Installation et mise en œuvre du module Zéphir

EOLE 2.6.2



création : Décembre 2016 Version : révision : Juin 2018 Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

EOLE 2.6.2

Version : révision : Juin 2018

Date : création : Décembre 2016

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Copyright : Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Licence : Cette documentation, rédigée par le Pôle national de compétences Logiciels Libres, est mise à disposition selon les termes de la licence :

Creative Commons Attribution - Partage dans les Mêmes Conditions 3.0 France (CC BY-SA 3.0 FR) : http://creativecommons.org/licenses/by-sa/3.0/fr/.

Vous êtes libres :

- de **reproduire, distribuer et communiquer** cette création au public ;
- de **modifier** cette création.

Selon les conditions suivantes :

- **Attribution** : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre) ;
- **Partage des Conditions Initiales à l'Identique** : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition. La meilleure manière de les indiquer est un lien vers cette page web.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits sur cette œuvre.

Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Cette documentation est basée sur une réalisation du Pôle national de compétences Logiciels Libres. Les documents d'origines sont disponibles sur le site.

EOLE est un projet libre (Licence GPL).

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

Pour toute information concernant ce projet vous pouvez nous joindre :

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

Table des matières

Chapitre 1 - Présentation et historique du projet EOLE 9
1. Les objectifs d'EOLE 9
2. Historique du projet EOLE 9
3. Versions des modules EOLE 13
4. Logiciel Libre 16
5. Méta-distribution EOLE 17
6. EOLE 2.6 18
7. Eolebase 20
8. Quelques références 22

Chapitre 2 - Introduction au module Zéphir 23
1. Qu'est ce que le module Zéphir ? 23
2. À qui s'adresse ce module ? 24
3. Les services Zéphir 25
4. Structure des conteneurs 25
5. Pré-requis 26
6. Les différences entre les versions 2.5 et 2.6 27
7. Errata 2.6.n 30

Chapitre 3 - Fonctionnement du module Zéphir 32
Chapitre 4 - Mise en œuvre du module 33
Chapitre 5 - Installation du module 35
1. Pré-requis 35
2. Médias d'installation 36
3. Déroulement de l'installation 40
4. Partitionnement personnalisé 42
5. Choisir le mode du module 58

Chapitre 6 - Configuration du module Zéphir 62
1. Configuration généralités 62
1.1. Configuration en mode autonome 63
1.1.1. Accès distant 65
1.1.2. La zone Menu 67
1.1.3. La zone Onglet 70
1.1.4. La zone Formulaire 71
1.1.5. La zone Validation 74
1.1.6. Enregistrer la configuration 74
1.1.7. Le mode Debug 75
1.1.8. FAQ 77
1.2. Configuration en mode Zéphir 79
2. Configuration en mode basique 88
2.1. Onglet Général 88
2.2. Onglet Interface-0 91
2.3. Onglet Messagerie 93
3. Configuration en mode normal 95
3.1. Onglet Général 96

3.2. Onglet Services 99
3.3. Onglet Interface-0 100
3.4. Onglet Annuaire 104
3.5. Onglet Onduleur 105
3.6. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 111
3.7. Onglet Nginx 115
3.8. Onglet Reverse proxy : Configuration du proxy inverse 116
3.9. Onglet Messagerie 120
3.10. Onglet Application zéphir 122
4. Configuration en mode expert 122
4.1. Onglet Général 124
4.2. Onglet Services 128
4.3. Onglet Système 129
4.4. Onglet Sshd : Gestion SSH avancée 137
4.5. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système 138
4.6. Onglet Logs : Gestion des logs centralisés 138
4.7. Onglet Interface-0 140
4.8. Onglet Interface-n 145
4.9. Onglet Réseau avancé 150
4.10. Onglet Certificats ssl : gestion des certificats SSL 155
4.11. Onglet Dépôt tiers 161
4.12. Onglet Annuaire 163
4.13. Onglet Onduleur 165
4.14. Onglet Saltstack 171
4.15. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 171
4.16. Onglet Ead-web : EAD et proxy inverse 178
4.17. Onglet Postgresql : Configuration du serveur PostgreSQL 179
4.18. Onglet Openldap : Configuration du serveur LDAP local 182
4.19. Onglet Nginx 183
4.20. Onglet Applications web nginx 185
4.21. Onglet Reverse proxy : Configuration du proxy inverse 185
4.22. Onglet Messagerie 189
4.23. Onglet Eoleflask 195
4.24. Onglet Application zéphir 196
5. Intégration d'un certificat et d'une chaîne d'authentification 197
6. Mise en place de l'agrégation de liens Ethernet (bonding) 200
Chapitre 7 - Instanciation du module 202
1. Principes de l'instanciation 202
2. Lancement de l'instanciation 203
2.1. Les mots de passe 203
2.2. Création d'un deuxième administrateur 204
2.3. Activation automatique de la mise à jour hebdomadaire 205
2.4. Le redémarrage 205
Chapitre 8 - Administration du module Zéphir 206
1. Présentation générale de l'application Zéphir 206
1.1. L'onglet serveurs 208
1.2. L'onglet établissements 209
1.3. L'onglet modules 210
1.4. L'onglet administration 210
1.5. Aide 211
2. Gestion des utilisateurs 211

2.1. Création d'un utilisateur 212
2.2. Affectation des droits et limitation des ressources 212
2.3. Préférences des utilisateurs 215
2.4. Gestion de la connexion aux serveurs 216
2.5. Suppression d'un utilisateur 217
2.6. Gestion en console des utilisateurs de l'annuaire LDAP local 218
3. Gestion des établissements 218
3.1. Ajout d'un d'établissement 219
3.2. Import d'établissements depuis un fichier 220
3.3. Recherche d'un ou de plusieurs établissements 222
3.4. Édition et suppression d'un établissement 223
3.5. Types d'établissement 223
4. Gestion des serveurs 224
4.1. Généralité sur la gestion des serveurs 224
4.1.1. Lister les serveurs 224
4.1.2. Ajouter un serveur 225
4.2. Enregistrement d'un serveur 227
4.3. L'état du serveur 234
4.4. Actions sur un serveur 237
4.4.1. Généralités sur les actions 237
4.4.2. Les actions Zéphir sur les serveurs 239
4.5. Personnalisation d'un serveur 245
4.5.1. Gestion des modifications personnelles 245
4.5.2. Modification unique sur un serveur 246
4.5.3. Gestion des permissions 246
4.5.4. Création et exécution de scripts personnalisés 248
4.6. Actions automatiques des agents de surveillance 250
4.7. Migration des serveurs enregistrés vers une nouvelle version de la distribution 253
4.7.1. Généralités sur la migration 253
4.7.2. Préparation de la migration depuis l'application Zéphir 255
4.7.3. Migration après réinstallation d'un serveur 262
4.7.4. Migration par mise à jour avec les procédure Upgrade-Auto / Maj-Release 263
4.8. Surveillance des serveurs enregistrés 264
4.8.1. État de la configuration 264
4.8.2. État des services / état système 266
4.8.3. État d'un groupe de serveurs 270
4.9. Gestion des alertes par courriers électroniques 270
4.10. Gestion par groupe de serveurs 274
4.10.1. Création des groupes 274
4.10.2. Gestion des groupes de serveurs 276
4.10.3. Actions supplémentaires 280
4.11. Les variantes 281
4.11.1. Créer une variante 281
4.11.2. Modifier une variante 284
4.11.3. Réutiliser une variante 288
4.12. Nouvelle gestion des dictionnaires Creole pour EOLE 2.4 et supérieur 290
4.13. Fonctions spécifiques à certains modules 296
4.13.1. Gestion des configurations RVP 296
4.13.2. Réplication LDAP entre un serveur Scribe/Horus et un serveur Seshat 297
4.13.3. Synchronisation depuis l'Annuaire Académique Fédérateur - AAF 298
4.14. Installation de paquets supplémentaires avec clés de signature 302

4.15. Désinscription d'un serveur 303
5. Changement de l'adresse IP du serveur Zéphir 303
6. Sauvegarde / Restauration 305
7. Migration vers le module Zéphir 2.6 308
8. Divers petits outils 310
8.1. Génération de fichiers de configuration pour clé USB 310
8.2. Mise à jour automatique du paquet zephir-client 312
Chapitre 9 - Personnalisation du module 313
1. Panorama des services 313
1.1. Services liés aux bases de données 313
1.1.1. eole-annuaire 313
1.1.2. eole-client-annuaire 314
1.1.3. eole-db 314
1.1.4. eole-interbase 315
1.1.5. eole-mysql 315
1.1.6. eole-postgresql 315
1.2. Services liés aux serveurs de fichiers 316
1.2.1. eole-ad-dc 316
1.2.2. eole-fichier-primaire 316
1.2.3. eole-fichier-membre 317
1.2.4. eole-cups 318
1.2.5. eole-proftpd 318
1.2.6. eole-dhcp 319
1.2.7. eole-nfs 319
1.3. Services liés au web 320
1.3.1. eole-web 320
1.3.2. eole-reverseproxy 321
1.3.3. eole-wpad 321
1.4. Services liés à la messagerie 322
1.4.1. eole-exim 322
1.4.2. eole-spamassassin 322
1.4.3. eole-courier 323
1.4.4. eole-sympa 323
1.5. Services liés au proxy et à l'authentification 324
1.5.1. eole-proxy 324
1.5.2. eole-radius 325
1.6. Services liés à la virtualisation 325
1.6.1. eole-libvirt 325
1.6.2. eole-one-frontend 326
1.6.3. eole-one-node 326
1.6.4. eole-one-singlenode 327
1.7. Autres services réseau 327
1.7.1. eole-antivirus 327
1.7.2. eole-apt-cacher-ng 328
1.7.3. eole-bareos 328
1.7.4. eole-dns 329
1.7.5. eole-dhcrelay 330
1.7.6. eole-ltsp-server 330
1.7.7. eole-nut 330
1.7.8. eole-open-iscsi 331
1.7.9. eole-pacemaker 331

1.7.10. eole-snmpd 332
1.7.11. eole-vpn 332
2. Personnalisation du serveur à l'aide de Creole 333
2.1. Répertoires utilisés par EOLE 333
2.2. Création de patch Creole 334
2.3. Les dictionnaires Creole 336
2.3.1. Ajouter un en-tête XML 336
2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu 337
2.3.3. Utiliser des familles, variables et des séparateurs 345
2.3.4. Comportement des variables 350
2.3.5. Mettre en place des contraintes 350
2.3.6. Afficher de l'aide 358
2.4. Le langage de template Creole 359
2.4.1. Déclarations du langage Creole 360
2.4.2. Fonctions prédéfinies 364
2.4.3. Utilisation avancée 368
2.4.4. Exemple 369
2.5. Le fichier de configuration Creole 370
2.6. Les scripts Creole 371
2.6.1. CreoleLint et CreoleCat 371
2.6.2. CreoleGet et CreoleSet 373
2.6.3. CreoleRun et CreoleService 376
2.6.4. CreoleLock 377
2.6.5. Indications pour la programmation 378
2.7. Ajout de script exécuté à l'instance ou au reconfigure 381
2.8. Ajout d'un test diagnose 382
2.9. Gestion des noyaux Linux 383
2.10. Gestion des tâches planifiées eole-schedule 384
2.11. Gestion du pare-feu eole-firewall 389
Chapitre 10 - Résolution de problèmes 391
1. Problèmes à la mise en œuvre 391
2. Problèmes à l'exploitation 392
3. Trouver de l'information 397
4. Demander de l'aide / Signaler un problème 400
5. Contribuer au projet EOLE 405
Chapitre 11 - Documentations techniques 407
1. Les dépôts EOLE 407
2. Gestion des journaux systèmes sur EOLE 409
3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation 410
3.1. Contexte juridique 410
3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation 411
Chapitre 12 - Compléments techniques 415
1. Les services utilisés sur le module Zéphir 415
1.1. eole-annuaire 415
1.2. eole-client-annuaire 415
1.3. eole-exim 416
1.4. eole-nut 417
1.5. eole-postgresql 417
1.6. eole-reverseproxy 418

2. Ports utilisés sur le module Zéphir 418
3. Ports à ouvrir sur le Pare-feu 419
4. Arborescence de la configuration des serveurs sur Zéphir 420
5. Méthodologie du serveur de commande 421
6. Présentation de l'API 421
7. Le client Zéphir 425
8. Annuaire : diagnostic et résolution de problème 426

Chapitre 13 - Questions fréquentes 428
1. Questions fréquentes communes aux modules 428
2. Questions fréquentes propres au module Zéphir 448

Glossaire 453

Chapitre 1
Présentation et historique du projet EOLE

EOLE est l'acronyme de Ensemble Ouvert Libre et Évolutif. C'est un projet collaboratif basé sur la philosophie du logiciel libre, la mutualisation des compétences et des moyens permet de réaliser des solutions économiques, fiables et performantes.



Le projet EOLE offre des solutions clé en main pour la mise en place de serveurs dans les établissements scolaires et académiques.

1. Les objectifs d'EOLE

Les objectifs du projet EOLE sont les suivants :

- offrir des solutions libres ;
- réaliser des produits modulaires, évolutifs et ouverts ;
- faciliter les mises en œuvre et les déploiements ;
- offrir un service d'administration à distance ;
- offrir des services mutualisés (Réseau Global Établissement) ;
- aider au respect des contraintes légales (droit d'auteur, brevet d'invention, droit des personnes et des enfants).

2. Historique du projet EOLE

Les dates significatives du projet

2000

- projet local à l'académie de Dijon pour répondre à un besoin identifié concernant la protection des élèves et des données administratives ;
- établissements pilotes : Cité scolaire Montchapet, Lycée Le Castel et Lycée Simone Weil ;
- distribution GNU/Linux utilisée : Mandrake 7.

2001

- projet national à la demande du ministère de l'Éducation nationale ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- naissance du premier module EOLE 1.0 à partir de la distribution Mandrake 8 : **Amon**, serveur pare-feu.

2002

- études de contenu nationales & développement par le CETIAD[p.455] :
- généralisation du module Amon 1.0 dans les collèges et les lycées de plusieurs académies : Clermont-Ferrand, Montpellier, Besançon… ;
- nouveau module 1.0 : **Sphynx**, concentrateur de réseaux privés virtuels et **Horus**, serveur de fichiers administratif

2003

- l'équipe EOLE devient pôle national de compétence EOLE ;
- module Amon 1.5.

2004

- module Sphynx 1.1 ;
- nouveau module 1.0 : **Scribe**, serveur de fichiers pédagogique ;
- écriture d'un éditeur de règles pour le module Amon nommé **ERA**.

2005

- VPN : abandon de Freeswan et ajout du mode multi-tunnels ;
- le module Amon 1.5 est déployé dans les écoles primaires ;
- nouveau module : **Zéphir**, pour l'administration des serveurs à distance ;
- filtrage Web dynamique : passage de Squidguard à DansGuardian.

2006

- outil de diagnostique réseau : ODR ;
- mise en place d'un serveur de sauvegardes Bacula ;
- début de la réécriture : EOLE NG.

2007

- intégration de @SSR (sécurité routière) sur le module Scribe ;
- EOLE NG 2.0 (en octobre), utilisation de la distribution Ubuntu 7.04 (Feisty Fawn) ;
- démonstrateur d'un module utilisant la technologie Xen[p.477].

2008

- EOLE NG 2.1 (mai), utilisation de la distribution Ubuntu 7.10 (Gutsy Gibbon) ;
- nouveau module 2.1 : **Eclair**, serveur de clients légers Linux.

2009

- EOLE NG 2.2 LTS (janvier), utilisation de la distribution Ubuntu 8.04 LTS (Hardy Heron) ;
- nouveaux modules :
  - **AmonEcole**, Scribe et Amon sont virtualisés avec la technologie OpenVZ[p.468] ;
  - **Seshat** le relais de messagerie pour le domaine intra-académique ;
- la console de visualisation de l'IDS Prélude (fonctionnant avec ZéphirLog) ;
- nouveau module 2.2 eSSL par le MEDDE[p.466] ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- intégration d'Envole[p.459] 2.0 sur le module Scribe.

2011

- EOLE NG 2.3 LTS (juin), utilisation de la distribution Ubuntu 10.04 LTS (Lucid Lynx) ;
- introduction du mode conteneur utilisant la technologie LXC[p.465] pour remplacer OpenVZ ;
- nouveaux modules 2.3 : eSBL et eCDL par le Ministère de l'Écologie, du Développement durable et de l'énergie (MEDDE)[p.466].

2012

- portage d'Eclair en 2.3 (juillet), repose sur ltsp-cluster, le serveur embarque le logiciel Gaspacho[p.460] ;
- nouveau module 2.3 : **AmonEcole+**, AmonEcole + Eclair.

2013

- le pôle de compétences EOLE devient pôle de compétences logiciel libre ;
- L'interface de configuration du module est basée sur de nouvelles technologies : Flask, Backbone.js, Marionette et Tiramisu ;
- les solutions EOLE sont inscrites au Socle Interministériel de Logiciel Libre (SILL)[p.473] 2013 ;
- EOLE 2.4 LTS alpha1 (septembre) ;
- EOLE 2.4 LTS alpha2 (octobre) ;
- nouveau module 2.4 : **Thot**, annuaire centralisé.

2014

- les solutions EOLE sont inscrites au Socle Interministériel de Logiciel Libre (SILL)[p.473] 2014 ;
- EOLE 2.4 LTS RC (février) ;
- EOLE 2.4 LTS (mai) : portage des modules Amon, Scribe, Horus et Sphynx.

2015

- EOLE 2.4.1 LTS (février), utilisation de la distribution Ubuntu 12.04 LTS (Precise Pangolin)
  - portage d'AmonEcole ;
  - nouveaux modules 2.4 : **Hâpy**, **Hâpy Node**, **Hâpy Market** et **Hâpy Master** sont des solutions de virtualisation basées sur OpenNebula[p.468].
- EOLE 2.4.1.1 LTS (mai)
- EOLE 2.5 LTS (juillet), utilisation de la distribution Ubuntu 14.04 LTS (Trusty Tahr) ;
  - portage du module Seshat ;
  - portage du module Zéphir ;
  - nouvelle charte graphique.
- EOLE 2.4.2 LTS (juillet)
  - nouvelle version d'Envole : version 4.
- EOLE 2.5.1 LTS (novembre)
  - portage du module Scribe ;
  - portage du module Amon ;
  - portage du module Horus ;
  - portage du module AmonEcole ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- portage du module eCDL ;
- portage du module eSBL ;
- portage d'Envole 4 sur EOLE 2.5.1 par la mutualisation Envole.

2016

- EOLE 2.5.2 LTS (avril)
  - portage du module Sphynx ;
  - publication d'Envole 5 sur EOLE 2.5.2 par la mutualisation Envole.
- EOLE 2.6 LTS (décembre), utilisation de la distribution Ubuntu 16.04 LTS (Xenial Xerus)
  - portage du module Scribe ;
  - portage du module Horus ;
  - portage des modules Hâpy : **Hâpy** et **Hâpy Node** ;
  - portage du module Sphynx ;
  - portage du module Eclair ;
  - portage du module eSBL ;
  - portage du module Zéphir ;
  - nouveau module 2.6 : **Seth** est une solution de contrôleur de domaine de type Active Directory élaborée conjointement par le Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche (MENSR) et le Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM[p.466]).

  Cette version d'EOLE marque l'arrêt du support pour l'architecture i386.

2017

- EOLE 2.6.1 LTS (mai)
  - portage des modules : Amon, AmonEcole, Seshat, Thot et eCDL ;
  - publication d'Envole 6 sur EOLE 2.6.1 par la mutualisation Envole.
- EOLE 2.6.2 LTS (décembre)
  - portage du module AmonEcoleEclair.

2018

- EOLE 2.7 LTS (décembre), utilisation de la distribution Ubuntu 18.04 LTS (Bionic Beaver)
  - portage du module Amon ;
  - portage du module Seth ;
  - portage du module eSBL ;
  - portage du module Sphynx ;
  - portage du module Seshat ;
  - portage du module Thot ;
  - portage du module Zéphir ;
  - portage des module Hâpy : Hâpy et Hâpy Node ;
  - abandon du module eCDL au profit du module Seth.

2019

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- EOLE 2.7.1 LTS (juin)
  - portage du module Eclair ;
  - portage des modules Scribe et Horus en Scribe AD et Horus AD, le mode NT est définitivement abandonné ;
  - abandon du module eSBL au profit du module Seth en mode membre.

2020

- EOLE 2.7.2 LTS (juillet)
- EOLE 2.8.0 LTS (décembre)
  - migration du code de la distribution de python2 vers python3 ;
  - possibilité d'utiliser LemonLDAP::NG[p.463] en tant qu'alternative à EoleSSO.

2021

- EOLE 2.8.1 LTS (juillet)
  - nouvelle version du module AmonEcole (non disponible sur EOLE 2.7) ;
  - possibilité de filtrer les flux HTTPS à l'aide d'une configuration type Man in the middle[p.465] (SSL interception) ;
  - mise à disposition des paquets `eole-fog` et `eole-lts-server` permettant respectivement la mise en œuvre de FOG[p.460] et d'un seveur LTSP[p.470] sur un module EOLE.

2023

- EOLE 2.9.0 LTS (février)
  - intégration du moteur de conteneur[p.456] Podman[p.469] avec une première implémentation pour le service EoleSSO et une seconde pour l'IHM ERA.

2025

- EOLE 2.10.0 LTS (mars)

3. Versions des modules EOLE

Versions supportées des modules EOLE

Version	**2.7.0**	**2.7.1**	**2.7.2**	**2.8.0**	**2.8.1**	**2.9.0**	**2.10.0**
Date de sortie	2018	2019	2020	2020	2021	2022	2025
Fin du support	Juin 2023	Juin 2023	Juin 2023	Juin 2025	Juin 2025	Juin 2027	Juin 2029
eCDL							
eSBL							
Amon							

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Eclair							
Hâpy							
Hâpy Node							
Horus (NT)							
Horus (AD)							
Scribe (NT)							
Scribe (AD)							
Seshat							
Seth							
Sphynx							
Thot							
AmonEcole							
AmonEcoleEclair							
Zéphir							
Envole							

Tableau des modules par versions d'EOLE

Versions non supportées des modules EOLE

Version	**2.0**	**2.1**	**2.2**	**2.3**	**2.4.0**	**2.4.1**	**2.4.2**	**2.5.0**	**2.5.1**	**2.5.2**	**2.6.0**	**2.**
Date de sortie	2007	2008	2009	2011	2014	2015	2015	2015	2015	2016	2016	20

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

eCDL				✓		✓	✓		✓	✓		
eSBL				✓		✓			✓	✓	✓	
Amon	✓	✓	✓	✓	✓	✓	✓		✓	✓		
Eclair		✓	✓	✓							✓	
Hâpy						✓	✓				✓	
Hâpy Node						✓	✓				✓	
Hâpy Market						✓	✓					
Hâpy Master						✓	✓					
Horus (NT)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Horus (AD)												
Scribe (NT)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Scribe (AD)												
Seshat			✓	✓				✓	✓	✓		
Seth											✓	
Sentinelle			✓									
Sphynx	✓	✓	✓	✓	✓	✓	✓			✓	✓	
Thot					✓	✓	✓		✓	✓		
AmonEcole			✓	✓		✓	✓		✓	✓		

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

AmonEcole+ AmonEcoleEclair												
AmonHorus												
Zéphir												
ZéphirLog												
Envole												

Tableau des modules par versions d'EOLE

4. Logiciel Libre

L'expression *logiciel libre* veut dire que le logiciel respecte la liberté de l'utilisateur et de la communauté.

Le logiciel libre garantit quatre niveaux de libertés :

- utilisation : la liberté d'utiliser/exécuter le logiciel pour quelque usage que ce soit ;
- étude : la liberté d'étudier le fonctionnement du programme, et de l'adapter à vos besoins ;
- redistribution : la liberté de redistribuer des copies ;
- modification : la liberté d'améliorer le programme, et de rendre publiques vos améliorations de telle sorte que la communauté tout entière en bénéficie.

La notion de logiciel libre ne doit pas être confondue avec celle de logiciel gratuit : graticiels (freewares), partagiciel (sharewares). Ce type de licence ne donne pas autant de latitude en ce qui concerne la distribution et la modification du logiciel.

De même il ne faut pas confondre logiciel libre avec ce qu'on appelle souvent logiciel Open Source ou « à sources ouvertes ». Les libertés définies par un logiciel libre sont bien plus étendues que le simple accès au code-source. Toutefois, la notion formelle de logiciel Open Source telle qu'elle est définie par l'Open Source Initiative est reconnue comme techniquement comparable au logiciel libre.

Le domaine public quand à lui désigne l'ensemble des œuvres de l'esprit et des connaissances dont l'usage n'est pas ou n'est plus restreint par la loi.

Licences

Il existe plusieurs licences qui font d'un logiciel un logiciel libre.

EOLE distribue et modifie des logiciels libres qui sont sous plusieurs de ces licences.

Pour ses développements internes, EOLE a choisi la licence libre CeCILL[p.464].

Contributions au libre

Contribuer au libre peut prendre plusieurs formes : promotion, amélioration, documentation, traduction,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

remontée de dysfonctionnement...

Le pôle de compétences Logiciels libres utilise et intègre de nombreux logiciels libres ce qui offre l'opportunité de contribuer à différents projets libres :

- Ubuntu Launchpad : https://bugs.launchpad.net/~eole-team ;
- AskUbuntu : https://askubuntu.com/users/389629/eole-team ;
- OpenNebula : https://dev.opennebula.org/users/1416.html ;
- GitHub : https://github.com/eole ;
- The Samba-Bugzilla : https://bugzilla.samba.org ;
- Wikipédia : https://fr.wikipedia.org/wiki/Spécial:Contributions/EOLE-team [https://fr.wikipedia.org/wiki/Sp%C3%A9cial:Contributions/EOLE-team] ;
- OpenStreetMap : https://www.openstreetmap.org/user/EOLE-Team.

Ces contributions prennent essentiellement la forme de traductions et de remontées de dysfonctionnements avec parfois la soumission de correctifs et de solutions.

Une page wiki sur la forge recense les contributions récentes d'EOLE à différentes communautés du logiciel libre :

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

5. Méta-distribution EOLE

Issu du projet éponyme, la méta-distribution EOLE est l'**association** d'une **distribution** GNU/Linux (Ubuntu, en l'occurrence) et des **outils** spécifiques d'**intégration** et d'**administration** issus du projet EOLE.

La méta-distribution EOLE regroupe l'ensemble des modules développés. Chaque module donne naissance à une distribution GNU/Linux à part entière.

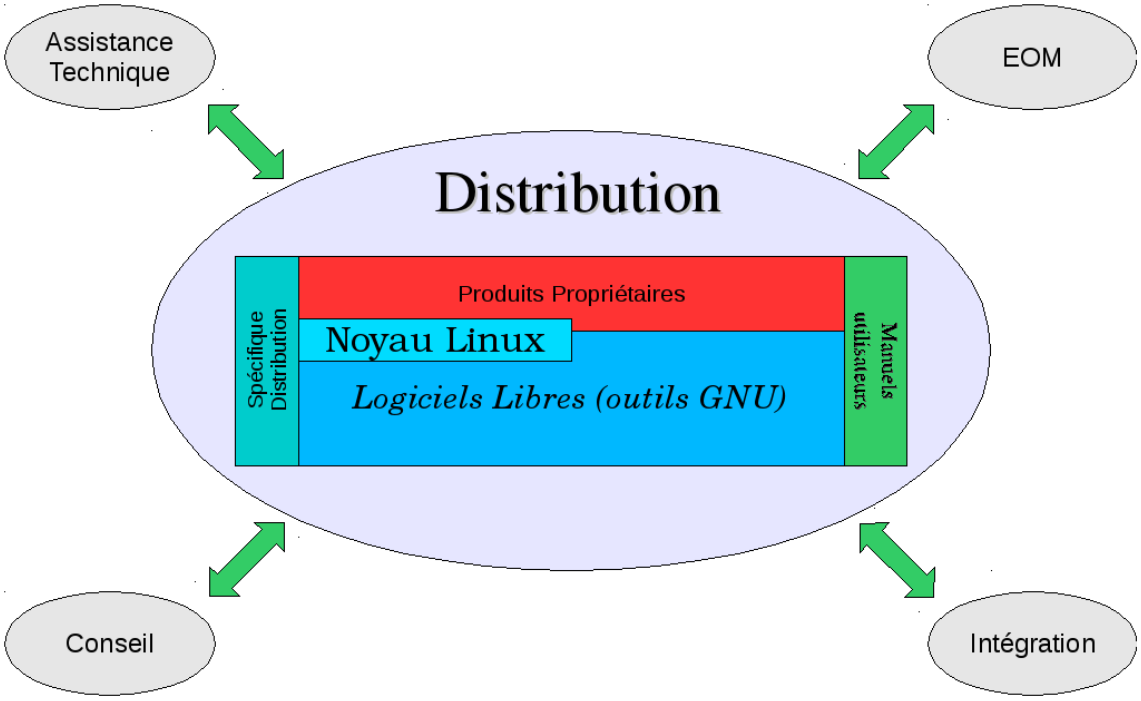
Une distribution GNU/Linux

Une distribution[p.457] GNU/Linux[p.464] est un ensemble cohérent de logiciels groupés autour d'un noyau (ou kernel) Linux.

Elle comporte :

- un installateur (procédure d'installation, interactive ou automatique) ;
- au moins un noyau ;
- des logiciels libres ;
- une imposante bibliothèque de logiciels libres prêts à être installés ;
- une procédure simple pour la mise à jour des logiciels.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Les modules EOLE

Chaque module est un ensemble de services répondant à un objectif de travail dans les établissements, sous la forme d'une sélection logicielles, associée aux procédures de déploiement (installation), configuration, préparation (instanciation) et exploitation (administration et utilisation) définies spécifiquement pour chacun de ces modules.

L'installation se déroule sans la moindre intervention de l'utilisateur. Il existe néanmoins un mode offrant une plus grande latitude dans la mise en œuvre du serveur (en particulier, la gestion du RAID et/ou du partitionnement).

Les modules EOLE disposent d'une maintenance (mises à jour de sécurité et fonctionnelles) simplifiée.

6. EOLE 2.6



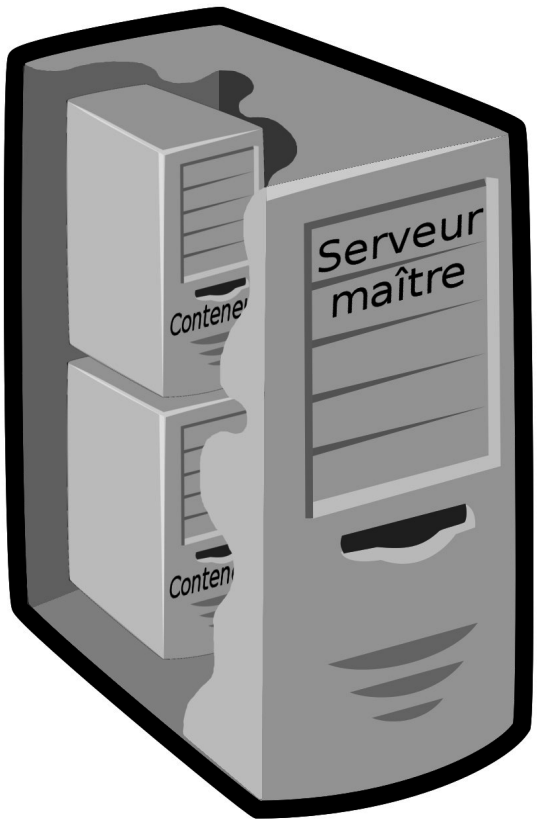
Logo officiel d'Ubuntu par Canonical Ltd

Les modules de la version EOLE 2.6 s'appuient sur la distribution GNU/Linux Ubuntu 16.04 LTS nommée également Xenial Xerus.

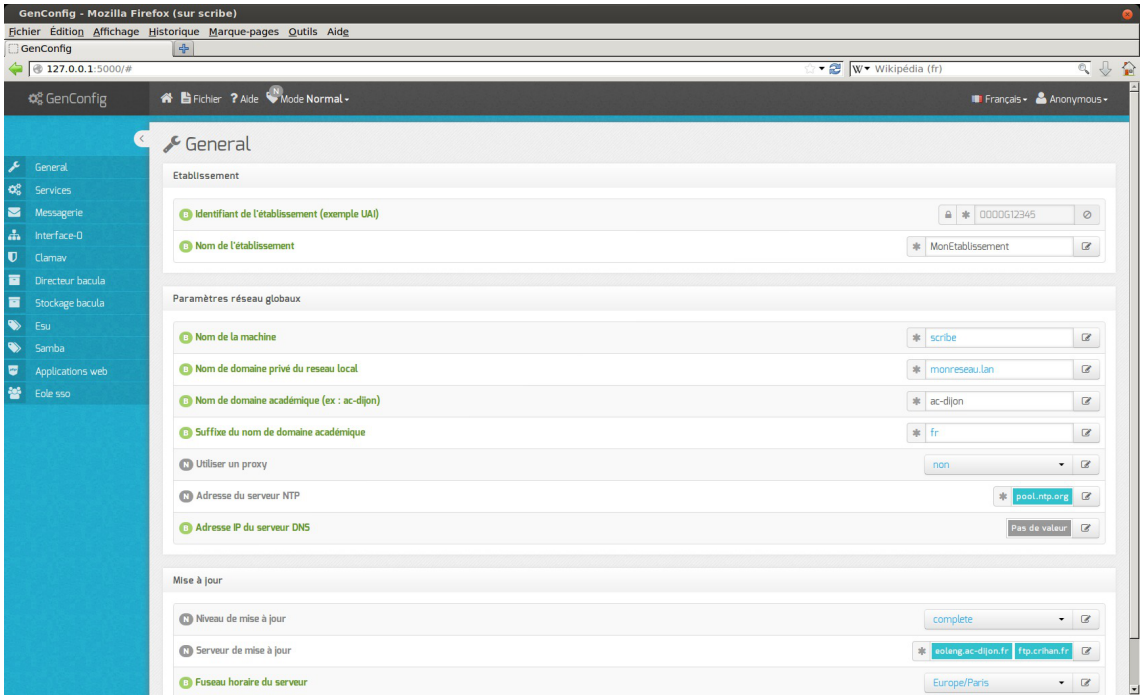
Ubuntu 16.04 LTS est disponible depuis le 21 avril 2016. Portant le label LTS[p.464], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2021. Le Pôle de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2021.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Module



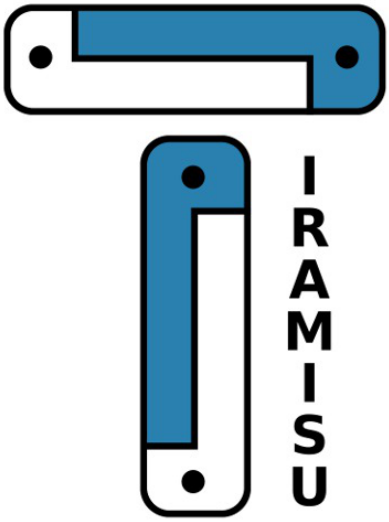
La version 2.6 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule instance du noyau présente sur le maître utilisée par l'ensemble des conteneurs. Cela permet, entre autre, une économie des ressources de la machine physique.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Écran d'accueil de l'interface de configuration du module

L'interface de configuration du module utilise la bibliothèque de gestion de configuration nommée Tiramisu[p.475].



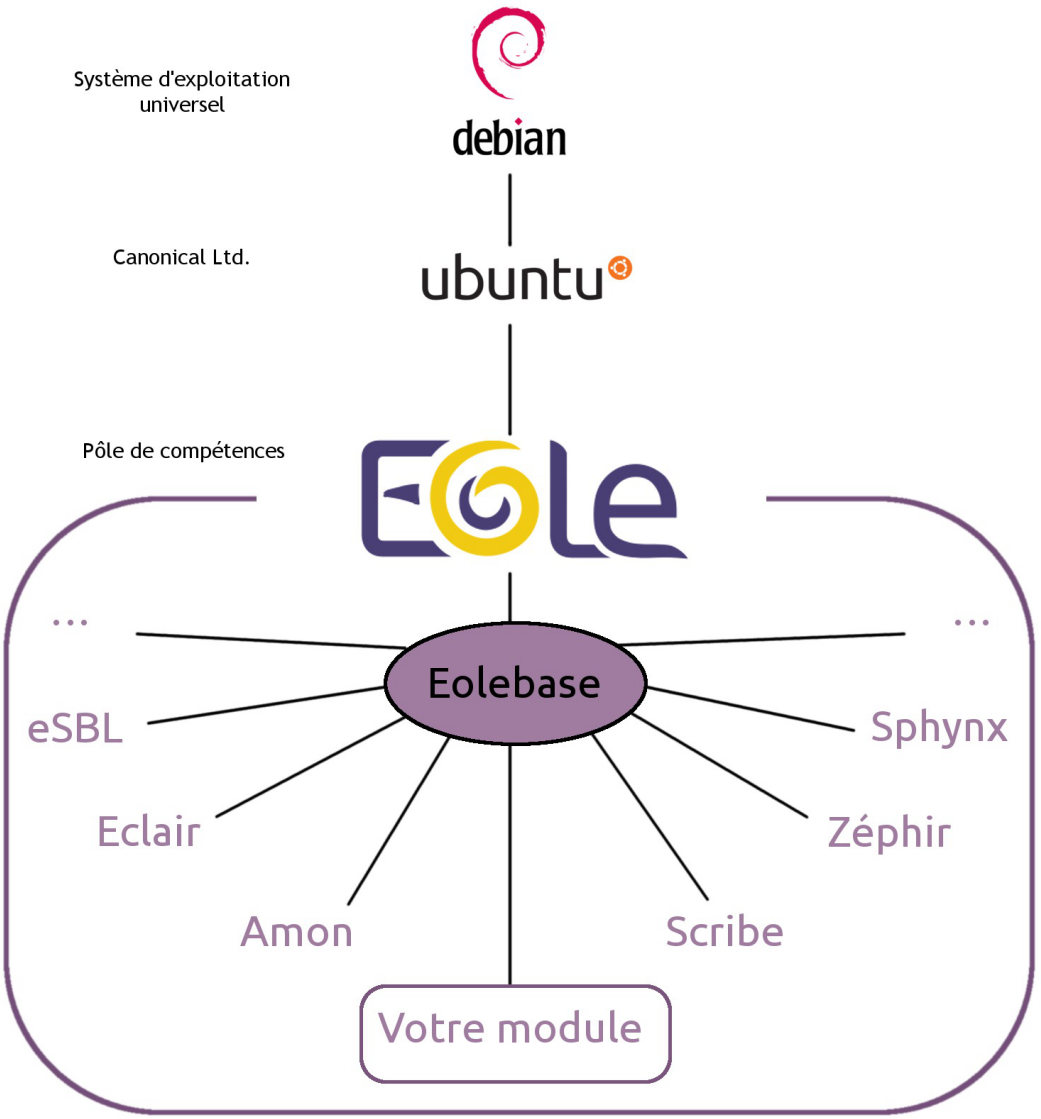
Logo du logiciel Tiramisu

7. Eolebase

Comme son nom l'indique, Eolebase est à la base des différents modules EOLE.

Tout en s'appuyant sur la stabilité et les mises à jour de sécurité de la distribution Ubuntu LTS, Eolebase contient les mécanismes techniques qui permettent de réaliser un module EOLE.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Eolebase met à disposition les technologies EOLE pour la création d'un nouveau module personnalisé :

- l'**Installeur** met à disposition une interface simple pour l'installation d'Eolebase ;
- **Creole** est un ensemble d'outils permettant de mettre en œuvre un serveur suivant une configuration définie ;
- l'**Interface de configuration du module** permettra de paramétrer le serveur; les services se configureront avec cette unique interface.

Creole est le cœur de la technologie EOLE.

C'est un ensemble d'outils qui permettent de modifier et/ou d'étendre les fonctionnalités offertes par un module EOLE sans risquer de créer une incohérence avec la configuration par défaut et les futures mises à jour.

Il gère entre autres :

- la personnalisation des options de configuration des modules ;
- le redémarrage des services ;
- l'installation de paquets additionnels ;
- la mise à jour du système.

Pour personnaliser un module, les outils suivants sont a disposition :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le **patch** : permettant de modifier les modèles (templates) fournit par EOLE ;
- le **dictionnaire** : permet d'ajouter des options à l'interface de configuration, d'installer de nouveaux paquets ou de gérer de nouveaux services ;
- le **template** : modèle de fichier de configuration qui suivant des choix de configuration sera complété et appliqué au module.

C'est cette technologie qui permet également de construire, à partir d'Eolebase, un nouveau module entièrement personnalisé.

8. Quelques références

- Les sites EOLE :
  - Site web Officiel : https://pcll.ac-dijon.fr/eole/
  - Listes de diffusion : https://pcll.ac-dijon.fr/listes
  - La forge : http://dev-eole.ac-dijon.fr/
- Logiciel Libre :
  - http://www.gnu.org/philosophy/free-sw.fr.html
- Licence GPL :
  - Gnu.org : http://www.gnu.org/licenses/licenses.fr.html#GPL
  - Wikipédia : http://fr.wikipedia.org/wiki/Licence_publique_générale_GNU [http://fr.wikipedia.org/wiki/Licence_publique_g%C3%A9n%C3%A9rale_GNU]
- Licence CeCILL :
  - CeCILL.info : https://cecill.info
  - Wikipédia : http://fr.wikipedia.org/wiki/Licence_CeCILL

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 2

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.

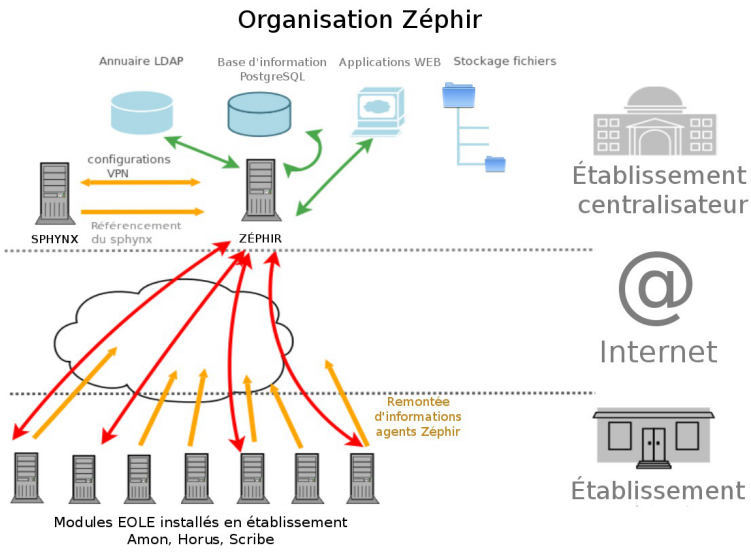
Le module permet la gestion des différentes configurations serveur.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 5.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 ;
- *Nginx* : proxy inverse et serveur web.

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.456].

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.473].

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

6. Les différences entre les versions 2.5 et 2.6

Cette version reprend donc les changements de la version 2.5 à savoir :

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

Il est à noter que cette nouvelle version du module Zéphir comporte tout de même des changements par rapport à la version 2.5 :

- suppression de la gestion des modules EOLE inférieurs à 2.4 ;
- passage à PostgreSQL 9.5.

La nouvelle version du module reproduit les mêmes fonctionnalités (iso-fonctionnel) que l'ancienne version.

La version 2.6 s'appuie sur la distribution GNU/Linux Ubuntu 16.04 LTS nommée également Xenial Xerus.

Ubuntu 16.04 LTS est disponible depuis le 21 avril 2016. Portant le label LTS[p.464], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2021.

Noyau

Cette nouvelle version d'Ubuntu implique également un changement de version du noyau avec de nouvelles prises en charge matériel. Les modules EOLE 2.6 utilisent par défaut le noyau le plus récent de la distribution Ubuntu.

Gestion des services

systemd[p.474] est, dorénavant, la seule méthode valide pour la gestion des services. upstart[p.476] est encore accepté pour assurer la rétrocompatibilité. Cependant, le service est, dans tous les cas, géré par systemd.

Interfaces réseau

Sur la nouvelle version d'EOLE les cartes réseau respectent la convention Consistent Network Device Naming[p.455] de udev[p.475] pour le nommage des cartes réseau. Le nom des cartes est fixé en fonction de leur ordre d'attachement au système et non plus uniquement dans l'ordre matériel.

Sous EOLE, le nommage des interfaces réseau change, elles se nomment désormais `em1`, `em2`,..., `emx`.

Architecture AMD64 uniquement

L'architecture i386 n'est plus supportée par le projet EOLE à partir de cette version.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Installation UEFI

Les nouvelles images ISO générées par EOLE intègrent le support de l'UEFI[p.475].

Le support de l'UEFI est également disponible sur les nouvelles images générées pour les versions d'EOLE précédentes (images 2.4.2.1, 2.5.2.1, ...).

Gestion des certificats du serveur Zéphir

Dans le cas d'utilisation de certificats non reconnus par une autorité de certification, il faut, pour procéder à l'enregistrement d'un serveur, copier et intégrer le certificat de la CA locale du serveur Zéphir sur le serveur à enregistrer.

Creole

Des modifications ont été réalisées dans Creole :

- du fait du passage à systemd, certains attributs de la balise `<service>` ont été supprimés : `pty`, `startlevel` et `stoplevel` ;
- ajout d'un nouveau type `password` permettant de présenter les valeurs avec un affichage brouillé ;
- ajout des nouvelles contraintes entre variables : `mandatory if in` et `mandatory if not in`.

Restauration des sauvegardes

La restauration du catalogue s'effectue désormais après instanciation du serveur.

L'option `--configeol` du script bareosrestore.py permet d'extraire le fichier config.eol.

Choix du type de partitionnement à l'installation

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

Suppression de la gestion des modules EOLE inférieurs à 2.4

Dans cette version, Zéphir ne prend en charge que les modules EOLE dans les versions 2.4, 2.5 et 2.6.



Les serveurs EOLE en version égale ou inférieure à 2.3 ne sont plus gérés.

En cas d'import d'une sauvegarde provenant d'une ancienne version de Zéphir, les serveurs 2.3 sont purgés par les commandes reconfigure et instance.

Passage à PostgreSQL 9.5

Cette nouvelle version de Zéphir s'appuie sur la version 9.5 de PostgreSQL.

2.6.1

Partitionnement

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.

À partir de la version 2.6.1 d'EOLE il est possible d'ajouter des partitions supplémentaires et d'attribuer l'espace libre à une partition au travers de l'interface de configuration du module pour ajuster le partitionnement avant l'instance.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Mise à jour

Les modifications apportées au proxy transparent provoquent le blocage de certaines mises à jour. La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon.

Ajout de dépôt supplémentaires

L'ajout de dépôt supplémentaires tels que les PPA est dorénavant géré nativement.

EAD 3

Une nouvelle version de l'EAD est disponible sur les modules et peut être activée. Pour le moment il ne remplace pas l'EAD existant, son activation permet de le découvrir, de l'utiliser ou de travailler à son développement.

Proxy inverse

Le paramétrage du proxy inverse est disponible sur tous les modules, il permet de relayer des accès extérieurs vers des serveurs situés derrière le pare-feu.

Le proxy inverse permet dorénavant la redirection de domaines.

Publication d'applications web par Nginx

L'accès à des applications web telles que l'EAD3 et l'interface de configuration du module se fait au travers de Nginx. Si un client accède au serveur avec un nom de domaine non déclaré, le flux est redirigé vers le domaine renseigné.

Désactivation de variables Creole entre esclaves du même groupe

À partir de la version 2.6.1 d'EOLE, il est possible de gérer la désactivation d'une variable esclave en fonction de la valeur d'une autre variable esclave du même groupe.

Dans les versions précédentes, il était possible de désactiver totalement une variable esclave mais pas de le faire pour une seule de ses valeurs.

Agrégation de liens Ethernet

Il est possible d'agréger plusieurs interfaces réseau physiques pour les utiliser comme s'il s'agissait d'une seule. Le but est d'accroître le débit au-delà des limites d'un seul lien, et éventuellement de mettre en œuvre de la redondance[p.471] de liens Ethernet.

Gestion des certificats Let's Encrypt

L'autorité de certification Let's Encrypt[p.463] permet de mettre en place, gratuitement, des certificats dont la distribution et le renouvellement sont automatisés.

Vous pouvez à présent gérer des certificats Let's Encrypt pour des serveurs accessibles depuis Internet ou au travers d'un proxy inverse.

2.6.2

Accès au backend EAD

À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD[p.458] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Par défaut, l'accès au backend est bloqué pour chaque interface.

Proxy inverse

Le proxy inverse permet dorénavant la redirection des sous-domaines.

Partitionnement et utilisation de l'espace libre

Le partitionnement à l'installation est toujours le modèle EOLE, mais il est modifiable avant l'instance par l'intermédiaire de l'interface de configuration du module.

L'administrateur a donc le choix entre :

- le modèle de répartition de l'espace disque EOLE : un pourcentage pour chaque volume en fonction des fonctionnalités propres au module et l'espace libre est attribué à l'un des volumes (exemple : `/home` sur Scribe et Horus) ;
- un partitionnement entièrement personnalisé : il est possible de créer des volumes et d'indiquer pour chaque volume quel pourcentage de l'espace libre il va utiliser en plus.

Certificat SSL

À partir de cette version, le choix du certificat SSL (autosigné, manuel ou Let's Encrypt) est disponible en mode basique. La commande diagnose affiche tous les noms DNS renseignés dans le certificat du serveur[p.473].

Serveurs de secours NTP

Il est désormais possible de désactiver l'utilisation d'un pool de serveurs de secours pour la synchronisation de l'horloge.

Cela s'effectue par le biais d'une variable disponible dans le nouvel onglet du mode expert : `Ntp`.

7. Errata 2.6.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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Une page d'errata recense des problèmes affectant chacune des versions EOLE 2.6.x. Les dysfonctionnement connus sont corrigés d'une version à une autre d'EOLE.

http://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Errata26

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 3
Fonctionnement du module Zéphir

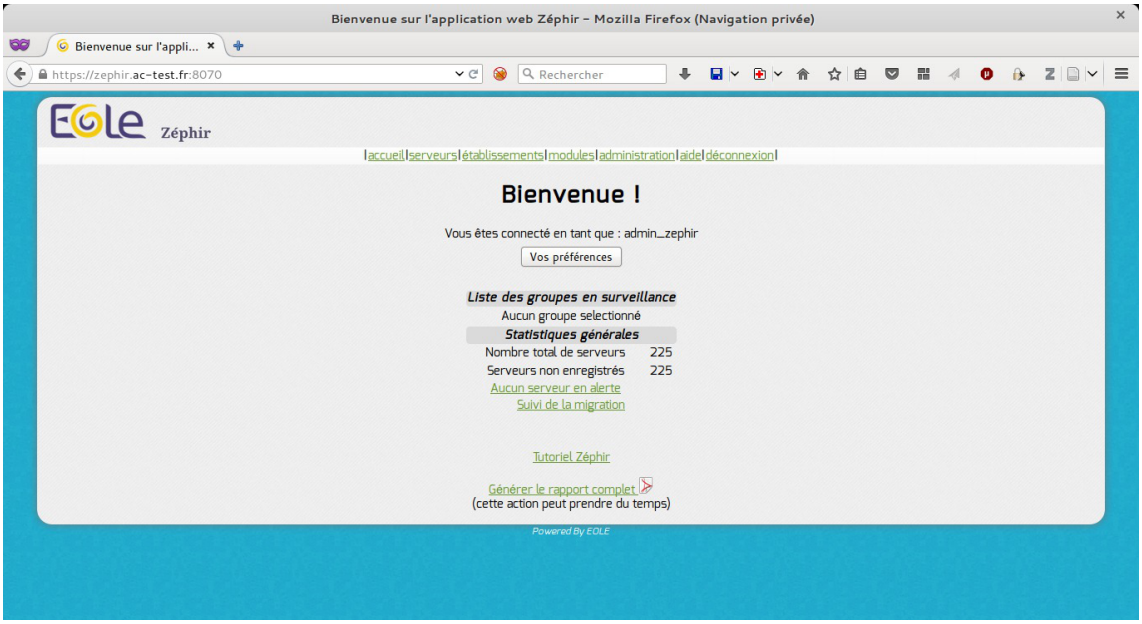
Pour jouer son rôle, le module Zéphir repose sur plusieurs projets libres : PostgreSQL, Twisted Matrix, OpenLDAP, ...

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.

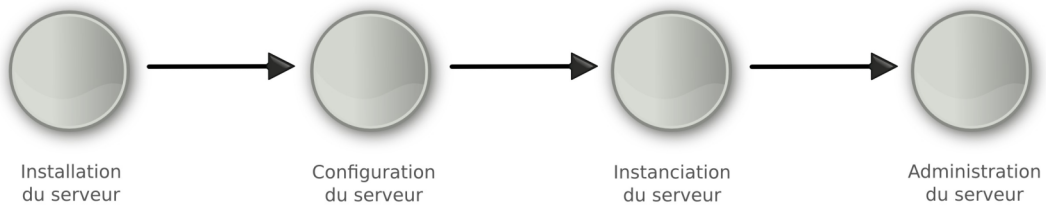
L'interface web Zéphir permet de gérer les serveurs surveillés.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 4

Mise en œuvre du module



Fil rouge de la mise en œuvre

La mise en œuvre d'un module EOLE s'effectue en quatre phases distinctes :

- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.462] 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.

- 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 première interface réseau 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.473], e2guardian[p.458], etc.

- 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` .

- La **phase d'administration** correspond à l'exploitation du serveur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chaque module possède des fonctionnalités propres, souvent complémentaires.

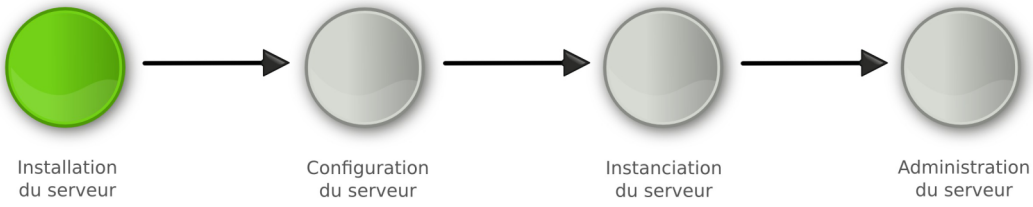
Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 5

Installation du module

La première des quatre phases



Installation

- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.462] 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.

1. Pré-requis

Matériel

Il est recommandé de vérifier la compatibilité matérielle en s'assurant que le serveur est compatible avec Ubuntu server 16.04 LTS (Xenial Xerus).

Les images ISO générées par EOLE intègrent le support de l'UEFI[p.475].

Architecture

Depuis la version EOLE 2.6 seule l'architecture 64 bits (AMD64[p.453]) est supportée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Médias d'installation

Les images d'installation des modules EOLE (format ISO et MD5SUMS) sont disponibles sur le site du projet EOLE en HTTP[p.461] :

- http://eole.ac-dijon.fr/pub/iso

Le fichier MD5SUMS sert à vérifier l'intégrité de l'image ISO téléchargée, avec la commande `md5sum` (l'image et le fichier MD5[p.465] sont dans le même répertoire) :

```
$ md5sum -c MD5SUMS
eole-2.6.x-alternate-amd64.iso: Réussi
```

Différents types de média sont utilisables pour installer les modules.

CD-ROM

1. graver l'image ISO préalablement téléchargée ;
2. démarrer le serveur cible sur le CD-ROM.

Clé USB

Créer une clé USB bootable depuis une distribution GNU/Linux

Pour créer une clé EOLE USB bootable avec l'image ISO EOLE depuis une distribution GNU/Linux ;

1. ouvrir un terminal en super utilisateur ;
2. insérer une clé USB, repérer le nom du périphérique (exemple : `/dev/sdx`) et démonter le support (`umount /dev/sdxy`) ;
3. se placer dans le répertoire contenant l'image ISO préalablement téléchargée ;
4. `# dd if=eole-2.6.x-alternate-amd64.iso of=/dev/sdx` (les données seront perdues !) ;
5. démarrer le serveur cible sur la clé USB.



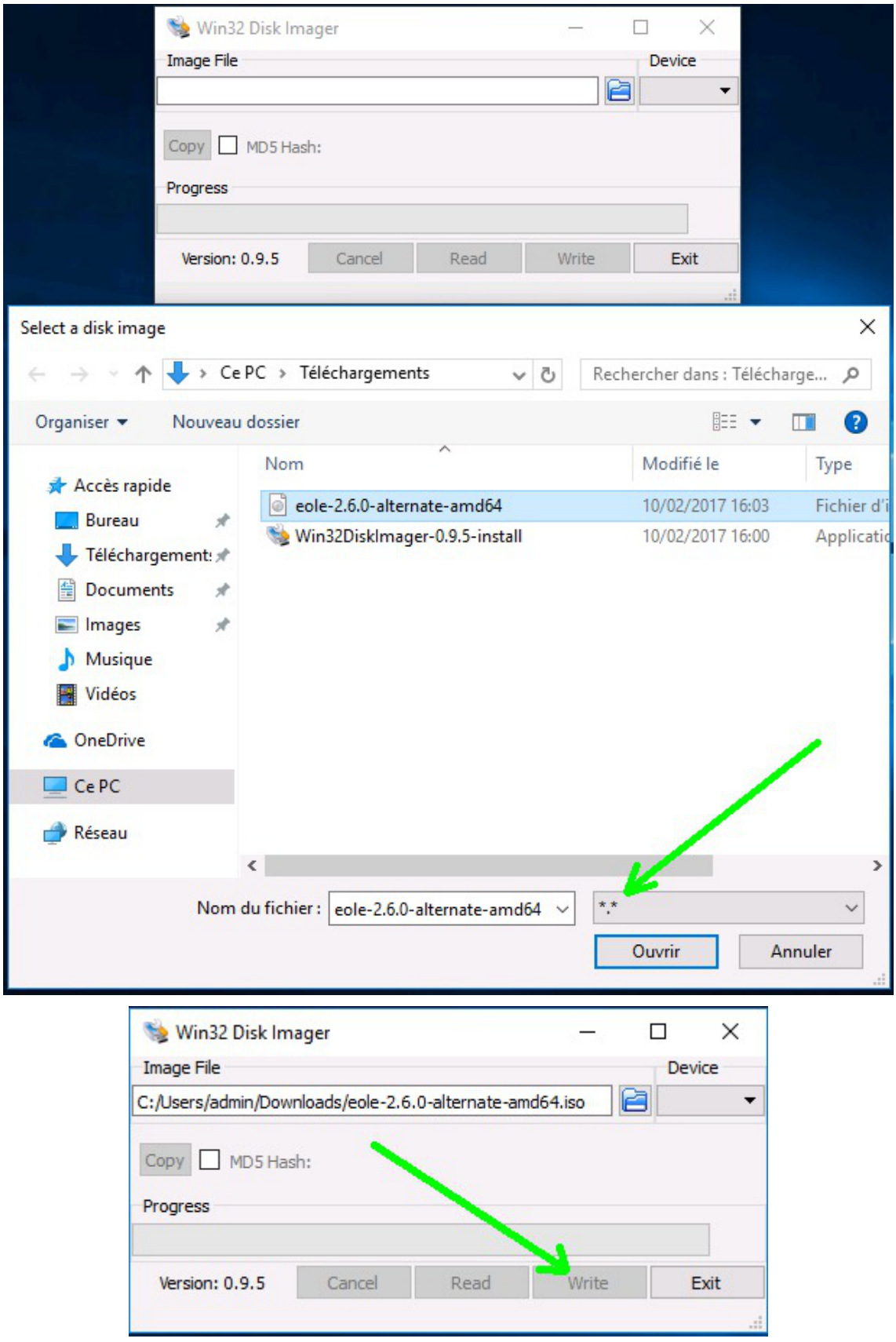
La commande `dd` écrase intégralement le contenu de la clé.

Créer une clé USB bootable depuis un poste Windows

Sur un poste Windows, il est possible de créer une clé USB bootable avec l'image ISO EOLE en utilisant le logiciel Win32 Disc Imager :

https://sourceforge.net/projects/win32diskimager/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



PXE

Le document suivant décrit la mise en place d'une configuration PXE[p.470] pour installer les modules

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

EOLE :
http://dev-eole.ac-dijon.fr/projects/pxe-menu/wiki

Installer EOLE depuis Ubuntu

Il est possible d'installer EOLE 2.6 sur une version installée de **Ubuntu LTS 16.04 édition serveur** [http://releases.ubuntu.com/16.04/] .



Il faut avoir à l'esprit que le partitionnement sera celui effectué à l'installation de la version d'Ubuntu et non le partitionnement automatique en LVM[p.465] proposé par l'installateur de l'image ISO EOLE.

La version d'Ubuntu pré-installée chez certains hébergeur peut être en anglais par défaut.
Il faut passer les locales à la valeur `fr_FR.UTF-8` :

```
# dpkg-reconfigure locales
```

Il faut également passer le clavier en français :

```
# dpkg-reconfigure keyboard-configuration
```

Utiliser les dépôts EOLE

- ajouter les dépôts EOLE

```
# cat > /etc/apt/sources.list.d/eole.list <<EOF
deb http://eole.ac-dijon.fr/eole eole-2.6.1 main cloud
deb http://eole.ac-dijon.fr/eole eole-2.6.1-security main cloud
deb http://eole.ac-dijon.fr/eole eole-2.6.1-updates main cloud
EOF
```

- ajouter la clé GPG publique d'EOLE (clé qui signe les paquets EOLE pour en vérifier l'intégrité)

```
# wget -q O - "http://eole.ac-dijon.fr/eole/project/eole-2.6-repository.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/eole-archive-keyring.gpg add -
```

- Désactiver l'architecture étrangère *i386*

```
# dpkg --remove-architecture i386
```

- mettre à jour les dépôts

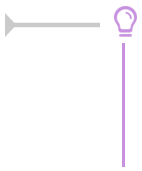
```
# apt-get update
```

Installer le module désiré



Attention les modules ne sont pas tous qualifiés pour être installés en mode conteneur et inversement certains modules ne sont pas installables en mode non conteneur (AmonEcole).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Les options `-y` et `--force-yes` de la commande `apt-get` indiquent au système de répondre automatiquement à toutes les questions pouvant apparaître lors de la configuration des paquets à installer.

