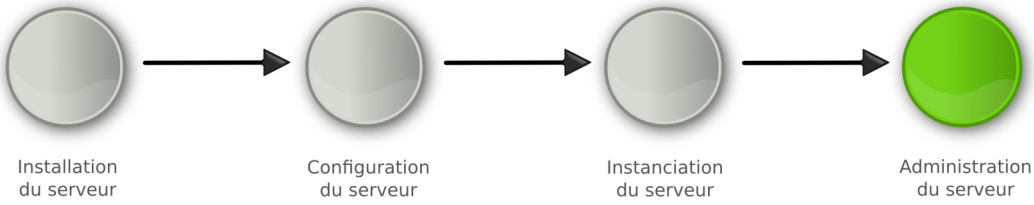
  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

  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 Zéphir



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. Présentation générale de l'application Zéphir

Le module Zéphir fournit l'application Zéphir.

Cette application propose une solution de **déploiement**, de **surveillance** et de **maintenance** des modules EOLE.

Elle est composée :

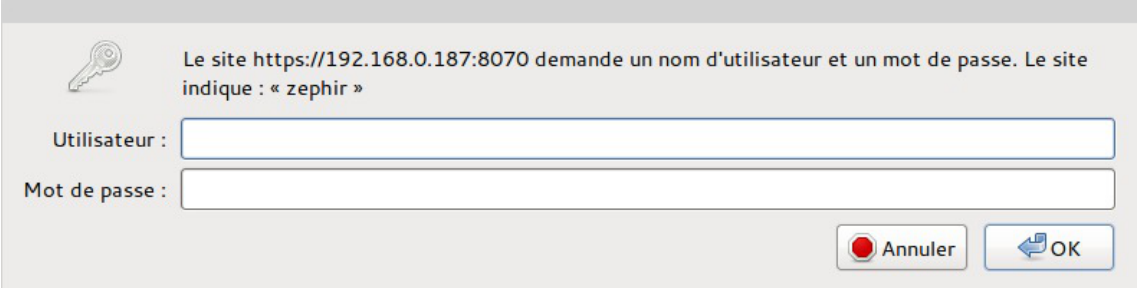
- d'une interface web Zéphir ;
- d'un serveur de commandes.

Accès à l'interface web Zéphir

L'interface web est accessible depuis l'adresse du serveur uniquement en HTTPS sur le port 8070 : `https://<adresse_du_serveur>:8070/`

Mire d'authentification

Après validation du certificat dans le navigateur, l'application demande de s'authentifier.



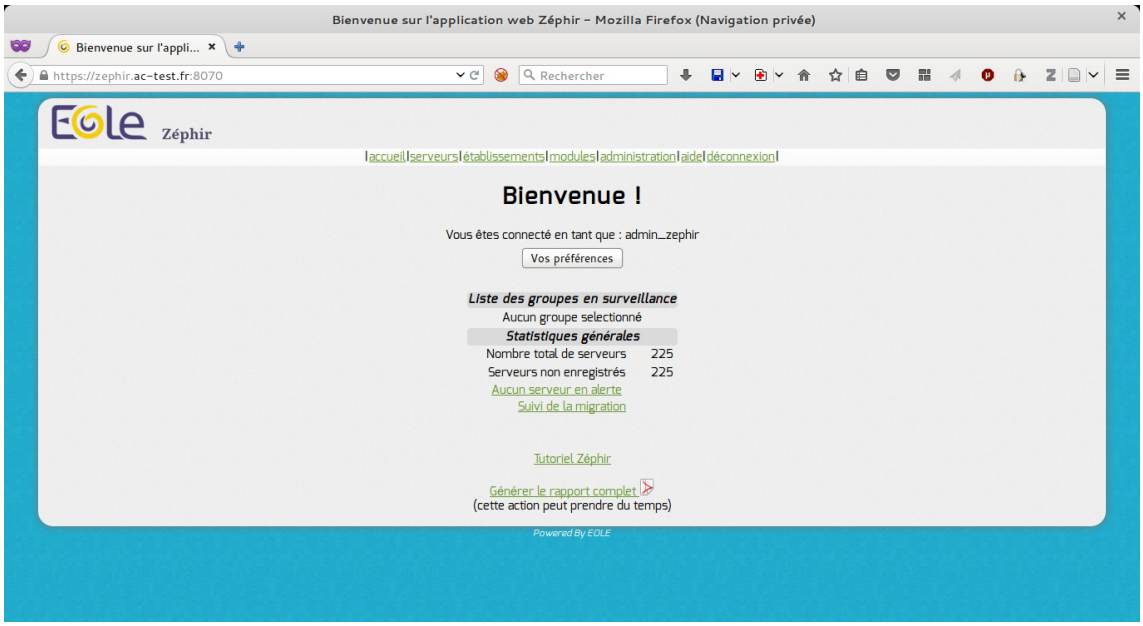
Le compte et le mot de passe associé sont ceux créés pendant la phase d'instanciation, par défaut le compte `admin_zephir`.

Déconnexion

La déconnexion se fait en cliquant sur l'item déconnexion du menu.

Une fois déconnecté de l'application il faut cliquer sur l'un des items du menu (accueil, établissements, serveurs, modules, etc) pour obtenir à nouveau la mire d'authentification.

Page d'accueil



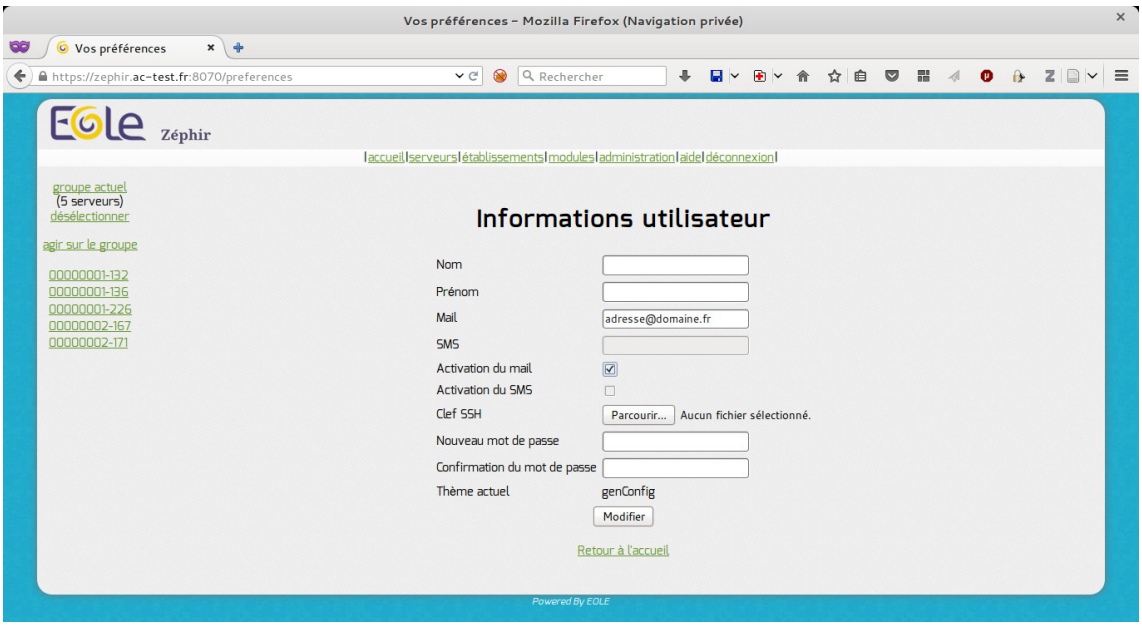
Sur la page d'accueil apparaît :

- un menu pour les différentes actions ;
- le compte de connexion : **Bienvenue admin_zephir** ;
- un bouton pour éditer `Vos préférences` ;
- un tableau récapitulatif de certaines données serveurs :
  - groupe sélectionné ;
  - nombre total de serveurs ;
  - serveurs non enregistrés ;
  - `serveurs en alerte (cf. Liste des serveurs en alerte)` ;
  - suivi de migration ;
  - gestion des identifiants ENT (si au moins un module Scribe a réclamé des identifiants ENT).
- un accès vers le `Tutoriel Zéphir (cf. Aide)` [p.101] (équivalent à l'onglet `aide (cf. Aide)` [p.101] dans la

barre menu) ;

- la possibilité de générer et d'actualiser un rapport complet en PDF.

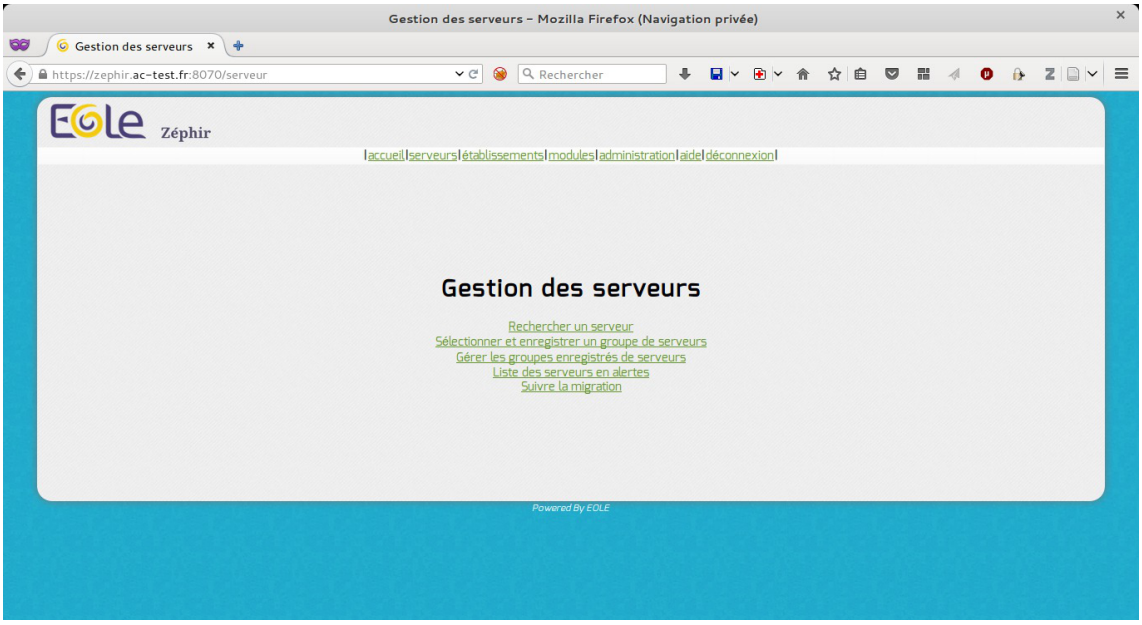
Vos préférences



Les informations utilisateur à saisir :

- le nom ;
- le prénom ;
- l'adresse courriel (pour recevoir les alertes) ;
- l'ajout de la clé SSH (pour se connecter aux serveurs enregistrés dans Zéphir sous réserve d'autorisation).

1.1. L'onglet serveurs



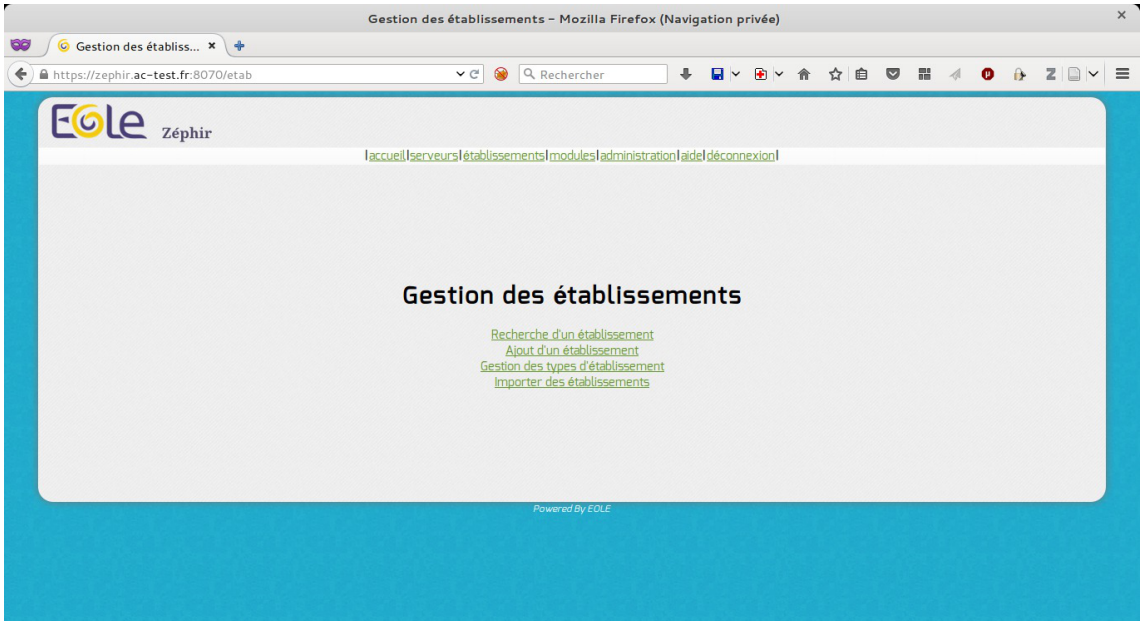
L'onglet serveurs propose un menu avec la possibilité de :

- lister les serveurs en alerte ;
- faire le suivi de la migration ;
- rechercher un serveur ;
- sélectionner un groupe de serveurs ;
- gérer des groupes de serveurs.

Voir aussi...

> Liste des serveurs en alerte

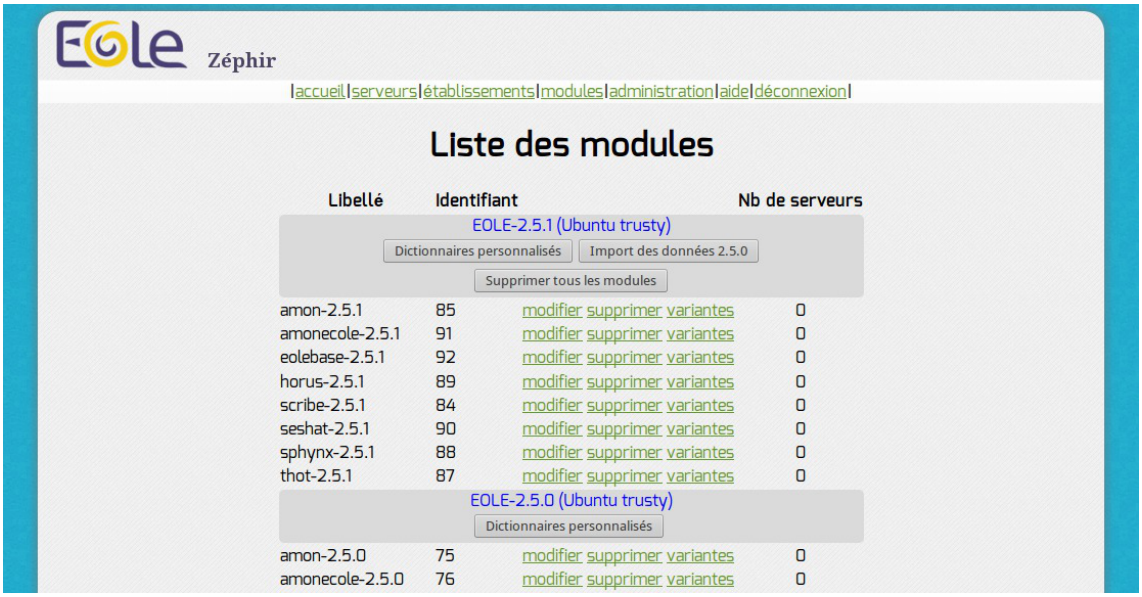
1.2. L'onglet établissements



L'onglet établissements propose un menu avec la possibilité de :

- rechercher un établissement enregistré
- ajouter d'un établissement ;
- gérer les types d'établissement ;
- importer des établissements.

1.3. L'onglet modules

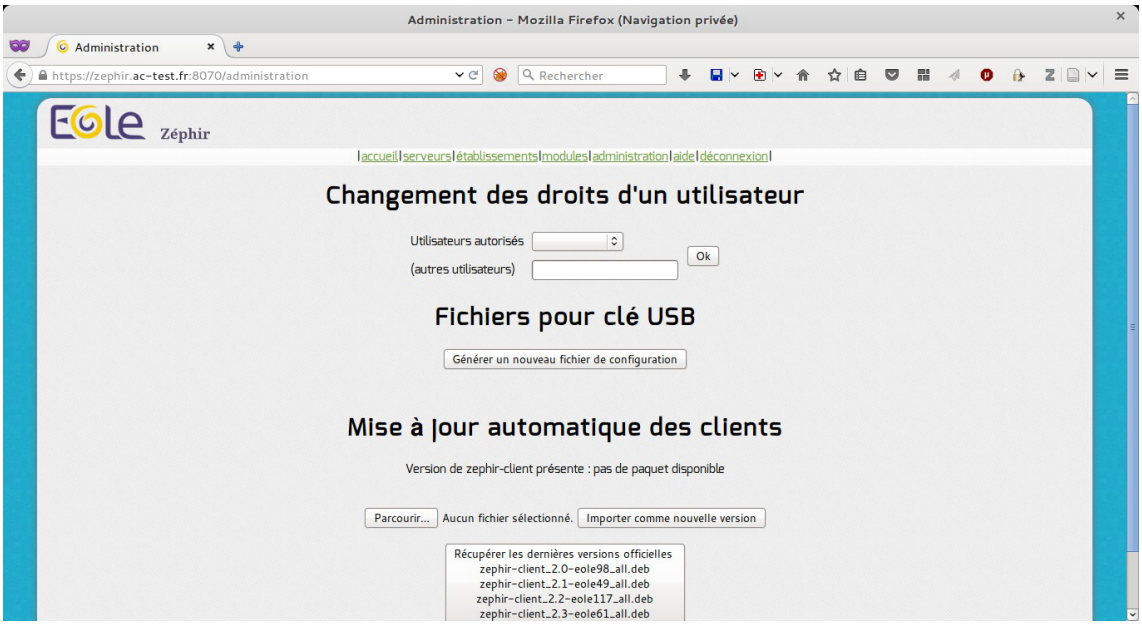


L'onglet modules propose une liste d'action possible à partir des modèles de module 2.3, 2.4 et 2.5 :

- modifier et/ou supprimer un modèle existant ;
- créer de nouvelles variantes ;
- créer des dictionnaires personnalisés qui seront utilisés dans les variantes ;
- créer un nouveau module.

Dans cet onglet s'affiche le nombre de serveurs par type de module par version.

1.4. L'onglet administration



L'onglet administration permet :

- gérer les utilisateurs de l'application web Zéphir et les droits associés ;
- créer un fichier de configuration à utiliser en établissement pour associer le module au serveur Zéphir ;
- gérer la mise et le déploiement de `zephir-client`.

1.5. Aide

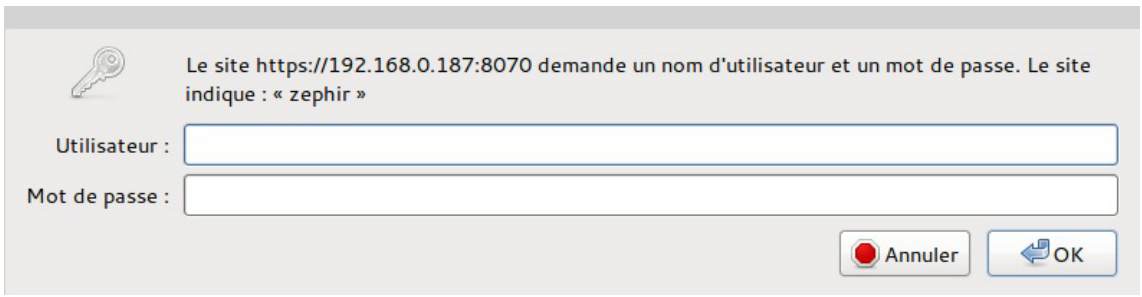
Cet item de menu ouvre une nouvelle fenêtre proposant une aide embarquée. Cette aide n'est pas maintenue, cependant beaucoup d'informations restent valides.

2. Gestion des utilisateurs

Selon comment vous avez configurer le module Zéphir, l'annuaire des utilisateurs est distant ou local.

Pour utiliser l'application Zéphir vous aurez besoin d'un compte présent dans l'annuaire LDAP.

Vous pouvez vous connecter à l'application Zéphir avec l'utilisateur spécifié lors de l'instance du module (par défaut `admin_zephir`).



Si vous souhaitez travailler avec l'utilisateur `admin zephir` la première chose à faire est de lui ajouter des droits.

2.1. Création d'un utilisateur

Ajouter un utilisateur dans l'application Zéphir

Les utilisateurs ajoutés par l'application Zéphir ne sont pas ajoutés à l'annuaire.

Ajouter un utilisateur à l'annuaire local LDAP

Si vous utilisez l'annuaire LDAP local pour gérer l'authentification, vous avez à votre disposition le script `/usr/share/zephir/utils/add_user.py` qui permet d'ajouter un utilisateur.

Si l'utilisateur existe déjà, vous pouvez modifier son mot de passe en relançant `add user.py`.

2.2. Affectation des droits et limitation des ressources

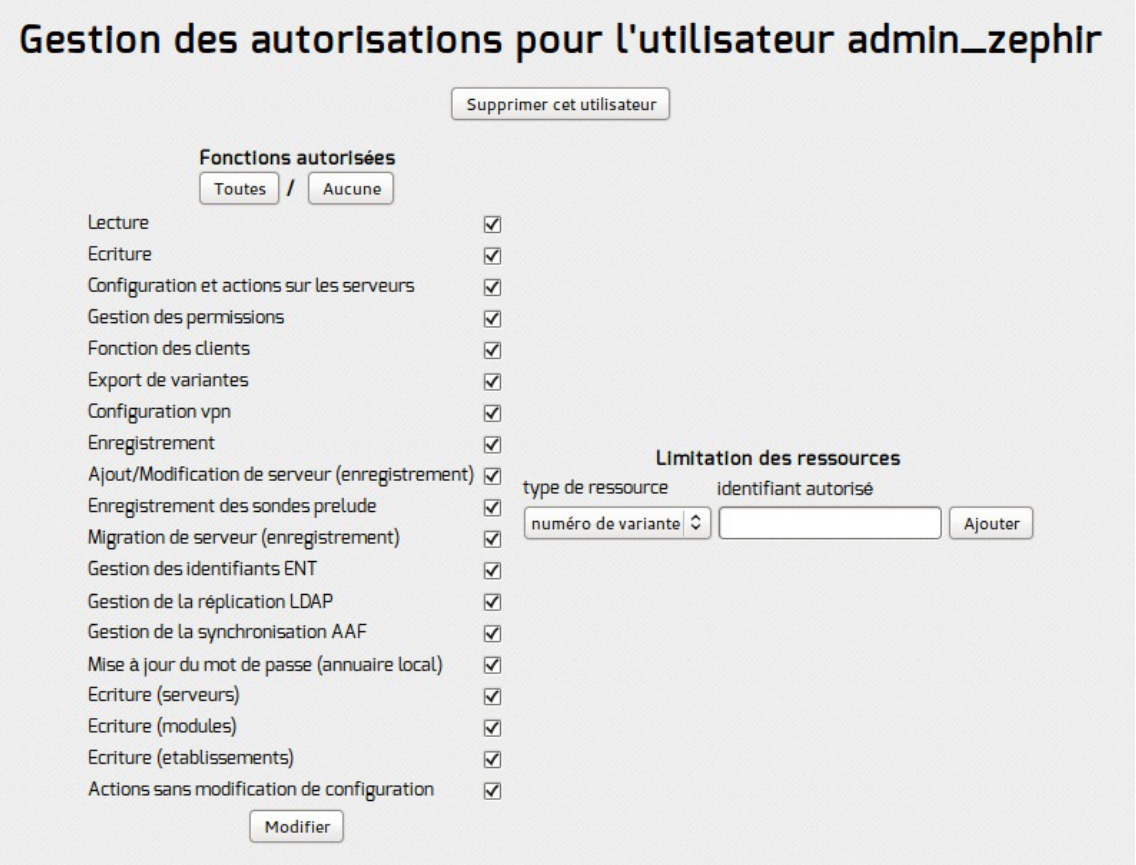
Affectation des droits

L'affectation des droits est accessible aux utilisateurs ayant le droit de `gestion des permissions` (ce qui est le cas par défaut de l'utilisateur `admin zephir`). Pour changer les droits d'un utilisateur, il faut se rendre dans l'onglet `administration` et choisir l'utilisateur dans la liste déroulante ou saisir le début du nom du compte dans le champ de texte dans la partie `Changement des droits d'un utilisateur`.

Si l'utilisateur possède déjà des droits, son compte apparaîtra dans la liste des utilisateurs, sinon il faut taper le nom exact du compte.

Cliquer sur le bouton `OK` pour valider la sélection de l'utilisateur.

Après avoir validé, une page affiche les droits de cet utilisateur. Pour modifier les droits de l'utilisateur, cocher un ou plusieurs groupes d'actions autorisées et cliquer sur le bouton `modifier`.



Il est possible de sélectionner et désélectionner rapidement tous les droits de la liste avec les boutons `Toutes` et `Aucune`.

Ajouter des droits à un utilisateur équivaut à lui autoriser l'accès à une liste de fonctions du serveur de commande Zéphir (fonctions accessibles par XML-RPC[p.237]).

Voici les principaux groupes d'actions autorisées :

- **Gestion des permissions**
  - permet de gérer les permissions des autres utilisateurs ;
  - permet d'associer les clefs SSH des utilisateurs à des serveurs ;
  - permet de mettre à disposition des serveurs clients un paquet `zephir-client` (utile pour tester des versions candidates du client).
- **Lecture** :
  - permet d'accéder aux informations connues de l'application Zéphir (base de données et fichiers remontés par les serveurs) ;
  - permet de créer / modifier / supprimer des groupes de serveurs.
- **Mise à jour du mot de passe (annuaire local)** : permet à l'utilisateur de modifier son mot de passe depuis ses préférences (seulement si Zéphir utilise l'annuaire local).
- **Écriture** :
  - permet de créer / modifier et supprimer des établissements / serveurs/ modules dans l'application Zéphir (touche principalement l'aspect base de données) ;
  - permet aussi de saisir la configuration des serveurs / migrer un serveur / gérer les fichiers personnalisés des serveurs.

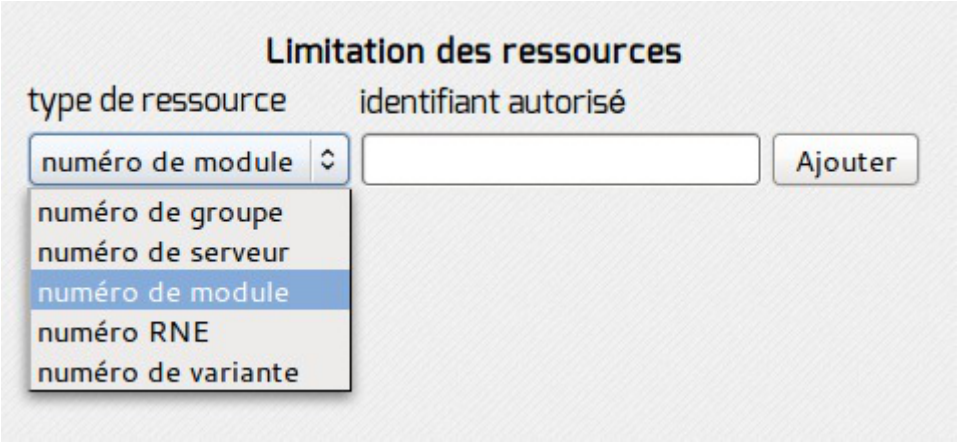
- **Configuration et actions sur les serveurs** :
  - permet d'accéder aux fonctions disponibles dans la page `Actions sur le serveur` ;
  - permet de modifier la configuration (`zephir.eol`) des serveurs.
- **Configuration VPN** : permet d'envoyer des configurations VPN sur le serveur Zéphir depuis un serveur Sphynx enregistré et de les récupérer sur un serveur Amon via le script `active_rvp.sh`.
- **Enregistrement** : permet d'enregistrer un serveur sur le serveur Zéphir (procédure `enregistrement_zephir`).
- **Ajout / modification de serveur (enregistrement)** : permet de créer un serveur non existant dans l'application au moment de l'enregistrement sur le serveur Zéphir.
- **Enregistrement des sondes prelude** : permet d'enregistrer automatiquement les sondes prelude d'un serveur client sur un serveur prelude-manager.
- **Migration de serveur (enregistrement)** : permet de migrer un serveur dans la base Zéphir au moment de l'enregistrement (par exemple, après installation d'un serveur Amon 2.3 pour remplacer un Amon 2.2).
- **Export de variantes** : permet d'envoyer une variante d'un module sur un autre serveur Zéphir.
- **Gestion des identifiants ENT** : permet la gestion de plages d'identifiants pour les ENT (cf. préconisations du SDET).
- **Gestion de la réplication LDAP** : permet de gérer les configurations de réplication d'annuaires des serveurs Scribe vers un serveur Seshat.
- **Gestion de la synchronisation AAF** : permet d'activer le transfert de fichiers AAF vers un serveur Scribe et d'automatiser leur envoi (notification).

Les autres droits sont pour la plupart des restrictions plus fines faisant partie d'un groupe d'actions autorisées (par exemple écriture sur les serveurs seulement).

Limitation des ressources

Il est possible de restreindre les accès d'un utilisateur à un lot de serveurs.

type de ressources .



La limitation d'accès se fait en sélectionnant un type de ressources : groupe, serveur, module, RNE[p.234] ou variante puis en saisissant l'identifiant de la ressource autorisée dans le champs `identifiant autorisé` et en cliquant sur le bouton `Ajouter`.

Les identifiants sont les ID des ressources renseignées dans l'application Zéphir.

Pour récupérer les ID :

- d'un groupe : sélectionner l'onglet `serveurs` puis `Gestion des groupes de serveurs` ;
- d'un serveur :
  - afficher tous les serveurs :

    sélectionner l'onglet `serveurs` puis cliquer sur `Sélection d'un groupe de serveurs`, cliquer directement sur le bouton `Suivant` sans rien choisir dans la liste des modules ;

    dans le formulaire suivant cliquer sur `Entrez un ou plusieurs critères de recherche`, choisir ou non, un ou des critères de sélection, cliquer sur le bouton `Suivant` ;

    dans le formulaire suivant cliquer sur `Sélection sur les valeurs de configuration` et enfin cliquer sur le bouton `Suivant`.
  - rechercher un serveur dans un établissement donné :

    sélectionner l'onglet `établissements` puis cliquer sur `Recherche d'un établissement`, choisir ou non, un ou des critères de sélection, cliquer sur le bouton `Ok` ;

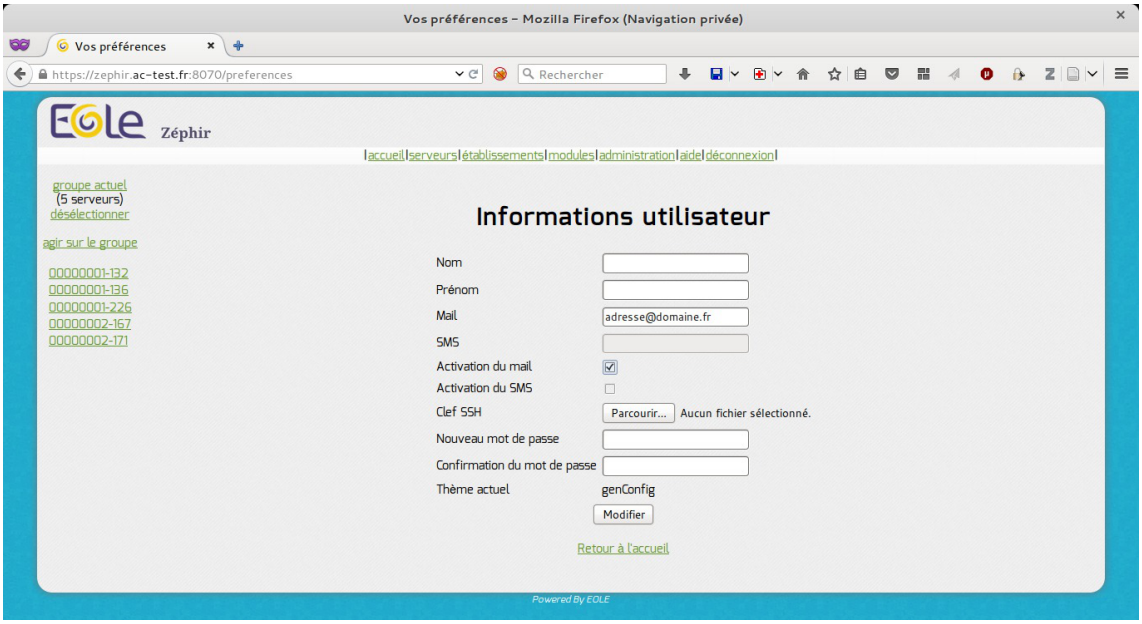
    dans la page suivante cliquer sur l'identifiant (RNE) de l'établissement recherché.
- d'un module : sélectionner l'onglet `modules` ;
- de type RNE : sélectionner l'onglet `établissements` puis cliquer sur `Recherche d'un établissement`, choisir ou non, un ou des critères de sélection, cliquer sur le bouton `Ok` ;
- d'une variante : sélectionner l'onglet `modules` puis cliquer sur `variantes` de la ligne correspondante au nom du module d'origine.

Au delà d'un certain nombre d'identifiant à ajouter il est conseillé de créer un groupe de serveur et de limiter les ressources en fonction de l'ID du groupe.

2.3. Préférences des utilisateurs

L'application web Zéphir intègre une page de préférences permettant de gérer des informations liées aux utilisateurs. Ces données sont facultatives mais certaines permettent d'accéder à des fonctionnalités avancées du serveur Zéphir (réception de messages d'alerte et connexion aux serveurs avec une clef SSH).

Lorsque vous êtes connecté, cliquer sur le lien `préférences` du menu principal pour renseigner vos préférences.



Les informations demandées sont les suivantes :

- nom et prénom de l'utilisateur ;
- adresse mail de l'utilisateur ;
- activation ou non des alertes par courrier électronique ;
- enregistrement d'une clef publique de connexion SSH (permet de se connecter aux serveurs sans mot de passe).

Dans le cas où l'annuaire utilisé est l'annuaire local, les utilisateurs ont la possibilité de modifier leur mot de passe depuis la page des préférences.

Pour que l'option soit disponible, il faut leur attribuer le groupe de droits `Mise à jour du mot de passe (annuaire local)`.

Les paramètres nom, prénom et adresse mail sont remplis automatiquement à l'affectation des droits s'ils sont présents dans l'annuaire (attributs : '*sn*', '*givenName*' et '*mail*').

La réception d'alertes est rattachée à la notion de groupes de serveurs.

2.4. Gestion de la connexion aux serveurs

Les utilisateurs peuvent déposer sur le serveur Zéphir une clef publique pour la connexion SSH sur les serveurs.

Les utilisateurs ayant les droits de gestion des permissions peuvent interdire ou autoriser l'utilisation de ces clefs sur les serveurs de leur choix. Pour envoyer la clef d'un utilisateur sur un (des) serveur(s), il faut sélectionner un groupe de serveurs, entrer le login d'un utilisateur dans la case sous "*connexion par clé ssh*" et cliquer sur `autoriser` (ou `interdire` pour retirer la clef).

La clef de l'utilisateur sera envoyée sur le serveur (fichier `authorized_keys`) au prochain envoi de

configuration (vous pouvez la planifier en appuyant sur action sur le groupe de serveurs, puis envoyer la configuration au serveur).

Vous pouvez envoyer votre clef SSH publique (en général sous linux : ~/.ssh/id_rsa.pub ou ~/.ssh/id_dsa.pub).

Si vous ne possédez pas de clé, vous pouvez en créer une avec la commande suivante :

```
$ ssh-keygen -t rsa
```

(vous pouvez laisser les options par défaut ou donner une phrase qui vous servira de mot de passe sur tous les serveurs ayant votre clef). Une fois la clef envoyée sur le serveur Zéphir, l'utilisateur admin_zephir (ou tout autre utilisateur ayant des droits équivalents) peut autoriser un utilisateur à se connecter à un groupe de serveurs à l'aide de sa clef.

Voir aussi...

Gestion par groupe de serveurs [p.160]

2.5. Suppression d'un utilisateur

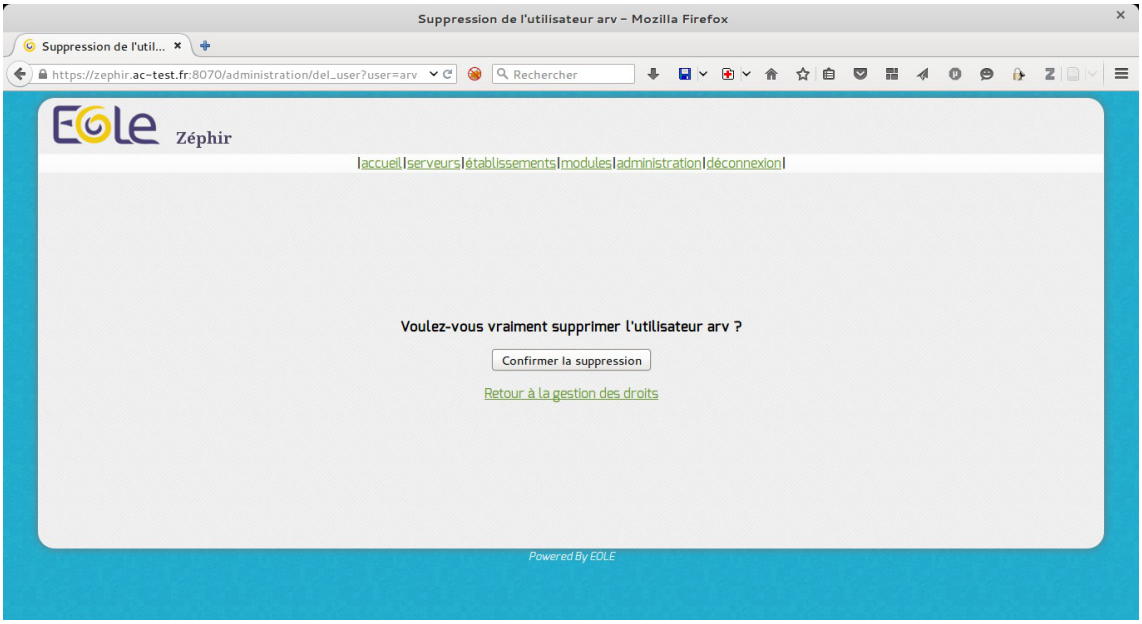
Supprimer un utilisateur de l'application Zéphir

Pour supprimer un utilisateur, il faut se rendre dans l'onglet administration et choisir l'utilisateur dans la liste déroulante ou saisir le début du nom du compte dans le champ de texte dans la partie Changement des droits d'un utilisateur.