Eolebase non conteneur

Installer la base d'EOLE pour un module non conteneur :

```
# apt-get install -y --force-yes eole-server eole-exim-pkg
```


Nécessite de télécharger environ 150 Mo d'archives.

Module non conteneur

Installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-all`, `eole-amon-all`) :

```
# apt-get -y --force-yes install eole-nomDuModule-all
```



Pour installer les modules Scribe ou eSBL (>=2.6.1) de cette manière, il faut ajouter le dépôt Envole 6 au fichier `/etc/apt/sources.list.d/eole.list` :

```
# echo "deb http://eole.ac-dijon.fr/envole envole-6 main" >> /etc/apt/sources.list.d/eole.list && apt-get update
```

Il faut ensuite procéder à l'installation du méta-paquet :

```
# apt-get -y --force-yes install eole-scribe-all
```


Nécessite de télécharger entre 180 Mo et 350 Mo d'archives selon le module à installer.

Eolebase conteneur

Installer la base d'EOLE pour un module conteneur :

```
# apt-get -y --force-yes install eole-lxc-controller ssmtp
```


Nécessite de télécharger environ 150 Mo d'archives.

Module conteneur

Installer la base d'EOLE pour un module conteneur :

```
# apt-get -y --force-yes install eole-lxc-controller ssmtp eole-nomDuModule-module
```

Installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-module`,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`eole-amon-module`).

Nécessite de télécharger entre 160 Mo et 200 Mo d'archives selon le module à installer.

Redémarrer le serveur

À la fin de l'installation il faut redémarrer le serveur pour mettre en place les mécanismes EOLE : interface de configuration du module, privilège via sudo…

Le mot de passe à utiliser pour se connecter en `root` est celui affiché dans la console.

Voir aussi...

Choisir le mode du module [p.58]

3. Déroulement de l'installation

Pour installer un module, il suffit de :

- démarrer le serveur cible avec le média d'installation choisi ;
- sélectionner le module à installer parmi ceux proposés ;
- valider en appuyant sur la touche Entrée.



Menu général de l'installeur EOLE

L'installation se déroule sans question, en plusieurs phases signalées par différents écrans de ce type :

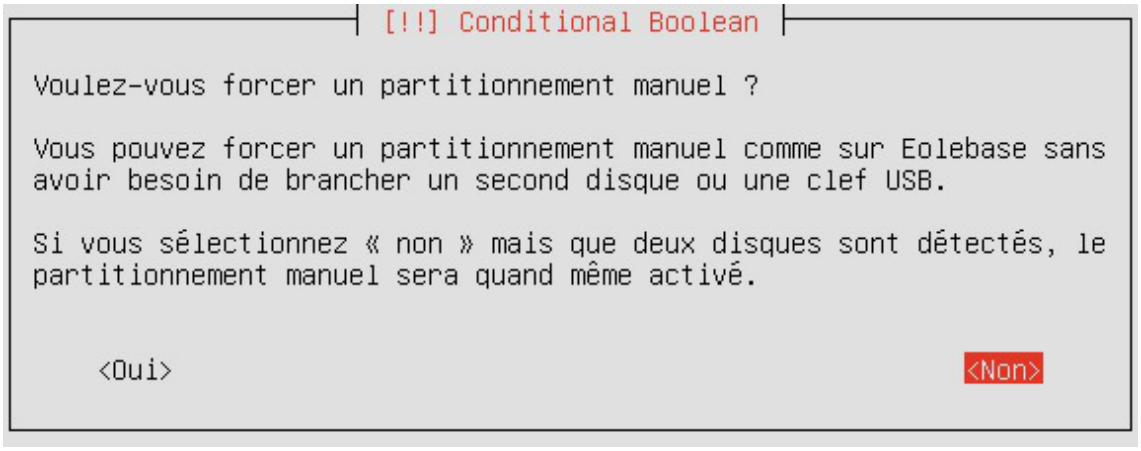
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Formatage des partitions du disque

Les différentes phases de l'installation sont :

1. détection du matériel ;
2. charger des composants supplémentaires ;
3. configuration du réseau avec DHCP ;
4. démarrage de l'outil de partitionnement ;
5. partitionnement LVM[p.465] assisté ou manuel ;



Forcer le partitionnement manuel en répondant oui à la question

6. formatage des partitions ;
7. partitionnement assisté ;
8. formatage des partitions ;
9. configuration de l'outil de gestion des paquets (Apt[p.454]) ;
10. choisir et installer des logiciels ;
11. installation du programme de démarrage GNU GRUB[p.461] ;
12. fin de l'installation.

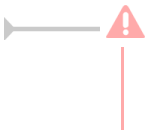
À la fin de l'installation l'écran suivant est affiché.



Fin de l'installation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En validant `Continuer`, le système redémarre automatiquement.



La bonne répartition de l'espace disque résultant d'un partitionnement automatique n'est pas garantie sur un disque inférieur à 30Go.

Une fois le système redémarré, comme indiqué par le prompt, vous pouvez ouvrir une session dans la console, mais aussi au travers de SSH, avec l'utilisateur **root** et le **mot de passe aléatoire** qui est **affiché**. Ce mot de passe sera bien évidemment changé lors de l'étape d'instanciation.

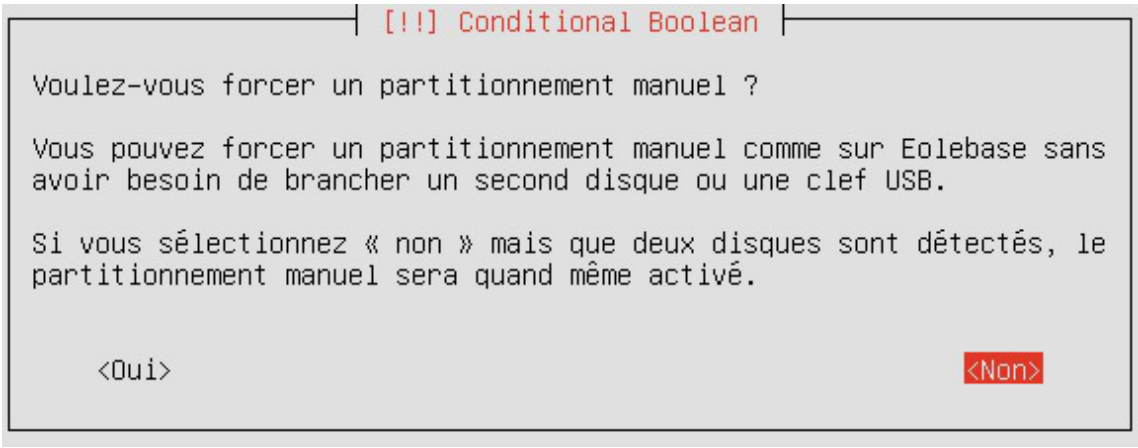
Voir aussi...

Les mots de passe [p.203]

4. Partitionnement personnalisé

Le partitionnement utilise le logiciel LVM[p.465].

- Sur une version d'EOLE inférieure à 2.5.1, seule l'installation d'`Eolebase`, aiguille systématiquement vers un partitionnement manuel et nécessite une intervention. Cependant, si l'installeur rencontre au moins deux disques dans l'ordinateur (2 disques durs ou 1 clé USB) il passe en partitionnement manuel quelque soit le module.
- Sur une version supérieure ou égale à 2.5.1 d'EOLE, une fenêtre propose de choisir un partitionnement manuel, il peut être refusé, le partitionnement sera alors automatique y compris sur un Eolebase.



Forcer le partitionnement manuel en répondant oui à la question



La présence d'une partition `/home` avec l'option `usrquota` est requise pour les modules **Horus**, **Scribe** et **AmonEcole**.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Si le mode conteneur est envisagé, le partitionnement doit prendre en compte le fait que les conteneurs sont mis en place dans le répertoire `/opt/lxc`.

La bonne répartition de l'espace disque résultant d'un partitionnement automatique n'est pas garantie sur un disque inférieur à 30Go.

Partitionnement manuel

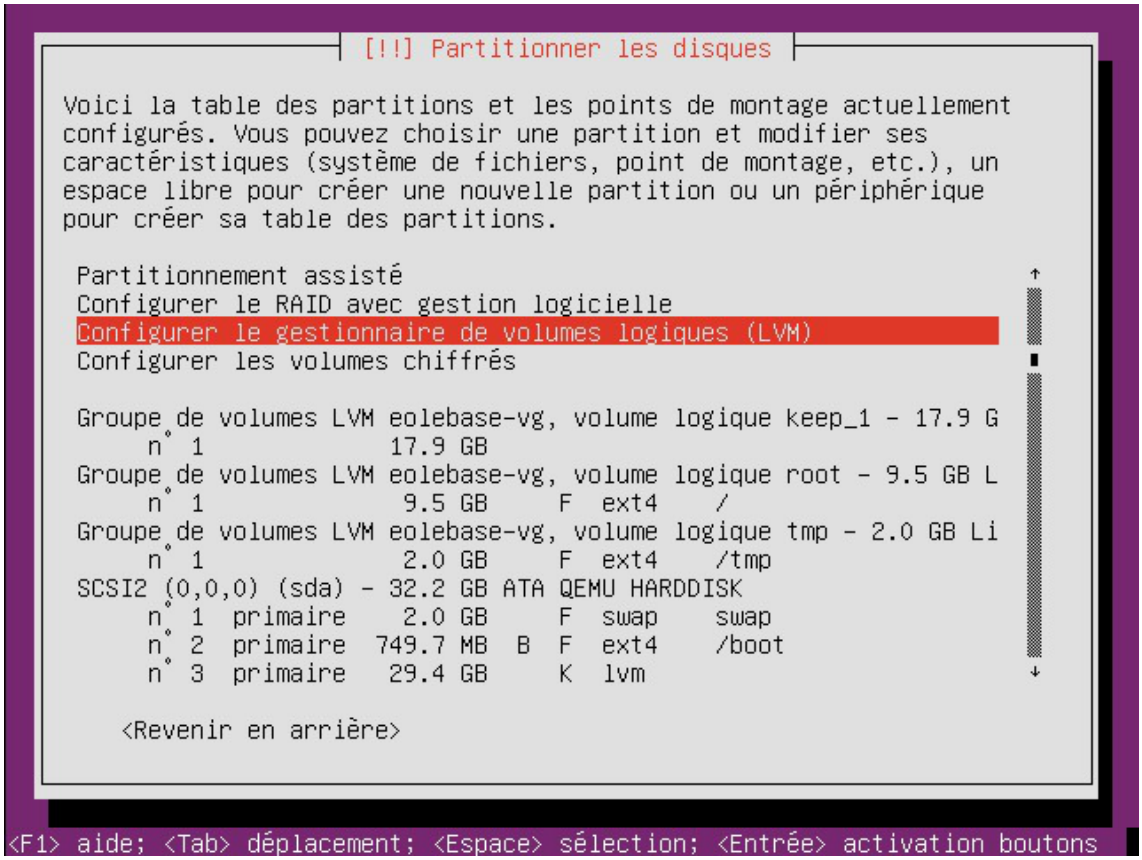
Lorsque le partitionnement manuel est déclenché une fenêtre propose de choisir le disque qu'il faut partitionner pour accueillir le système d'exploitation.



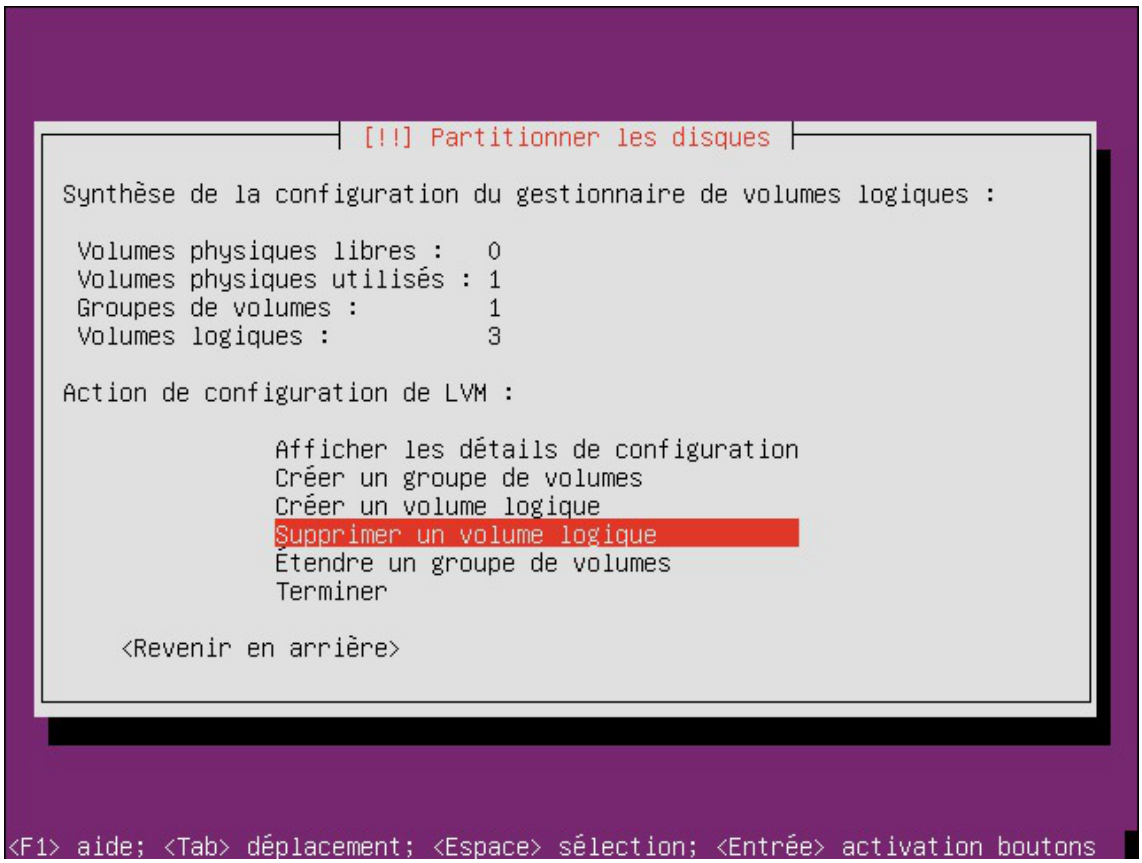
Un volume logique nommé `keep_x` sans point de montage et sans système de fichiers contient l'espace qui n'a pas été attribué lors du calcul des autres volumes.
Sur un Eolebase il n'y a pas de volume proposé pour le point de montage `/home`.

- Sélectionner `Configurer le gestionnaire de volumes logiques (LVM)`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

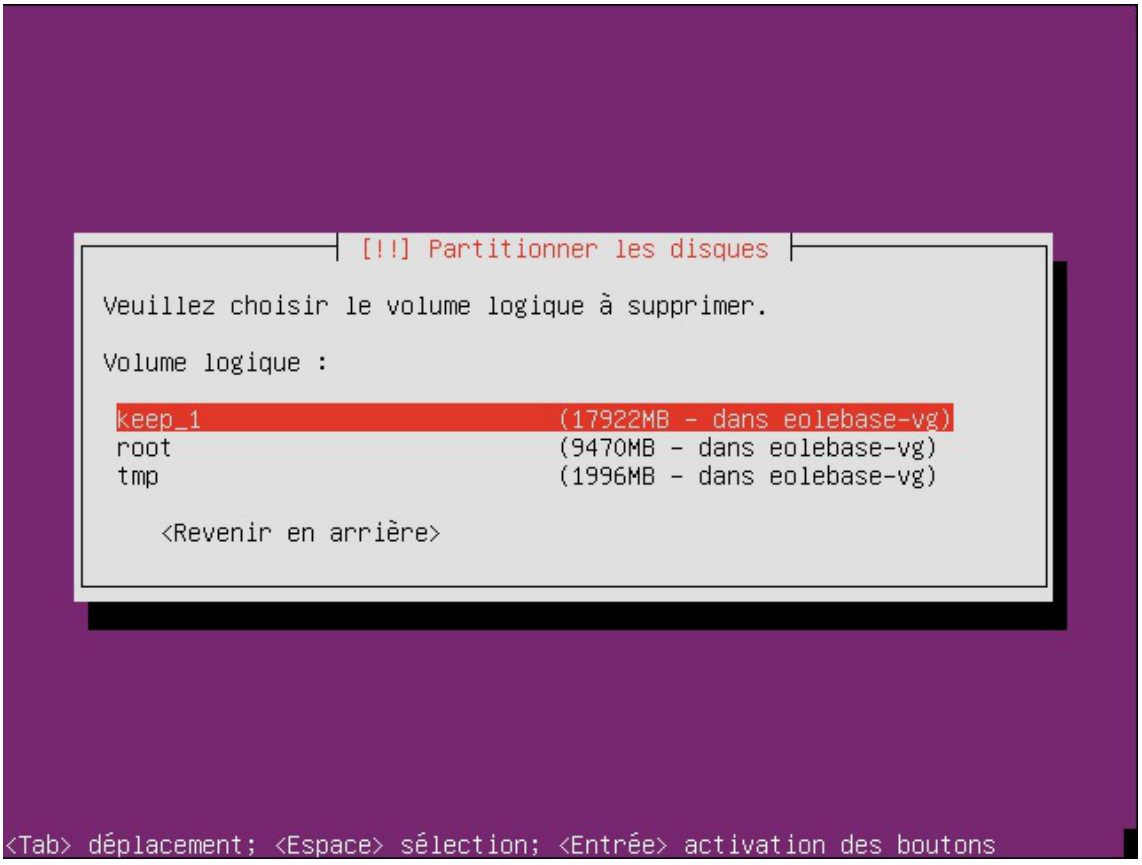


- Sélectionner `Supprimer un volume logique`

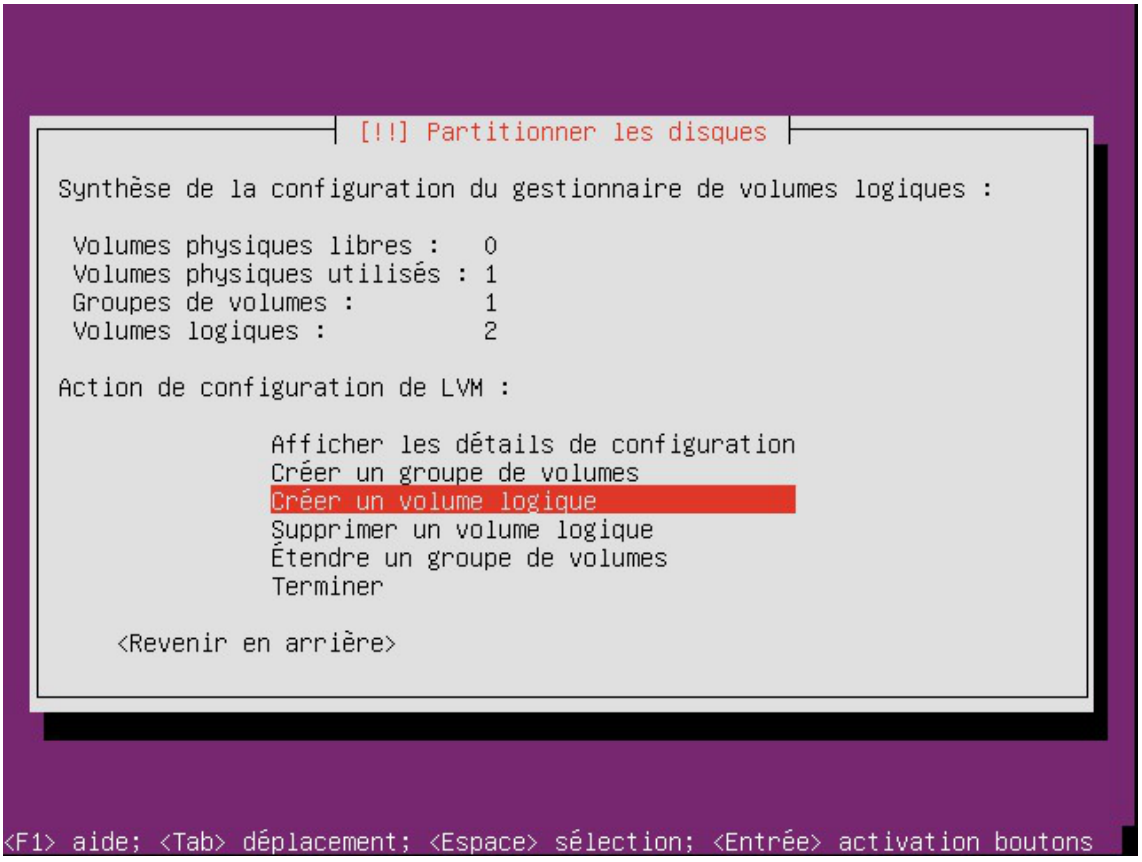


- Sélectionner le volume logique `keep_x`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

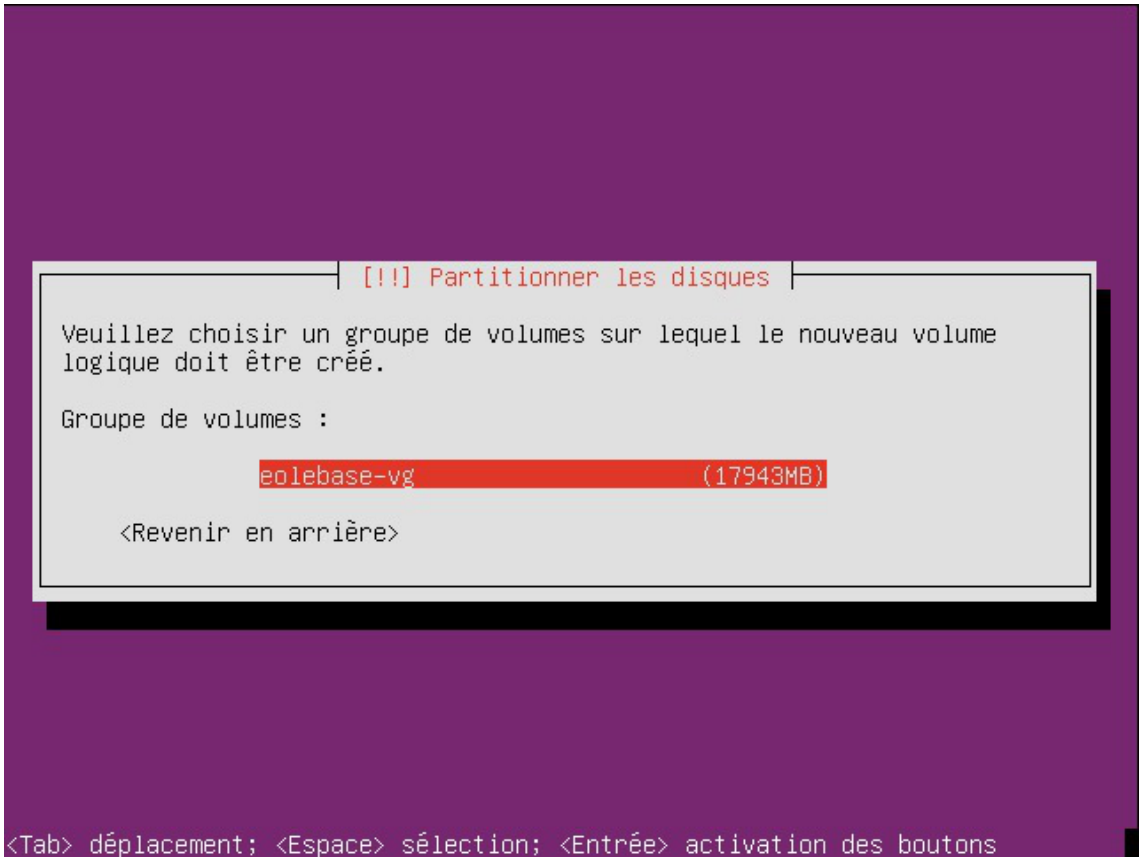


- De retour sur la gestion des volumes logiques, sélectionner `Créer un volume logique`

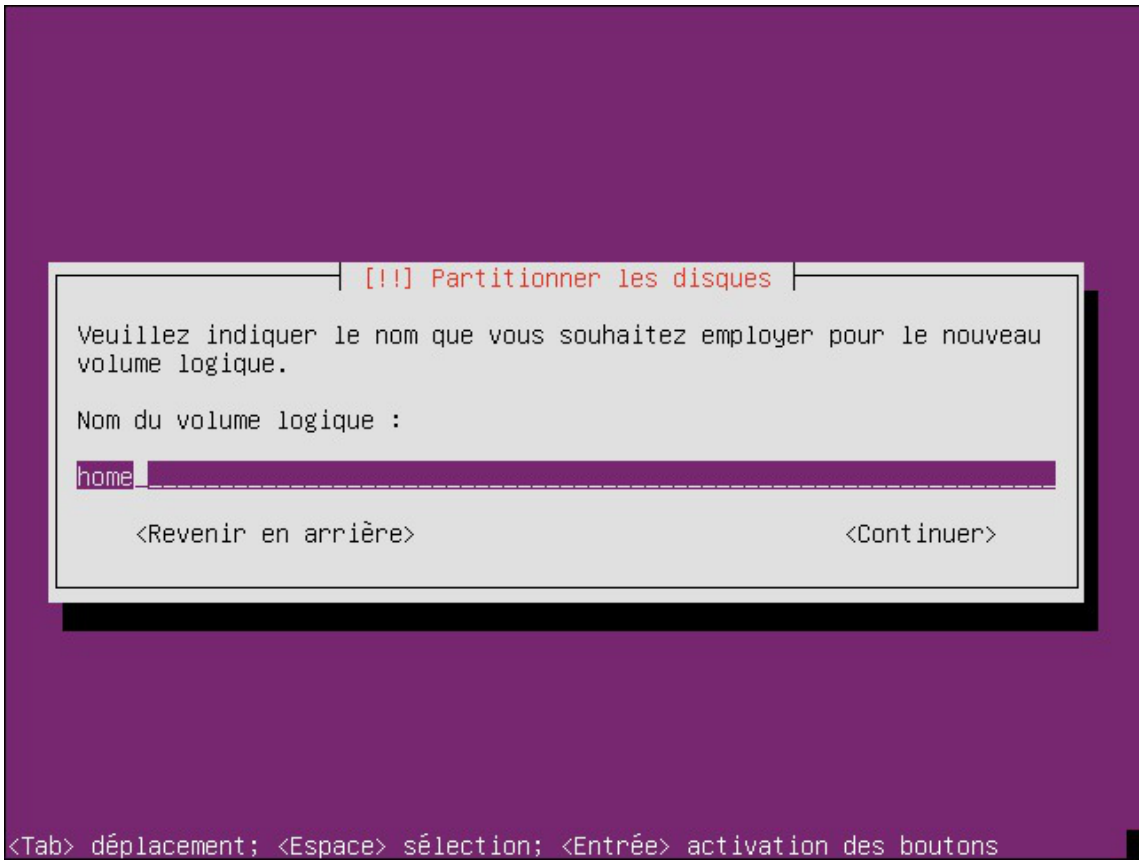


- Valider l'unique `Groupe de volumes` proposé

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

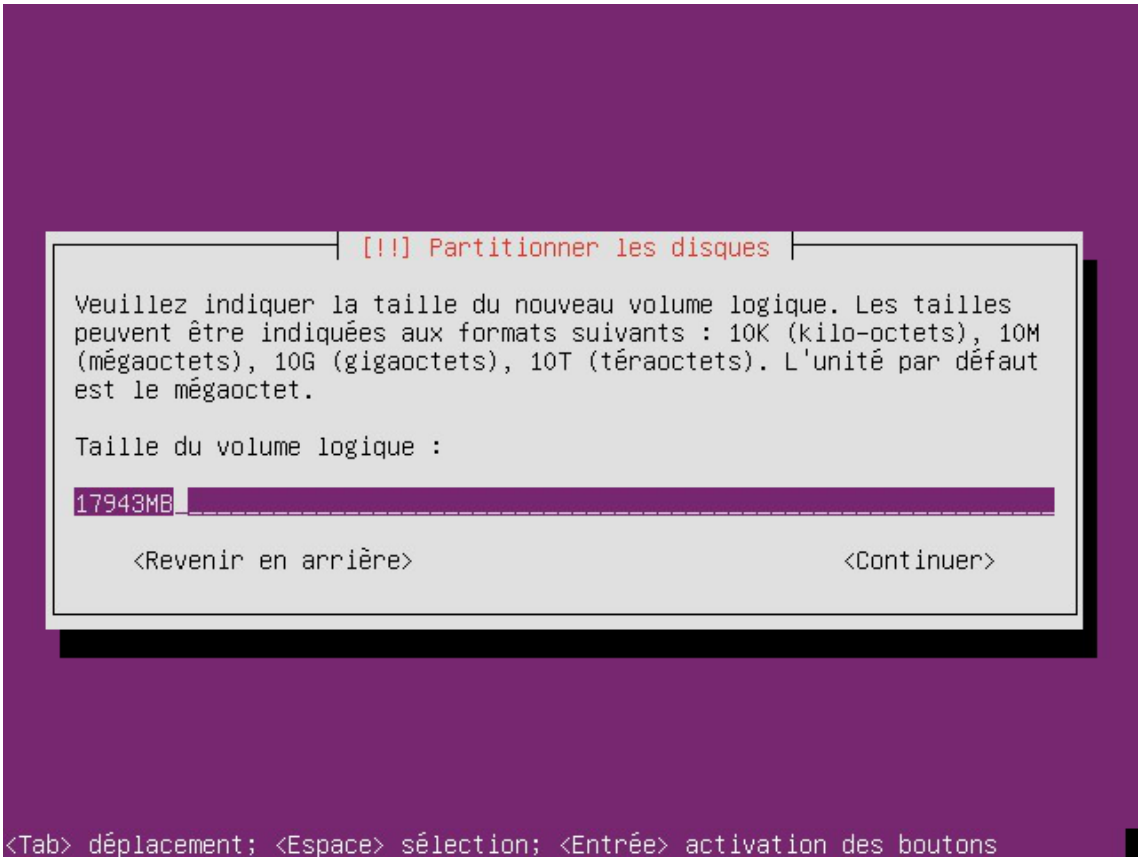


- Choisir le nom du nouveau volume logique

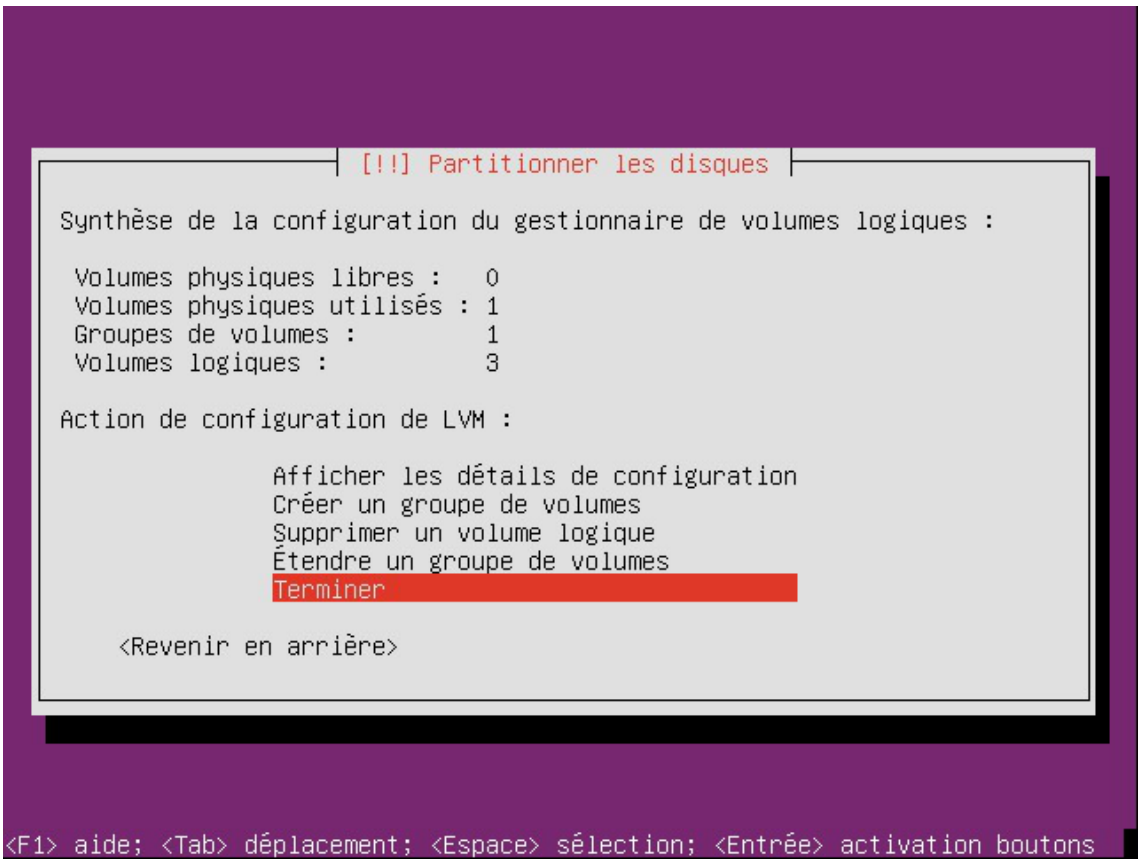


- Puis choisir l'espace à octroyer au nouveau volume, par défaut la taille affichée est la taille maximale

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

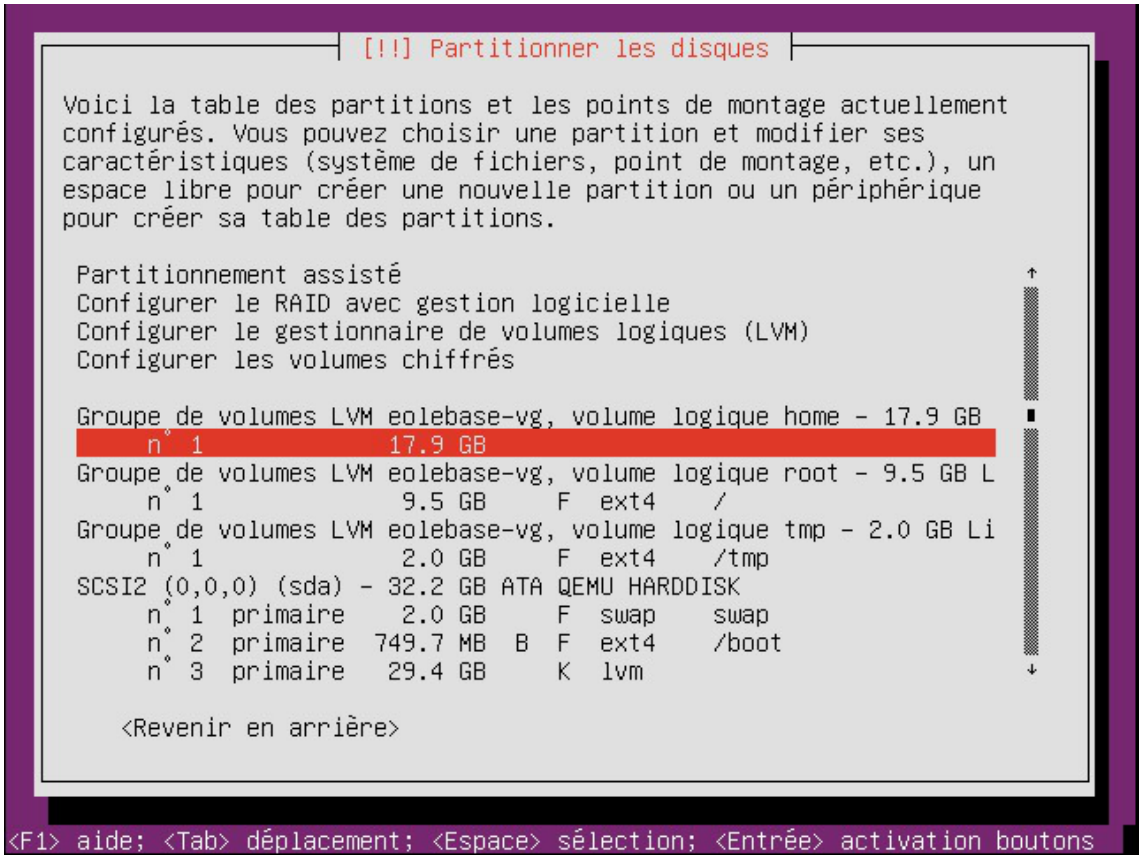


- De retour sur la synthèse de la configuration, sélectionner `Terminer`

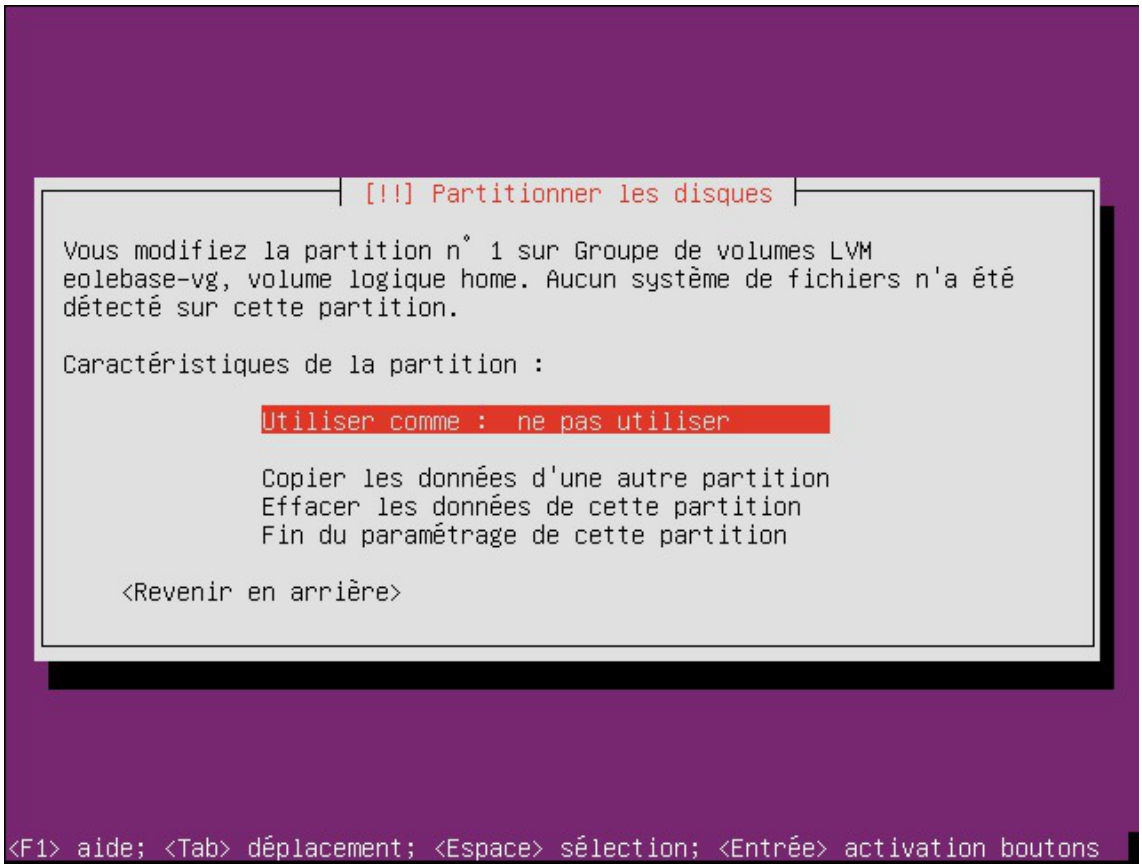


- L'outil de partitionnement affiche maintenant le volume `home`, sélectionner le pour édition

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

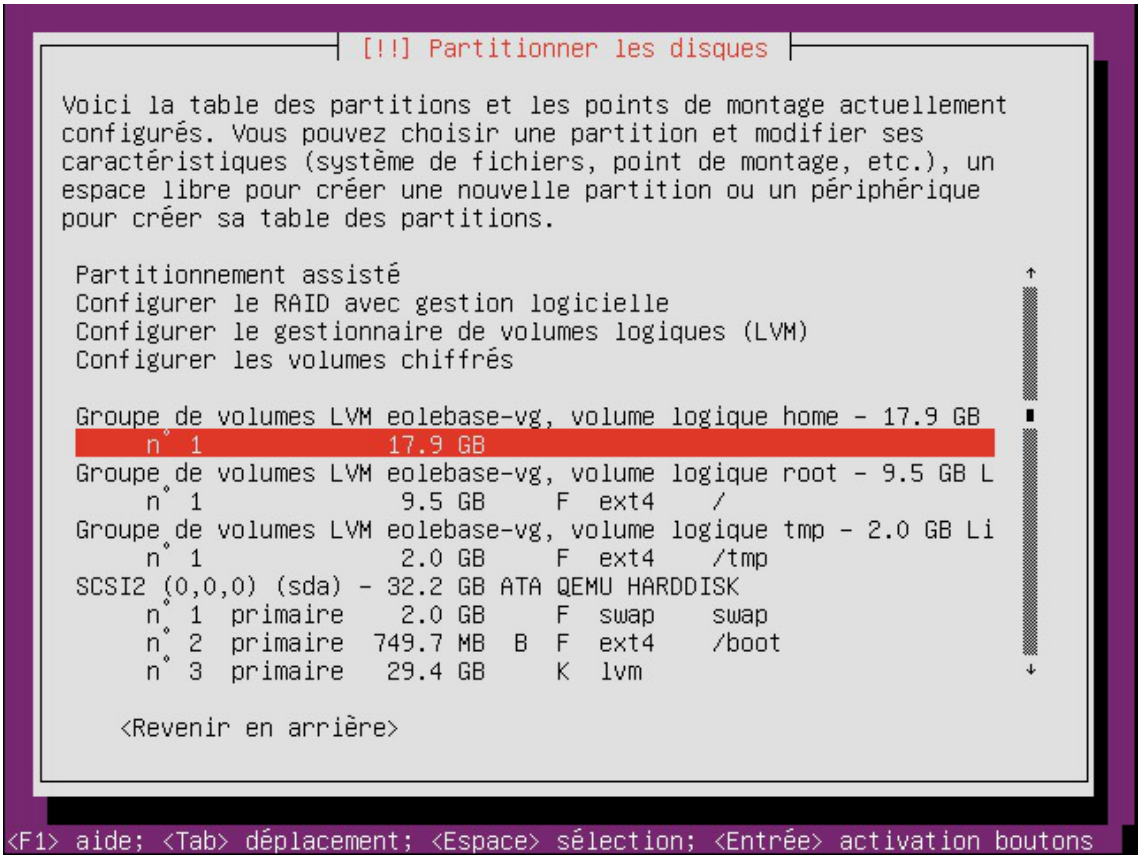


- Sélectionner `Utiliser comme : ne pas utiliser` pour choisir les caractéristiques du volume

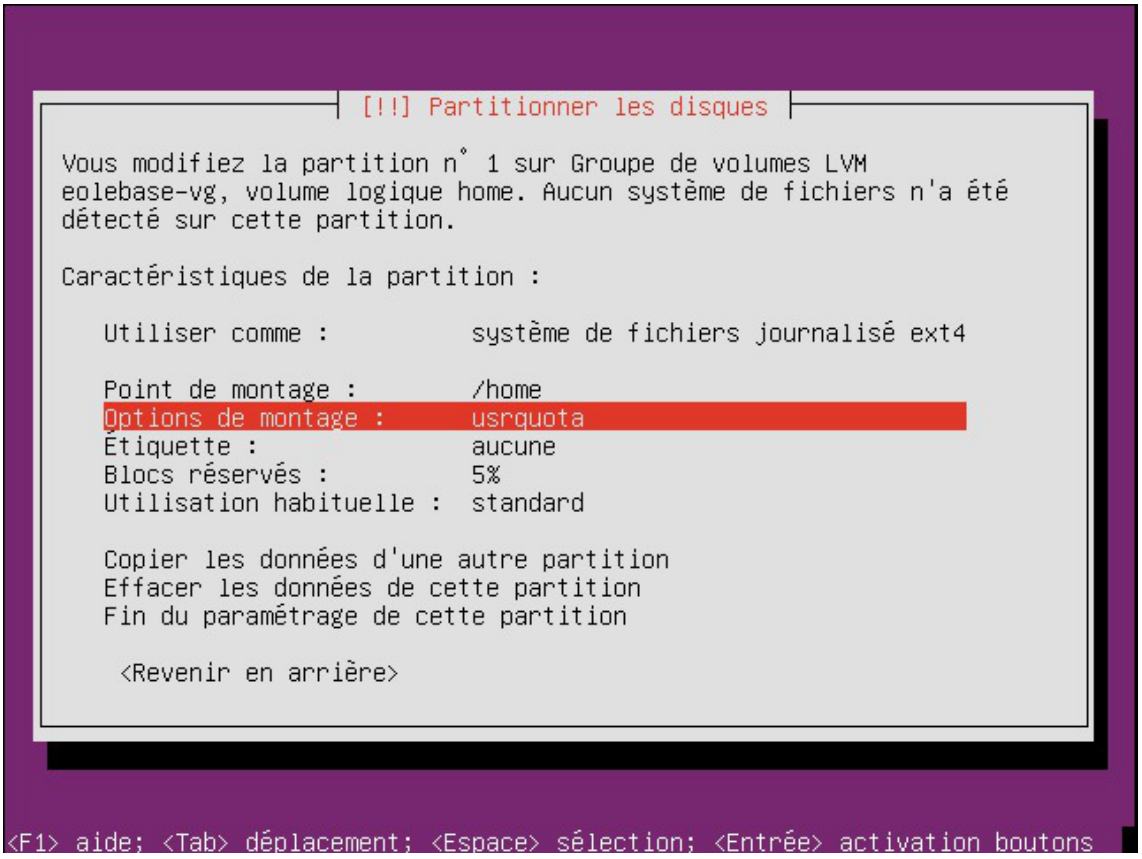


- Sélectionner le type système de fichier

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

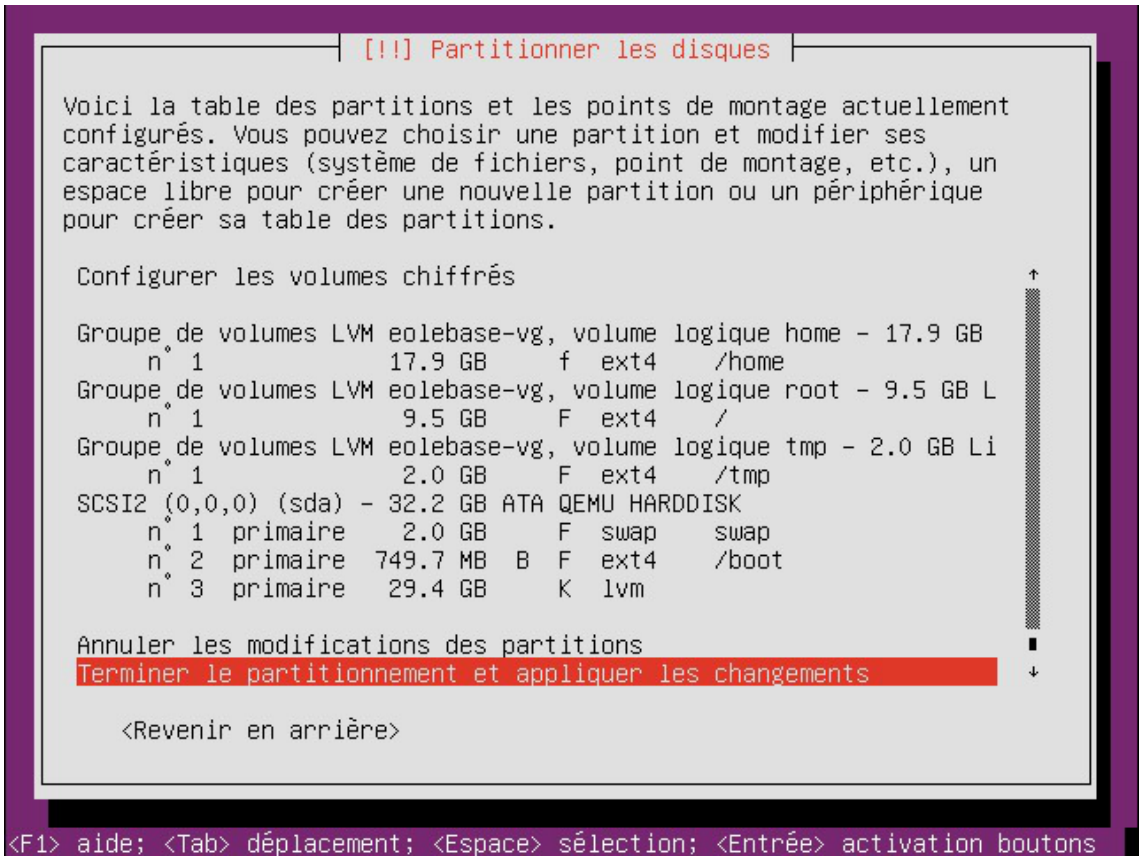


- Puis définir le point de montage et les options de montage

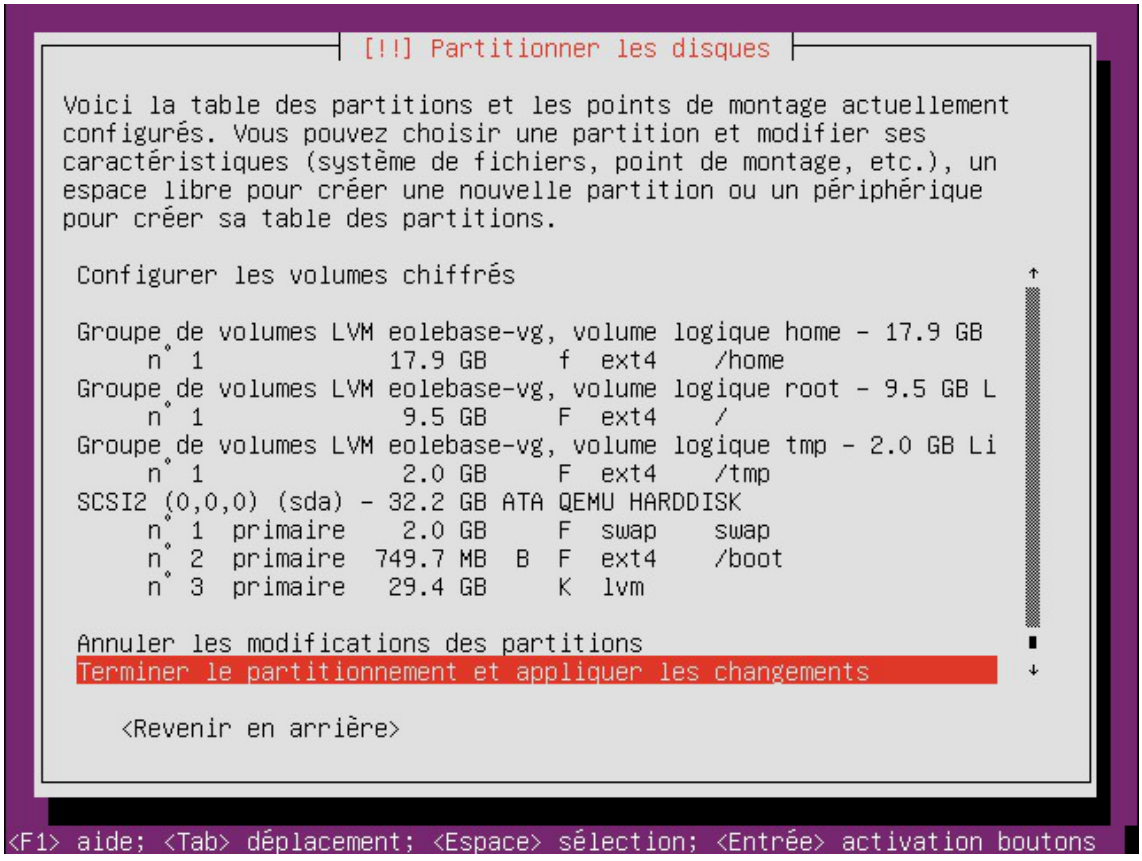


- Sélectionner la `Fin du paramétrage de cette partition`, de retour sur la fenêtre principale du partitionnement

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Sélectionner Terminer le partitionnement et appliquer les changements.



Ajouter de l'espace disque à un volume LVM

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  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.

Ajustement du partitionnement au travers de l'interface de configuration



L'ajustement du partitionnement n'est disponible dans l'interface de configuration du module en mode expert qu'avant l'instance et seulement si le volume physique contient de l'espace libre. Cette fonctionnalité est donc visible par défaut sur Eolebase et sur d'autres modules si le partitionnement manuel à été utilisé pour réserver de l'espace.

Pour maîtriser correctement ce qui va être fait il faut consulter l'état du partitionnement avant de saisir les paramètres souhaités à l'aide de la commande `df -h /` et des commandes `vgdisplay` et `lvdisplay`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     2,1G  6,5G  25% /
tmpfs                          1000M      28K 1000M   1% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     2,9M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
root@eolebase:~#
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  8
  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       5550 / 21,68 GiB
  Free  PE / Size       4510 / 17,62 GiB
  VG UUID               ctPVcP-76Se-EpMp-FLO3-13aR-Ghg9-PdIdUW

root@scribe:~#
```

```
root@scribe:~# lvdisplay

  --- Logical volume ---
  LV Path                /dev/scribe-vg/root
  LV Name                root
  VG Name                scribe-vg
  LV UUID                uN8emF-hD9j-eNwv-zdaC-mEeK-9XGe-uBu2OU
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-10-05 18:37:11 +0200
  LV Status              available
  # open                 1
  LV Size                8,94 GiB
  Current LE             2288
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:0

[...]
```

Ajuster le partitionnement sur une version d'EOLE inférieur à 2.6.2

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour ajuster le partitionnement sur une version d'EOLE inférieure à 2.6.2, ouvrir l'interface de configuration du module, passer en mode Expert et se rendre dans l'onglet `Système`.



Après avoir passer `Ajuster le partitionnement` à `oui` et après avoir cliquer sur le bouton `+ Nom du volume à créer` un certain nombre de paramètres s'affiche.



- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;
- point de montage ;
- les options du montage (indispensable pour la gestion des quotas par exemple).

Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

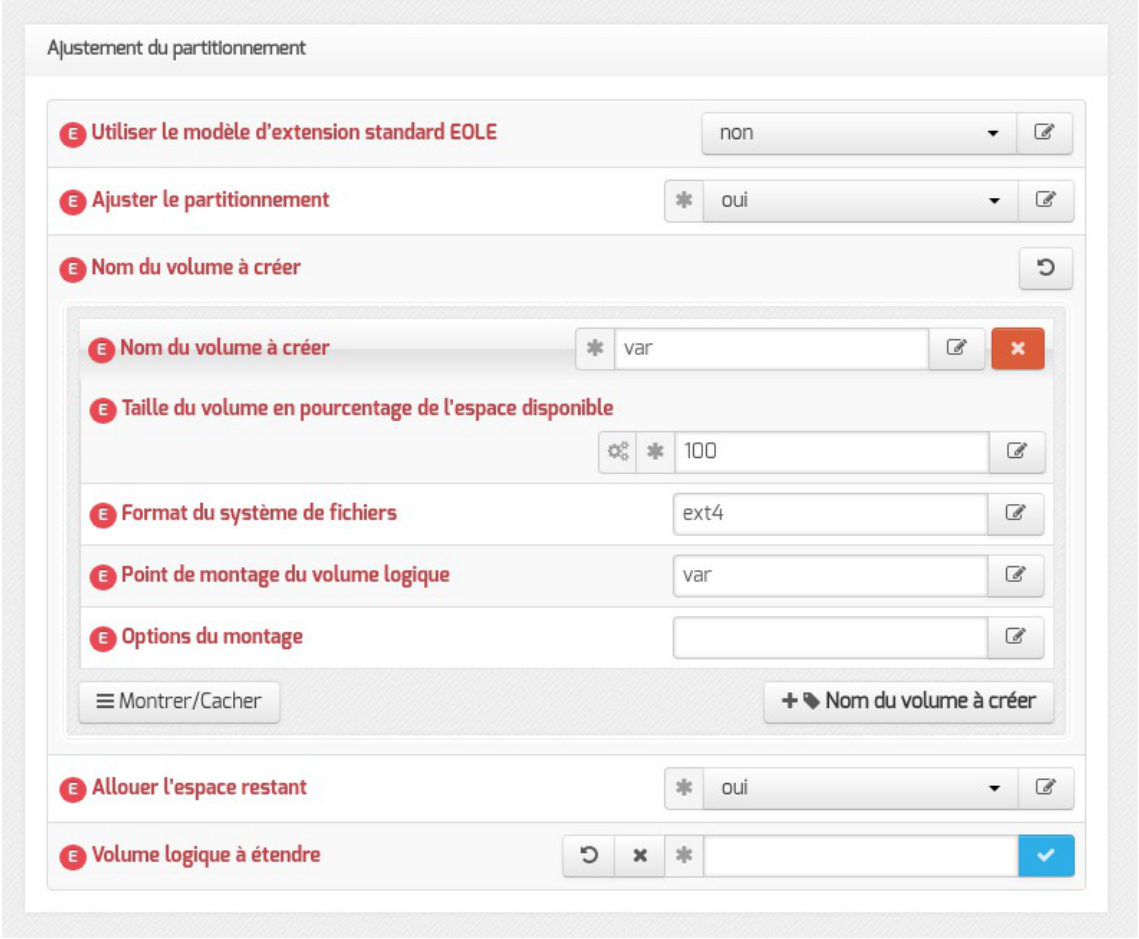
Ajuster le partitionnement sur une version d'EOLE supérieure ou égale à 2.6.2

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques et d'ajouter de l'espace à des partitions existantes.

Pour ajuster le partitionnement à partir de la version 2.6.2 d'EOLE, ouvrir l'interface de configuration du

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

module, passer en mode Expert et se rendre dans l'onglet `Système`. Puis il faut passer `Utiliser le modèle d'extension standard EOLE` à `non` pour ajuster le partitionnement.



Ajustement du partitionnement à partir d'EOLE 2.6.2

Après avoir passer `Ajuster le partitionnement` à `oui`, les partitions existantes sont affichées et un certain nombre de paramètres s'affichent.



- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- point de montage ;
- les options du montage (indispensable pour la gestion des quotas par exemple).

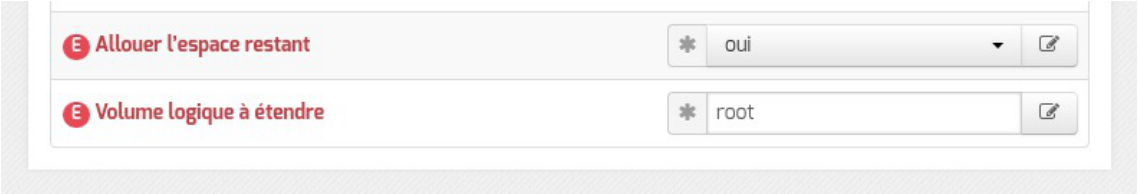
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

Allouer l'espace restant

Positionner la variable `Allouer l'espace restant` à `oui` permet de choisir un volume existant auquel ajouter la totalité de l'espace libre restant.



La valeur à saisir est la partie du nom du volume qui permet d'identifier le point de montage, par exemple pour le volume `/dev/mapper/eolebase--vg-root` il faut saisir `root` dans le nom du `Volume logique à étendre`. S'il ne reste pas d'espace, ce jeu de paramètres est sans effet.

Résultat après instance

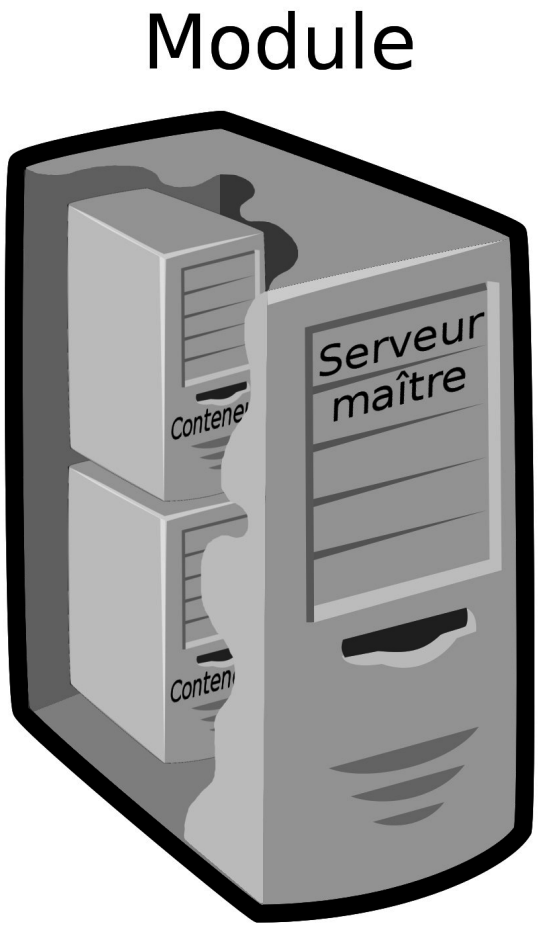
Le paramétrage est effectif après l'instanciation du module.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     1,9G  6,7G  22% /
tmpfs                          1000M       0 1000M   0% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     3,6M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
/dev/mapper/eolebase--vg-var     27G     311M   25G   2% /var
root@eolebase:~#
```

Le nouveau volume logique est présent et la partition `/root` s'est vu augmentée du reste de l'espace libre.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

5. Choisir le mode du module



EOLE propose un système évolué et cohérent de conteneurs[p.456].

Les conteneurs permettent d'isoler un environnement et d'en limiter les ressources allouées.

Cela permet également d'exécuter séparément et plus efficacement différentes tâches spécifiques.

Contrairement à la virtualisation, une seule instance du noyau est lancée.

EOLE utilise les conteneurs pour séparer des processus sans augmenter le nombre de serveurs physiques.

Modules en mode non conteneur

La quasi totalité des modules EOLE 2.6 sont installables en mode non conteneur :

- `Amon` ;
- `eSBL` ;
- `eCDL` ;
- `Hâpy` et ses dérivés ;
- `Horus` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Scribe` ;
- `Seshat` ;
- `Thot` ;
- `Sphynx` ;
- `Zéphir`.



Si vous avez choisi un module ne nécessitant pas le mode conteneur ou que vous n'avez pas forcé la mise en place du mode conteneur vous pouvez faire les mises à jour ou passer directement à l'étape de configuration du module.

Mise à jour du module

Après l'installation du module, la mise à jour n'est pas obligatoire mais fortement recommandée. Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto`.

Module en mode conteneur

Contrairement à ceux cités précédemment, le module `AmonEcole` installable **obligatoirement** en *mode conteneur*.

Sur ce module, certains services installés sont dans différents conteneurs et ne sont pas compatibles entre eux. L'installation en *mode non conteneur* est donc impossible.

À partir d'un module



Si vous avez choisi un module nécessitant le *mode conteneur* ou que vous avez forcé la mise en place du *mode conteneur* il est nécessaire de générer les conteneurs après une mise à jour du module.

Mise à jour

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



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

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

Installation des conteneurs

La génération des conteneurs se fait à l'aide de la commande `gen_conteneurs`.

Les conteneurs seront installés sur le réseau **192.0.2.0/24**.

Le masque sera obligatoirement 255.255.255.0.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Attention si ce réseau est déjà utilisé dans votre architecture.

Il n'est plus possible, depuis la version 2.4.x d'EOLE, d'installer les conteneurs sur un réseau différent.

Des logs sur la génération des conteneurs sont disponibles après la génération des conteneurs dans le fichier `/var/log/isolation.log`.

L'option `-l` permet de choisir le niveau des messages (info, warning,error ou critical).

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande `gen_conteneurs` suivie du paramètre `-h` permet d'obtenir de l'aide.

À partir d'EoleBase

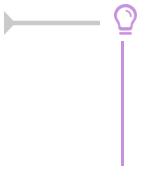
Dans le cas d'une installation faite depuis une `EoleBase`, il est possible d'installer un module en mode conteneur.

La procédure recommandée actuellement est la suivante :

- installer un module `Eolebase`
- mettre à jour la liste des paquets :
  `Query-Auto` ou `Query-Cd`
- installer le paquet `eole-lxc-controller` :
  `apt-eole install eole-lxc-controller ssmtp`
- installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-module`, `eole-amon-module`) :
  `apt-eole install eole-scribe-module`

Mise à jour

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



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

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

Installation des conteneurs

La génération des conteneurs se fait à l'aide de la commande `gen_conteneurs`.

Les conteneurs seront installés sur le réseau **192.0.2.0/24**.

Le masque sera obligatoirement 255.255.255.0.

Attention si ce réseau est déjà utilisé dans votre architecture.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il n'est plus possible, depuis la version 2.4.x d'EOLE, d'installer les conteneurs sur un réseau différent.

Des logs sur la génération des conteneurs sont disponibles après la génération des conteneurs dans le fichier `/var/log/isolation.log`.

L'option `-l` permet de choisir le niveau des messages (info, warning,error ou critical).

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande `gen_conteneurs` suivie du paramètre `-h` permet d'obtenir de l'aide.

- Il n'est pas possible de passer du mode non conteneur au mode conteneur, et vice versa ;
- La présence d'une partition `/home` avec l'option `usrquota` est requise sur pour les modules Horus, Scribe et AmonEcole ;
- Le partitionnement doit prendre en compte le fait que les conteneurs sont mis en place dans le répertoire `/opt/lxc`.

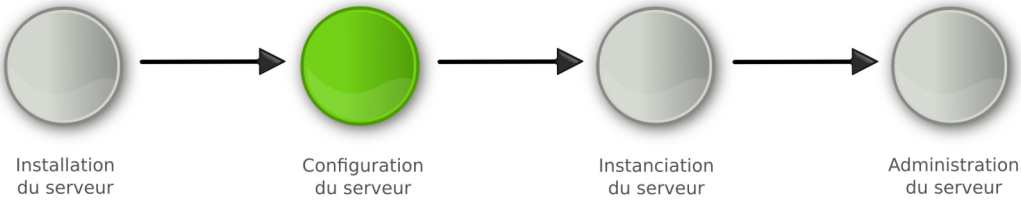
Voir aussi...

Les mises à jour

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 6

Configuration du module Zéphir



Configuration

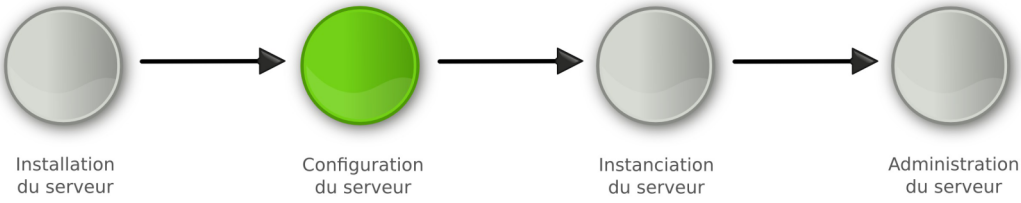
- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config` .

  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 première interface réseau 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.473], e2guardian[p.458], etc.

1. Configuration généralités



Configuration

La configuration suit la phase d'installation du serveur.

Il s'agit de collecter et de renseigner les paramètres nécessaires au fonctionnement du serveur.

Les paramètres saisis peuvent être internes au serveur (par exemple le nombre d'interfaces réseau) ou externes (par exemple l'adresse du DNS[p.458], l'adresse du serveur de temps NTP[p.467], ...). Cette étape nécessite une bonne connaissance de l'architecture réseau dans laquelle sera installé le serveur.

À condition d'avoir renseigné les valeurs obligatoires vous pouvez enregistrer la configuration pour

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'effectuer en plusieurs temps.

On obtient alors un fichier `config.eol`, dans lequel sont stockées toutes les valeurs saisies.

La configuration du module porte aussi bien sur les paramètres propres à EOLE que sur le paramétrage d'applications tierces embarquées dans le module. On retrouve par exemple les paramètres du fichier `squid.conf` dans l'interface de configuration du module.

Il existe deux modes de configuration :

- **mode autonome**

  Le mode autonome est l'utilisation de l'interface de configuration du module pour paramétrer le serveur.

  À son lancement, l'interface de configuration du module récupère dans les différents dictionnaires, les variables, leur valeur par défaut et les libellés qui seront affichés dans l'interface.

  Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, vous bénéficier d'un accès distant à l'interface de configuration du module au travers d'un navigateur web.

- **mode Zéphir**

  Le mode Zéphir consiste à configurer le module au travers de l'application Zéphir depuis le module du même nom. Ce module permet la mise en place d'un serveur de gestion de parc de serveurs EOLE. Par le mécanisme de variante, vous pouvez avoir des configurations pré-définies pour un ensemble de serveurs.

1.1. Configuration en mode autonome

La configuration en mode autonome signifie que la configuration est réalisée directement sur le serveur à l'aide de l'interface de configuration du module.

Ce mode est recommandé pour la configuration d'un petit nombre de serveurs.

La méthode autonome permet d'exporter et/ou d'importer le fichier `config.eol`.

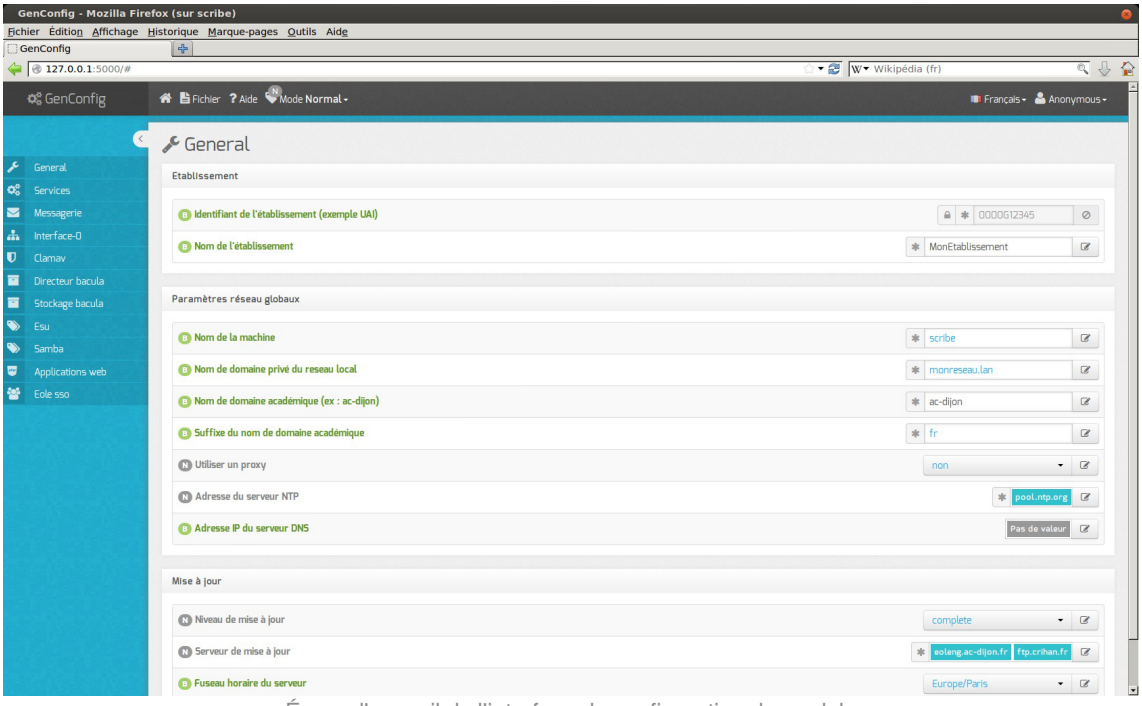
Il est donc possible d'utiliser le fichier `config.eol` d'un serveur en production pour en *instancier* un nouveau.



En mode autonome le fichier `config.eol` peut être préparé avant l'installation du serveur et peut être confié à une personne tierce, comme par exemple la personne en charge d'installer le serveur dans l'établissement. Celui-ci n'aura plus qu'à instancier le serveur.

L'interface de configuration du module se lance avec la commande : `gen_config`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Écran d'accueil de l'interface de configuration du module

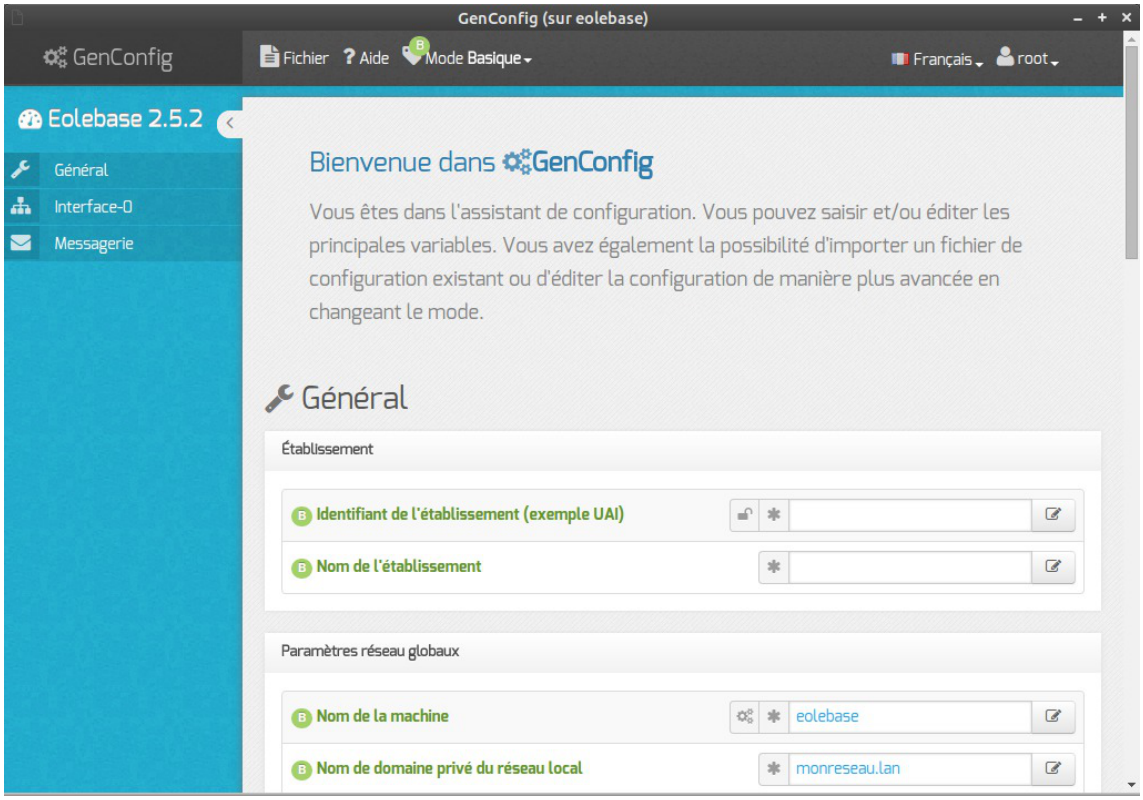
Une fois la commande `gen_config` lancée, comme indiqué dans la mire, vous devez ouvrir une session avec l'utilisateur **root** et le **mot de passe aléatoire** généré à l'installation.



Ce mot de passe sera bien évidement changé lors de l'étape d'instanciation.

Lors de son premier lancement l'interface de configuration du module propose un assistant de configuration rapide.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Seules les variables indispensables pour un fonctionnement minimum sont proposées dans l'assistant.

L'interface se découpe en quatre zones :

- la zone *Menu* ;
- la zone *Onglet* ;
- la zone *Formulaire* ;
- la zone *Validation*.

Certains onglets sont générés dynamiquement en fonction des éléments activés ou non dans le formulaire.

Les onglets correspondant au mode **expert** apparaissent si ce dernier est activé.

1.1.1. Accès distant

Accès distant via le port 7000

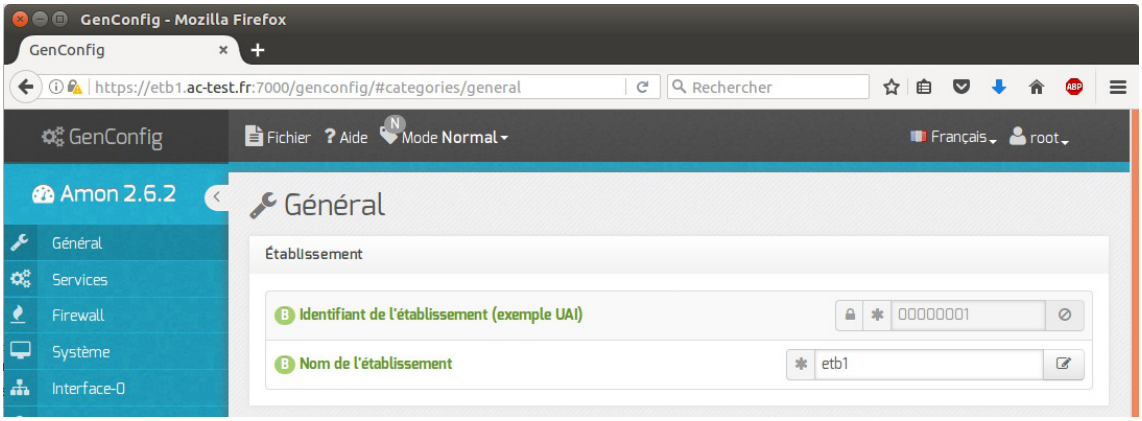
Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

`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.

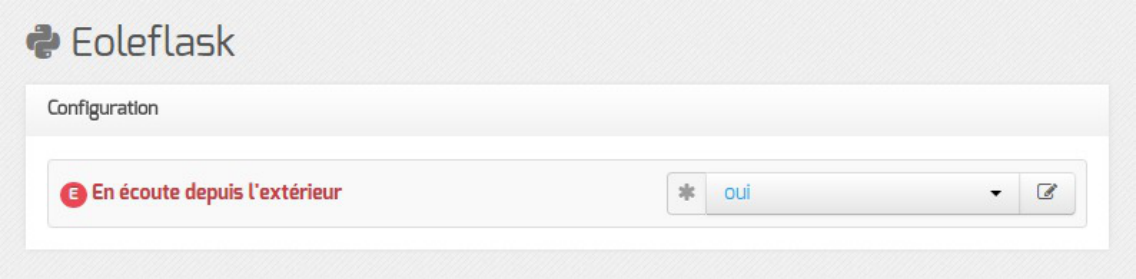
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de l'interface de configuration au travers d'un navigateur web (port 7000)

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`.

Cette fonctionnalité est désactivable dans l'onglet `Eoleflask` en mode expert.



Passer la variable `En écoute depuis l'extérieur` à `non`.

Accès distant via le port 443

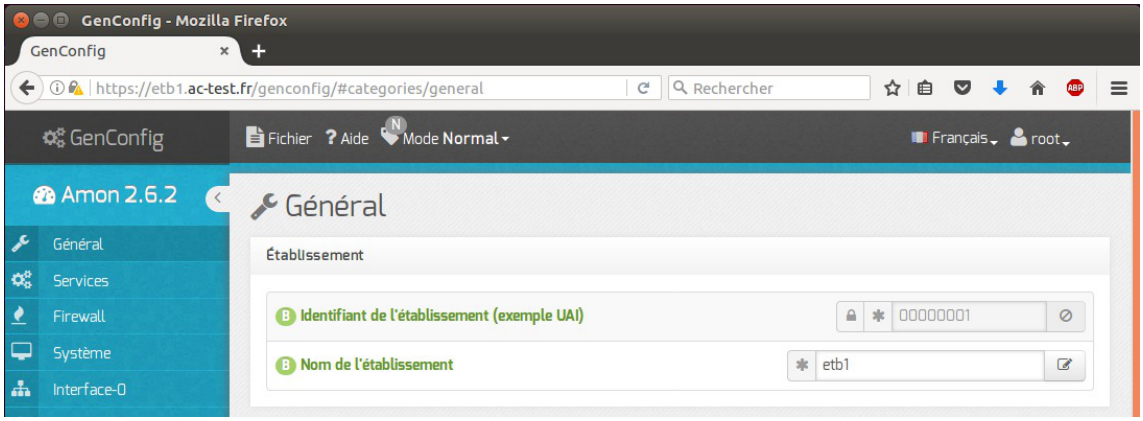
À partir d'EOLE 2.6.1, l'interface est également disponible sur le port 443 si la variable experte `Activer l'interface de configuration du module (GenConfig)` est à `oui` dans l'onglet `Services`. C'est le cas par défaut à partir d'EOLE 2.6.2.

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 depuis un navigateur web en HTTPS à l'adresse suivante :

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

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de l'interface de configuration au travers d'un navigateur web (port 443)

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`.

1.1.2. La zone Menu

La zone de Menu, en haut de l'interface, propose les items suivants :

- Fichier : gestion de la configuration
- Aide : permet de lancer l'assistant et d'afficher l'aide de l'application
- Mode : choix des modes de configuration à activer
- Langue : choix de la langue pour l'interface
- Session : permet de se déconnecter.

Sous-menu Fichier

- Enregistrer la configuration
- Recharger/Annuler les modifications
- Re-syncroniser la configuration
- Exporter la configuration
- Importer une configuration
- Quitter GenConfig

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Sous menu Fichier

Enregistrer la configuration permet l'enregistrement du paramétrage dans le fichier `config.eol` du serveur.

Recharger/Annuler les modifications permet de revenir à l'état initial à l'ouverture.

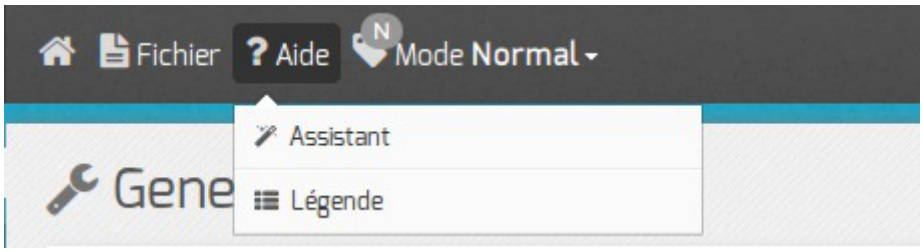
Re-synchroniser la configuration permet de récupérer les informations stockées en session sur le serveur si une coupure arrivait pendant la configuration.

Exporter la configuration propose le téléchargement du fichier `config.eol` du serveur.

Importer une configuration permet de téléverser un fichier `config.eol` sur le serveur.

Sous-menu Aide

- Assistant
- Légende



Sous menu Aide

L'assistant bascule l'interface de configuration du module en mode *Basique* et propose une page synthétique qui récapitule l'essentiel des variables à configurer.

Il est démarré par défaut si aucun fichier de configuration n'a été trouvé.

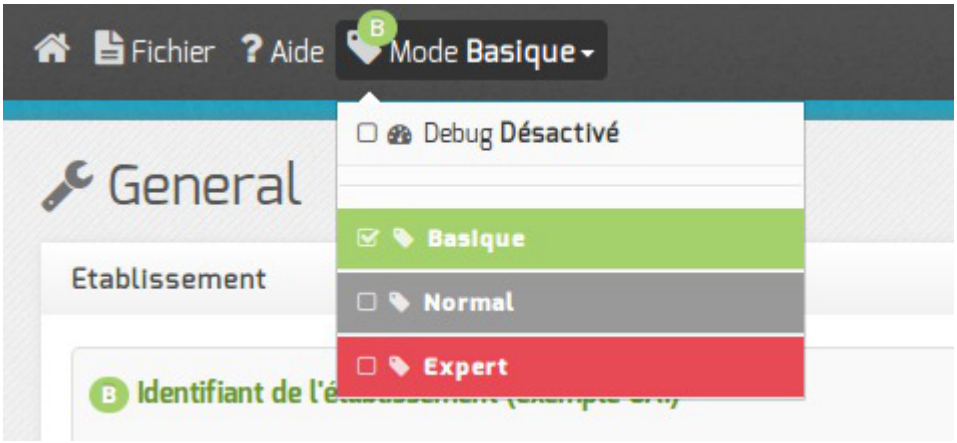
La légende présente un récapitulatif des différentes icônes que l'on peut rencontrer dans l'interface.

Sous-menu Mode

- Debug
- Basique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Normal
- Expert



Sous menu Mode

Le mode *Debug* permet d'afficher le nom des variables utilisées dans les dictionnaires (en rouge à droite du libellé). Le mode Debug est cumulable avec chacun des autres modes.

Le mode *Basique* n'affiche que les onglets et variables indispensables permettant une configuration rapide du module, il est le mode par défaut.

Le mode *Normal* active les onglets et les variables pour une configuration personnalisée du module.

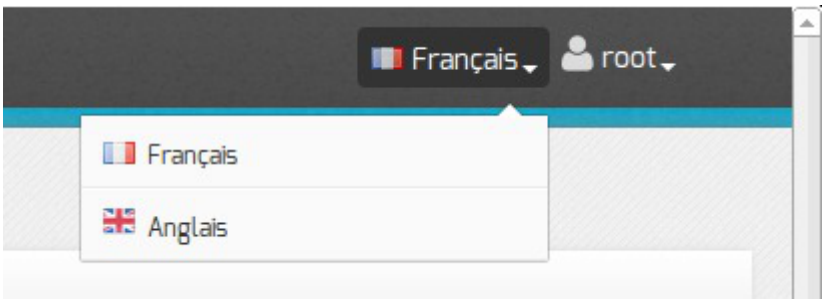
Le mode *Expert* active les onglets et les variables pour une configuration avancée.

Ce mode demande une très bonne maîtrise du système GNU/Linux et de ses composants.

Par exemple, pour le module Amon, l'activation du mode expert fait apparaître les onglets *Filtrage web*, *Proxy parent*, *Squid*, *Zone-dns*, ...).

Sous-menu Langue

- Français
- Anglais

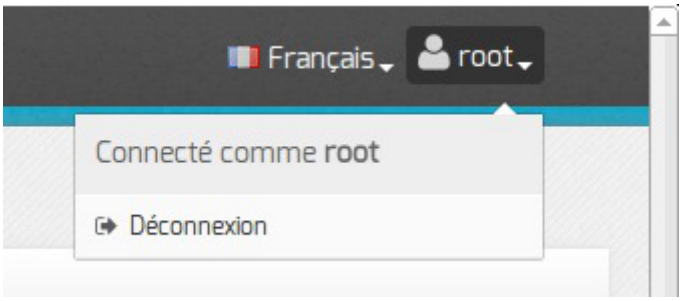


Langue permet de choisir la langue utilisé dans l'interface.

Sous-menu Session

- Connecté comme
- Déconnexion

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Session permet de connaître l'utilisateur courant et de se déconnecter.

1.1.3. La zone Onglet

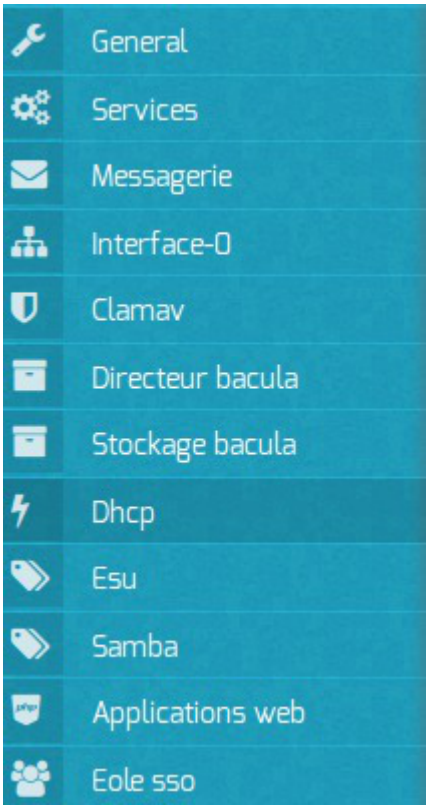
La zone Onglet, côté gauche de l'interface, présente des onglets de trois types :

- **les onglets de base** sont systématiquement présents au lancement de l'outil `gen_config` ;
- **les onglets optionnels** s'affichent si un paramètre du formulaire est activé.

  Exemple : si dans l'onglet `Services` le paramètre `Activer DHCP` est passé à `oui`, l'onglet `Dhcp` s'affiche dynamiquement au même niveau que les onglets de base ;
- **les onglets experts** correspondent essentiellement au paramétrage de fichiers de configuration d'outils spécifiques.

  Ils sont disponibles si le mode *Expert* est activé.

L'onglet en cours est en sous-brillance, dans l'image ci-dessous l'onglet `Dhcp` est actif.



L'onglet courant

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.1.4. La zone Formulaire

La zone Formulaire est la partie centrale de l'interface. Elle regroupe les paramètres de l'onglet activé.

Le bouton Modifier ou un clic dans le champ de saisie permet de modifier la valeur.

La modification de la valeur affiche deux boutons supplémentaires permettant l'annulation des modifications (pictogramme en forme de croix) et l'autre la réinitialisation de la valeur par défaut (pictogramme en forme de flèche tournant dans le sens anti-horaire).



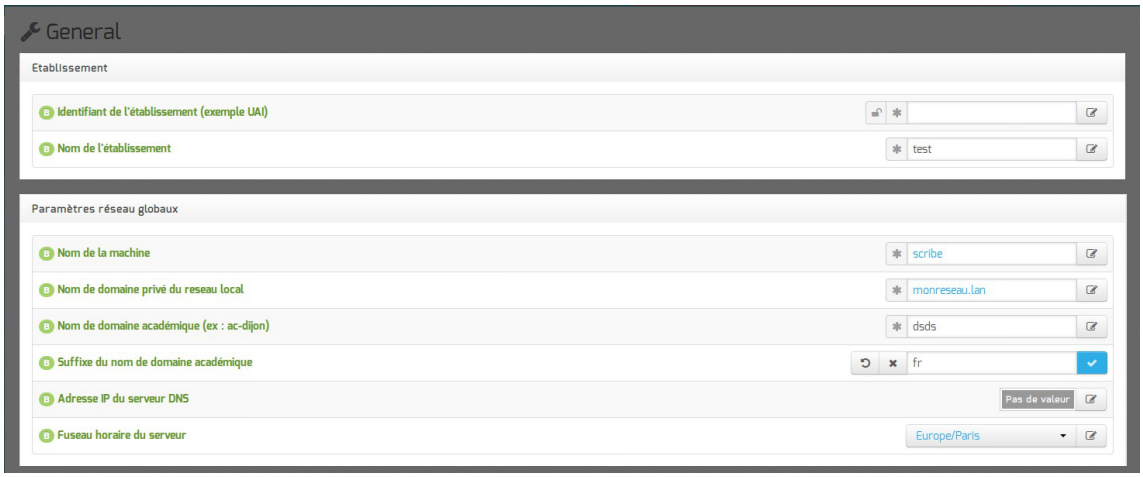
Bouton modifier sur la première ligne à droite, la deuxième ligne a le focus

La légende de chaque icône se trouve dans l'aide de l'interface : Aide / Légende.

Regroupement des paramètres par bloc

Les paramètres de chaque onglet sont répartis dans des blocs thématiques.

Chaque bloc regroupe un ou plusieurs paramètres.

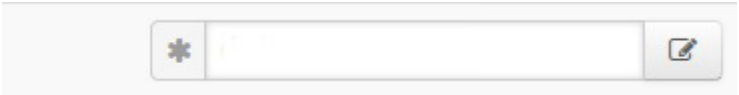


Les blocs thématiques

Les variables obligatoires

Les variables obligatoires sont des variables pour lesquelles il est nécessaire de spécifier une valeur, sans quoi il sera impossible d'enregistrer le fichier de configuration.

Les variables obligatoires se distinguent à l'aide du pictogramme en forme d'étoile placé devant le champ.



Les variables obligatoires sont précédées d'une étoile

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les variables des modes basiques, normales et expertes

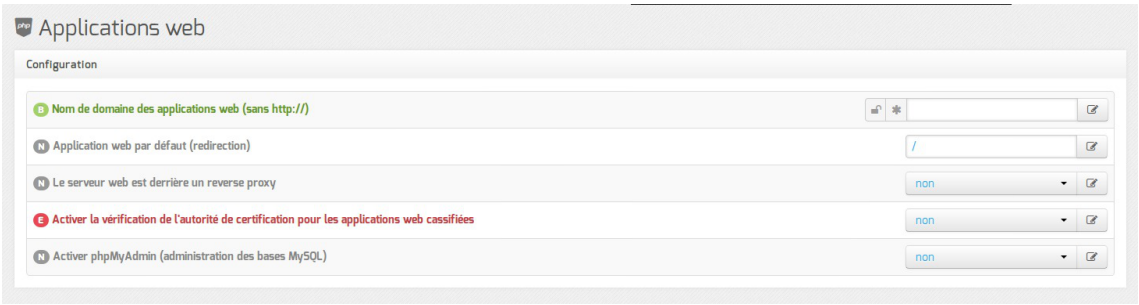
Le mode détermine l'affiche de variable plus ou moins complexes : basiques, normales ou expertes.

Lorsque l'on passe d'un mode à l'autre, un ensemble de nouvelles variables peuvent apparaître ou disparaître de l'interface.

Ces variables sont identifiables grâce au pictogramme `B`, `N` ou `E` qui précède l'étiquette de la variable.

Un code couleur est également utilisé pour le pictogramme et le libellé :

- vert pour basique ;
- gris pour normale ;
- rouge pour experte.

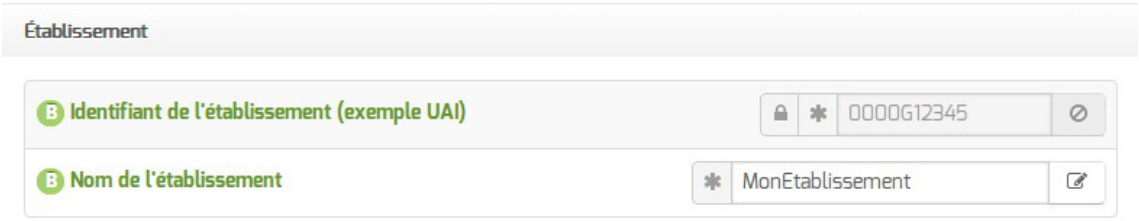


Les variables et leur niveau de complexité

Les variables simples

La valeur des variables simples s'affiche en couleur sur fond blanc :

- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée ;
- gris pour une variable verrouillée (dans le cas d'une ré-édition de la configuration après instanciation du module).



Les variables multiples

Certains paramétrages peuvent accueillir plusieurs valeurs, nous parlons alors de variable multiple.

Les variables multiples se présentent sur fond coloré :

- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée ;
- gris pour une variable sans valeur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Apparence graphique des variables multiples

Pour ajouter une valeur, il faut cliquer sur modifier pour faire apparaître le champ de saisie.

Pour supprimer une valeur, il faut d'abord cliquer sur modifier puis sur la croix à droite du champ.



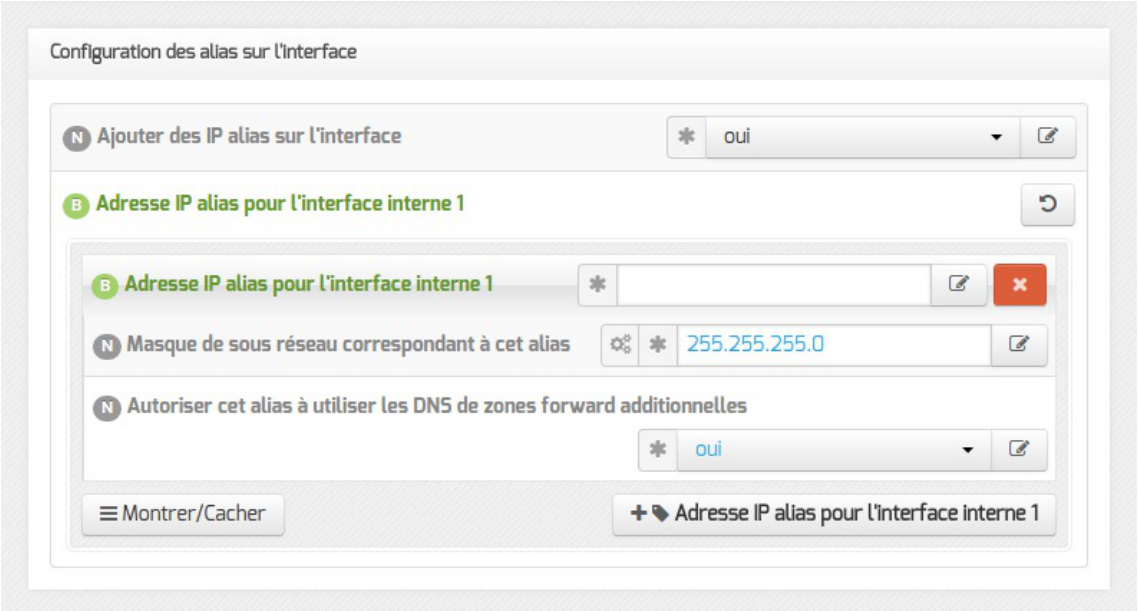
Édition d'une variable multiple

Les variables multiples groupées

Certains groupes de variables réunies au sein d'un même cartouche peuvent accueillir plusieurs valeurs, nous parlons alors de variable multiple groupée.

Les variables multiples groupées se présentent sur fond blanc dont la valeur s'affiche en couleur :

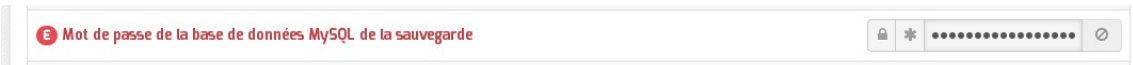
- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée.



Les variables brouillées

Certaines variables sensibles ont un affichage brouillé dès lors qu'elles sont validées. Le contenu de la variable est remplacé par une série de points.

Ces variables sont de nouveau visibles lorsqu'elles sont éditées.



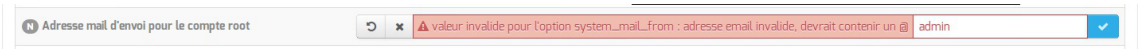
Validation des variables

Suivant les variables, il est possible que des validations soient faites.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Si la valeur ne correspond pas aux critères de validation de l'interface de configuration du module, un message d'erreur avertira l'utilisateur.

Il existe de nombreux critères de validation : le type de valeur, leur construction (séparateur), etc.



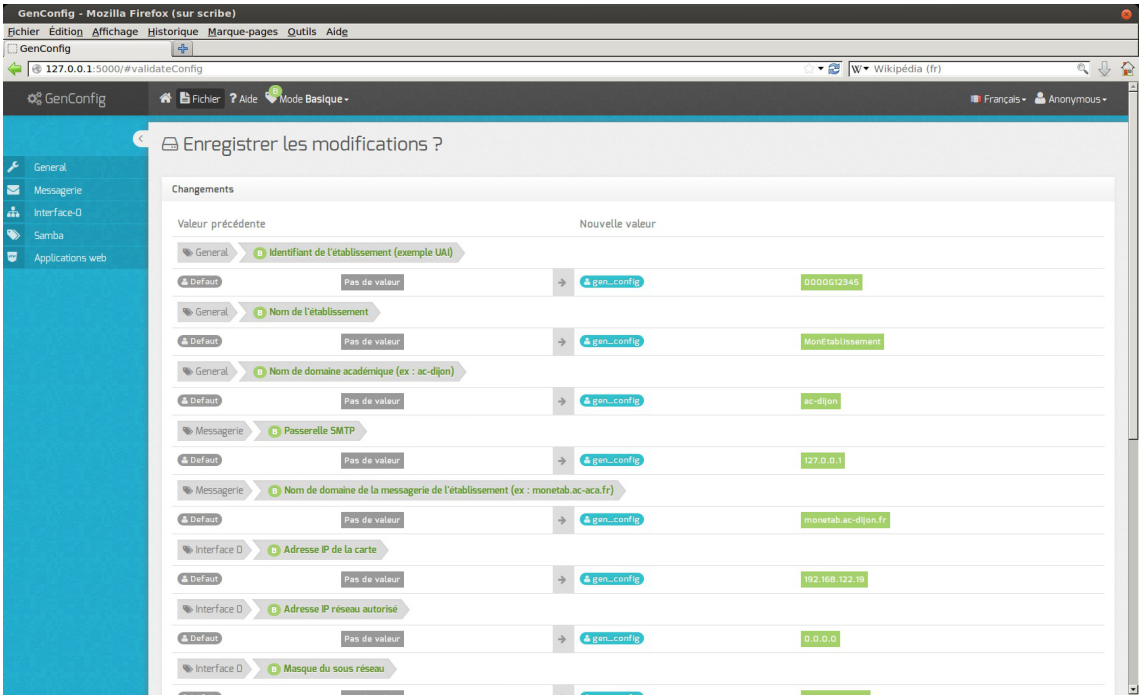
Validation d'une variable

1.1.5. La zone Validation

Cette zone est visible lors de l'enregistrement des modifications. Elle propose un récapitulatif des informations saisies.

Elle affiche également les variables obligatoires qui ne sont pas renseignées.

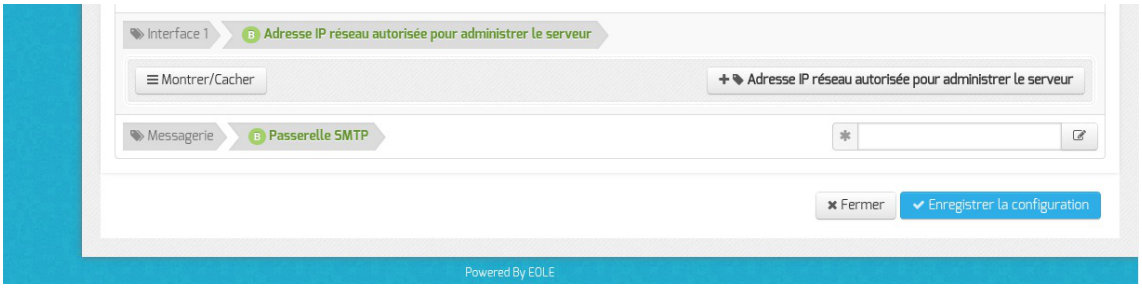
Lors d'une réédition de la configuration cette zone ne montre que les changements qui ont eu lieu.



Zone de validation

1.1.6. Enregistrer la configuration

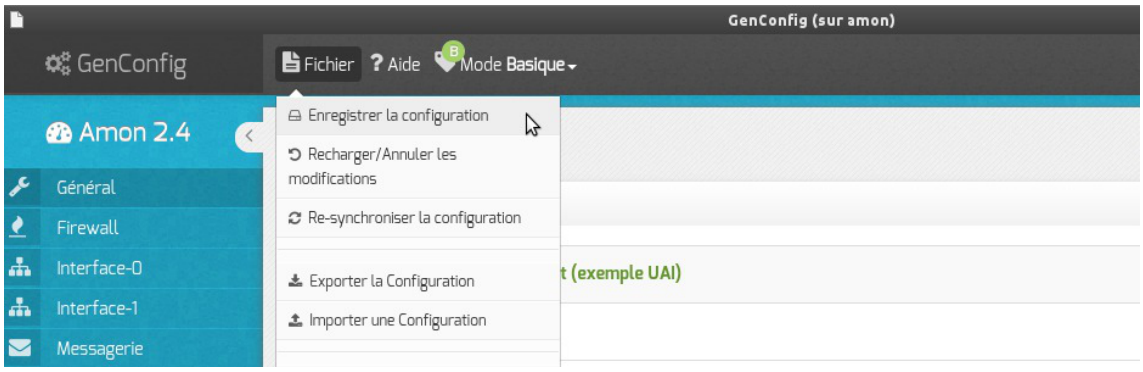
L'utilisation du mode assistant propose l'enregistrement de la configuration en bas de page avec le bouton Enregistrer la configuration.



Dans les autres cas l'enregistrement de la configuration se fait en cliquant sur Enregistrer la

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`configuration` dans le menu `Fichier`.



Une page récapitulative propose l'enregistrement de la configuration en bas de page avec le bouton `Enregistrer la configuration`.

Les différentes valeurs attribuées aux variables sont enregistrées dans un fichier `config.eol` au format JSON[p.463] dans le répertoire `/etc/eole/`.

Il convient donc de réaliser les modifications sur ce fichier en utilisant l'interface de configuration du module.



Un fichier `config.eol.bak` est sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

S'il existe une différence entre `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'a pas encore été appliquée.

L'utilisation de la nouvelle interface de configuration du module sur une petite configuration peut poser problème.

Cela se traduit par des erreurs de timeout[p.475] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Gunicorn[p.461].



La valeur de timeout peut être changée à la ligne `timeout = '120'` dans le fichier de configuration de eoleflask : `/etc/eole/flask/eoleflask.conf`. Celui-ci n'est pas templatisé et n'est donc pas écrasé en cas de reconfiguration du serveur.

Le changement de valeur doit être suivi d'une relance du service eoleflask :

```
# CreoleService eoleflask restart
```

1.1.7. Le mode Debug

Dans la zone de Menu le sous-menu Mode propose le mode Debug.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le mode *Debug* permet d'afficher le nom des variables utilisées dans les dictionnaires (en rouge à droite du libellé).



Les valeurs des variables peuvent être modifiées par différentes applications.

En gris, à droite du nom de la variable, est précisé le nom de l'application et/ou de l'action ayant modifié en dernier sa valeur :

- `default` : valeur par défaut et/ou calculée (n'est jamais enregistrée dans le fichier `config.eol`) ;
- `forced` : valeur par défaut enregistrée d'office pour les variables à verrouillage automatique (**auto_freeze**) ou à enregistrement obligatoire (**auto_save**) ;
- `gen_config` : valeur modifiée par l'interface de configuration du module ;
- `creoleset` : valeur modifiée avec la commande `CreoleSet` ;
- `zephir` : valeur modifiée pour un serveur donné dans l'interface web de Zéphir ;
- `variante` : valeur par défaut de la variante Zéphir ;
- `module` : valeur par défaut du module dans Zéphir ;
- `import` : valeur récupérée depuis un fichier de configuration importé dans l'interface de configuration du module ;
- `zephir_import` : valeur récupérée depuis un fichier de configuration importé dans l'interface web de Zéphir ;
- `upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE ;
- `zephir_upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE dans l'interface web de Zéphir.

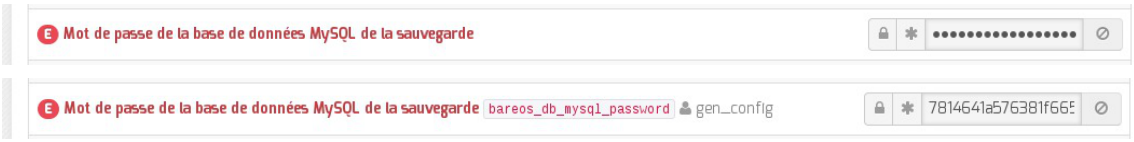
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette information est également enregistrée dans le fichier de configuration config.eol du module.

La clé associée à cette valeur est `owner` :

```
"numero_etab": {"owner": "gen_config", "val": "0000000A"}
```

Le mode *Debug* permet également d'afficher les valeurs des variables verrouillées de type *password*, dont l'affichage est normalement brouillé.



Lorsque le champ est trop petit par rapport à la valeur, celle-ci est tronquée. L'info-bulle qui s'affiche au survol du champ permet toutefois de prendre connaissance de la valeur complète.



Voir aussi...

La zone Menu [p.67]

1.1.8. FAQ

Certaines interrogations reviennent souvent et ont déjà trouvées une ou des réponses.



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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>/genconfig/`

ou : `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.eol.bak` est sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

S'il existe une différence entre `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'a pas encore été appliquée.

Comment modifier la valeur d'une variable verrouillée

Il est vivement recommandé de ne pas éditer manuellement le fichier `config.eol` pour éviter les erreurs de frappe ou de type de données.



Exporter puis importer le fichier de configuration courant permet de passer outre le verrouillage des variables.



Cette astuce demande une bonne maîtrise des implications que peut avoir le changement d'une valeur verrouillée. Et une valeur n'est jamais verrouillée sans raison.

Par exemple, le changement de l'identifiant de l'établissement ne se répercute pas sur l'annuaire dont le schéma n'est construit qu'une fois au moment de l'instance du serveur.



Pour modifier la valeur verrouillée `Identifiant de l'établissement` :

- ouvrir l'interface de configuration du module ;
- importer le fichier de configuration courant : `Fichier` → `Importer une Configuration` → `/etc/eole/config.eol` ;
- modifier la valeur de l'identifiant de l'établissement ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- enregistrer la configuration : `Fichier` → `Enregistrer la configuration` ;
- procéder à une reconfiguration du serveur à l'aide de la commande `reconfigure`.

Erreurs de timeout ou erreur 504 avec Nginx

L'utilisation de la nouvelle interface de configuration du module sur une petite configuration peut poser problème.

Cela se traduit par des erreurs de timeout[p.475] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Gunicorn[p.461].



La valeur de timeout peut être changée à la ligne `timeout = '120'` dans le fichier de configuration de eoleflask : `/etc/eole/flask/eoleflask.conf`. Celui-ci n'est pas templatisé et n'est donc pas écrasé en cas de reconfiguration du serveur.

Le changement de valeur doit être suivi d'une relance du service eoleflask :

```
# CreoleService eoleflask restart
```

Interface de configuration en mode console

Impossible de trouver le mode console de l'interface de configuration du module.



Le mode console a été supprimé par contre il est possible :

- d'accéder à distance à l'interface de configuration du module via un navigateur web ;
- d'utiliser la commande CreoleSet pour configurer une variable en ligne de commande.

Consultation des mots de passe dans l'interface de configuration

Sur les versions d'EOLE supérieures à 2.6.0, les valeurs des variables de type *password* sont masquées lorsque le champ n'est pas en mode édition, donc inaccessibles lorsque le champ est verrouillé.



La consultation d'un mot de passe non éditable (stocké dans une variable verrouillée par exemple) est possible en passant en mode Debug. Le mot de passe pouvant malgré tout apparaître tronqué, sa valeur intégrale est accessible dans l'info-bulle qui s'affiche lors du survol du champ.

1.2. Configuration en mode Zéphir

La configuration en mode Zéphir permet, au lancement de l'interface de configuration du module à l'aide de la commande `gen_config`, de faire apparaître un fenêtre d'identification qui permet de s'identifier avec un compte Zéphir. Les modifications apportées dans la configuration locale seront synchronisées avec le serveur Zéphir.

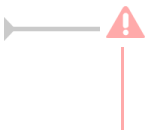
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La configuration en mode Zéphir se fait en deux étapes :

- configuration :
  - soit sur le serveur à enregistrer
  - soit sur le serveur Zéphir (utilisation éventuelle de variantes)
- enregistrement du serveur et synchronisation de la configuration.

Pré-requis

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



La procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

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`.

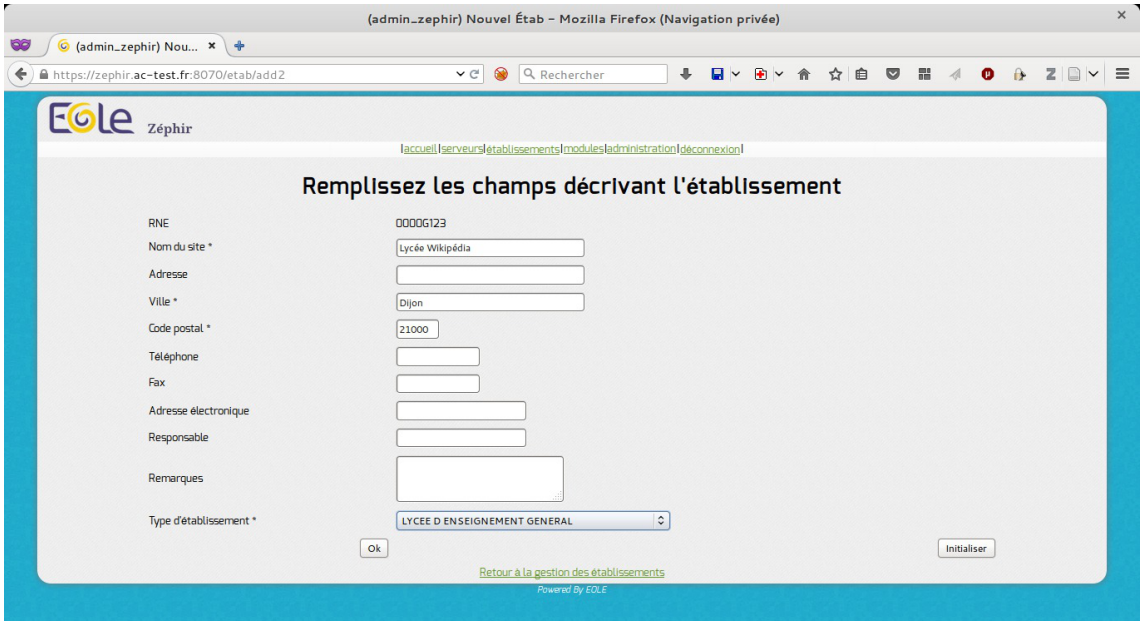


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese[p.470]) CSV[p.457] 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 d'un serveur

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.



Dans le cas d'utilisation de certificats non reconnus par une autorité de certification la procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

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

- lancer la procédure d'enregistrement à l'aide de la commande `enregistrement_zephir` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 ;
- dans le cas d'utilisation de certificats non reconnus par une autorité de certification, il faut, pour procéder à l'enregistrement d'un serveur, copier le certificat de la CA locale du serveur Zéphir `/etc/ssl/certs/ca_local.crt` sur la machine à enregistrer dans le répertoire `/usr/local/share/ca-certificates/` et mettre à jour les certificats sur la machine locale à l'aide de la commande `update-ca-certificates` ;
- relancer la procédure d'enregistrement avec la commande `enregistrement_zephir` ;
- 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.

Certificat de Zéphir non validé !

 utiliser sur Zéphir un certificat signé par une autorité reconnue,
  ou
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
 Copier le fichier /etc/ssl/certs/ca_local.crt de Zéphir dans
 /usr/local/share/ca-certificates et lancer update-ca-certificates.
root@eolebase:~#

root@eolebase:~# scp root@zephir.ac-test.fr:/etc/ssl/certs/ca_local.crt
/usr/local/share/ca-certificates/
Warning: Permanently added 'zephir.ac-test.fr,192.168.0.20' (ECDSA) to the
list of known hosts.
root@zephir.ac-test.fr's password:
ca_local.crt
100% 1736     1.7KB/s   00:00
root@eolebase:~#

root@eolebase:~# update-ca-certificates
Updating certificates in /etc/ssl/certs...
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate ca.crt
WARNING: Skipping duplicate certificate ca.crt
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
root@eolebase:~#

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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.

Lancement de l'interface de configuration

Une fois la procédure terminée, exécuter l'interface de configuration du module à l'aide de la commande `gen_config`.