Si l'utilisateur possède déjà des droits, son compte apparaîtra dans la liste des utilisateurs, sinon il faut taper le nom exact du compte.

Cliquer sur le bouton OK pour valider la sélection de l'utilisateur.

Le bouton Supprimer cet utilisateur, présent en haut de page, permet de le supprimer. Une confirmation est demandée.



Supprimer un utilisateur signifie le supprimer de la base de données interne à l'application Zéphir. À aucun moment l'utilisateur n'est supprimé de l'annuaire LDAP.

Supprimer un utilisateur de l'annuaire local LDAP

Si vous utilisez l'annuaire LDAP local pour gérer l'authentification, vous avez à votre disposition le script `/usr/share/zephir/utils/del_user.py` qui permet de supprimer un utilisateur.

2.6. Gestion en console des utilisateurs de l'annuaire LDAP local

Si vous utilisez l'annuaire LDAP local pour gérer l'authentification, vous avez à votre disposition des scripts permettant de créer des utilisateurs, de modifier leur mot de passe et de les supprimer. Ces scripts sont situés dans le répertoire `/usr/share/zephir/utils`.

- `add_user.py` : permet de créer un utilisateur dans l'annuaire et de lui donner un mot de passe ;
- `del_user.py` : supprime un utilisateur de l'annuaire ;
- `list_users.py` : affiche la liste des utilisateurs présents dans l'annuaire local.

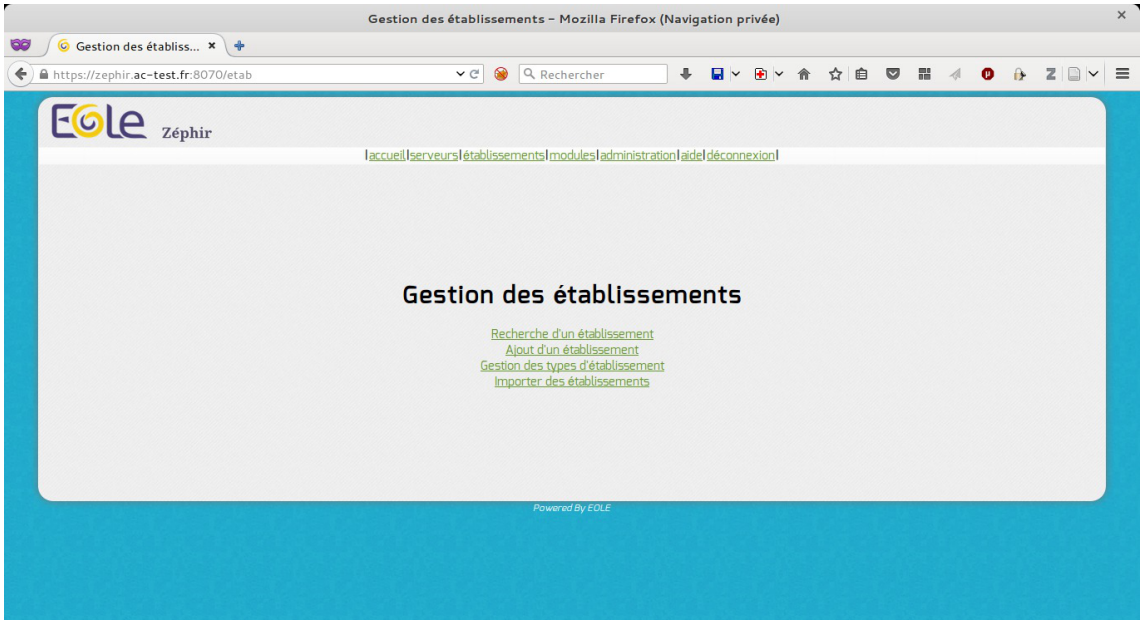
Si l'utilisateur existe déjà, vous pouvez modifier son mot de passe en relançant `/usr/share/zephir/utils/add_user.py`.

3. Gestion des établissements

Dans l'application Zéphir, un serveur est systématiquement rattaché à un établissement.

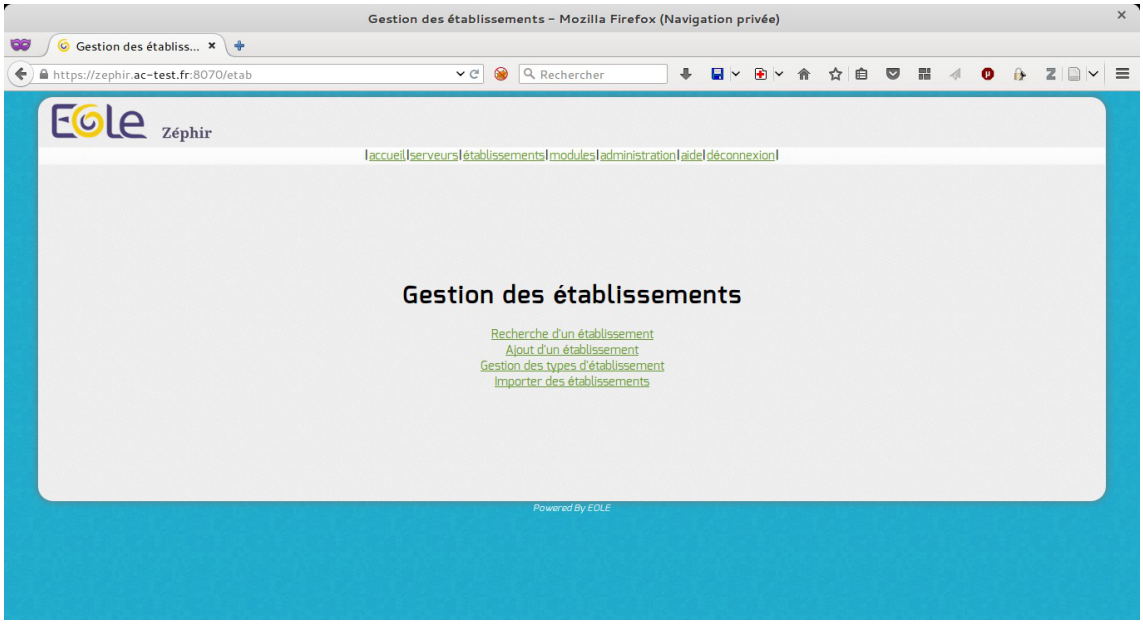
Il est possible de créer, rechercher ou afficher un établissement depuis le menu `établissements` de

l'application Zéphir.



3.1. Ajout d'un d'établissement

Pour ajouter un établissement il faut se rendre dans l'application Zéphir et cliquer sur l'entrée `établissement` du menu.

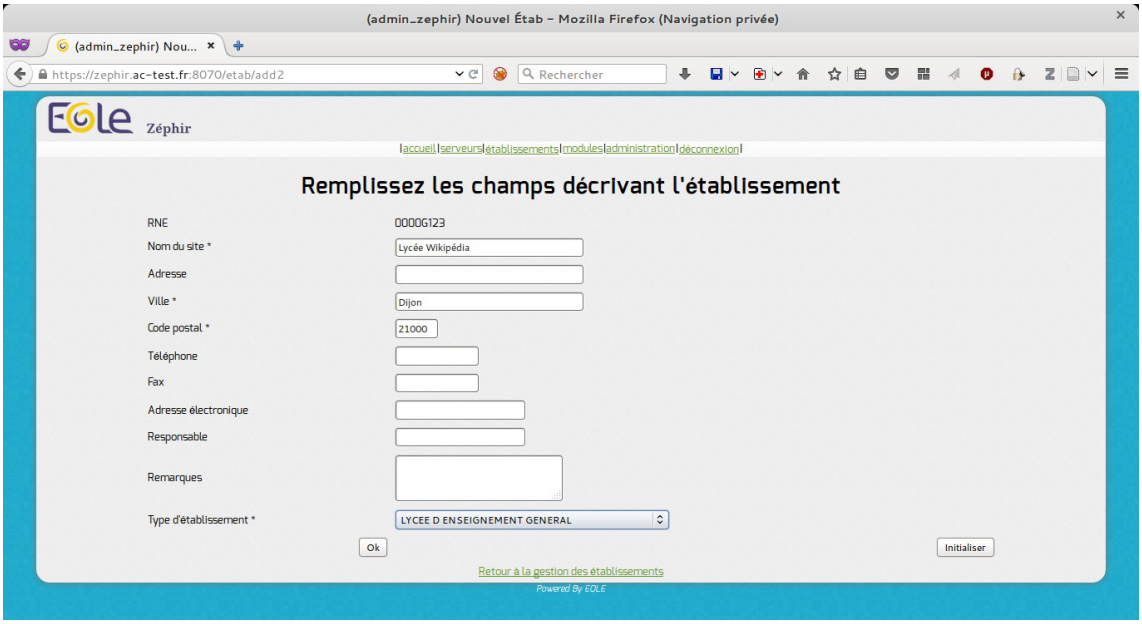


Puis cliquer sur `Ajout d'un établissement`.

L'identifiant à saisir correspond au RNE de l'établissement (8 caractères maximum).

Le RNE est la seule information que l'on ne pourra pas modifier. Il faut donc prendre garde à saisir le bon numéro. En cas d'erreur, la seule solution sera de supprimer l'établissement fraîchement créé et le recréer.

Il faut ensuite renseigner la description de l'établissement (adresse physique, moyens de communication, ...).



Seuls les champs pourvus d'une `*` sont obligatoires (nom du site, ville, code postal et type d'établissement). Des types d'établissement peuvent être ajoutés dans établissement / Gestion des types d'établissement mais il faut le faire avant d'ajouter un nouvel établissement. Un fois validé avec le bouton OK, l'établissement est créé.

3.2. Import d'établissements depuis un fichier

Il est possible d'importer un fichier texte comprenant la liste des établissements depuis l'application web Zéphir.

Pour cela il faut cliquer sur le menu établissements et choisir Importer des établissements.

L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese[p.234]) CSV[p.231] avec comme séparateur un "|".

Les champs suivants sont attendus :

```
1 RNE|LIBELLE CODE NATURE|CODE NATURE|LIBELLE ETAB|NOM ETAB|CODE
  POSTAL|LOCALITE|MAIL|FAX|TEL
```

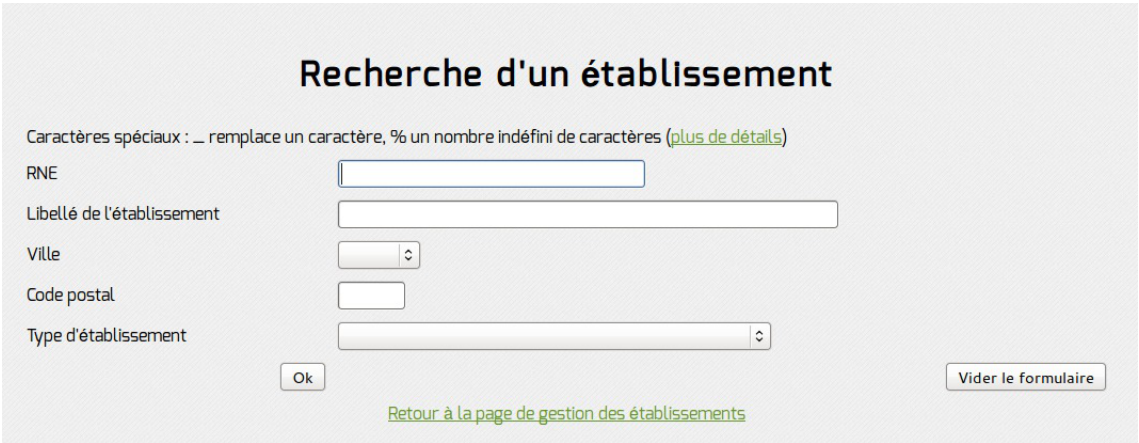
```
1
2 210024M|CLG|340|COLLEGE|CHAMPOLLION|21000|DIJON|ce.0210024M@ac-dijon.fr|038073
  0210026P|CLG|340|COLLEGE|EPIREY|21000|DIJON|ce.0210026P@ac-dijon.fr|0380732916|
```

Après l'importation un rapport est affiché.

3.3. Recherche d'un ou de plusieurs établissements

Pour accéder à la page d'affichage d'un établissement, il faut renseigner un (ou plusieurs) paramètres le concernant, à savoir :

- l'identifiant (RNE) ;
- le nom de l'établissement ;
- le lieu ;
- le type d'établissement.



Le symbole générique `%` remplace un nombre indéfini de caractères.

Par exemple :

- `021%` dans le champs RNE correspond à tous les établissements dont le RNE commence par 021 ;
- `%` dans le champs RNE renvoie tous les établissements.

3.4. Édition et suppression d'un établissement

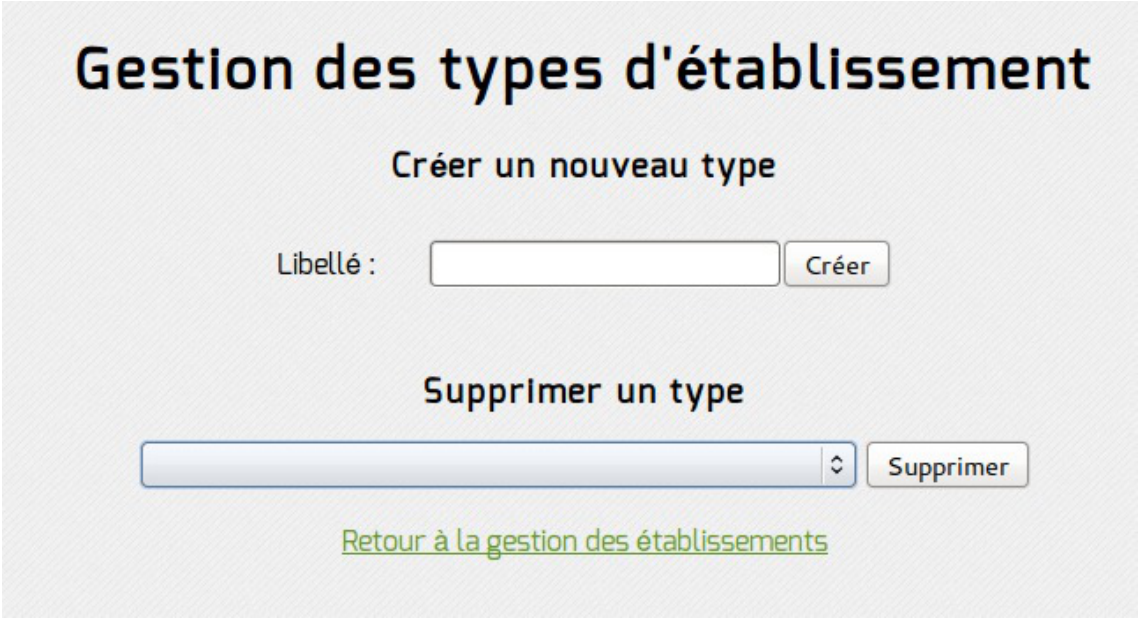
L'édition, la suppression d'un établissement ainsi que les opérations sur les serveurs de cet établissement sont disponibles depuis la page d'affichage de ce dernier :

Il n'est pas possible d'effacer un établissement ayant des serveurs. Il est nécessaire de supprimer d'abord les serveurs, puis l'établissement.

3.5. Types d'établissement

Le type d'établissement n'est qu'une information permettant de distinguer rapidement les établissements.

Il est possible d'ajouter de nouveaux types d'établissement ou d'en supprimer. Pour cela, cliquer sur le menu `établissements`, puis sur `gestion des types d'établissement` :



4. Gestion des serveurs

4.1. Généralité sur la gestion des serveurs

4.1.1. Lister les serveurs

Il est possible d'accéder à un serveur de 3 façons différentes :

- faire une recherche par serveur ;
- travailler avec des groupes de serveur ;
- faire une recherche par établissement.

Recherche d'un serveur particulier

La recherche d'un serveur particulier nécessite de connaître au préalable l'identifiant Zéphir du serveur.
Cliquer sur `serveurs`, puis `Recherche d'un serveur particulier` et entrer l'identifiant.

Sélection d'un groupe de serveurs

Il est possible d'accéder à un serveur en utilisant la fonction sélection d'un groupe de serveurs.
Cliquer sur `serveurs`, puis `Sélection d'un groupe de serveurs` et remplir les divers critères de sélection.

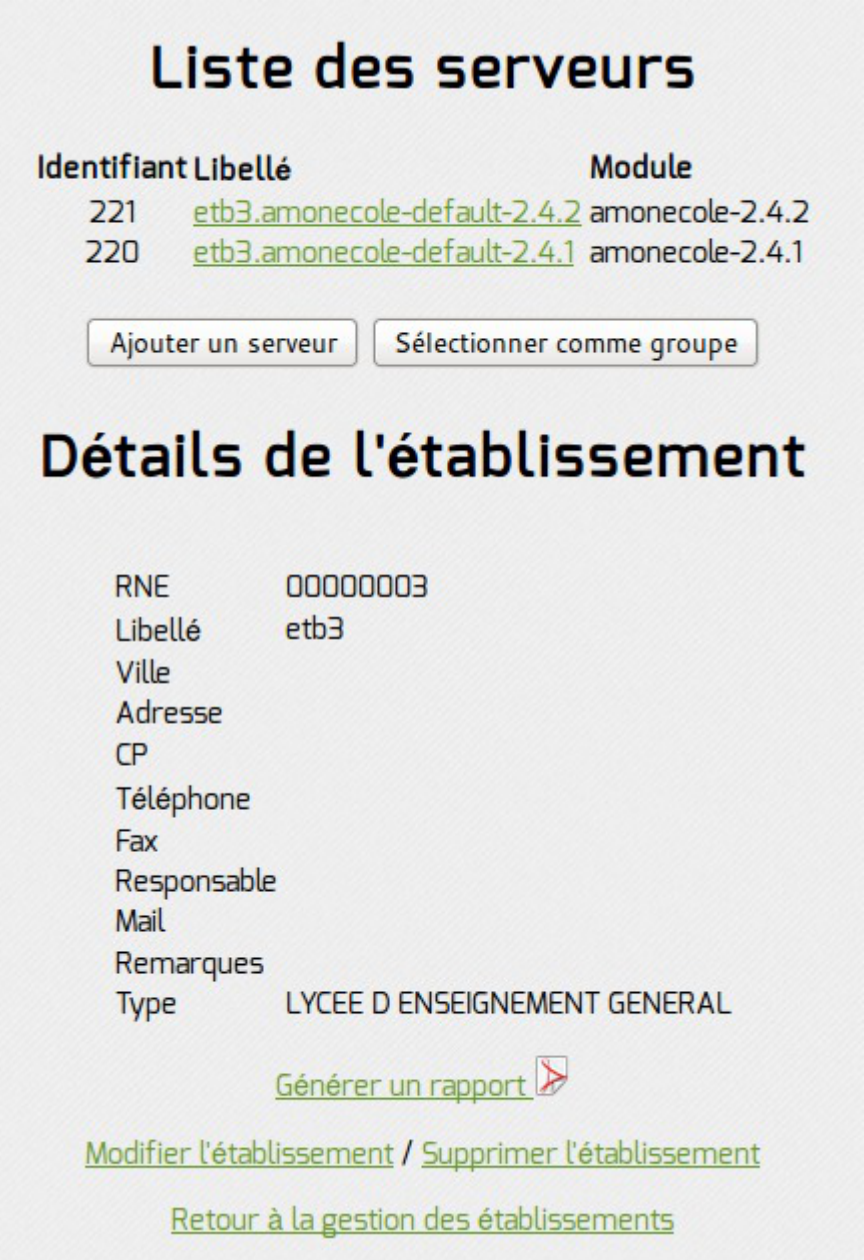
Serveurs d'un établissement

On accède aux serveurs d'un établissement à partir de la page d'affichage de l'établissement considéré.

4.1.2. Ajouter un serveur

L'ajout d'un serveur s'effectue à partir de la page d'affichage de l'établissement auquel le serveur est rattaché.

Se rendre sur la page de gestion des établissements, filtrer à l'aide du formulaire les établissements afin d'obtenir l'établissement auquel le serveur est rattaché.



Cliquer sur le bouton `Ajouter un serveur` et choisir le module EOLE associé au nouveau serveur.

Puis renseigner les paramètres permettant de décrire le serveur.

Le `Délai entre 2 connexions` correspond à l'intervalle entre deux connexions du serveur sur le Zéphir.

Il est possible de créer directement le serveur depuis la commande `enregistrement zephir` (nécessite les droits d'enregistrement et/ou d'écriture).

4.1.2.a. Configurer un serveur

Après avoir ajouté le serveur, il faut renseigner sa configuration. Pour cela, se rendre sur la page `état actuel` du serveur et cliquer sur `générer`. L'outil propose des fonctionnalités équivalentes à celles de la procédure locale `gen_config`.

Cela permet de préparer à l'avance la configuration du serveur.

Une fois le fichier enregistré, ou si celui ci a été remonté depuis un serveur réel les options suivantes sont disponibles :

- `générer` : saisir à nouveau la configuration en partant des valeurs par défaut ;
- `modifier` : rééditer la configuration déjà présente ;
- `télécharger` : récupérer le fichier de configuration du serveur sur votre poste de travail.

L'utilisation d'une variante permet de personnaliser les valeurs par défaut (il est aussi possible de les définir au niveau d'un module).

Voir aussi...

Configuration en mode Zéphir

L'état du serveur [p.123]

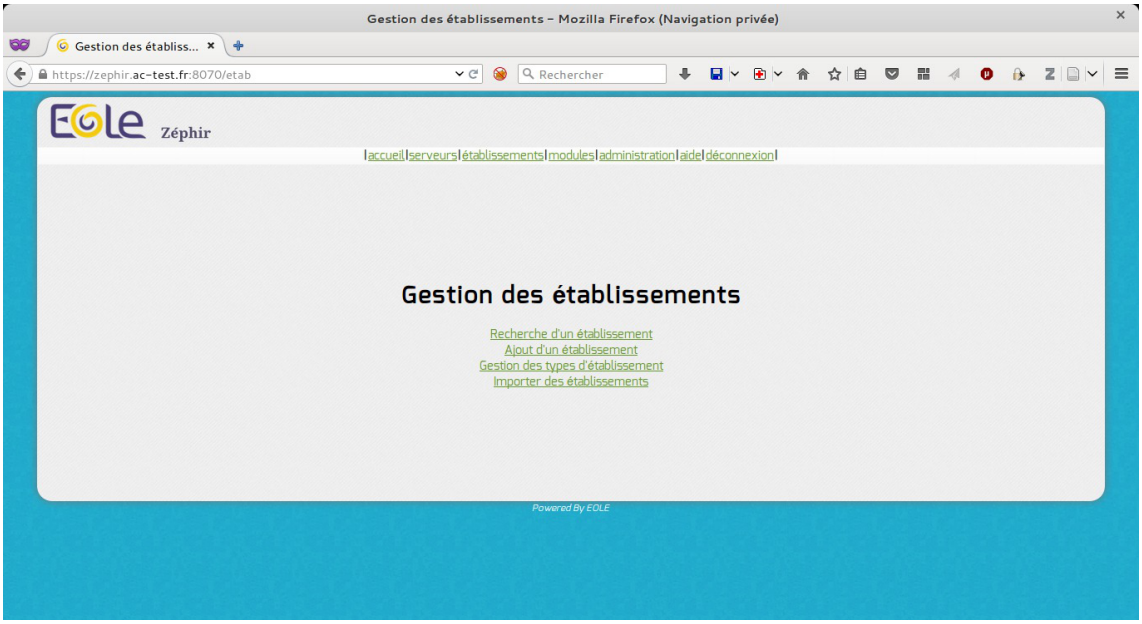
4.2. Enregistrement d'un serveur

Pré-requis

L'établissement d'appartenance du serveur doit déjà exister dans la base des serveurs.

Enregistrement d'un établissement

Pour ajouter un établissement il faut se rendre dans l'application Zéphir et cliquer sur l'entrée `établissement` du menu.

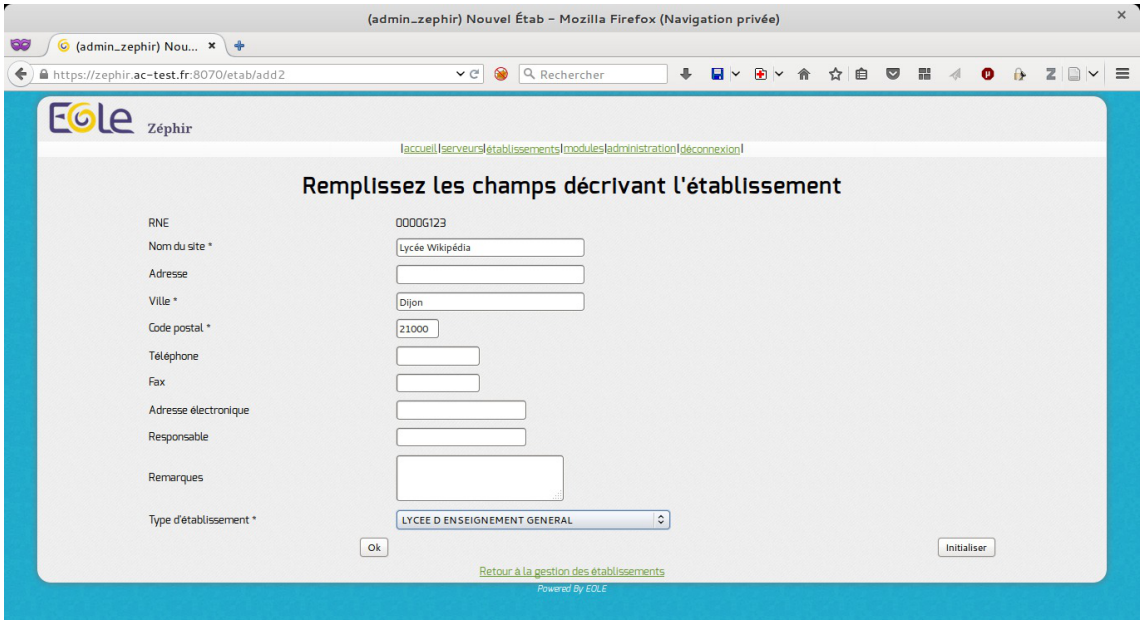


Puis cliquer sur `Ajout d'un établissement`.

L'identifiant à saisir correspond au RNE de l'établissement (8 caractères maximum).

Le RNE est la seule information que l'on ne pourra pas modifier. Il faut donc prendre garde à saisir le bon numéro. En cas d'erreur, la seule solution sera de supprimer l'établissement fraîchement créé et le recréer.

Il faut ensuite renseigner la description de l'établissement (adresse physique, moyens de communication, ...).



Seuls les champs pourvus d'une `*` sont obligatoires (nom du site, ville, code postal et type d'établissement). Des types d'établissement peuvent être ajoutés dans établissement / Gestion des types d'établissement mais il faut le faire avant d'ajouter un nouvel établissement. Un fois validé avec le bouton OK, l'établissement est créé.

Enregistrement d'un lot d'établissements

Il est possible d'importer un fichier texte comprenant la liste des établissements depuis l'application web Zéphir.

Pour cela il faut cliquer sur le menu établissements et choisir Importer des établissements.

L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese[p.234]) CSV[p.231] avec comme séparateur un "|".

Les champs suivants sont attendus :

```
1 RNE|LIBELLE CODE NATURE|CODE NATURE|LIBELLE ETAB|NOM ETAB|CODE
  POSTAL|LOCALITE|MAIL|FAX|TEL
```

```
1
  210024M|CLG|340|COLLEGE|CHAMPOLLION|21000|DIJON|ce.0210024M@ac-dijon.fr|0380732
2
  0210026P|CLG|340|COLLEGE|EPIREY|21000|DIJON|ce.0210026P@ac-dijon.fr|0380732916|
```

Après l'importation un rapport est affiché.

L'enregistrement

La procédure d'enregistrement est requise pour tous les serveurs à administrer avec Zéphir. Elle permet

de créer les données nécessaires dans la base de données et de configurer la transmission sécurisée entre Zéphir et le serveur. L'enregistrement est effectué manuellement sur le module avec la commande `enregistrement_zephir`.

Configuration minimale du réseau

Si le réseau n'est pas paramétré sur le module il est possible d'appeler manuellement le script `network_zephir` pour une mise en place rapide.

```
root@eolebase:~# network_zephir
interface connectée sur l'extérieur (eth0 par défaut) :
adresse_ip eth0 : 192.168.240.100
masque de réseau pour eth0 : 255.255.255.0
adresse de la passerelle : 192.168.240.254
adresse du serveur DNS (ou rien) : 192.168.240.1
root@scribe:~#
```

Pour obtenir de l'aide sur la commande il faut utiliser `--help` :

```
root@eolebase:~# network_zephir --help
Usage: network_zephir [OPTION]
Procédure de configuration minimum d'un réseau
Options facultatives disponibles:
-p, --pppoe Si le réseau n'est pas encore configuré, cette option permet la mise en place d'une connexion par pppoe
```

Si le réseau n'est pas paramétré sur le module à enregistrer et que vous n'avez pas appelé manuellement le script `network_zephir`, sa configuration vous sera proposée par le script `enregistrement_zephir` :

voulez-vous établir une configuration réseau minimale (O/N), répondre `oui` à la question ;

Si vous voulez enregistrer le serveur depuis une connexion PPPoE, il est nécessaire de lancer enregistrement_zephir avec l'option `--pppoe`.

S'il faut une configuration réseau particulière au moment de l'enregistrement, lancer la commande enregistrement_zephir avec l'option `--force`.

Déroulement de l'enregistrement

- saisir l'adresse du serveur Zéphir, ainsi qu'un nom d'utilisateur et un mot de passe autorisé en écriture dans l'application web Zéphir ;
- si le serveur n'a pas été pré-créé sur le serveur Zéphir, répondre `oui` à la question Créer le serveur dans la base Zéphir ? ;
- saisir le numéro RNE qui doit au préalable exister dans l'application Zéphir ;

- saisir le libellé du serveur ;
- répondre aux diverses questions sur le matériel ;
- répondre aux diverses questions sur l'installateur ;
- choisir un module et une variante dans les listes proposées ;
- synchronisation de la configuration :
  - si la configuration a été faite en mode autonome sur le module à enregistrer choisir `Sauver la configuration actuelle sur Zephir`
  - si la configuration a été réalisé sur le serveur Zéphir choisir `Récupérer les fichiers de variante sur Zéphir`
- un message indiquera que la configuration est bien sauvegardée et que les communications avec Zéphir sont configurées. Dans le cas où des paramètres du serveur ne seraient pas renseignés (paramètres provenant d'une variante), un message vous préviendra que ceux-ci doivent être saisis.

Un numéro sera indiqué (id du serveur) à la fin de la procédure d'enregistrement. Ce numéro permettra d'accéder directement aux informations de ce serveur dans l'application web Zéphir.

Exemple de l'enregistrement d'un serveur déjà instancié :

```
root@eolebase:~# enregistrement_zephir
Procédure d'enregistrement sur le serveur Zéphir
Entrez l'adresse du serveur Zéphir : 192.168.240.254
Entrez votre login pour l'application Zéphir (rien pour sortir) : admin_zephir
Mot de passe pour l'application Zéphir pour admin_zephir :
```

Saisir l'adresse du serveur Zéphir, le compte et le mot de passe pour l'application Zéphir.

```
créer le serveur dans la base du serveur Zéphir (O/N) : o
```

Le script détecte que le module n'a jamais été enregistré et demande si vous souhaitez le créer.

```
Etablissement du serveur (n° RNE) (0000G123 par défaut) :
libellé du serveur (eolebase Lycée de Dijon par défaut) :
matériel (Bochs () par défaut) :
processeur ( QEMU Virtual CPU version 1.0 2294 MHz par défaut) :
disque dur (43 Go par défaut) :
nom de l'installateur (admin_zephir par défaut) :
telephone de l'installateur :
commentaires :
Délai entre deux connexions à zephir
minutes (30 par défaut) :
** liste des modules disponibles **
```

```
47 amon-2.4
46 eolebase-2.4
42 horus-2.4
45 scribe-2.4
43 sentinelle-2.4
44 sphynx-2.4
48 thot-2.4
module (eolebase-2.4 par défaut):
** liste des variantes de ce module **
45 * standard
variante (45 par défaut):
```

Ici les paramètres proposés par défaut sont validés par un retour chariot.

```
** Configuration des communications vers le serveur Zéphir **
1 -> Ne rien faire
2 -> Récupérer les fichiers de variante sur le serveur Zéphir
3 -> Sauver la configuration actuelle sur le serveur Zéphir
4 -> Modifier la variante du serveur
Entrez le numéro de votre choix : 3
```

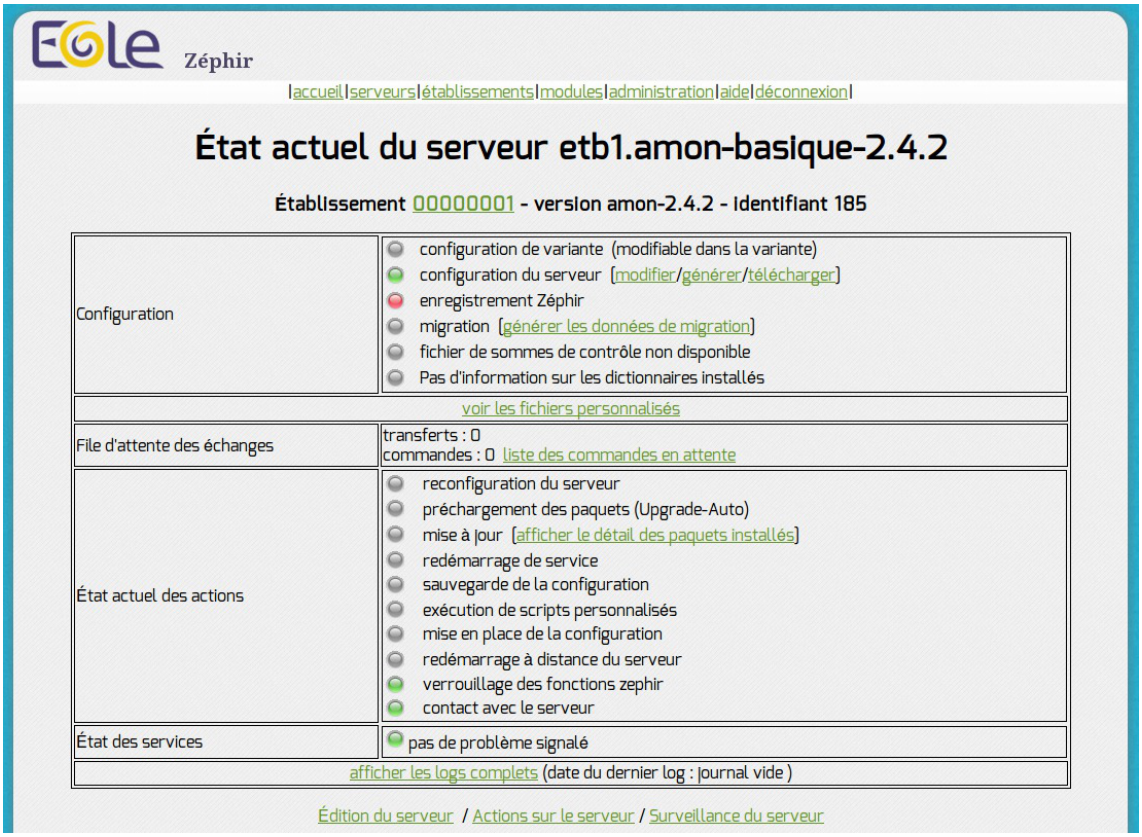
Pour l'enregistrement il faut choisir l'option 3.

```
-- sauvegarde en cours (veuillez patienter) --
-- OK --
--récupération des patchs et dictionnaires (veuillez patienter)--
** le numéro attribué à ce serveur sur le serveur Zéphir est : 1
**
root@eolebase:~#
```

Le module est correctement enregistré sur le serveur Zéphir.

4.3. L'état du serveur

Cette page permet d'afficher l'état du serveur mais donne également accès aux actions possibles sur le serveur sélectionné.



Lorsque des actions sont effectuées sur un serveur, des journaux remontent sur le serveur Zéphir et les voyants dans la page d'état du serveur sont mis à jour suivant le code couleur suivant :

- vert : ok ;
- jaune : en cours ;
- rouge : erreur.

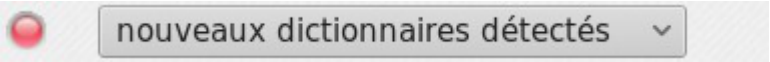
Configuration

- configuration de variante : l'utilisation d'une variante permet de personnaliser les valeurs par défaut (il est aussi possible de les définir au niveau d'un module)
- configuration du serveur

  Une fois le fichier enregistré, ou si celui-ci a été remonté depuis un serveur réel les options suivantes sont disponibles :

  - `générer` : saisir à nouveau la configuration en partant des valeurs par défaut ;
  - `modifier` : rééditer la configuration déjà présente ;
  - `télécharger` : récupérer le fichier de configuration du serveur sur votre poste de travail.
- enregistrement Zéphir : montre si le serveur déclaré dans Zéphir est enregistré ou non
- fichier de sommes de contrôle non disponible : si le voyant est rouge, une liste montre un certain nombre de fichiers qui ne sont pas en adéquation entre le serveur et Zéphir (modifié sur le serveur mais non remonté ou modifié sur Zéphir mais non envoyé au serveur, patch non remonté, configuration EAD : Bareos, politique de filtrage...)

- Pas d'information sur les dictionnaires installés : si le voyant est rouge, une liste montre un certain nombre de dictionnaires qui ne sont pas en adéquation entre le serveur et Zéphir (modifié sur le serveur mais non remonté ou modifié sur Zéphir mais non envoyé au serveur, création d'un dictionnaire local)



En production la diode devrait toujours être verte, sinon il y a des risques d'écrasement des personnalisations utilisateurs.

Le lien `voir les fichiers personnalisés` permet d'accéder au formulaire de personnalisation du serveur.

Des informations spécifiques à certains modules peuvent apparaître :

- `configurations RVP` pour le module Sphynx ;
- `configurations de réplication` pour le module Seshat ;
- ...

File d'attente des échanges

- transfert : affiche le nombre de transferts en attente pour le serveur
- commandes : affiche le nombre d'actions en attentes d'exécution pour le serveur

État actuel des actions

- reconfiguration du serveur
- préchargement des paquets (Upgrade-Auto)
- mise à jour : mise à jour disponibles ou non
- redémarrage de service
- sauvegarde de la configuration finie] sauvegarde de la configuration : sauvegarde terminée sans erreur
- exécution de scripts personnalisés
- mise en place de la configuration : état de la configuration
- redémarrage à distance du serveur : redémarrage en cours
- verrouillage des fonctions zephir : Zéphir est actif sur ce serveur
- contact avec le serveur : en contact ou non

État des services d'un serveur

Si un problème est détecté sur un serveur, celui-ci est affiché en rouge dans l'application Zéphir. Le

tableau de bord détaillé permet de diagnostiquer le problème. Le système de diodes permet de voir les services qui ne fonctionnent pas correctement.

Voir aussi...

Les variantes [p.167]

Personnalisation d'un serveur [p.132]

Fonctions spécifiques à certains modules [p.182]

État des services / état système [p.152]

4.4. Actions sur un serveur

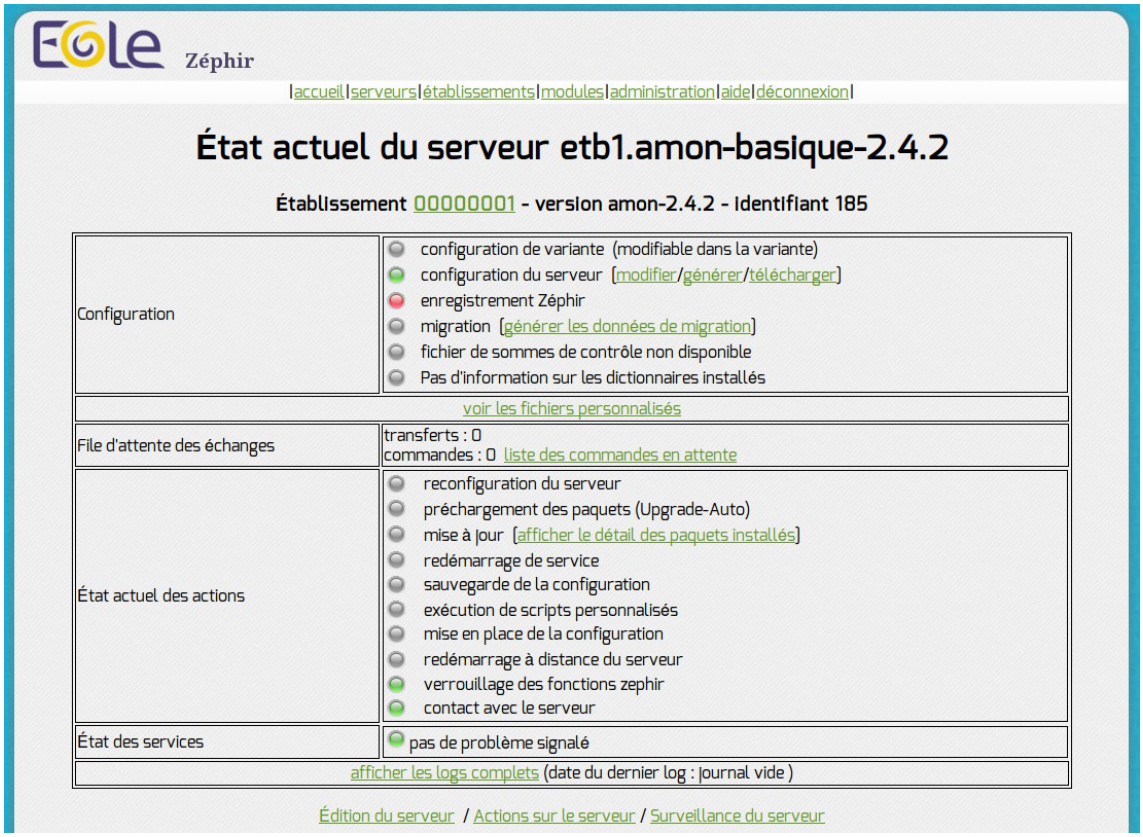
4.4.1. Généralités sur les actions

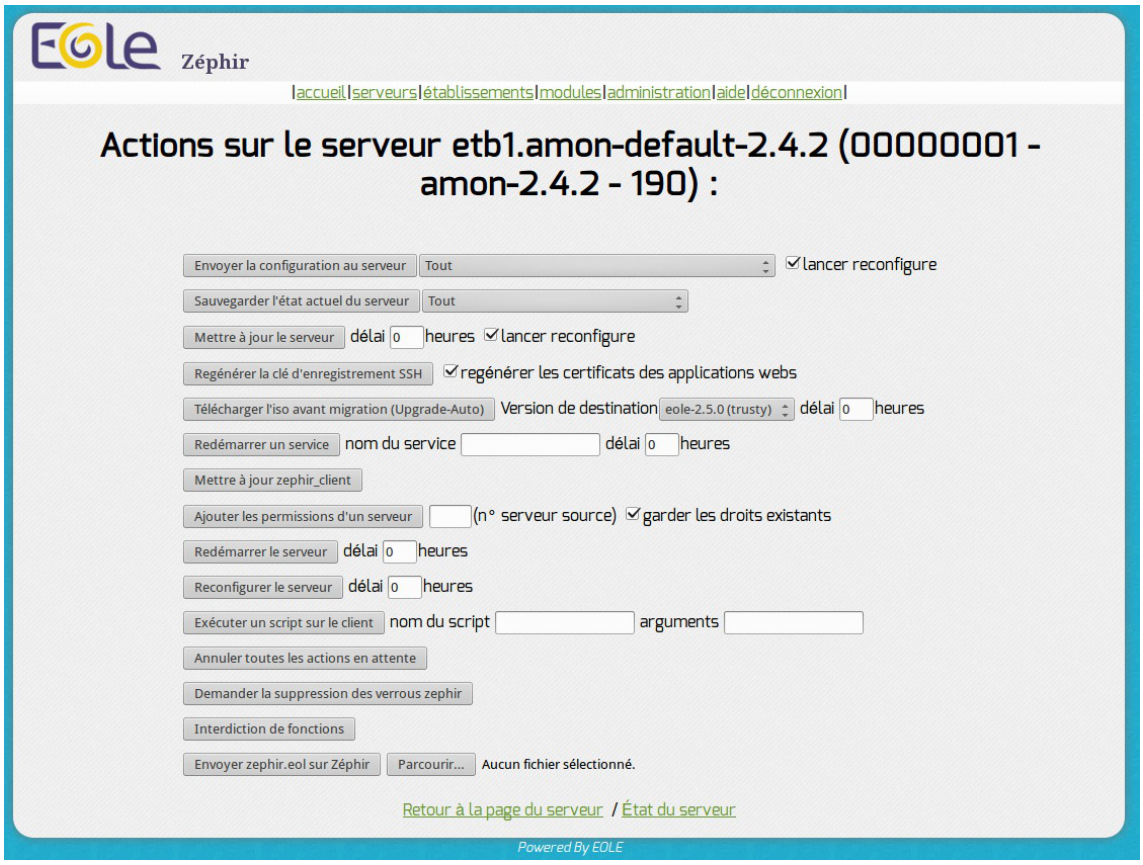
L'application Zéphir permet d'agir à distance sur les serveurs par des actions. Les actions sont principalement regroupées dans la page `Actions` accessible depuis la page d'état de chaque serveur. Elles sont mises en file d'attente et sont exécutées à la connexion du serveur enregistré au serveur Zéphir.

Toutes les actions fonctionnent selon le principe suivant :

- préparation d'une archive si un envoi de fichier est nécessaire ;
- mise en file d'attente du fichier à envoyer ;
- mise en file d'attente de l'action à exécuter ;
- récupération des fichiers, puis exécution des commandes par le serveur lorsque celui-ci se connecte au serveur Zéphir.

À partir de la fiche d'état d'un serveur, cliquer sur Actions sur le serveur.





Liste des actions

La communication est toujours à l'initiative du serveur enregistré qui vient vérifier si il a des actions à effectuer lorsqu'il envoie ses statistiques de surveillance au serveur Zéphir. Vous pouvez annuler une action mise en attente tant que le serveur ne l'a pas récupérée, via le lien

> liste des commandes en attente de la page d'état du serveur.

Lorsque les actions sont effectuées, des journaux remontent sur le serveur Zéphir et les voyants dans la page d'état du serveur sont mis à jour suivant le code couleur suivant :

- vert : ok ;
- jaune : en cours ;
- rouge : erreur.

> Le serveur Zéphir ne fait pas de vérification sur l'enchaînement des actions que vous demandez, il faut donc veiller à rester cohérent (par exemple, ne pas demander une mise à jour suivie d'une reconfiguration, et un envoi de configuration en même temps).

4.4.2. Les actions possibles

Envoyer la configuration au serveur

Le bouton Envoyer la configuration au serveur permet de préparer le transfert des fichiers nécessaires à la configuration du serveur.

Si vous cochez ☑ lancer reconfigure après l'envoi, la commande reconfigure sera lancée sur le serveur après avoir mis en place les nouvelles données

Mise à jour

L'application Zéphir vous offre la possibilité de forcer la mise à jour d'un serveur (bouton mettre à jour le serveur). Le serveur en question se mettra à jour lors de sa prochaine connexion au serveur Zéphir. Il est possible de programmer le reconfigure en même temps.

Le bouton Mettre à jour zephir_client permet d'envoyer à un serveur enregistré la version de `zephir-client` disponible sur le serveur Zéphir.

Si le serveur possède une version plus récente du paquet `zephir-client`, elle sera conservée. Par la suite si une version plus récente est disponible en cas de mise à jour du serveur enregistré, la version envoyée sera écrasée .

Régénérer la clé d'enregistrement SSH

Cette action a été ajoutée suite à des problèmes de génération de certificats Debian / Ubuntu. Elle permet de régénérer les clefs SSH sur le client. Cette action n'a pas d'utilité sur des serveurs nouvellement installés.

Une case à cocher permet également de demander une régénération des certificats utilisés par les applications web (Apache / EAD / EoleSSO).

Redémarrer un service

Il est possible de redémarrer des services sur le serveur enregistré. Pour cela, il faut connaître le nom

exact du service à redémarrer.

Ajouter les permissions d'un serveur

Le bouton Ajouter les permissions d'un serveur permet de copier les permissions (droits Unix) définies sur les fichiers personnalisés d'un serveur existant (serveur source) vers le serveur sélectionné.

Si ☑ garder les droits existants est cochée, les permissions sont ajoutées à la liste des permissions actuelles, sinon seules les permissions copiées sont conservées.

Redémarrer le serveur

Cette action redémarrera le serveur la prochaine fois qu'il se connectera au serveur Zéphir.

Sauvegarder l'état actuel du serveur

Le bouton de sauvegarde des serveurs indique au serveur Zéphir qu'il doit sauvegarder la configuration actuelle d'un serveur (dictionnaires, patchs et templates personnalisés). Lors de la prochaine connexion de ce serveur, celui-ci créera une archive comportant toutes les données personnalisées et l'enverra au serveur Zéphir. Ces données seront alors prises en compte sur le serveur Zéphir.

En cas de problème sur un serveur sauvegardé, il vous suffira d'envoyer à nouveau la configuration sur celui-ci pour qu'il retrouve la dernière configuration sauvegardée.

Exécuter un script sur le client

Il est possible d'exécuter un script personnalisé sur le client.

Les paramètres à fournir sont le nom du script sans l'extension et ses éventuels paramètres.

Annuler toutes les actions en attente

Le bouton Annuler toutes les actions en attente permet de supprimer toutes les actions qui n'ont pas encore été exécutées.

Demander la suppression des verrous Zéphir

Lorsque certaines actions lancées par le serveur Zéphir se terminent mal, un verrou est positionné pour empêcher que d'autres actions ne soient lancées par la suite.

Pour supprimer ce verrou sans vous connecter sur le serveur (il est recommandé de vérifier l'état du serveur après une erreur sur des fonctions importantes comme la mise à jour, l'envoi de configuration, ...), cliquer sur Demander la suppression des verrous Zéphir. Le serveur concerné supprimera automatiquement les verrous lors de son prochain contact avec le serveur Zéphir.

Interdiction de fonctions

Vous pouvez interdire à un serveur (ou un groupe de serveurs) d'exécuter certaines fonctions. Actuellement, les fonctions qui peuvent être bloquées sont la reconfiguration et la mise à jour. Chaque fois que le serveur tentera de lancer une de ces procédures, il vérifie auprès du serveur Zéphir qu'il a le

droit de la lancer (si il n'arrive pas à joindre le serveur Zéphir, il conserve les dernières autorisations reçues).

Envoyer zephir.eol sur le serveur Zéphir

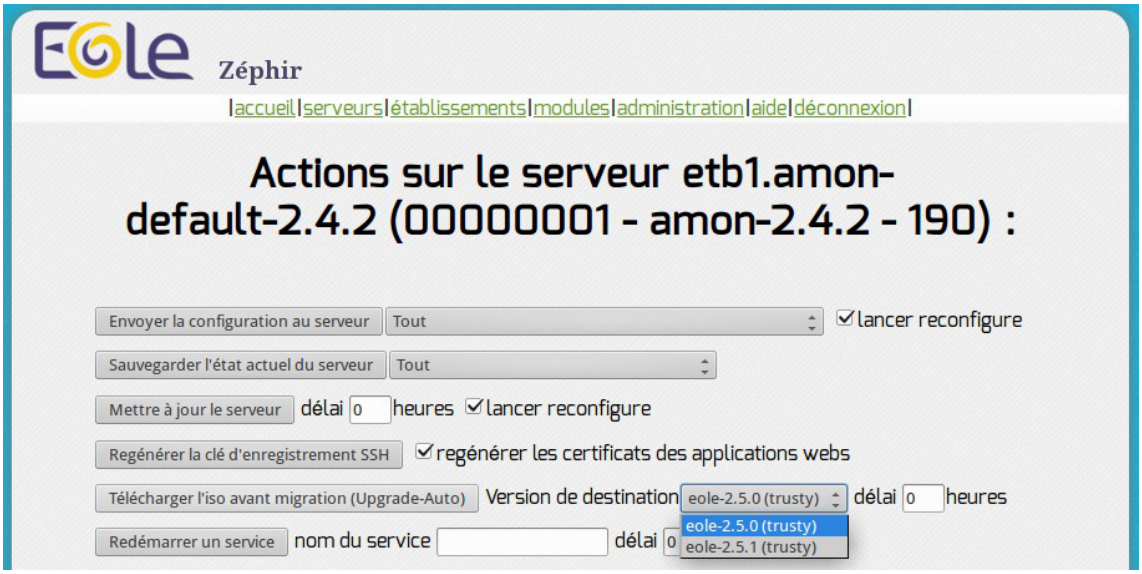
Il est possible d'envoyer un fichier de configuration pré-rempli sur le serveur Zéphir. Pour cela, appuyer sur le bouton `parcourir...` de la page d'action et rechercher le fichier que vous désirez envoyer dans votre arborescence locale. Ce fichier servira de fichier de configuration au serveur concerné (fichier `zephir.eol`).

> Cette fonctionnalité n'est pas indispensable, car la modification du fichier de configuration peut-être faite directement dans l'interface web par le formulaire de saisie. Utilisez cette procédure si vous avez généré des fichiers de configuration avec une autre application (ou si vous avez archivé la configuration de vos serveurs sur votre machine).
>
> Envoyer le fichier sur le serveur Zéphir ne suffit pas pour que les paramètres soient appliqués. Il faut penser à envoyer la configuration sur le serveur de destination.

Télécharger l'ISO avant migration (Upgrade-Auto)

Dans certains établissements, le débit n'est pas suffisant pour imaginer faire une migration rapide de plusieurs serveurs EOLE. Le bouton `Télécharger l'ISO avant migration (Upgrade-Auto)` permet de lancer à l'avance un téléchargement de l'image ISO (indépendamment de la procédure de migration) pour gagner en rapidité.

Il suffira ensuite d'utiliser la commande `Upgrade-Auto` sur le serveur pour lancer la migration.



> Cette option n'est proposée qu'à partir de la version 2.4.2, et seulement si il existe des versions supérieures de la distribution pour le serveur sélectionné.
>
> Dans le cas d'un groupe de serveurs, cette action est toujours disponible et peut proposer des versions inférieures ou égales à certains serveurs du groupe (au lancement de l'action, un message précisera sur quels serveurs l'action n'a pas pu être lancée).

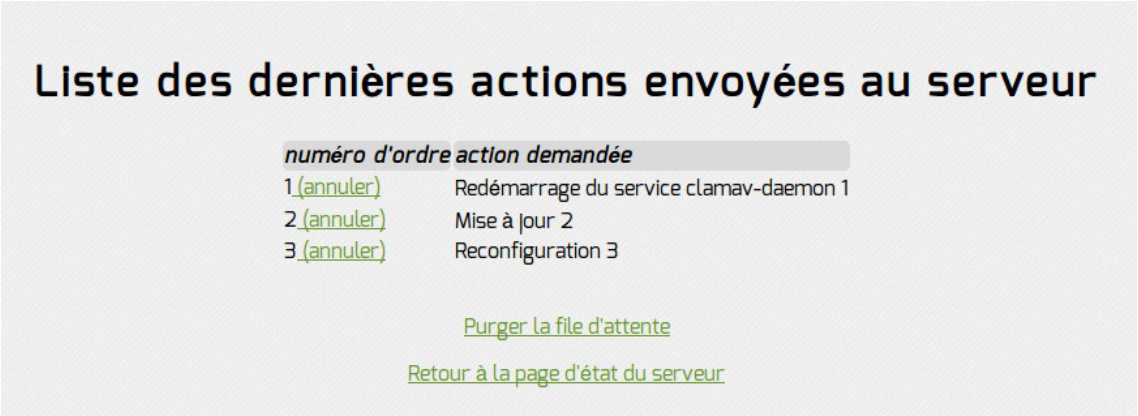
Purge des journaux (groupe de serveurs seulement)

Vous pouvez ici purger les journaux de l'application Zéphir (logs consultables depuis la page d'état du serveur). Vous pouvez spécifier des paramètres comme le type de journaux à purger, et une date limite (tous les logs antérieurs seront purgés).

Cela concerne uniquement les journaux de l'application et non les journaux locaux des serveurs (syslog, squid, ...).

Gestion de la file d'attente des actions

Les actions sont stockées dans une file d'attente, et ne sont exécutées que lorsque le serveur concerné se connecte au serveur Zéphir. Vous pouvez voir, pour chaque serveur, la liste des actions qui sont en attente d'exécution. Pour cela, utiliser la page État actuel du serveur concerné, et cliquer sur le lien liste des commandes en attente.



Liste des dernières actions envoyées au serveur

Cette page montre toutes les actions qui n'ont pas encore été envoyées au serveur. Il est possible d'annuler ces actions, soit en cliquant sur annuler à côté d'une action particulière, soit en cliquant sur Purger la file d'attente pour supprimer toutes les actions. Vous pouvez également supprimer toutes les actions d'un groupe de serveurs depuis la page d'action sur le groupe.

Le temps d'attente est défini dans la page de configuration du serveur. Pour lancer les actions aussitôt, il faut se connecter en `root` sur le serveur cible et utiliser la commande `synchro zephir` .

Actions disponibles seulement sur le groupe :

- modifier un paramètre sur un groupe permet de modifier :
  - une valeur de configuration sur un groupe entier (seulement les variables communes à tous les serveurs du groupe) ;
  - le délai de connexion des serveurs ;
  - la liste des alertes activées sur tous les serveurs.
- supprimer les permissions : permet de virer des permissions sur les fichiers personnels pour tout le groupe.

Voir aussi...

Personnalisation d'un serveur [p.132]

Ajout de scripts personnalisés [p.134]

4.5. Personnalisation d'un serveur

4.5.1. Gestion des modifications personnelles

En fonction du module et en dehors du fichier `zephir.eol`, un certain nombre de fichiers du serveur sont sauvegardés sur le serveur Zéphir.

La liste de ces fichiers apparaît sur la page `Liste des fichiers personnalisés` accessible depuis la page d'état des serveurs de l'application web Zéphir par le lien `voir les fichiers personnalisés` .

Les fichiers sauvegardés sont les suivants :

- les dictionnaires additionnels installés sur le serveur (fichiers `.xml` situés dans `/usr/share/eole/creole/dicos/`) ;
- les fichiers situés dans `/etc/eole/` qui apparaissent dans les listes de fichiers des dictionnaires locaux ;
- des fichiers spécifiques à chaque module (exemple : les fichiers générés par l'EAD) ;
- des fichiers spécifiques à une variante du module ;
- les patchs situés dans `/usr/share/eole/creole/patch/` ;
- des paquets additionnels (si disponibles sur le serveur de mise à jour).

Ajout de fonctions Creole pour des dictionnaires personnalisés

Si vous créez des fonctions Creole supplémentaires pour les utiliser dans des dictionnaires personnalisés, pensez que celles-ci doivent être disponibles sur le serveur Zéphir lui-même. La méthode à suivre dans ce cas est la suivante :

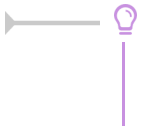
- pour des serveurs de version inférieure à 2.4, mettre le fichiers de fonction dans le répertoire `/usr/share/creole/funcs_creole2/` du serveur Zéphir (le créer si besoin) ;
- pour des serveurs en version 2.4 et supérieure , utiliser le répertoire `/usr/share/creole/funcs/` (le créer si besoin) ;
- redémarrer les services `zephir` et `zephir_web` ou reconfigurer le serveur ;
- ajouter le fichier de fonctions sur les différents serveurs par l'intermédiaire de Zéphir web :
  - page d'état du serveur → `voir les fichiers personnalisés` → `fichiers divers` ;
  - importer le fichier de fonctions par l'intermédiaire du bouton Parcourir, et choisir `/usr/share/creole/funcs/<nom_fichier>.py` comme destination ;
  - utiliser l'action envoi de configuration pour diffuser les fichiers sur le serveur : page d'état du serveur → `Actions sur le serveur` → `Envoyer la configuration au serveur`.
- Il est également possible d'effectuer cette modification au niveau d'une variante pour l'appliquer à plusieurs serveurs ;
- éditer la configuration d'un serveur concerné pour vérifier le fonctionnement.

4.5.2. Modification unique sur un serveur

Si vous souhaitez faire des modifications sur un serveur sans en faire une variante (vous ne pourrez pas réutiliser ces modifications sur d'autres serveurs), suivre la même procédure, mais laissez les patchs dans `/usr/share/eole/creole/patch/` et les dictionnaires locaux dans `/usr/share/eole/creole/dicos/`.

Vous devez ajouter le nom des fichiers et des paquets supplémentaires dans le fichier `/usr/share/zephir/zephir_conf/fichiers_zephir`.

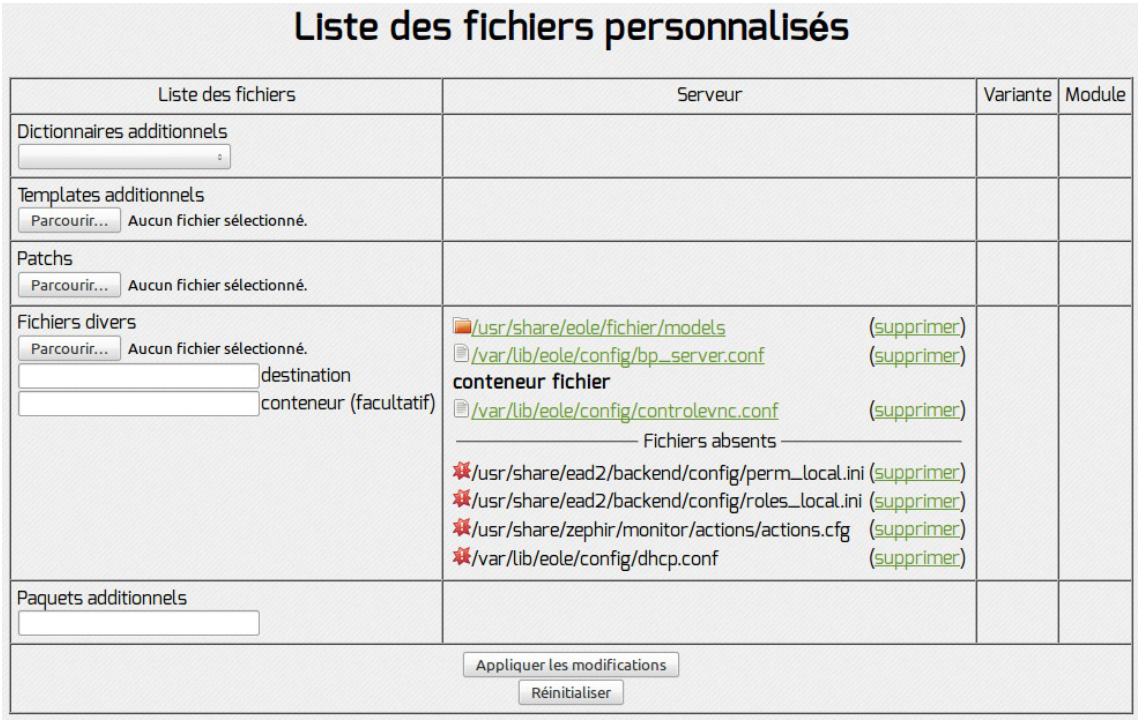
Les modifications seront ainsi sauvegardées sur le serveur Zéphir.



Pour remonter les fichiers sur le serveur Zéphir, lancer le script `/usr/share/zephir/scripts/zephir_client save_files` sur le serveur enregistré.

4.5.3. Gestion des permissions

Il se peut que les fichiers sauvegardés sur le serveur Zéphir (ou mis en place par l'application web Zéphir) n'aient pas les droits voulus une fois envoyés sur le serveur Amon. Il est possible de forcer l'application de droits pour les fichiers divers et les templates additionnels (fichiers liés aux dictionnaires additionnels). Cela peut aussi être utile dans le cas ou un utilisateur système n'a pas le même UID sur tous les serveurs de destination (dans le cadre d'une variante).



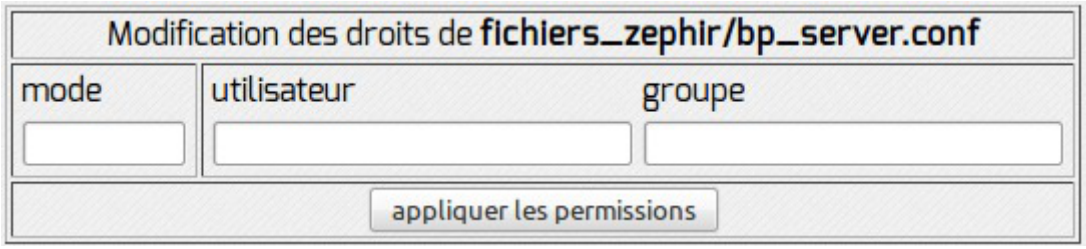
Liste des fichiers personnalisés

Pour définir des permissions sur un fichier ou répertoire, cliquez sur celui-ci pour aller dans la page d'édition du fichier. Le formulaire en haut de page permet de définir le mode du fichier (forme numérique), ainsi que l'utilisateur et le groupe.

La case à cocher ☑ récursif permet d'appliquer les options de propriété (pas le mode) récursivement, et n'a donc d'intérêt que dans le cas d'un répertoire. Les droits seront appliqués sur le serveur de destination au prochain envoi de configuration.

Dans la page des fichiers personnalisés, le lien `voir les permissions définies` permet de voir la liste des

permissions définies sur le serveur, et également de les supprimer.



Modification des droits du fichiers personnalisé

Ces fonctions sont disponibles de la même façon dans le cadre d'une variante, depuis la page de modification d'une variante.

Il existe deux fonctionnalités permettant de simplifier la mise en place des droits sur un groupe de serveurs. Celles-ci sont accessibles depuis la page d'action sur un groupe :

- supprimer des permissions affiche un résumé des fichiers pour lesquels les serveurs du groupe ont des permissions définies. Le lien `supprimer` permet de supprimer les permissions relatives à ce fichier sur tous les serveurs (tout supprimer supprime toutes les permissions définies sur ces serveurs) ;
- ajouter les permissions d'un serveur permet de copier toutes les permissions définies pour un serveur (serveur source) sur l'ensemble des serveurs du groupe (serveurs de destination). Si la case ☑ garder les droits existants est cochée, les permissions définies sur les serveurs de destination ne seront pas écrasées par celles du serveur source.

4.5.4. Ajout de scripts personnalisés

Les scripts personnalisés doivent obligatoirement avoir l'extension `.zephir` et être placés sur le serveur client dans le répertoire : `/usr/share/zephir/scripts/`.

Pour placer le script au bon endroit, vous pouvez utiliser le mécanisme de variante.

Ce script peut être inséré dans les fichiers divers d'un serveur avec pour destination : `/usr/share/zephir/scripts/test_perso.zephir`.

Il ne fait rien de particulier mais peut servir de base pour utiliser les mécanismes de log et de remontée d'état.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
##############################################################################
# Eole NG - 2007
# Copyright Pole de Competence Eole (Ministere Education - Academie Dijon)
# Licence CeCill cf /root/LicenceEole.txt
```

```
# eole@ac-dijon.fr
#
# test_perso.zephir
#
# exemple de script personnalisé pour le client zephir
#
#####################################################################
import os, sys
from zephir.lib_zephir import *
from creole import fonctionseole
if fonctionseole.init_proc('PERSO') == False:
    fonctionseole.zephir("MSG" , "procédure test perso bloquée par Zéphir", "PERSO")
    sys.exit(1)
fonctionseole.zephir("INIT" , "script test perso en cours d'execution", "PERSO")
try:
    message = sys.argv[1]
    fonctionseole.zephir("MSG" , "test perso lancé avec l'argument %s" % message, "PERSO")
except:
    fonctionseole.zephir("ERR" , "test perso lancé sans argument", "PERSO")
    exit(1)
if is_locked(['reconfigure']):
    fonctionseole.zephir("ERR" , "test perso stoppé : reconfigure en cours", "PERSO")
    exit(1)
else:
    fonctionseole.zephir("FIN" , "test perso : OK", "PERSO")
```

L'appel à la fonction `init_proc('PERSO')` permet de vérifier et de bloquer l'exécution de la procédure depuis l'application Zéphir. L'interdiction peut être faite depuis l'action interdiction de fonctions dans les actions du serveur.

Nous avons ajouté une catégorie `PERSO` qui peut être utilisée dans des scripts additionnels si besoin. La fonction Zéphir du module `fonctionseole` permet de faire remonter des informations au serveur Zéphir par l'intermédiaire de fichiers journaux. L'appel est fait sous la forme suivante :

```
fonctionseole.zephir(<etat>, <message>, <type>)
```

- `<etat>` indique au serveur Zéphir la finalité du message :
  - `INIT` pour indiquer le début d'une action ;

- `MSG` pour un message d'information ;
- `ERR` pour indiquer que l'action s'est mal terminée (suivant la valeur du champ type, le serveur peut passer en alerte dans Zéphir) ;
- `FIN` pour indiquer que l'action s'est terminée correctement.

- `<message>` est le message à afficher dans les logs du serveur ;
- `<type>` est un libellé qui permet au serveur Zéphir de classer les jounaux dans différentes catégories (par exemple `MAJ`, `RECONFIGURE`, ...).

  Pour les scripts personnalisés, il est recommandé d'utiliser le type `PERSO`.

Ces journaux sont envoyés en temps réel au serveur Zéphir (en cas d'erreur de connexion, ils sont stockés et réexpédiés après un retour à la normale). Ils sont également envoyés dans le fichier `syslog` sur la machine cliente avec le préfixe `zephir`.

Par exemple : `Apr 15 15:41:15 horus zephir: INSTANCE => FIN : Instanciation terminée`.

Le client Zéphir lance les scripts en tant qu'utilisateur `uucp`. Si des droits plus élevés sont nécessaires, il est possible d'utiliser la commande `sudo script` pour lancer un script avec des droits `root` :

```
from zephir.lib zephir import sudo script
sudo script('mon script.zephir')
```

Dans le cas d'ajout d'un nouveau script, il faut redémarrer le service `z_stats` pour que le script soit pris en compte par `sudoers`.

4.6. Actions automatiques des agents de surveillance

Nous avons ajouté la possibilité pour les agents de surveillance d'effectuer des actions en cas de changement d'état.

Il est possible de définir des actions pour tous les états en définissant des fonctions du type:

- `action_unknown` -> état de l'agent inconnu ;
- `action_ok` -> pas d'erreur ;
- `action_warn` -> avertissement détecté ;
- `action_error` -> erreur détectée ;
- `action_dependant` -> état non significatif du à un autre agent en erreur (exemple : état de l'agent de surveillance des imprimantes si l'agent cups est en erreur).

Ces actions seront exécutées chaque fois que l'agent en question passera à l'état correspondant.

Activer / désactiver des actions

Par défaut, les actions définies ne sont pas exécutées. Lorsqu'un agent change d'état il va faire les tests suivants pour savoir si il doit exécuter une action :

- une fonction doit être définie pour le nouvel état ;

- l'action doit être configurée comme active dans un fichier du répertoire `/usr/share/zephir/monitor/actions/`

3 fichier différents sont utilisés par ordre de priorité croissante :

- `actions_eole.cfg` : actions activées par défaut à l'installation (à ne pas modifier) ;
- `actions_acad.cfg` : actions activées(/désactivées) au **niveau académique** (par exemple). L'idéal est de le gérer dans une **variante** de Zéphir
- `actions.cfg` : idem au niveau de l'établissement (**spécifique au serveur**).

Par défaut, seul le fichier `actions_eole.cfg` est présent, et il active les actions de relance des services suivants :

- dns ;
- sshd ;
- e2guardian.

Les fichiers `actions_acad.cfg` et `actions.cfg` doivent être créés, ils sont de type .ini et la syntaxe est la suivante :

`[nom de l'agent]`

`nom de l'action=True` (False pour désactiver)

Les actions non définies sont considérées comme inactives

Exemple pour l'activation d'actions sur le passage en erreur et le retour à la normale pour SSH et PostgreSQL

```
[ssh]
action_error=True
action_ok=True
[postgresql]
action_error=True
action_ok=True
```

Ajout de nouvelles actions

Les actions sont définies dans un fichier `<nom_agent>.actions`.

Ces fichiers sont à placer dans le répertoire : `/usr/share/zephir/monitor/actions/`

Certaines actions sont proposées par défaut dans le sous-répertoire `eole` et peuvent servir d'exemple.

Ces fichiers doivent contenir des fonctions python dont le nom correspond à `action_<état>` (cf. paragraphes précédents). Si la fonction retourne un message, celui-ci sera journalisé sur le serveur Zéphir (journaux de type SURVEILLANCE), ou dans les journaux systèmes du serveur si il n'est pas enregistré sur le module Zéphir.

Les fonctions reçoivent automatiquement 3 arguments :

- une référence à l'objet agent (permet de récupérer son nom, sa description, ...) ;
- l'état précédent ;

- le nouvel état.

On peut imaginer les actions suivantes pour l'agent `vir` (détection des virus, présent sur les modules Scribe et Horus) :

- passage en avertissement (`action_warn`) : envoi d'un courrier électronique à l'administrateur réseau ;
- passage en erreur : blocage du poste client en cause ;
- retour à la normale : déblocage du poste si en erreur précédemment, rien si avertissement.

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-

def action_error(agent, old_status, new_status):
    """redémarre le service ipsec si il est en erreur
    """
    from os import system, path
    if path.isfile('/var/run/sshd.pid'):
        res = system('/etc/init.d/ssh restart')
        if res == 0:
            return "agent %s : service ssh relancé" % agent.name
        else:
            return "agent %s : erreur lors de la relance du service ssh" % agent.name
    else:
        return "agent %s : le service ssh est stoppé" % agent.name
```

Action de relance du service ssh, fichier /usr/share/zephir/monitor/actions/eole/ssh.actions (livré avec zephir-client)

Si vous utilisez des bibliothèques python non disponibles par défaut, importez-les à l'intérieur des fonctions et non en début de fichier.

Ces bibliothèques sont accessibles par défaut dans les fonctions :

- **librairie standard**

  gettext, locale, os (sys est disponible à travers os.sys), pwd, random, shutil
- **librairies eole**

  cfg : zephir.monitor.agentmanager.config
- **librairies twisted**

  utils : twisted.internet.utils

  static : twisted.web.static

  log : twisted.python.log (permet de journaliser dans le log des agents via log.msg())

  service : twisted.application.service

  internet : twisted.application.internet

  xmlrpc : twisted.web.xmlrpc

  util : twisted.web.util

  resource : twisted.web.resource

  server : twisted.web.server

Si une action non existante est configurée comme active au niveau d'un agent, l'agent journalisera le changement d'état dans le fichier `/var/log/zephir/agent.log` ou dans le fichier `/var/log/rsyslog/local/zephir_backend/zephir_backend.info.log` sur le serveur Zéphir).

Les actions ne sont exécutées qu'au changement d'état. Par exemple si un agent passe en erreur, l'action ne sera pas lancée à chaque mesure.

Pour l'instant seules quelques actions sont proposées par défaut, n'hésitez pas à nous proposer vos contributions en envoyant un courrier électronique à l'équipe Eole (**eole@ac-dijon.fr**).

Les actions présentes dans `/usr/share/zephir/monitor/actions` sont prioritaires sur les fonctions fournies par défaut (dans le sous répertoire `eole`). Cela permet de redéfinir les actions proposées si elles ne conviennent pas.