Lors de l'accès à l'interface d'administration d'un module enregistré sur un serveur Zéphir, la mire d'authentification permet d'ouvrir une session avec un compte utilisateur Zéphir ou un compte local.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Désinscription d'un serveur

Pour désinscrire un serveur il faut exécuter la commande `enregistrement_zephir` et la désinscription est proposée.

```
root@eolebase:~# enregistrement_zephir

  Procédure d'enregistrement sur le serveur Zéphir


** Ce serveur est déjà enregistré sur le serveur Zéphir **

 - n°identifiant : 454
 - adresse de Zéphir : zephir.ac-test.fr

1 -> Désinscrire ce serveur du serveur Zéphir
2 -> Relancer l'enregistrement
3 -> Ne rien faire

  Entrez le numéro de votre choix : 1

Désinscription auprès du serveur Zéphir terminée

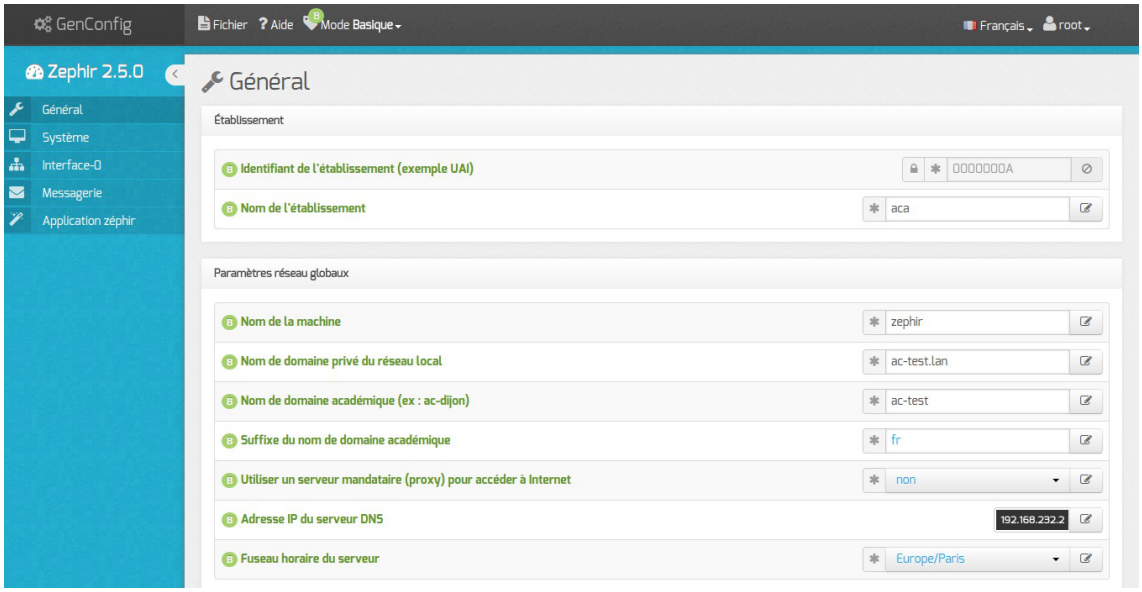
root@eolebase:~#
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. 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`.

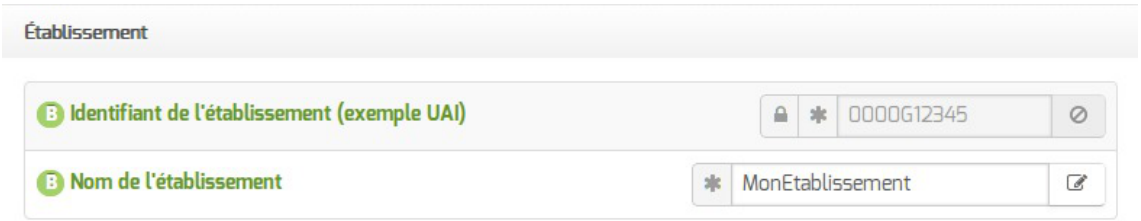


Vue générale de l'interface de configuration du module

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`.

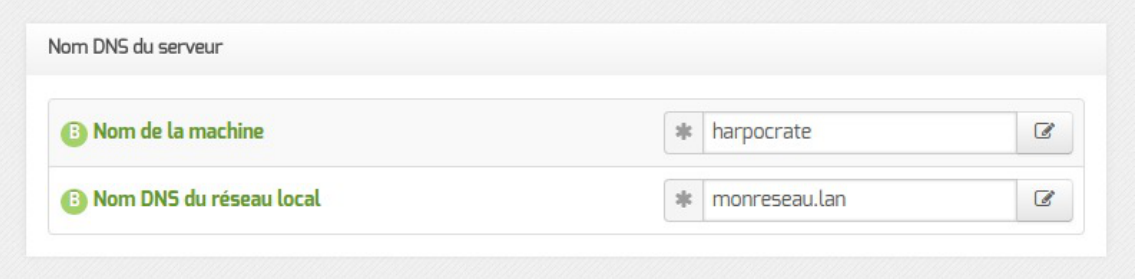
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.463] local, ces variables sont utilisées pour créer l'arborescence.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

Nom DNS du serveur



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Le `Nom DNS du serveur` 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 domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

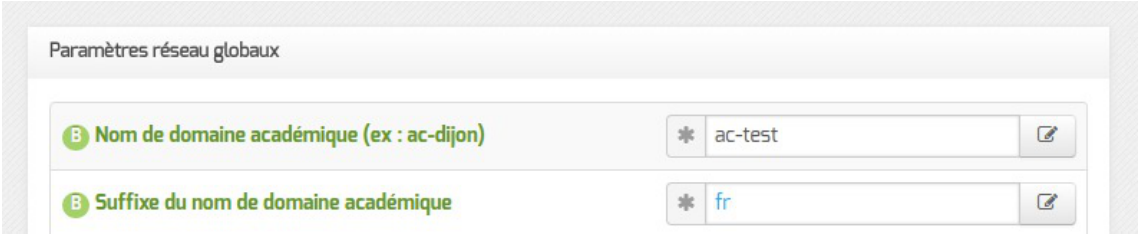
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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.

Paramètres réseau globaux

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Cette information est découpée en plusieurs champs :

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

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`.



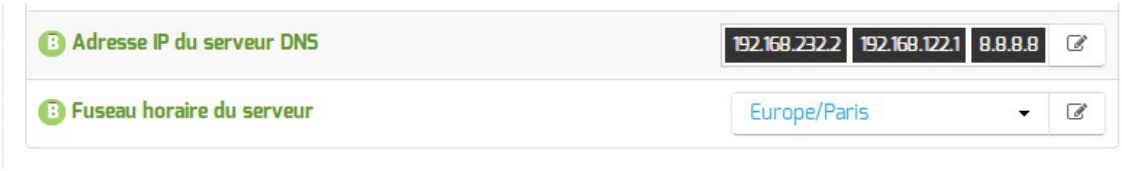
Il devient alors possible de saisir la configuration du serveur proxy :

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



La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait protégé par un module Amon.

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.458].

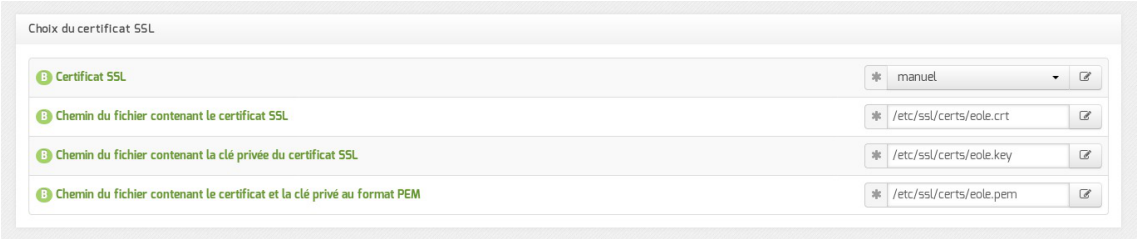
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

Choix du certificat SSL

Cette rubrique apparaît sur un module EOLE 2.6 dont la version est supérieure ou égale à 2.6.2.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Elle remplace l'ancienne rubrique `Types de certificats à utiliser` du même onglet en mode normal.



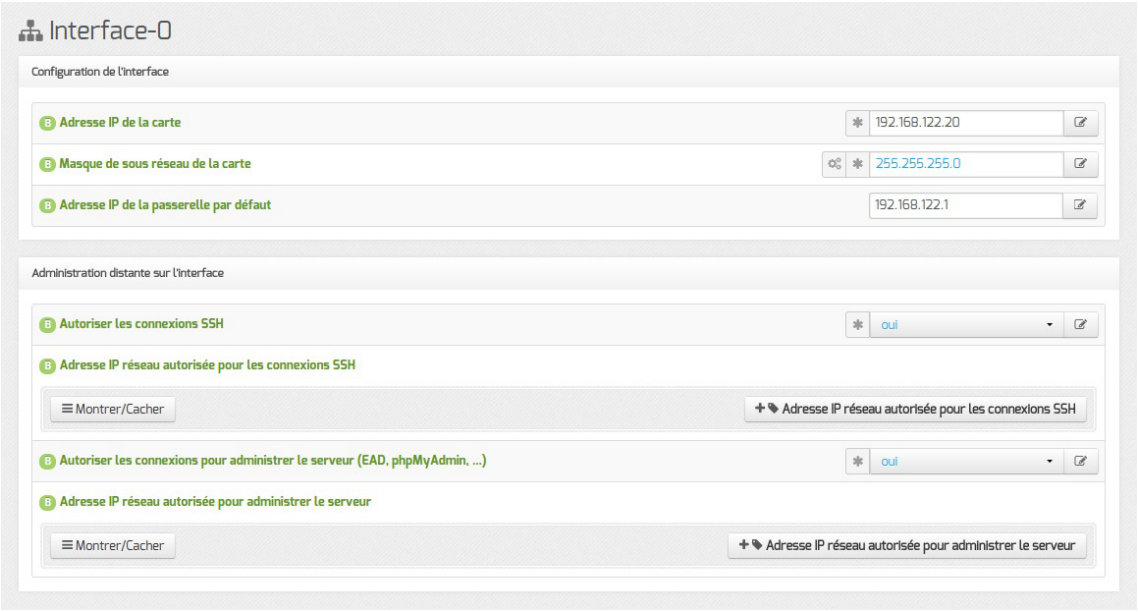
Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.475] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.454] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.463] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour se faire, il faut disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

> Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.
>
> Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

2.2. Onglet Interface-0

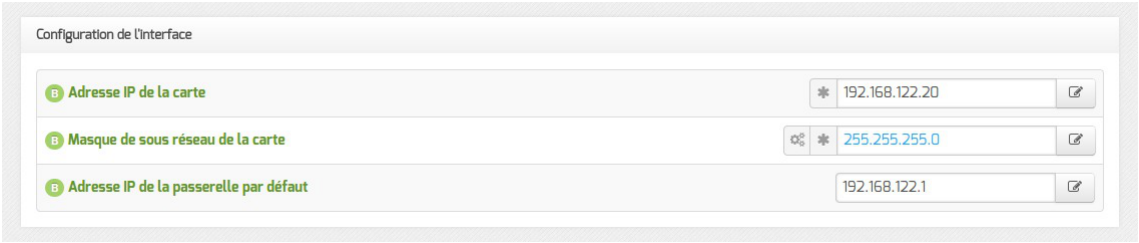
Présentation des différents paramètres de l'onglet `Interface-0`.



Vue de l'onglet Interface-n

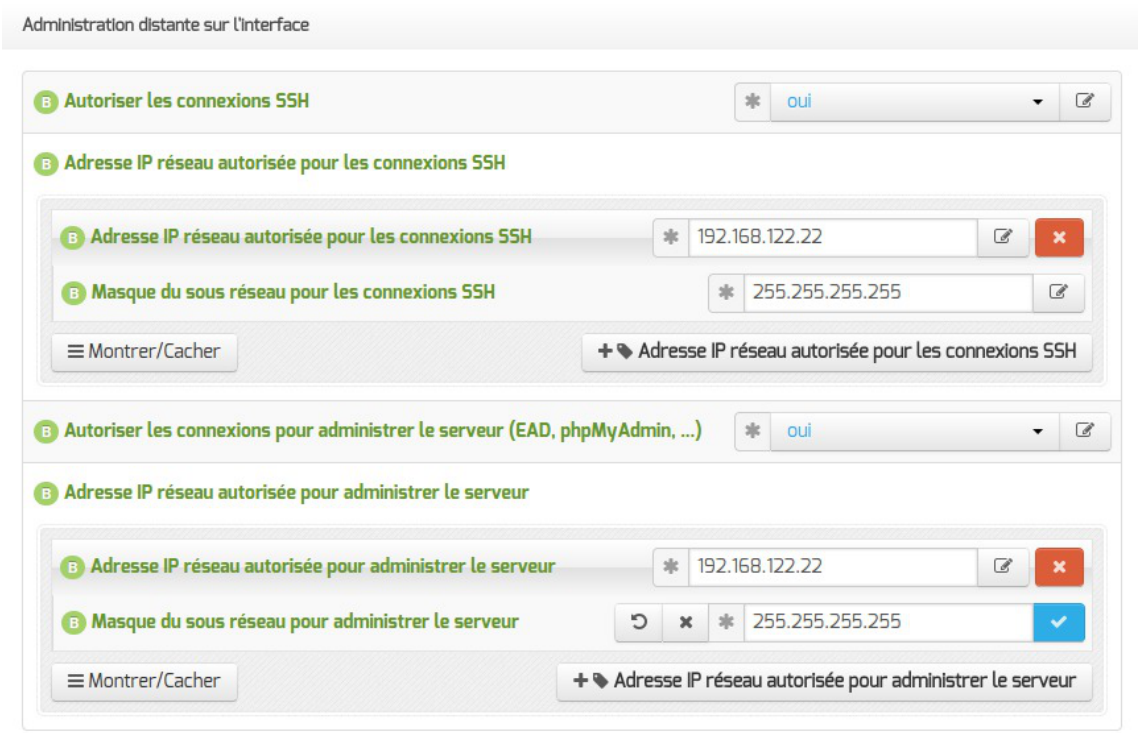
Configuration de l'interface

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Administration à distance



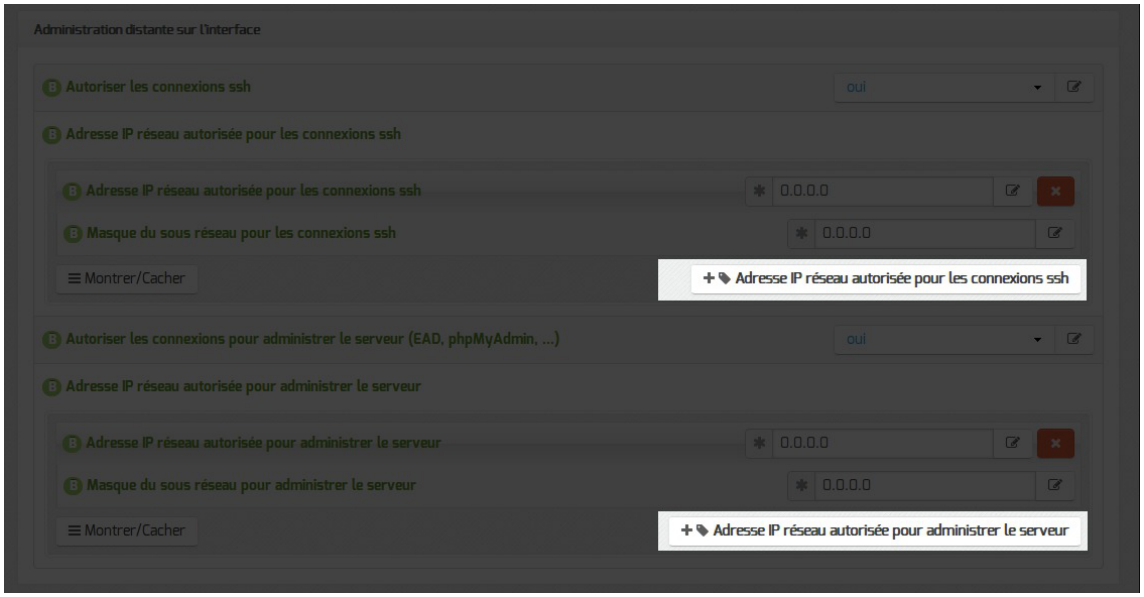
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.473] 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

2.3. 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 courriers électroniques.

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

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

Serveur d'envoi/réception (SMTP)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

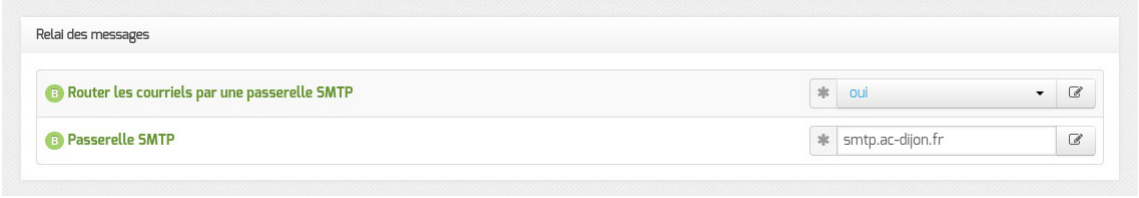


Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

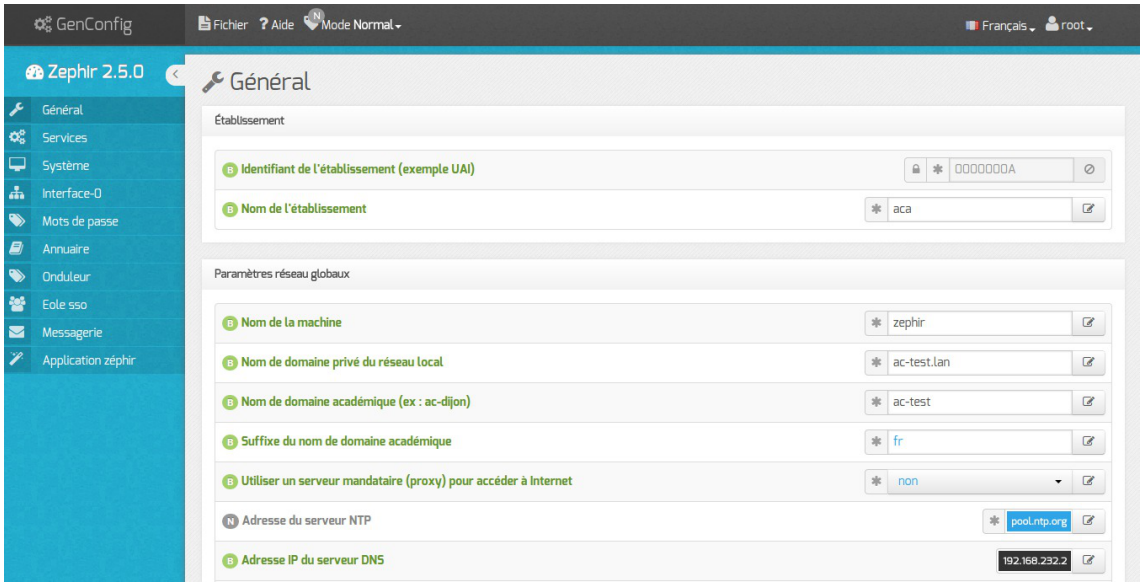
3. Configuration en mode normal

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 * ;
- Nginx ;
- Reverse proxy * ;
- Messagerie ;
- Application zéphir.

* Certains onglets ne sont visibles qu'après activation du service associé dans l'onglet Services.



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.

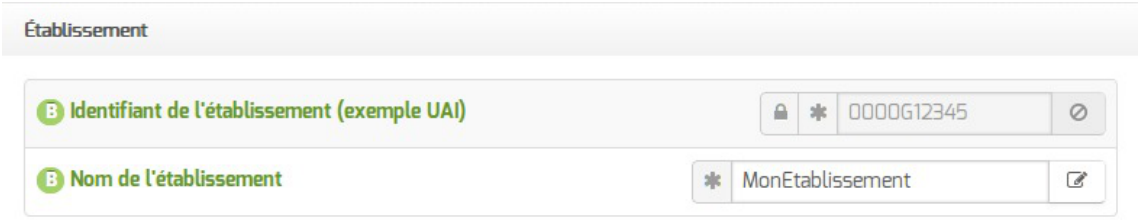
Il est cependant possible de spécifier un annuaire distant lors de la configuration du module (par exemple : l'annuaire d'un module Horus, l'annuaire d'un module Scribe, ou encore un annuaire académique). Vous pourrez alors vous connecter avec un compte de l'annuaire utilisé.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

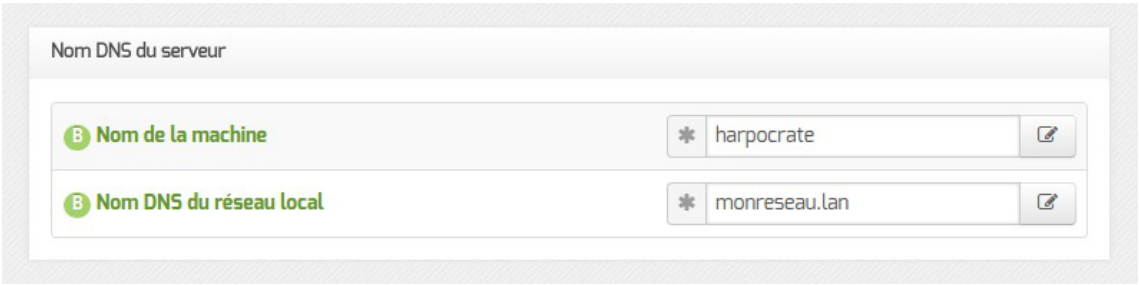
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.463] 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.

Nom DNS du serveur



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Le `Nom DNS du serveur` 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

résolution par défaut. Il sera utilisé par les machines pour résoudre l'ensemble des adresses locales.

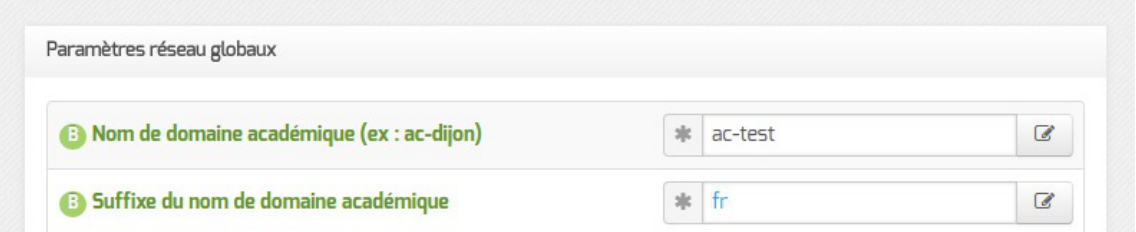
Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

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.

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.

Paramètres réseau globaux



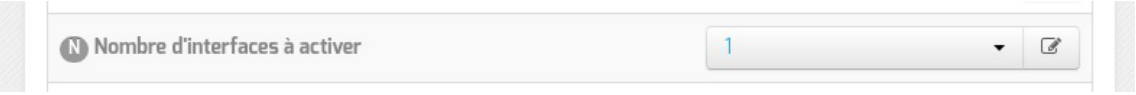
En deuxième lieu, il convient de configurer les noms de domaine de la machine.

Cette information est découpée en plusieurs champs :

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

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

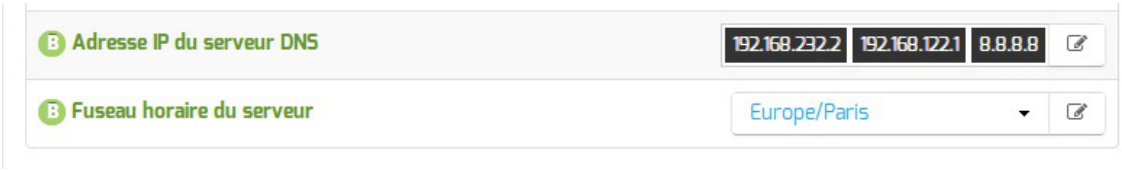


Il devient alors possible de saisir la configuration du serveur proxy :

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

> La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait protégé par un module Amon.

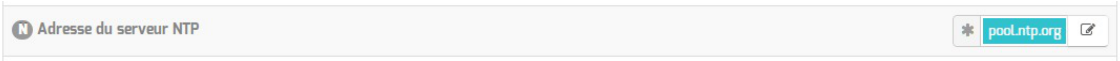
DNS et fuseau horaire



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.458].

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

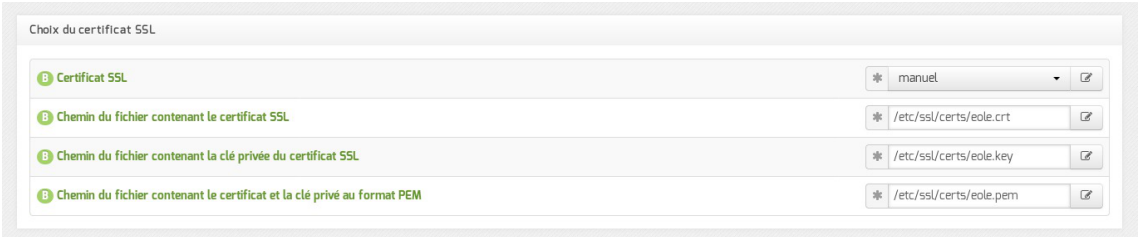
NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.467]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Choix du certificat SSL

> Cette rubrique apparaît sur un module EOLE 2.6 dont la version est supérieure ou égale à 2.6.2.
>
> Elle remplace l'ancienne rubrique `Types de certificats à utiliser` du même onglet en mode normal.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

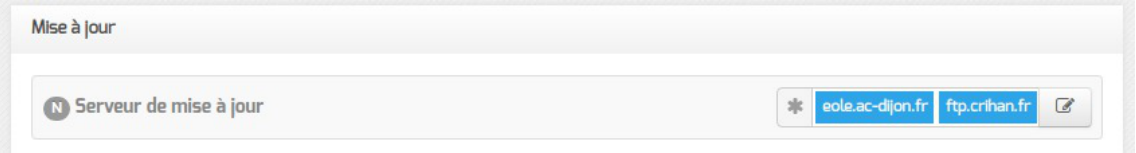
Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.475] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.454] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.463] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour se faire, il faut disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.

Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

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

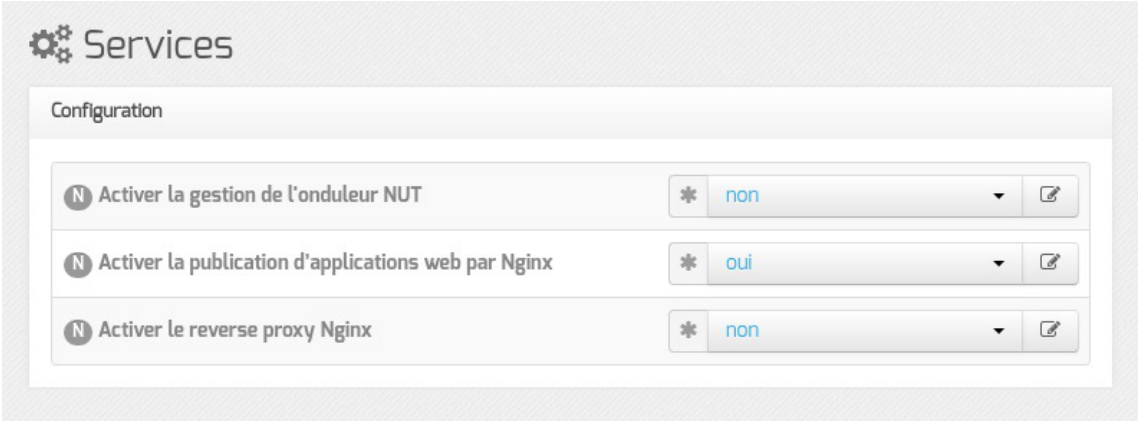
3.2. Onglet Services

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de l'onduleur Services en mode normal

Les services de base communs à tous les modules sont la gestion de l'onduleur NUT[p.467], l'activation d'applications web par Nginx et l'activation du proxy inverse.

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 :

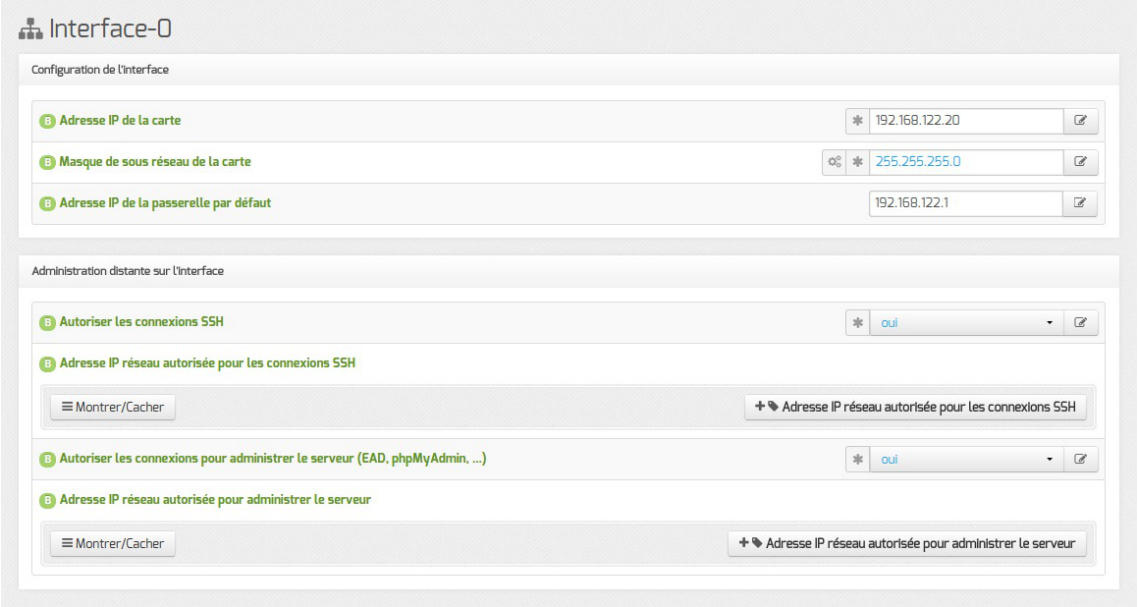
- le serveur LDAP ;
- le service d'authentification unique EoleSSO.

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

3.3. Onglet Interface-0

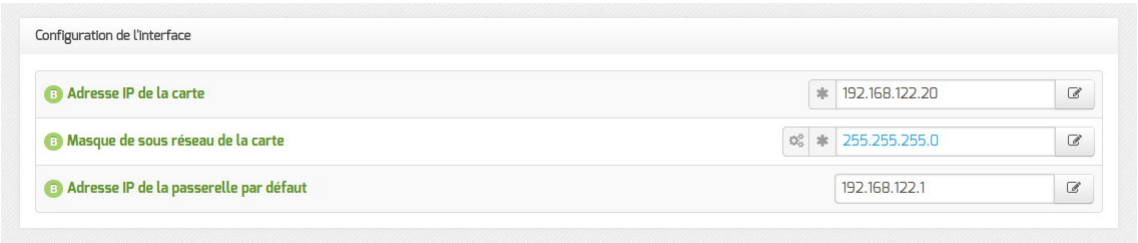
Présentation des différents paramètres de l'onglet `Interface-0`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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



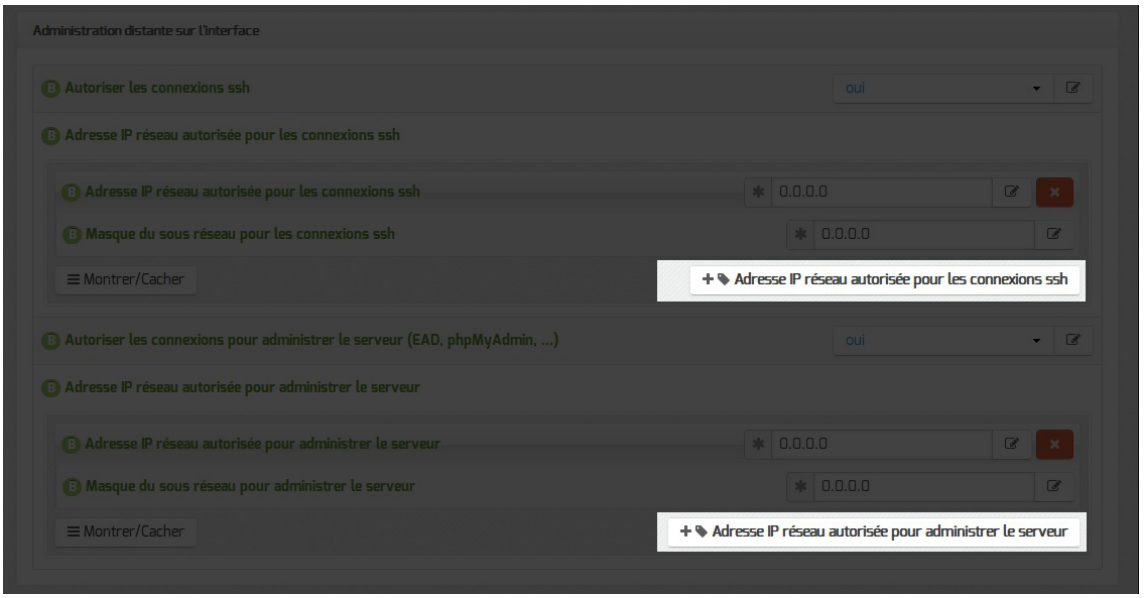
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.473] 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.

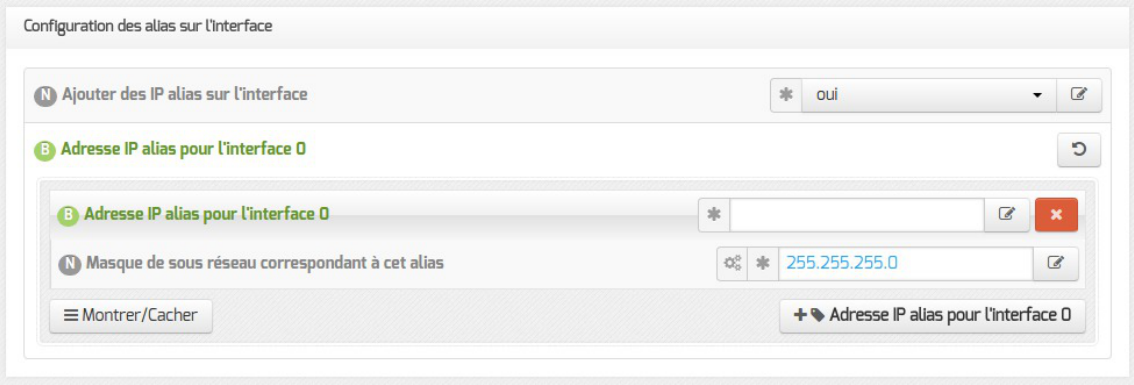
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



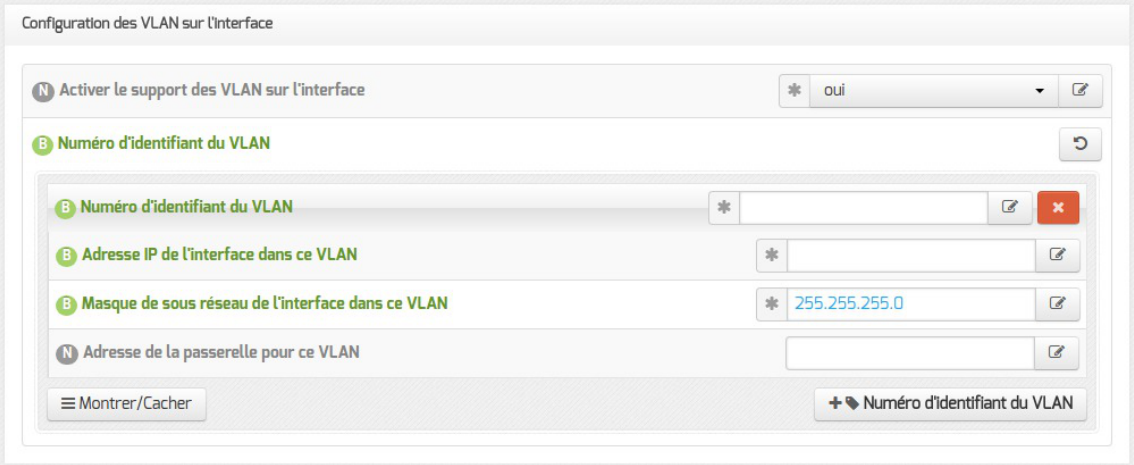
Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.



Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.476] (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.



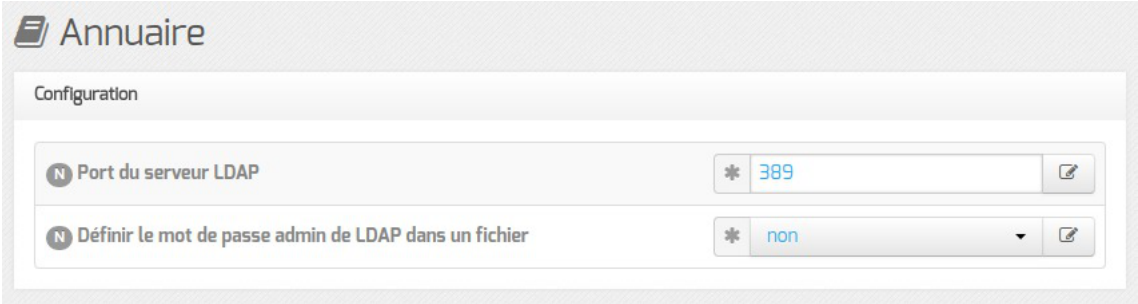
Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3.4. 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.

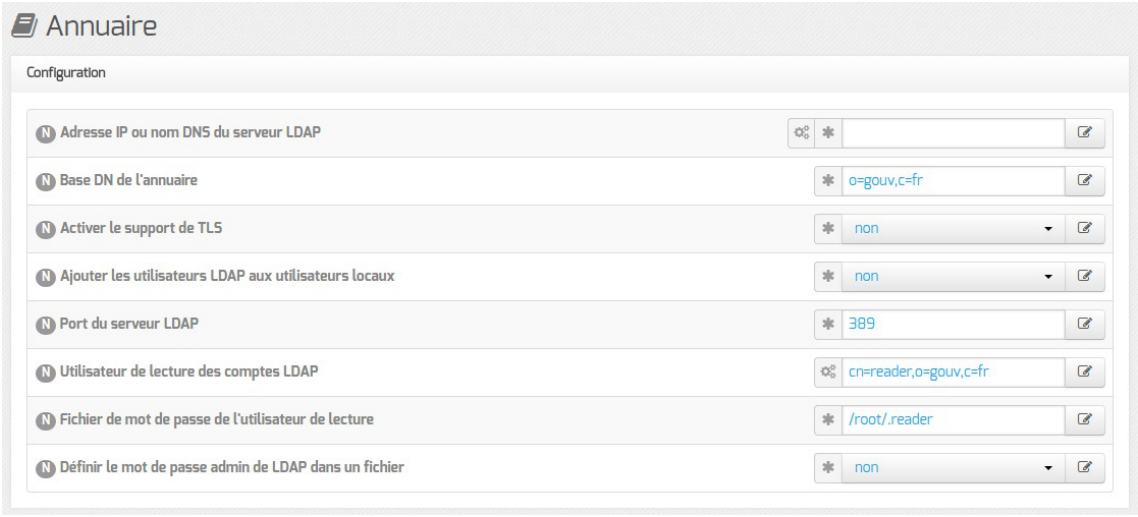
Annuaire LDAP local



Lorsque l'annuaire est configuré comme étant local, l'onglet propose plusieurs 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.475] 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

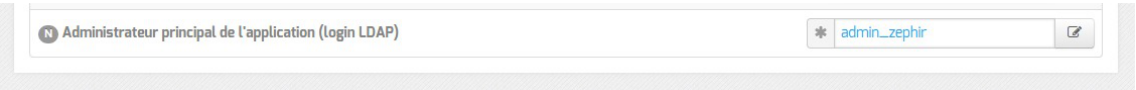


Lorsque l'annuaire est configuré comme étant distant, l'onglet propose plusieurs paramètres :

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `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.475] 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.

3.5. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.467]. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

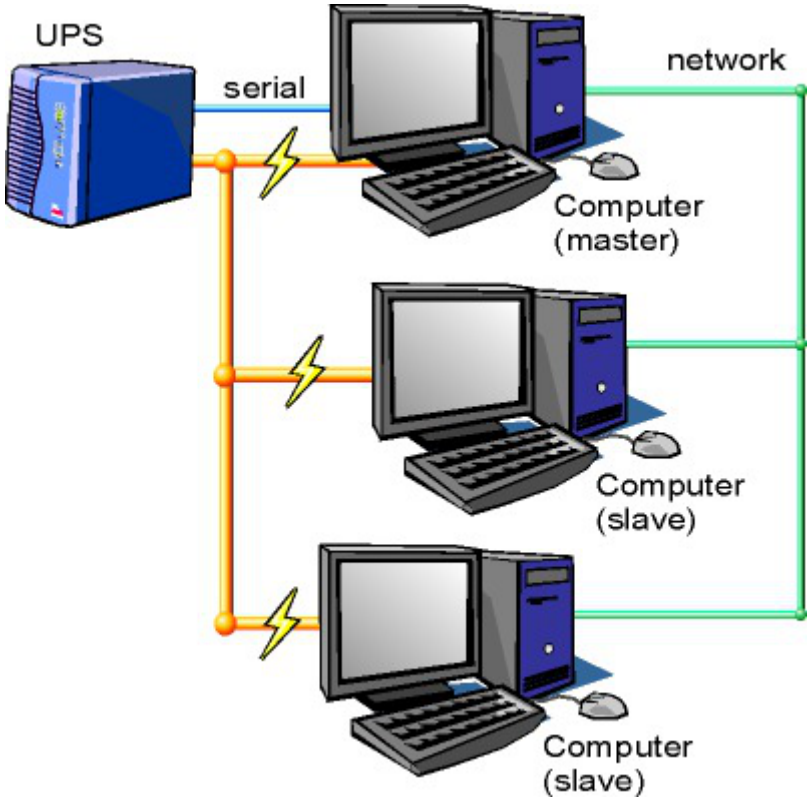


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

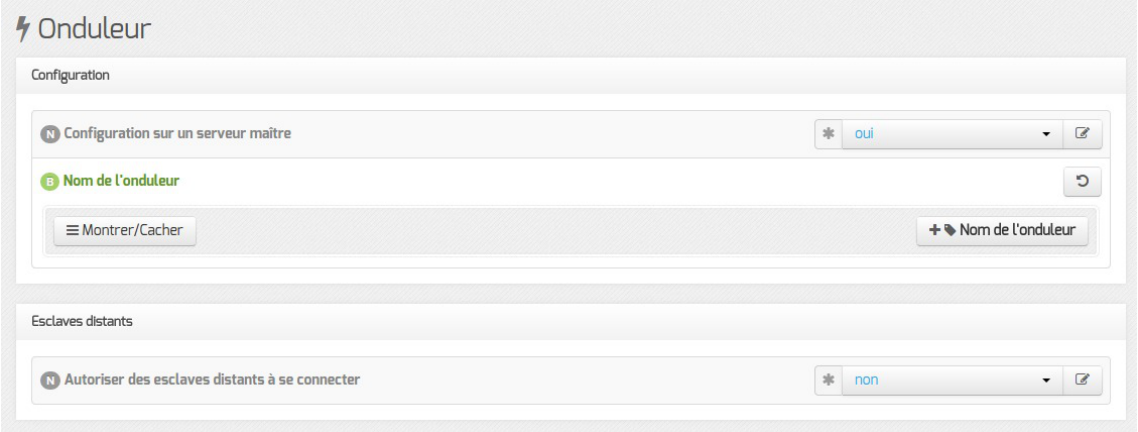
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

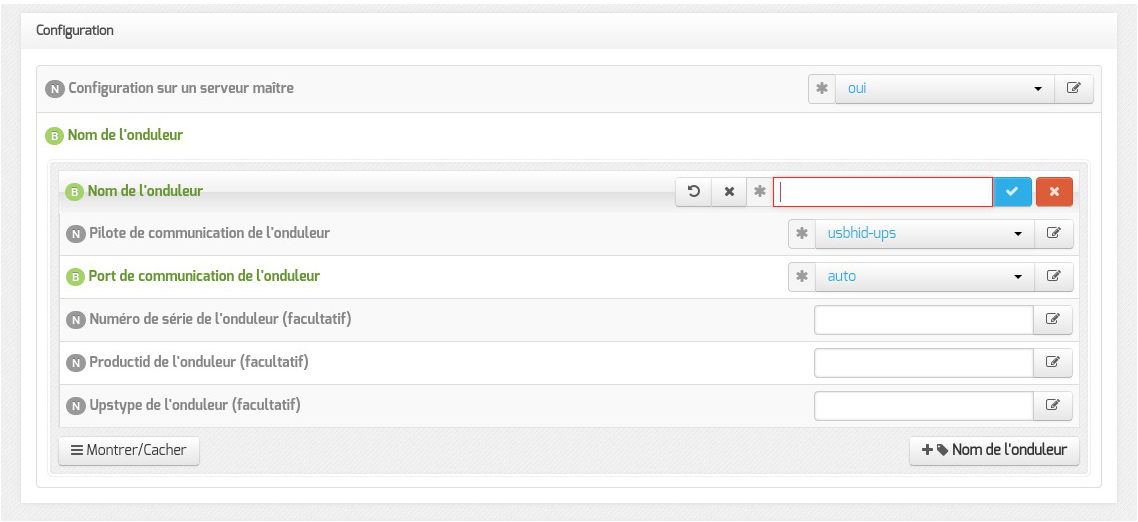
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

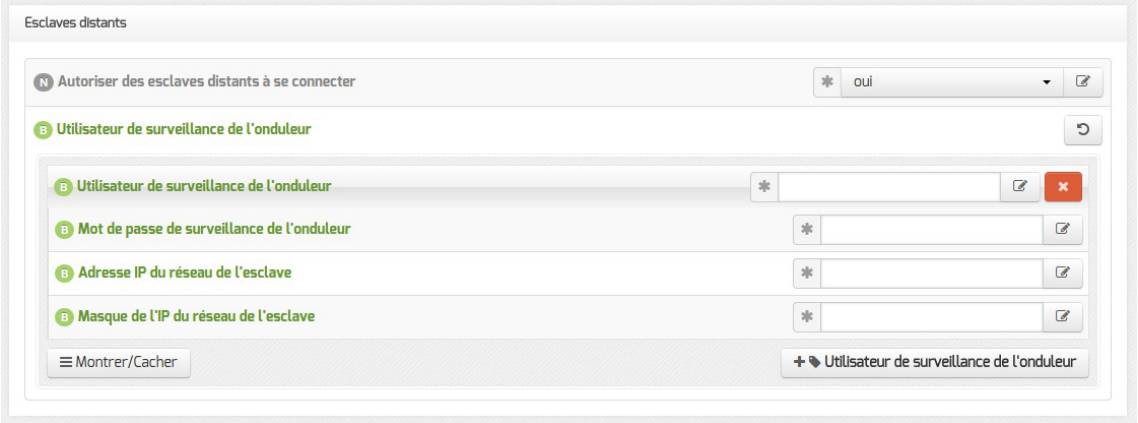
- Port de communication de l'onduleur : `auto`.

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`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/xenial/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` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

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

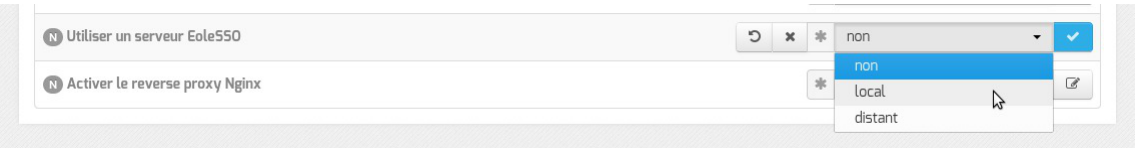
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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`.



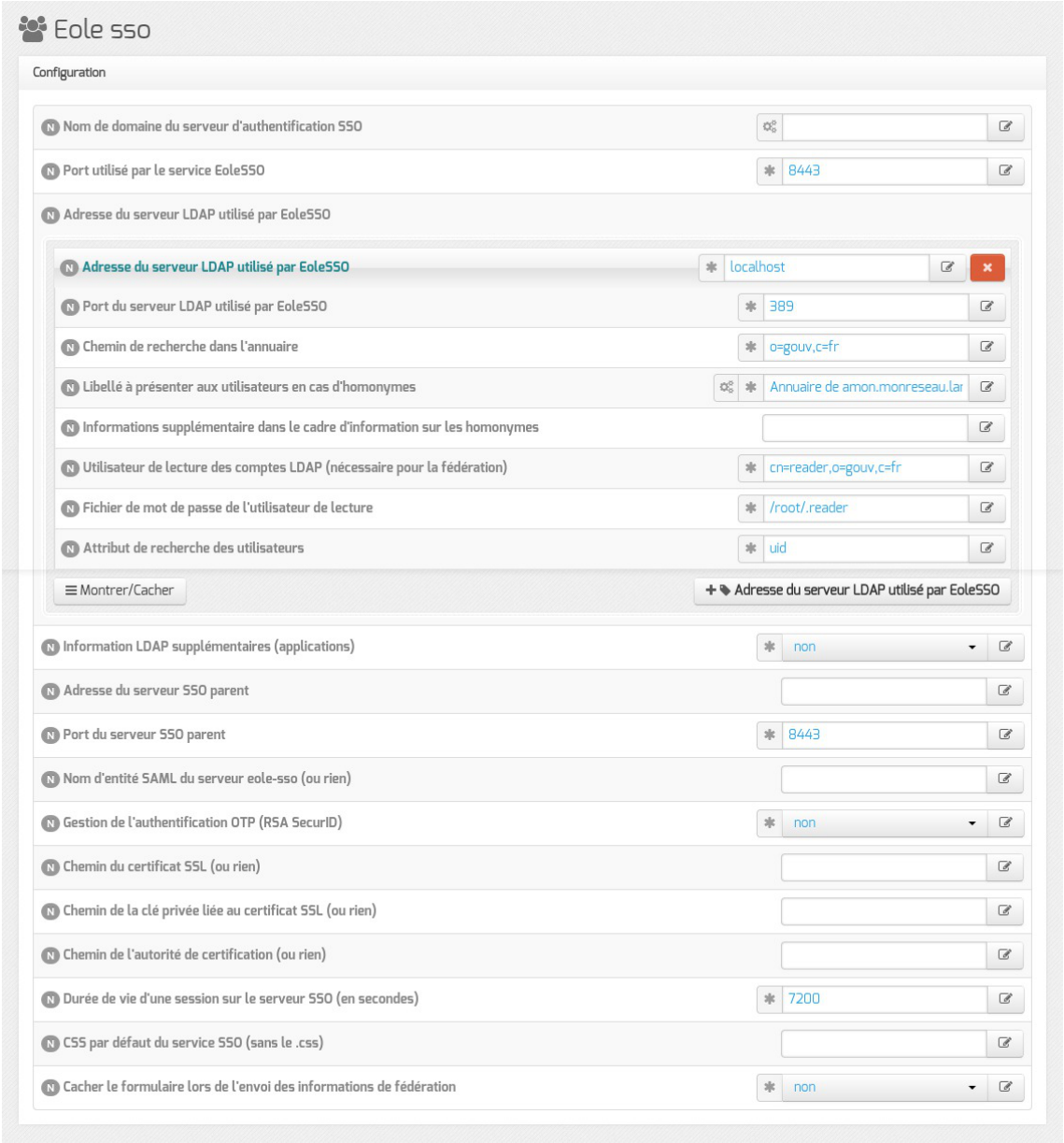
La variable `Utiliser un serveur EoleSSO` permet :

- `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

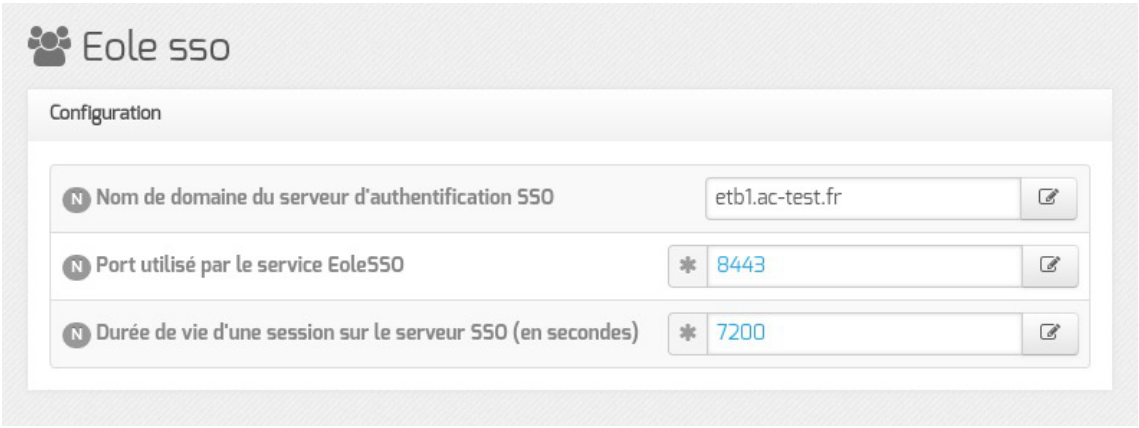
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Configuration d'un serveur EoleSSO local

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.



Configuration d'un serveur EoleSSO distant

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

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 modifier également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.463] 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 (basedn) ;
- 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[p.458] 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.468] 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 en tant que 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 s'effectue par l'intermédiaire d'appels XML-RPC[p.477] 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.472] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.462] 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.472] (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

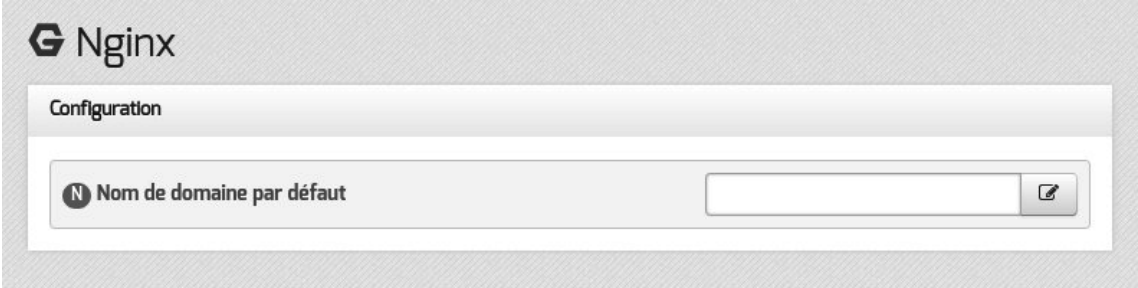
3.7. Onglet Nginx

L'onglet `Nginx` est disponible si au moins l'un des deux paramètres suivants est activé dans l'onglet `Services` :

- `Activer la publication d'applications web par Nginx` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Activer le reverse proxy Nginx`.



En mode normal, cet onglet permet de saisir permet de saisir le `Nom de domaine par défaut` vers lequel sera redirigé un client qui accède au serveur avec un nom de domaine non déclaré.

3.8. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.467].

Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ[p.457] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.473].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables*[p.462]*/DNAT*.

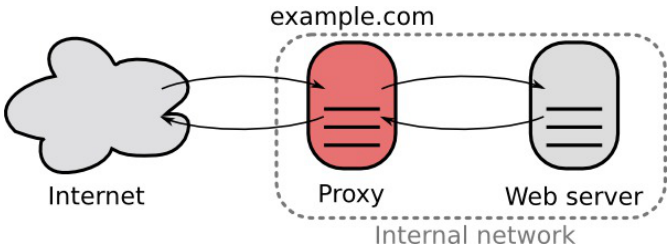
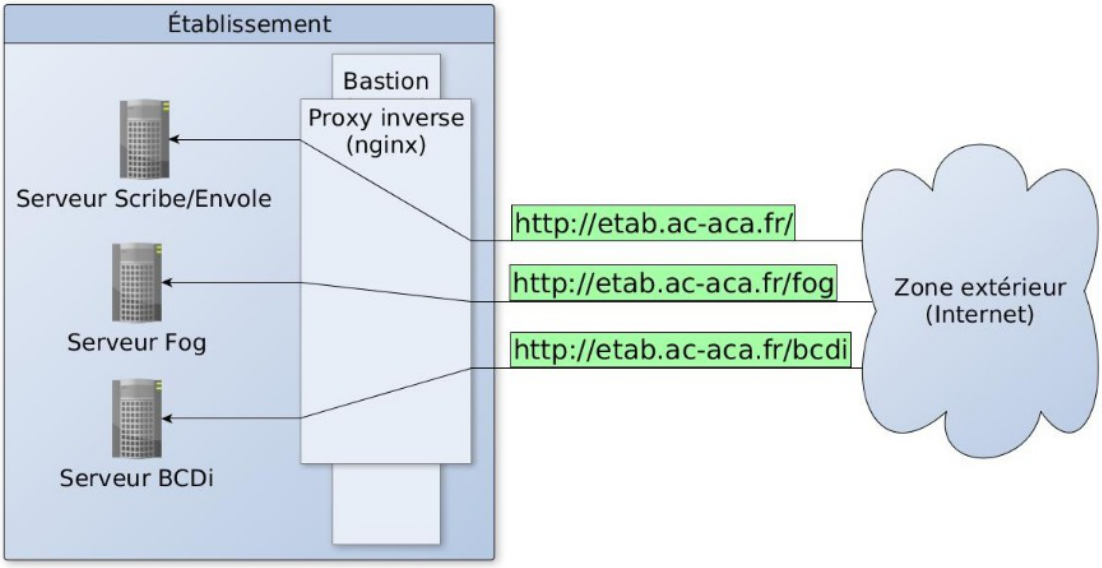


Diagramme d'un proxy inverse - Licence CC0

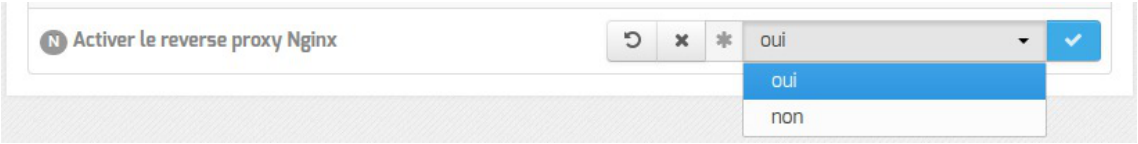
Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD[p.458] ;
- application EOP ;
- protocole HTTP[p.461] ;
- protocole HTTPS[p.461].

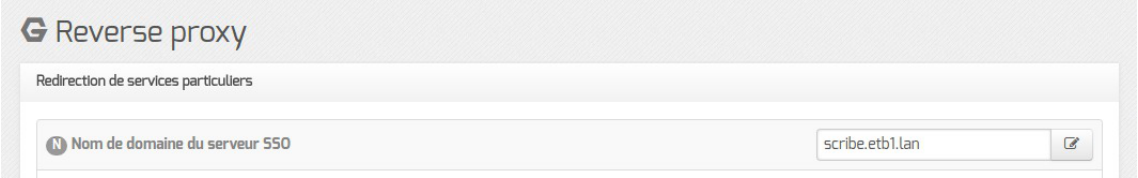
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Avant toute chose, le proxy inverse doit être activé dans l'onglet `Services` en passant `Activer le reverse proxy Nginx` à `oui`.

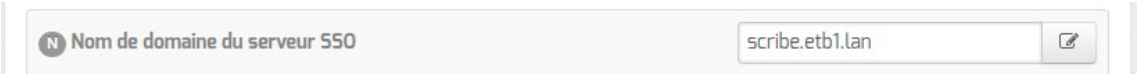


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

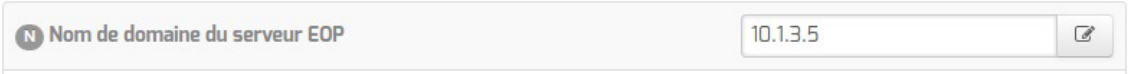
Redirection du service EoleSSO



Pour rediriger le service EoleSSO (port 8443), il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

Cette fonctionnalité n'est disponible que dans le cas ou le serveur EoleSSO n'est pas activé en local (`Utiliser un serveur EoleSSO` doit être différent de `local` dans l'onglet `Services`).

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.476]).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour rediriger l'application EOP, il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

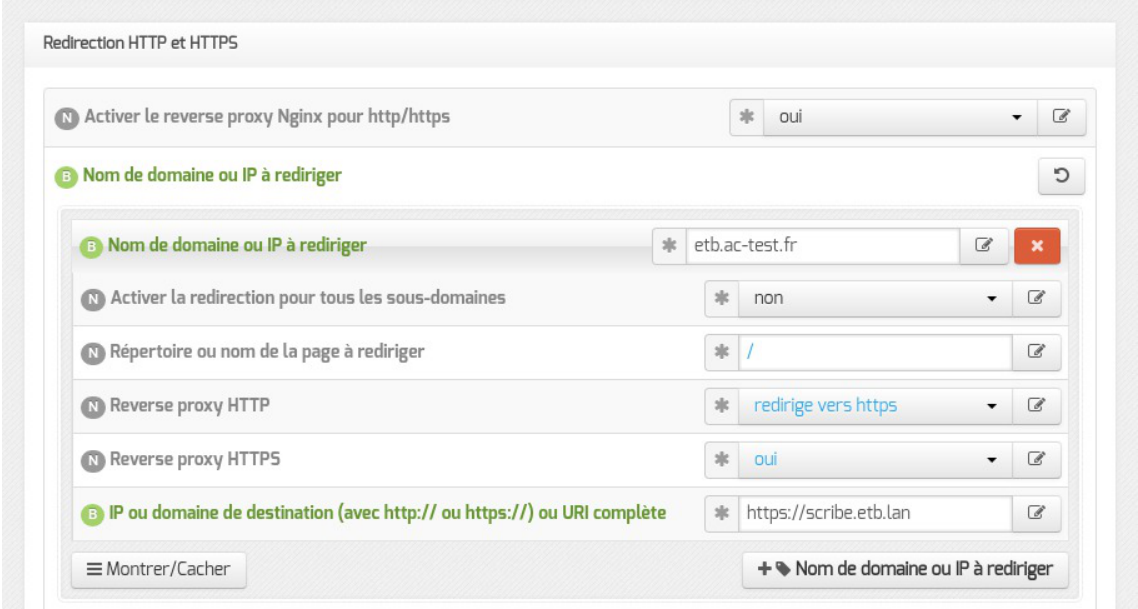
Redirection de l'interface d'administration EAD



Pour accéder de manière sécurisée à l'EAD d'un serveur depuis l'extérieur de l'établissement, il est recommandé :

- d'activer l'interface web de l'EAD du serveur interne sur un second port (4203 par défaut) dans l'onglet expert `Ead-web` de ce module ;
- d'activer la redirection sur le serveur faisant office de reverse proxy en configurant l'adresse IP ou le nom de domaine interne de la machine de destination et son port d'écoute.

Redirection HTTP et HTTPS



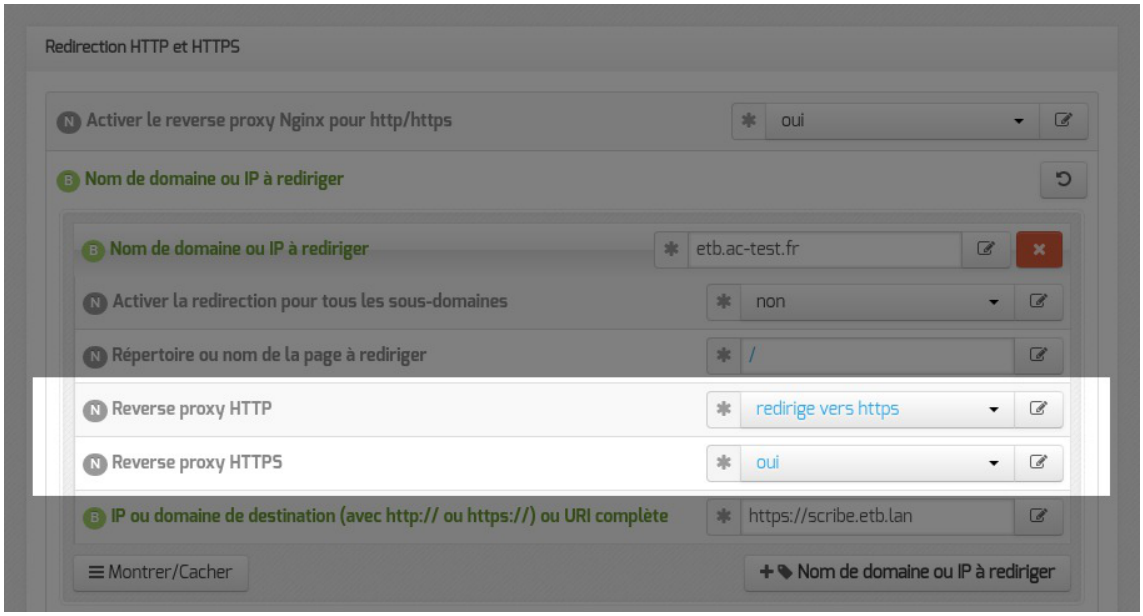
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- le `Nom de domaine ou IP à rediriger` : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- `Activer la redirection pour tous les sous-domaines` : cette variable est disponible à partir de la version 2.6.2 d'EOLE, elle permet la prise en charge de tous les sous-domaines par le proxy inverse ;
- `Demander un certificat à Let's Encrypt pour ce domaine` ? : cette variable est disponible à partir de la version 2.6.2 d'EOLE si la redirection pour tous les sous-domaines n'est pas activé et que le certificat SSL est Let's Encrypt ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

une machine. La valeur par défaut est `/` ;

- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.476] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse `http://monetab.fr` sera automatiquement redirigé vers `https://monetab.fr`

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

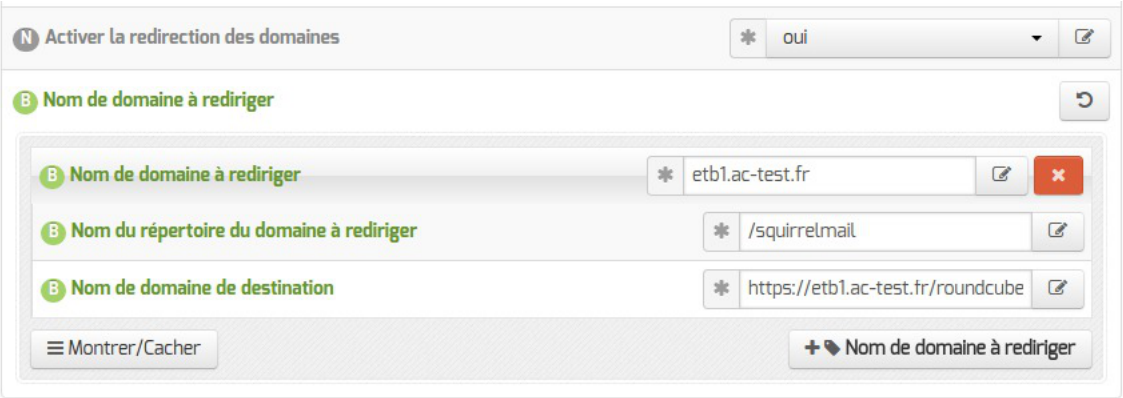
Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `+ Nom de domaine ou IP` à `rediriger`.



> Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.470], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Redirection de domaines

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le reverse proxy permet de rediriger automatiquement les utilisateurs voulant accéder à une page particulière vers une autre page.

L'exemple ci-dessus illustre le remplacement de SquirrelMail par Roundcube : si l'utilisateur cherche à accéder à l'adresse `http://etb1.ac-test.fr/squirrelmail/`, la page se recharge automatiquement avec l'URL de la nouvelle messagerie : `http://etb1.ac-test.fr/roundcube/`.

3.9. 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 courriers électroniques.

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

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

Serveur d'envoi/réception (SMTP)



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.



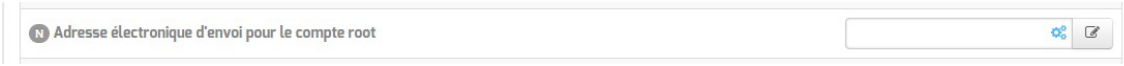
Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

(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.

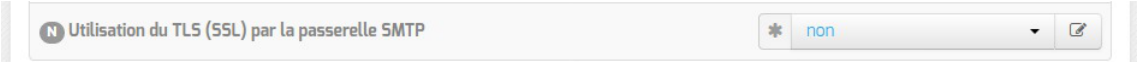
Relai des messages



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`.

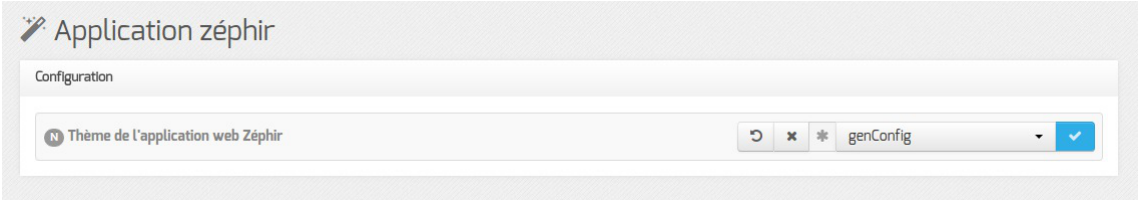
Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.475] pour l'envoi de message. Si la passerelle SMTP[p.472] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.473] (port 25) ou non (port 465).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3.10. 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.

4. 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

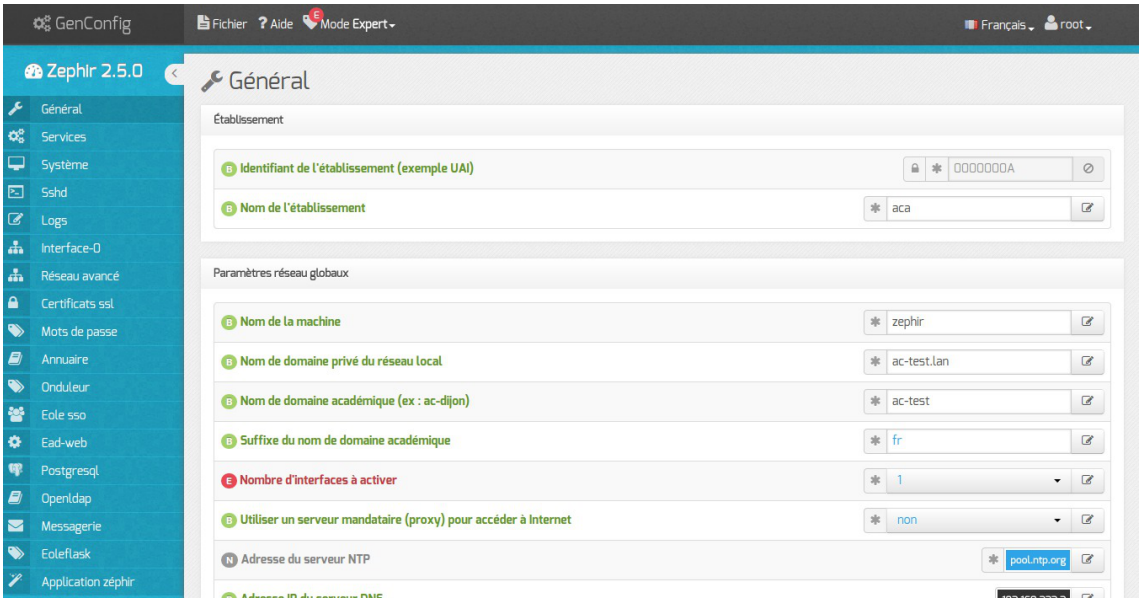
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Zéphir :

- `Général` ;
- `Services` ;
- `Système` ;
- `Sshd` ;
- `Ntp` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-n` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificat ssl` ;
- `Dépôt tiers` ;
- `Annuaire` ;
- `Onduleur` * ;
- `Saltstack` * ;
- `Eole sso` * ;
- `Ead-web` ;
- `Postgresql` ;
- `Openldap` * ;
- `Nginx` ;
- `Applications web nginx` *;
- `Reverse proxy` * ;
- `Messagerie` ;
- `Eoleflask` ;
- `Application zéphir`.

* Certains onglets ne sont visibles qu'après activation du service associé dans l'onglet `Services`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue générale de l'interface de configuration du module

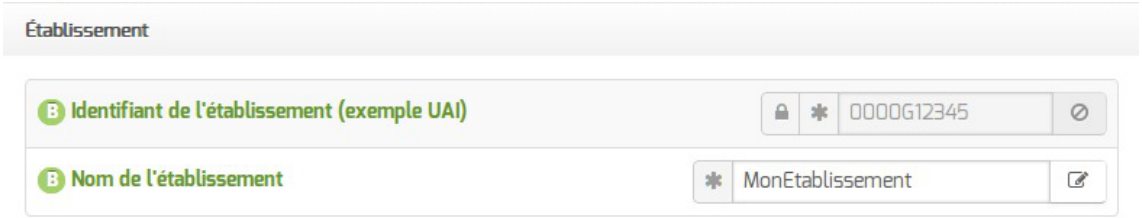
Par défaut, le module Zéphir est livré avec un annuaire LDAP local qui sert à enregistrer des utilisateurs et leur mot de passe.

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.

4.1. 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, ...

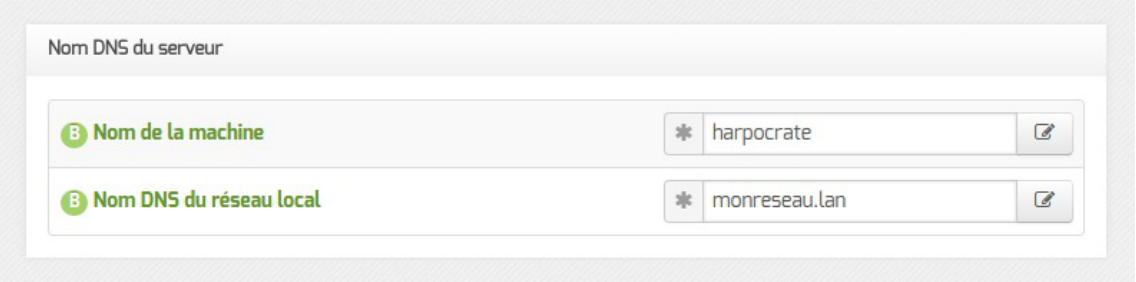
Sur les modules fournissant un annuaire LDAP[p.463] local, ces variables sont utilisées pour créer l'arborescence.



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Nom DNS du serveur



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Le `Nom DNS du serveur` 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.

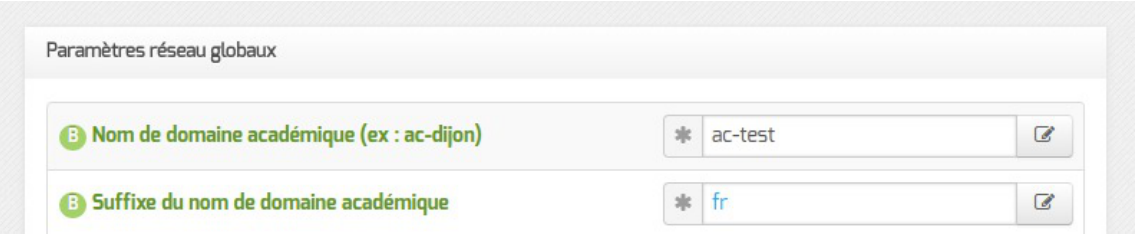
Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

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.

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.

Paramètres réseau globaux



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

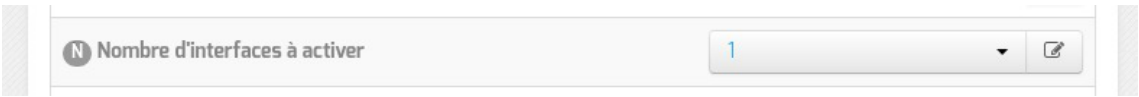
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette information est découpée en plusieurs champs :

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

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`.



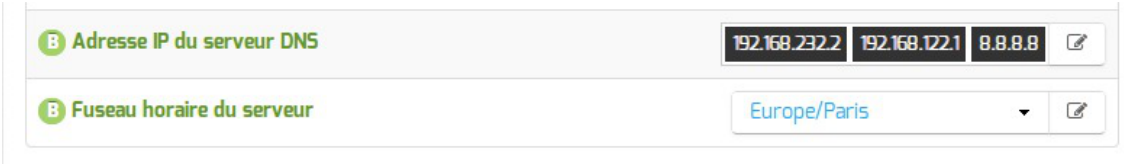
Il devient alors possible de saisir la configuration du serveur proxy :

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



La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait protégé par un module Amon.

DNS et fuseau horaire

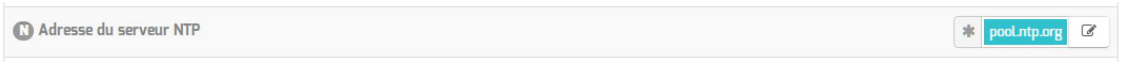


La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.458].

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

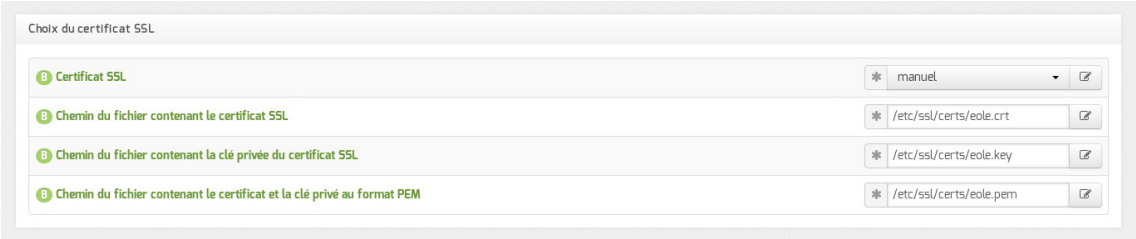
NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.467]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Choix du certificat SSL

> Cette rubrique apparaît sur un module EOLE 2.6 dont la version est supérieure ou égale à 2.6.2.
>
> Elle remplace l'ancienne rubrique `Types de certificats à utiliser` du même onglet en mode normal.



Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.475] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.454] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.463] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour se faire, il faut disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

> Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.
>
> Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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...

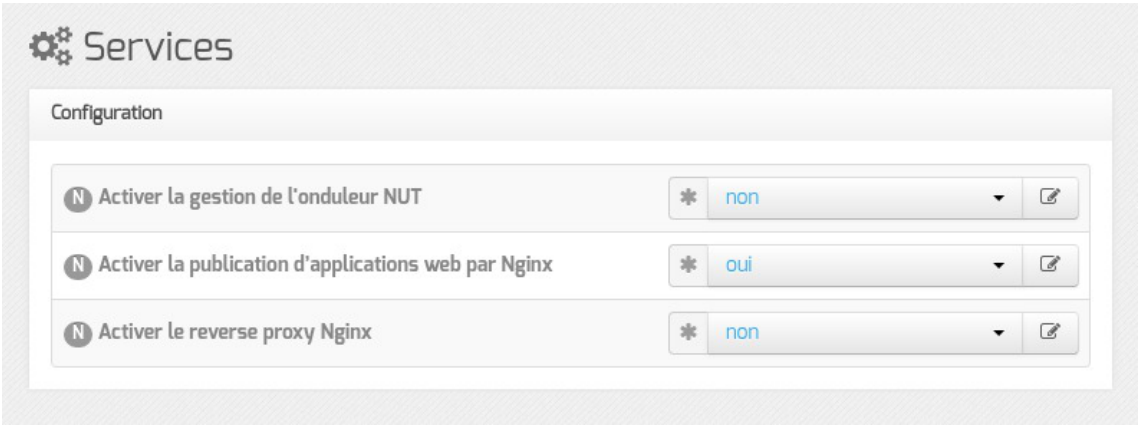
> Les différents types de mises à jour

4.2. 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.467].

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

4.3. 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.
- `Nuance du fond d'écran dans VIM` : l'éditeur VIM peut utiliser différents thèmes pour la coloration syntaxique et adapter ceux-ci en fonction de la valeur de la couleur d'arrière-plan pour en améliorer la lisibilité. La variable prend une valeur parmi dark et light, permettant d'adapter la coloration syntaxique à un arrière-plan sombre et clair respectivement.

Optimisations système



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `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 par défaut est proposé mais il est possible d'adapter.

La complexité des mots de passe peut être réglée 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`.

La valeur 0 permet de désactiver une classe de caractères.



Pour obliger l'utilisation de 2 classes de caractères minimum et d'un minimum de 7 caractères :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 0

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Taille minimum du mot de passe utilisant deux classes de caractères` : 7
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7
- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7



Pour obliger l'utilisation de 3 classes de caractères minimum et d'un minimum de 7 caractères :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 0
- `Taille minimum du mot de passe utilisant deux classes de caractères` : 0
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7
- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7



Il est impossible d'obliger l'utilisation de 3 classes minimum sans obliger l'utilisation de 2 classes minimum, exemple de valeur impossible :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 7
- `Taille minimum du mot de passe utilisant deux classes de caractères` : 0
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7
- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7

Les valeurs doivent être respectivement : 0, 0, 7 et 7.



Deux librairie sont utilisées pour vérifier la validité des mots de passe : `pam_passwdqc.so` et `pam_unix.so`.

Les réglages de la première librairie s'effectuent via les variables proposées. Si les règles établies par la première librairie ne sont pas suffisamment sécurisées, d'autres règles seront imposées par la seconde :

- le mot de passe ne peut être basé sur l'identifiant du compte ;
- le mot de passe ne peut être basé sur l'ancien mot de passe ;
- le mot de passe ne peut pas comporter des mots du dictionnaire ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le mot de passe ne peut être basé sur une séquence connue (suite de lettre sur le clavier par exemple) ;
- le mot de passe doit contenir suffisamment de caractères différents ;
- les lettres majuscules au début du mot de passe et les chiffres à la fin du mot de passe ne comptent pas comme l'utilisation d'une classe de caractère.



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



Il est possible de désactiver la validation des mots de passe en passant `Vérifier la complexité des mots de passe` à `non`.

Il ne faut bien évidement pas désactiver cette fonctionnalité dans un contexte de production.

Cette fonctionnalité est intéressante pour faciliter la mise en place d'une infrastructure de test.



Ce paramétrage concerne uniquement les comptes système du serveur. Les utilisateurs LDAP ne sont pas soumis aux mêmes restrictions.

Ajustement du partitionnement



L'ajustement du partitionnement n'est disponible dans l'interface de configuration du module en mode expert qu'avant l'instance et seulement si le volume physique contient de l'espace libre. Cette fonctionnalité est donc visible par défaut sur Eolebase et sur d'autres modules si le partitionnement manuel à été utilisé pour réserver de l'espace.

Pour maîtriser correctement ce qui va être fait il faut consulter l'état du partitionnement avant de saisir les paramètres souhaités à l'aide de la commande `df -h /` et des commandes `vgdisplay` et `lvdisplay`.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     2,1G  6,5G  25% /
tmpfs                          1000M      28K 1000M   1% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     2,9M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
root@eolebase:~#
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  8
  VG Access             read/write
  VG Status             resizable
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  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       5550 / 21,68 GiB
  Free  PE / Size       4510 / 17,62 GiB
  VG UUID               ctPVcP-76Se-EpMp-FLO3-13aR-Ghg9-PdIdUW

root@scribe:~#
root@scribe:~# lvdisplay

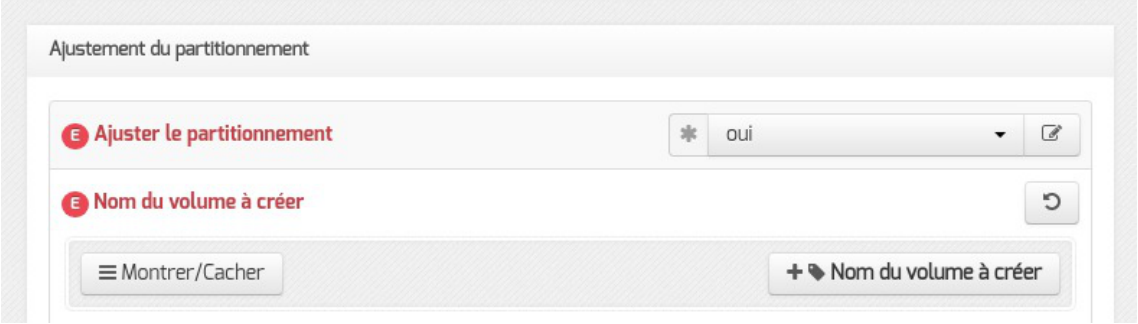
  --- Logical volume ---
  LV Path                /dev/scribe-vg/root
  LV Name                root
  VG Name                scribe-vg
  LV UUID                uN8emF-hD9j-eNwv-zdaC-mEeK-9XGe-uBu2OU
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-10-05 18:37:11 +0200
  LV Status              available
  # open                 1
  LV Size                8,94 GiB
  Current LE             2288
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:0

[...]
```