Ne modifiez pas les fichiers présents dans `eole`, car ils seront écrasés en cas de mise à jour.

4.7. Migration des serveurs enregistrés vers une nouvelle version de la distribution

4.7.1. Généralités sur la migration

Le serveur Zéphir prend en compte la migration des serveurs enregistrés lors du passage à une nouvelle version de la distribution (suivant les cas supportés). Le but est de conserver l'identifiant du serveur en mettant à jour les informations sur la machine et en changeant le nom du module. Il propose également des fonctions permettant de préparer les configurations des serveurs à migrer lorsque cela est nécessaire.

La migration des données applicatives des serveurs enregistrés n'est pas gérée par le serveur Zéphir. La migration réelle du serveur est gérée par des scripts spécifiques à chaque module (si disponible) :

- `Upgrade-Auto` et `Maj-Release` (dans le cas où le serveur peut être mis à niveau par mise à jour) ;
- Scripts spécifiques de sauvegarde / restauration si une réinstallation est nécessaire (ex : `migration25.sh`).

Une documentation spécifique est mise à disposition pour ces procédures lorsqu'elles deviennent disponibles.

Certaines données connues du serveur Zéphir (fichiers divers : voir le chapitre suivant pour les différents cas gérés) peuvent être récupérées automatiquement. Par contre, les modifications effectuées sur les serveurs (patchs, dictionnaires locaux, ...) doivent être mises à jour manuellement (en re-créant des variantes équivalentes pour la nouvelle version des modules).

La migration d'un serveur dans l'application Zéphir est effectuée lors de l'enregistrement d'un serveur réinstallé avec la nouvelle version sur son ancien identifiant ou en fin de procédure `Upgrade-Auto` (ou `Maj-Release`).

Lorsqu'un serveur est ré-enregistré, les clés de connexion de l'ancien serveur sont invalidées et les anciennes données sont sauvegardées dans un répertoire de sauvegarde (si nécessaire, éteindre

l'ancien serveur pour éviter qu'il remonte des journaux systèmes d'échec de surveillance).

Dans le cas d'une migration nécessitant une préparation de configuration (voir chapitre suivant), il est possible de revenir dans la configuration d'origine pour remettre l'ancien serveur en service.

Retour en arrière après migration

Dans la page de description du serveur dans l'application web Zéphir, un bouton `retour en version XXX` permet de remettre en place les données du module dans sa version précédente.

Cette manipulation entraîne la perte des modifications effectuées depuis le passage sur la nouvelle version (données éditées sur Zéphir, ou remontées sur Zéphir par le serveur). Il faut recommencer la procédure d'enregistrement pour migrer à nouveau le serveur.

Migration du serveur Zéphir

Le serveur Zéphir est le premier serveur à migrer lorsqu'une nouvelle version de la distribution est disponible.

Zéphir gère les serveurs dont la version est inférieure ou égale à sa propre version (à l'exception de Zéphir 2.3 qui gère jusqu'à la version 2.4.1)

Les procédures de migration de Zéphir gérées actuellement sont :

- Depuis Zéphir 2.3 vers Zéphir 2.5.x : Vérifier que le serveur est bien à jour en version stable, puis :
  - Lancer le script `sauvegarde.sh` et mettre de côté l'archive générée ;
  - Installer la version voulue de Zéphir et effectuer une mise à jour stable (de préférence, conserver l'ancienne machine temporairement en cas de soucis) ;
  - Mettre en place l'archive créée précédemment dans `/var/lib/zephir_backups` sur le nouveau serveur
  - Lancer `restauration.sh` ;
  - Éditer et sauvegarder la configuration avec `gen_config` et lancer `instance` (répondre non lorsqu'il est demandé de recréer les données).
- Depuis Zéphir 2.5.0/2.5.1 vers Zéphir 2.5.1/2.5.2 :
  - Utiliser le script `Maj-Release` pour effectuer la mise à niveau du serveur (La configuration de Zéphir sera adaptée automatiquement si besoin) ;
  - reconfigurer le serveur.

Migration des serveurs enregistrés auprès de Zéphir

À ce jour (Zéphir 2.5.2) :

- EOLE 2.2 : migration possible vers EOLE 2.3 / 2.4.X / 2.5.X. Elle nécessite une réinstallation et une préparation de la configuration des serveurs. Les variantes doivent être re-créées et adaptées dans la nouvelle version. La migration est effectuée par le script `migration<version>.sh`

- EOLE 2.3 : migration possible vers EOLE 2.4.X avec réinstallation ou sans (`migration24.sh` ou `Upgrade-Auto`), vers EOLE 2.5.X avec réinstallation (`migration25.sh`). Demande dans tous les cas une préparation de configuration et une refonte des variantes (changements importants dans la librairie Creole et le format des dictionnaires).
- EOLE 2.4.0 / 2.4.1 : Mise à niveau vers EOLE 2.4.X + 1 par la procédure `Upgrade-Auto` . Les variantes 2.4.X+1 peuvent être recopiées automatiquement depuis la version 2.4.X (voir chapitres suivants). Les configurations des serveurs sont adaptées automatiquement lors de la mise à niveau. Migration possible vers 2.5.X avec réinstallation en préparant les configurations (pour la migration des données, un script de migration est à l'étude).
- EOLE 2.4.2 : migration vers Eole 2.5.X par la procédure `Upgrade-Auto` . Les variantes doivent être recréées (ou copiées et adaptées) et les configurations préparées.
- EOLE 2.5.X : Mise à niveau vers la version 2.5.n+x par la procédure `Maj-Release` . Copie automatique des variantes entre 2 versions successives (chapitre suivant). Les configurations des serveurs sont adaptées automatiquement lors de la mise à niveau.

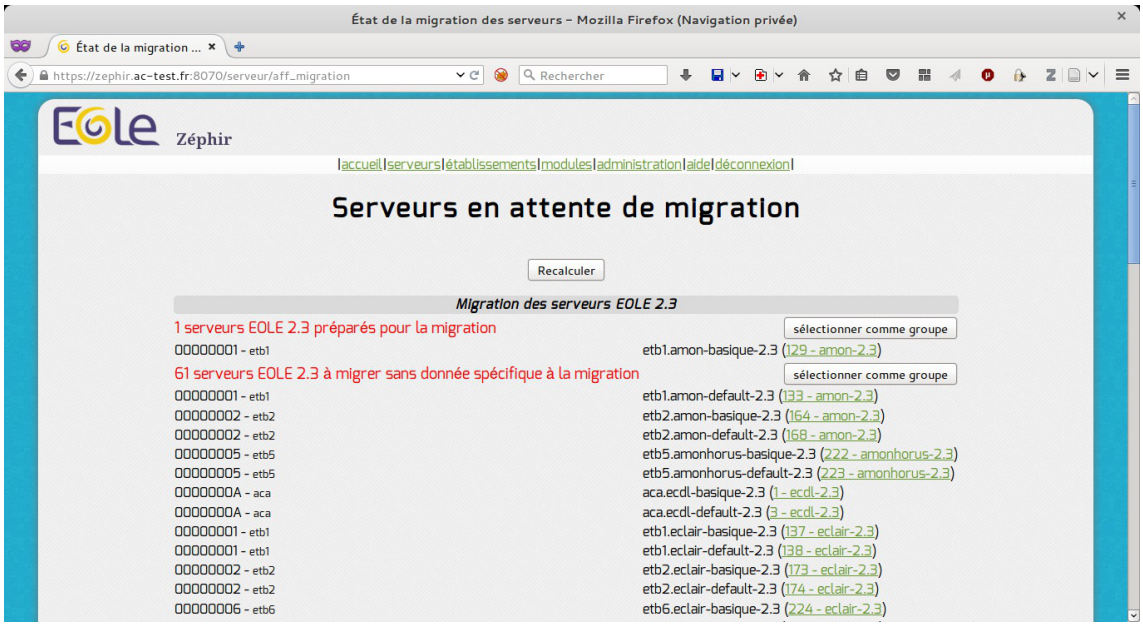
4.7.2. Préparation de la migration depuis l'application Zéphir

Page de suivi de la migration

Depuis la page d'accueil, un lien `suivi de la migration` affiche une page avec les informations suivantes pour chacune des version d'EOLE utilisée sur les serveurs :

- la liste des serveurs à migrer sans donnée spécifique à la migration ;
- la liste des serveurs préparés (dans l'application Zéphir) pour la migration.

Le bouton `sélectionner comme groupe` permet de créer un groupe contenant tous les serveurs de la liste.



Cette page concerne les migrations nécessitant de préparer la configuration des serveurs, pas les migrations entièrement automatisées (adaptation automatique du fichier de

> configuration par `Upgrade-Auto` sur la machine).

Préparation des variantes avant migration

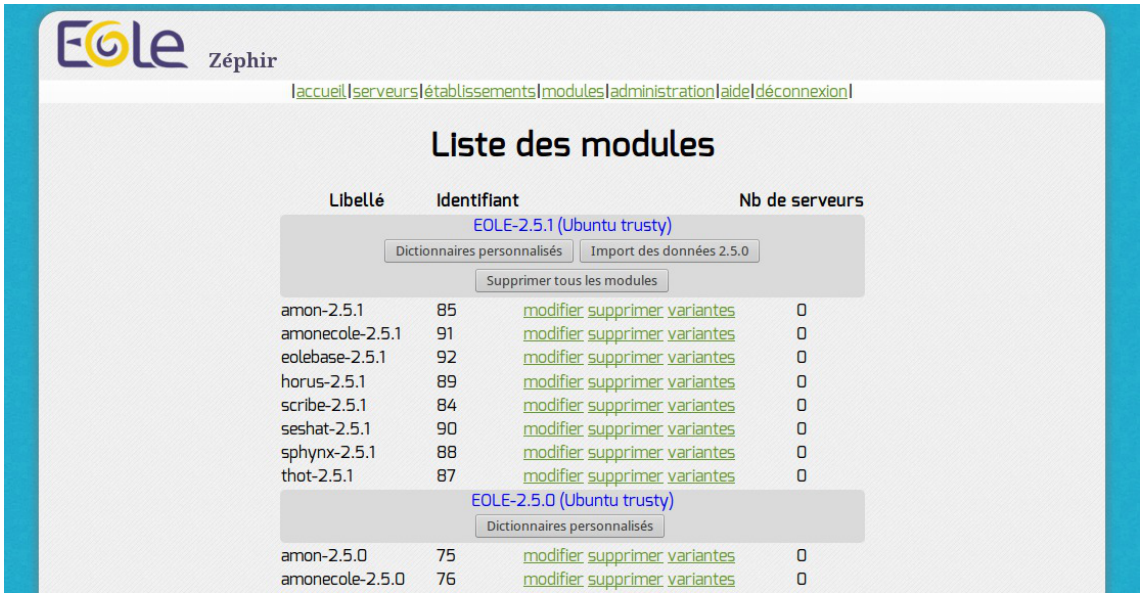
La première tâche à prendre en compte pour préparer la migration est l'adaptation des variantes dans la nouvelle version. Suivant la version, deux cas sont possibles :

- adaptations nécessaires : pour les modules dont la configuration n'est pas directement compatible, les variantes du nouveau module doivent être créées manuellement dans l'application (il est toujours possible d'utiliser la fonction de copie de variante, sans garantie sur la compatibilité des fichiers transférés)
- pour les modules compatibles d'une version à l'autre (versions mineures successives), un bouton `Import des données X` est présent au niveau du menu des modules (par exemple, `Import des données 2.4.1` pour la distribution 2.4.2).

Cette fonction va effectuer les actions suivantes :

- Les dictionnaires locaux de la version X sont recopiés si ils n'existent pas ;
- les variante n'existant pas (test sur le libellé) sont copiées et définies comme équivalentes (voir ci-dessous) ;
- les valeurs par défaut des modules X sont recopiées sur tous les modules ou aucune n'est définie.

En cas de lancement successif de cette fonction, seuls les dictionnaires / variantes et fichiers de valeurs non présents dans la nouvelle version sont pris en compte. Cela évite d'écraser d'éventuelles adaptations faites entre-temps sur les nouvelles variantes. Cela implique qu'en cas d'ajout d'un fichier dans une variante X-1 déjà copiée, il faudra faire manuellement l'ajout dans la version X de la variante.

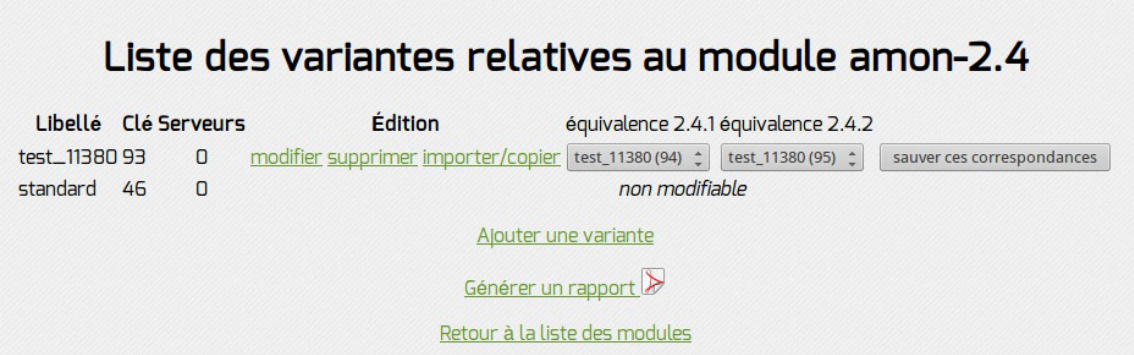


Équivalence des variantes entre deux versions

Zéphir propose une notion d'équivalence de variantes entre deux versions successives de la distribution EOLE. Lorsque deux variantes sont définies comme équivalentes, Zéphir sera capable de choisir automatiquement la variante à attribuer au serveur lors de la procédure Upgrade-Auto (et Maj-Release à partir de la version 2.5.0).

Les équivalences entre variantes peuvent être définies de deux façons :

- automatiquement, lorsque des variantes sont importées d'une version à l'autre de la distribution (voir ci-dessus). Dans ce cas, il est également possible de redéfinir manuellement ces équivalences.
- manuellement, en se rendant sur la page des variantes d'un module. Si la fonction est gérée pour cette version de la distribution, il sera possible de définir des équivalences pour chaque variante et chaque version de destination possible.



Dans le cas d'une migration nécessitant une préparation de configuration, la variante à utiliser dans la nouvelle version est choisie au moment de générer la configuration, les équivalences ne sont donc pas prises en compte dans ce cas.

Saut de plusieurs versions

Il est possible dans certains cas de faire un saut de plusieurs versions (par exemple, Upgrade-Auto de 2.4.0 vers 2.4.2).

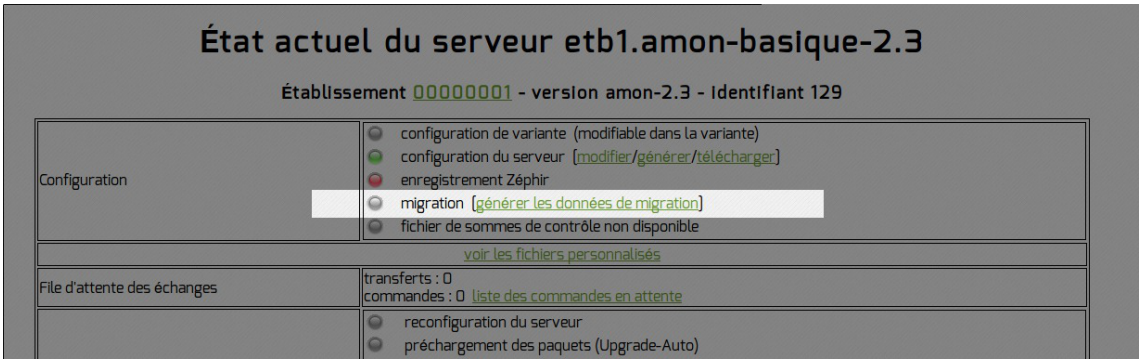
Dans ce cas, il faut renseigner manuellement les équivalences des variantes depuis la page

> des variantes du module d'origine (par exemple, la page des variantes du module Amon 2.4.0). Zéphir définit les correspondances automatiquement, mais seulement lors de l'import des données entre deux versions mineures successives.
>
> Cette étape est particulièrement importante si vous avez des variables supplémentaires définies dans des dictionnaires de variantes.

Générer une configuration de migration dans l'application web

Le serveur Zéphir permet de préparer à l'avance la configuration des serveurs à migrer. Cette fonction est disponible en cas de changement de version de la librairie Creole (nécessite d'adapter les dictionnaires personnalisés des variantes ou des serveurs), ou lorsque les fichiers de configuration sont trop différents pour être adaptés automatiquement d'une version à l'autre.

- sur la page d'état d'un serveur à migrer (amon-2.3 par exemple), cliquer sur le lien `générer les données de migration` ;

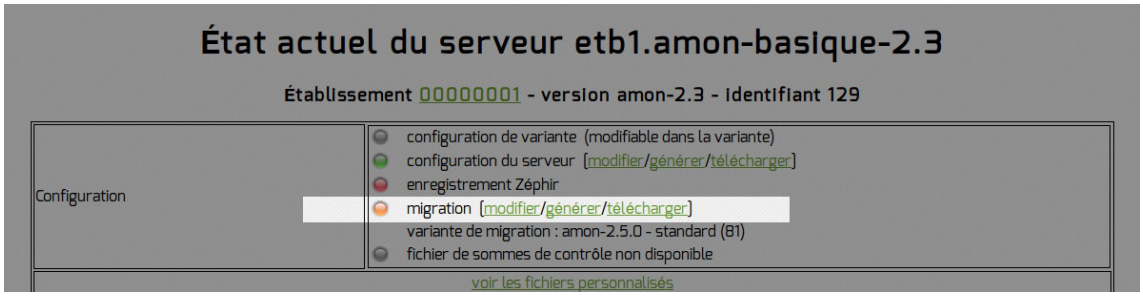


- dans la liste choisir la variante à utiliser lors de la migration du serveur et cliquer sur `Générer la configuration` ;

- pour les modules 2.4 et supérieurs, la saisie de configuration passe par l'interface de configuration du module qui a été intégrée au serveur Zéphir, le formulaire interne a été abandonné ;

- une fois tous les onglets renseignés, cliquez sur `Fichier` puis `Enregistrer la configuration`. Quitter l'interface de configuration du module. Un fichier `migration.eol` est alors enregistré dans le répertoire de données du serveur ainsi qu'un fichier `variante_migration` indiquant la variante sélectionnée.

Une fois la configuration enregistrée, vous pouvez choisir de modifier la configuration de migration ou de la re-générer en partant des valeurs par défaut (si vous voulez utiliser une autre variante par exemple). Les liens correspondants sont à coté du voyant migration en haut de la page d'état.



Cette étape de génération de configuration concerne seulement le fichier de configuration `config.eol` du serveur. Pour migrer les données applicatives (données de l'EAD, données des utilisateurs, ...), il faut passer par les scripts fournis pour sauvegarder/restaurer les données.

Si vous ne voulez pas passer par ces procédures, ou si vous avez des fichiers divers spécifiques à reprendre sur certains serveurs (hors variante) , il est possible de définir une liste de fichiers à conserver sur Zéphir d'une version à l'autre (voir chapitre suivant).

Migration automatisée de fichiers de type 'fichiers divers'

Lors de la migration d'un serveur dans l'application, `les fichiers divers` ne sont pas repris automatiquement, aux exceptions suivantes près :

- les fichiers définis par défaut pour chaque module (configuration EAD, options de filtrage sur le serveur Amon et partages personnalisés sur les serveurs Horus / Scribe) sont remontés depuis le serveur migré en fin de procédure. Ce sont les scripts de migration (`migrationXX.sh` ou `Upgrade-Auto`) qui se chargent de les restaurer sur la machine ;

- certains fichiers seront repris tels quels dans le répertoire du serveur sur le serveur Zéphir : configurations VPN sur sphynx / fichiers de réplication LDAP sur le module Seshat.

Pour d'autre cas (fichiers spécifiques à un serveur ou définis dans le fichier `fichiers_acad` d'une variante), il est possible de spécifier une liste de fichiers à remettre en place dans le répertoire `fichiers_zephir` du serveur après migration. Vous pouvez indiquer au serveur Zéphir la façon de les traiter en créant un fichier `/usr/share/zephir/migration_perso.py`. Les fichiers définis seront envoyés au serveur migré (avant la remontée des fichiers par défaut). Les données sont décrites sous la forme suivante :

```
# entête nécessaire pour que python sache comment traiter les accents
# -*- coding: UTF-8 -*-

# fichiers supplémentaires à transférer lors de la migration des données
migration_perso = {'amon-2.4':{'files':[('static-routes', 'static-routes', False)],
                               'rights':[('static-routes', '', 'root', 'root', '0755')],
                               'exclude':[],
                              },
                   'horus-2.4': ...
                  }
# liste des destinations à ajouter dans fichiers_zephir
destinations_perso = {'amon-2.4':['/etc/sysconfig/static-routes'],'horus-2.4':...}
```

exemple de migration d'un fichier static-routes vers amon-2.4

Le service `zephir` doit être relancé après ajout ou modification du fichier pour que celui-ci soit pris en compte.

La structure `migration_perso` décrit les fichiers à recopier dans le répertoire `fichiers_divers` après bascule sur la nouvelle version.

Le libellé complet du module de destination (nom-version) doit être spécifié, les fichiers pouvant ne plus être au même emplacement d'une version à l'autre de la distribution :

- `files` : source, destination, et booléen indiquant si le fichier doit être traduit de l'iso en utf-8 ;
- `rights` : fichier copié, options pour chmod / chown (par exemple, `-R` pour récursif), utilisateur, groupe, droits ;
- `exclude` : fichiers à exclure lors de la copie (utile si copie des répertoires entiers).

Les permissions définies dans la section `rights` sont automatiquement retranscrites dans le fichier `droits_zephir` du serveur (elles peuvent ensuite être modifiées / supprimées dans l'application web Zéphir si besoin). le chemin des fichiers source et destination sont donnés par rapport au répertoire `fichiers_zephir` du serveur sur le serveur Zéphir (pour référence : `/var/lib/zephir/conf/<id_etab>/<id_serveur>/fichiers_zephir/`)

- `destinations_perso` permet de renseigner la destination du fichier sur le serveur client. Cette liste de fichiers sera ajoutée dans le fichier `fichiers_zephir` du serveur (équivalent de la case `fichier de destination` dans la gestion des fichiers divers de l'application web Zéphir).

- Il est possible de mettre plusieurs entrées dans `migrations_perso` pour un même fichier de destination, seuls ceux retrouvés dans le répertoire du serveur seront recopiés (utile si un des fichier a changé de nom entre EOLE 2.3 et EOLE 2.4 par exemple).

- Pour les destinations, elles seront toujours ajoutées au fichier `fichiers_zephir`, même si le fichier n'est pas présent. Dans ce cas, le fichier sera listé dans la section `fichiers absents` des fichiers personnalisés du serveur. Si besoin, Il est possible de les supprimer manuellement depuis l'application web Zéphir une fois le serveur migré.

Automatisation de la génération des configurations de migration

Il est possible de passer par l'API (XMLRPC) de l'application Zéphir pour générer en mode *batch* les configurations de migration. En particulier, dans le cas où les serveurs à migrer possèdent des variables supplémentaires définies dans des variantes.

Un squelette de script a été mis à disposition sur le serveur Zéphir pour aider à la migration vers EOLE 2.4 (`/usr/share/zephir/utils/gen_migration_sample.py`).

Le fonctionnement est le suivant :

- le script lit un fichier CSV indiquant les numéros de serveurs à préparer et le numéro de variante à leur appliquer une fois migrés ;
- pour chaque serveur, Il génère une configuration équivalente à celle obtenue via la fonction `générer les données de migration` dans l'application web Zéphir ;
- il passe ensuite dans une fonction *update_conf*, qui reçoit en paramètre la configuration actuelle du serveur, la configuration de migration générée et la variante de destination.

C'est cette fonction qu'il convient d'adapter pour remplir les informations manquantes dans la configuration de migration (voir les commentaires et exemples dans le script pour plus de détails).

Pour faciliter ce travail, il peut être intéressant de générer manuellement une première configuration depuis l'application web Zéphir afin de repérer les éventuelles données manquantes.

Dans le cas d'une migration vers EOLE 2.4, la nouvelle application de saisie de configuration offre quelques fonctions intéressantes :

- dans la liste de choix du mode (basique / normal / expert), il est possible d'activer le mode *debug* pour voir le nom des variables ;
- en cliquant sur `fichier` -> `enregistrer la configuration`, un tableau récapitulatif présente toutes les variables obligatoires non renseignées.

Une variable `debug` est présente dans le script, et permet d'afficher les valeurs de la configuration de migration sans la sauvegarder réellement sur le serveur Zéphir.

Il est aussi possible d'importer les fonctions dans un shell python pour récupérer les objets de configuration et faire des essais de manipulation. se placer dans le répertoire ou se trouve le script et lancer l'invite python :

```
import gen_migration_sample
gen_migration_sample.debug = True
conf_actuelle, conf_migration = gen_migration_sample('nom_du_fichier_CSV')
```

Le script contient également quelques fonctions utilitaires pour comparer / récupérer et

assigner des valeurs aux variables.

4.7.3. Migration après réinstallation d'un serveur

Cette procédure correspond au cas où la migration est effectuée suite à la réinstallation d'un serveur client. Cela est nécessaire dans certain cas :

- lorsque la migration n'est pas prise en compte par la distribution Ubuntu, ou que des modifications structurantes du système de fichiers sont nécessaires (par exemple, migration depuis EOLE 2.2 vers EOLE 2.3 ou 2.4) ;
- en cas de remplacement du matériel.

L'étape de migration des données du serveur est effectuée par un script effectuant une sauvegarde / restauration spécifiques à la migration (exemple : script `migration24.sh` dans le cas d'une migration vers EOLE 2.4). Si le serveur n'a pas de données spécifiques à récupérer (ou uniquement des données gérées au niveau du serveur Zéphir), il est aussi possible de partir d'une installation vierge.

Une fois le serveur installé, la mise à jour du serveur dans l'application web Zéphir se fait par la procédure `enregistrement_zephir` :

- à la question `créer le serveur dans la base du serveur Zéphir ?` répondre `non` ;
- renseigner le numéro d'établissement (optionnel) et le n° identifiant l'ancien serveur ;
- un message d'avertissement indique que le serveur doit être migré dans l'application Zéphir, répondre `oui` ;
- différents cas sont possibles une fois arrivé au menu de finalisation :
  1. Une configuration a été préparée sur le serveur Zéphir (voir chapitres suivants) : utilisez le choix 2 → `Utiliser la configuration définie sur le serveur Zéphir`
  2. Aucune configuration n'est préparée, mais vous voulez récupérer des dictionnaires provenant d'une variante : modifier la variante (choix 4), puis utilisez le choix 2 → `Récupérer les fichiers de variante sur le serveur Zéphir` . Utiliser `gen_config` après l'enregistrement pour renseigner la configuration
  3. Vous avez généré la configuration (ou importé l'ancienne) avec l'outil `gen_config` local : utiliser le choix 3 → `Sauver la configuration actuelle sur le serveur Zéphir`
- si des fichiers divers ont été déclarés dans le fichier `migration_perso.py` (voir plus loin), répondez `oui` à la question `Voulez vous migrer ces données ?` ;
- dans le cas 1, suivez les instructions données en fin d'enregistrement pour instancier le serveur, dans les autres cas, lancez la procédure `instance` ;
- un fois le serveur instancié, lancer si besoin le script de restauration des données (ex : `migration24.sh`) pour restaurer les données de l'ancien serveur.

A la fin de la procédure de restauration des données (`migration24.sh`), une sauvegarde de configuration est lancée par le client Zéphir pour remonter d'éventuels fichiers restaurés (configuration EAD, configuration de filtrage locale, etc ...).

Si vous avez renseigné la configuration après l'enregistrement (cas 2) et que vous n'utilisez pas la restauration, pensez à effectuer l'une des deux actions suivantes après instance :

- lancer `/usr/share/zephir/scripts/zephir_client save_files` sur le serveur migré ;
- demander une sauvegarde de la configuration du serveur depuis l'application Zéphir.

4.7.4. Migration par mise à jour avec les procédure Upgrade-Auto / Maj-Release

Les procédures `Upgrade-Auto` et `Maj-Release` permettent de migrer un serveur existant vers une version supérieure sans réinstallation.

À partir d'Eole 2.4.2, `Upgrade-Auto` permet la migration entre 2 versions majeures d'EOLE, et `Maj-Release` entre 2 versions mineures (même version d'Ubuntu).

Cas gérés

`Upgrade-Auto` :

- Migration depuis EOLE 2.3 vers EOLE 2.4.X ;
- Migration entre deux versions d'EOLE 2.4 ;
- Migration d'Eole 2.4.2 vers 2.5.X.

`Maj-Release` :

- Remplace `Upgrade-Auto` pour la migration entre deux versions d'EOLE 2.5.

La version de l'outil Creole étant différente entre 2.3 et 2.4, cette migration nécessite une création manuelle des variantes dans la nouvelle version, et une génération de la configuration de migration pour chaque serveur (voir les chapitres précédents).

C'est également le cas pour chaque première version majeure de la distribution (Des différences importantes de version des logiciels de base pouvant impliquer des ajouts ou suppression de variables de configuration).

Le script `Upgrade-Auto` (ou `Maj-Release`) se charge de télécharger les nouveaux paquets et de mettre à jour le système vers sa nouvelle version.

Dans le cas d'un serveur enregistré sur les serveur Zéphir, la dernière étape de cette procédure consiste à mettre à jour les informations du serveur dans l'application Zéphir et à récupérer une éventuelle configuration préparée à l'avance sur le serveur Zéphir.

Le déroulement de cette étape est le suivant :

- saisie d'un compte valide (login / mot de passe) de l'application Zéphir.

  L'utilisateur doit avoir les droits suivants :

  - lecture ;
  - actions sur les clients (avec ou sans modification de configuration) ou enregistrement ;
  - écriture sur les serveurs et les modules (ou Migration de serveur + Ecriture (modules)).
- Si la configuration n'a pas été préparée à l'avance, la liste des variantes disponibles est proposée ;
- Si des fichiers divers ont été déclarés dans le fichier `migration_perso.py`, la procédure propose de

les récupérer ;

- Après descente de ces fichiers et des données de variante, une sauvegarde est effectuée pour remonter les fichiers locaux (configuration EAD,...) auprès du serveur Zéphir ;
- Suivre les indications données en fin de procédure pour finaliser la configuration du serveur.

Préchargement d'image ISO (Upgrade-Auto)

Le script Upgrade-auto comporte une option --download permettant de télécharger l'image ISO de migration sans lancer la procédure de migration. Une action est disponible dans l'application Zéphir pour lancer le téléchargement à distance sur un serveur ou un groupe de serveurs (serveurs 2.4.2 ou supérieurs).

4.8. Surveillance des serveurs enregistrés

Zéphir offre la possibilité de surveiller les serveurs à distance.

Les informations mises à disposition sont les suivantes :

- résumé de l'état du système (mémoire, système de fichiers, ...) ;
- aperçu de la configuration du serveur ;
- état des différents services (exemple : SSH, DNS et proxy sur le module Amon) ;
- diverses informations selon le module installé sur le serveur.

4.8.1. État de la configuration

Ces informations sont disponibles depuis la page de chaque serveur : **État actuel**.

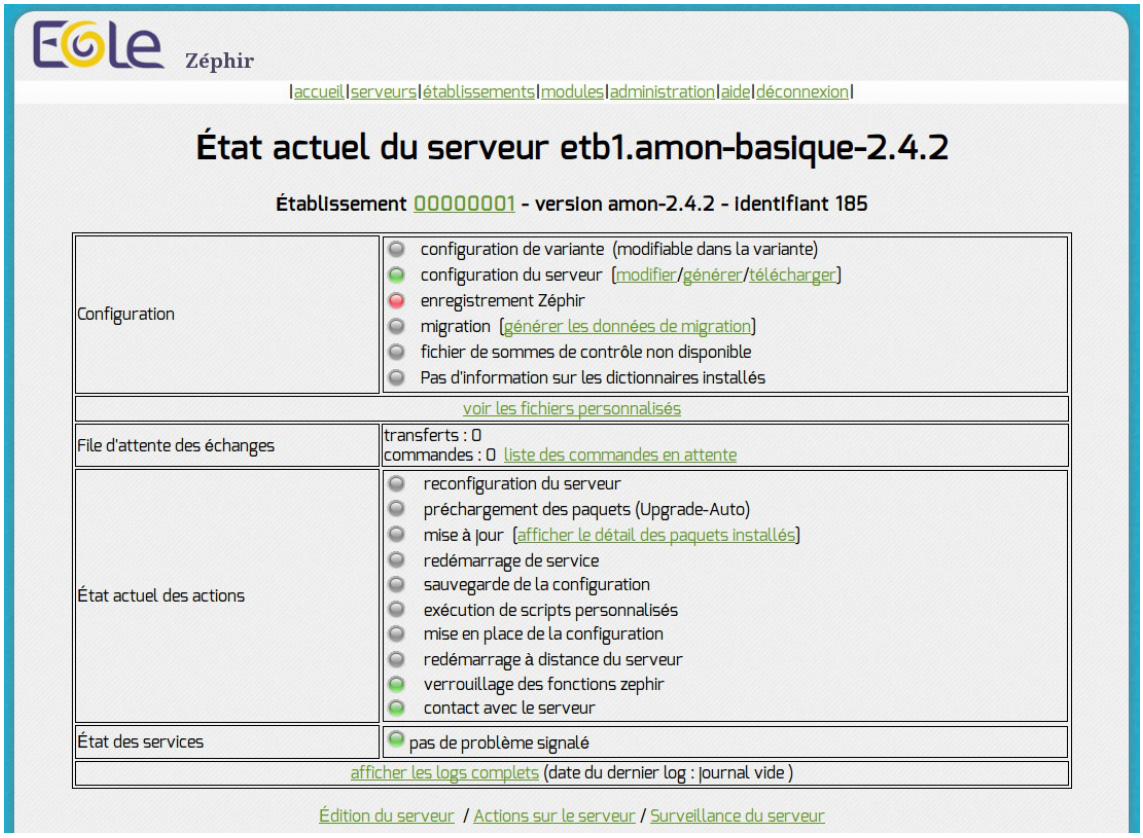
La première partie (Configuration) donne des renseignements sur les fichiers principaux de paramétrage du serveur (zephir.eol).

Une diode indique l'état de chacun des fichiers :

- diode verte : fichier sauvegardé ;
- diode rouge : fichier différent entre Zéphir et le serveur ;
- diode grise : fichier absent.

Vous pouvez accéder au formulaire de saisie des paramètres du serveur en cliquant sur modifier (reprise des valeurs actuelles) ou générer (reprise des valeurs par défaut). Ce formulaire est équivalent à la procédure gen_config disponible sur tout module EOLE. Les nouveaux paramètres seront sauvegardés sur Zéphir, et envoyés au serveur la prochaine fois que vous utiliserez l'action '*envoi de la configuration au serveur*' pour ce serveur.

La diode enregistrement Zéphir indique si la procédure d'enregistrement a déjà été effectuée.



A chaque contact avec un serveur, celui-ci envoie à Zéphir un fichier contenant les sommes md5 des fichiers suivants :

- `config.eol` (valeurs renseignées par gen_config ou via le formulaire de Zéphir) ;
- tous les fichiers ayant l'extension `.patch` dans `/etc/eole/patch` et `/etc/eole/patch/variante` ;
- tous les fichiers `.xml` dans `/etc/eole/dicos` et `/etc/eole/dicos/variante`.

Si un de ces fichiers n'est pas identique sur Zéphir ou sur le serveur (ou si des fichiers ont été ajoutés/supprimés), la liste de ces fichiers sera indiquée dans une liste déroulante.

Le lien `voir les fichiers personnalisés` renvoie sur un résumé des différents fichiers spécifiques au serveur, comme le fichier de description de règles de pare feu sur Amon (voir la partie 'personnalisation du serveur').

La section File d'attente des échanges indique les transferts de fichiers et commandes à distance qui sont en attente pour ce serveur (ils seront traités par celui-ci lors de sa connexion à Zéphir).

Le détail des dernières commandes envoyées est disponible en cliquant sur `liste des dernières commandes en attente`. Il est possible d'annuler des actions en attente depuis cette liste.

Le cadre état actuel des actions indique si les dernières actions distantes se sont bien déroulées ou non.

Les états possibles sont les suivants :

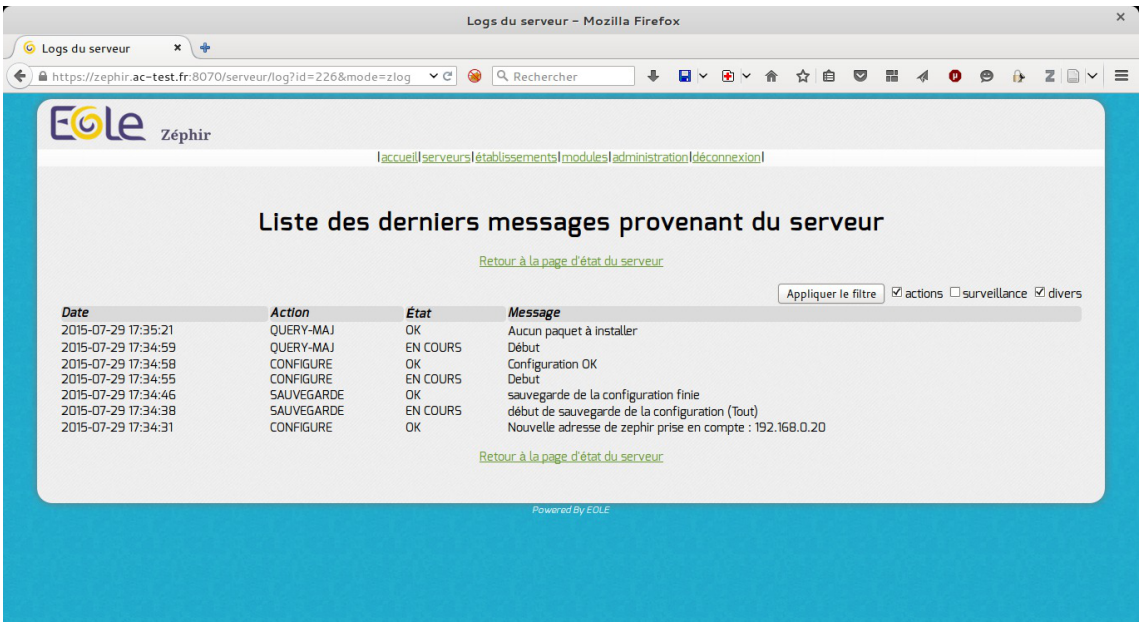
- vert : indique que l'action s'est terminée normalement ;
- jaune : indique que l'action a débuté, mais n'est pas encore terminée ;
- rouge : indique que l'action s'est terminée de façon anormale (erreur de transfert de fichiers, erreur système, ...) ;
- gris : aucune indication n'est connue pour cette action (elle n'a jamais été lancée ou les logs la concernant ont été effacés).