Ajuster le partitionnement sur une version d'EOLE inférieur à 2.6.2

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques.

Pour ajuster le partitionnement sur une version d'EOLE inférieure à 2.6.2, ouvrir l'interface de configuration du module, passer en mode Expert et se rendre dans l'onglet `Système`.



Après avoir passer `Ajuster le partitionnement` à `oui` et après avoir cliquer sur le bouton `+ Nom du volume à créer` un certain nombre de paramètres s'affiche.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;
- point de montage ;
- les options du montage (indispensable pour la gestion des quotas par exemple).

Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.

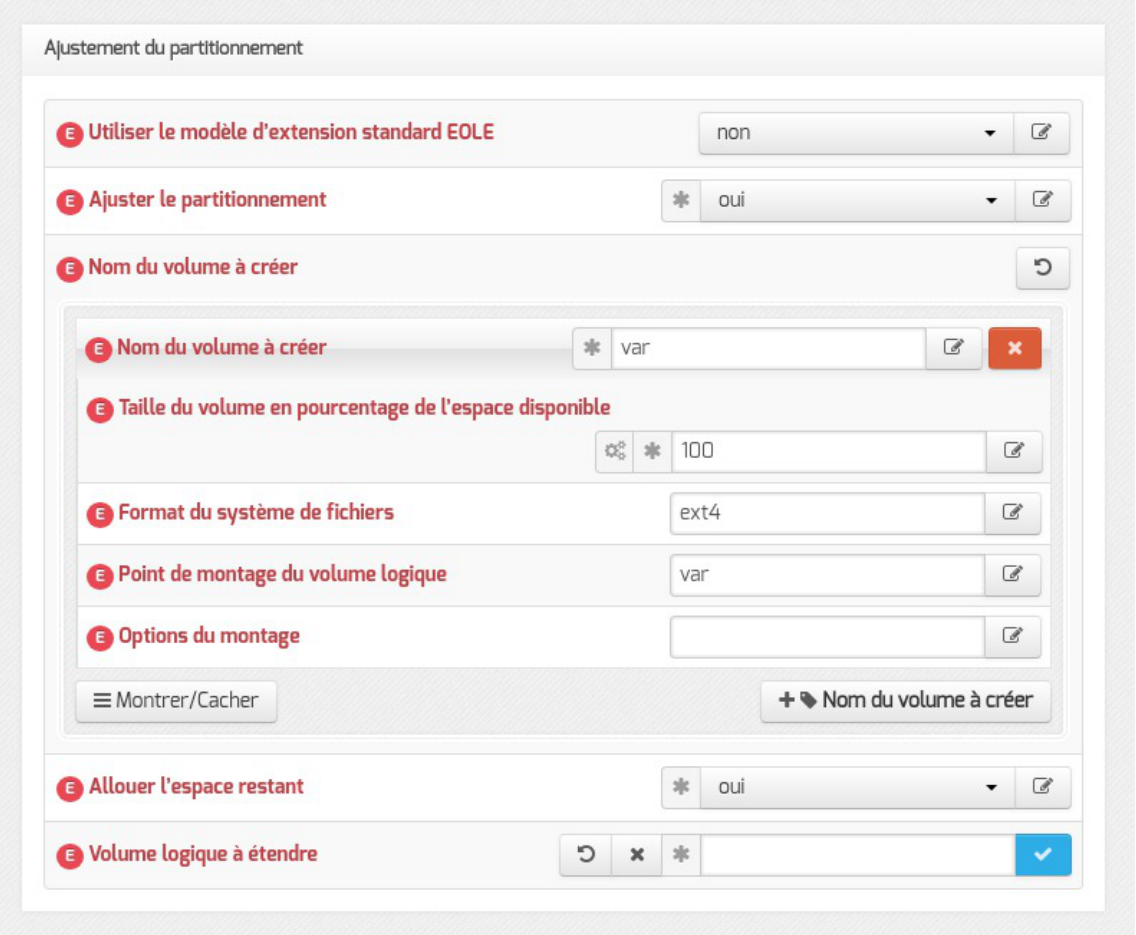
Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

Ajuster le partitionnement sur une version d'EOLE supérieure ou égale à 2.6.2

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques et d'ajouter de l'espace à des partitions existantes.

Pour ajuster le partitionnement à partir de la version 2.6.2 d'EOLE, ouvrir l'interface de configuration du module, passer en mode Expert et se rendre dans l'onglet `Système`. Puis il faut passer `Utiliser le modèle d'extension standard EOLE` à `non` pour ajuster le partitionnement.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ajustement du partitionnement à partir d'EOLE 2.6.2

Après avoir passer `Ajuster le partitionnement` à `oui`, les partitions existantes sont affichées et un certain nombre de paramètres s'affichent.

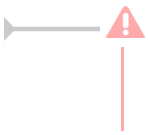


- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;
- point de montage ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- les options du montage (indispensable pour la gestion des quotas par exemple).

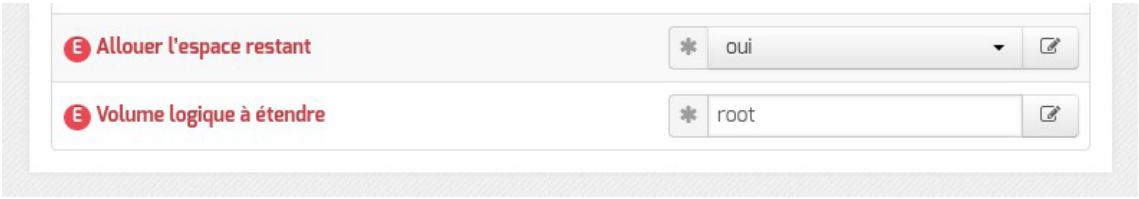
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

Allouer l'espace restant

Positionner la variable `Allouer l'espace restant` à `oui` permet de choisir un volume existant auquel ajouter la totalité de l'espace libre restant.



La valeur à saisir est la partie du nom du volume qui permet d'identifier le point de montage, par exemple pour le volume `/dev/mapper/eolebase--vg-root` il faut saisir `root` dans le nom du `Volume logique à étendre`. S'il ne reste pas d'espace, ce jeu de paramètres est sans effet.

Résultat après instance

Le paramétrage est effectif après l'instanciation du module.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     1,9G  6,7G  22% /
tmpfs                          1000M       0 1000M   0% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     3,6M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
/dev/mapper/eolebase--vg-var     27G     311M   25G   2% /var
root@eolebase:~#
```

Le nouveau volume logique est présent et la partition `/root` s'est vu augmentée du reste de l'espace libre.

Voir aussi...

Les mots de passe [p.203]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.4. 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`).

Autoriser les connexions SSH pour l'utilisateur root

Permet d'interdire les connexions SSH avec le compte utilisateur `root` (paramètre `PermitRootLogin`).

Autoriser les connexions SSH par mot de passe (si non clef RSA obligatoire)

Permet d'interdire les connexions SSH par mot de passe. Dans ce cas, seules les connexions par clef RSA seront autorisées (paramètre `PasswordAuthentication`).

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)`.

Autoriser les connexions SSH pour les groupes

Permet de déclarer des groupes Unix supplémentaires autorisés à se connecter en SSH au serveur (paramètre `AllowGroups`).

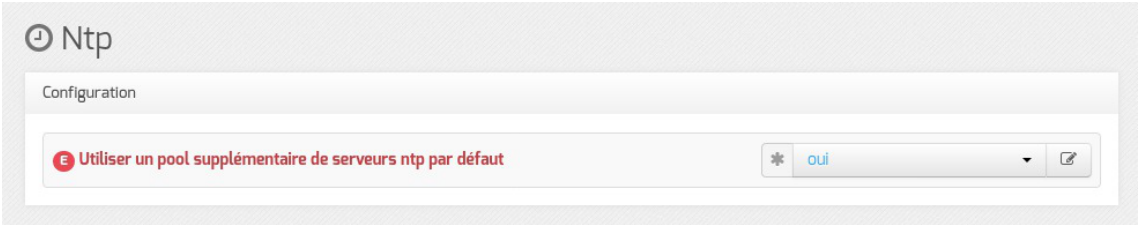
Par défaut, les groupes Unix autorisés sont `root` et `adm`.

Critères à appliquer pour le blocage des tentatives de connexions par force brute

La première valeur est le nombre de tentatives de connexions échouées tolérées. La dernière valeur est le nombre de connexions échouées maximales. La deuxième valeur fixe le pourcentage de refus aléatoire une fois le nombre de connexions tolérées atteint. Ce pourcentage de refus augmente à chaque échec supplémentaire jusqu'à ce que le nombre de connexions maximales soit atteint (paramètre `MaxStartups`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.5. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système



À partir d'EOLE 2.6.2, le paramètre disponible dans ce nouvel onglet du mode expert permet de désactiver l'utilisation d'un pool de serveurs de secours pour la synchronisation de l'horloge.

Recourir aux serveurs de ce pool permet de pallier une défaillance du ou des serveurs NTP renseignés dans l'onglet `Général` (variable `serveur_ntp`).

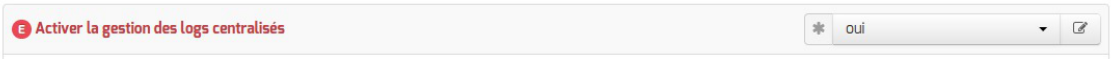
Par défaut, l'utilisation du pool est activée.

Sa désactivation est parfois requise pour limiter la bande passante utilisée par le service de synchronisation du temps, celui-ci cherchant à contacter un grand nombre de sources de temps pour déterminer l'heure du serveur.

4.6. Onglet Logs : Gestion des logs centralisés

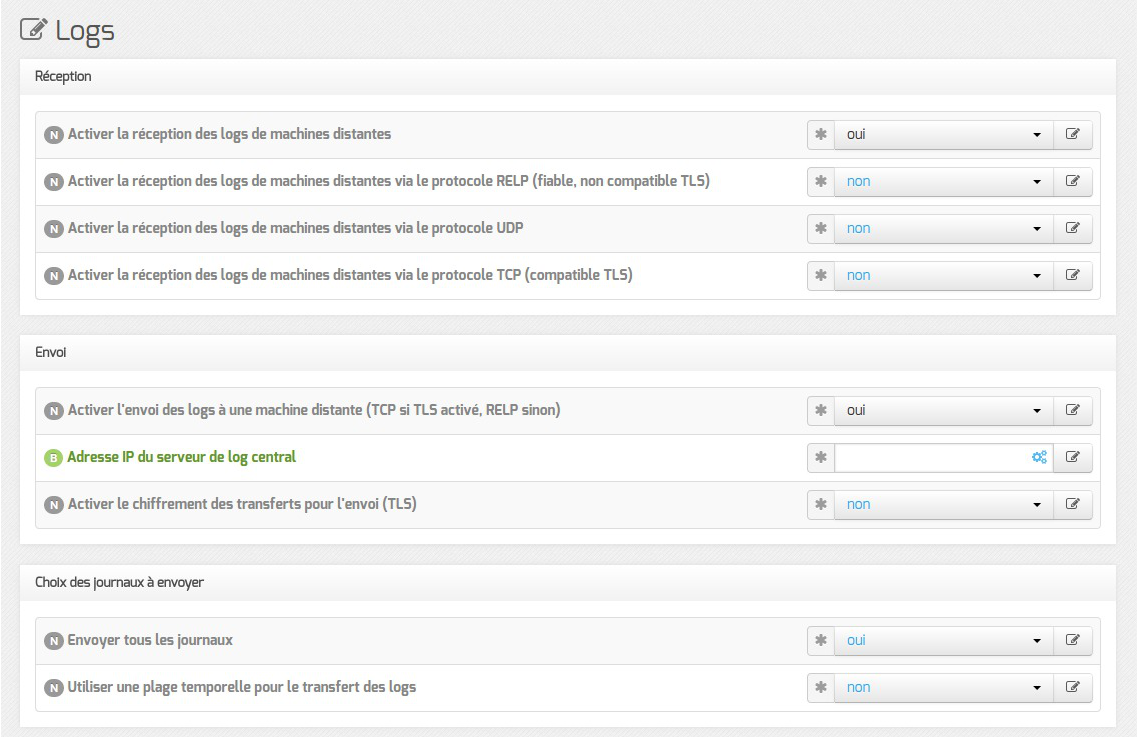
La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.477]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



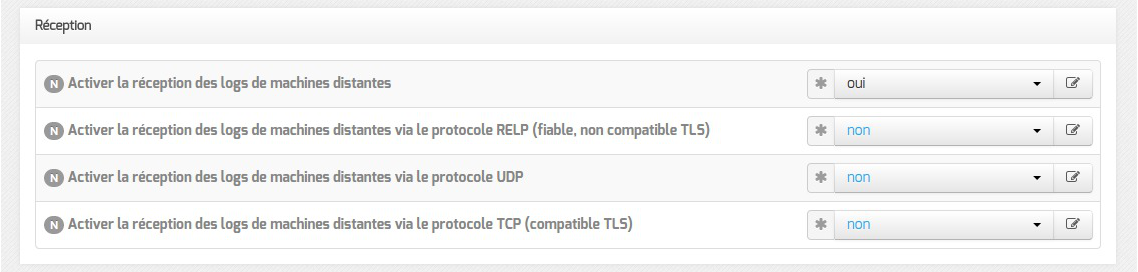
Vue de l'onglet Logs

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.474] ou RELP[p.471]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.475]) ;
- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.453].

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.

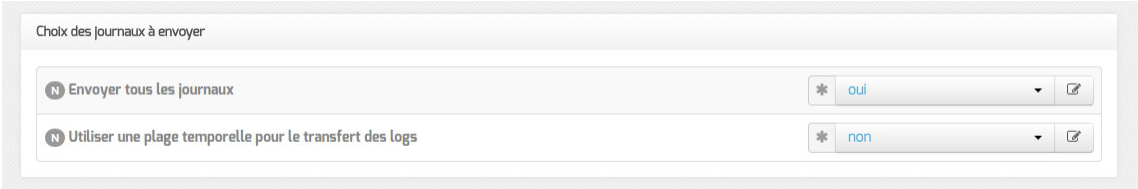


Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.453].

Choix des journaux à envoyer

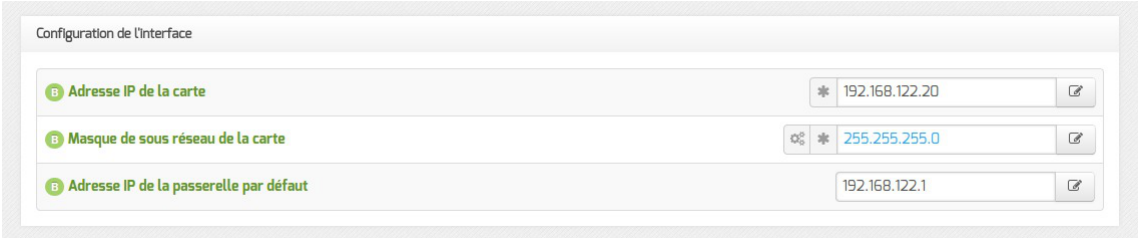
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



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.

4.7. Onglet Interface-0

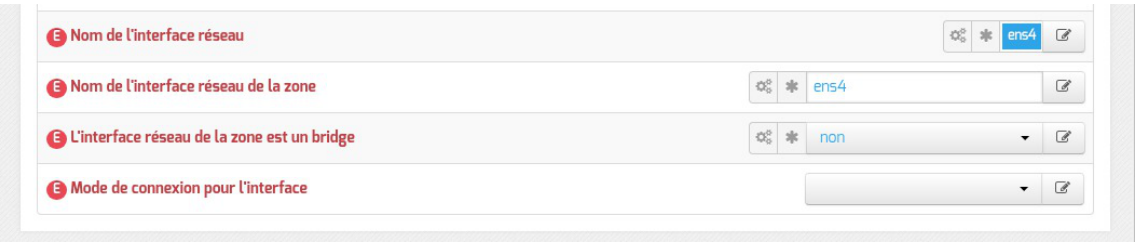
Configuration de l'interface



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Nom de l'interface réseau

À partir de la version EOLE 2.6, afin de respecter la convention Consistent Network Device Naming[p.455], le nom de l'interface réseau proposé dans l'interface de configuration du module correspond à son emplacement physique.

L'ordre de chargement des cartes réseau n'est donc plus susceptible d'être modifié en cas de changement matériel, contrairement aux versions précédentes qui utilisaient les adresses MAC[p.453] des cartes pour les identifier.

De ce fait, l'ancien fichier de configuration `/etc/udev/rules.d/70-persistent-net.rules` n'existe plus.

Ajouter des interfaces physiques supplémentaires à la variable `Nom de l'interface réseau` permet d'activer l'agrégation de liens Ethernet[p.453].

Afin de sécuriser la mise à jour depuis la version 2.5.2 d'EOLE, l'ancienne politique de nommage des interfaces est conservée lorsque la procédure `Upgrade-Auto` est utilisée.

Les noms réels des interfaces sont visibles dans le répertoire `/sys/class/net/` :

```
# ls -d /sys/class/net/*
/sys/class/net/ens4 /sys/class/net/lo
```

Les interfaces gérées par EOLE sont enregistrées dans le fichier spécial : `/var/lib/eole/config/persistent-net.cfg`.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface logique associée à l'interface physique pour cette 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

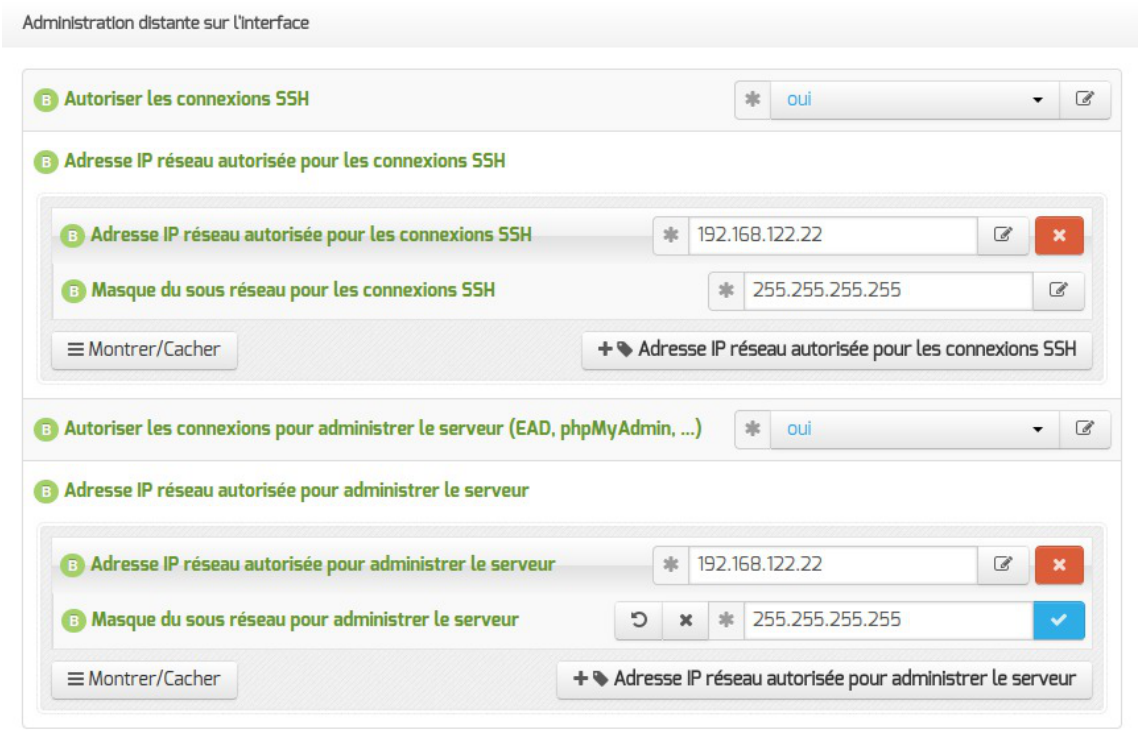
Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possibles :

- `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



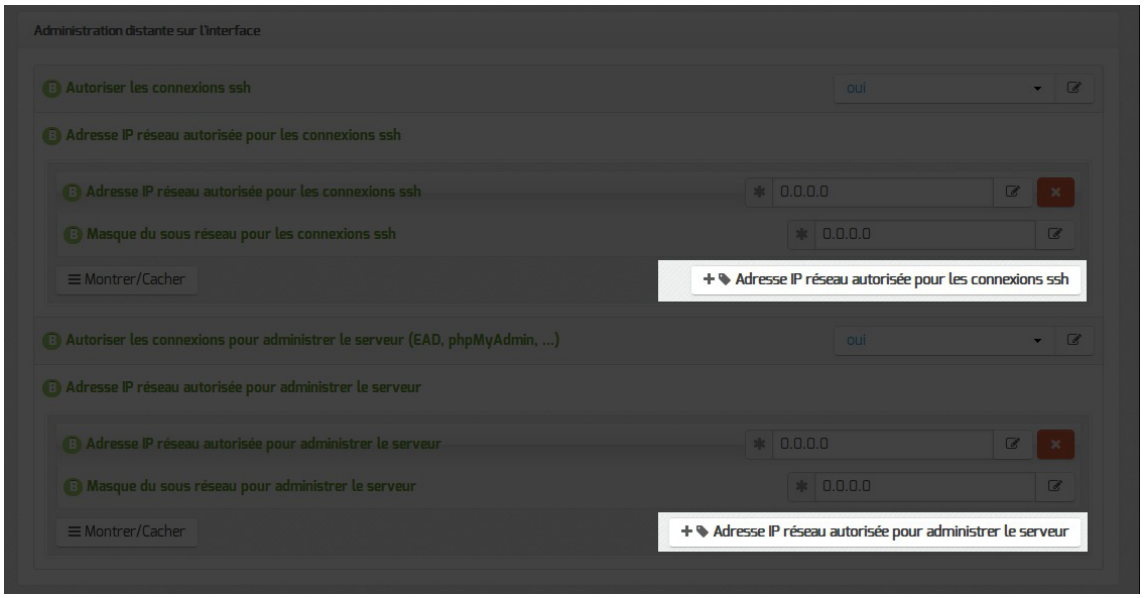
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.473] 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

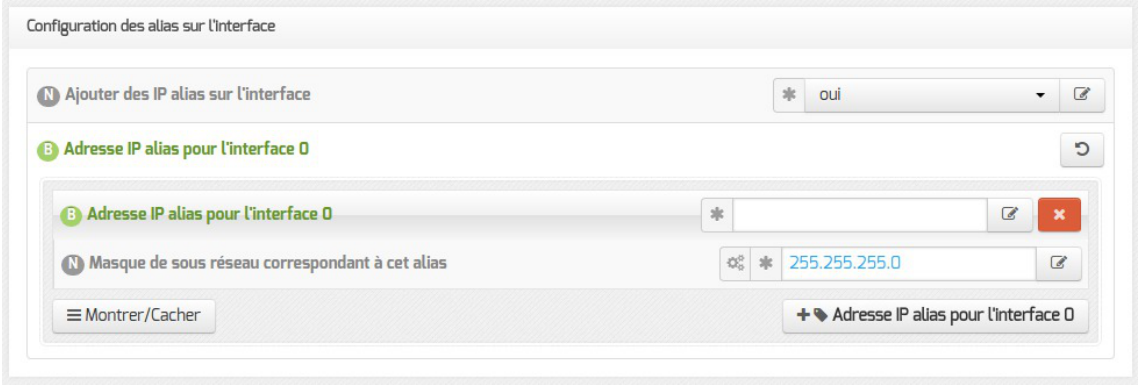
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

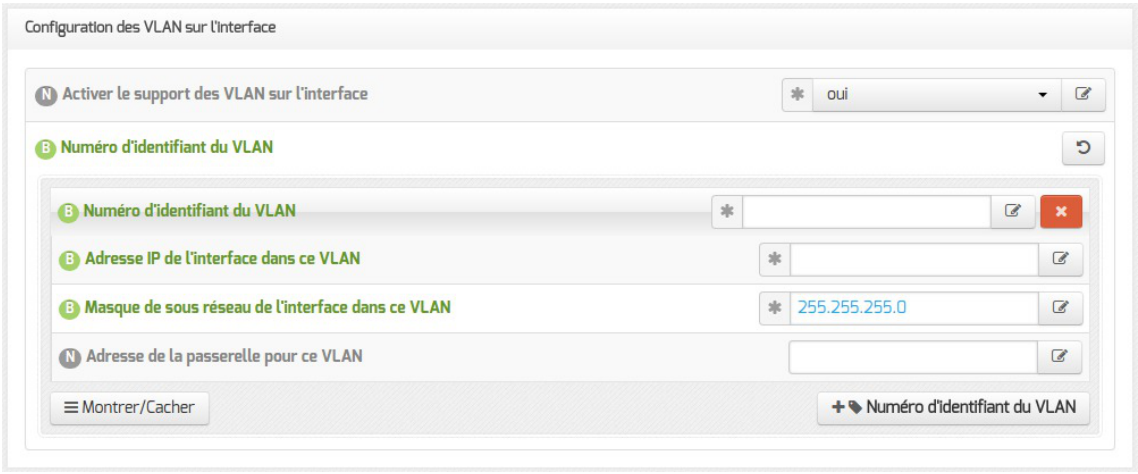


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

> Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.476] (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

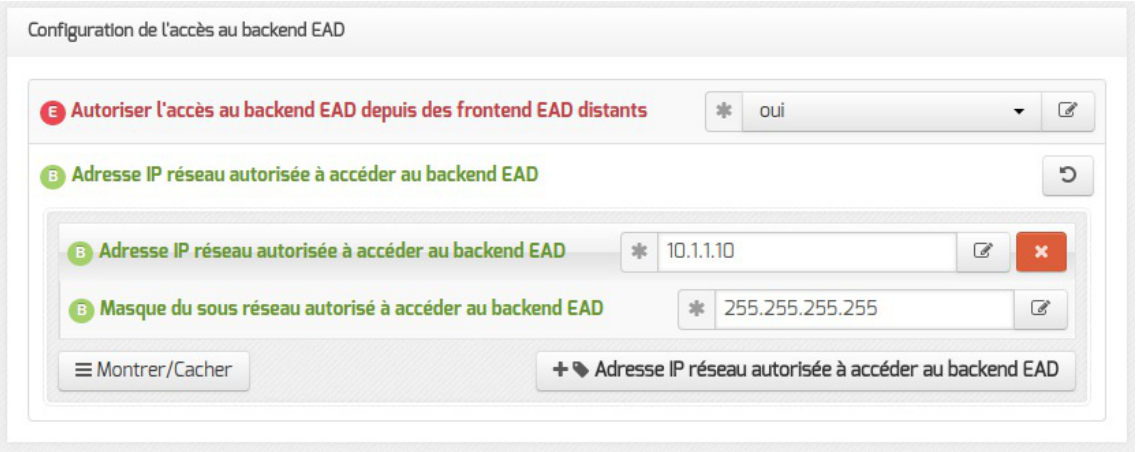
- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.

> Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Accès au backend EAD

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD[p.458] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Par défaut, l'accès au backend est bloqué pour chaque interface.

Si le pare-feu est désactivé (mode expert dans l'onglet `Réseau avancé`), ces autorisations ne sont plus visibles et l'accès est autorisé à tous les frontend depuis toutes les interfaces.

Voir aussi...

Mise en place de l'agrégation de liens Ethernet (bonding) [p.200]

4.8. 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.

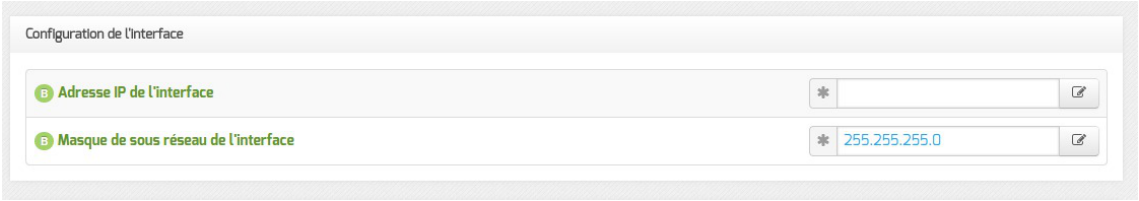


Cela ajoute autant d'onglet `Interface-n` que le nombre d'interfaces à activer choisi.

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

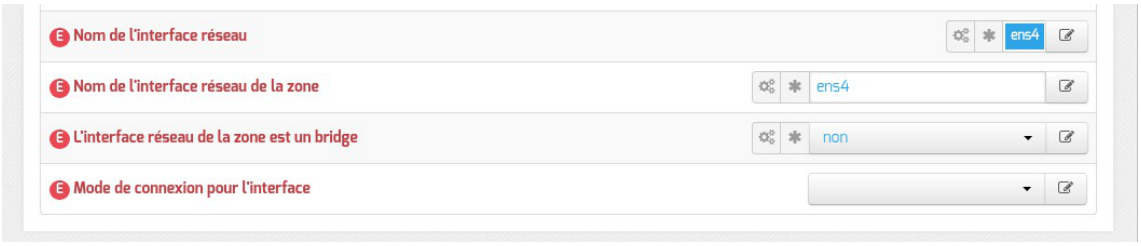
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

À partir de la version EOLE 2.6, afin de respecter la convention Consistent Network Device Naming[p.455], le nom de l'interface réseau proposé dans l'interface de configuration du module correspond à son emplacement physique.

L'ordre de chargement des cartes réseau n'est donc plus susceptible d'être modifié en cas de changement matériel, contrairement aux versions précédentes qui utilisaient les adresses MAC[p.453] des cartes pour les identifier.

De ce fait, l'ancien fichier de configuration `/etc/udev/rules.d/70-persistent-net.rules` n'existe plus.

Ajouter des interfaces physiques supplémentaires à la variable `Nom de l'interface réseau` permet d'activer l'agrégation de liens Ethernet[p.453].

Afin de sécuriser la mise à jour depuis la version 2.5.2 d'EOLE, l'ancienne politique de nommage des interfaces est conservée lorsque la procédure `Upgrade-Auto` est utilisée.

Les noms réels des interfaces sont visibles dans le répertoire `/sys/class/net/` :

```
# ls -d /sys/class/net/*
/sys/class/net/ens4 /sys/class/net/lo
```

Les interfaces gérées par EOLE sont enregistrées dans le fichier spécial : `/var/lib/eole/config/persistent-net.cfg`.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface logique associée à l'interface physique pour cette zone.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 possibles :

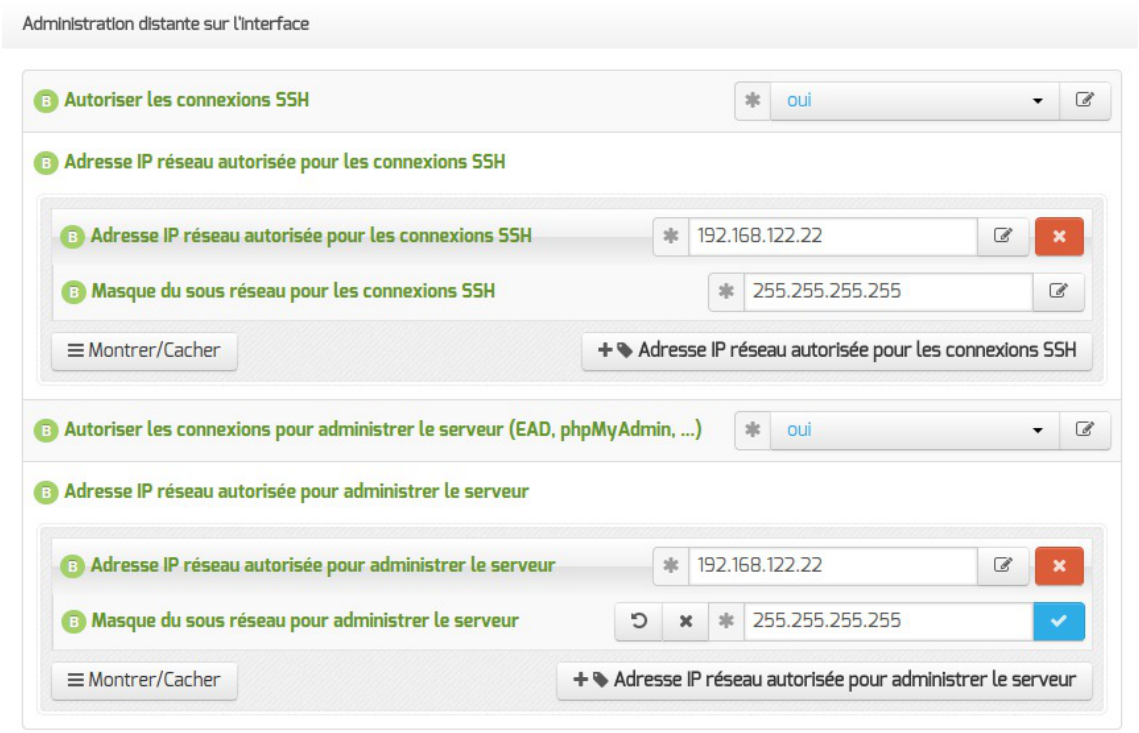
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

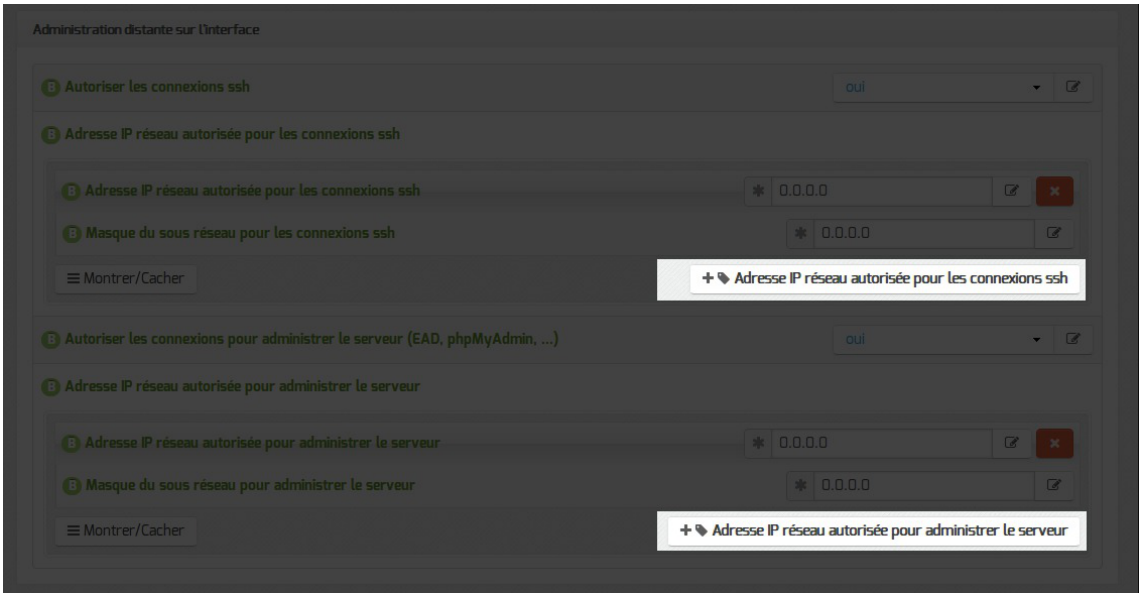


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.473] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

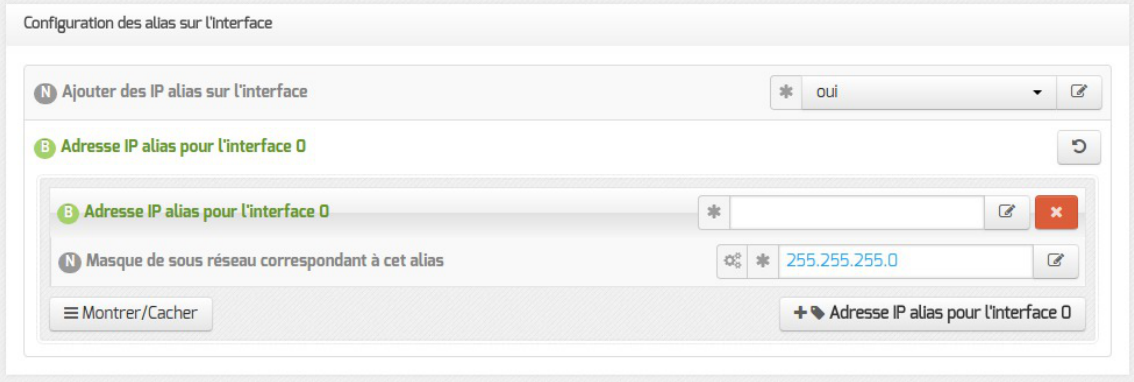
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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.

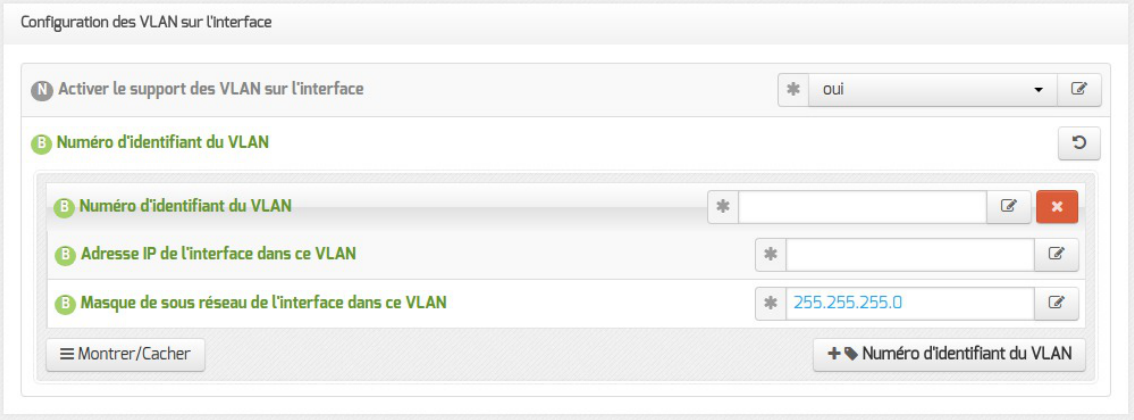


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.476] (réseau local virtuel) sur une interface déterminée du module.



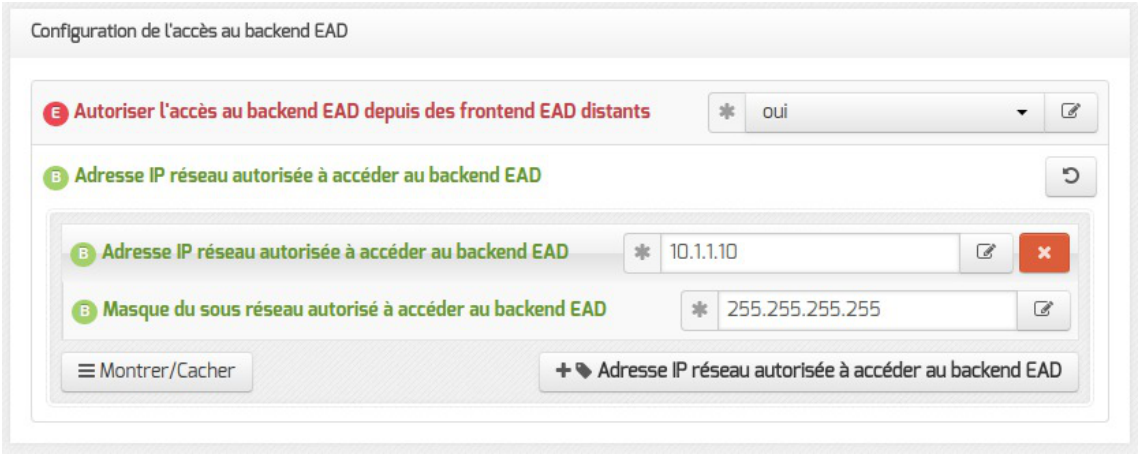
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Accès au backend EAD



À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD[p.458] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Par défaut, l'accès au backend est bloqué pour chaque interface.

Si le pare-feu est désactivé (mode expert dans l'onglet `Réseau avancé`), ces autorisations ne sont plus visibles et l'accès est autorisé à tous les frontend depuis toutes les interfaces.

Voir aussi...

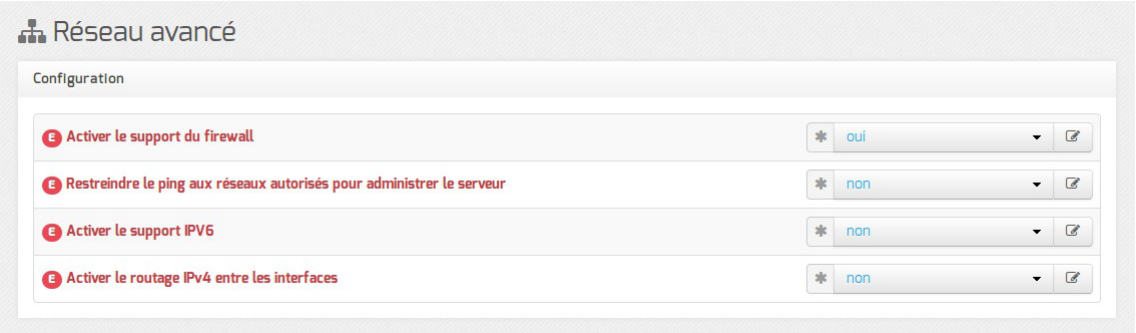
Mise en place de l'agrégation de liens Ethernet (bonding) [p.200]

4.9. Onglet Réseau avancé

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

Configuration IP

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.462] 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`).

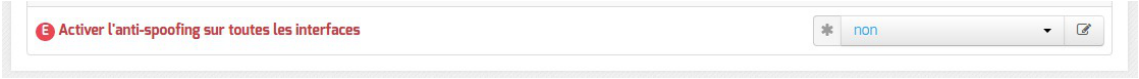
Sécurité



Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

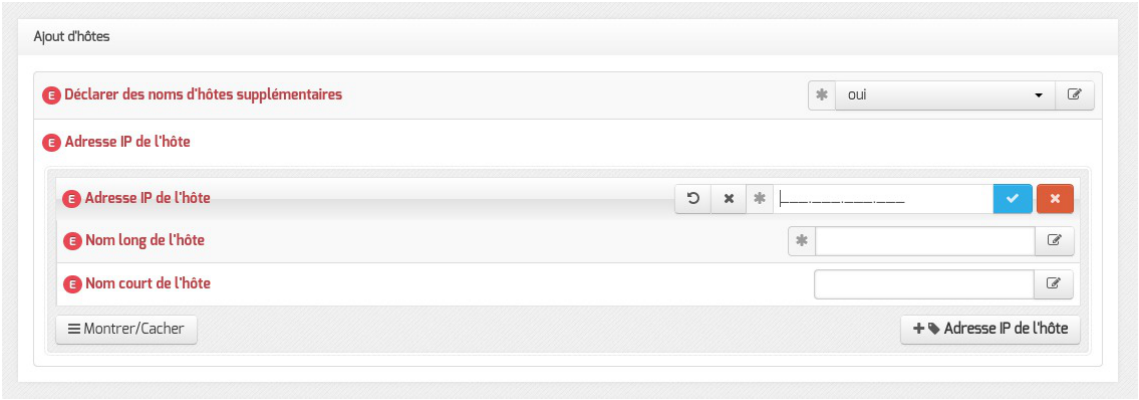
utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.454] est activé sur l'interface-0 des modules EOLE.

Sur les serveurs ayant 2 interfaces réseau ou plus d'activées (cas par défaut sur les modules Amon, Sphynx et Hâpy), 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`.

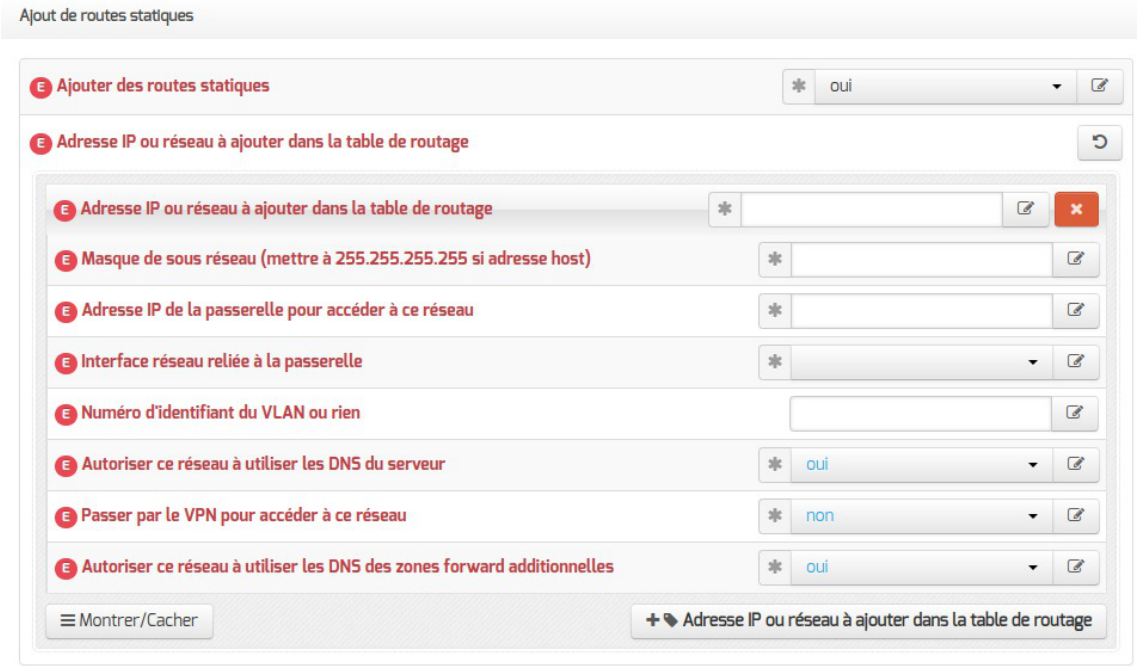
Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte`.

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.454] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 configurer 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 ;
- `Numéro d'identifiant du VLAN ou rien` : permet d'associer une route à un VLAN ;

Les deux paramètres suivants apparaissent uniquement su le service `eole-dns` est installé sur le module :

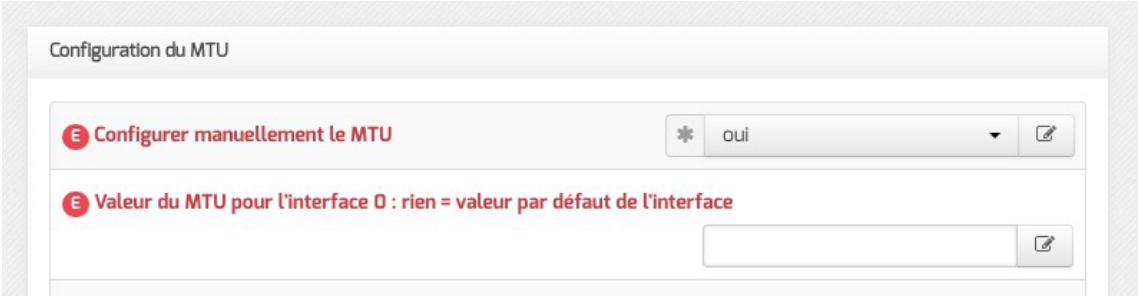
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Le paramètre suivant apparaît uniquement si le réseau virtuel privé RVP est activé :

- `Passer par le VPN pour accéder à ce réseau` : ce réseau n'est pas un réseau local. C'est un réseau distant accessible par le VPN.

Configuration du MTU

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.466] (paramètre : /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.461] 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.466] pour toutes les interfaces déclarées

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

Si l'interface externe est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le champ : `Valeur du MTU pour l'interface 0`.



Si l'interface externe d'un module Amon ou AmonEcole est de type PPPoE[p.470] et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le champ dédié : `Valeur du MTU pour l'interface ppp0`. Il ne faut rien saisir ou supprimer la valeur présente dans `Valeur du MTU pour l'interface 0`.

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

Configuration de la "neighbour table"

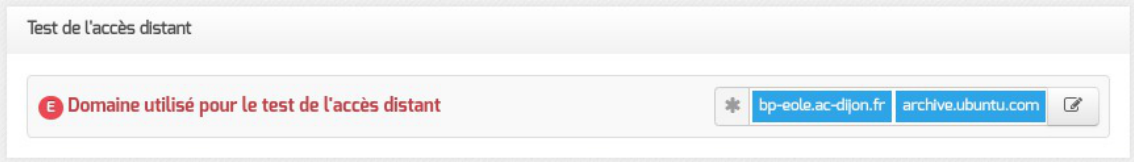


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

4.10. Onglet Certificats ssl : gestion des certificats SSL

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

Le choix du type de certificat à mettre en place sur le serveur s'effectue dans l'onglet `Général`.

Certificat de type Let's Encrypt

L'autorité de certification Let's Encrypt[p.463] permet de mettre en place, gratuitement, des certificats dont la distribution et le renouvellement sont automatisés.

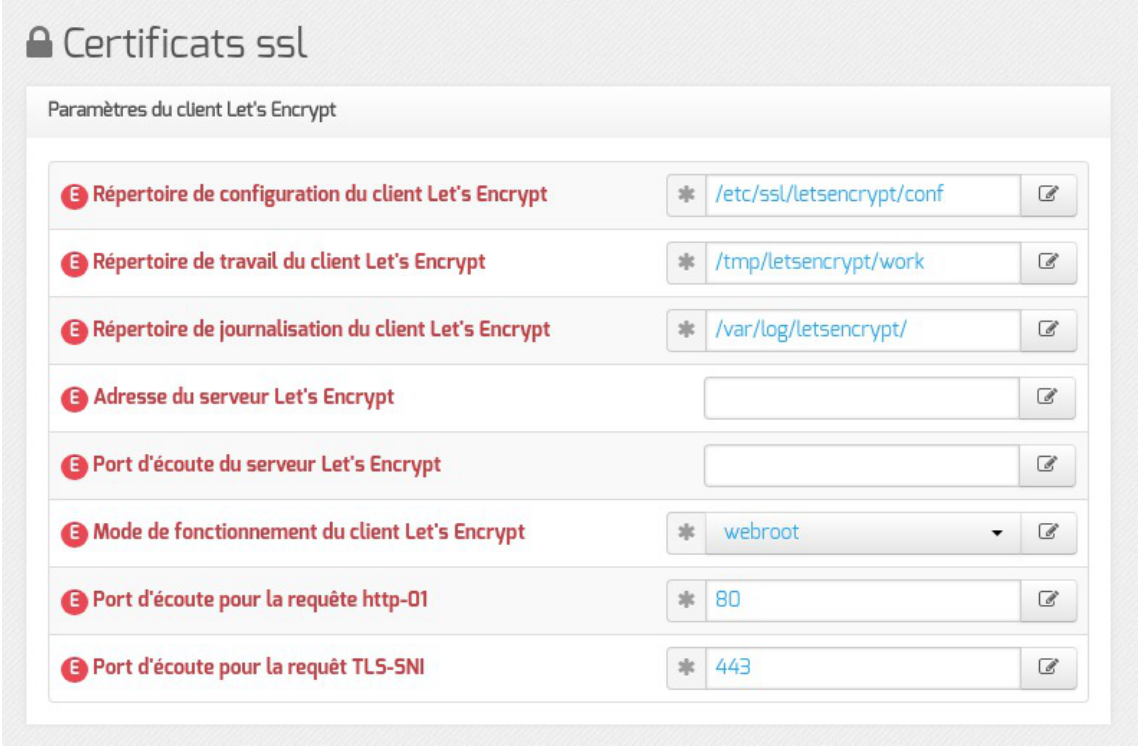
Vous pouvez à présent gérer des certificats Let's Encrypt pour des serveurs accessibles depuis Internet ou au travers d'un proxy inverse.

Serveurs accessibles depuis Internet ou au travers d'un proxy inverse

L'utilisation de certificats Let's Encrypt requiert l'utilisation de noms DNS connus d'Internet.

Le certificat sera fait au nom résultant de la concaténation du nom de la machine et du nom de DNS local.

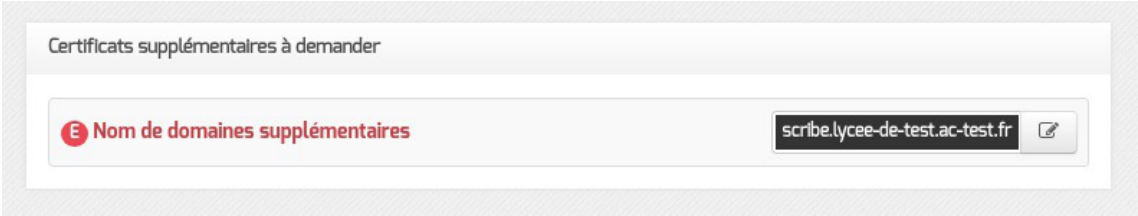
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Seule la variable `Mode de fonctionnement du client Let's Encrypt` nécessite un paramétrage en fonction de l'accessibilité du serveur :

- accessible depuis Internet → utiliser la valeur `standalone` ;
- accessible au travers d'un proxy inverse → utiliser la valeur `webroot`.

Nom DNS supplémentaires



Il est possible de faire des requêtes supplémentaires pour d'autres noms DNS connus d'Internet en renseignant la variable `Nom de domaines supplémentaires`.

> Il y aura autant de certificats supplémentaires que de noms DNS déclarés dans la variable `Nom de domaines supplémentaires`.

Certificat de type autosigné et manuel

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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

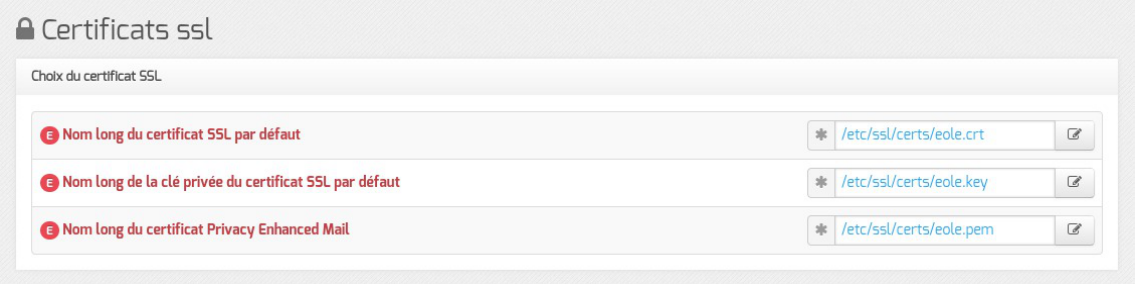
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un 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`.

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 trois variables dans l'onglet `Certificats ssl` de l'interface de configuration du module.



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.

Sur un module dont la version est supérieure ou égale à 2.6.2, la configuration des chemins est proposée dans l'onglet `Général`.

Le répertoire `/etc/ssl/local_ca/` accueille uniquement des certificats CA.

Paramètres SSL

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les variables de la section `Paramètres SSL` permettent de personnaliser la configuration OpenSSL[p.468] à utiliser pour générer les certificats auto-signés.



Taille de la clé

Cette variable permet de définir le paramètre `default_bits` de la section `[req]` du fichier de configuration d'OpenSSL.

Par défaut la taille de la clé est de 2048 bits.

Durée de validité du certificat

Cette variable permet de définir le paramètre `default_days` des sections `[ CA_default ]` et `[req]` du fichier de configuration d'OpenSSL.

Par défaut la CA et les certificats générés expirent au bout de 3 ans (1096 jours).

Sujet du certificat

Les variables de la section `Subject (DN)` permettent de configurer le nom complet du serveur (distinguished name[p.458]) à utiliser pour générer les certificats auto-signés.



Nom du pays (C=)

Cette variable permet de définir le paramètre `countryName` de la section `[req_distinguished_name]` du fichier de configuration d'OpenSSL.

Il s'agit du code du nom de pays sur deux lettres, par défaut `FR` pour la France.

Nom de l'organisation (O=)

Cette variable permet de définir le paramètre `organizationName` de la section `[req_distinguished_name]` du fichier de configuration d'OpenSSL.

Il s'agit du nom de la structure, par défaut `Ministere Education Nationale (MENESR)` dans le cadre de l'Éducation Nationale.

Nom de l'unité de l'organisation (OU=)

Cette variable est utilisée pour ajouter des unités organisationnelles[p.475] dans le paramètre

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`organizationalUnitName` de la section *`[req_distinguished_name]`* du fichier de configuration d'OpenSSL.

La valeur par défaut `110 043 015` représente le numéro SIREN du Ministère de l'Éducation Nationale.

Nom DNS du serveur (CN=)

Cette variable permet de définir le paramètre `commonName` de la section *`[req_distinguished_name]`* du fichier de configuration d'OpenSSL.

Le CN[p.455] du serveur est pré-renseigné à l'aide des informations fournies dans l'onglet Général.

La commande suivante permet d'afficher les DN de l'émetteur et du sujet du certificat généré :

```
root@dc1:~# openssl x509 -in /etc/ssl/certs/eole.crt -noout -issuer
-subject
issuer=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043
015, OU = ac-test, CN = CA-dc1.domseth.ac-test.fr
subject=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043
015, OU = ac-test, CN = dc1.domseth.ac-test.fr
```

Nom DNS alternatif

La section `Nom Alternatif` de la machine permet de renseigner tous les noms DNS associés au serveur.



Nom DNS alternatif du serveur

Cette variable permet d'ajouter tous les noms DNS nécessaires dans la section *`[ ALIASES ]`* du fichier de configuration d'OpenSSL.

Elle doit notamment contenir les noms de domaine utilisés pour accéder aux applications web (l'EAD[p.458] par exemple).

Pour que les modifications soient prises en compte, il faut reconfigurer le serveur puis re-générer les certificats.

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`

Re-génération des certificats

Si les certificats auto-signés sont expirés ou si ils ne sont plus adaptés à la configuration du serveur, il est possible de les re-générer à l'aide de la commande suivante :

```
/usr/share/creole/gen_certif.py -f
```

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
```

Re-génération des certificats

Si les certificats auto-signés sont expirés ou si ils ne sont plus adaptés à la configuration du serveur, il est possible de les re-générer à l'aide de la commande suivante :

```
/usr/share/creole/gen_certif.py -f
```

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

Si la chaîne de certification du serveur contient une ou plusieurs autorités intermédiaires, vous devez concaténer le certificat du serveur avec les certificats des autorités intermédiaires dans l'ordre de la chaîne de certification vers l'autorité racine.

Par exemple, pour une chaîne de certification suivante :

1. `CA-ROOT`
2. `CA-SUB1` signée par `CA-ROOT`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3. `CA-SUB2` signée par `CA-SUB1`
4. `mon-serveur` signé par `CA-SUB1`

```
cat mon-serveur.crt ca-sub2.crt ca-sub1.crt > /etc/ssl/cert/mon-serveur.crt
```

Voir aussi...

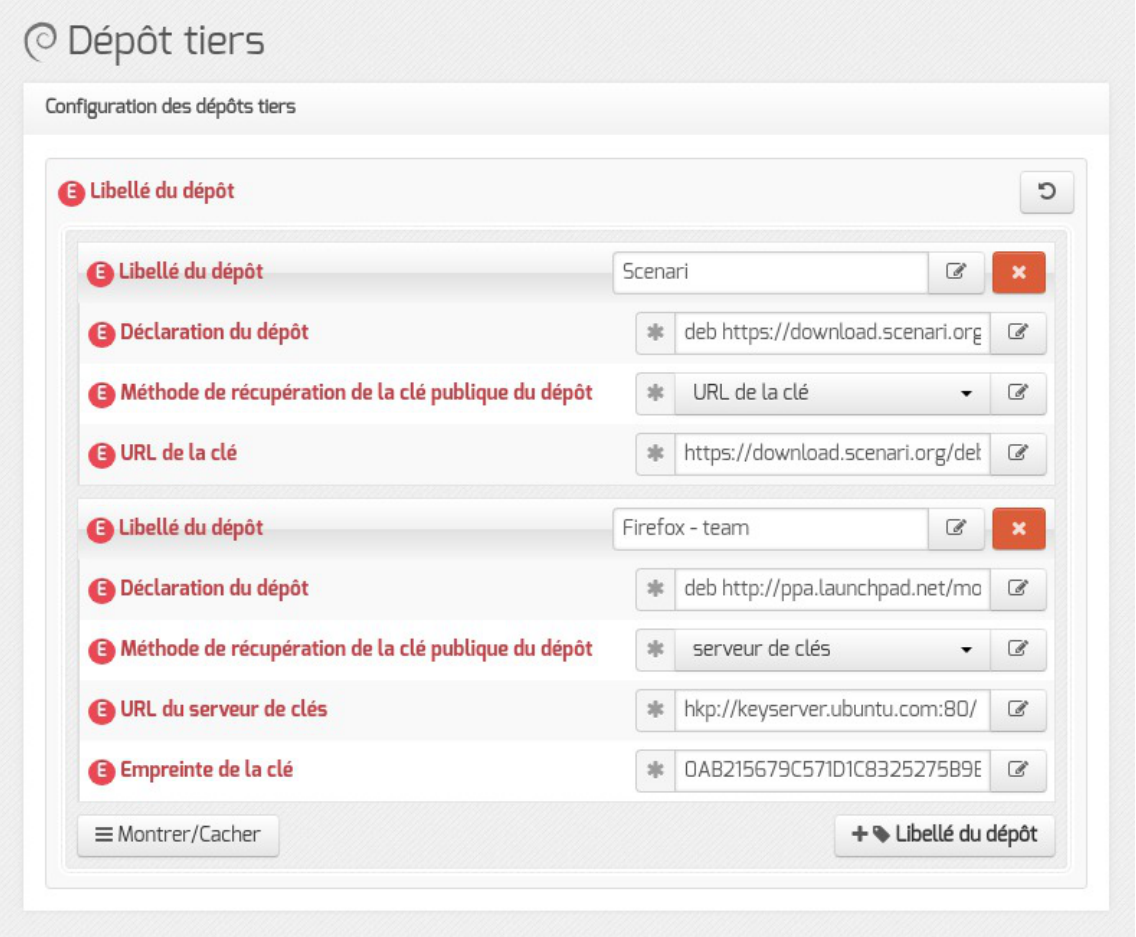
Intégration d'un certificat et d'une chaîne d'authentification [p.197]

4.11. Onglet Dépôt tiers

L'utilisation de dépôts tiers permet d'ajouter de nouveaux paquets absents des dépôts officiels, ou de proposer des versions plus récentes.

L'introduction de paquets tiers n'est pas sans risque et peut présenter des dangers pour votre système.

Cette onglet permet la prise en charge de dépôts de paquet de type `.deb`.



Un dépôt nouvellement configuré s'ajoute dans le fichier `/etc/apt/sources.list.d/additional.list`.

```
1 root@scribe:~# cat /etc/apt/sources.list.d/additional.list
2 #template genere par Maj-Auto
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
#
# dépôt Scenari
deb https://download.scenari.org/deb xenial main
# dépôt Firefox - team
deb http://ppa.launchpad.net/mozillateam/firefox-next/ubuntu xenial main
root@scribe:~#
```

L'ajout du dépôt est effectif après l'exécution de `Query-Auto` ou de `Maj-Auto`. L'installation d'un paquet supplémentaire s'effectue en ligne de commande.

Il est possible d'ajouter plusieurs dépôts en cliquant sur le bouton `+ Libellé du dépôt`.

La clé de signature d'un paquet permet de vérifier l'émetteur et l'intégrité du paquet, 2 méthodes sont disponibles pour récupérer la clé publique :

- serveur de clés ;
- URL de la clé.

Méthode de téléchargement de la clé publique : URL de la clé

Libellé du dépôt : `Scenari`

Déclaration du dépôt : `deb https://download.scenari.org/deb xenial main`

Méthode de récupération de la clé publique du dépôt : `URL`

URL de la clé : `https://download.scenari.org/deb/scenari.asc`

Méthode de téléchargement de la clé publique : serveur de clés

Libellé du dépôt : `Firefox - team`

Déclaration du dépôt : `deb http://ppa.launchpad.net/mozillateam/firefox-next/ubuntu xenial main`

Méthode de récupération de la clé publique du dépôt : `serveur de clés`

URL du serveur de clés : `hkp://keyserver.ubuntu.com:80/`

Empreinte de la clé : `0AB215679C571D1C8325275B9BDB3D89CE49EC21`

Si le serveur fonctionne conjointement avec le module Amon et que le proxy est activé, il faut paramétrer une exception pour le domaine du dépôt dans le champ `Liste des domaines de destination à ne pas authentifier` de l'onglet `Exceptions proxy`.

Prise en charge du nouveau dépôt

```
root@scribe:~# Query-Auto
Mise à jour le jeudi 13 avril 2017 11:01:17
*** scribe 2.6.1 (0000000A) ***

Configuration du dépôt Ubuntu avec la source test-eole.ac-dijon.fr
Configuration du dépôt EOLE avec la source test-eole.ac-dijon.fr
Configuration du dépôt Envole avec la source test-eole.ac-dijon.fr
Configuration du dépôt Scenari avec la source download.scenari.org
Configuration du dépôt Firefox - team avec la source ppa.launchpad.net
Action update pour root
Action list-upgrade pour root
Mise à jour OK
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
13 Aucun paquet à installer.
14 root@scribe:~#
```

Utiliser un fichier meta-release-lts alternatif

Le fichier `meta-release-lts` contient les adresses de tous les dépôts Ubuntu.

Dans un environnement sans accès direct à internet, on peut définir, via ce fichier, l'emplacement interne des dépôts à utiliser par `Upgrade-Auto`.

Dans l'interface de configuration du module, en mode expert, aller dans l'onglet `Dépôt tiers`.

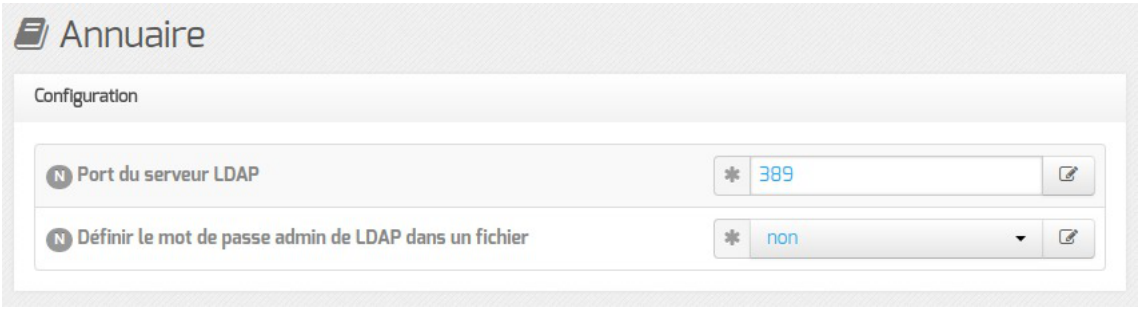


La variable `upgrade auto meta release repo` permet de définir où est téléchargé le fichier `meta-release-lts`.

4.12. 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

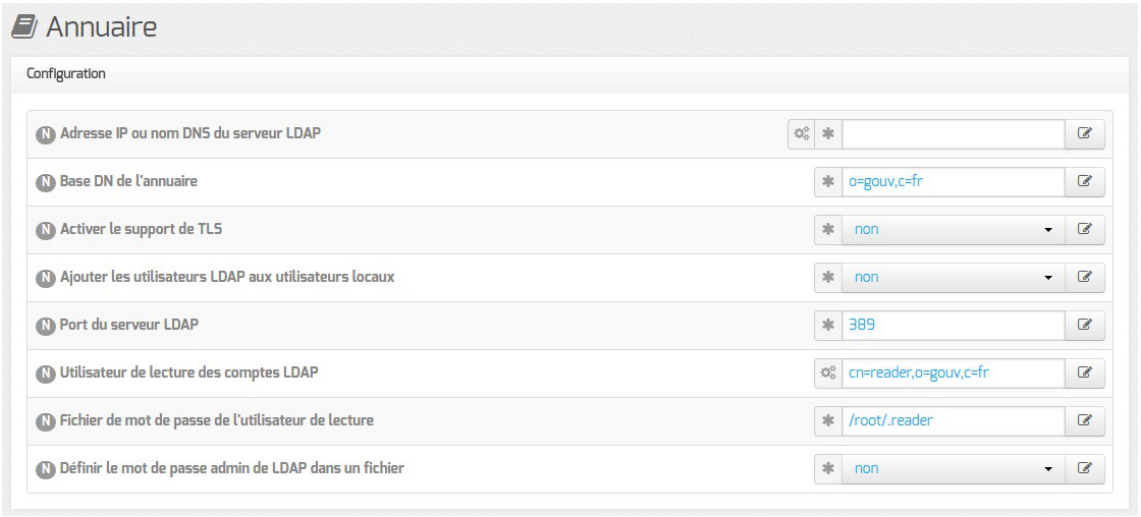


Lorsque l'annuaire est configuré comme étant local, l'onglet propose plusieurs paramètres :

- `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.475] 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.

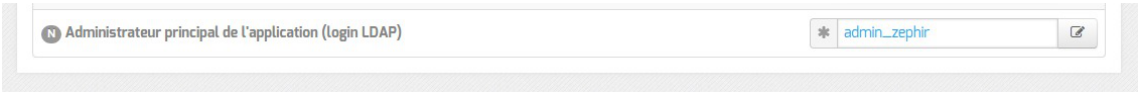
Annuaire LDAP distant

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Lorsque l'annuaire est configuré comme étant distant, l'onglet propose plusieurs 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.475] 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.

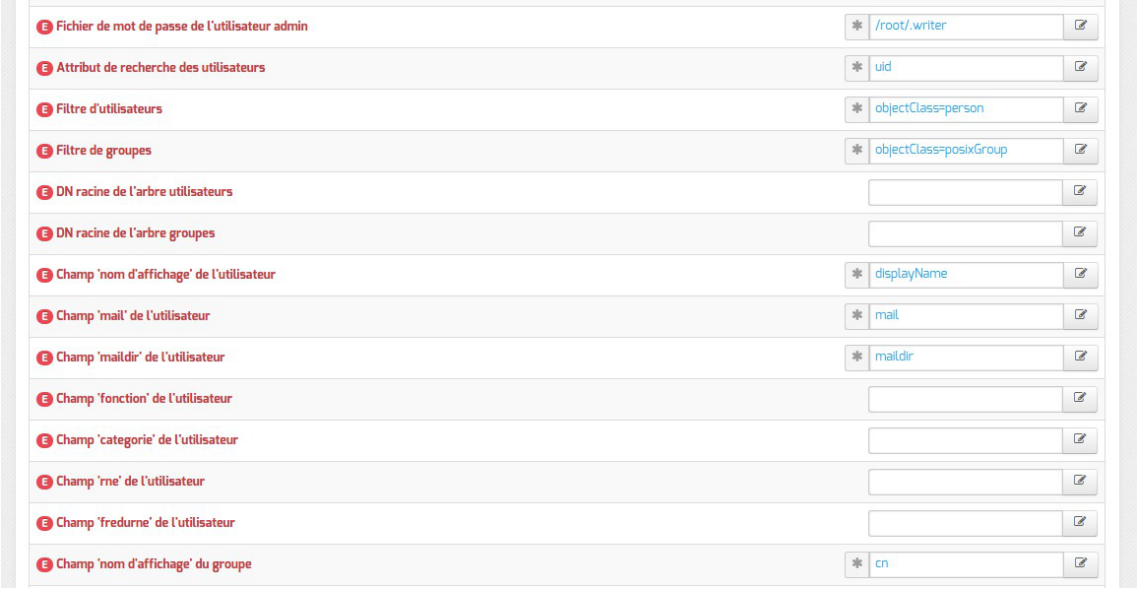
Mode expert



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

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 s'effectue dans l'onglet `Openldap`.

Voir aussi...

Onglet Openldap : Configuration du serveur LDAP local

4.13. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.467]. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

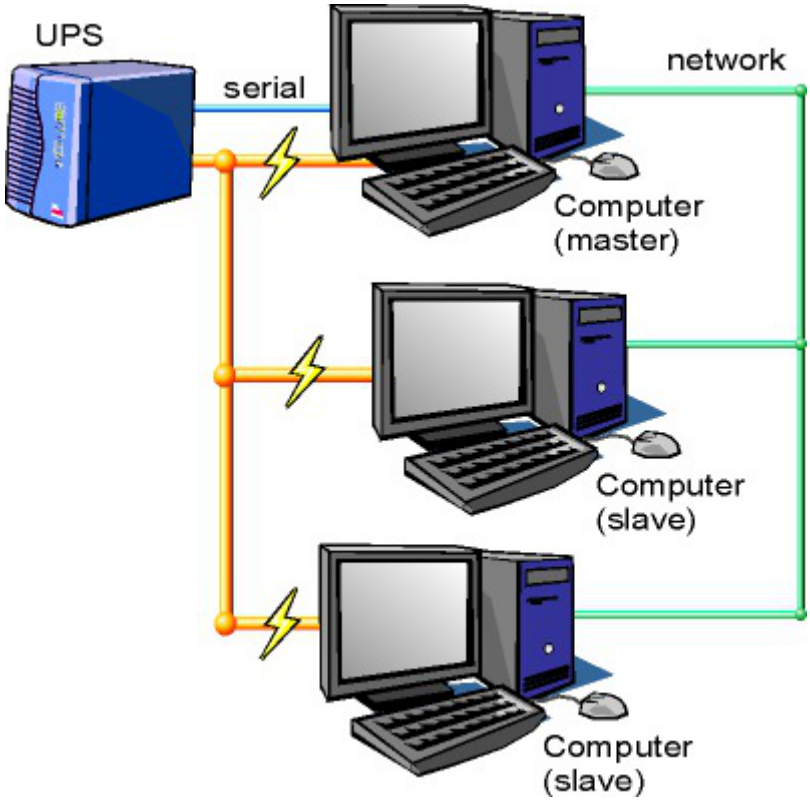


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

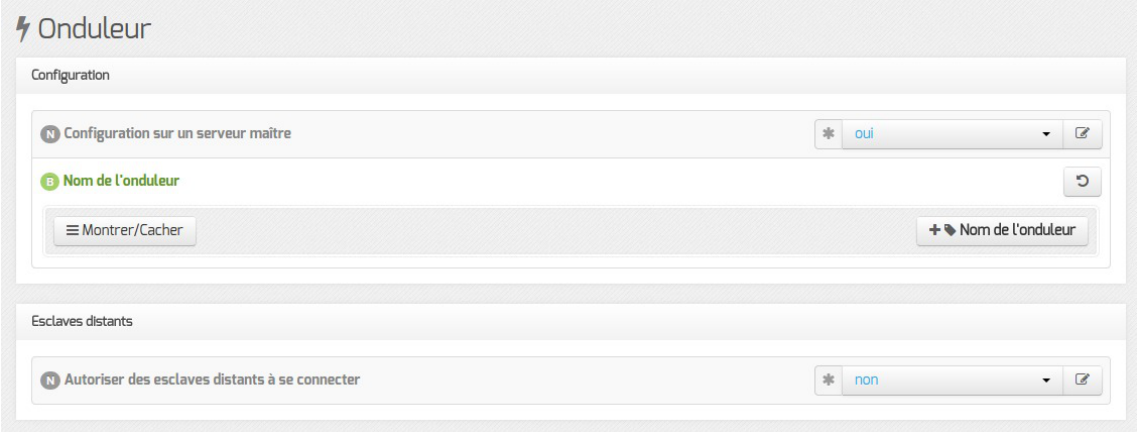
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

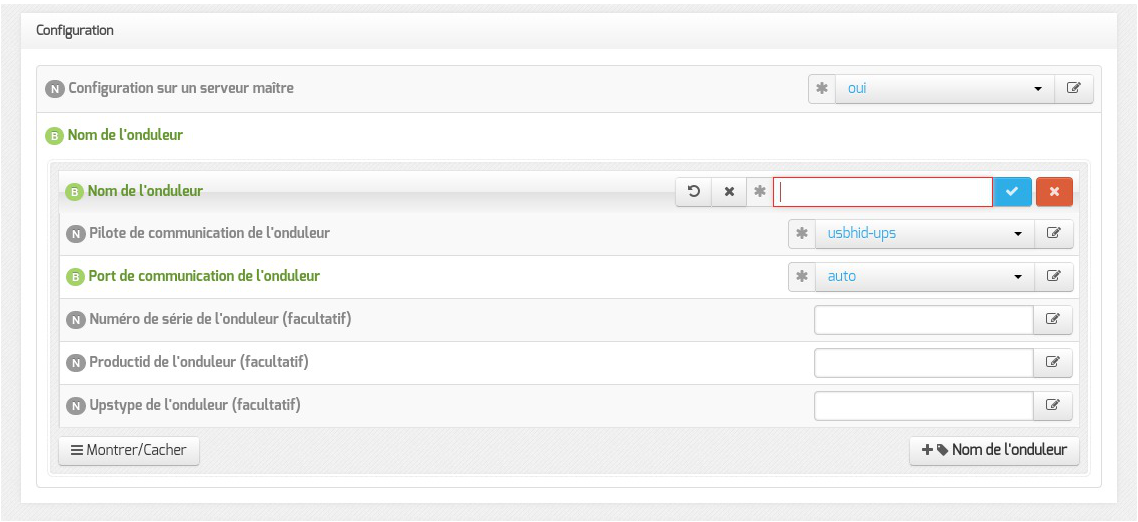
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

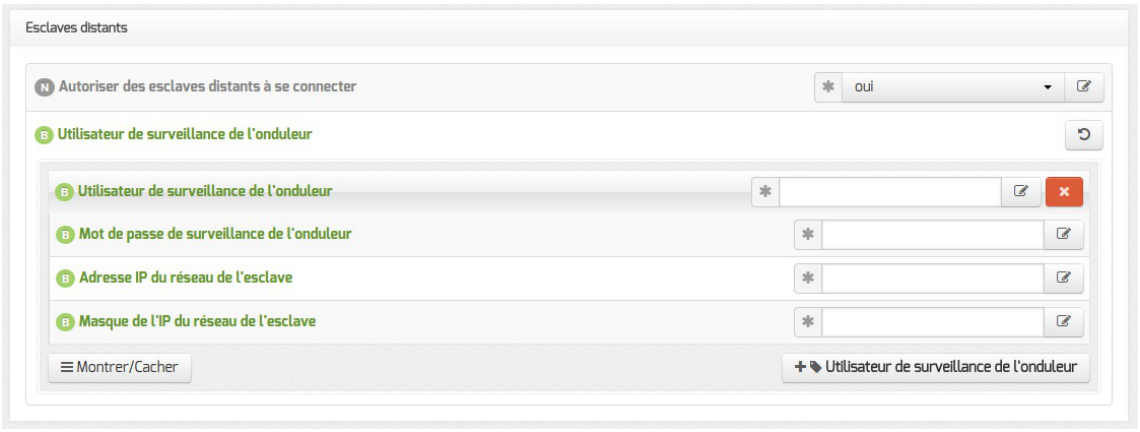
- Port de communication de l'onduleur : `auto`.

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`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/xenial/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` ;

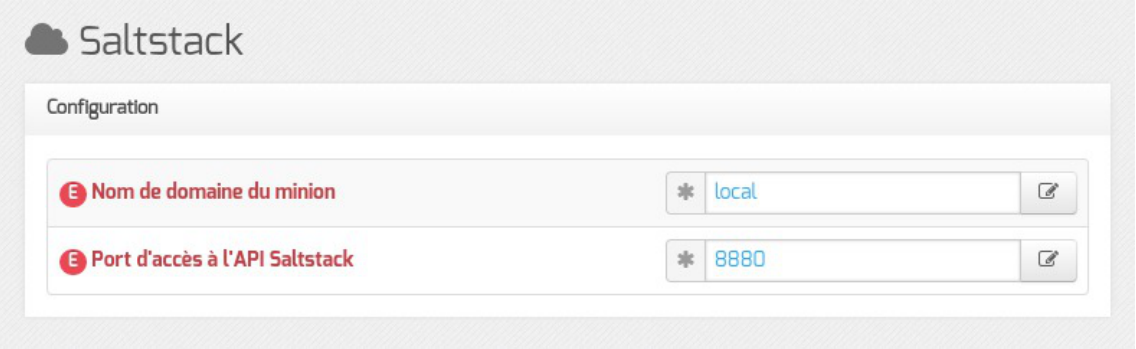
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

4.14. Onglet Saltstack

L'onglet `Saltstack` permet de personnaliser la configuration de Saltstack[p.472].

Il n'est accessible que si l'interface d'administration du module (EAD3) est activée dans l'onglet `Services`.



Le port d'écoute par défaut de l'API Saltstack est 8880.

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

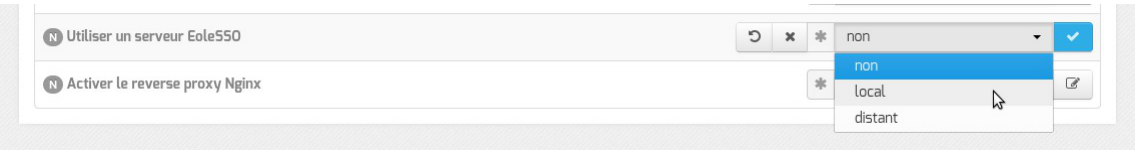
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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`.



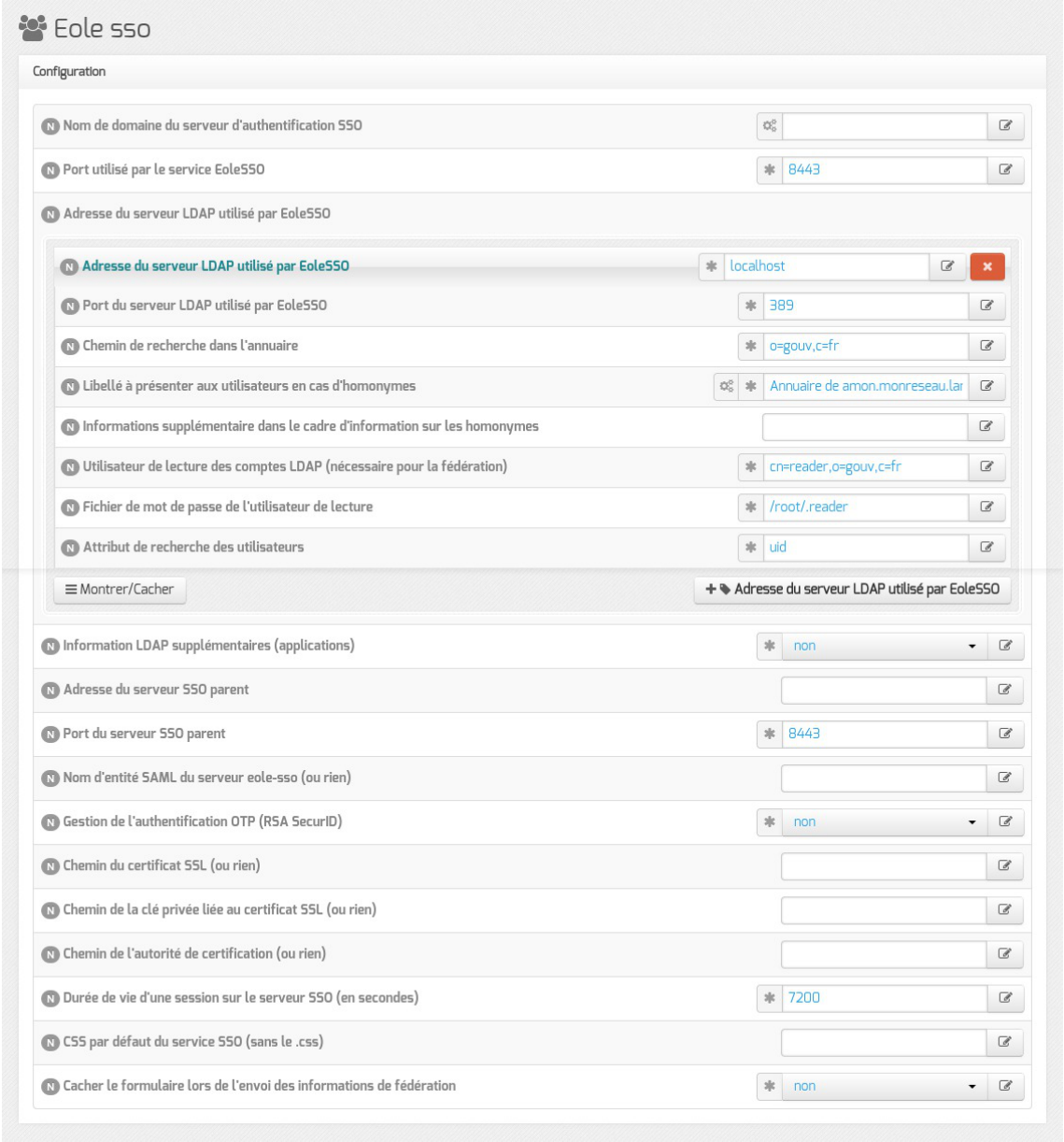
La variable `Utiliser un serveur EoleSSO` permet :

- `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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

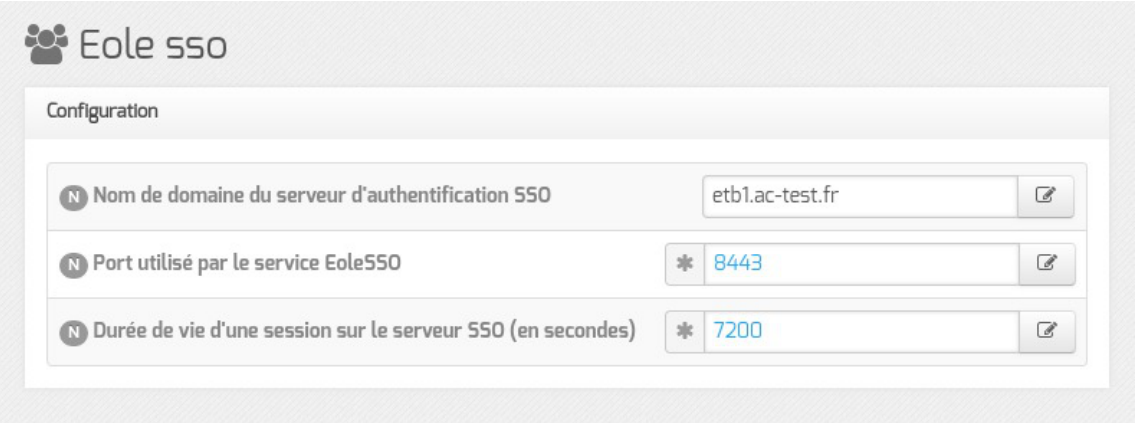
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Configuration d'un serveur EoleSSO distant

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.

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 modifier également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.463] 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 (basedn) ;
- 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[p.458] 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.468] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 en tant que 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 s'effectue par l'intermédiaire d'appels XML-RPC[p.477] 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.472] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.462] 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.472] (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

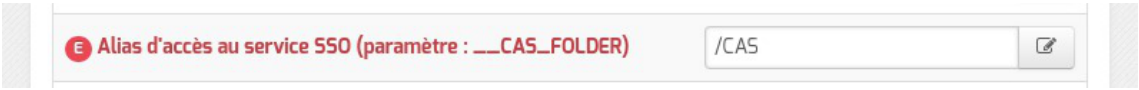
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

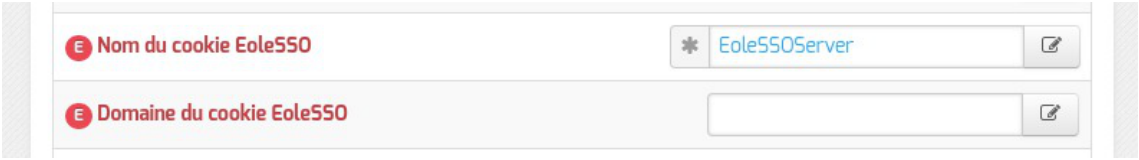
Options générales

En mode expert plusieurs nouvelles variables sont disponibles :

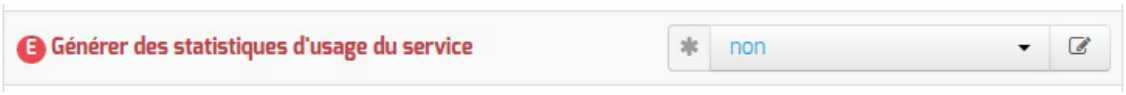


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP[p.463] ou keycloak[p.463].

  Cette variable est disponible uniquement à partir de la version 2.6.2 d'EOLE.

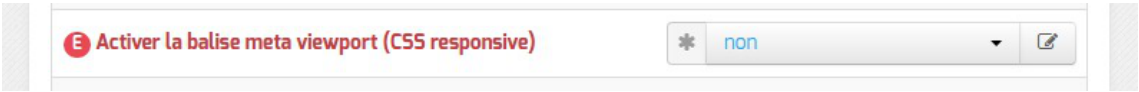


- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.



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

  Si ce paramètre est à `oui`, EoleSSO 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 disponibles 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 ;

- À partir d'EOLE 2.6.2, la variable `Nombre maximum de sessions en attente (backlog)`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

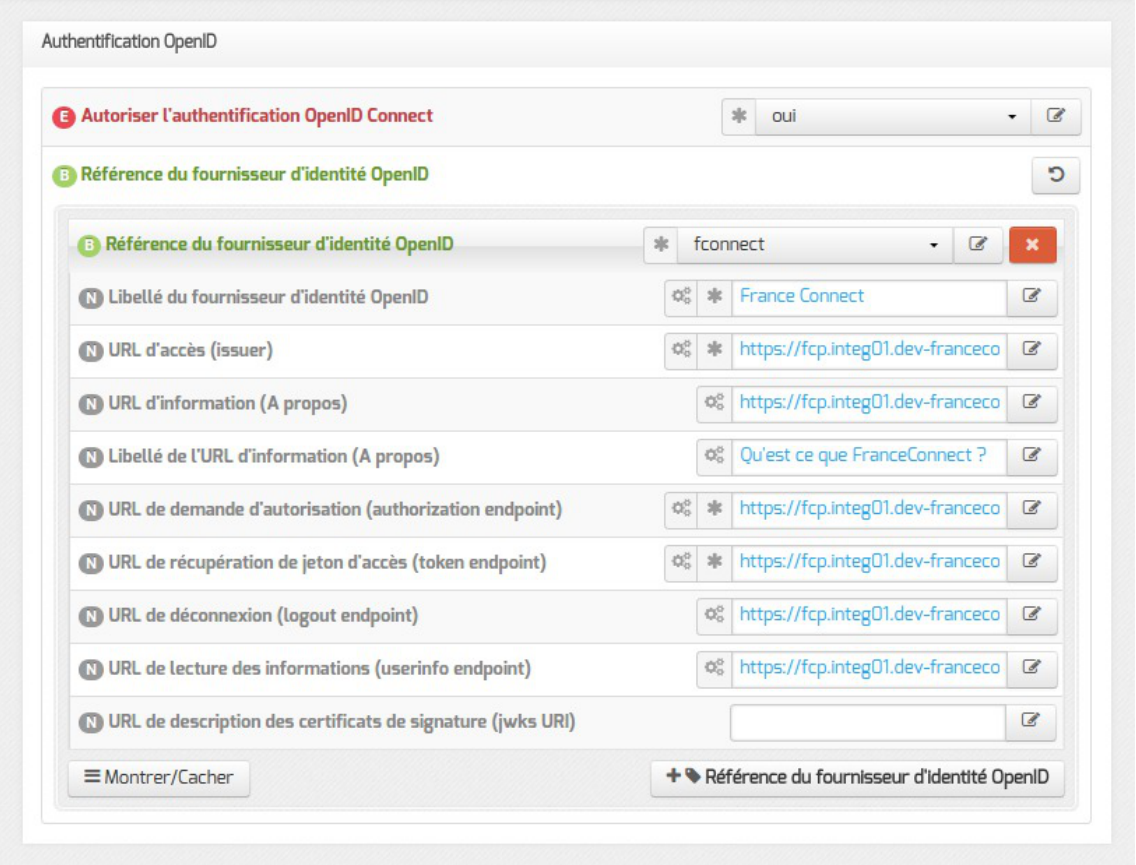
permet de définir la taille de la file d'attente des sessions.

Augmenter cette valeur est susceptible de résoudre des problèmes de lenteur voir de rejet des demandes d'authentification ;

- `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") ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

  - /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`.

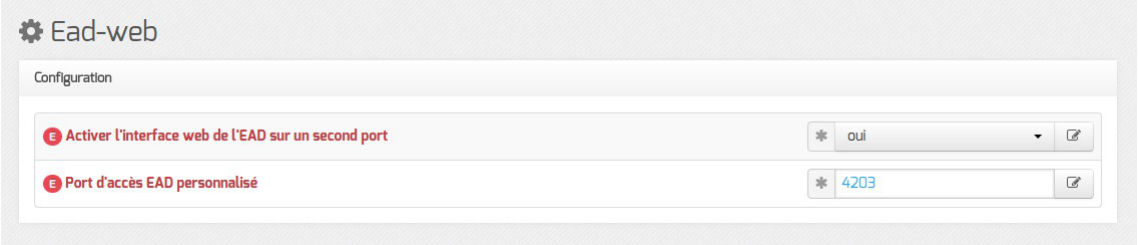
Voir aussi...

- Gestion des sources d'authentification multiples
- Compatibilité OpenID Connnect

4.16. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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...

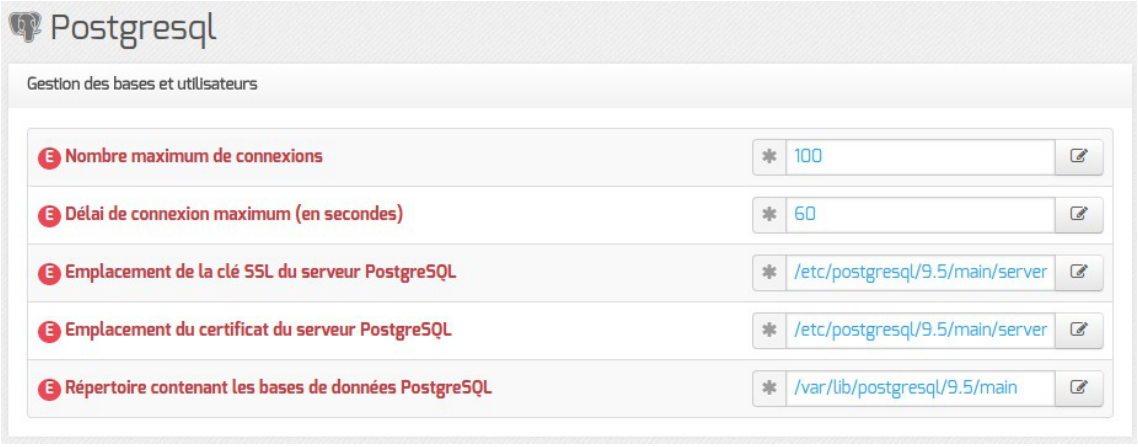
> Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur

4.17. Onglet Postgresql : Configuration du serveur PostgreSQL

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

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

Gestion des bases et utilisateurs



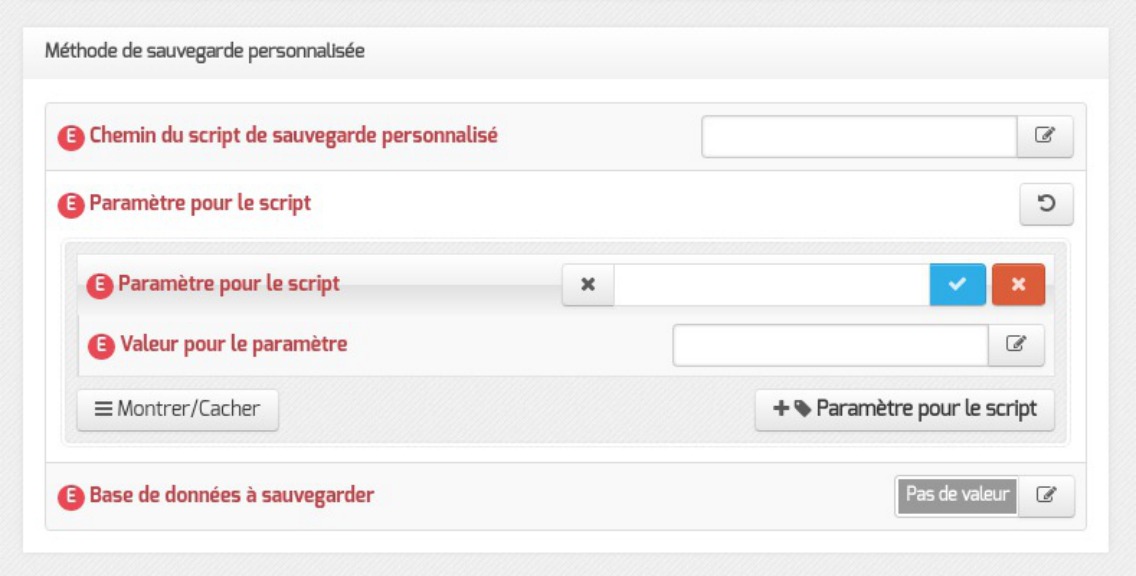
- `Nombre maximum de connexions` : permet de définir le nombre maximum de connexions concurrentes au serveur de base de données ;
- `Délai de connexion maximum (en secondes)` : permet de définir le temps maximum pour terminer l'authentification du client ;
- `Emplacement de la clé SSL du serveur PostgreSQL` : permet de changer le chemin par défaut de la clé SSL ;
- `Emplacement du certificat du serveur PostgreSQL` : permet de changer le chemin par

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

défaut du certification ;

- `Répertoire contenant les bases de données PostgreSQL` : par défaut `/var/lib/postgresql/9.5/main`.

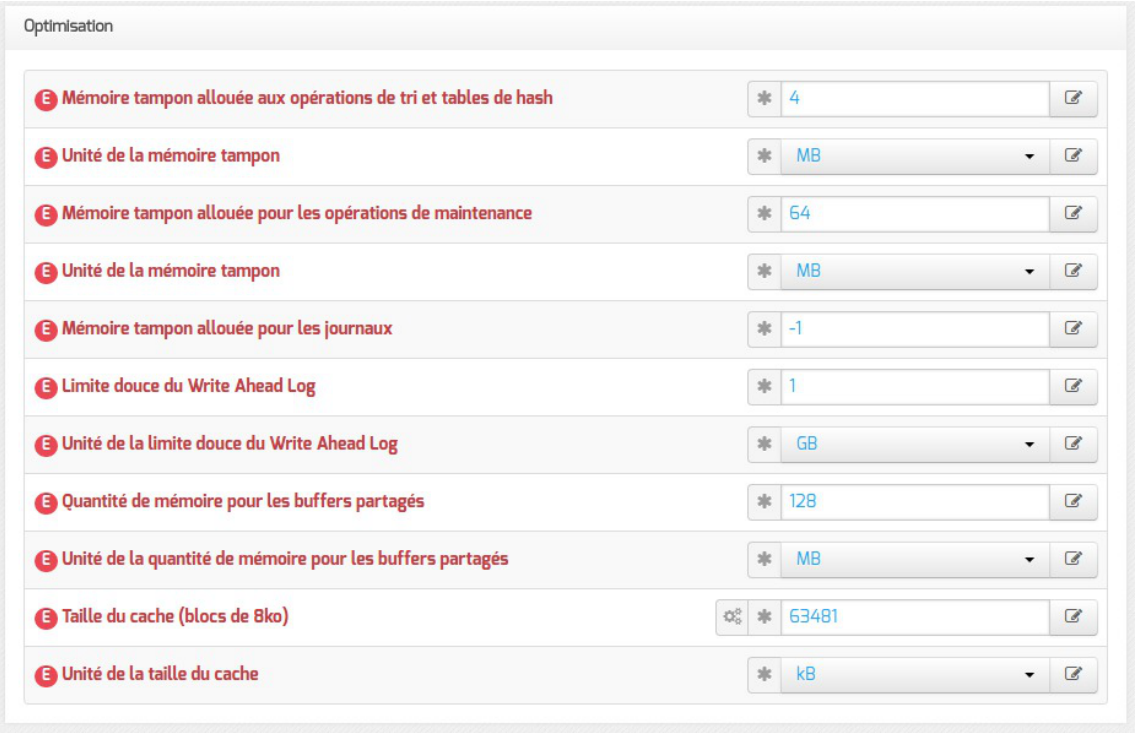
Méthode de sauvegarde personnalisée



- `Chemin du script de sauvegarde personnalisé` : emplacement personnalisé du script de sauvegarde prenant le pas sur la sauvegarde normale des bases de données spécifiées ;
- `Paramètre pour le script` : nom du paramètre à fournir au script de sauvegarde ;
  `Valeur pour le paramètre` : valeur à fournir au script pour le paramètre associé ;
  Il est possible d'ajouter autant de paramètres que souhaité en cliquant sur le bouton `+ Paramètre pour le script`.
- `Base de données à sauvegarder` : nom des bases de données à sauvegarder via le script personnalisé (ces bases seront exclues de la gestion des sauvegardes EOLE).

Optimisation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- `Mémoire tampon allouée aux opérations de tri et tables de hash` : quantité de mémoire allouée à chaque opération avant écriture sur le disque (par défaut 4MB sur PostgreSQL 9.5)
- `Unité de la mémoire tampon` : permet de choisir l'unité kB ou MB utilisée pour le paramètre ci-dessus ;
- Mémoire tampon allouée pour les opérations de maintenance ;
- `Unité de la mémoire tampon` : permet de choisir l'unité kB ou MB utilisée pour le paramètre ci-dessus ;
- `Mémoire tampon allouée pour les journaux` : quantité de mémoire allouée à chaque opération avant écriture sur le disque (par défaut 64MB sur PostgreSQL 9.5) ;
- `Limite douce du Write Ahead Log` : quantité de mémoire allouée avant écriture sur le disque (par défaut : -1, soit 1/32ème de la valeur de shared_buffers) ;
- `Unité de la limite douce du Write Ahead Log` : permet de choisir l'unité kB, MB ou GB utilisée pour le paramètre ci-dessus ;
- `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.

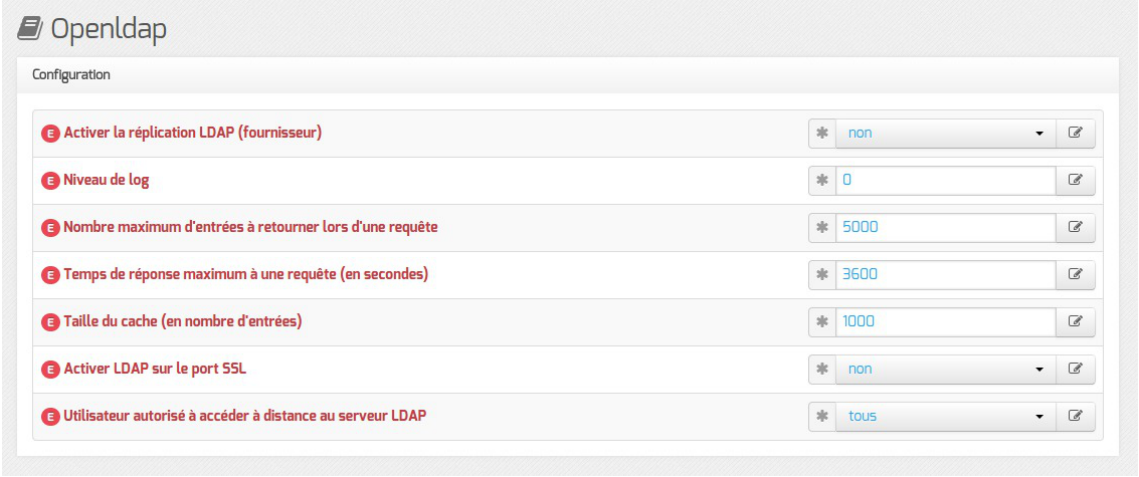
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

4.18. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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/xenial/en/man5/slapd.conf.5.html

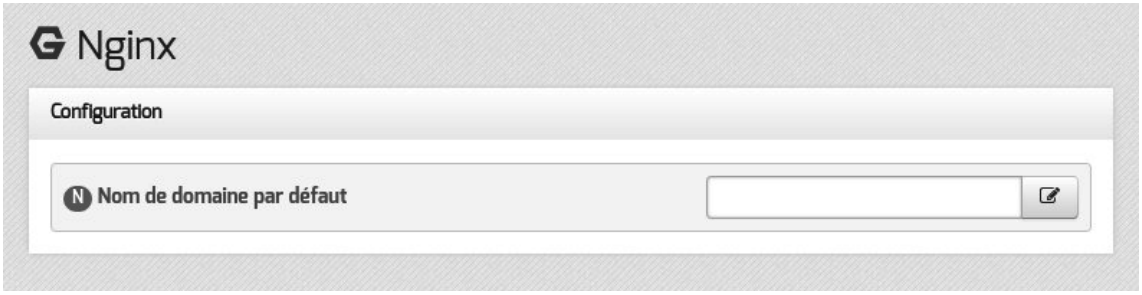
4.19. Onglet Nginx

L'onglet `Nginx` est disponible si au moins l'un des deux paramètres suivants est activé dans l'onglet

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Services :

- Activer la publication d'applications web par Nginx ;
- Activer le reverse proxy Nginx.



En mode normal, cet onglet permet de saisir permet de saisir le Nom de domaine par défaut vers lequel sera redirigé un client qui accède au serveur avec un nom de domaine non déclaré.

En mode expert, la configuration du service peut être affinée.



Dégrader la sécurité en HTTP

Il est possible de dégrader la sécurité du service Nginx en désactivant l'utilisation du HTTPS.

> Si le protocole HTTPS est désactivé, certaines applications critiques publiées par Nginx telles que l'outil d'administration EAD3 ou l'interface de configuration du module ne seront plus disponibles.

Longueur maximum pour un nom de domaine

Sur une installation recevant de très nombreuses connexions, diminuer la valeur de la Longueur maximum pour un nom de domaine (server_names_hash_bucket_size) pourra améliorer les performances du proxy inverse. La valeur optimale varie d'une installation à l'autre.

> Avec une valeur trop basse, le service Nginx refusera de démarrer et affichera un message d'erreur ressemblant à :
>
> `could not build the server names hash, you should increase server names hash bucket size: 32`
>
> Nginx Optimization : http://nginx.org/en/docs/http/server_names.html#optimization

Taille maximale des données reçues par la méthode POST

L'option Taille maximale des données reçues par la méthode POST (en Mo) permet

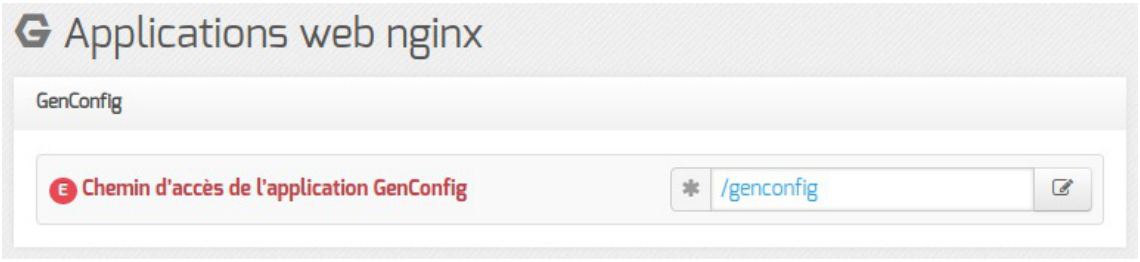
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

de spécifier la taille des données HTTP au delà de laquelle Nginx renverra une erreur (message : `Request Entity Too Large`).

> Sur les versions antérieures à 2.6.2, cette variable était située dans l'onglet `Reverse Proxy`.
>
> Dans le cas où, sur un module, le service `eole-web` est installé en plus du service `eole-reverseproxy` (ce qui est le cas sur les modules AmonEcole), le paramétrage de cette option s'effectue dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

4.20. Onglet Applications web nginx

L'onglet `Applications web nginx` n'est visible qu'après activation de l'une des applications utilisant ce service (interface de configuration du module, interface d'administration du module…) dans l'onglet `Services` en mode expert. Dans cet onglet `Activer la publication d'applications web par Nginx` doit également être à `oui` ce qui est le cas par défaut.



Le chemin d'accès des applications activées est personnalisable.

4.21. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.467].

Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ[p.457] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.473].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables*[p.462]*/DNAT*.