Vous pouvez laisser la souris au dessus du bouton pour avoir plus de détails.

Le cadre État des services résume les information présentes dans la page 'surveillance des serveur'. Si le voyant est rouge, c'est que le serveur a remonté une alerte.

La dernière ligne donne la date et l'heure de la dernière action enregistré pour ce serveur.

Le lien Logs complets permet d'accéder à la liste complète des logs.



4.8.2. État des services / état système

Vous pouvez accéder à ces informations à partir de la page d'état du serveur en cliquant sur Surveillance du serveur (en bas de page). Un résumé de l'état du système et des services sera alors ouvert dans une nouvelle fenêtre (les différentes sections disponibles sont accessibles depuis le menu de gauche).

Il est possible d'accéder directement à la page faisant état du serveur lorsqu'on connaît son ID :

```
https://<adresse_zephir>:8090/agents/<idServeur>/
```

Les remontés des agents Zéphir sont classées dans 3 catégories : Système, Services et Utilisation.

4.8.2.a. Système

Quelques agents sont fournis de base et sont commun à tous les modules :

- Informations systèmes
- Occupations des disques

- Statistiques réseau
- État des sommes MD5 de paquets

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- Onduleur

> Surveillance de l'état des sommes MD5 des paquets

L'outil `eole-debsums` permet de surveiller les modifications apportées aux fichiers présents sur les modules EOLE grâce à la vérification des sommes de contrôle MD5[p.233] des paquets installés.

Les fichiers de configuration (en général ceux situés dans `/etc`) ne sont pas concernés par cette vérification.

La vérification des sommes de contrôle est exécutée toutes les nuits via une commande cron[p.231].

La commande suivante permet de forcer la vérification des MD5 (compter entre 1 et 2 minutes) :

```
/usr/share/eole/debsums/eole-debsums.sh
```

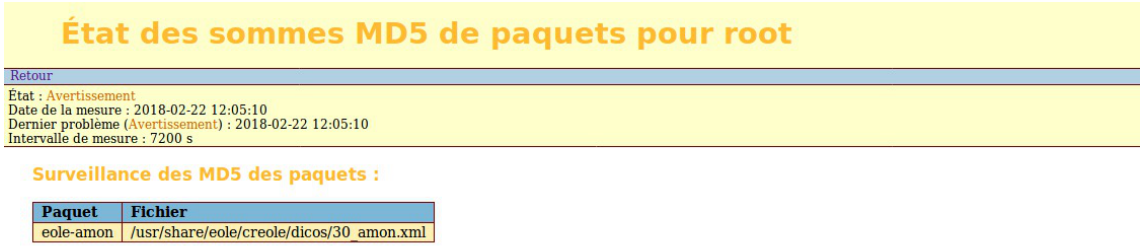
Rapport et suivi des modifications

La commande suivante affiche un rapport d'exécution :

```
root@amon:~# /usr/share/eole/debsums/show-reports.py
Container: root
===============

Filename: /var/log/eole-debsums/report.log
Last update: 2018-02-22 11:09:15

eole-amon:
    /usr/share/eole/creole/dicos/30_amon.xml

Ignored by eole
---------------

```

Un agent[p.230] de surveillance Zéphir permet de surveiller les sommes MD5 des paquets.

Il permet également de consulter la liste des fichiers signalés comme modifiés.



4.8.2.c. Services

Quelques agents sont fournis de base et sont commun à tous les modules :

- État des interfaces réseau
- Services distants
- État des services

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- État des démons bacula

Enfin d'autres agents sont propres à un module en particulier :

- État des tunnels

4.8.2.d. Utilisation

Quelques agents sont fournis de base et sont commun à tous les modules :

- Mise à jour

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- Sauvegarde

Enfin d'autres agents sont propres à un module en particulier :

- Statistiques Squid
- Statistiques courrier
- Application des règles bastion
- Instance Dansguardian
- Mise à jour antivirus Clam

4.8.3. État d'un groupe de serveurs

La page d'affichage d'un groupe donne une indication globale sur l'état des serveurs sélectionnés.

La diode de la colonne état peut prendre les états suivants :

- grise : pas d'informations remontées par le serveur ;
- verte : aucun problème remonté par le serveur ;
- rouge : problème détecté sur le serveur (service indisponible, problème matériel, ...).

Dans le cas d'une diode rouge, vous pouvez cliquer sur la diode pour obtenir le détail des erreurs reportées.

Le principe est le même pour les voyants des colonnes md5 et mise à jour.

4.9. Gestion des alertes par courriers électroniques

Il est possible d'activer des alertes par courriers électroniques pour un groupe de serveurs et de désactiver des alertes pour un agent ou un serveur donné. Par défaut, les alertes sont activées sur tous les serveurs.

Alertes par courrier électronique

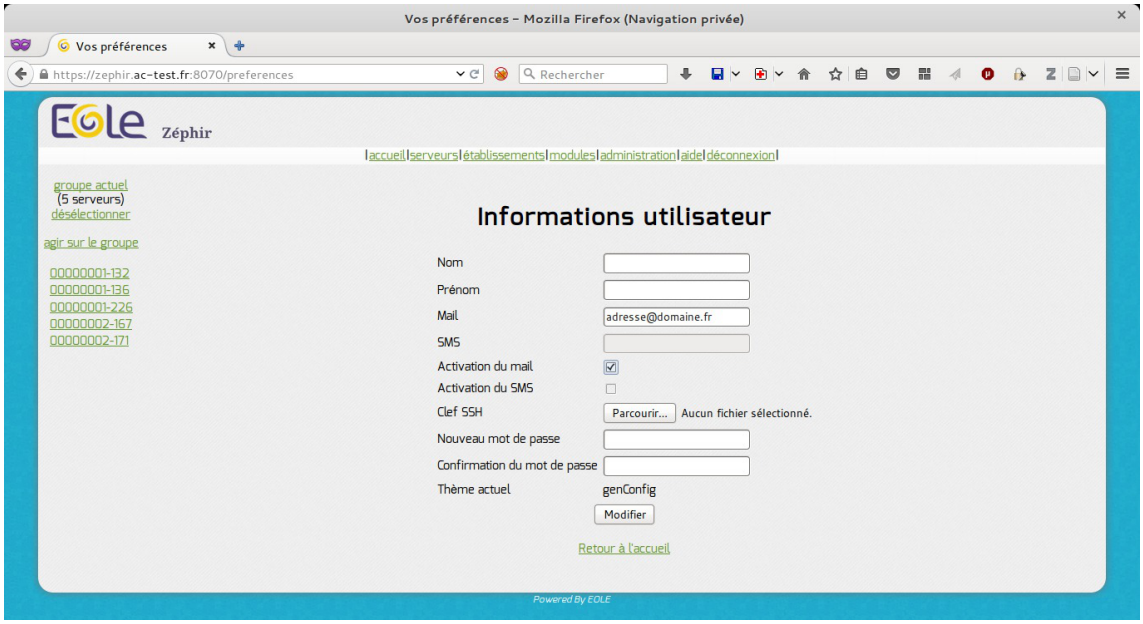
Le serveur Zéphir intègre la possibilité d'envoyer un courrier électronique quand un problème est détecté sur un des serveurs qu'il gère.

Les différents types d'erreurs possibles sont les suivants :

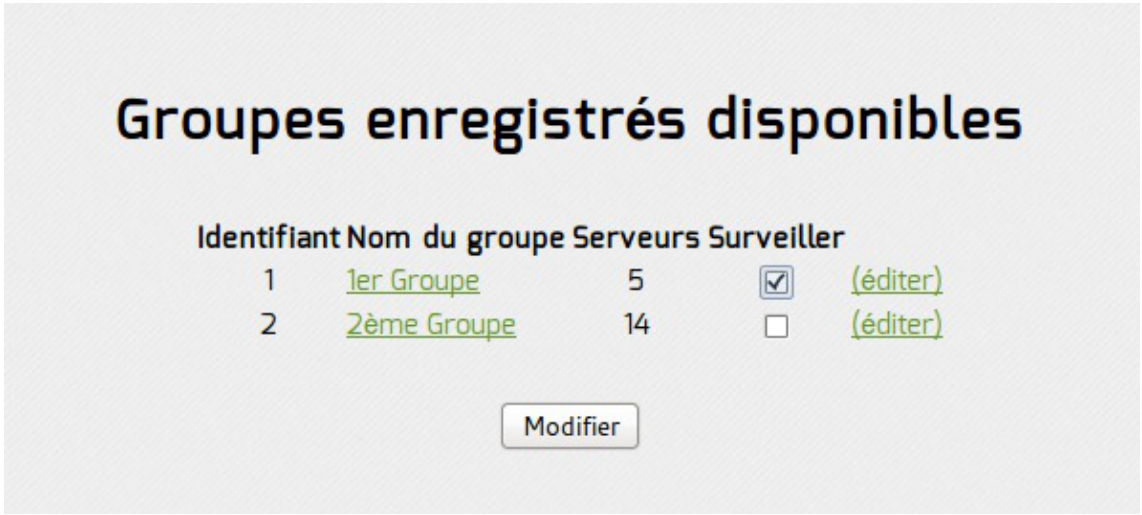
- remontée par le serveur d'une erreur sur un de ses services (DNS, Apache, ...) ou un problème système ;
- un serveur n'a pas contacté le serveur Zéphir depuis un certain temps (délai limite configurable pour chaque serveur) ;
- une opération s'est mal déroulée sur le serveur (mise à jour, sauvegarde, ...).

Pour recevoir des courriers électroniques d'alerte, il faut :

- avoir renseigné votre adresse électronique et coché la case ☑ activation du mail dans Vos préférences depuis la page d' accueil ;



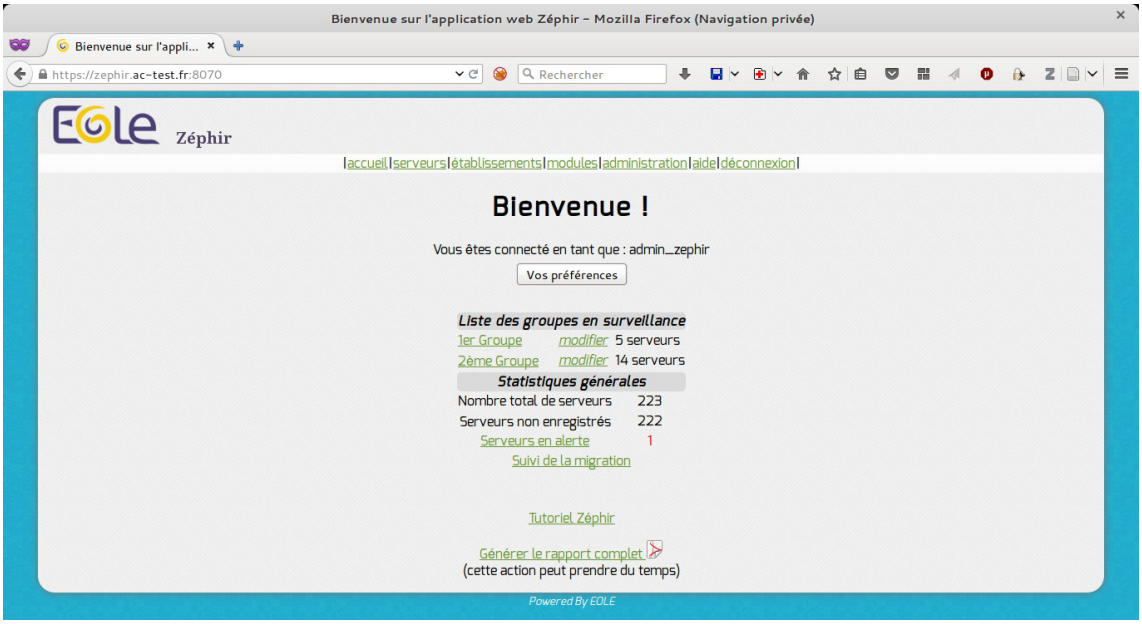
- sélectionner un groupe de serveurs dans l'onglet `serveurs` / `Gérer les groupes enregistrés de serveurs`
- éditer éventuellement le groupe avec le bouton `(éditer)` pour enlever les serveurs non désirés
- sinon cocher la case `☑ Surveiller` dans la ligne du groupe à surveiller puis cliquer sur le bouton `Modifier` pour valider ce choix ;



Vous recevrez un courrier électronique en cas de problème sur un serveur et un autre lorsque le serveur retrouvera son état normal.

Exemple d'alerte mail

Les groupes surveillés apparaissent sur la page d'accueil de l'application.



Désactivation des alertes pour un agent ou un serveur donné

Il est possible d'indiquer une liste d'agents qui ne déclencheront pas d'alerte s'ils sont en erreur. Pour cela, il faut créer un fichier `/var/lib/zephir/data/ignore_list` sur le serveur Zéphir et ajouter un nom d'agent par ligne.

> Les erreurs sur l'application des patches et sur les services distants ne seront pas prises en compte dans l'état global des serveurs si le fichier `/var/lib/zephir/data/ignore_list` contient :
>
> `patches`
>
> `web`

Les agents existants par défaut sont :

- network ;
- web ;
- tcpservices ;
- rvp ;
- nut ;
- sysinfo ;
- diskspace ;
- netstats ;
- patches ;
- squid-stats ;
- conn ;
- vir ;
- config ;

- annuaire ;
- printers ;
- eximstats.

Il est possible de mettre ce fichier dans le répertoire `/usr/share/zephir/monitor/stats/` sur les serveurs EOLE enregistrés.
Ce fichier sera remonté et pris en compte par le serveur Zéphir pour le serveur enregistré en question (il peut être distribué comme fichier divers dans une variante Zéphir).

Cela peut être utile dans le cas d'un serveur qui présente régulièrement des problèmes (mauvaise connexion , mémoire limitée ...), afin d'éviter des alertes inutiles.

On peut empêcher un serveur de générer des alertes en passant le paramètre `Désactiver les alertes pour ce serveur` à `oui` dans la fiche du serveur (`État actuel du serveur`) / `Description du serveur` .
Ce paramètre peut également être modifié sur tous les serveurs d'un groupe de la façon suivante :

- Sélectionner un groupe de serveurs ;
- Utiliser le lien `Actions sur le groupe de serveurs` sur la page `Liste des Serveurs sélectionnés` ou utiliser le lien `agir sur le groupe` dans le menu de gauche ;
- Utiliser l'action `Modifier un paramètre sur le groupe` en bas de page ;
- Cliquer sur `Désactiver les alertes` ;

Cela peut être utile dans le cas d'un serveur de test.

Lors de la `Sélection d'un groupe de serveurs` , il est possible de choisir le `Blocage des alertes` comme critère de sélection.

4.10. Gestion par groupe de serveurs

Agir individuellement sur chaque serveur peut vite devenir une tâche fastidieuse. L'application Zéphir implémente la notion de groupe de serveurs qui permet de faciliter le travail lorsque le nombre de serveurs devient important.

4.10.1. Création des groupes

Sélection des serveurs

La première étape pour travailler avec un groupe est de définir les serveurs qui lui appartiennent. Accédez au menu `serveurs` de l'application Zéphir, et cliquez sur `Sélection d'un groupe de serveurs` afin de spécifier les critères de votre groupe. Vous pourrez en premier lieu choisir de travailler avec un module particulier (Amon, Horus, ...). Pour travailler sur tous les modules, il est possible de laisser le champ vide.

Ensuite, il est possible de spécifier d'autres critères comme une variante particulière du module choisi, un numéro d'établissement, le nom de l'installateur du serveur, un type de matériel, ...

Vous pouvez utiliser le caractère `%` comme caractère générique, seul, devant ou derrière une chaîne (par exemple `021%` pour sélectionner tous les RNE commençant par `021`).

Il est également possible de laisser le formulaire vide.

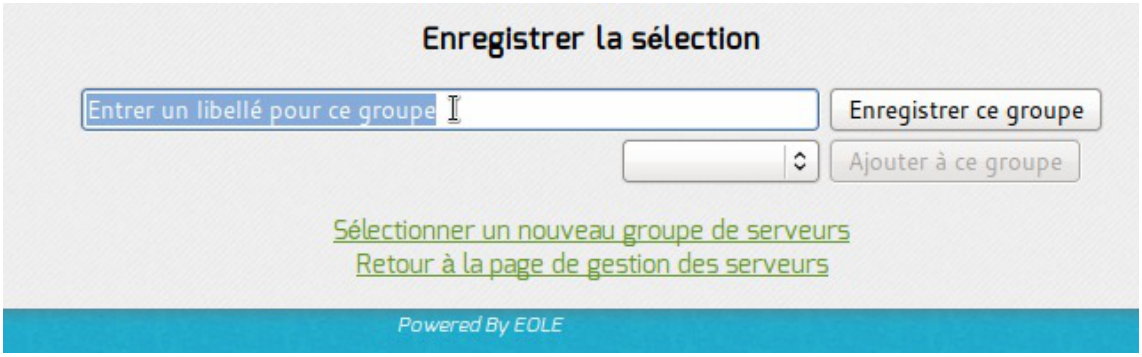
Après avoir cliquer sur le bouton Suivant, il est possible de sélectionner une ou plusieurs variables spécifiques. Il est également possible de laisser le formulaire vide.

Une fois les conditions validées, un clique sur le bouton Continuer renvoie la liste les serveurs sélectionnés en rapport avec les critères précédemment choisis.

Ajout d'une sélection de serveurs à un groupe existant

Si un ou plusieurs groupes existes déjà une liste déroulante permet de sélectionner le groupe auquel ajouter les serveurs sélectionnés, cliquer sur le bouton `Ajouter à ce groupe` pour valider.

Sauvegarde de la liste de serveurs en tant que groupe

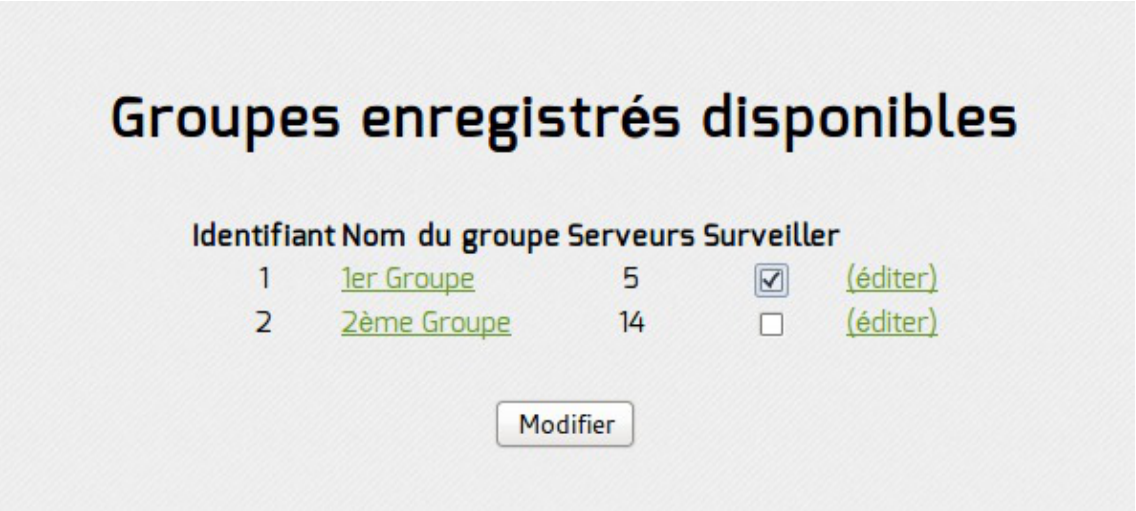


Pour enregistrer cette liste en tant que groupe il faut saisir un libellé pour le groupe et cliquer sur le bouton `Enregistrer le groupe`.

Les groupes enregistrés sont statiques. Si un nouveau serveur entre dans les critères, il faudra le rajouter manuellement.

4.10.2. Gestion des groupes de serveurs

Les groupes enregistrés sont accessibles par la page `Gestion des groupes de serveurs` dans l'onglet `serveurs` du menu.



Dans cette page, vous pouvez :

- demander la surveillance d'un ou de plusieurs groupes de serveur ;
- lister les serveurs d'un groupe ;
  - agir sur le groupe de serveurs (`Actions sur le groupe de serveurs`) ;
  - ajouter des serveurs (`Nouvelle sélection`) ;
  - autoriser la connexion par clé SSH pour un identifiant donné ;
- éditer (libellé, suppression de serveur) / supprimer le groupe.

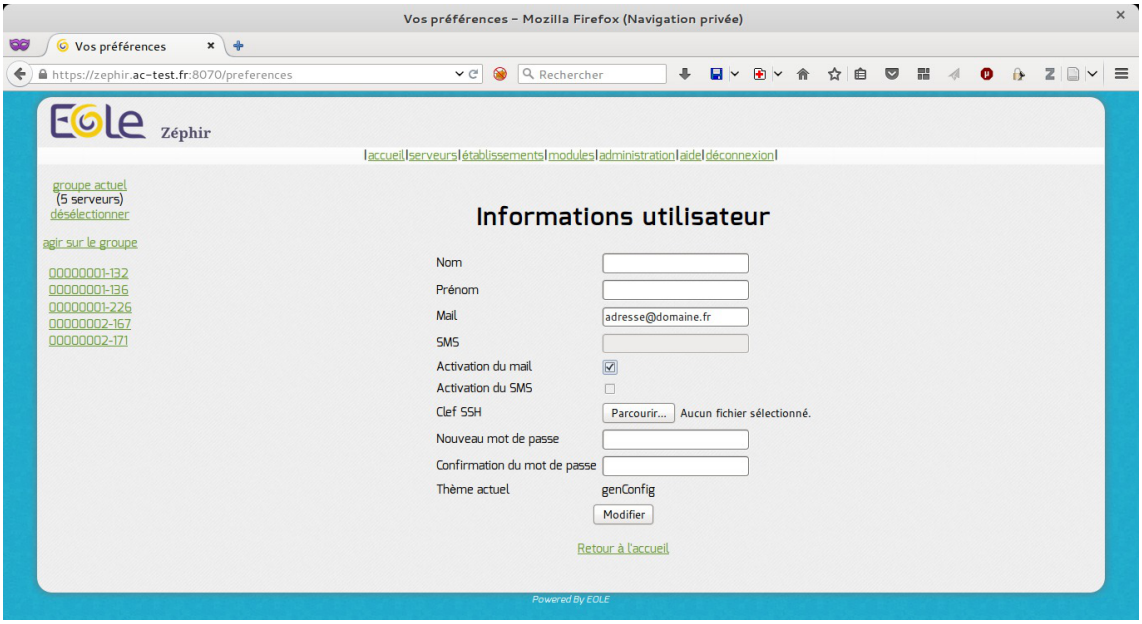
Alertes par courrier électronique

Le serveur Zéphir intègre la possibilité d'envoyer un courrier électronique quand un problème est détecté sur un des serveurs qu'il gère.
Les différents types d'erreurs possibles sont les suivants :

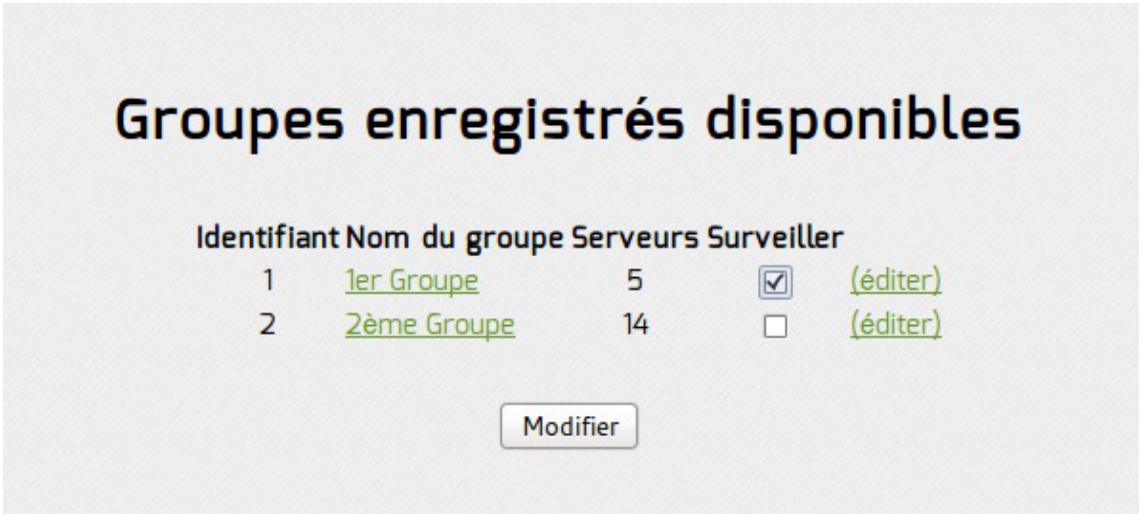
- remontée par le serveur d'une erreur sur un de ses services (DNS, Apache, ...) ou un problème système ;
- un serveur n'a pas contacté le serveur Zéphir depuis un certain temps (délai limite configurable pour chaque serveur) ;
- une opération s'est mal déroulée sur le serveur (mise à jour, sauvegarde, ...).

Pour recevoir des courriers électroniques d'alerte, il faut :

- avoir renseigné votre adresse électronique et coché la case ☑ `activation du mail` dans `Vos préférences` depuis la page d' `accueil` ;



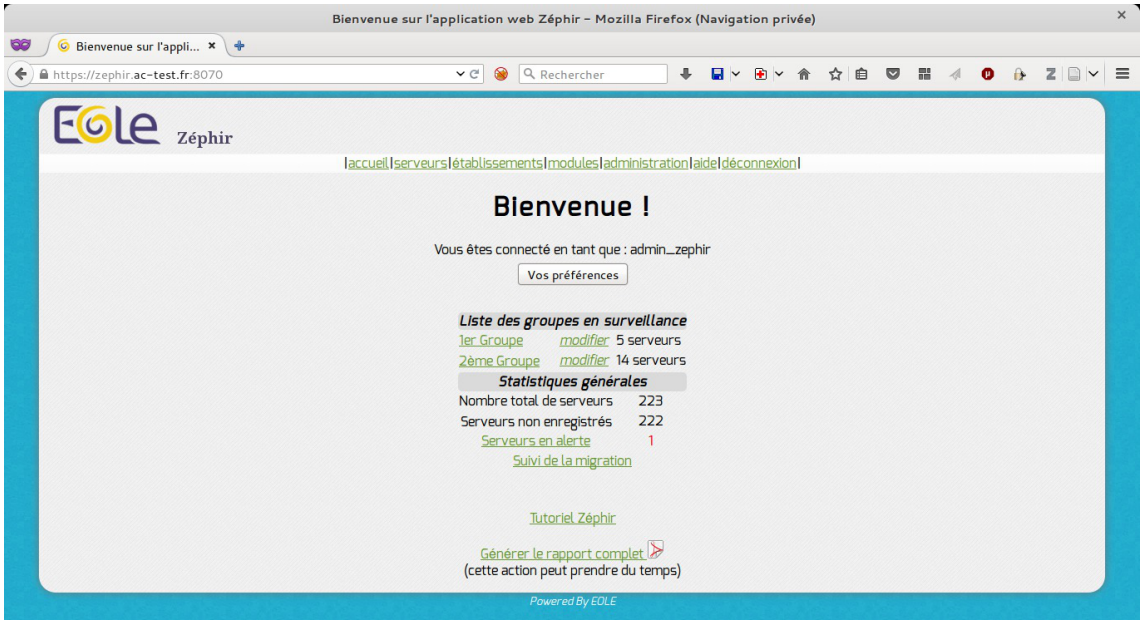
- sélectionner un groupe de serveurs dans l'onglet `serveurs` / `Gérer les groupes enregistrés de serveurs`
- éditer éventuellement le groupe avec le bouton `(éditer)` pour enlever les serveurs non désirés
- sinon cocher la case ☑ `Surveiller` dans la ligne du groupe à surveiller puis cliquer sur le bouton `Modifier` pour valider ce choix ;



Vous recevrez un courrier électronique en cas de problème sur un serveur et un autre lorsque le serveur retrouvera son état normal.

Exemple d'alerte mail

Les groupes surveillés apparaissent sur la page d'accueil de l'application.



Désactivation des alertes pour un agent ou un serveur donné

Il est possible d'indiquer une liste d'agents qui ne déclencheront pas d'alerte s'ils sont en erreur. Pour cela, il faut créer un fichier `/var/lib/zephir/data/ignore_list` sur le serveur Zéphir et ajouter un nom d'agent par ligne.

Les erreurs sur l'application des patches et sur les services distants ne seront pas prises en compte dans l'état global des serveurs si le fichier `/var/lib/zephir/data/ignore_list` contient :

```
patches
web
```

Les agents existants par défaut sont :

- network ;
- web ;
- tcpservices ;
- rvp ;
- nut ;
- sysinfo ;
- diskspace ;
- netstats ;
- patches ;
- squid-stats ;
- conn ;
- vir ;
- config ;

- annuaire ;
- printers ;
- eximstats.

Il est possible de mettre ce fichier dans le répertoire `/usr/share/zephir/monitor/stats/` sur les serveurs EOLE enregistrés.
Ce fichier sera remonté et pris en compte par le serveur Zéphir pour le serveur enregistré en question (il peut être distribué comme fichier divers dans une variante Zéphir).

Cela peut être utile dans le cas d'un serveur qui présente régulièrement des problèmes (mauvaise connexion , mémoire limitée ...), afin d'éviter des alertes inutiles.

On peut empêcher un serveur de générer des alertes en passant le paramètre `Désactiver les alertes pour ce serveur` à `oui` dans la fiche du serveur (`État actuel du serveur`) / `Description du serveur` .
Ce paramètre peut également être modifié sur tous les serveurs d'un groupe de la façon suivante :

- Sélectionner un groupe de serveurs ;
- Utiliser le lien `Actions sur le groupe de serveurs` sur la page `Liste des Serveurs sélectionnés` ou utiliser le lien `agir sur le groupe` dans le menu de gauche ;
- Utiliser l'action `Modifier un paramètre sur le groupe` en bas de page ;
- Cliquer sur `Désactiver les alertes` ;

Cela peut être utile dans le cas d'un serveur de test.

Lors de la `Sélection d'un groupe de serveurs` , il est possible de choisir le `Blocage des alertes` comme critère de sélection.

4.10.3. Actions supplémentaires

Un tableau de résumé vous indique l'état de chaque serveur (voyant rouge si un problème est détecté),

et vous pouvez accéder à la page d'état de ceux-ci (en cliquant sur le libellé du serveur dans la deuxième colonne), ou à la page de l'établissement correspondant (colonne RNE).

Deux boutons permettent d'autoriser ou interdire à un utilisateur d'accéder à ces serveurs grâce à sa clé de connexion SSH. (entrer le login de l'utilisateur dans le champ texte) à condition que vous ayez accès aux fonctions de gestion des droits. Cette autorisation sera effective au prochain envoi de configuration aux serveurs concernés.

La clé SSH (clé publique) doit être envoyée sur le serveur Zéphir par l'intermédiaire de la page 'préférences'. Pour des raisons de sécurité, cette clé est propre à chaque utilisateur, et seul celui-ci peut envoyer sa clé au serveur Zéphir.

Voir aussi...

Préférences des utilisateurs

4.11. Les variantes

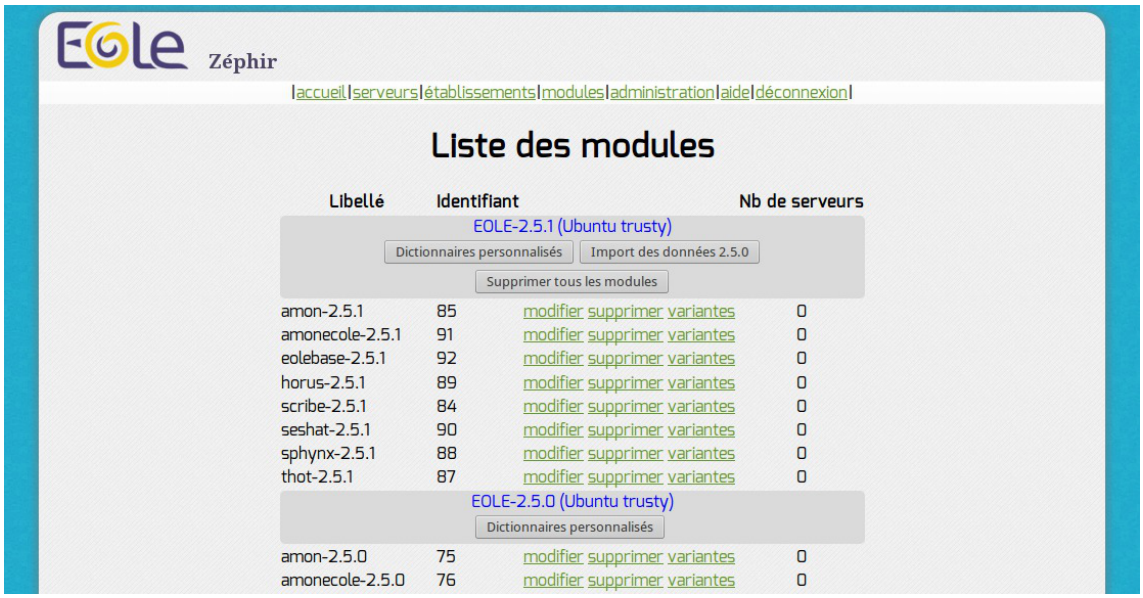
La notion de variante[p.236] est une fonctionnalité majeure de Zéphir. Une variante est une version modifiée d'un module EOLE que l'on veut pouvoir reproduire et déployer à volonté. Modifier une variante permet de modifier l'ensemble des serveurs utilisant cette variante.

Chaque module possède au moins une variante par défaut (`standard`) qui ne peut pas être modifiée.

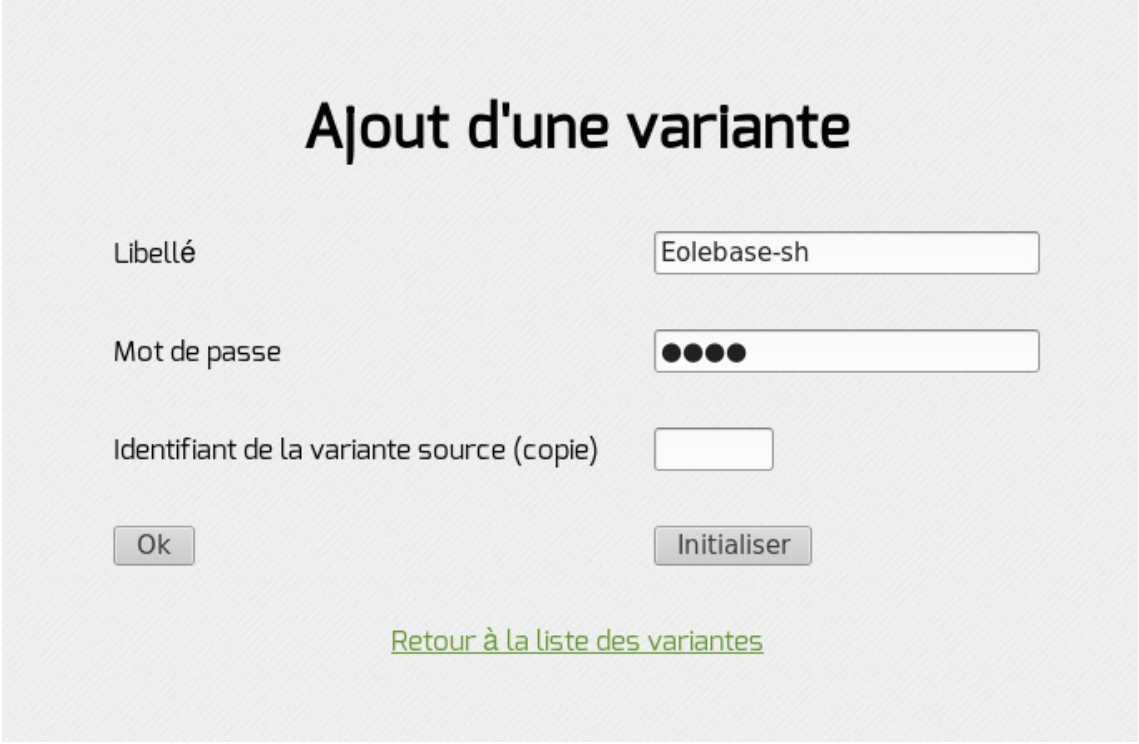
4.11.1. Créer une variante

Depuis l'interface web

L'ajout d'une variante se fait depuis le menu `modules`, en cliquant sur sur `variantes` sur la ligne du module désiré.



Il faut ensuite cliquer sur `ajouter une variante` ce qui affiche un formulaire de création.



- le champ `Libellé` permet de préciser à quoi se rapporte la variante ;
- le champ `Mot de passe` permet à d'autres utilisateurs de modifier cette variante. Si aucun mot de passe n'est défini, seul l'utilisateur ayant créé la variante pourra la modifier ;
- le champ `Identifiant de la variante source (copie)` permet de créer la nouvelle variante à partir d'une variante existante.

Une fois la variante créée, elle s'affiche dans la liste des variantes relatives au module. Il est ainsi possible de l'éditer ou de la supprimer.