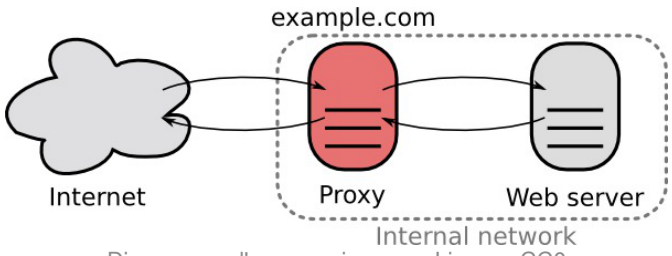


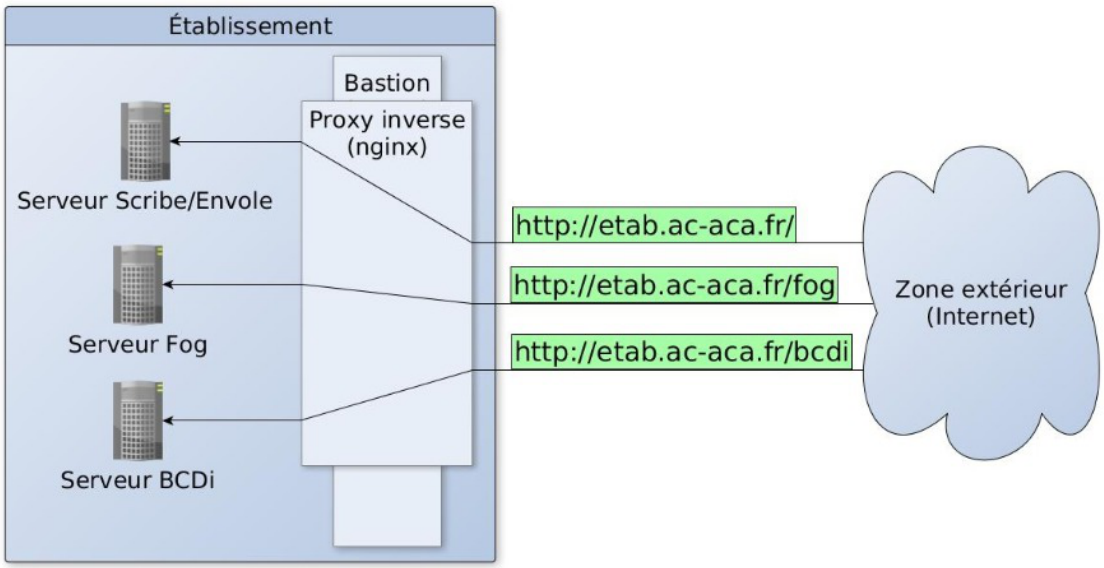
Diagramme d'un proxy inverse - Licence CC0

Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

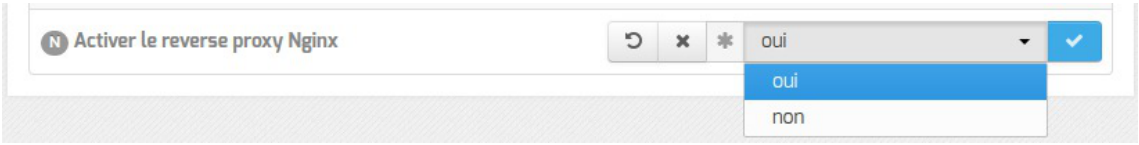
- serveur EoleSSO ;
- outil d'administration EAD[p.458] ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

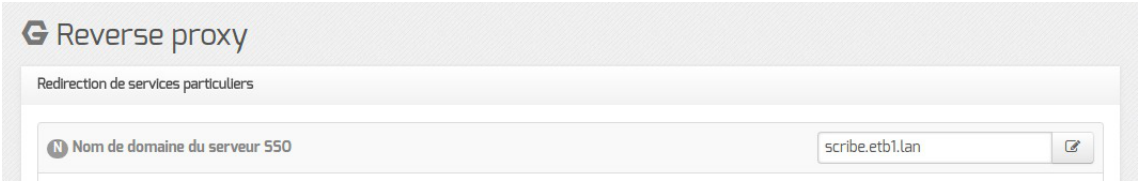
- application EOP ;
- protocole HTTP[p.461] ;
- protocole HTTPS[p.461].



Avant toute chose, le proxy inverse doit être activé dans l'onglet `Services` en passant `Activer le reverse proxy Nginx` à `oui`.

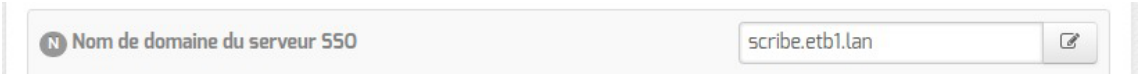


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

Redirection du service EoleSSO

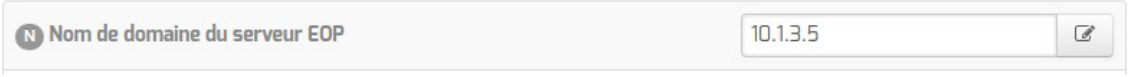


Pour rediriger le service EoleSSO (port 8443), il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

Cette fonctionnalité n'est disponible que dans le cas ou le serveur EoleSSO n'est pas activé en local (`Utiliser un serveur EoleSSO` doit être différent de `local` dans l'onglet `Services`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.476]).

Pour rediriger l'application EOP, il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

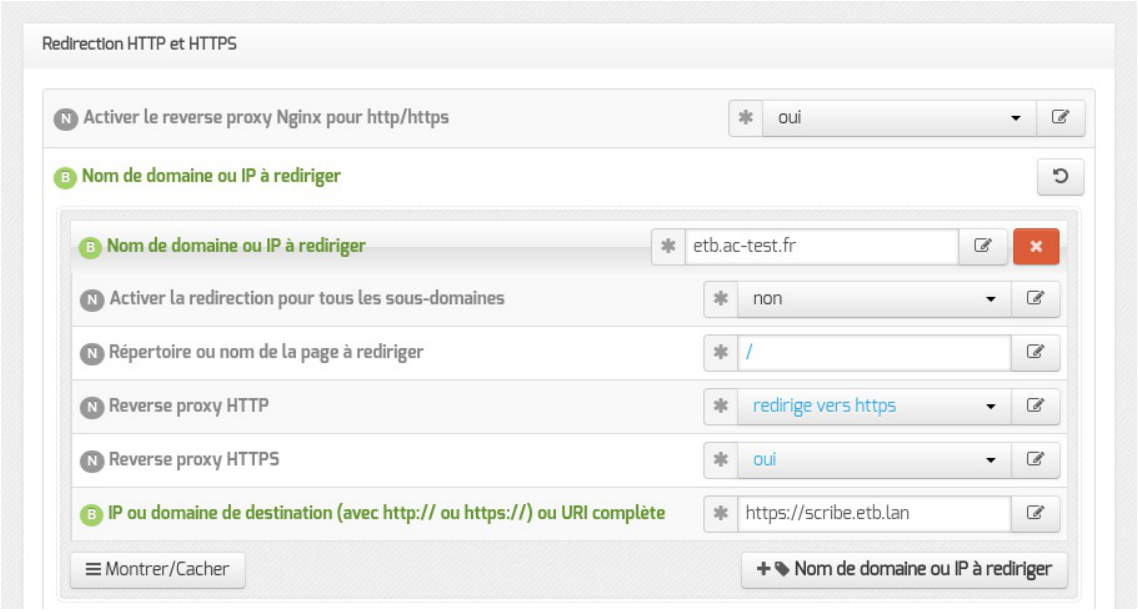
Redirection de l'interface d'administration EAD



Pour accéder de manière sécurisée à l'EAD d'un serveur depuis l'extérieur de l'établissement, il est recommandé :

- d'activer l'interface web de l'EAD du serveur interne sur un second port (4203 par défaut) dans l'onglet expert `Ead-web` de ce module ;
- d'activer la redirection sur le serveur faisant office de reverse proxy en configurant l'adresse IP ou le nom de domaine interne de la machine de destination et son port d'écoute.

Redirection HTTP et HTTPS



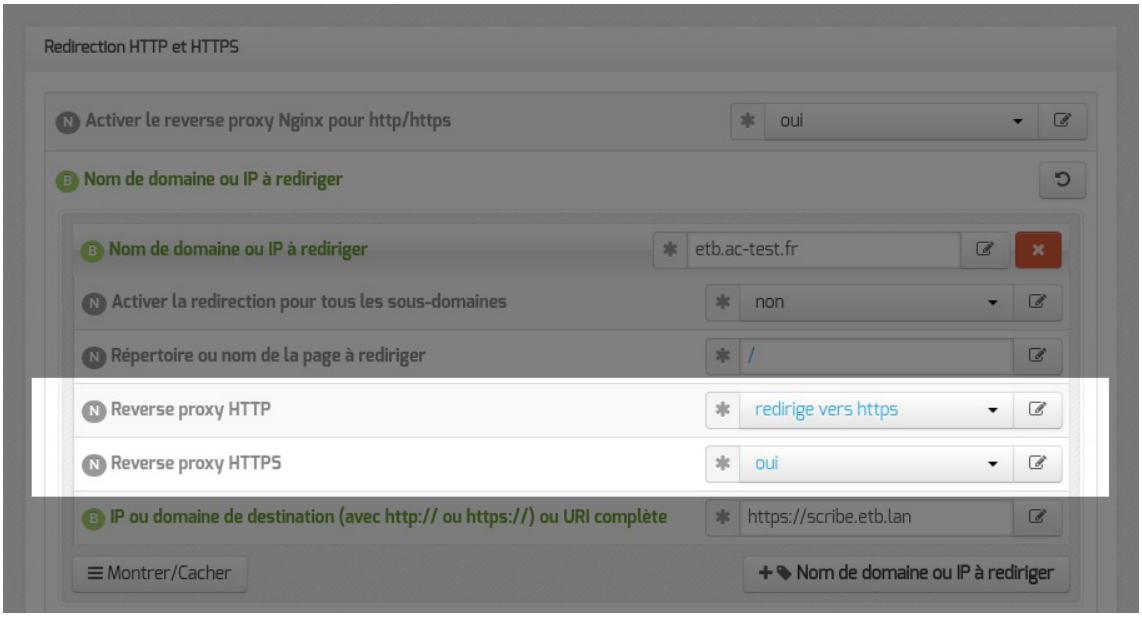
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- le `Nom de domaine ou IP à rediriger` : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- `Activer la redirection pour tous les sous-domaines` : cette variable est disponible à

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

partir de la version 2.6.2 d'EOLE, elle permet la prise en charge de tous les sous-domaines par le proxy inverse ;

- `Demander un certificat à Let's Encrypt pour ce domaine` ? : cette variable est disponible à partir de la version 2.6.2 d'EOLE si la redirection pour tous les sous-domaines n'est pas activé et que le certificat SSL est Let's Encrypt ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;
- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.476] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse `http://monetab.fr` sera automatiquement redirigé vers `https://monetab.fr`

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `+ Nom de domaine ou IP à rediriger`.

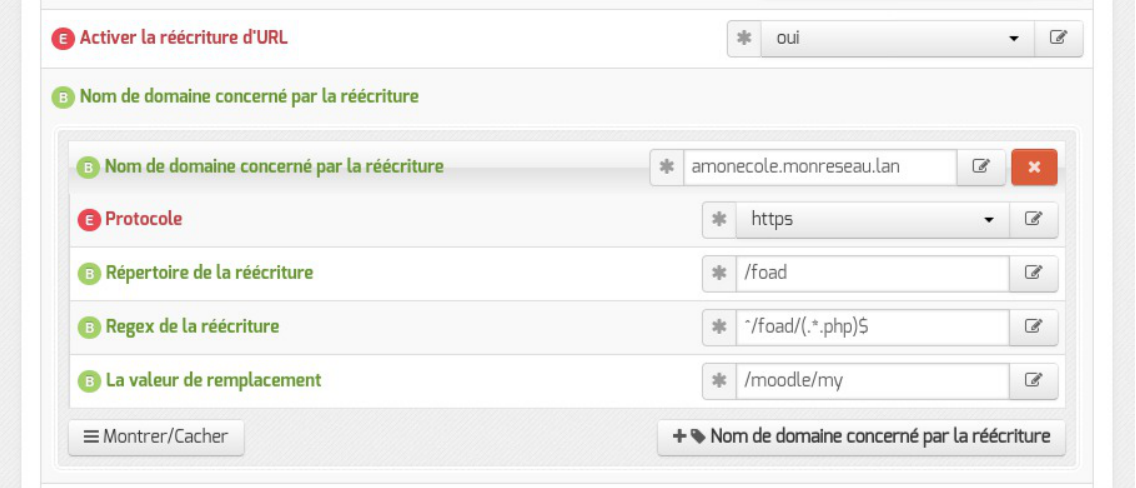


Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.470], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Réécriture d'URL

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

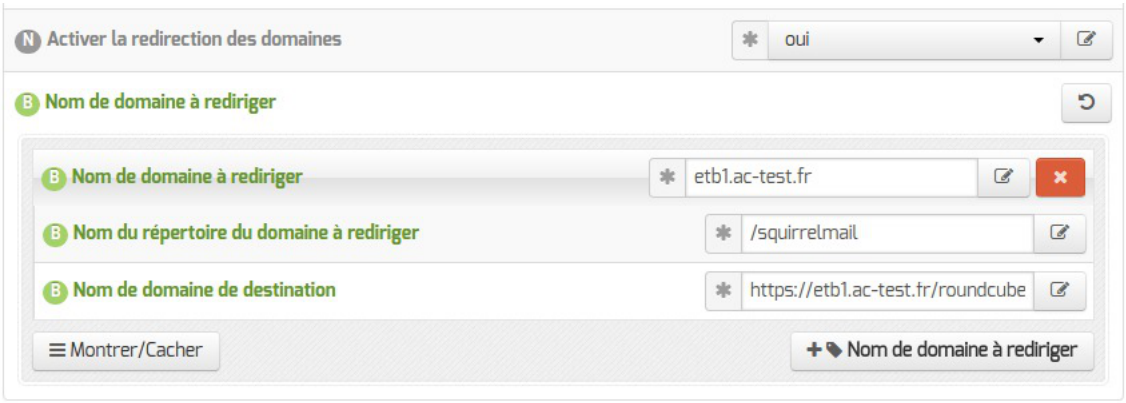
L'activation de la réécriture d'URL permet d'ajouter une expression rationnelle et une valeur de remplacement.



Il n'y a pas de lien automatique entre une "redirection" Nginx renseignée et une réécriture d'URL.

Pour que la réécriture d'URL s'applique à une règle il faut que le nom de domaine, le protocole et le répertoire de la réécriture correspondent aux paramètres saisis dans la règle de "redirection" renseignée.

Redirection de domaines



Le reverse proxy permet de rediriger automatiquement les utilisateurs voulant accéder à une page particulière vers une autre page.

L'exemple ci-dessus illustre le remplacement de SquirrelMail par Roundcube : si l'utilisateur cherche à accéder à l'adresse `http://etb1.ac-test.fr/squirrelmail/`, la page se recharge automatiquement avec l'URL de la nouvelle messagerie : `http://etb1.ac-test.fr/roundcube/`.

4.22. 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 courriers électroniques.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

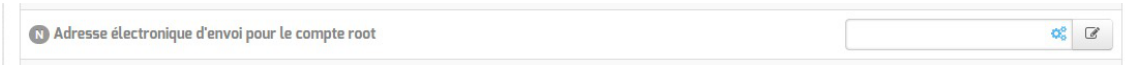
Serveur d'envoi/réception (SMTP)



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.

En mode expert, il est possible d'écraser les en-têtes 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

configuration définie dans `/etc/mailname`

- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs[p. 456] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

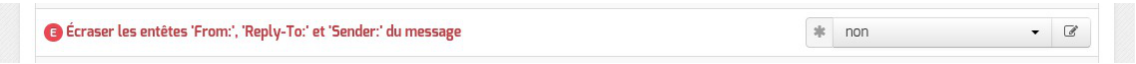
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

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

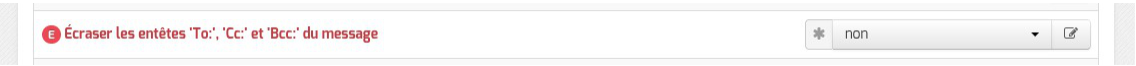
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

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 :

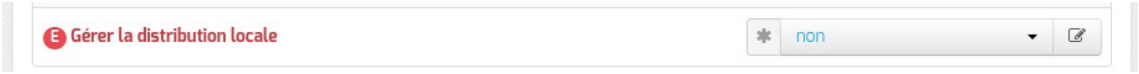
	system_mail_from_for_headers = non	system_mail_from_for_headers = oui
MAIL FROM	system_mail_from	system_mail_from
From :	user@conteneur.machine.domaine	system_mail_from
Reply-To :	user@conteneur.machine.domaine	system_mail_from
Sender :	user@conteneur.machine.domaine	system_mail_from

Réécriture du destinataire :

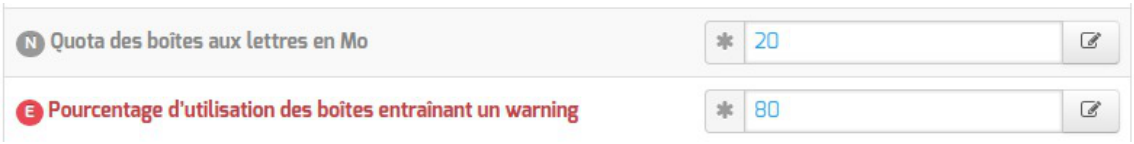
	system_mail_to_for_headers = non	system_mail_to_for_headers = oui
RCPT TO	system_mail_to	system_mail_to
To :	user@conteneur.machine.domaine	system_mail_to
Cc :	user@conteneur.machine.domaine	system_mail_to
Bcc :	user@conteneur.machine.domaine	system_mail_to

Par défaut, la distribution locale des messages est désactivée, sauf sur les modules Scribe et AmonEcole sur lesquels cette variable est masquée.

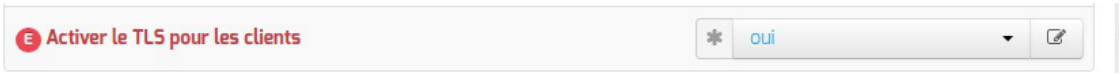
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Son activation (forcée sur les modules Scribe et AmonEcole) permet d'avoir un domaine local et un domaine privé.



Lorsqu'elle est activée, il est possible d'agir sur le quota et sur le pourcentage d'occupation des boîtes, qui entraîne un message électronique d'avertissement.



Le support du TLS[p.475] pour l'envoi de message est activé par défaut. La commande StartTLS[p.473] est supportée sur le port 25 (la connexion est initiée en mode non chiffré) et permet de basculer en TLS sur le port 465.

Passer cette variable à `non` rend l'authentification SMTP impossible ce qui empêche les utilisateurs d'envoyer des messages.

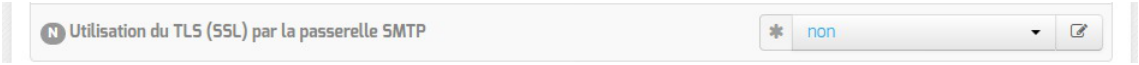
Relai des messages



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.475] pour l'envoi de message. Si la passerelle SMTP[p.472] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.473] (port 25) ou non (port 465).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



Configuration experte

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`

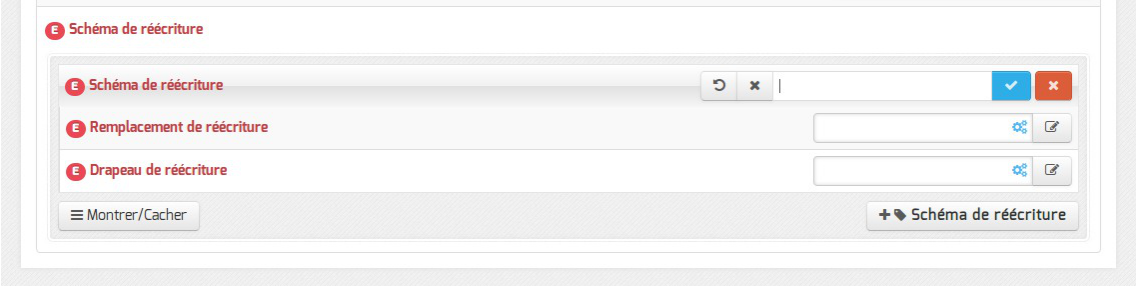
  Permet de désactiver l'envoi des logs.
- `Dupliquer les logs dans des fichiers`

  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`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

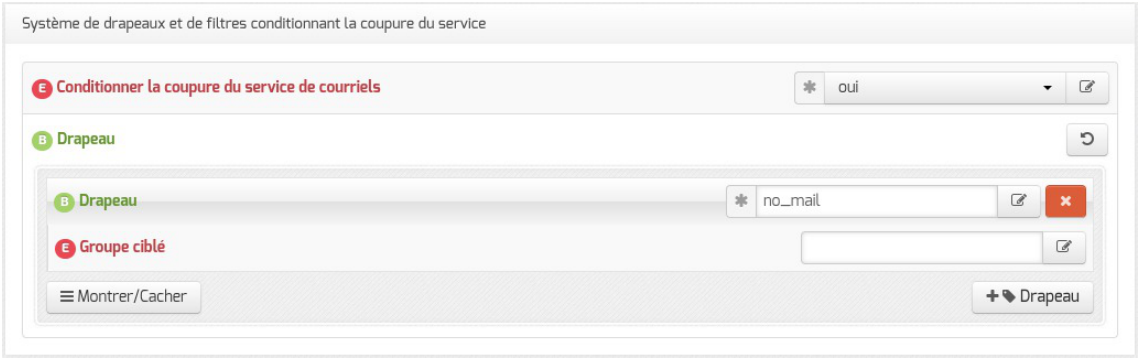
Fermeture de la messagerie

Le service de messagerie peut-être coupé sur la base de la présence d'un drapeau (fichier sur le système de fichiers).

Optionnellement, lorsque le serveur de messagerie est configuré pour accéder à l'annuaire (via la configuration du client LDAP), la coupure peut être conditionnée sur l'appartenance de l'utilisateur émetteur à un groupe de l'annuaire.

La configuration de la coupure repose sur l'identification du ou des drapeaux et sur l'identification optionnelle d'un groupe d'utilisateurs par drapeau.

L'accès à ces paramètres est conditionné à la variable `Conditionner la coupure du service de courriels`.



- `Drapeau` : nom du fichier qui sera recherché dans le répertoire `/var/run/eole/flags` par le serveur de courriels.

  La présence du fichier est interprétée par le serveur de courriels comme un ordre de coupure du service. La coupure affecte tous les utilisateurs sauf si le paramètre optionnel suivant est renseigné.
- `Groupe ciblé` : groupe de l'annuaire permettant de restreindre la coupure à ses membres.

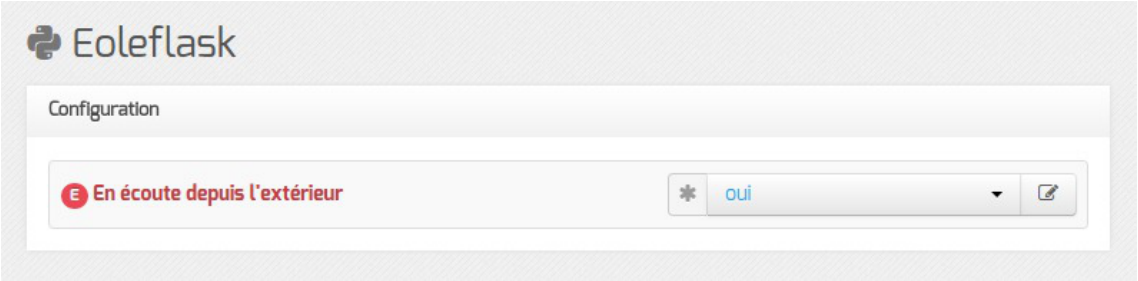
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sur EOLE 2.6.2, la création du drapeau n'est pas gérée automatiquement et le dossier `/var/run/eole/flags` n'existe pas par défaut.

Il est nécessaire de créer ce répertoire en cas d'activation de la fonctionnalité.

4.23. 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 (port 7000)

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.

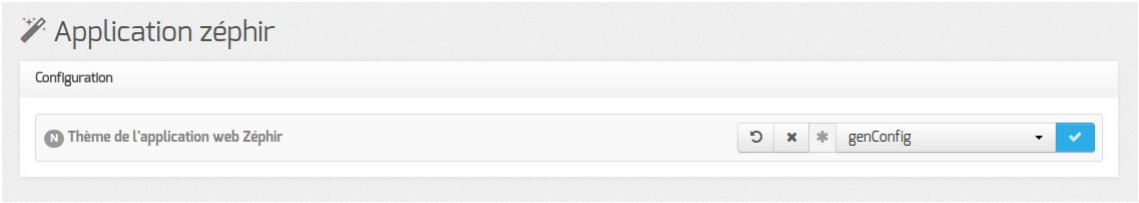


Vue de l'interface de configuration au travers d'un navigateur web (port 7000)

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.24. 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
  ```

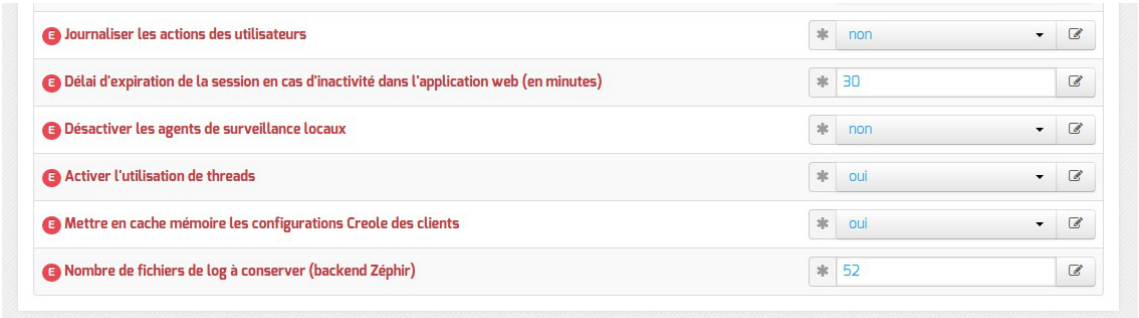
- copier le tout dans /usr/share/zephir/web/themes/monTheme :

  ```
  # 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.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `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.

5. Intégration d'un certificat et d'une chaîne d'authentification

L'exemple ci-dessous concerne la mise en œuvre d'un certificat et de sa chaîne d'authentification sur un serveur Zéphir. La procédure est en tout point identique sur un autre module pour la partie génération des fichiers. Elle diffère dans la mise en œuvre en fonction du service utilisation le certificat.

Génération du .pem

L'IGC de type ANTS nous fournit le certificat du serveur et sa clé privée dans un fichier p12 protégé par mot de passe.

À partir du fichier p12, il faut générer un certificat au format .pem ainsi qu'un fichier de clé :

```
thierry@hoth:~/certifs$ openssl pkcs12 -in certificate-56577-zephir01.p12 -out package.pem -nodes
Enter Import Password:
MAC verified OK
thierry@hoth:~/certifs$ ls
certificate-56577-zephir01.p12 package.pem
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

On obtient une concaténation en sortie, soit un fichier `package.pem`

Ce fichier contient à la fois les données de la clé et celles du certificat.

Pour être intégré au serveur Zéphir, il faut que la clé soit distincte du certificat (on duplique donc le fichier).

```
thierry@hoth:~/certifs$ cp package.pem zephir-01.pem
thierry@hoth:~/certifs$ cp package.pem zephir-01.key
```

Il faut alors éditer ces deux fichiers de façon à ne garder pour :

- le certificat, que le bloc BEGIN CERTIFICATE
- la clé, que le bloc BEGIN PRIVATE KEY

Il est possible de vérifier le contenu du fichier .pem avec la commande suivante :

```
thierry@hoth:~/certifs$ openssl x509 -noout -text -in zephir-01.pem
```

Cette commande permet notamment de vérifier que les alias d'enregistrement DNS sont corrects

```
X509v3 Subject Alternative Name:DNS:zephir-01.eole.e2.rie.gouv.fr,
DNS:zephir-vnf-ac.eole.e2.rie.gouv.fr, DNS:zephir-ac.eole.e2.rie.gouv.fr,
DNS:zephir-cerema.eole.e2.rie.gouv.fr
```

Vérification de la chaîne de certification

Pour vérifier que le certificat et la clé privée associée sont cohérents, il faut vérifier que les modulus de sortie sont identiques.

Pour la clé

```
thierry@hoth:~/certifs/zephir-01$ openssl rsa -noout -modulus -in
zephir-01.key
Modulus=C0E1FB7D415B4E6B8A6E0E51033B2FA3603BB4AD1C0D0A2C3D954865
FCE26AD71A140A
71E0608E75351DF54EE0490998972E7FE39E556910B8814FFC627C5E312CA0A1EB1
2F4067257CE6D305C49E49FE96CCAD7EB4E5CA6CA399B0D40F7827649F16D96C36C
794B7CB3C1EA5374E7B40A429E8440DEA484654859C9DB53DBF650EDF496BC61CE3
991A47DC80B7E186BD9FEA2846C3BC0D6EE13CA73C70B6193A20624F35CBBB864FF
964DD87A2E9E00A3EBBB44FA2C89B4C6879442814DAA30B198AF57F23ACAD3D86D4
E9BE998D09D01F31C388C781DC30DF6BA8CEAA49D219D9D46FE1
```

L'extraction s'est ici bien passée.

Pour le certificat

```
thierry@hoth:~/certifs/zephir-01$ openssl x509 -noout -modulus -in
zephir-01.pem
Modulus=C0E1FB7D415B4E6B8A6E0E51033B2FA3603BB4AD1C0D0A2C3D954865FCE
71E0608E75351DF54EE0490998972E7FE39E556910B8814FFC627C5E312CA0A1EB1
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
2F4067257CE6D305C49E49FE96CCAD7EB4E5CA6CA399B0D40F7827649F16D96C36C
794B7CB3C1EA5374E7B40A429E8440DEA484654859C9DB53DBF650EDF496BC61CE3
991A47DC80B7E186BD9FEA2846C3BC0D6EE13CA73C70B6193A20624F35CBBB864FF
964DD87A2E9E00A3EBBB44FA2C89B4C6879442814DAA30B198AF57F23ACAD3D86D4
E9BE998D09D01F31C388C781DC30DF6BA8CEAA49D219D9D46FE1
```

L'extraction s'est ici bien passée.

Il reste à vérifier que la chaîne complète est cohérente. On utilise alors le certificat racine qui valide la chaîne applicative qui valide elle-même le serveur.

```
thierry@hoth:~/certifs/zephir-01$ openssl verify -verbose -CAfile <(cat chaineACs-ANTSv3-SA-1.pem AC-ANTSv3-Racine-1.pem )
zephir-01.pemzephir-01.pem: OK
```

Dépôt du certificat et de la chaîne de certification sur le module

Le certificat généré ainsi que la clé doivent être copiés sur la machine cible sous `/etc/ssl/certs`. Cependant, le serveur Zéphir veut la présence de la chaîne intermédiaire dans un fichier .crt.

```
thierry@hoth:~/certifs$ cat zephir-01.pem chaineACs-ANTSv3-SA-1.pem > zephir.crt
```

De plus, la clé privée et la chaîne doivent être concaténées dans le fichier pem.

```
thierry@hoth:~/certifs$ cat chaineACs-ANTSv3-SA-1.pem zephir-01.key > zephir.pem
```

On déploie le tout sur le serveur Zéphir de destination :

```
thierry@hoth:~/certifs$ scp zephir.crt root@zephirDestination:/etc/ssl/certs/zephir.crt
thierry@hoth:~/certifs$ scp zephir-01.key root@zephirDestination:/etc/ssl/certs/zephir.key
thierry@hoth:~/certifs$ scp zephir.pem root@zephirDestination:/etc/ssl/certs/zephir.pem
```

Il faut aussi fournir les certificats CA de la chaîne de certification (cf .zip attaché) sous `/etc/ssl/local_ca`.

```
thierry@hoth:~/certifs$ scp AC-ANTSv3-Racine-1.pem root@zephirDestination:/etc/ssl/local_ca/
thierry@hoth:~/certifs$ scp chaineACs-ANTSv3-SA-1.pem root@zephirDestination:/etc/ssl/local_ca/
```

Configuration sur le module Zéphir

Dans l'onglet Certificats SSL de l'interface de configuration du module il faut remplir les champs suivants :

#fixme capture d'écran

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Nom long du certificat SSL par défaut (server_cert) => fichier déposé sous /etc/ssl/certs soit zephir.crt ici (indiquer le chemin complet)
- Nom long de la clé privée du certificat SSL par défaut (server_key) => fichier déposé sous /etc/ssl/certs soit zephir.key ici (indiquer le chemin complet)
- Nom long du certificat Privacy Enhanced Mail (server_pem) => fichier déposé sous /etc/ssl/certs soit zephir.pem ici (indiquer le chemin complet)
- Nom DNS du serveur (de la forme nom-serveur.ac-acad.fr) (CN=) (ssl_server_name) => nom FQDN du serveur soit zephir-01.eole.e2.rie.gouv.fr (indiquer le chemin complet)
- Nom DNS/IP alternatif du serveur ssl_subjectaltname : tous les noms DNS renseignés dans le certificat serveur.

Installation de l'autorité racine sur le module

Dans le cas où l'autorité racine n'est pas reconnue par défaut sur le serveur il faut la recopier sur le module.Ce qui est le cas pour la chaîne de certification ANTS.

```
thierry@hoth:~/certifs$ scp AC-ANTSv3-Racine-1.pem
root@zephirDestination:/usr/local/share/ca-certificates/medde/AC-ANTSv3-Raci
```

L'extension crt est obligatoire

Puis, depuis le module, rafraîchir la liste des certificats

```
root@eolebase:/usr/local/share/ca-certificates# update-ca-certificates
Updating certificates in /etc/ssl/certs...
WARNING: Skipping duplicate certificate ACInfraEducation.pem
WARNING: Skipping duplicate certificate ACInfraEducation.pem
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

L'enregistrement du module auprès du serveur Zéphir est désormais possible à l'aide du script `enregistrement_zephir`.

Voir aussi...

Onglet Certificats ssl : gestion des certificats SSL [p.155]

6. Mise en place de l'agrégation de liens Ethernet (bonding)

Activation de l'agrégation de liens Ethernet

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'activation de l'agrégation de liens Ethernet[p.453] s'effectue en déclarant au minimum deux interfaces réseau dans la variable experte `Nom de l'interface réseau` dans un onglet `Interface-n`.



L'utilisation de l'agrégation de liens Ethernet[p.453] nécessite de disposer d'un Commutateur réseau[p.455] compatible et configuré.

Pour configurer l'agrégation de liens Ethernet, il faut rafraîchir l'onglet (cliquer sur un autre onglet et revenir #21016 [https://dev-eole.ac-dijon.fr/issues/21016]).

Configuration de l'agrégation de liens Ethernet



Il est possible de choisir le mode d'agrégation en accord avec la configuration de votre Commutateur réseau[p.455] parmi :

- balance-rr ;
- active-backup ;
- balance-xor ;
- broadcast ;
- 802.3ad ;
- balance-tlb ;
- balance-alb.

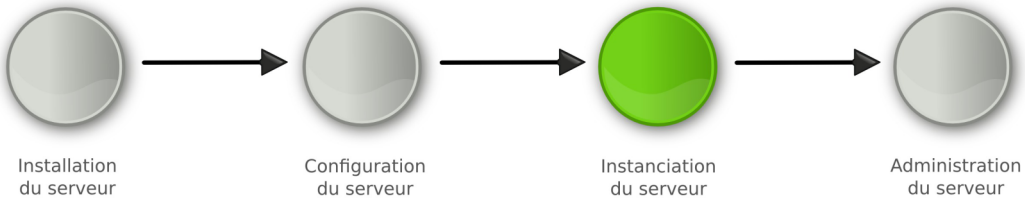
Les autres variables permettent d'adapter la sensibilité de la détection de la perte et du retour de lien.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 7

Instanciation du module

La troisième des quatre phases



Instanciation

- 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` .

1. Principes de l'instanciation

Les modules EOLE sont livrés avec un ensemble de **templates**.

Les templates[p.475] sont les fichiers de configuration de chacun des logiciels utilisés. Ils sont pré-paramétrés et contiennent des variables.

Parallèlement les modules fournissent des dictionnaires décrivant l'ensemble de ces variables, comme expliqué dans la phase de configuration.

L'instanciation consiste à remplacer les variables par les valeurs renseignées dans le fichier `/etc/eole/config.eol` et à copier les fichiers vers leur emplacement cible.

Si des patchs EOLE[p.469] ont étés créés pour personnaliser le serveur, ils seront pris en compte durant cette phase.

Voir aussi...

Personnalisation du serveur à l'aide de Creole [p.333]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Lancement de l'instanciation

Pour lancer l'instanciation, il faut utiliser la commande `instance`.

Le compte rendu d'exécution est dans le fichier `/var/log/creole.log`.

En plus de remplacer les variables par les valeurs renseignées dans le fichier `/etc/eole/config.eol` et de copier les fichiers vers leur emplacement cible, l'instanciation :

- arrête et redémarre des services ;
- lance des commandes ;
- effectue certaines tâches en fonction des réponses aux dialogues proposés.

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

La commande `instance` utilise le fichier `/etc/eole/config.eol`. Il n'est plus nécessaire de spécifier le nom du fichier à utiliser.

2.1. Les mots de passe

Mots de passe à l'installation

Lors de l'installation, les mots de passe des comptes `root` et `eole` sont générés aléatoirement selon les critères suivants :

- 12 caractères ;
- au moins une majuscule ;
- au moins un chiffre ;
- pas de caractère ambigu (l ou 1, 0 ou O, ...).



Après installation, la connexion SSH par mot de passe pour l'utilisateur `root` est permise.

Cependant, le mot de passe généré aléatoirement de l'utilisateur `root` est affiché uniquement sur la console, il faut donc avoir un accès physique à la machine pour en prendre connaissance.

Mots de passe à l'instanciation

Lors de l'instanciation, la modification des mots de passe est demandée pour les comptes :

- de l'utilisateur `root` ;
- du ou des utilisateurs à droits restreints (`eole`, `eole2`, ...) ;
- de l'utilisateur `admin` sur les modules Scribe, Horus et AmonEcole ;
- de l'utilisateur `admin_zephir` sur le module Zéphir ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- de l'utilisateur `Administrator` sur le module Seth avec le rôle de contrôleur de domaine principal.

Sur un module Amon, en cas d'utilisation d'un réseau pédagogique et d'un réseau administratif, le second administrateur (`eole2`) permet d'administrer le réseau pédagogique.

Par défaut, le système vérifie la pertinence des mots de passe. Pour cela, il utilise un système de classes de caractères :

- les lettres en minuscule [a-z] ;
- les lettres en majuscule [A-Z] ;
- les chiffres [0-9] ;
- les caractères spéciaux (exemple : $*ùµ%£, ; : !§/. ?).

Il faut utiliser différentes classes de caractères pour que le mot de passe soit considéré comme valide. Il n'est pas possible de réutiliser le mot de passe par défaut fourni à l'installation.

Par défaut, voici les restrictions :

- une seule classe de caractères : impossible ;
- deux classes de caractères : 9 caractères ;
- trois et quatre classes : 8 caractères ;
- un mot de passe commençant par une majuscule ou se terminant par un chiffre n'est pas considéré comme un mot de passe utilisant plusieurs classes de caractères ;
- ne pas utiliser le login comme partie du mot de passe.

Cette configuration est modifiable durant l'étape de configuration, en mode expert (onglet `Système`).

Il s'agit de comptes d'administration donc sensibles sur le plan de la sécurité. Il est important de renseigner des mots de passe forts.

Cet article du CERTA[p.455] donne une explication détaillée sur la stratégie des mots de passe.

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

2.2. Création d'un deuxième administrateur

À l'instance il est possible de créer un compte pour un nouvel administrateur.

```
Créer un nouvel administrateur eole2 ? [oui/non]
[non] : non
```

Des comptes administrateurs supplémentaires peuvent être créés en dehors de l'instance grâce à la commande `add_restricted_admin`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3. Activation automatique de la mise à jour hebdomadaire

À la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée.

La mise à jour permet de maintenir votre serveur avec le niveau de fonctionnalité le plus récent et surtout de bénéficier des dernières corrections. Certaines corrections peuvent combler des failles de sécurité importantes, il est donc important de les appliquer aussitôt qu'elles sont publiées.

Il est conseillé d'effectuer la mise à jour immédiatement, comme proposé à la fin de l'instance.

```
Une mise à jour est recommandée
Voulez-vous effectuer une mise à jour via le réseau maintenant ? [oui/non]
```

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.

Voir aussi...

> Gestion des tâches planifiées eole-schedule [p.384]

2.4. Le redémarrage

Il est possible qu'un redémarrage soit proposé à la fin de l'instanciation.

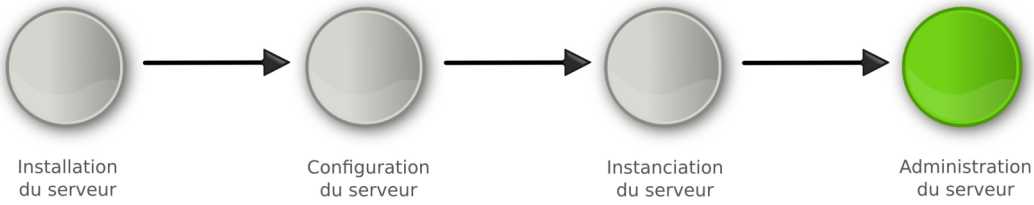
Si le noyau (kernel) a été mis à jour, le serveur doit redémarrer pour pouvoir l'utiliser. Dans ce cas, la question suivante apparaîtra :

```
Un redémarrage est nécessaire
Faut-il l'effectuer maintenant ? [oui/non]
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 8

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.

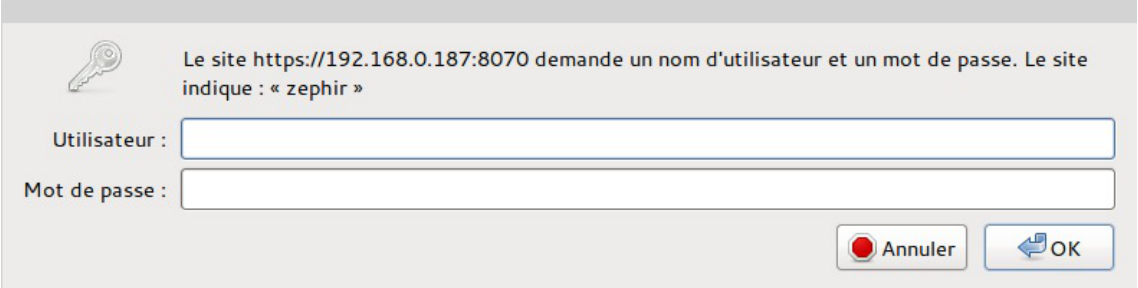
Accès à l'interface web Zéphir

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



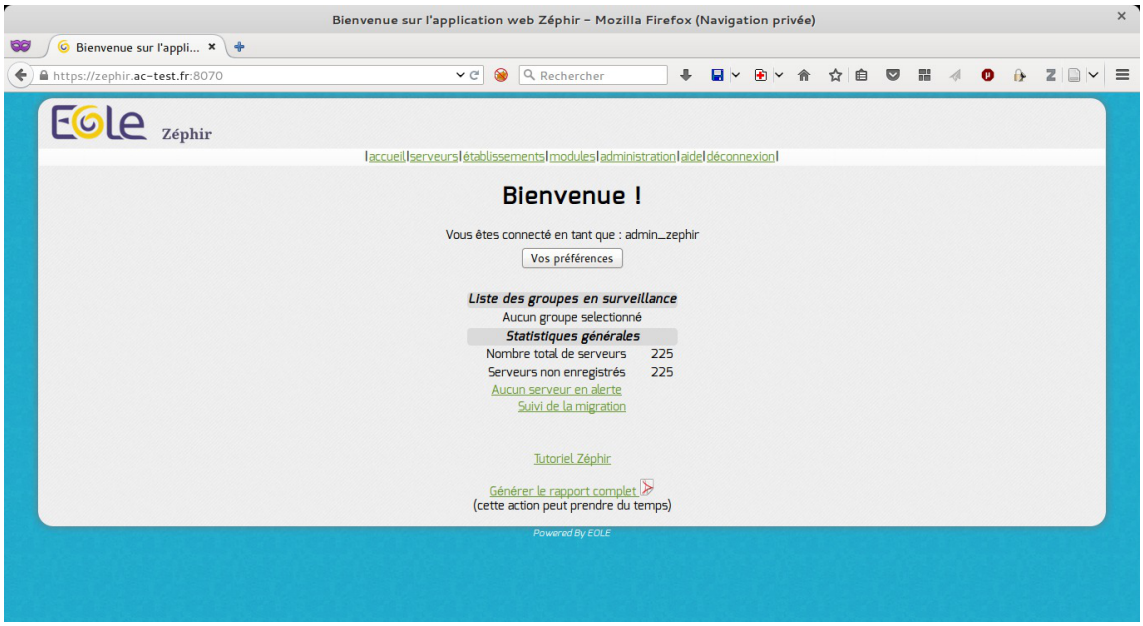
Le compte et le mot de passe associé sont ceux créés pendant la phase d'instanciation, par défaut le compte `admin_zephir`.

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 :

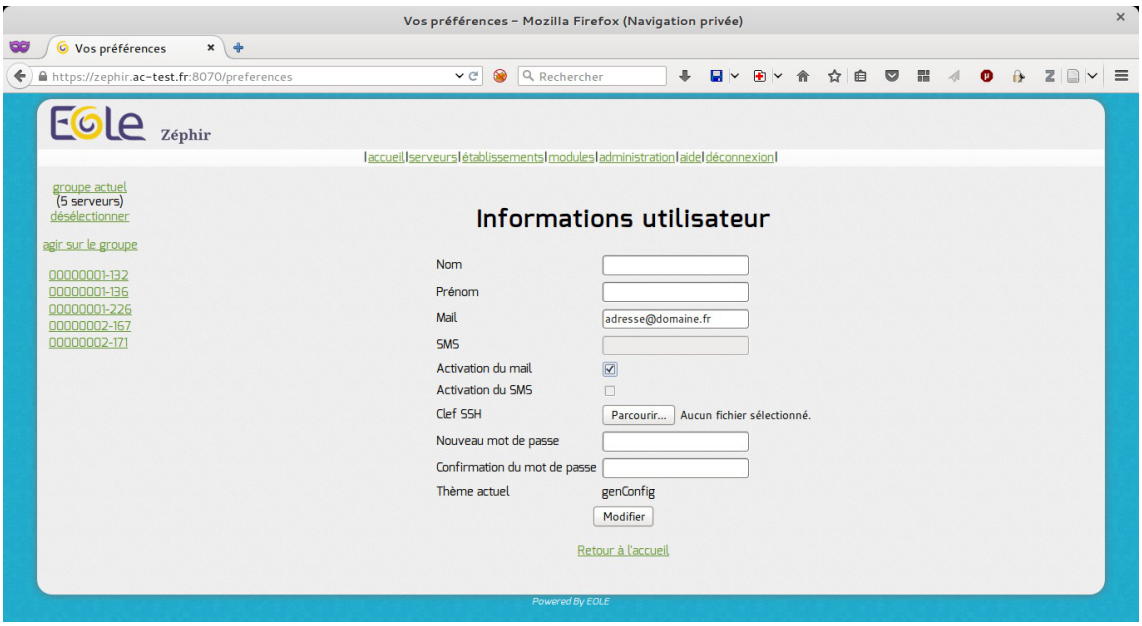
- un menu pour les différentes actions ;
- le compte de connexion : **Bienvenue admin_zephir** ;
- un bouton pour éditer `Vos préférences` ;
- un tableau récapitulatif de certaines données serveurs :
  - groupe sélectionné ;
  - nombre total de serveurs ;
  - serveurs non enregistrés ;
  - `serveurs 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.211] (équivalent à l'onglet `aide (cf. Aide)` [p.211] dans la

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

barre menu) ;

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

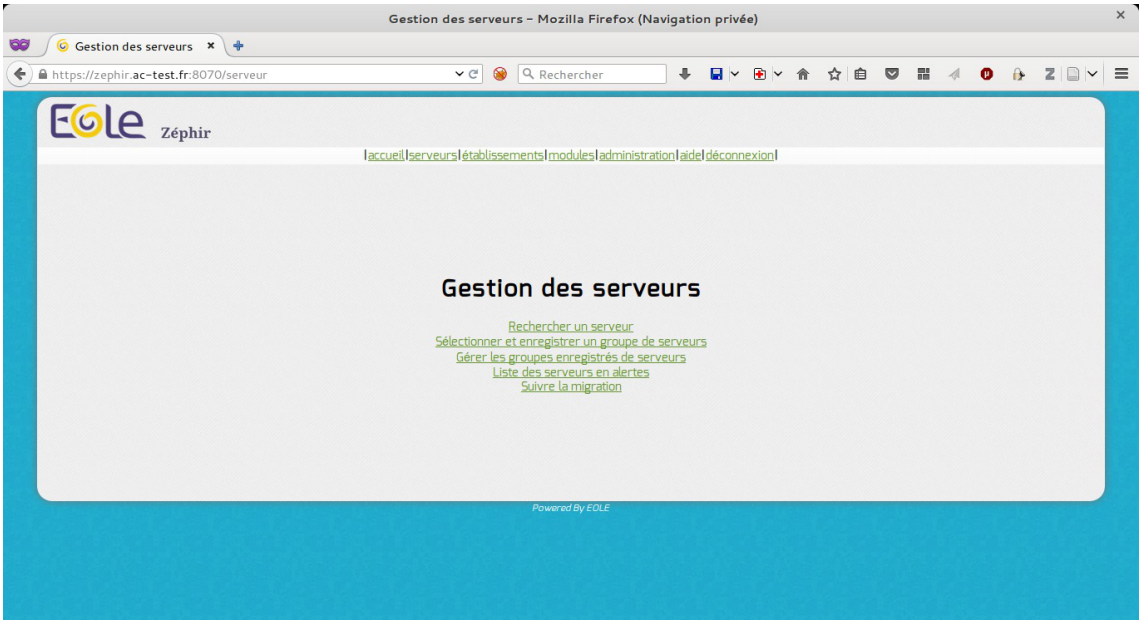
Vos préférences



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 :

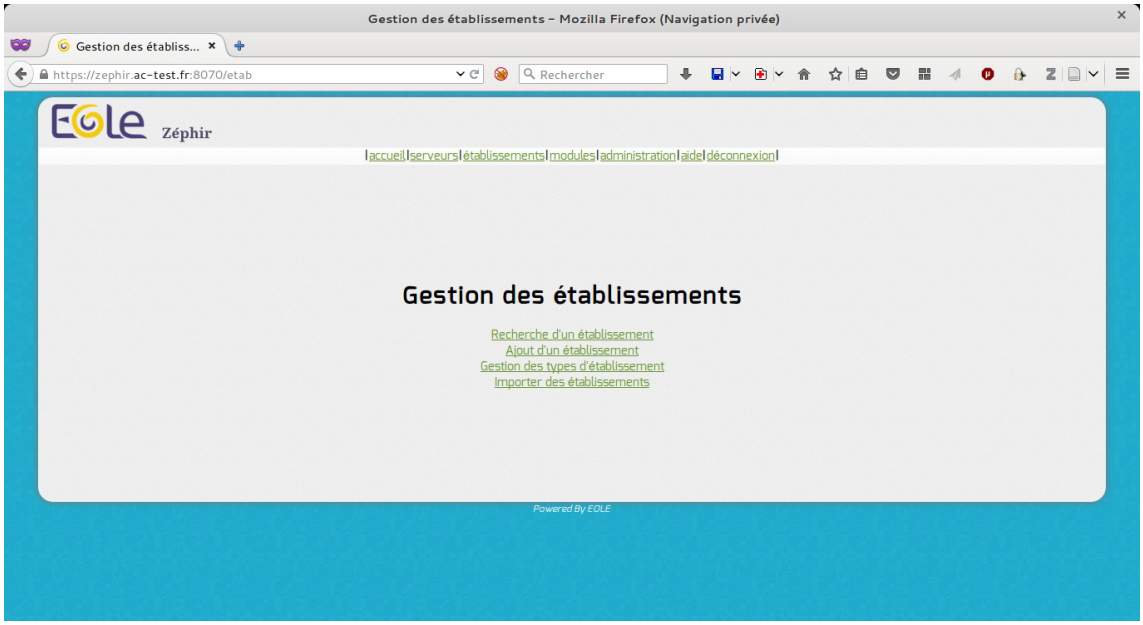
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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

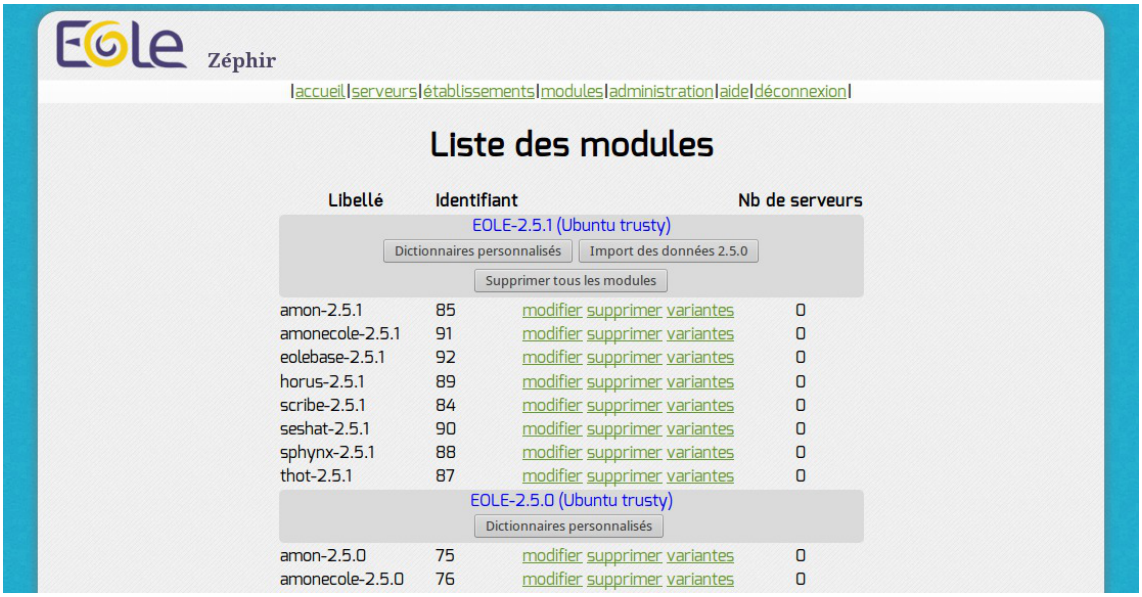


L'onglet établissements propose un menu avec la possibilité de :

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.3. L'onglet modules

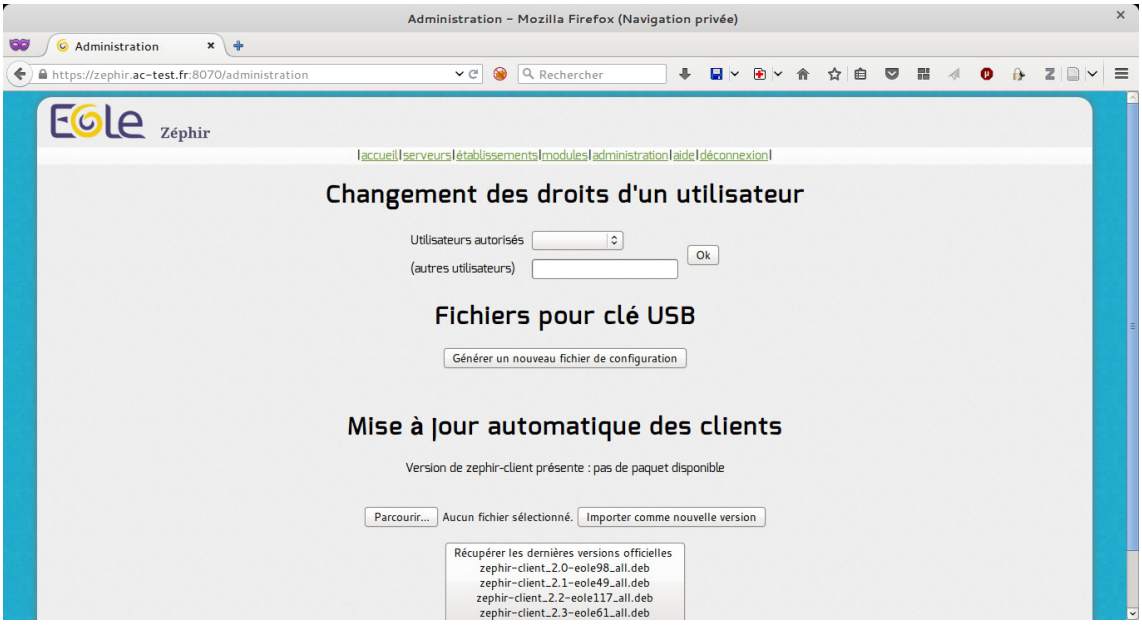


L'onglet modules propose une liste d'action possible à partir des modèles de module 2.3, 2.4 et 2.5 :

- 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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



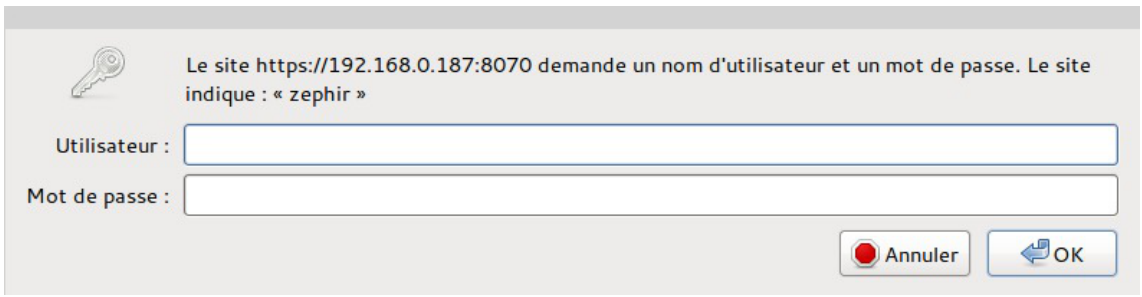
Cet item de menu ouvre une nouvelle fenêtre proposant une aide embarquée. Cette aide n'est pas maintenue, cependant beaucoup d'informations restent valides.

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`).



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

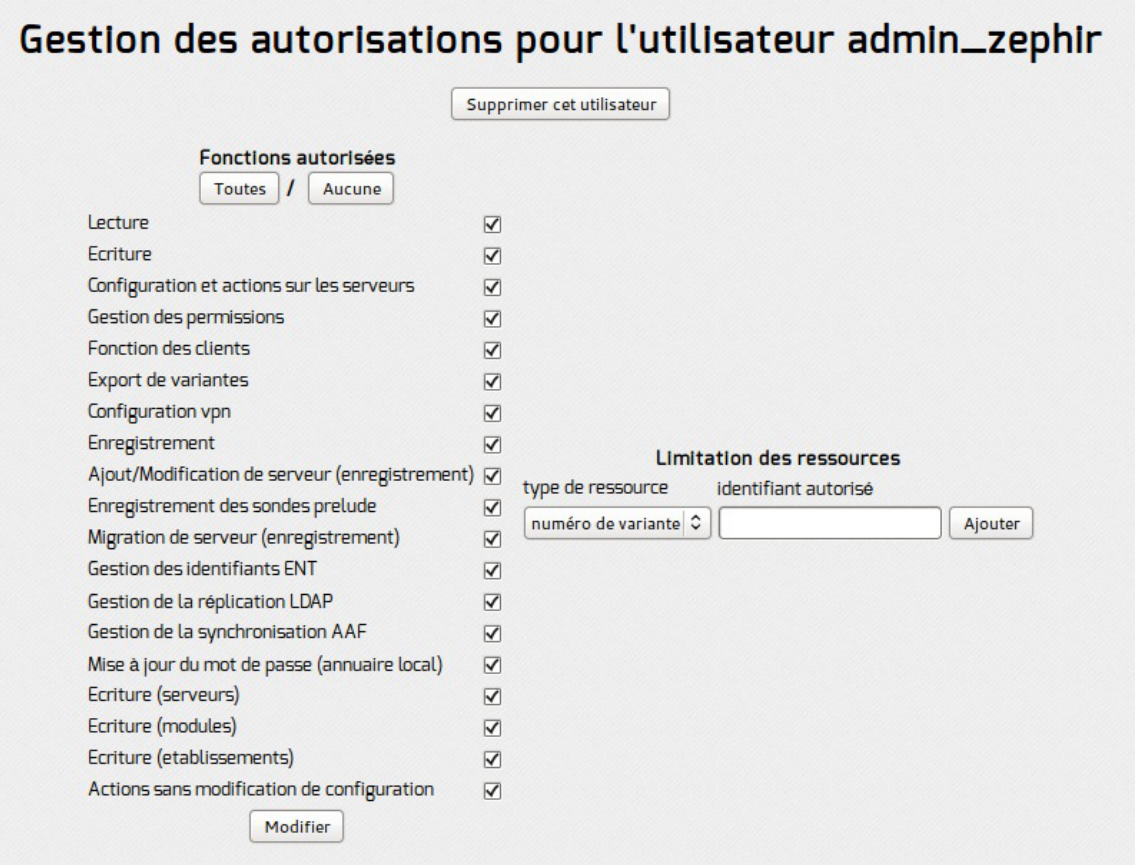
Si l'utilisateur possède déjà des droits, son compte apparaîtra dans la liste des utilisateurs, sinon il faut taper le nom exact du compte.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.477]).

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

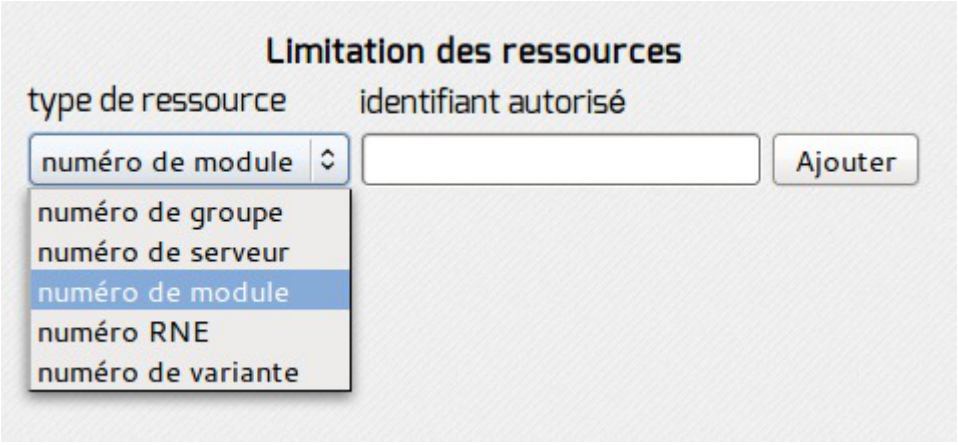
- **Configuration et actions sur les serveurs** :
  - permet d'accéder aux fonctions disponibles dans la page `Actions sur le serveur` ;
  - permet de modifier la configuration (`zephir.eol`) des serveurs.
- **Configuration VPN** : permet d'envoyer des configurations VPN sur le serveur Zéphir depuis 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.471] 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



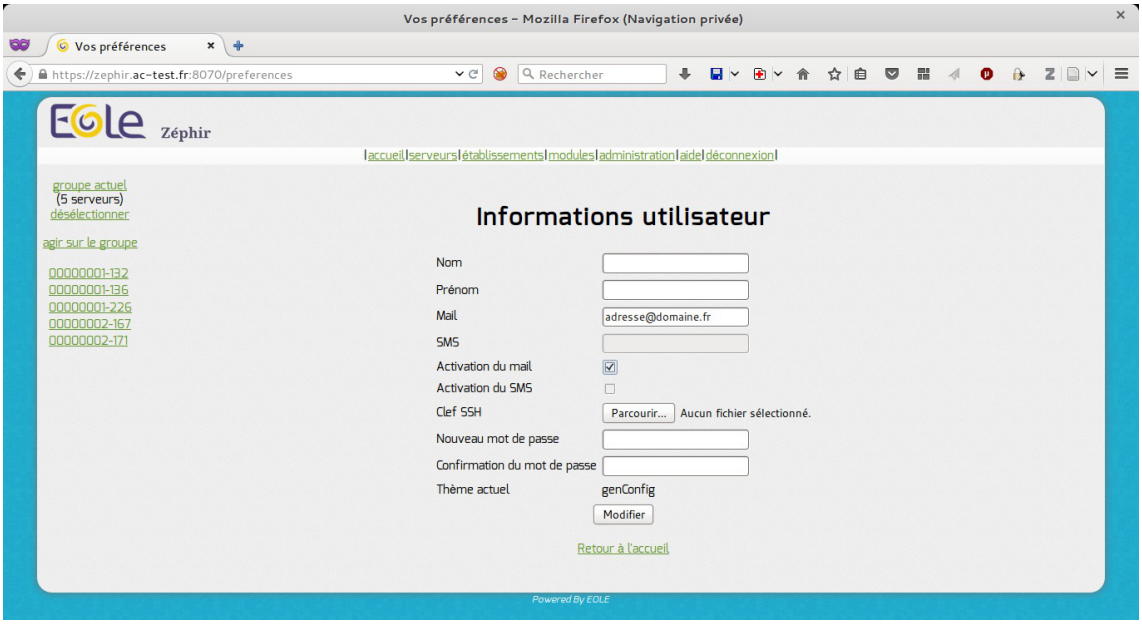
Au delà d'un certain nombre d'identifiant à ajouter il est conseillé de créer un groupe de serveur et de limiter les ressources en fonction de l'ID du groupe.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.274]

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.

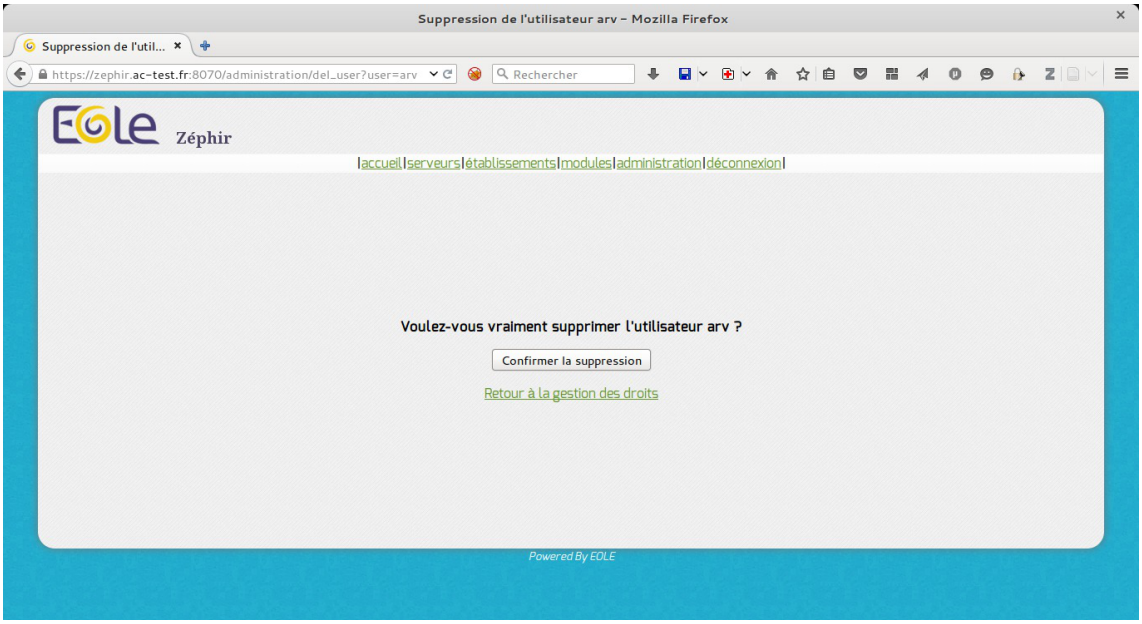
Si l'utilisateur possède déjà des droits, son compte apparaîtra dans la liste des utilisateurs, sinon il faut taper le nom exact du compte.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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`.

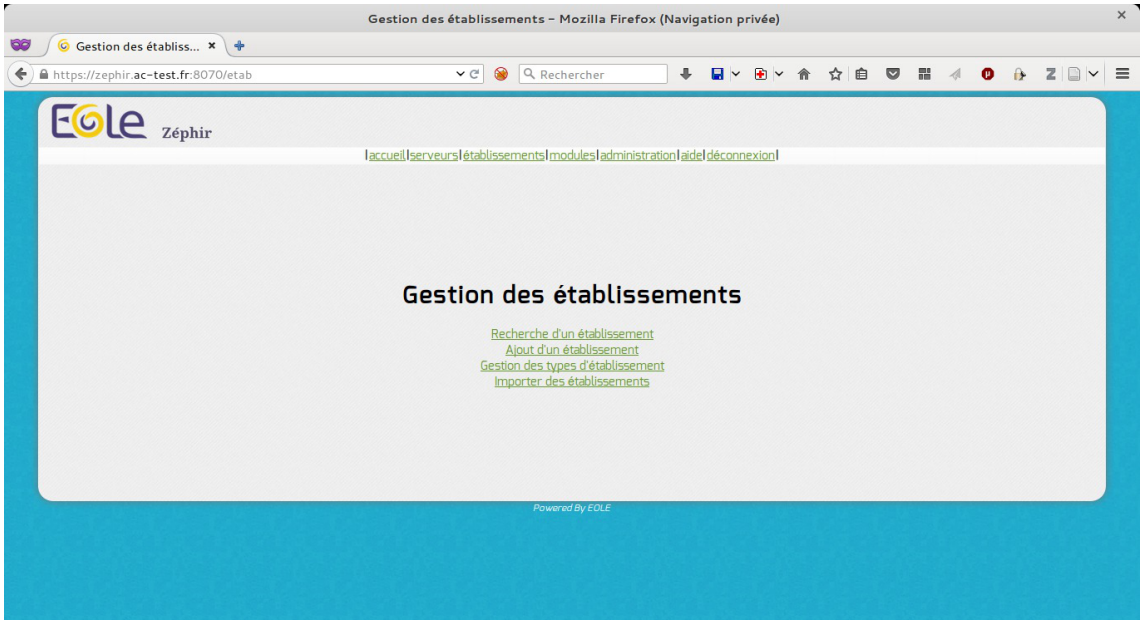
3. Gestion des établissements

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

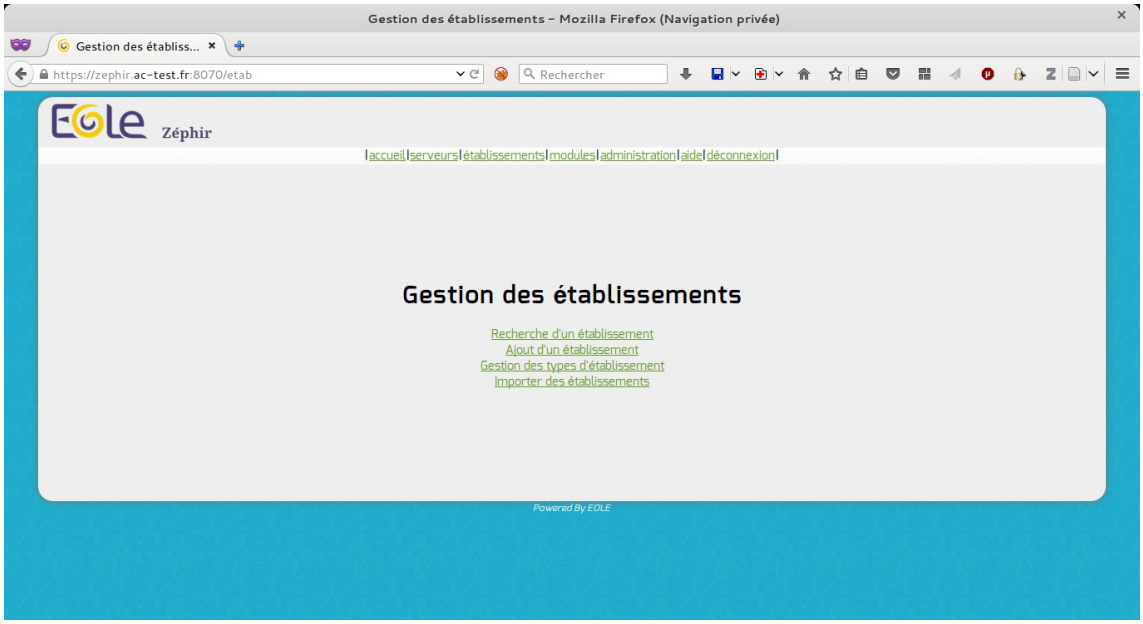
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'application Zéphir.



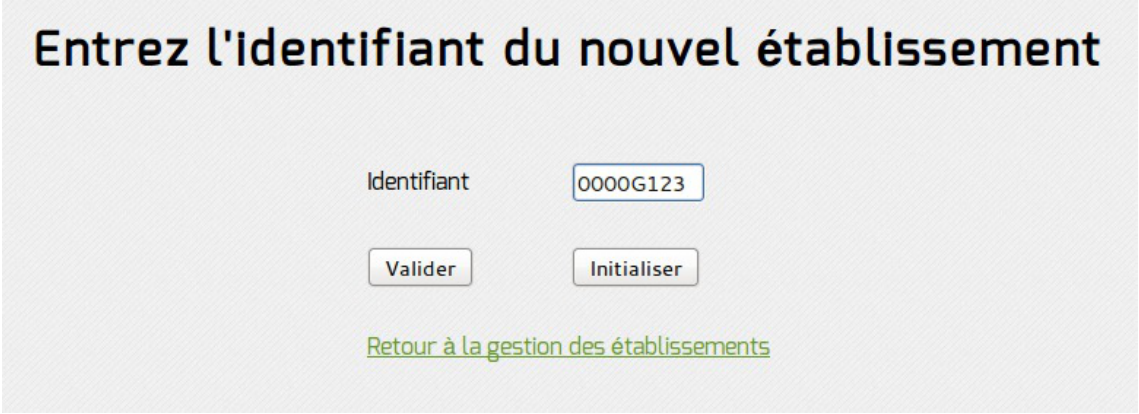
3.1. Ajout d'un d'établissement

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

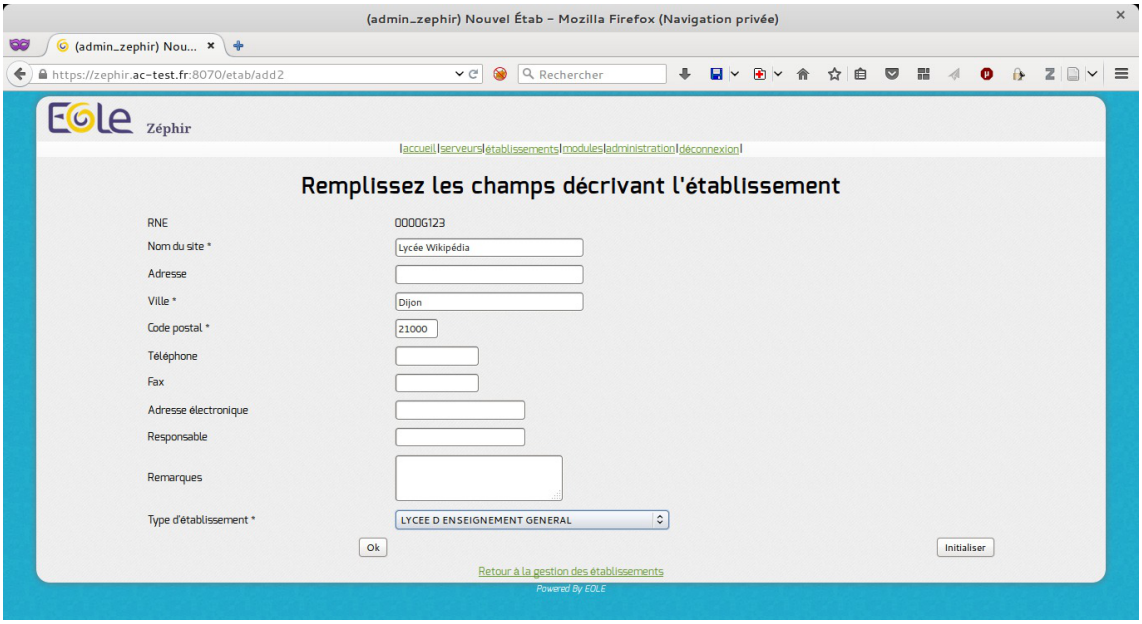


L'identifiant à saisir correspond au RNE de l'établissement (8 caractères maximum).



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.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.470]) CSV[p.457] 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|038073
2
  0210026P|CLG|340|COLLEGE|EPIREY|21000|DIJON|ce.0210026P@ac-dijon.fr|0380732916|
```