Depuis un serveur

La procédure de création d'une variante depuis un serveur est la suivante :

- installation d'un serveur avec le module EOLE (ou utilisation d'un serveur existant) ;
- enregistrement du serveur sur Zéphir ;
- création des modifications sur le serveur avec patchs, dictionnaires locaux, ou installation de paquetages supplémentaires. Attention de bien tester les modifications sur le serveur avant de créer une variante ;
- une fois le résultat désiré obtenu :
  - déplacer les patchs dans `/usr/share/eole/creole/patch/variante/` ;
  - les dictionnaires doivent être gérés depuis l'interface Zéphir ;
  - les paquets propres à EOLE qui contiennent des dictionnaires sont à gérer dans la variante dans l'interface Zéphir ;
  - si vous avez ajouté des paquets non EOLE ou des fichiers qui ne sont pas référencés dans des dictionnaires locaux, vous pouvez les spécifier dans le fichier `/usr/share/zephir/zephir_conf/fichiers_variante`.

- lancer le script de création de variante `/usr/share/zephir/scripts/creation_variante`.

  Le mot de passe donné lors de la création de la variante est le mot de passe à donner à d'autres utilisateurs pour qu'ils puissent modifier la variante.

```
root@eolebase:~# /usr/share/zephir/scripts/creation_variante

** procédure de création de variante **

Attention, les dictionnaires ne sont pas remontés automatiquement sur Zéphir

Veuillez :
- les gérer via la page 'dictionnaires personnalisés' de la distribution 2.5
- les activer ensuite dans la variante

login pour l'application zephir : admin_zephir
mot de passe pour admin_zephir :

** création d'une variante pour le module 'eolebase-2.5.2' **

entrez le nom de la nouvelle variante
[rien pour la liste des variantes existantes] : Eolebase-sh
mot de passe de la variante (ou rien) :
Entrez à nouveau le mot de passe pour vérification :


** mise en place de la variante **
 - ajout de la variante dans la base zephir...
 - création de l'archive des patchs et dictionnaires locaux...
 - création de la signature md5 de l'archive...
 - envoi de l'archive au serveur zephir...
 - variante créée dans la base avec l'id 112 ...
 - inscription du serveur à cette variante...
 - vérification de l'archive et mise en place des données...
 - suppression de l'archive locale...
** installation de la variante terminée **

root@eolebase:~#
```

Une fois la procédure terminée, les données de la variante sont stockées sur le serveur Zéphir et le serveur est déclaré comme utilisant cette variante.

Exemple de fichiers fichiers_variante

Pour installer le paquet `phpsite`, il faut pouvoir récupérer le répertoire `/var/www/html/phpsite/conf/` et le fichier `/etc/apache/conf/phpsite.conf`.

Pour cela, il faut remplir le fichier `/usr/share/zephir/zephir_conf/fichiers_variante` de la manière suivante :

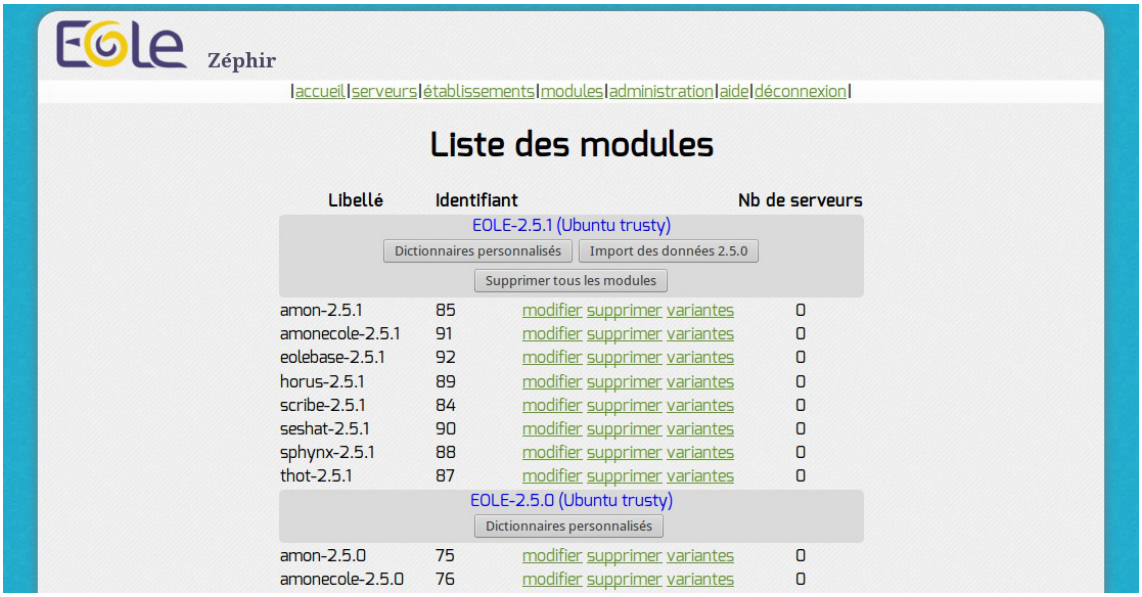
```
# section 1
# liste des fichiers à sauvegarder pour la variante
# (ne pas modifier sauf pour créer ou mettre à jour la variante)
/var/www/html/phpsite/conf/
/etc/apache/conf/phpsite.conf
%%
# section 2
# inscrire les noms des paquetages qui seront installés à la mise à jour du serveur
# (ils doivent être présents sur le serveur de mise à jour)
# activation des actions
phpsite
```

Pour vérifier l'enregistrement de la variante, il faut se rendre sur la page d'`État actuel du serveur` sur l'application web de Zéphir, la liste des fichiers ajoutés sont visibles depuis le lien `voir les fichiers personnalisés` et le nom de la variante apparaît sur la page de description du serveur lorsqu'on clique sur `Édition du serveur`.

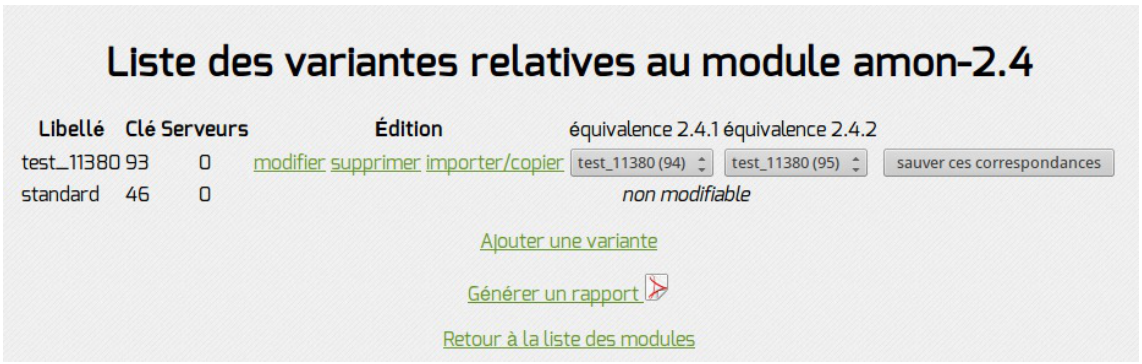
4.11.2. Modifier une variante

Depuis l'interface web

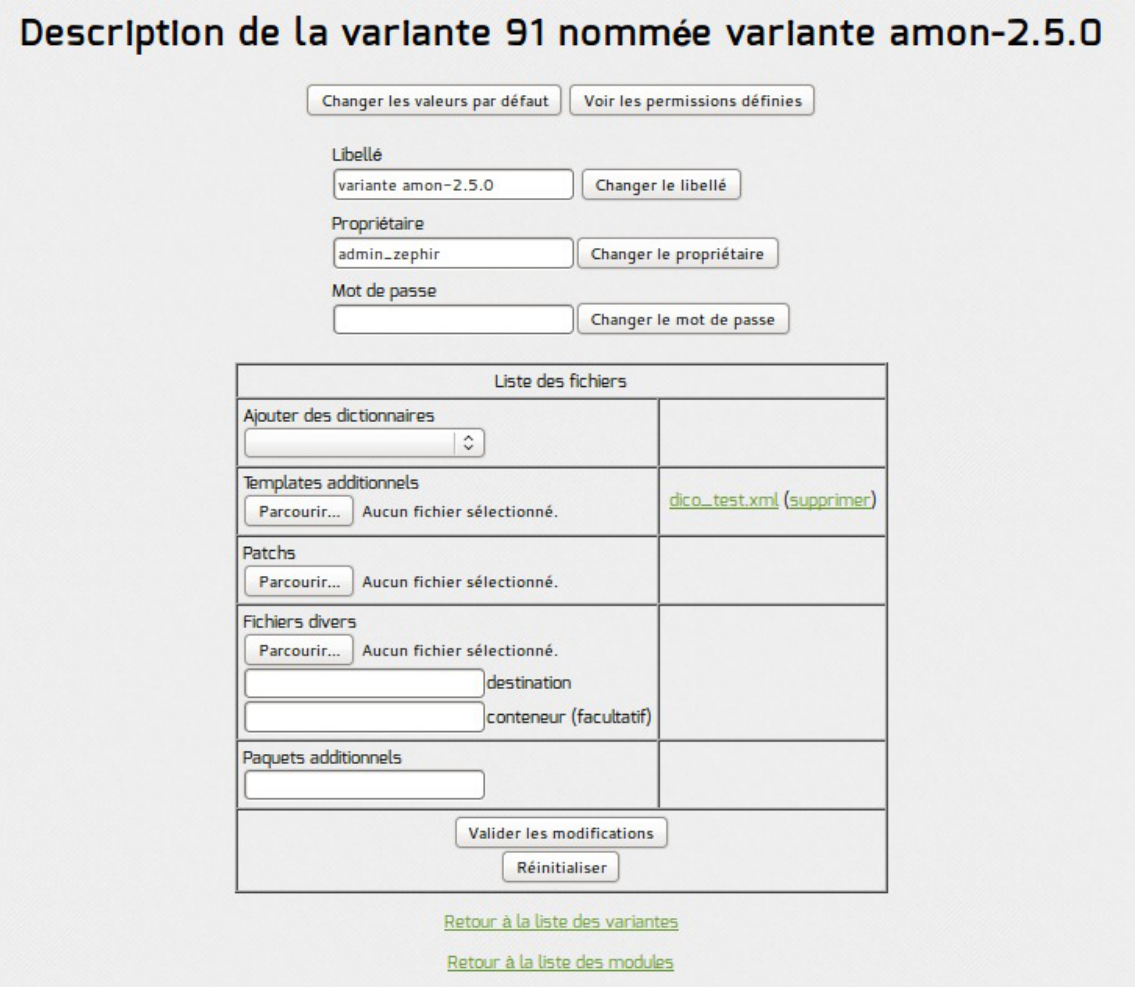
Depuis la page `modules`, il est possible de modifier certains aspects d'une variante.



Cliquer sur le bouton `variantes` de la ligne correspondant au module choisi. Une liste des variantes apparaît.



Cliquer sur le bouton `modifier` de la ligne de la variante à modifier. La page suivante apparaît :



Les modifications possibles sont :

- changer le libellé de la variante ;
- renseignement des valeurs par défaut en cliquant sur `Changer les valeurs par défauts` (ouverture de l'interface de configuration du module) ;
- ajouter des fichiers à la variante (dictionnaires, templates, ...).

Les valeurs par défaut seront utilisées à la première saisie de la configuration d'un serveur. Il est également possible de les définir au niveau du module. Les valeurs de la variante sont prioritaires sur celles du module.

Différents types de fichiers peuvent être ajoutés via cette page. Certaines contraintes doivent être respectées suivant le type de fichier :

- les dictionnaires additionnels (ou locaux) doivent avoir une extension `.xml` pour être pris en compte. De plus, les fichiers templates référencés dans ces dictionnaires doivent être ajoutés également ;
- les patchs sont des patchs EOLE standards ;
- les fichiers divers sont des fichiers quelconques, mais vous devez préciser leur destination sur le serveur dans le champ prévu à cet effet.

Dans le cas ou des dictionnaires nécessitent l'ajout de nouvelles fonctions Creole (répertoire `/usr/share/creole/funcs/` sur les serveurs clients), se reporter à l'explication fournie dans le paragraphe traitant des fichiers personnalisés d'un serveur.

La gestion des dictionnaires est différente pour les serveurs en version 2.4 ou supérieure. Se reporter à la section suivante pour plus de détails.

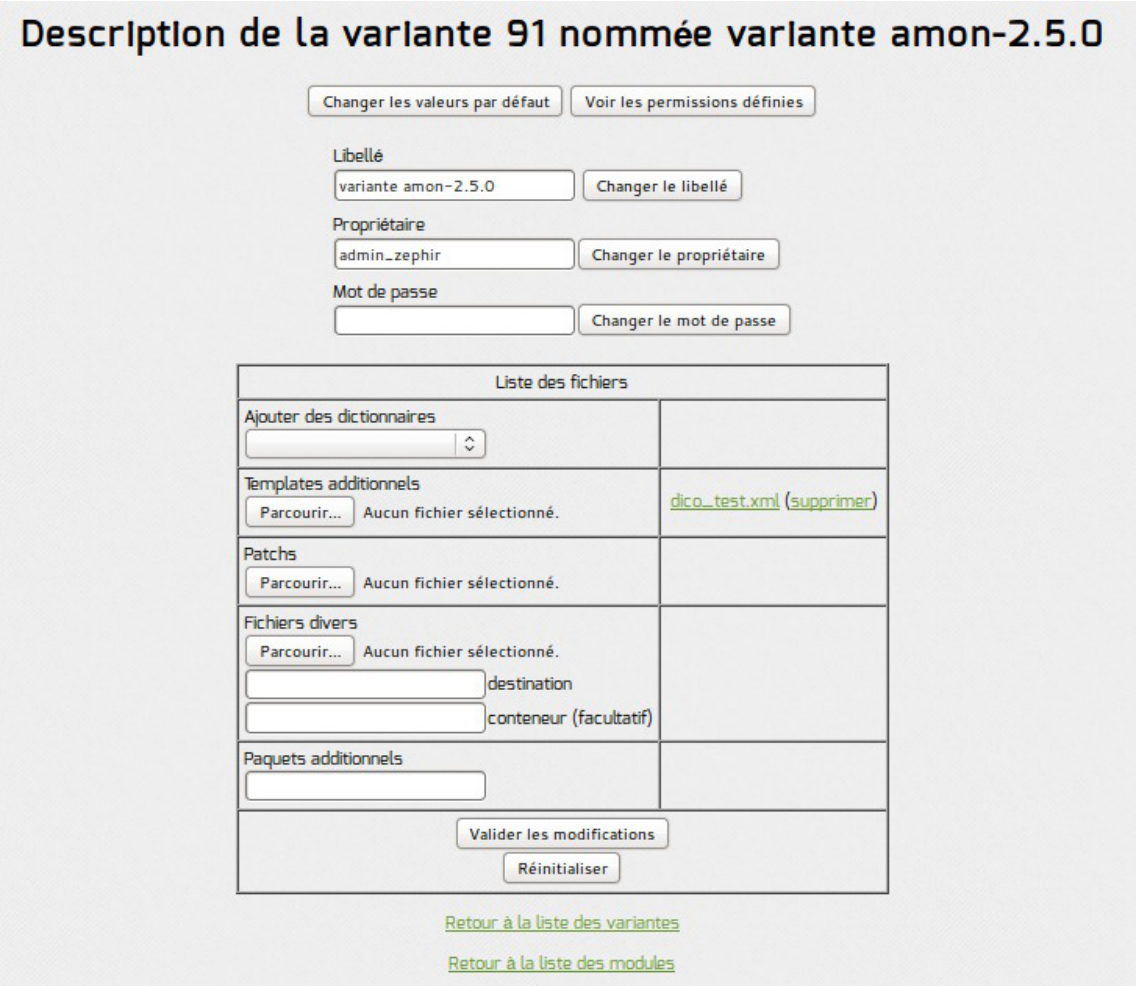
Si vous êtes connecté avec l'utilisateur qui a créé la variante vous pouvez ajouter les fichiers sans avoir à vous soucier du mot de passe. Celui-ci sera demandé si vous ajoutez des fichiers avec un autre utilisateur.

Vous pouvez également supprimer des fichiers en cliquant sur le lien supprimer à côté de chaque fichier. Seul l'utilisateur qui a créé la variante peut supprimer des fichiers. Si vous supprimez un dictionnaire additionnel, vous devrez supprimer vous même les fichiers templates qui deviennent inutiles (non référencés dans d'autres dictionnaires) sur les serveurs.

Pour certains types de fichiers, il peut vous être demandé si vous désirez également que les fichiers soient supprimés sur les serveurs de la variante. Si vous répondez `oui`, une liste des fichiers à supprimer pour la variante est créée. Vous pouvez l'éditer depuis le lien `Fichiers à supprimer sur les clients`.

Définir un fichier à sauvegarder au niveau serveur depuis une variante.

Les `fichiers divers` d'une variante sont communs à tous les serveurs de cette variante. ils ne peuvent donc pas être remontés sur Zéphir pour chaque serveur. Un mécanisme à été mis en place pour permettre d'ajouter automatiquement des fichiers de type `fichiers divers` à sauvegarder sur chaque serveur d'une variante :



- Créer un fichier `fichiers_acad` dans la rubrique `fichiers divers` de la variante avec pour destination `/usr/share/zephir/zephir_conf/fichiers_acad` ;
- ajouter dans ce fichier le chemin absolu des fichiers ou répertoires à sauvegarder (équivalent du champ `destination` lors de l'ajout d'un `fichier divers` à un serveur) ;
- Valider les modifications ;
- pour un serveur il faut se rendre sur la page de description du serveur, le lien `Actions` affiche une page qui permet de lancer l'action `Envoyer la configuration au serveur` sur le serveur concerné ;
- pour un groupe de serveurs il faut cliquer sur `Actions sur le groupe de serveurs`, une page s'affiche et permet de lancer l'action `Envoyer la configuration au serveur` sur les serveurs concernés ;
- à la réception de leur configuration, les serveurs ajouteront ces entrées à leur liste de `fichiers divers` si nécessaire ;
- lors du prochain appel à l'action `Sauvegarder l'état actuel du serveur`, ces fichiers seront remontés sur Zéphir (les 2 actions peuvent être envoyées en une fois en faisant attention de respecter l'ordre).

Depuis le serveur

Pour les serveurs en version 2.4, n'utilisez pas cette méthode si vous avez des dictionnaires personnalisés au niveau de la variante. Ceux ci sont gérés depuis l'interface web (voir le chapitre suivant).

Après avoir effectué des corrections sur un serveur utilisant la variante à mettre à jour, comme indiqué dans le processus de création, utiliser le script `/usr/share/zephir/scripts/maj_variante`.

```
root@eolebase:~# /usr/share/zephir/scripts/maj_variante

** procédure de mise à jour de variante **

Attention, les dictionnaires ne sont pas remontés automatiquement sur Zéphir

Veuillez :
- les gérer via la page 'dictionnaires personnalisés' de la distribution 2.4
- les activer ensuite dans la variante

login pour l'application zephir : admin_zephir
mot de passe pour admin_zephir :

mise à jour des patchs et dictionnaires :
 variante 'mavariante' (n°113) du module eolebase-2.5.2

** Attention, les anciens patchs et dictionnaires locaux vont être écrasés. **
Entrez le mot de passe de la variante (ou rien) :
 - création de l'archive des patchs et dictionnaires locaux...
 - création de la signature md5 de l'archive...
 - envoi de l'archive au serveur zephir...
 - vérification de l'archive et mise en place des données...
 - suppression de l'archive locale...
```

```
** mise à jour de la variante terminée **

root@eolebase:~#
```

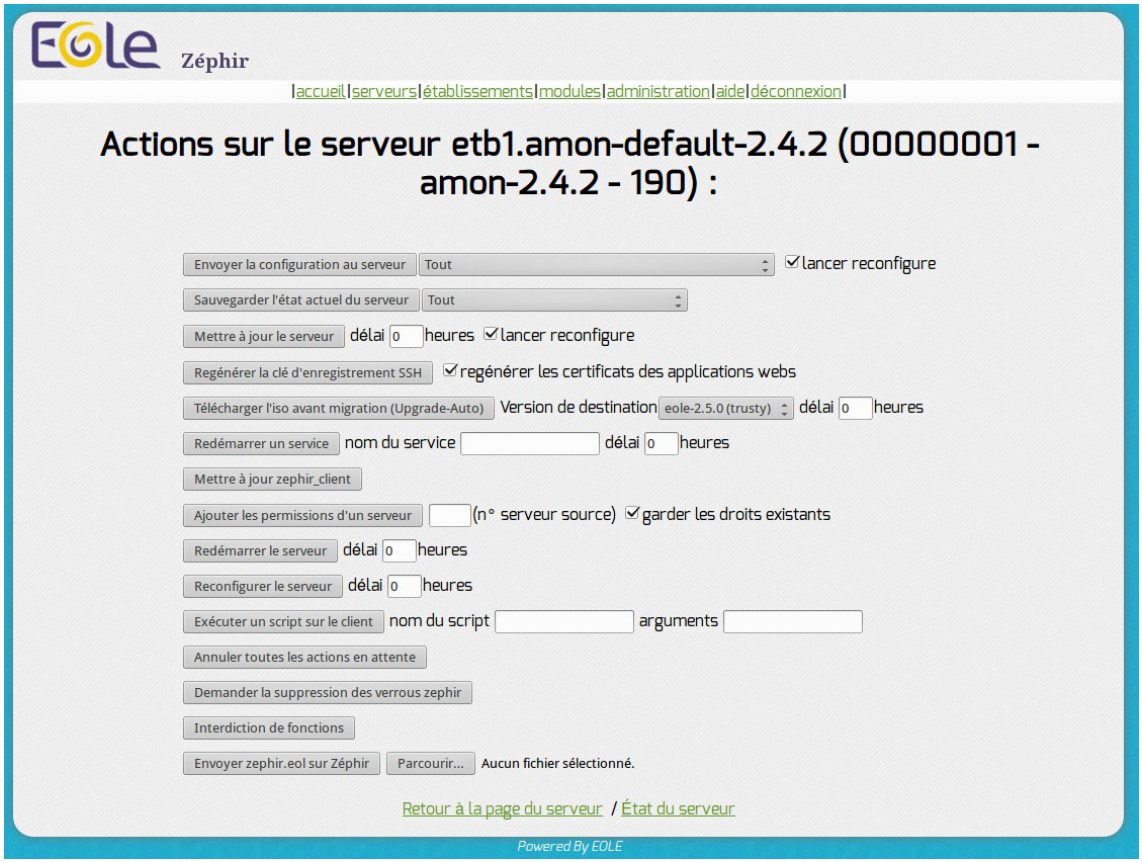
La mise à jour de variante est déconseillée une fois que plusieurs serveurs l'utilisent. En particulier soyez attentifs à d'éventuelles variables obligatoires sans valeur par défaut déclarées dans les dictionnaires.

4.11.3. Réutiliser une variante

Installer une variante sur d'autres serveurs basés sur le même module

Une fois qu'une variante est créée, il est possible de l'installer sur d'autres serveurs basés sur le même module :

- pour sur un serveur déjà inscrit :
  - aller sur la page d'état de ce serveur ;
  - cliquer sur `Édition du serveur` ;
  - cliquer sur `modifier` ;
  - choisir la variante dans la liste déroulante ;
  - se rendre sur la page des actions du serveur ;
  - cliquer sur `Envoyer la configuration au serveur`, vous devrez peut-être aller modifier les paramètres du serveur si de nouvelles variables ont été ajoutées dans les dictionnaires locaux ;



Liste des actions

- lancer la reconfiguration du serveur à l'aide de la commande `reconfigure` ;
- pour un serveur non enregistré, la façon la plus simple est de choisir cette variante avant d'effectuer la procédure d'enregistrement (lors de la création du serveur dans la base de données).

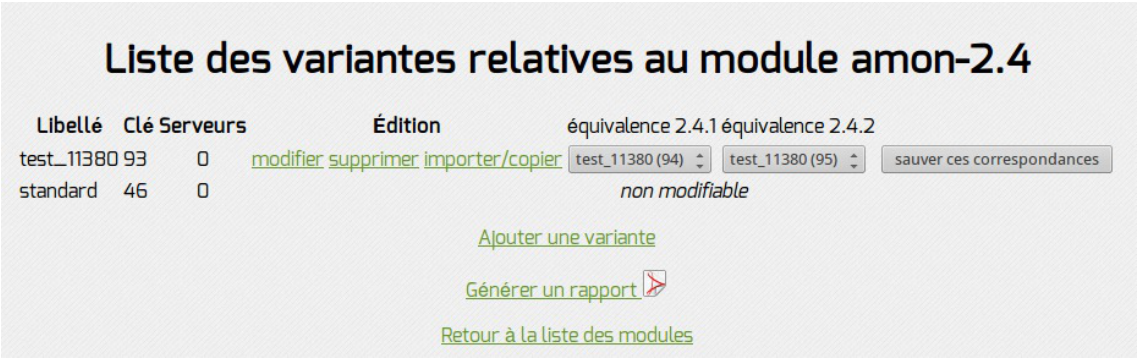
> Il est possible que les fichiers de la variante apparaissent comme modifiés dans la page d'état du serveur. Dans ce cas, il suffit d'attendre la prochaine synchronisation du serveur vers Zéphir.

Importer une variante depuis un autre serveur Zéphir

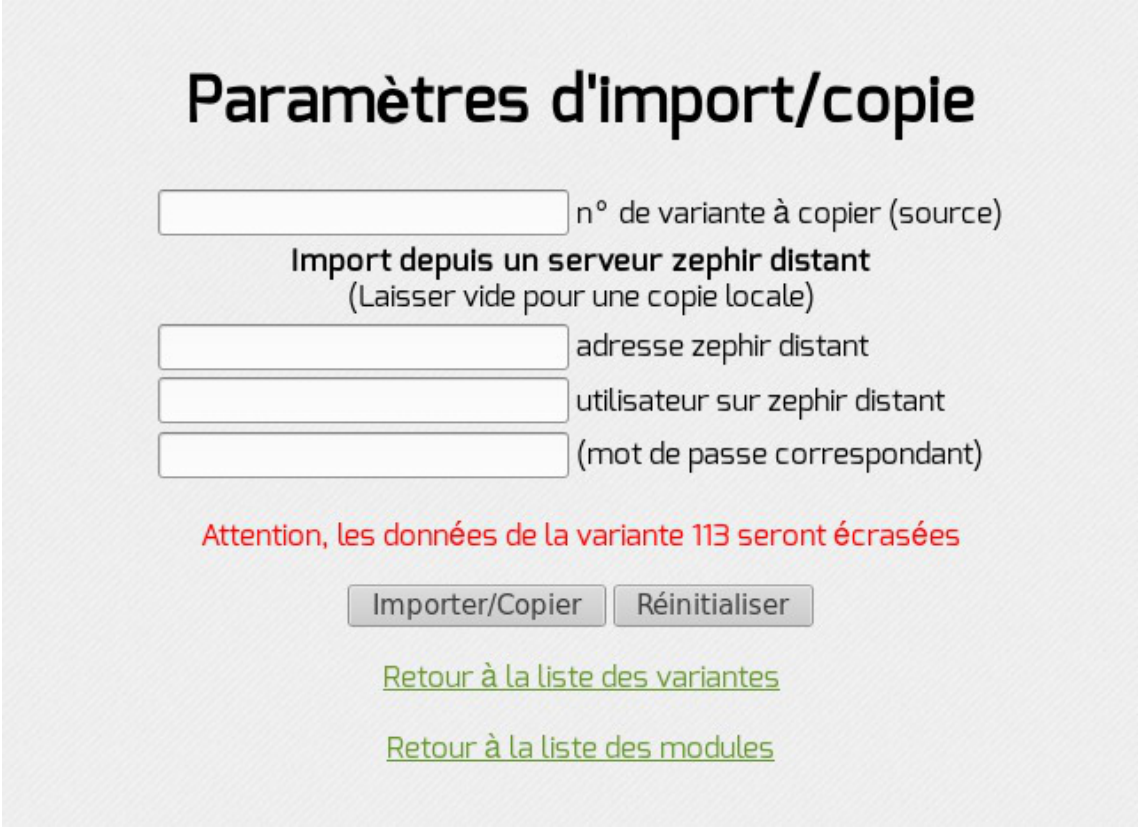
Vous pouvez échanger des variantes entre deux serveurs Zéphir.

Pour cela, créer une variante pour un module depuis l'application web `modules` / `variantes` / `ajouter une variante`.

Dans le menu des variantes, cliquer sur `importer/copier` à côté de votre nouvelle variante.



Dans la page qui apparaît, préciser l'adresse du serveur Zéphir où se trouve la variante que vous voulez récupérer, le numéro de cette variante sur celui-ci, ainsi que le compte et le mot de passe d'un utilisateur pouvant exporter des variantes.



4.12. Nouvelle gestion des dictionnaires Creole pour EOLE 2.4 et supérieur

La bibliothèque de dictionnaires

Principe général

Les dictionnaires Creole sont désormais communs à l'ensemble des modules d'une même version de la distribution EOLE.

Les dictionnaires livrés par les paquets de la distribution EOLE sont pré-installés sur le serveur Zéphir et sont activables au niveau d'une variante ou d'un serveur.

Les types de dictionnaires

- Les `dictionnaires de paquets` : Ces dictionnaires sont installés sur les serveurs clients par l'intermédiaire de paquets disponibles sur le serveur de mise à jour. Ils sont utilisés lors de la saisie de la configuration dans l'application web Zéphir, mais ne sont pas envoyés aux serveurs. Lorsqu'un paquet de dictionnaires est activé pour un module / variante / serveur, le paquet est ajouté à la liste des paquets à installer pour le(s) serveur(s) concerné(s).
- Les `dictionnaires locaux à Zéphir` : Ces dictionnaires sont présents sur le serveur Zéphir, mais ne sont pas liés à un paquet. Ils sont envoyés aux serveurs pour lesquels ils sont activés lors d'un envoi de configuration.

Dictionnaires par défaut d'un module

La liste des dictionnaires installés par défaut pour chaque module est gérée par un fichier, par exemple : `/usr/share/zephir/default_modules/6/amon-2.4` pour le module `Amon 2.4`.

Ce fichier contient la liste des paquets de dictionnaires installés par défaut (par exemple : eole/eole-proxy).

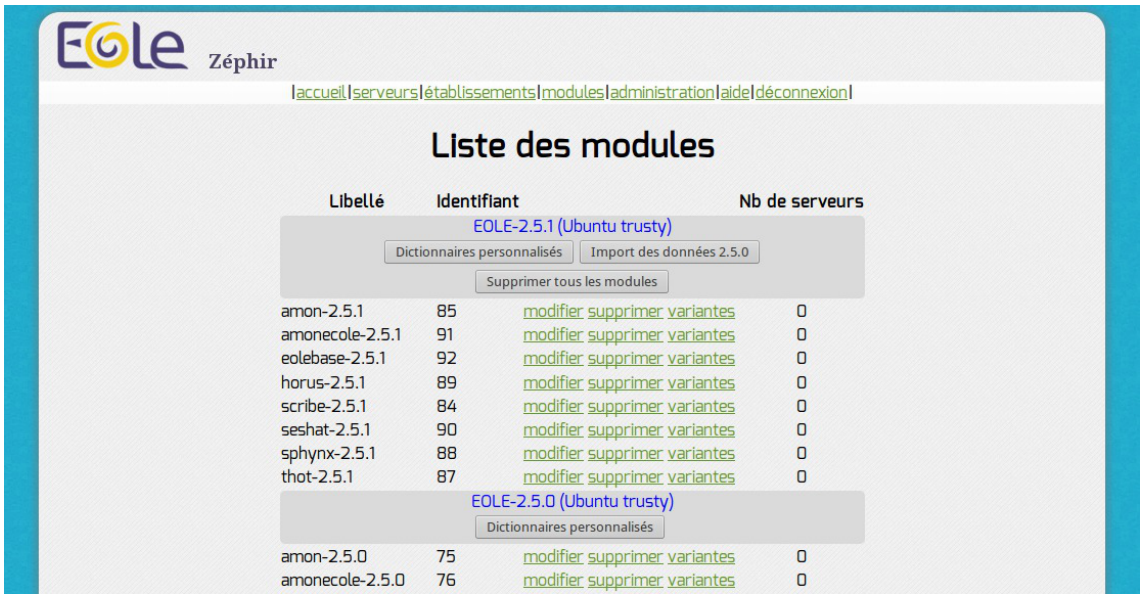
Pour les modules n'utilisant pas ce mode de gestion des dictionnaires (2.3 et antérieurs), le fichier existe mais est vide.

- Dans l'ancien mode, chaque module possède un répertoire avec une copie des dictionnaires par défaut.
- Dans le nouveau mode, des liens sont créés vers les dictionnaires de chaque paquet activé.

Gestion des dictionnaires locaux

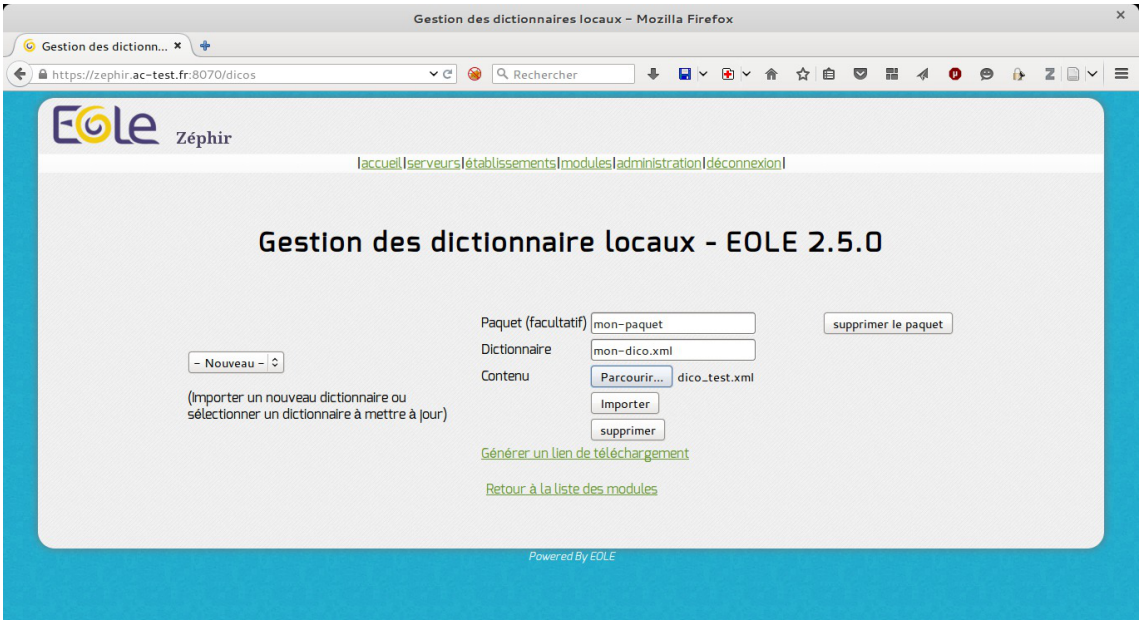
Une interface de gestion des dictionnaires additionnels est disponible pour les versions de la distribution les supportant.

L'accès se fait par l'entrée `modules` du menu et en cliquant sur le bouton `Dictionnaires personnalisés`.



L'interface permet de :

- mettre à jour le contenu d'un dictionnaire existant ;
- ajouter un nouveau dictionnaire (lié à un paquet ou local au serveur Zéphir) ;
- supprimer un dictionnaire existant ;
- supprimer un paquet de dictionnaires ;



Ajout d'un nouveau paquet de dictionnaires

Dictionnaires livrés par EOLE

Les paquets de dictionnaires disponibles dans la distribution EOLE sont pré-installés par défaut sur le serveur Zéphir. Ils ne peuvent être ni modifiés ni supprimés.

Sur le serveur Zéphir les dictionnaires sont stockés dans les répertoires suivants :

- `/usr/share/zephir/dictionnaires/2.4/local/*.xml` : dictionnaires locaux au serveur Zéphir ;
- `/usr/share/zephir/dictionnaires/2.4/local/<nom_paquet/*.xml` : dictionnaires livrés par des paquets hors distribution EOLE ;
- `/usr/share/zephir/dictionnaires/2.4/eole/<nom_paquet>/*.xml` : dictionnaires de la distribution EOLE ;

Seule la partie `/local/` est gérée par la page d'édition de la bibliothèque, les dictionnaires livrés par EOLE sont maintenus par les paquets de l'application Zéphir.

Utilisation sur les serveurs et variantes

Une fois les dictionnaires renseignés au niveau de la bibliothèque, il devient possible de les activer / désactiver pour une variante d'un module ou pour un serveur particulier.

- pour une variante, aller dans l'onglet `modules` puis dans `variantes` (lien sur la ligne du module en question) puis sur `modifier` ;
- pour un serveur, aller sur la `page d'état d'un serveur` et cliquer sur le lien `fichiers personnalisés`.

Une liste déroulante devrait apparaître dans la section correspondant aux dictionnaires. Sélectionnez le dictionnaire / paquet de dictionnaires voulu et validez le formulaire.

Activation d'un paquet de dictionnaires dans une variante

Si un dictionnaire ou paquet est activé au niveau d'une variante, il ne sera pas proposé dans la liste des fichiers personnalisés des serveurs de celle-ci (il apparaîtra dans la colonne `variante`.

À propos des paquets de dictionnaires

Dans le cas d'un paquet de dictionnaires, le paquet apparaîtra également dans la section `paquets additionnels`.

En passant le pointeur de la souris sur un nom de paquet dans la section des dictionnaires activés, les fichiers livrés par celui-ci seront indiqués.

Cohérence des dictionnaires activés

Les dépendances ne sont pas gérées automatiquement. Par exemple, si vous activez un paquet d'application web sur un module Eolebase, il faudra également activer `eole-web` et `eole-mysql`.

Après l'ajout de nouveaux dictionnaires, il est conseillé de :

- lancer une édition de la configuration du serveur (pour une variante: `changer les valeurs par défaut`) pour vérifier qu'il ne manque pas de variables (il suffit de vérifier que l'interface d'édition se lance correctement) ;
- Dans le cas d'une variante, il est également recommandé d'effectuer un `envoi de configuration` sur un serveur témoin pour valider le fonctionnement.

Activer le mode conteneur sur un serveur

Dans le cas où vous voulez activer le mode conteneur sur un serveur dont ce n'est pas le mode par défaut (par exemple, le module Amon), il faut activer dans les fichiers personnalisés du serveur les paquets de dictionnaires suivants :

- eole-lxc-controller
- eole-apt-cacher-ng

Vous pouvez également faire cette manipulation au niveau d'une variante pour activer le mode conteneur sur tous les serveurs de la variante.

Envoi des dictionnaires aux serveurs

Lors de l'appel à l'action `envoi de configuration` à un serveur géré par le serveur Zéphir, les dictionnaires activés sont pris en compte de la façon suivante :

- les dictionnaires locaux au serveur Zéphir (non gérés par un paquet) sont envoyés au serveur
- les dictionnaires de paquets (paquets EOLE activés mais non installés par défaut, ou paquets non EOLE) ne sont pas envoyés, mais les paquets concernés sont installés sur le serveur client si il n'est pas déjà présent.

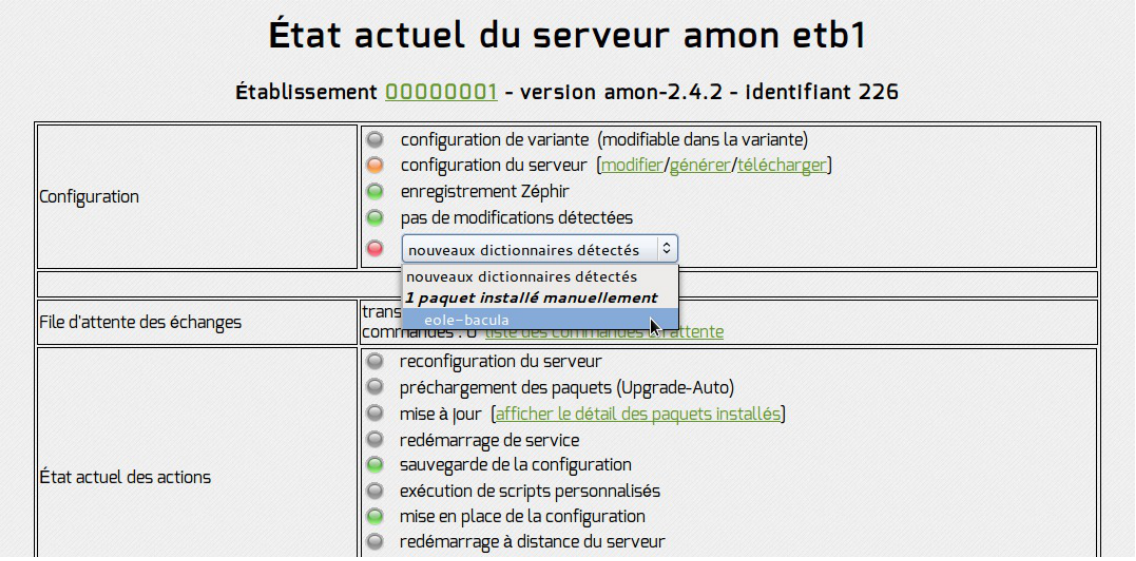
Détection des paquets avec dictionnaires installés manuellement sur un serveur

Si un utilisateur installe un paquet contenant des dictionnaires sans passer par le serveur Zéphir, certains problèmes peuvent survenir :

- si le serveur Zéphir effectue un envoi de configuration sans avoir fait de sauvegarde auparavant, les valeurs saisies sur d'éventuelles nouvelles variables seront perdues ;
- en cas d'édition de la configuration depuis l'application Zéphir, les nouvelles variables n'apparaîtront pas (même si les valeurs sont présentes dans le fichier de valeurs).

Pour limiter les risques, le serveur Zéphir vérifie à chaque synchronisation des serveurs si de nouveaux paquets de ce type ont été installés (paquets livrés par la distribution EOLE, ou paquets `locaux` déclarés sur le serveur Zéphir). Si c'est le cas, différentes alertes et messages apparaissent dans l'application :

- un courrier électronique est envoyé aux utilisateurs surveillant le serveur en question dans l'application Zéphir ;
- la diode présente sur la page d'état du serveur passe au rouge, et les paquets sont affichés dans une liste ;



- Cette diode est également affichée dans la page d'affichage d'un groupe de serveurs (colonne `dicos`) ;

- un message d'information est affiché dans le cadre dictionnaires de la page des fichiers personnalisés du serveur (les paquets sont en rouge dans la liste des paquets disponibles) ;
- dans la page d'action sur un serveur ou groupe de serveurs, un message d'avertissement est affiché en dessous du bouton d'envoi de configuration pour informer des risques potentiels.

Pour résoudre le problème :

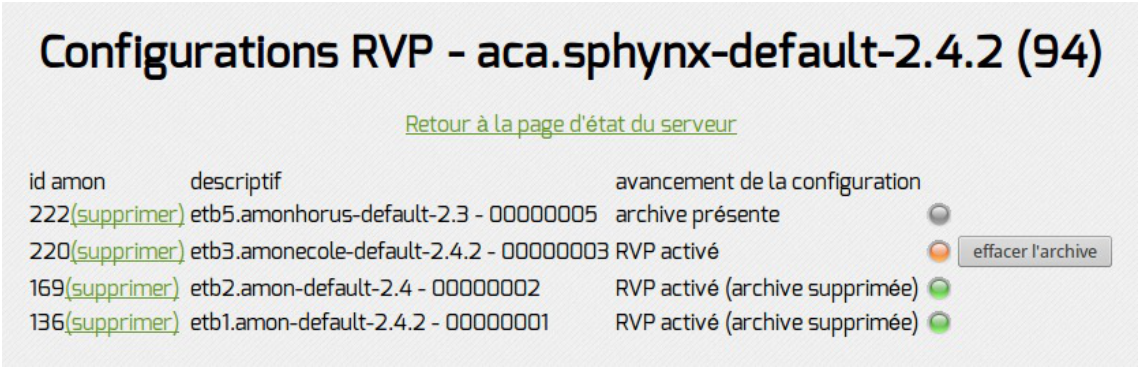
- activer le paquet manquant au niveau de la variante ou au niveau du serveur ;
- demander une sauvegarde de l'état du serveur pour récupérer la configuration locale, ou éditer la configuration depuis le serveur Zéphir et envoyer la configuration au serveur.

> Un critère de recherche a été ajouté dans l'onglet `serveurs` / `Sélection d'un groupe de serveurs` sous forme de case à cocher ☑ `Serveurs sur lesquels une installation manuelle de dictionnaires est détectée`.

4.13. Fonctions spécifiques à certains modules

4.13.1. Gestion des configurations RVP

4.13.1.a. Page de listing des configurations RVP



liste des configurations RVP enregistrées pour un Sphynx

Cette page est accessible depuis la page d'état d'un serveur Sphynx enregistré sur le serveur Zéphir. Elle permet de lister les configurations RVP des Amon remontées par ce serveur Sphynx. Les stades suivants de configuration apparaissent lors du déploiement :

- archive de configuration reçue (équivalent de la disquette échangée par le serveur Sphynx et le serveur Amon) : voyant gris ;
- archive récupérée par le serveur Amon et encore présente sur le serveur Zéphir : voyant jaune ;
- archive récupérée par le serveur Amon et supprimée sur le serveur Zéphir : voyant vert ;
- archive supprimée avant sa récupération par le serveur Amon (ce cas ne devrait pas se présenter) : voyant rouge clignotant.

Il est possible de supprimer l'archive une fois celle-ci récupérée par le serveur Amon. La ligne correspondante reste listée pour conserver un historique. Le bouton supprimer à coté de l'identifiant du serveur Amon supprime l'archive et la ligne correspondante dans la base de données.

4.13.1.b. Enregistrement et mise en place des configuration RVP

Serveur Sphynx 2.2 et antérieur

Pour mettre en place un fichier de configuration RVP, il faut se connecter sur le serveur Sphynx et renseigner depuis le menu de gestion du serveur Sphynx l'identifiant du serveur Amon correspondant.

Le serveur Zéphir envoie les informations concernant le serveur Amon au serveur Sphynx, qui génère la configuration et l'envoie sur le serveur Zéphir.

Serveur Sphynx 2.3 ou supérieur

La gestion des configuration RVP est effectuée par l'intermédiaire de l'application ARV. Consulter la documentation du module Sphynx pour plus d'information.

Récupération de la configuration sur un serveur Amon

Lors de l'instance sur le module Amon, choisissez l'activation RVP par le serveur Zéphir, en indiquant l'identifiant (Zéphir) du serveur Sphynx. Les fichiers (certificats, configuration des tunnels) sont récupérés automatiquement. Répéter l'opération pour activer des tunnels sur différents serveurs Sphynx (procédure active_rvp).

4.13.2. Réplication LDAP entre un serveur Scribe/Horus et un serveur Seshat

Les modules Scribe et Horus disposent de fonctions pour répliquer leur annuaire sur un serveur Seshat (annuaire centralisé).

Zéphir permet de simplifier cette mise en œuvre.

Pré-requis

Serveur Scribe ou Horus

- la réplication LDAP (fournisseur) doit être activée dans l'interface de configuration du module (dans l'onglet `Openldap`, en mode expert).

Réseau

- le port 389 et/ou le port 636 (selon la configuration mise en place) doit être ouvert du serveur Seshat vers le serveur Scribe ou Horus et si possible dans le sens inverse.

Mise en œuvre

Si le serveur Scribe (ou Horus) et le serveur Seshat sont enregistrés sur le même serveur Zéphir, celui-ci peut se charger de la mise en place de la configuration sur le serveur Seshat.

La mise en œuvre de la réplication se fait depuis le serveur Scribe ou Horus en exécutant le script `active_replication.py`

Si le serveur Scribe (ou Horus) est enregistré, la connexion à Zéphir est proposée automatiquement en fin d'exécution du script :

```
Veuillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :
```

Il est impératif de connaître l'identifiant Zéphir du serveur Seshat pour finaliser la transaction.

```
Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :
```

```
root@scribe:~# active_replication.py

Utilisation du compte de réplication existant

Génération de la configuration client
Répliquer également les groupes [oui/non]
[non] : oui
Ajouter des uid à exclure de la réplication [oui/non]
[non] : oui
uid à exclure (entrée pour terminer la saisie) :
Adresse utilisée pour accéder au module Scribe depuis le client
[10.1.3.5] :
LDAP n'est pas activé sur le port SSL : utilisation du protocole ldap (port 389)

Ecriture du fichier /root/replication-00000001.conf

Envoi de la configuration sur Zephir

Veuillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :admin_zephir
Mot de passe pour admin_zephir :

Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :226
Cette configuration sera prise en compte par le serveur
de réplication lors de sa prochaine connexion à Zéphir

fin
root@scribe:~#
```

Les configurations de réplication envoyées *via* Zéphir sont consultables dans l'application web Zéphir en utilisant le lien `configurations de réplication LDAP` disponible sur la page décrivant l'état du serveur Seshat.

Consultation des configurations de réplications LDAP dans l'application Zéphir

Les configurations envoyées *via* Zéphir sont stockées dans le répertoire `/etc/ldap/replication/zephir` du serveur Seshat.

Voir aussi...

Réplication LDAP

4.13.3. Synchronisation depuis l'Annuaire Académique Fédérateur - AAF

Fonctionnement général de la synchronisation

1. la machine ODI[p.233] génère une archive `tar.gz` par établissement à synchroniser ;

2. dès l'archive terminée, elle est envoyée sur le module Zéphir accompagnée d'une notification ;
3. le module Zéphir envoie l'archive sur le module Scribe auquel elle a été associée ;
4. le module Scribe lance l'import de l'archive (mode automatique) ou la stocke pour l'EAD (mode manuel).

Comment récupérer les fichier tar.gz ?

Information et documentation à retrouver sur le site **intranet** de diffusion de l'académie de Toulouse :

http://nservdiff.in.ac-toulouse.fr/appli/infra/versions/ver_majaaf.html [http://nservdiff.in.ac-toulouse.fr/appli/infra/versions/ver_majaaf.html]

Guide utilisateur 1.5 en version format privateur `.doc` :

http://nservdiff.in.ac-toulouse.fr/appli/infra/documentation/aaf/Guide_UtilisateurV1_5.doc

Guide d'exploitation 1.5 en version format privateur `.doc` :

http://nservdiff.in.ac-toulouse.fr/appli/infra/documentation/aaf/Dossier_exploitationV1_5.doc

Association archive - module Scribe

L'association d'un module Scribe avec son archive se fait pour l'instant manuellement, à l'aide du code python suivant :

```
import xmlrpclib
z = xmlrpclib.Server("https://utilisateur:codeSecret@adresse_zephir:7080")
z.aaf.add_file(idZéphir, 'nomArchive.tar.gz')
```

Pour afficher la liste des archives associées au module Scribe possédant l'identifiant Zéphir `idZéphir` :

```
z.aaf.get_list(idZéphir)
```

Pour supprimer l'association entre l'archive et le module Scribe :

```
z.aaf.del_file('nomArchive.tar.gz')
```

Dans cet exemple, on associe l'archive `0000001a.tar.gz` au module Scribe possédant l'identifiant `58` dans l'application web Zéphir :

```
import xmlrpclib
z = xmlrpclib.Server("https://user:password@adresse_zephir:7080")
z.aaf.add_file(58, '0000001A.tar.gz')
```

Pour afficher la liste des archives associées au module Scribe possédant l'identifiant 58 dans l'application web Zéphir :

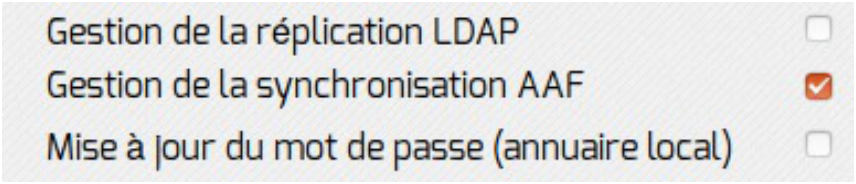
```
z.aaf.get_list(58)
```

Pour supprimer l'association entre l'archive `0000001A.tar.gz` et le module Scribe :

```
z.aaf.del_file('0000001A.tar.gz')
```

L'utilisateur Zéphir utilisé pour effectuer les manipulations décrites ci-dessus doit posséder le

droit `Gestion de la synchronisation AAF` dans l'application Zéphir.



Envoi des fichiers sur le module Zéphir

Les archives générées (de la forme `<numéro UAI>.tar.gz`) doivent être envoyées dans le répertoire : `/var/lib/zephir/aaf`.

L'envoi des fichiers peut être réalisé par la méthode de votre choix : `rsync`, `scp`, ...

Une fois l'archive envoyée, il faut notifier cet envoi au module Zéphir.

Cela peut être fait par les lignes python suivantes :

```
import xmlrpclib
z = xmlrpclib.Server("https://utilisateur:codeSecret@adresse zephir:7080")
z.aaf.notify_upload('numeroUAI.tar.gz')
```

L'utilisateur Zéphir utilisé pour effectuer les manipulations décrites ci-dessus doit posséder le droit `Gestion de la synchronisation AAF` dans l'application Zéphir.

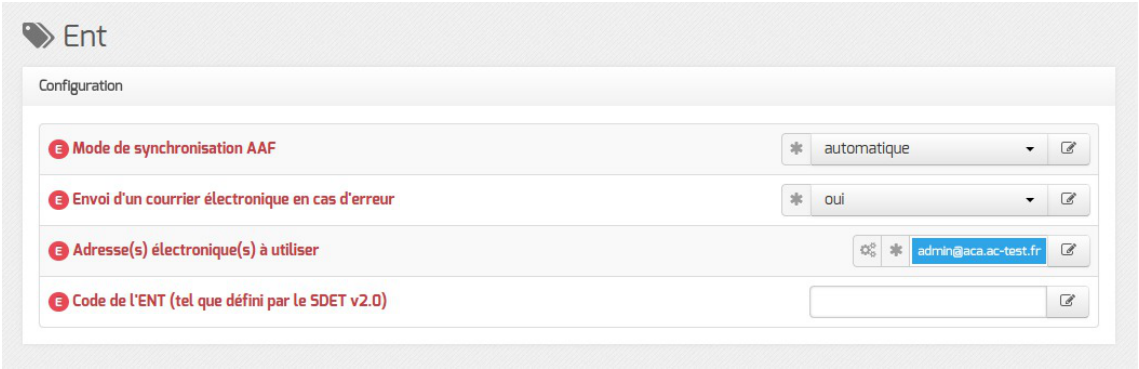
Gestion de l'archive sur le module Scribe

Dès que le module Zéphir est notifié de l'arrivée d'une nouvelle archive, il prépare son envoi vers le module Scribe qui lui est associé (sauf si l'archive possède la même signature que sa version précédente).

Le module Scribe récupère l'archive lors de sa connexion au module Zéphir.

Il est possible de configurer la façon dont le module importe les données de l'archive récupérée.

Cela se paramètre dans l'interface de configuration du module, en mode expert, dans l'onglet `Ent`.



La variable `Mode de synchronisation AAF` permet de choisir entre deux modes :

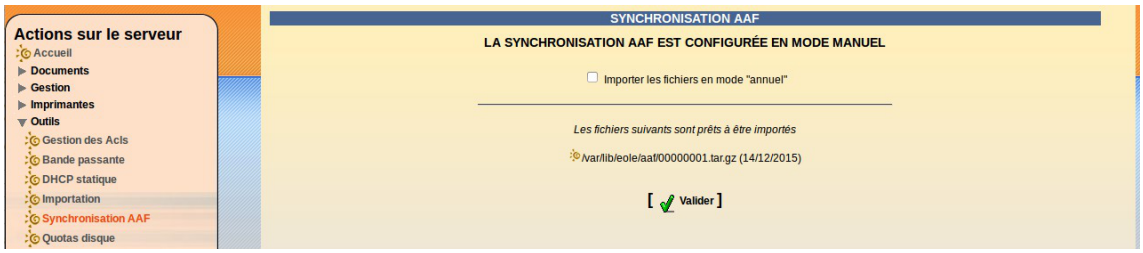
- **automatique** : l'importation des fichiers est exécutée dès leur réception ;
- **manuel** : l'archive est stockée et l'importation est prête à être exécuté par l'EAD (menu `Outils` / `Synchronisation AAF`).

La variable `Envoi d'un courrier électronique en cas d'erreur` active l'envoi d'un

courrier électronique en cas d'erreur lors de l'import manuel ou automatisé des fichiers AAF. Le ou les destinataires de ce message sont à ajouter dans `Adresse(s) électronique(s) à utiliser`.

Si le module Scribe est configuré en mode manuel, l'import des archives envoyées sur le module Scribe se réalise à la demande en allant dans l'EAD.

Le formulaire d'import est accessible par le menu `Outils` / `Synchronisation AAF`.



Importation des fichiers AAF synchronisés via l'EAD

Par défaut l'import est réalisé en mode *Mise à jour des bases*, mais il est possible de l'effectuer en mode *Importation annuelle des bases* en cochant la case `☑ Importer les fichiers en mode "annuel"`.

- *Mise à jour des bases* : ajoute les utilisateurs et groupes manquants sans modifier les groupes existants ;
- *Importation annuelle des bases* : ajoute les utilisateurs et groupes manquants après avoir purgé les options (import des élèves) ou les équipes pédagogiques (import des professeurs).

L'import peut également être exécuté en ligne de commande en utilisant le script `synchro_aaf` avec comme paramètre l'un des fichiers cité dans `/var/lib/eole/aaf/aaf_files/`.

Exemple de boucle en bash[p.230] qui permet de traiter tous les fichiers :

```
for f in `cat /var/lib/eole/aaf/aaf_files`; do
    /usr/bin/synchro_aaf $f
done
```

Suivi de la synchronisation et de l'importation

Agent Zéphir

Un agent Zéphir permet de vérifier le bon déroulement de l'envoi des fichiers sur le module.

L'agent de surveillance de la synchronisation des fichiers AAF

Application web Zéphir

Des informations sont également disponibles en allant dans `Logs complets` depuis la page d'état de l'un des serveurs Scribe et en filtrant sur `divers`.

Surveillance de la prise en compte des fichiers AAF dans Zéphir

Rapports d'importation

L'importation des fichiers AAF synchronisés utilise les même scripts que l'importation habituelle, on retrouve donc les rapports de l'importation AAF aux endroits suivants :

- page d'accueil de l'EAD (`/usr/share/ead2/backend/tmp/importation/rapport.txt`) ;
- répertoire personnel de l'utilisateur `admin` : `/home/a/admin/perso/importation` ;
- journaux complets : `/var/log/eole/importation.log`.

4.14. Installation de paquets supplémentaires avec clés de signature

Pour installer des paquets supplémentaires Ubuntu, par PPA[p.234] ou des paquets réalisés en interne, il est indispensable de vérifier leur signature pour être sûr qu'ils ne sont pas modifiés par un tiers entre leur mise à disposition et leur installation.

La solution pour éviter l'utilisation de la commande `apt-key add` sur chacun des serveurs est de générer un trousseau de clefs, de l'exporter au format texte dans le répertoire `/etc/apt/trusted.gpg.d/` puis d'ajouter le fichier généré à la liste des fichiers divers d'une variante Zéphir.

Exporter une clef au format texte :

```
user@machine:~$ gpg --export -a eole@ac-test.fr > clef-gpg.txt
```

Importer la clef dans un keyring dédié :

```
user@machine:~$ gpg --no-default-keyring --keyring
ac-test-keyring.gpg --import < clef-gpg.txt
```

> Il faut ensuite intégrer le fichier `.gpg` dans la variante pour qu'il soit installé dans `/etc/apt/trusted.gpg.d/`
> Il faut ensuite intégrer le fichier `.list` dans la variante pour qu'il soit installé dans `/etc/apt/sources.list.d/`

> Le fichier GPG est pris en compte durant l'installation des paquets lors de l'exécution de la commande `enregistrement_zephir`.

5. Changement de l'adresse IP du serveur Zéphir

Sur le serveur Zéphir, le script `/usr/share/zephir/utils/prepare_ip.py` permet de préparer les serveurs enregistrés à un changement d'adresse IP du serveur Zéphir.

Le lancement de la commande `prepare_ip.py` nécessite un compte Zéphir et la nouvelle adresse du serveur Zéphir.

```
root@zephir:~# /usr/share/zephir/utils/prepare_ip.py

Entrez votre login zephir (rien pour sortir) : admin_zephir
Mot de passe zephir pour admin_zephir :

Entrez la nouvelle adresse du serveur zephir : 192.168.0.30

Envoi de l'adresse aux serveurs ...

L'adresse a été définie pour 1 serveurs

Adresse non envoyée aux serveurs suivants :

  1, 6, 4, 2, 11, 9, 3, 5, 8, 7, 10, 12, 13, 18, 16

root@zephir:~#
```

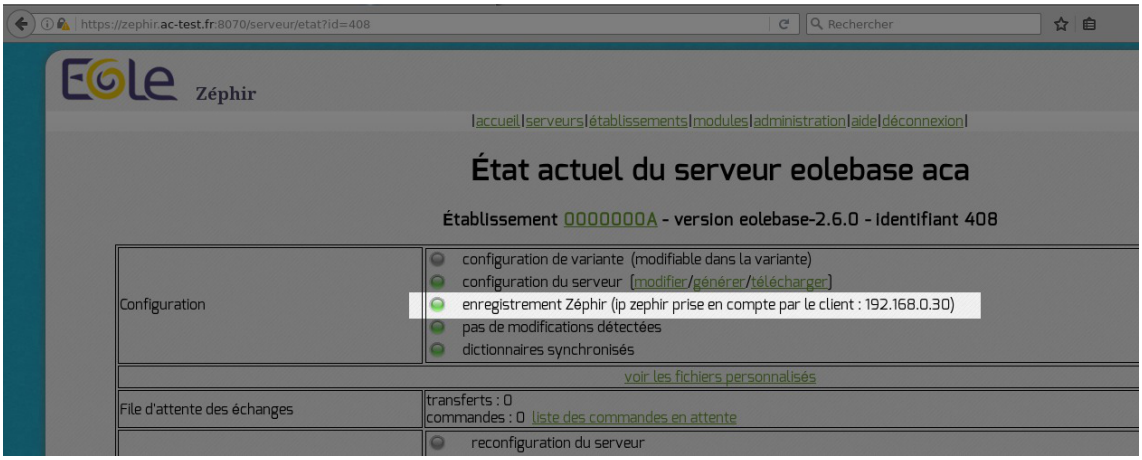
Pendant cette étape, le serveur Zéphir va générer les nouvelles clés et ajouter une action d'envoi de la clé à tous les clients.

> La commande `/usr/share/zephir/utils/prepare_ip.py --help` permet d'avoir de l'aide sur les options du script.

L'utilisation de l'option --check (ou -c) `usr/share/zephir/utils/prepare_ip.py -c` permet de vérifier l'avancement de la prise en compte du changement par les différents serveurs.

Il y a plusieurs états possibles pour les serveurs enregistrés :

- serveur non préparé : il n'y a pas de nouvelle clé disponible pour ce serveur ;
- serveur en attente de récupération de l'adresse : une clé est disponible sur le serveur Zéphir, mais le client ne l'a pas prise en compte ;
- serveur ayant récupéré l'adresse : le client a confirmé avoir récupéré la nouvelle adresse.



Les 2 derniers états sont affichés sous forme de message dans la page d'état du serveur.

Une fois que tous les serveurs ont confirmé avoir récupéré la nouvelle adresse IP du serveur Zéphir, le changement peut être effectué.

- changer l'adresse du serveur Zéphir via l'interface de configuration du module ;
- appliquer la modification à l'aide de la commande `reconfigure`.

Les serveurs se connecteront automatiquement sur cette nouvelle adresse et confirmeront leur nouvelle clé d'échange au serveur Zéphir.

Le commande `usr/share/zephir/utils/prepare_ip.py -c` permet de vérifier l'état d'avancement.

Les serveurs doivent tous repasser dans l'état "non préparé" après s'être connectés au serveur Zéphir.

La commande `/usr/share/zephir/utils/prepare_ip.py -p` (ou --purge) permet d'annuler un changement d'adresse IP demandé sur l'ensemble des serveurs.

Si des serveurs ont déjà récupéré la nouvelle adresse IP, ils seront notifiés de l'annulation à leur prochaine connexion.

6. Sauvegarde / Restauration

Des scripts de sauvegarde et de restauration des données sont intégrés au serveur Zéphir.

Ces scripts sont à utiliser pour effectuer un changement de machine ou un changement de version majeure du module EOLE Zéphir.

Sauvegarde

Pour effectuer une sauvegarde, exécuter la commande `sauvegarde.sh` sur le serveur Zéphir.

```
root@zephir:~# sauvegarde.sh

Sauvegarde en cours, veuillez patienter ...
 - base PostgreSQL
 - base LDAP
 - configuration des serveurs
```

```
 - clés de connexion
 - configuration EOLE
 - configuration EAD et certificats SSL
 - configuration d'EoleSSO
 - dictionnaires personnalisés
 - fonctions CREOLE personnalisées
 - modules personnalisés
Compression de l'archive...

Archive créée : /var/lib/zephir_backups/29-11-2016-15h36.tar.gz

root@zephir:~#
```

Il n'y a rien de particulier à faire dans cette procédure. Le fichier de sauvegarde créé est `/var/lib/zephir_backups/'date du jour'.tar`.

Les sauvegardes générées sont stockées localement. Il est recommandé de sauvegarder le répertoire `/var/lib/zephir_backup/` avec un système de sauvegarde externe.

Restauration sur la même machine

La restauration s'effectue via la commande `restauration.sh`. Une liste des sauvegardes présentes est affichée. Entrer le nom de la sauvegarde à restaurer (date de création de la sauvegarde).

```
root@zephir:~# restauration.sh
     Utilitaire de restauration Zéphir

!! Attention : toutes les modifications effectuées
   après la sauvegarde restaurée seront perdues !!

Liste des sauvegardes présentes :

29-11-2016-15h36

Sauvegarde à restaurer (rien pour sortir): 29-11-2016-15h36
Arrêt du service Zéphir...
Décompression en cours...
Vérification des données...
Restaurer la base de données (o/n) ? o

 - base PostgreSQL
 - initialisation de la base
 - injection des données
 - régénération du mot de passe
 - mise à jour du schéma de la base
 - base LDAP
 - configuration des serveurs
 - dictionnaires personnalisés
 - modules personnalisés
 - configuration EAD
 - certificats SSL
 - configuration EoleSSO
 - configuration EOLE

La configuration présente avant restauration a été copiée sous /etc/eole/config.old
Pour reprendre cette version, copier ce fichier sur /etc/eole/config.eol

```

```
Reconfigurez le serveur après la fin de la restauration


Système restauré

root@zephir:~#
```

Attention, toutes les données modifiées depuis la sauvegarde (serveurs enregistrés, journaux, variantes, ...) seront perdues lors de la restauration.

Restauration sur une nouvelle machine

Récupérer l'archive de sauvegarde ,soit depuis l'ancien serveur Zéphir, soit depuis la sauvegarde des archives.

Créer le répertoire `/var/lib/zephir_backups` sur la nouvelle machine sur laquelle le module Zéphir est fraîchement installé :

```
# ssh root@zephir.ac-test.fr "mkdir -p /var/lib/zephir_backups"
```

Copier l'archive sur la nouvelle machine sur laquelle le module Zéphir est fraîchement installé :

```
# scp 04-10-2016-10h09.tar.gz root@zephir:/var/lib/zephir_backups/
```

Pour exécuter la restauration sur une nouvelle machine non instanciée il faut préciser le chemin absolu de la commande `/usr/share/eole/restauration.sh` (en effet les PATHS ne sont pas encore renseignés).

```
root@zephir:~# /usr/share/eole/restauration.sh
     Utilitaire de restauration Zéphir

!! Attention : toutes les modifications effectuées
   après la sauvegarde restaurée seront perdues !!

Liste des sauvegardes présentes :

30-11-2016-14h25

Sauvegarde à restaurer (rien pour sortir): 30-11-2016-14h25
Arrêt du service Zéphir...
Décompression en cours...
Vérification des données...
Restaurer la base de données (o/n) ? o

 - base PostgreSQL
 - initialisation de la base
 - injection des données
 - régénération du mot de passe
 - mise à jour du schéma de la base
 - base LDAP
 - configuration des serveurs
 - dictionnaires personnalisés
 - modules personnalisés
 - configuration EAD
 - certificats SSL
 - configuration EoleSSO
 - configuration EOLE

```

```
Le fichier /etc/eole/config.eol est différent de la version restaurée
Le fichier présent avant restauration a été sauvegardé sous /etc/eole/config.old
Pour reprendre cette version, copier ce fichier sur /etc/eole/config.eol

Utilisez la commande instance sans écraser la base de données


Système restauré

root@zephir:~#
```

Enfin il faut instancier le serveur à l'aide de la commande `instance`.

Répondre `non` à la question proposant de re-créer les utilisateurs et les données de base.

```
[...]
*run-parts: executing /usr/share/eole/posttemplate/10-conf-zephir instance

## Regénération des mots de passe ##
Voulez-vous re-créer les utilisateurs et données de base (attention toutes les
données actuelles seront perdues) ? [oui/non]
[non] : non
Start System V service postgresql
[  OK  ]
L'utilisateur admin_zephir n'est pas présent dans l'annuaire, renseignez son mot de
passe ci-dessous

################################################################################
# Initialisation du mot de passe de l'administrateur de base (admin_zephir) #
################################################################################
Mot de passe :
[...]
```

7. Migration vers le module Zéphir 2.5.n

Le serveur Zéphir est le premier serveur à migrer lorsqu'une nouvelle version de la distribution est disponible. Zéphir gère les serveurs dont la version est inférieure ou égale à sa propre version (à l'exception de Zéphir 2.3 qui gère jusqu'à la version 2.4.1)

Les procédures de migration de Zéphir gérées actuellement sont :

- Depuis Zéphir 2.3 vers Zéphir 2.5.n : Vérifier que le serveur est bien à jour en version stable, puis :
  - Lancer le script `sauvegarde.sh` et mettre de côté l'archive générée ;
  - Installer la version voulue de Zéphir et effectuer une mise à jour stable (de préférence, conserver l'ancienne machine temporairement en cas de soucis) ;
  - Mettre en place l'archive créée précédemment dans `/var/lib/zephir_backups` sur le nouveau serveur
  - Pour exécuter la restauration sur une nouvelle machine non instanciée il faut préciser le chemin absolu de la commande `/usr/share/eole/restauration.sh` (en effet les PATHS ne sont pas encore renseignés).
  - Éditer et sauvegarder la configuration avec `gen_config` et lancer `instance` (répondre `non` lorsqu'il est demandé de recréer les données).
- Depuis Zéphir 2.5.n vers Zéphir 2.5.n+x :

- Utiliser le script `Maj-Release` pour effectuer la mise à niveau du serveur (La configuration de Zéphir sera adaptée automatiquement si besoin) ;
- reconfigurer le serveur.

8. Migration vers le module Zéphir 2.6

Le serveur Zéphir est le premier serveur à faire migrer lorsqu'une nouvelle version de la distribution est disponible. Zéphir gère les serveurs dont la version est inférieure ou égale à sa propre version (à l'exception de Zéphir 2.3 qui gère jusqu'à la version 2.4.1 et à l'exception de Zéphir 2.6 qui ne gère qu'à partir de la version 2.4).

Les procédures de migration de Zéphir gérées actuellement sont :

- Depuis Zéphir 2.3 vers Zéphir 2.6.n : Vérifier que le serveur est bien à jour en version stable, puis :
  - Lancer le script `sauvegarde.sh` et mettre de côté l'archive générée ;
  - Installer la version voulue de Zéphir et effectuer une mise à jour stable (de préférence, conserver l'ancienne machine temporairement en cas de soucis) ;
  - Mettre en place l'archive créée précédemment dans `/var/lib/zephir_backups/` sur le nouveau serveur
  - Pour exécuter la restauration sur une nouvelle machine non instanciée il faut préciser le chemin absolu de la commande `/usr/share/eole/restauration.sh` (en effet les PATHS ne sont pas encore renseignés).
  - Éditer et sauvegarder la configuration avec `gen_config` et lancer `instance` (répondre `non` lorsqu'il est demandé de recréer les données).

Sur un module Zéphir 2.6, les serveurs EOLE en version égale ou inférieure à 2.3 ne sont plus gérés.

Si la base est importée dans la nouvelle version de Zéphir, tous les serveurs 2.3 seront supprimés.

Une solution consiste à migrer tous les serveurs en version EOLE 4 ou EOLE 2.5 pour ensuite effectuer la migration du serveur Zéphir en 2.6.

Si des migrations sont souhaitées vers 2.6 alors qu'il existe encore des serveurs en 2.3. Il faut passer par le déploiement d'un deuxième serveur Zéphir pour permettre la transition.

Plusieurs scénarios sont possibles et certains plus intéressants en fonction du nombre de serveurs en version 2.3 et en version 2.6.

- les nouveaux serveurs 2.6 peuvent être enregistrés sur un serveur Zéphir 2.6 provisoire. Il faudra réintégrer les serveurs 2.6 enregistrés sur le Zéphir courant après sa migration en

version 2.6 ;

- l'utilisation de la procédure de sauvegarde/restauration sur un nouveau serveur Zéphir 2.6 permet d'importer tous les serveurs sauf les serveurs en version 2.3. L'adresse IP de l'ancien serveur Zéphir devra être changée et les serveurs en version 2.3 devront être re-enregistrés sur celui-ci. La migration pourra se faire jusqu'à la version 2.5.2 et il faudra les réintégrer sur le nouveau serveur Zéphir pour les faire migrer en version 2.6.

Dans les deux cas il faut procéder à un ré-enregistrement d'une partie des serveurs, cependant le ré-enregistrement provoque la perte de l'identifiant du serveur, des autorisations et des groupes de serveurs.

- Depuis Zéphir 2.5.2 vers Zéphir 2.6 :
  - Utiliser le script `Upgrade-Auto` pour effectuer la mise à niveau du serveur (La configuration de Zéphir sera adaptée automatiquement si besoin) ;
  - reconfigurer le serveur.

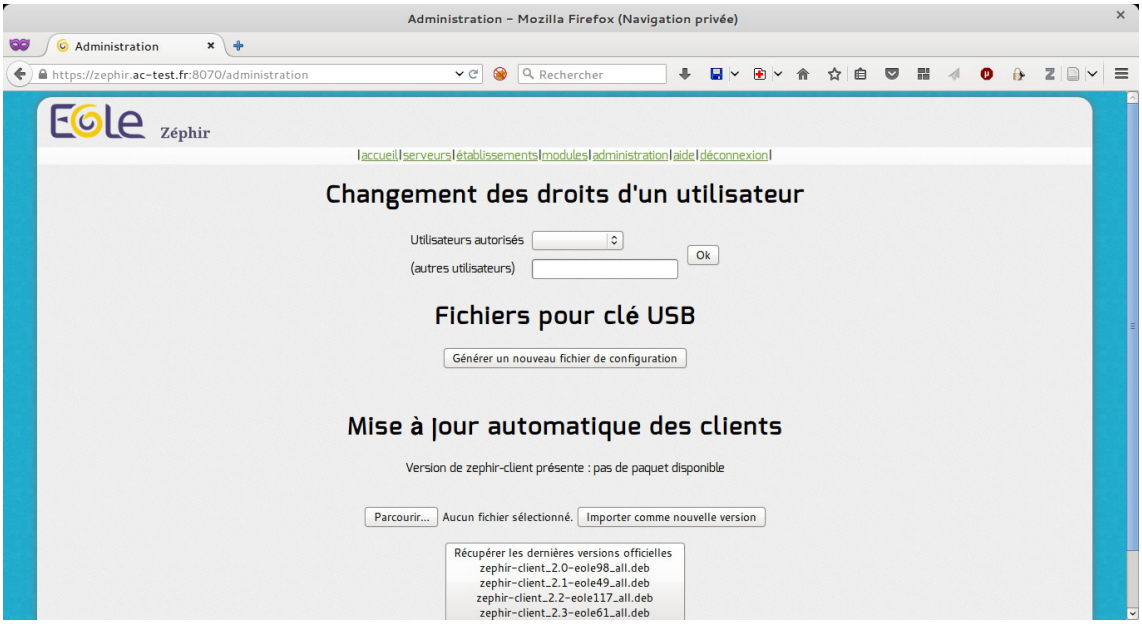
- Depuis Zéphir 2.6.n vers Zéphir 2.6.n+x :
  - Utiliser le script `Maj-Release` pour effectuer la mise à niveau du serveur (La configuration de Zéphir sera adaptée automatiquement si besoin) ;
  - reconfigurer le serveur.

9. Divers petits outils

9.1. Génération de fichiers de configuration pour clé USB

Le serveur Zéphir permet de simplifier la procédure d'enregistrement par l'intermédiaire d'un fichier de configuration stocké sur une clé USB qui peut ensuite être utilisé sur un site de production par d'autres personnes (en établissement scolaire par exemple) pour associer le module au serveur Zéphir.

Pour créer un fichier de configuration, il faut se rendre dans l'onglet `administration` de l'application Zéphir et cliquer sur le bouton `Générer un nouveau fichier de configuration`.



Vous arrivez alors sur un formulaire vous permettant de spécifier un certain nombre de paramètres qui seront utilisés par défaut à l'enregistrement du serveur.

Génération de fichiers de configuration pour clé USB

Une fois le formulaire validé avec le bouton Générer le fichier, une deuxième page s'affiche avec un résumé des paramètres saisis, ainsi qu'un lien vers le fichier à télécharger.

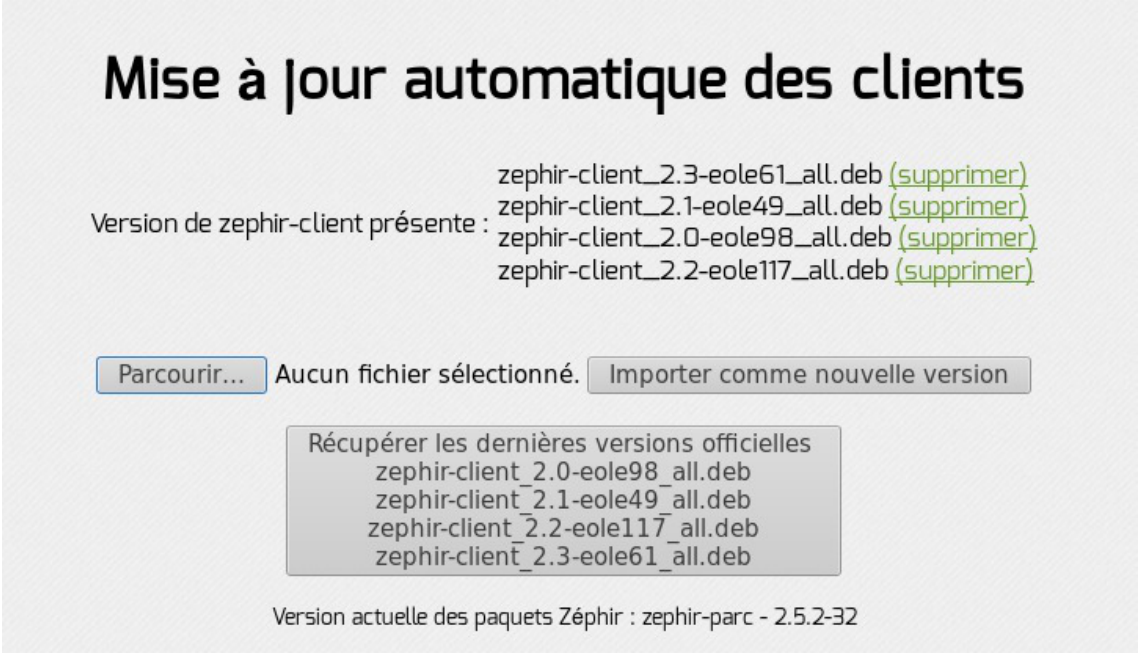
Enregistrer le fichier en faisant un clique droit et enregistrer la cible du lien sous le nom `zephir.conf`. Le fichier doit être placé à la racine d'une clé USB. Vous pouvez ensuite distribuer ce fichier aux personnes chargées d'installer les serveurs sur site (en établissement) pour leur éviter de saisir eux même les paramètres de connexion au serveur Zéphir.

La clé devra être montée manuellement sur le répertoire `/mnt/removable/` qu'il faut créer.

9.2. Mise à jour automatique du paquet zephir-client

Dans l'onglet `administration` de l'application Zéphir il est possible de préparer une mise à jour automatique de la partie cliente des serveurs.

Il est possible d'importer la dernière version du paquet `zephir-client` téléchargée directement sur les serveurs de diffusion d'EOLE. Une fois récupéré il faut cliquer sur le bouton `Parcourir` et choisir la version du paquet `zephir-client` et appuyer alors sur le bouton `Importer comme nouvelle version`.



Mise à jour automatique des clients Zéphir

Une nouvelle page affiche le nom du fichier envoyé. Lorsqu'un client effectuera une procédure d'enregistrement, il se mettra à jour avec cette nouvelle version de `zephir-client`.

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 Zéphir

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-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un serveur OpenLDAP.

L'installation d'`eole-annuaire` entraîne celle d'`eole-client-annuaire`.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

http://www.openldap.org/

Historique

L'annuaire LDAP est la brique centrale de plusieurs modules EOLE.

Grâce au paquet `eole-annuaire`, la configuration de base est identique sur les modules Horus, Scribe, Zéphir, Seshat et Thot bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `annuaire (id=10)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.2. eole-client-annuaire

Le paquet `eole-client-annuaire` permet de configurer l'utilisation d'un annuaire OpenLDAP distant (ou local dans le cas où le paquet `eole-annuaire` est également installé).

Logiciels et services

Le paquet `eole-client-annuaire` fournit les outils de base pour interroger et s'authentifier sur un annuaire OpenLDAP.

http://www.openldap.org/

Historique

Ce paquet est présent sur tous les modules fournissant un annuaire (Horus, Scribe, Zéphir, Seshat et Thot) et également sur ceux utilisant un annuaire comme base d'authentification (Eclair, Hâpy).

Conteneurs

Par défaut, la configuration LDAP cliente est déployée sur le maître mais les templates EOLE fournis par ce paquet sont également utilisés dans les conteneurs en fonction des besoins.

1.3. 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)`.

1.4. 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).

1.5. eole-postgresql

Le paquet `eole-postgresql` permet la mise en place d'un serveur de base de données PostgreSQL.

Logiciels et services

Le paquet `eole-postgresql` s'appuie principalement sur le service postgresql.
http://www.postgresql.org

Historique

Uniquement utilisé sur Zéphir, le paquet `eole-postgresql` est installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `postgresql (id=11)`.

À ce jour, aucun module EOLE n'implémente l'utilisation de ce service en mode conteneur.

2. Ports utilisés sur le module Zéphir

Le module Zéphir propose de nombreux services.
Ce document donne la liste exhaustive des ports utilisés sur un module Zéphir standard.

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 Zéphir

- 22/tcp : uucp-SSH
- 389/tcp : ldap (OpenLDAP)
- 636/tcp : ldaps (OpenLDAP sur le port SSL)
- 5432/tcp : PostgreSQL
- 7080/tcp: Zéphir-backend (publique), remontée des logs
- 7081/tcp : Zéphir-backend (restreint)
- 8070/tcp : application web Zéphir
- 8090/tcp : mise à jour automatique du client Zéphir

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. Ports à ouvrir sur le Pare-feu

Les serveurs distants doivent pouvoir accéder à Zéphir sur les ports suivants :

- 22/tcp : uucp-SSH
- 7080/tcp : remontée des logs
- 8090/tcp : mise à jour automatique du client Zéphir

Dans certains cas il peut être nécessaire d'ouvrir des ports supplémentaires :

- 8070/tcp : application web Zéphir, si Zéphir est utilisé en frontend
- 7000/tcp : gen_config, si l'administrateur est amené à faire du gen_config à distance

4. Arborescence de la configuration des serveurs sur Zéphir

Données associées aux modules et à leurs variantes

Les données concernant les modules EOLE sont stockées dans le répertoire `/var/lib/zephir/modules`.

Il qui contient, pour chaque module, identifié par un numéro de module, les dictionnaires et les données de ses différentes variantes.

Il est possible des définir des variantes pour chaque module, avec les informations suivantes :

- des dictionnaires supplémentaires ;
- les fichiers listés dans ces dictionnaires ;
- des patchs ;
- des fichiers quelconques devant être sauvegardés sur Zéphir ;
- un fichier dico.eol permettant de pré-remplir les variables de configuration.

Données des serveurs

Le répertoire `/var/lib/zephir/conf` contient un dossier par établissement, qui contient lui même un répertoire par serveur déclaré dans l'établissement.

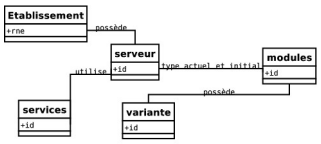
Les répertoires des serveurs contiennent les données suivantes :

- une clé RSA permettant de faire passer UUCP à travers SSH ;
- des dictionnaires supplémentaires ;
- des fichiers listés dans ces dictionnaires ;
- des patchs ;

- les fichiers de configuration UUCP du serveur ;
- un fichier zephir.eol correspondant à config.eol sur le serveur ;
- un lien sur le dictionnaire du module ;
- un lien sur dico.eol de la variante ;
- les répertoires fichier_zephir, fichiers_persos, dicos et patchs contiennent des liens sur les dossiers équivalents de la variante.

5. Méthodologie du serveur de commande

Le serveur de commande est composé d'une base de données PostgreSQL qui n'est accédée que par ce serveur XML-RPC qui se charge de faire toute les requêtes (accès, édition, modification...)



Modèle de la base

6. Présentation de l'API

L'API permet d'automatiser certaines tâches peu pratiques dans l'application web (génération batch de configurations de migration, mise à jour de groupes existants, ...).

Toutes les fonctions présentes dans l'application web sont accessibles via XML-RPC[p.237].

L'aide au développement se trouve dans l'application web Zéphir à l'adresse :
`https://<adresse_zephir>:8070/aide/devel/`
Les fonctions de l'API sont documentées et disponibles à l'adresse :
`https://<adresse_zephir>:8070/aide/api`/

Exemple 1 - Affichage d'information

Dans cet exemple le script se connecte sur le serveur Zéphir et propose de choisir un des modules 2.4.1 pour afficher l'ID, le RNE, le serveur DNS et les adresses IP des interfaces eth0 et eth1.

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-
import xmlrpclib, getpass, sys

# fonction d'affichage de chaque serveur du groupe.
def affichage_infos(zephir_proxy):
    """récupère des valeurs de configuration sur un groupe de serveurs"""
    rc, liste_modules = zephir_proxy.modules.get_module()
    print "\n* modules 2.4.1 disponibles *\n"
    modules = {}
    for module in liste_modules:
        if module['libelle'].endswith('-2.4.1'):
            print module['id'], " - ", module['libelle']
            # dictionnaire id_module -> libelle
            modules[module['id']] = module['libelle']
    id_module = raw_input('\nchoix du module : ')
    try:
        assert int(id_module) in modules.keys()
    except:
        sys.exit('Erreur, module invalide')
    # critères de séléction (d'autres critères sont possibles : rne, variante, libelle ...)
    criteres_selection = {'module_actuel':id_module}
    # récupération du groupe de serveurs correspondants
    rc, groupe_serv = zephir_proxy.serveurs.groupe_serveur(criteres_selection)
    for serveur in groupe_serv:
        # affichage des données pour chaque serveur : (identifiant, rne, adresses dns, eth0 et eth1)
        rc, config = zephir_proxy.serveurs.get_config(serveur['id'])
        print '\n* serveur %s (etablissement %s) :' % (serveur['id'], serveur['rne'])
        if 'adresse_ip_dns' in config: print '- dns : ', config['adresse_ip_dns']
        print '- ip eth0 : ', config['adresse_ip_eth0']
        if 'adresse_ip_eth1' in config: print '- ip eth1 : ', config['adresse_ip_eth1']

if __name__ == '__main__':
    # executé si lancement du script en ligne de commande
    user = raw_input("\nlogin Zéphir de l'utilisateur : ")
    pwd = getpass.getpass("mot de passe                  : ")
    zephir_proxy = xmlrpclib.ServerProxy('https://%s:%s@192.168.0.20:7080' % (user, pwd))
    affichage_infos(zephir_proxy)
```

Exemple 2 - Affichage d'information avec interaction

Dans cet exemple le script se connecte sur le serveur Zéphir et propose de choisir un groupe de machine ou une version de module pour afficher l'ID, le RNE, le serveur DNS et les adresses IP des interfaces eth0 et eth1.

```python
#!/usr/bin/env python
# -*- coding: UTF-8 -*-
################################
#
# script basique pour récupérer des valeurs de configuration sur un groupe de serveurs
#

import xmlrpclib, getpass, sys


def selection_serveurs(zephir_proxy):

    # exemple : utiliser un groupe existant
    rc, liste_groupes = zephir_proxy.serveurs.get_groups()
    print "* groupes disponibles *"
    # affichage id et libelle des groupes
    groupes = {}
    for groupe in liste_groupes:
        print groupe[0], " - ", groupe[1]
        # dictionnaire id_groupe -> libelle, liste des serveurs
        groupes[groupe[0]] = (groupe[1], groupe[2])
    print ""
    id_groupe = raw_input('choix du groupe (rien pour choisir un module) : ')
    if id_groupe != '':
        try:
            id_groupe = int(id_groupe)
            assert id_groupe in groupes.keys()
        except:
            sys.exit('Erreur, groupe inconnu')
        # récupération des serveurs de ce groupe
        rc, groupe_serv = zephir_proxy.serveurs.groupe_reload(groupes[id_groupe][1])
        print "\nServeurs du groupe %s : " % groupes[id_groupe][0]
        return groupe_serv

    # récupération par type de module si pas de groupe demandé
    # si besoin, on peut récupérer la liste des variantes avec zephir_proxy.modules.get_variantes()
    rc, liste_modules = zephir_proxy.modules.get_module()
    print "* modules disponibles *"
    # affichage id et libelle des groupes
    modules = {}
    for module in liste_modules:
        print module['id'], " - ", module['libelle']
        # dictionnaire id_module -> libelle
        modules[module['id']] = module['libelle']
    print ""
    id_module = raw_input('choix du module : ')
    try:
        id_module = int(id_module)
        assert id_module in modules.keys()
    except:
        sys.exit('Erreur, module invalide')
    # critères de séléction des serveurs (d'autres critères sont possibles : rne, variante, libelle ...)
    criteres_selection = {'module_actuel':id_module}
    # récupération du groupe de serveurs correspondants
    rc, groupe_serv = zephir_proxy.serveurs.groupe_serveur(criteres_selection)
    print "\nServeurs de type %s : " % modules[id_module]
    return groupe_serv

# fonction d'affichage de chaque serveur du groupe.
def affichage_infos(zephir_proxy, groupe_serveur):

    print ""
    for serveur in groupe_serv:
        # affichage des données pour chaque serveur : identifiant, rne, adresse dns, adresses eth0 et eth1 si disponible
        rc, config = zephir_proxy.serveurs.get_config(serveur['id'])
        print '* serveur %s (etablissement %s) :' % (serveur['id'], serveur['rne'])
        if 'adresse_ip_dns' in config:
```

Exemple du retour d'affichage des informations :

```
choix du module : 54
Serveurs de type amon-2.4.1 :
* serveur 115 (etablissement 00000001) :
- dns : 192.168.232.2
- ip eth0 : 192.168.0.31
- ip eth1 : 10.1.1.1
* serveur 118 (etablissement 00000001) :
- dns : 192.168.232.2
- ip eth0 : 192.168.0.31
- ip eth1 : 10.1.1.1
```

Exemple 3 - Affichage d'information avec interaction et authentification

Dans cet exemple le script, proposé par Karim Ayari, se connecte sur le serveur Zéphir, demande une authentification, récupère la valeur d'une variable ou de plusieurs variables sur une machine ou sur un groupe de machine.

```
#!/usr/bin/python
# -*- coding: UTF-8 -*-
# Karim Ayari
# DSI - Rectorat de Lyon
# récupére la valeur d'une variable demandée

import xmlrpclib, getpass, sys, os, socket
from zephir.backend import serveurs_rpc
from pyeole.ansiprint import print_red,print_green
from getpass import getpass


def GetVar(variable,amon=None,val=None,groupe=None):
    """
    récupére la valeur d'une ou plusieurs variables
    """
    if amon != "" and amon != None and variable != "":
        config = zephir_proxy.serveurs.get_config(amon)
        print amon,config[1]['libelle_etab']
        for var_ in variable.split(","):
      try:
          config[1][var_]
      except KeyError:
          print_red("La variable '%s' n'existe pas !" % (var_))
      else:
                print var_,config[1][var_]
    elif variable != "" and val != None and amon == "" and groupe != None:
        #on récupére le groupe
        gr = zephir_proxy.serveurs.get_groups()
        #groupe
        for gr_ in enumerate(gr[1]):
            if gr_[1][1] == groupe:
                amons=gr_[1][2]
        #on cherche dans les configurations des amons
        res=[]
        for idz in amons:
      for var_ in variable.split(","):
                config = zephir_proxy.serveurs.get_config(idz)
                try:
                    val in config[1][var_]
                except KeyError:
                    print "%s | %s | Existe pas" % (idz, config[1][
'libelle_etab'])
                    pass
                else:
              #on stocke le résultat (id zéphir) dans une liste pour
traitement.
              res.append(idz)
              #on affiche le résultat (id et nom établissement)
                    print "%s : %s | %s | %s" % (var_,idz, config[1][
'libelle_etab'], config[1][var_])


if __name__ == "__main__":
    user = raw_input("Utilisateur Zephir: ")
    password = getpass("mot de passe pour %s :" % user)
```

```
    try:
        zephir_proxy = xmlrpclib.ServerProxy('http://%s:%s@127.0.0.1:7081'
 % (user, password))
    except:
        raise
    else:
  val = None
  groupe = None
  amon = None
        amon = raw_input("Id zéphir du serveur ? laisser vide pour saisir
un groupe : ")
        if amon == "":
            groupe = raw_input("Saisir le nom du groupe : ")
            variante = raw_input("Saisir le nom de la variante : ")
        variable = raw_input("Quelle variable interroger (séparer par , si
plusieurs) : ")
        if variable != "":
            val = raw_input("Valeur à rechercher : ")
        GetVar(variable,amon,val,groupe)
```

Exemple du retour d'affichage des informations :

```
Utilisateur Zephir: admin_zephir
mot de passe pour admin_zephir :
Id zéphir du serveur ? laisser vide pour saisir un groupe :
Saisir le nom du groupe : Amon261
Saisir le nom de la variante :
Quelle variable interroger (séparer par , si plusieurs) :
maxchildren1,maxchildren2
Valeur à rechercher :
maxchildren1 : 236 | etab1 | 256
maxchildren2 : 236 | etab1 | 256
```

7. Le client Zéphir

Les scripts du client Zéphir sont dans le répertoire `/usr/share/zephir/scripts/` fournis par le paquet `zephir-client`.

Bien que l'utilisation de ces scripts ne soit pas prévu pour fonctionner tel quel il est possible de les exécuter manuellement.

Ces scripts correspondent le plus souvent à des actions programmable depuis Zéphir web.

Le script `zephir_client` regarde si le paramètre est une fonction sinon il cherche un script `.zephir` correspondant dans le répertoire.

Exemple de fonction interne :

`# /usr/share/zephir/scripts/zephir_client del_lock` permet de supprimer les verrous du client Zéphir

Exemple d'un script `.zephir` :

`# /usr/share/zephir/scripts/zephir_client save_files` permet de faire remonter les modifications locales sur le serveur Zéphir

Pour utiliser les `.zephir` il faut donc les passer en paramètre de la commande zephir_client sans l'extension :

```
# zephir_client nomDuScript
```

D'autres scripts sont utilisables et dans le PATH :

- `enregistrement_zephir` : permet l'enregistrement du serveur sur le serveur Zéphir ;
- `synchro_zephir` : permet de déclencher manuellement la synchronisation avec le serveur.

8. Annuaire : diagnostic et résolution de problème

Exécuter le service en mode débogage

Les commandes suivantes permettent de relancer le service *slapd* en mode débogage :

```
# service slapd stop
# slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 256
```

L'option -d pour le débogage est suivie de la valeur de masquage 256 qui offre la verbosité nécessaire.

Ré-indexer l'annuaire

Dans certaines situations, la ré-indexation de l'annuaire s'avère nécessaire.

Les commandes suivantes permettent de re-créer les fichiers d'index :

```
# service slapd stop
# su openldap -s /bin/bash -c "slapindex -f /etc/ldap/slapd.conf -v"
```

Sauvegarde et restauration de l'annuaire

Export automatique de l'annuaire

Sur les modules EOLE possédant un annuaire local, un export de l'annuaire est réalisé toutes les nuits dans le fichier `/home/backup/sauv_ldap.ldif`.

C'est le cas même si la sauvegarde Bareos n'est pas activée car c'est `eole-schedule` qui gère l'export.

La programmation de l'export quotidien peut-être vérifiée à l'aide de la commande suivante :

```
# manage_schedule -l
```

Si l'export automatique est bien activé, les lignes suivantes apparaissent dans le résultat :

```
  * les tâches journalières se feront tous les jours à 01:14 (hors sauvegarde)
   - avant sauvegarde
    + Exportation de l'annuaire LDAP (annuaire)
```

Restauration de l'export quotidien

En cas de crash de l'annuaire OpenLDAP, restaurer l'annuaire tel qu'il était la nuit précédente peut permettre de gagner du temps sur la mise à disposition des services.

La restauration s'effectue à l'aide des commandes habituelles :

```
# service slapd stop
# rm -f /var/lib/ldap/[^D]*
# slapadd -f /etc/ldap/slapd.conf -l /home/backup/sauv_ldap.ldif
# chown -R openldap: /var/lib/ldap/
# service slapd start
```

Restauration de la dernière sauvegarde

Dans le cas où la sauvegarde Bareos est utilisée, il est possible de restaurer l'annuaire tel qu'il était lors de la dernière sauvegarde.

La restauration de l'annuaire depuis la sauvegarde s'effectue à l'aide de la commande :

```
# bareosrestore.py --ldap
```

Export manuel de l'annuaire

La commande suivante permet d'exporter le contenu de l'annuaire dans un fichier :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > annuaire.ldif
```

Voir aussi...

- Gestion des tâches planifiées eole-schedule
- Restauration partielle

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 :

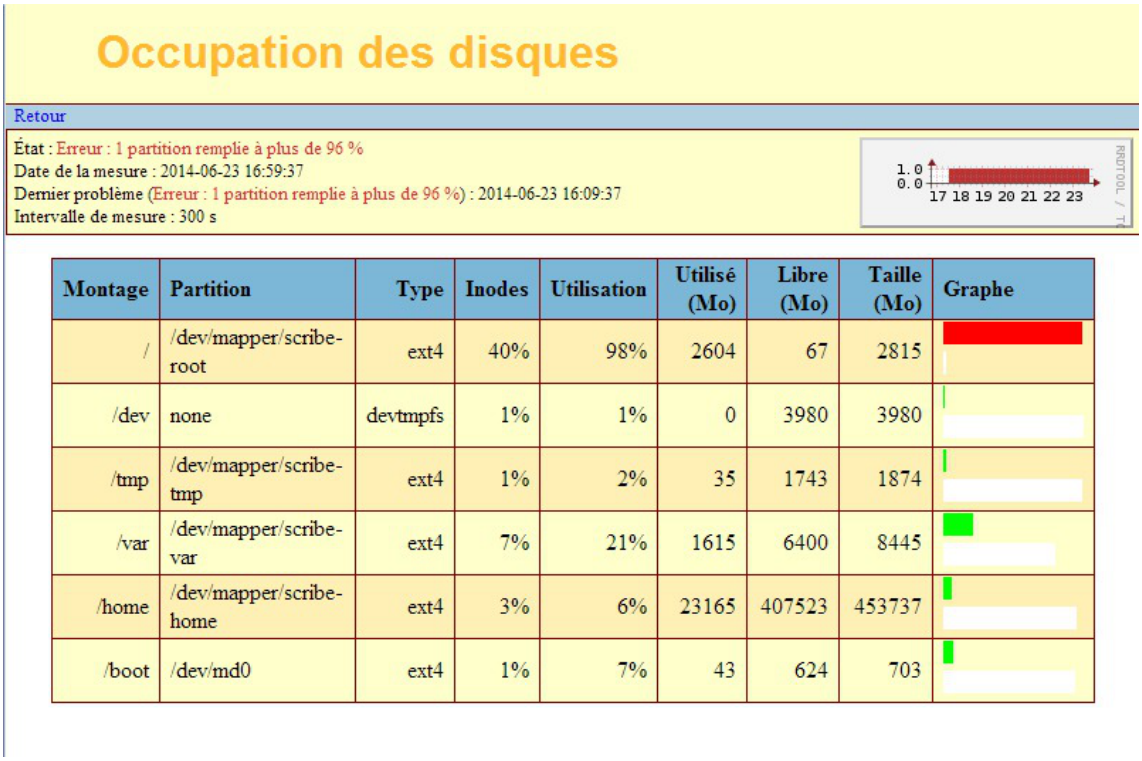
```
Échec de la connexion sécurisée
Une erreur est survenue pendant une connexion à IP:Port.
Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :
Votre certificat contient le même numéro 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

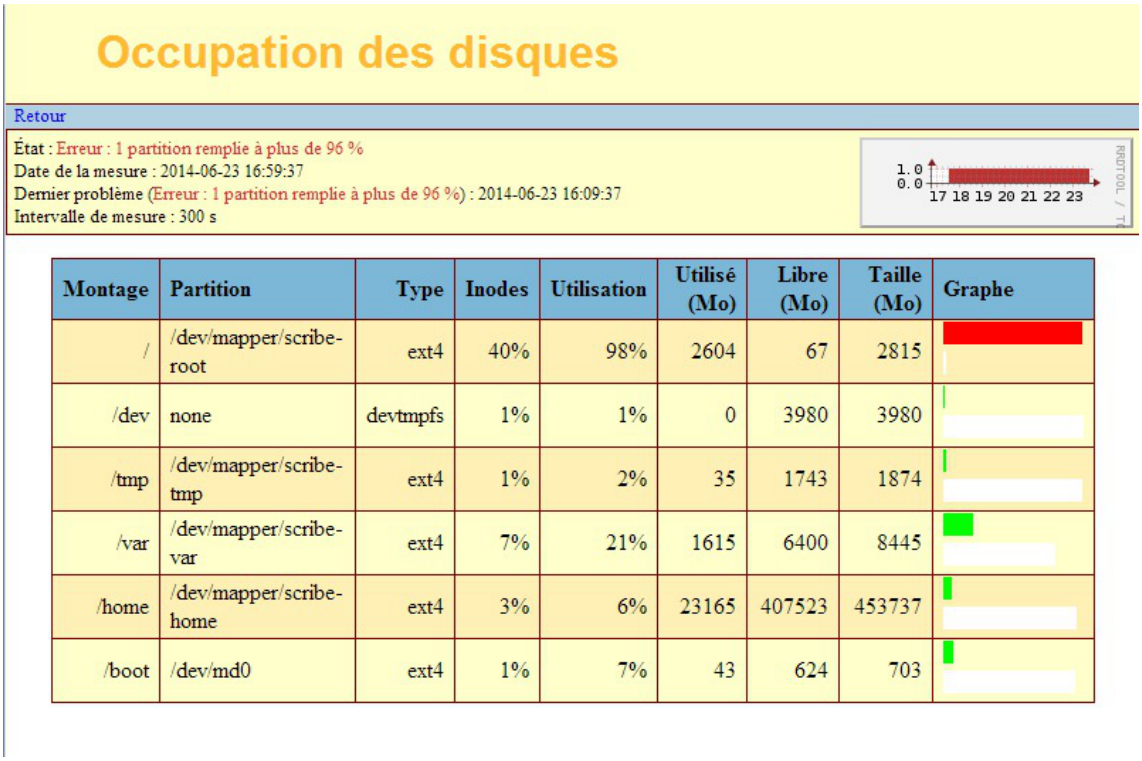
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	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 / T

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. 232]).

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. 232]).

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.236] 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 Zéphir

Depuis une session sur un serveur client, comment forcer l'exécution immédiate des actions mises en attente sur le module Zéphir ?

Il peut être intéressant de forcer la récupération des actions en attente sur le serveur Zéphir.

Utilisation du script `synchro zephir`

Le script `synchro zephir` va forcer la synchronisation auprès du serveur Zéphir

(remontée des statistiques et exécutions des actions).

```
root@amonecole:~# synchro_zephir
Demande de synchronisation au service z_stats : ok
La synchronisation avec Zéphir est en cours, vous pouvez suivre les transferts UUCP :
# tail -f /var/log/uucp/Log
Le résultat des éventuelles des actions lancées sera disponible dans les fichiers suivants :
/var/log/zephir/last_action.log (dernière action exécutée)
/var/log/zephir/actions.log (actions précédentes)
root@amonecole:~#
```

L'appel du script `synchro zephir` provoque une erreur se terminant par `socket.error: [Errno 111] Connection refused`

Le script `synchro zephir` fait appel au service `z_stats`, cette erreur se produit si celui-ci est arrêté.

Relancer le service z_stats

Relancer le service avec la commande :

```
# service z_stats restart && synchro_zephir
```

Les statistiques ou la liste des paquets installés d'un serveur ne remontent pas sur Zéphir

Les commandes restent en attente.

Les transferts de fichiers et de commandes utilisent le protocole UUCP au travers de SSH.

Les problèmes rencontrés le plus fréquemment sont les suivants:

- le port 22 (SSH) du serveur Zéphir est non accessible depuis le serveur client ;
- clé SSH est invalide pour l'utilisateur `uucp`

  Ce problème est détecté au lancement du script `synchro zephir`, qui proposera une solution pour corriger le problème
- divers problèmes ont été rencontrés au niveau du protocole UUCP, la commande `uulog` permet de voir les derniers logs. Le problème le plus courant est celui de fichiers corrompus dans le répertoire `/var/spool/uucp/`. Tous les fichiers et sous-répertoires (`.Status/.Temp,...`) peuvent être supprimés, à l'exception du répertoire `/var/spool/uucp/.ssh` qui contient la clé d'accès au serveur Zéphir.

Comment autoriser plusieurs utilisateurs à se connecter à un serveur sans les autoriser un par un

Dans l'application Zéphir, la démarche est la même que pour une clé.

Concaténer plusieurs clés dans un fichier

Concaténer plusieurs clés dans un fichier (avec saut de ligne entre chaque clé) et déposer ce fichier dans les préférences d'un seul utilisateur (par exemple, créer un compte générique dédié à cet usage).

Il suffit ensuite d'autoriser cet utilisateur à accéder aux serveurs d'un groupe pour que toutes les clés soient prises en compte.

Dans la gestion d'un groupe de serveurs, utiliser l'action `Envoyer la configuration au serveur` pour que les clés soient envoyées à chacun des serveurs du groupe.

Il n'est pas possible d'ajouter un dictionnaire personnalisé à un serveur (ou un module / une variante) EOLE 2.4

La gestion des dictionnaires personnalisés a été modifiée pour les serveurs 2.4.

Consulter la documentation de l'application Zéphir (cf. Présentation générale de l'application Zéphir) [p. 96].

J'ai saisi la configuration d'un serveur EOLE 2.4, mais je ne peux pas la modifier

Dans l'état actuel, l'application de saisie pour les serveurs 2.4 s'ouvre dans une fenêtre à part. Après l'avoir quitté, la page de l'application Zéphir n'est pas rechargée.

Actualisez la page pour faire apparaître le lien.

Les droits de l'utilisateur `admin_zephir` ne permettent plus la gestion des permissions

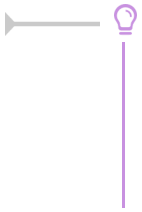
Pour remettre les droits de gestion des permissions à l'utilisateur `admin_zephir` il faut se connecter à la base de données.

Pour rétablir les droits utiliser les commandes suivantes :

```
# su - postgres
$ psql zephir
psql (8.4.20 ) Saisissez « help » pour l'aide.
zephir=# update users SET droits='[4]' where login='admin_zephir';
UPDATE 1
zephir=# \q
$ ctrl + d
#
```

Installation de paquets supplémentaires avec clés de signature

Pour installer des paquets supplémentaires Ubuntu, par PPA[p.234] ou des paquets réalisés en interne, il est indispensable de vérifier leur signature pour être sûr qu'ils ne sont pas modifiés par un tiers entre leur mise à disposition et leur installation.



La solution pour éviter l'utilisation de la commande `apt-key add` sur chacun des serveurs est de générer un trousseau de clefs, de l'exporter au format texte dans le répertoire `/etc/apt/trusted.gpg.d/` puis d'ajouter le fichier généré à la liste des fichiers divers d'une variante Zéphir.

Exporter une clef au format texte :

```
user@machine:~$ gpg --export -a eole@ac-test.fr > clef-gpg.txt
```

Importer la clef dans un keyring dédié :

```
user@machine:~$ gpg --no-default-keyring --keyring ac-test-keyring.gpg --import < clef-gpg.txt
```

Il faut ensuite intégrer le fichier `.gpg` dans la variante pour qu'il soit installé dans `/etc/apt/trusted.gpg.d/`

Il faut ensuite intégrer le fichier `.list` dans la variante pour qu'il soit installé dans `/etc/apt/sources.list.d/`

Le fichier GPG est pris en compte durant l'installation des paquets lors de l'exécution de la commande `enregistrement_zephir`.

Glossaire

Agent Zéphir	Les agents Zéphir sont des sondes qui génèrent divers statistiques et rapports sur les modules EOLE. Sur un module, elles sont consultables en HTTP sur le port 8090. Elles sont également accessibles via la page d'accueil de l'interface d'administration EAD. Si le module est enregistré sur un serveur Zéphir, ces données sont remontées à intervalles réguliers et sont susceptibles de générer des alertes centralisées dans l'interface web Zéphir.
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.
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/
bash *= Bourne-Again shell*	Bash est un interpréteur en ligne de commande de type script. C'est le shell Unix du projet GNU. Fondé sur le Bourne shell, Bash lui apporte de nombreuses améliorations, provenant notamment du Korn shell et du C shell. Bash est un logiciel libre publié sous licence publique générale GNU. Il est l'interprète par défaut sur de nombreux Unix libres, notamment sur les systèmes GNU/Linux. C'est aussi le shell par défaut de Mac OS X et il a été porté sous Microsoft Windows par le projet Cygwin. Source Wikipédia : http://fr.wikipedia.org/wiki/Bourne-Again shell

BIND *= Berkeley Internet Name Domain*	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet. http://www.isc.org/downloads/bind/
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.
cron	cron est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiées à l'avance, ou selon un cycle défini à l'avance.
CSV *= Comma-separated values*	Le CSV est un format informatique ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules. Il est souvent utilisé pour l'interopérabilité entre applications.
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/
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.
instance *= instanciation, instancier*	Instancier un serveur correspond à la troisième étape de mise ne œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande `instance`.
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/
MD5 *= Message Digest 5*	L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. Il a été inventé par Ronald Rivest en 1991. Source : https://fr.wikipedia.org/wiki/MD5
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
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`.
ODI *= Oracle Data Integrator*	ODI - Ex Sunopsis est un logiciel propriétaire de Oracle Corporation développé en java pour réaliser des tâches de type ETL/EAI. Les développements sont centralisés dans un référentiel stocké sur une base de données. Le référentiel stocke également l'ensemble des métadonnées permettant une vision globale du système d'information ainsi que des flux d'alimentation développés dans ODI. Le principal objectif d'ODI est de faciliter les développements et la maintenance par l'intermédiaire de références croisées, cet outil permet l'automatisation de l'échange entre toutes les applications du SI.
OTP *= One-time password*	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà

	utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisé par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir. Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique
PPA *= Personal Package Archives*	Les PPA sont des dépôts de paquets logiciels offerts aux individus et aux équipes de développeurs désireux de proposer facilement leurs logiciels pour les utilisateurs d'Ubuntu.
Ramsese *= Répertoire académique et ministériel sur les établissements du système éducatif*	Une base Ramsese est le fichier de gestion des établissements secondaires d'une académie : EPLE (établissements publics locaux d'enseignements) et EREA (établissements régionaux d'enseignements adaptés) publics et privés. Il contient toutes les informations concernant chaque établissement, notamment sa localisation, son code. Caractéristiques techniques : • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
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.
RNE *= UAI*	Depuis 1978, chaque établissement scolaire (écoles, collèges, lycées, CFA, enseignement supérieur, public ou privé) possède un code unique dans le répertoire national des établissements, aussi appelé RNE. En 1996, le « RNE » a changé de nom et s'intitule désormais « UAI » pour Unité Administrative Immatriculée qui concerne 135 000 établissements. Chaque établissement scolaire bénéficie d'un code UAI (ex-RNE) composé de 7 chiffres et d'une lettre (par exemple 0951099D) : • 3 premiers chiffres (095) qui correspondent au département (par exemple 012 pour l'Aveyron, 095 pour le Val-d'Oise, 974 pour la Réunion...) ; • 4 chiffres (1099) qui permettent d'identifier un établissement de façon unique dans le département ; • 1 lettre (D) qui sert de checksum (ou somme de contrôle) pour vérifier la bonne saisie du code. Cette dernière lettre est calculée ainsi : • on prend le nombre composé par les 7 premiers chiffres (exemple : 0951099) ;

	• on divise ce nombre par 23 et on garde le reste (exemple : reste de (0951099/23) = 3) ; • on prend ensuite les lettres de l'alphabet auxquelles on a enlevé les I, O et Q soient 23 lettres (a,b,c,d,e,f,g,h,j,k,l,m,n,p,r,s,t,u,v,w,x,y,z) ; • la lettre choisie est celle de la position reste + 1 (exemple : position 3+1=4, soit la lettre D). Source : http://blog.juliendelmas.com/?qu-est-ce-que-le-code-rne-ou-uai
SAML *= Security assertion markup language*	SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.
SecurID	SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID
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.
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
Variante	Une variante est une extension personnalisée de la procédure de configuration proposée sur les modules EOLE. C'est un ensemble de patch et de fichiers modifiés permettant de configurer un groupe de serveurs.
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
XML-RPC *= XML Remote procedure call*	XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau. XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et avec n'importe quel langage de programmation. Le serveur est lui même sur n'importe quel système et est programmé dans n'importe quel langage. Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage. Source : http://fr.wikipedia.org/wiki/XML-RPC
ZéphirLog	ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.