Après l'importation un rapport est affiché.

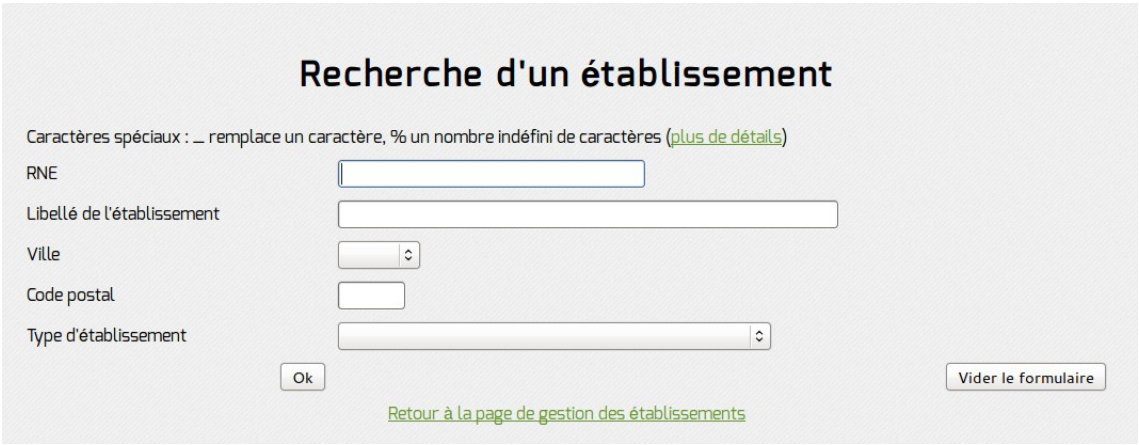
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :



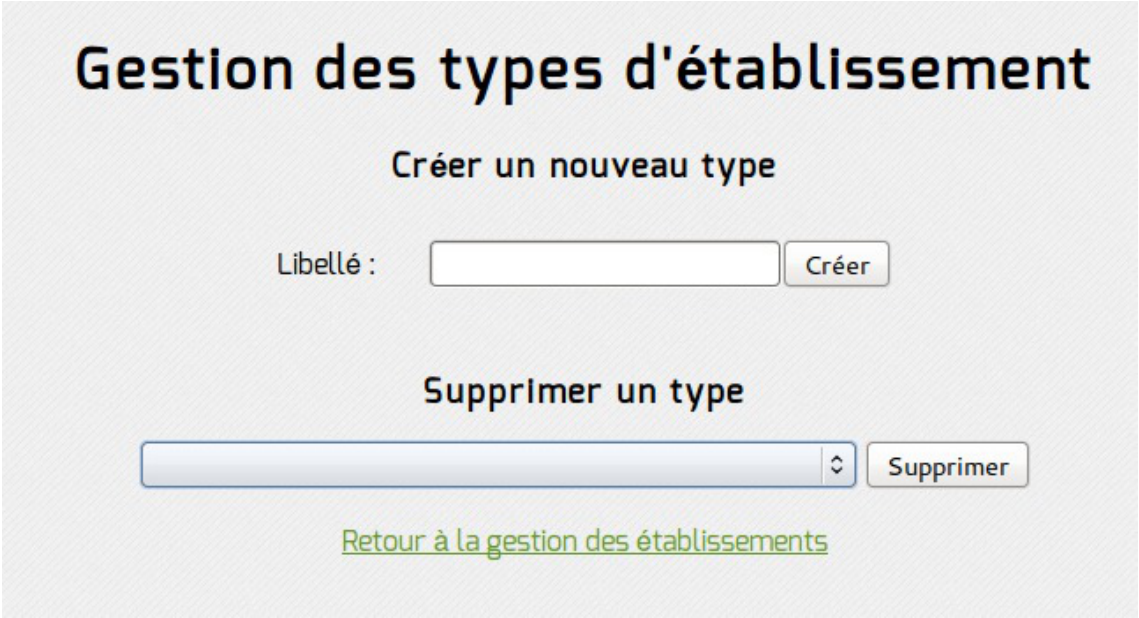
Il n'est pas possible d'effacer un établissement ayant des serveurs. Il est nécessaire de supprimer d'abord les serveurs, puis l'établissement.

3.5. Types d'établissement

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

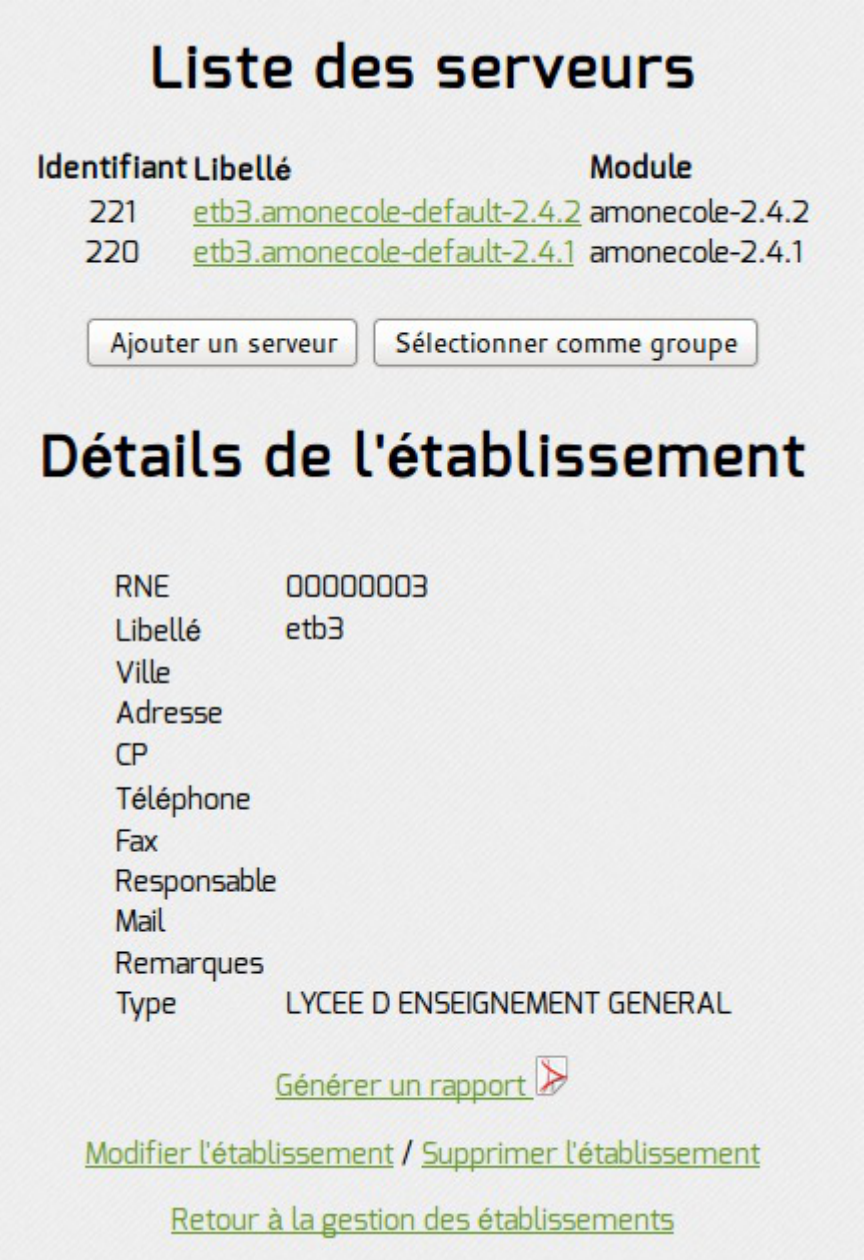
On accède aux serveurs d'un établissement à partir de la page d'affichage de l'établissement considéré.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.234]

4.2. Enregistrement d'un serveur

Pré-requis

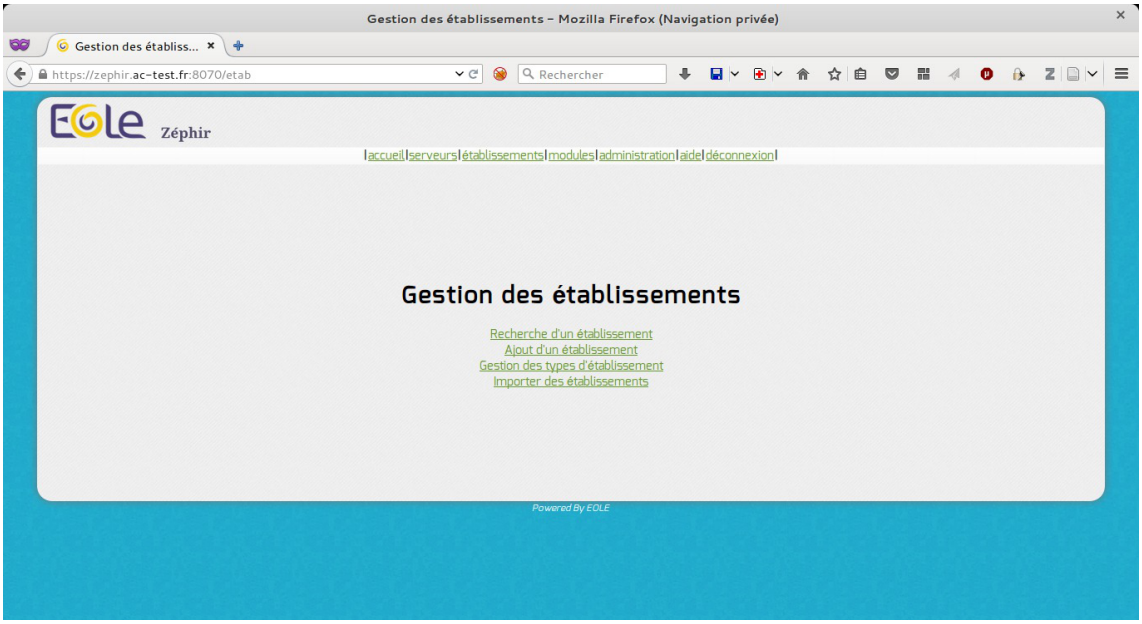
L'établissement d'appartenance du serveur doit déjà exister dans la base des serveurs.

La procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

Enregistrement d'un établissement

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Puis cliquer sur `Ajout d'un établissement`.



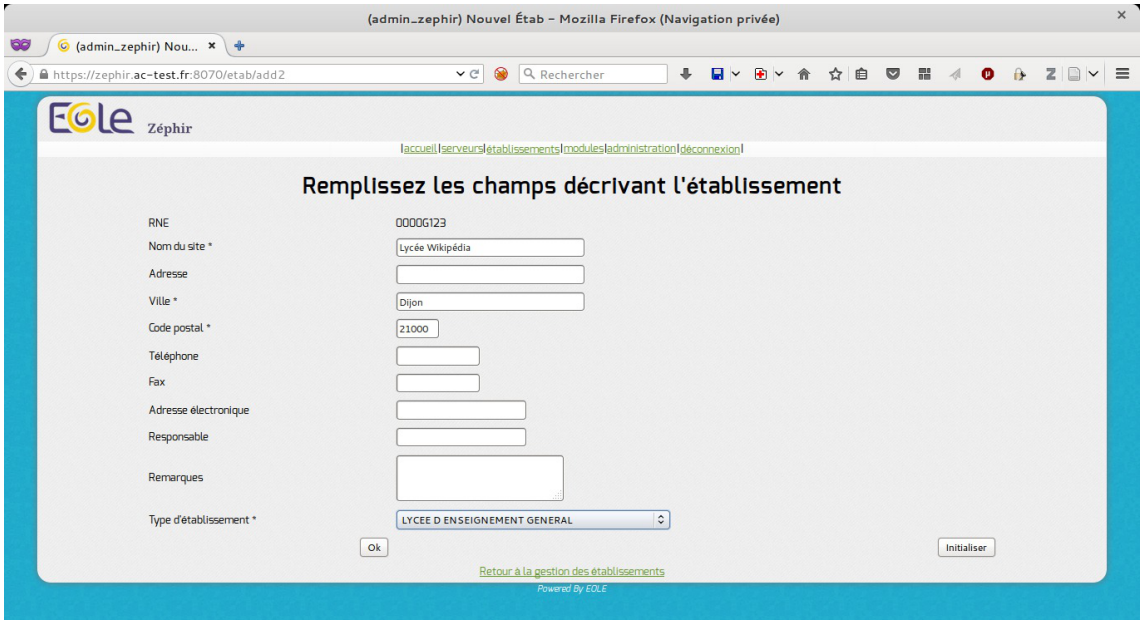
L'identifiant à saisir correspond au RNE de l'établissement (8 caractères maximum).



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, ...).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese[p.470]) CSV[p.457] 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 d'un serveur

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.



Dans le cas d'utilisation de certificats non reconnus par une autorité de certification la procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

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

- lancer la procédure d'enregistrement à l'aide de la commande `enregistrement_zephir` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 ;
- dans le cas d'utilisation de certificats non reconnus par une autorité de certification, il faut, pour procéder à l'enregistrement d'un serveur, copier le certificat de la CA locale du serveur Zéphir `/etc/ssl/certs/ca_local.crt` sur la machine à enregistrer dans le répertoire `/usr/local/share/ca-certificates/` et mettre à jour les certificats sur la machine locale à l'aide de la commande `update-ca-certificates` ;
- relancer la procédure d'enregistrement avec la commande `enregistrement_zephir` ;
- 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.

Certificat de Zéphir non validé !

 utiliser sur Zéphir un certificat signé par une autorité reconnue,
  ou
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
 Copier le fichier /etc/ssl/certs/ca_local.crt de Zéphir dans
 /usr/local/share/ca-certificates et lancer update-ca-certificates.
root@eolebase:~#

root@eolebase:~# scp root@zephir.ac-test.fr:/etc/ssl/certs/ca_local.crt
/usr/local/share/ca-certificates/
Warning: Permanently added 'zephir.ac-test.fr,192.168.0.20' (ECDSA) to the
list of known hosts.
root@zephir.ac-test.fr's password:
ca_local.crt
100% 1736     1.7KB/s   00:00
root@eolebase:~#

root@eolebase:~# update-ca-certificates
Updating certificates in /etc/ssl/certs...
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate ca.crt
WARNING: Skipping duplicate certificate ca.crt
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
root@eolebase:~#

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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 --

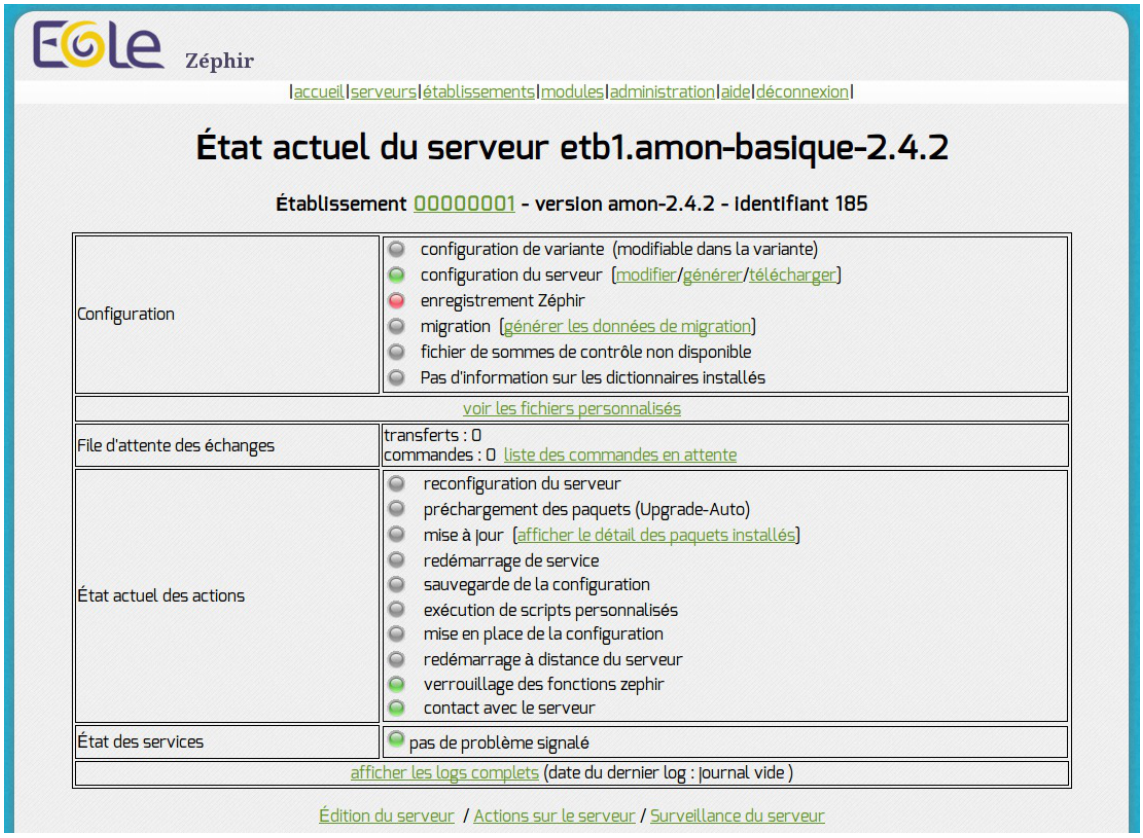
--récupération des patchs et dictionnaires (veuillez patienter)--
** le numéro attribué à ce serveur sur le serveur Zéphir est : 1 **
root@eolebase:~#
```

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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...)



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.281]

Personnalisation d'un serveur [p.245]

Fonctions spécifiques à certains modules [p.296]

État des services / état système [p.266]

4.4. Actions sur un serveur

4.4.1. Généralités sur les actions

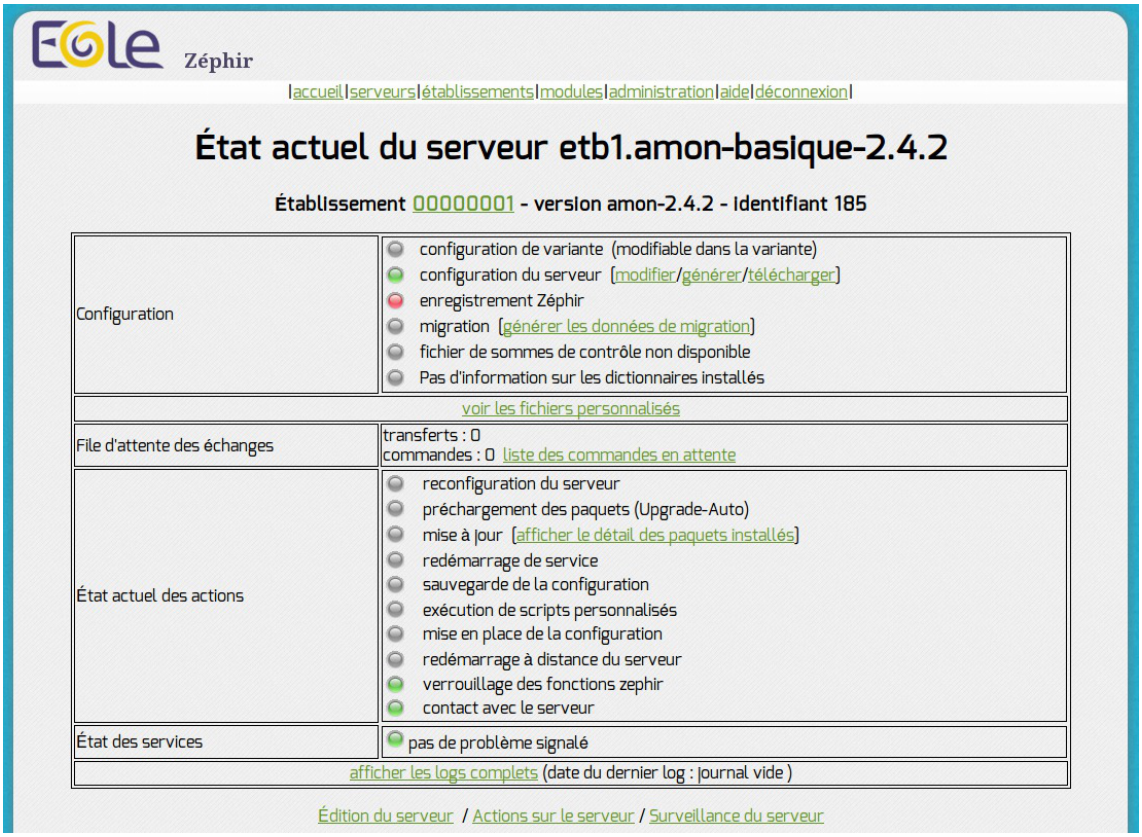
L'application Zéphir permet d'agir à distance sur les serveurs par des actions. Les actions sont principalement regroupées dans la page `Actions` accessible depuis la page d'état de chaque serveur. Elles sont mises en file d'attente et sont exécutées à la connexion du serveur enregistré au serveur Zéphir.

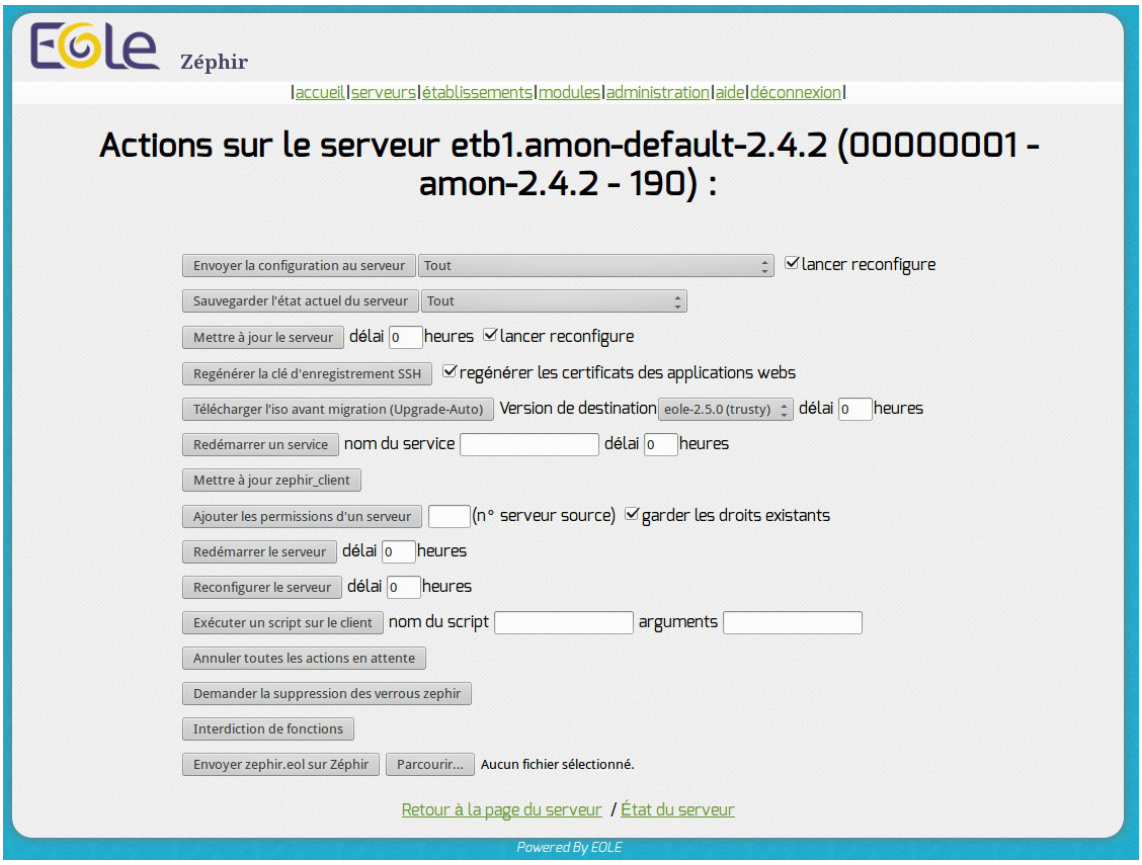
Toutes les actions fonctionnent selon le principe suivant :

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)





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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

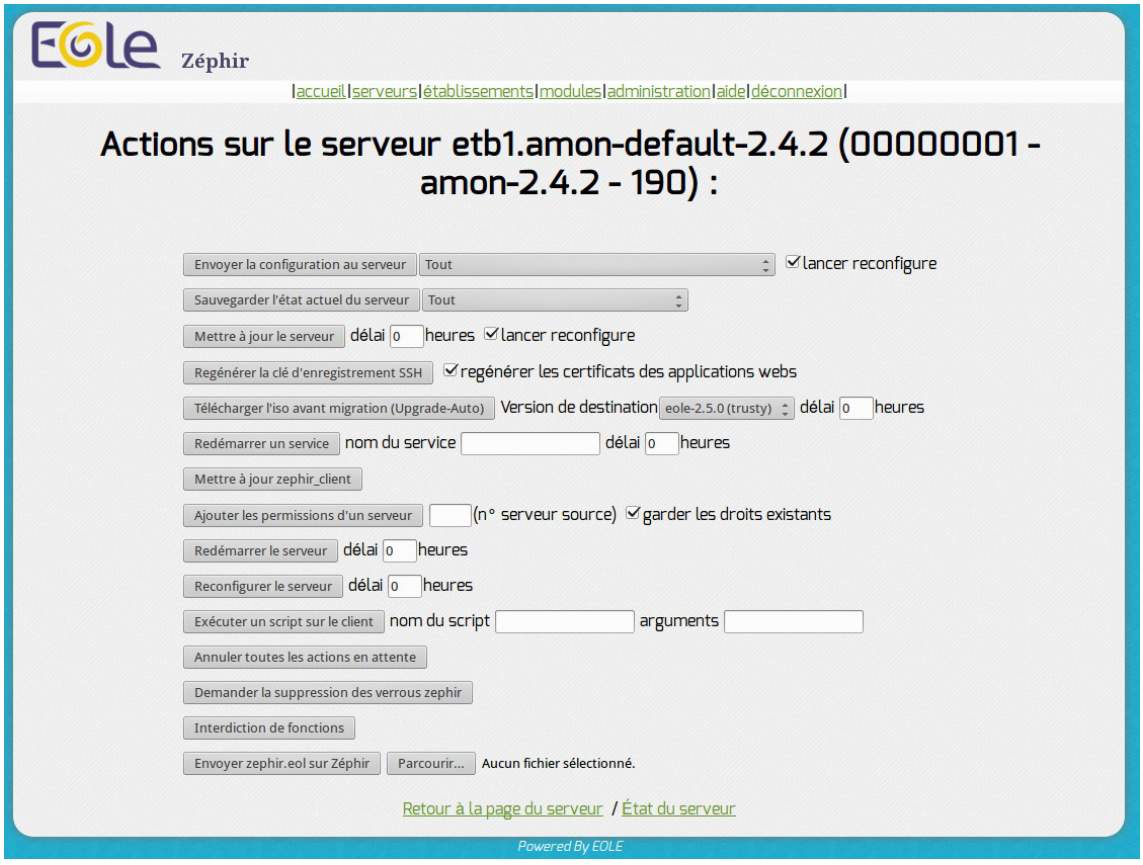
> liste des commandes en attente de la page d'état du serveur.

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 Zéphir sur les serveurs



Liste des actions

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est possible de demander l'exécution d'un script personnalisé sur le client.



Exécution d'un script personnalisé dans le formulaire "Actions sur le serveur"

Les informations à fournir sont le nom du script sans l'extension `.zephir` 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.

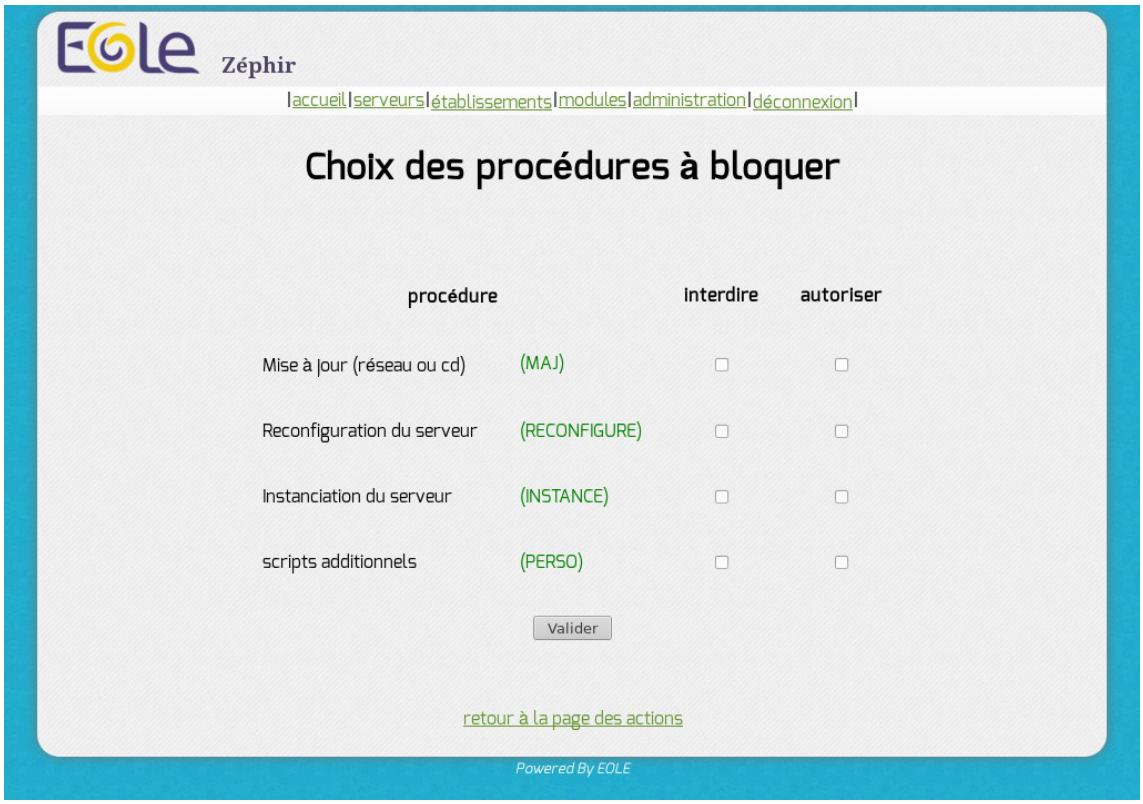
Demander la suppression des verrous Zéphir

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

Il est possible d'interdire à un serveur (ou un groupe de serveurs) d'exécuter certaines fonctions.



Les fonctions qui peuvent être bloquées sont :

- la mise à jour (hebdomadaire ou manuelle) ;
- la reconfiguration ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'instanciation ;
- l'exécution des scripts additionnels.

Chaque fois que le serveur tente d'exécuter l'une de ces procédures, il vérifie auprès du serveur Zéphir qu'il a le droit de le faire (s'il n'arrive pas à joindre le serveur Zéphir, il conserve les dernières autorisations reçues).



Sur le serveur, l'option `-f` permet de passer outre les interdictions appliquées pour certaines commandes :

- `Maj-Auto -f`
- `reconfigure -f`
- `instance -f`

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).

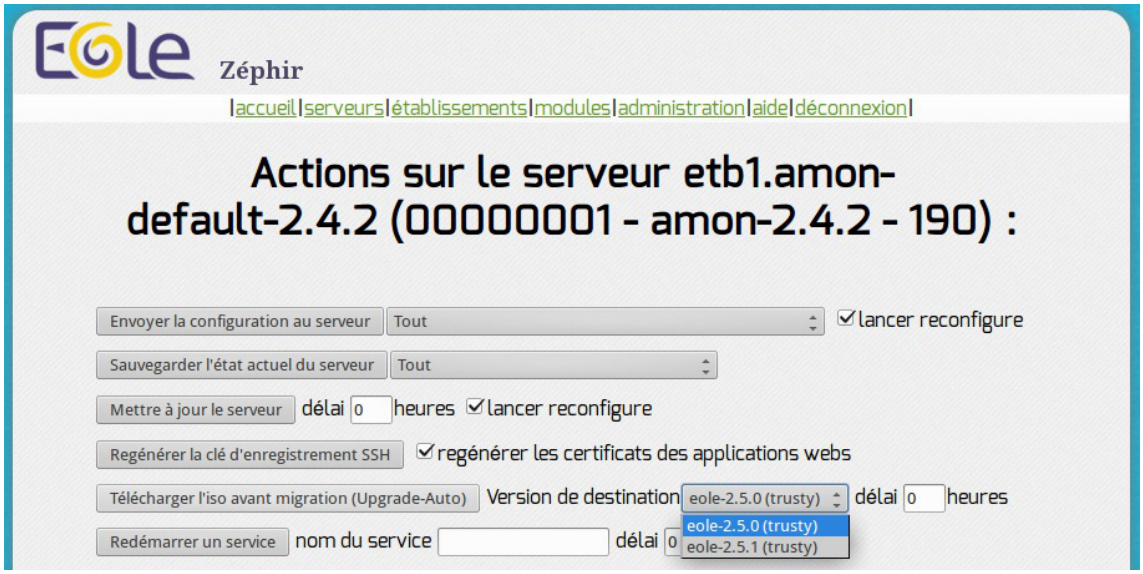
Envoyer le fichier sur le serveur Zéphir ne suffit pas pour que les paramètres soient appliqués. Il faut penser à envoyer la configuration sur le serveur de destination.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



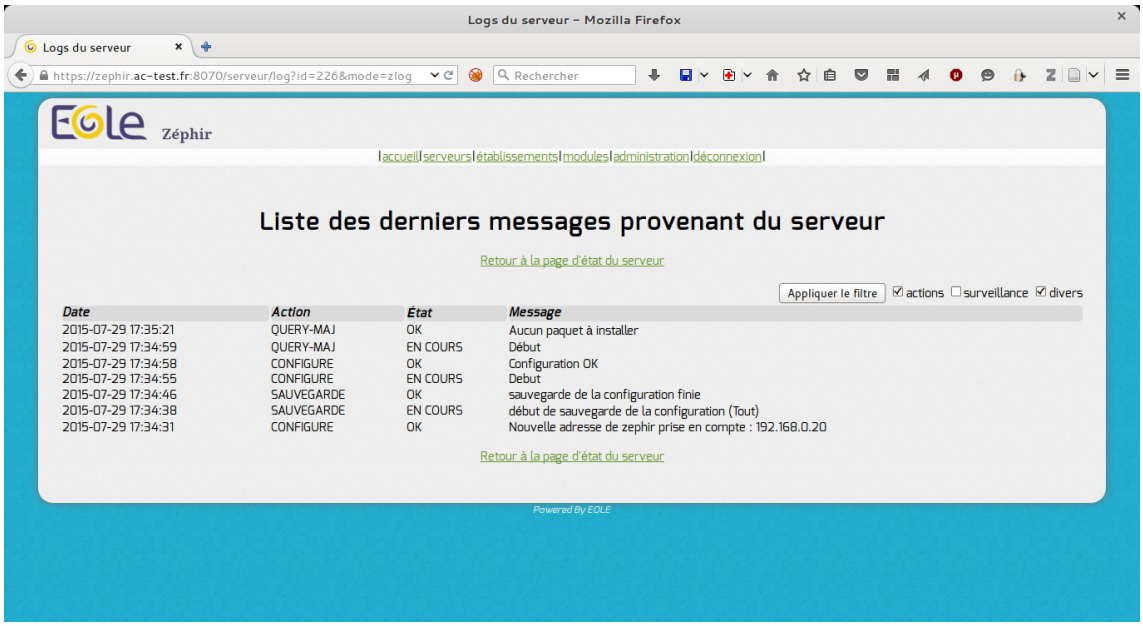
Cette option n'est proposée qu'à partir de la version 2.4.2, et seulement s'il existe des versions supérieures de la distribution pour le serveur sélectionné.

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).

Consultation des journaux

La dernière ligne en bas de page affiche la date et l'heure de la dernière action enregistré pour ce serveur.

Le lien Logs complets permet d'accéder aux journaux du serveur.



Si les journaux sont très nombreux l'affichage peut être ralenti. Il peut être nécessaire de procéder à une purge des journaux systèmes.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

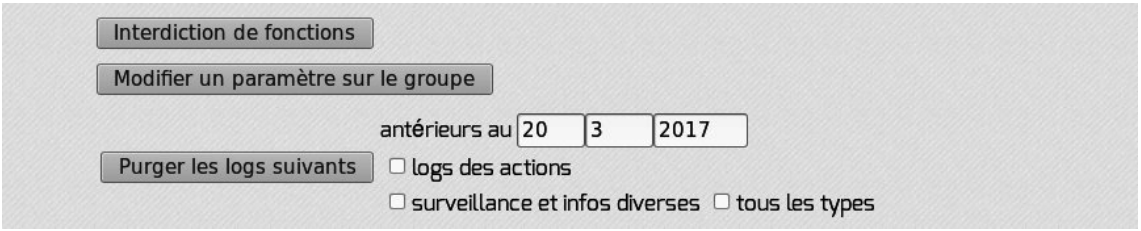
Cela concerne uniquement les journaux de l'application et non les journaux locaux des serveurs (syslog, squid, ...).

Purge des journaux

Le script de purge `/usr/share/eole/schedule/scripts/zephir_weekly` est exécuté régulièrement mais peut ne pas suffire car la purge ne se fait pas sur tous les types de journaux.

Il est donc proposé dans l'interface de 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 (logs des action, surveillance et infos diverses...), et une date limite (tous les logs antérieurs seront purgés).

La purge des journaux n'est pas accessible par serveur sur la page d'état du serveur, elle s'effectue au travers des groupes de serveurs.



Liste des dernières actions envoyées au serveur

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

Si les journaux sont trop nombreux l'action peut ne pas aboutir.

Dans ces cas il peut être intéressant d'utiliser l'action de purge directement en ligne de commande :

```
# /usr/share/eole/purge_logs.py -t all -d JJ/MM/AAAA
```

Tous les journaux antérieurs à la date sont purgés.

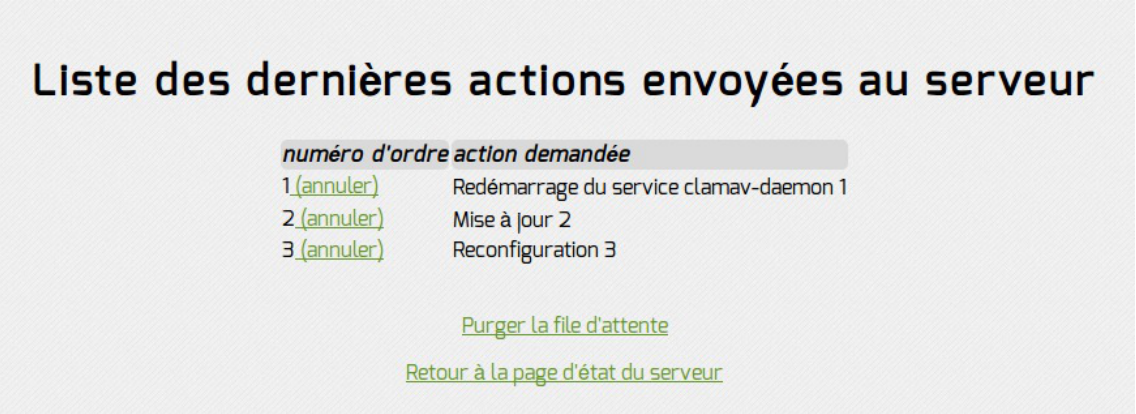
Pour plus d'information sur les paramètres à utiliser :

```
# /usr/share/eole/purge_logs.py --help
```

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.245]

Création et exécution de scripts personnalisés [p.248]

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/`) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

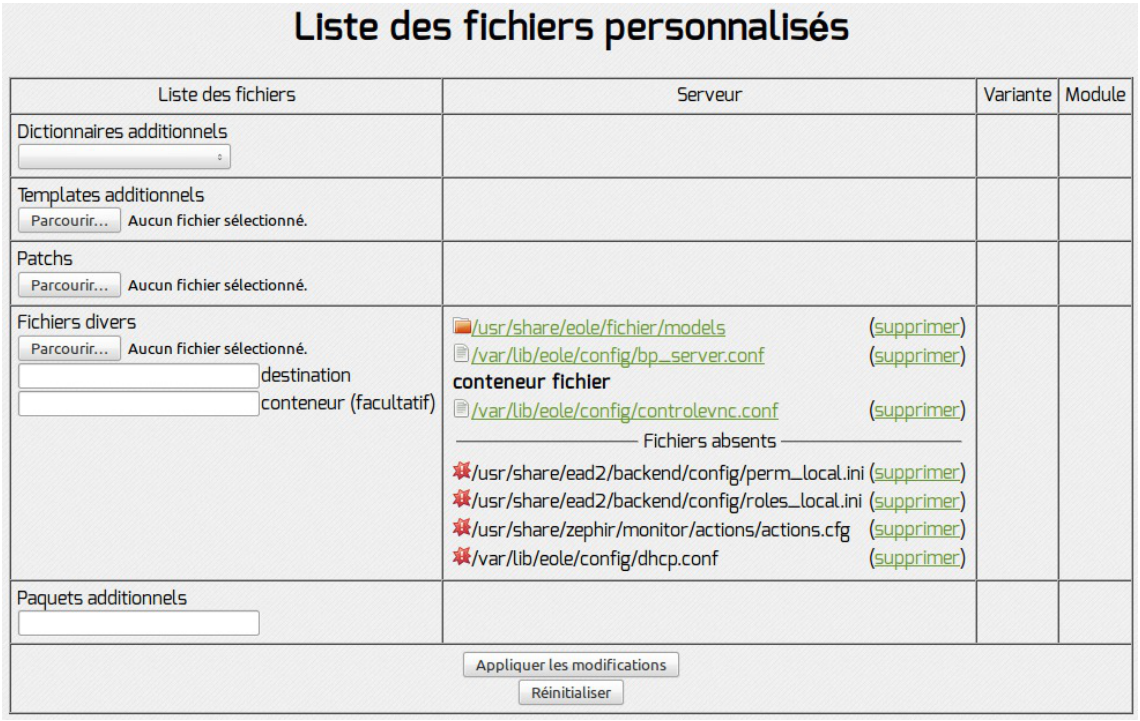
Pour remonter les fichiers sur le serveur Zéphir, lancer le script `/usr/share/zephir/scripts/zephir_client save_files` sur le serveur enregistré.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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).

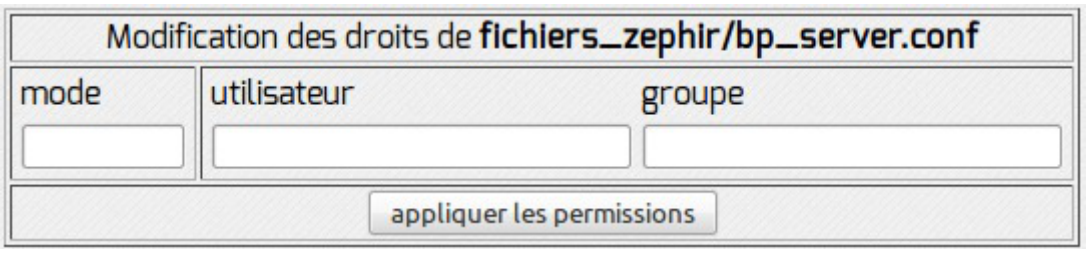


Liste des fichiers personnalisés

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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. Création et exécution de scripts personnalisés

L'ajout d'un script personnalisé est très encadré, les conditions suivantes doivent être respectées :

- le script personnalisé doit être placé dans le répertoire `/usr/share/zephir/scripts/`
- le script personnalisé doit obligatoirement posséder l'extension `.zephir`
- le script personnalisé doit être exécutable

Le client Zéphir s'exécute en tant qu'utilisateur `uucp`. Afin d'obtenir des droits supplémentaires, les scripts personnalisés sont exécutés avec sudo[p.474].

Pour qu'un nouveau fichier personnalisé soit pris en compte par sudo, il faut re-démarrer le service `z_stats`.

Cela peut s'effectuer via l'interface web de Zéphir ou directement sur le serveur client à l'aide de la commande : `systemctl restart z_stats`

Création d'un script personnalisé sur le serveur client

Il est possible de créer un fichier personnalisé en l'éditant directement sur le serveur cible.

Cela est pratique pour tester la fonctionnalité ou si le script concerne ne concerne qu'un seul serveur.

```
cat > /usr/share/zephir/scripts/test.zephir <<EOF
#!/bin/bash
echo "Exécution du script \$0 en tant que $(whoami)" > /tmp/zephir
EOF
chmod +x /usr/share/zephir/scripts/test.zephir
service z_stats restart
```

Création d'un script personnalisé via l'interface Zéphir

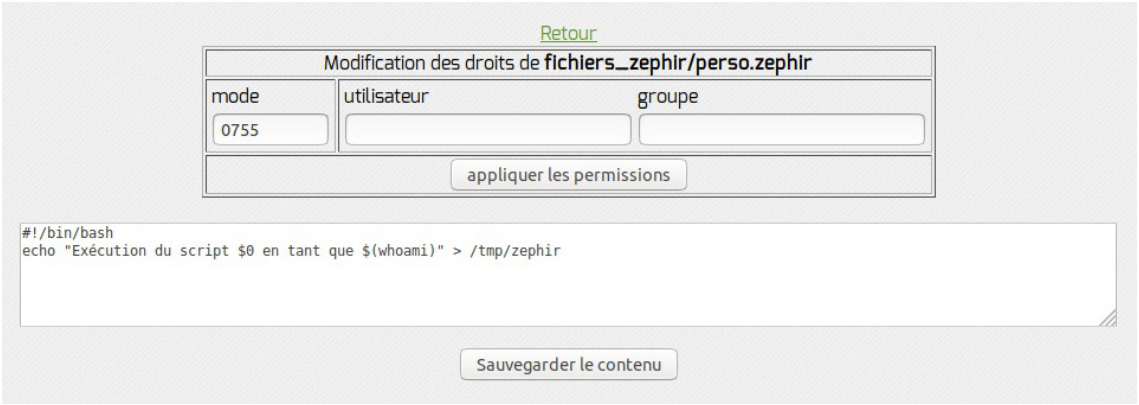
Il est possible de déployer un script via Zéphir en utilisant le mécanisme des fichiers personnalisés.

Avec ce mécanisme, le fichier peut être déployé sur un serveur ou un ensemble de serveurs si le fichier est déclaré au niveau d'une variante[p.476].

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Déclaration d'un script en tant que fichier divers dans le formulaire "Liste des fichiers personnalisés"



Édition des droits et du contenu du script personnalisé

Pour que le fichier personnalisé soit pris en compte par sudo, il faut que le service `z stats` ait été redémarré sur le serveur client.

Exécution d'un script personnalisé

Il est possible de demander l'exécution d'un script personnalisé sur le client.



Exécution d'un script personnalisé dans le formulaire "Actions sur le serveur"

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

Création d'un script python avancé

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

```
1  #!/usr/bin/env python
2  # -*- coding: utf-8 -*-
3  ###############################################################################
4  # Eole NG - 2007
5  # Copyright Pole de Competence Eole (Ministere Education - Academie Dijon)
6  # Licence CeCill cf /root/LicenceEole.txt
7  # eole@ac-dijon.fr
8  #
9  # test_perso.zephir
10 #
11 # exemple de script personnalisé pour le client zephir
12 # ###############################################################################
13 import os, sys
14 from zephir.lib_zephir import *
15 from creole import fonctionseole
16
```

```
17 if fonctionseole.init_proc('PERSO') == False:
18     fonctionseole.zephir("MSG" , "procédure test_perso bloquée par Zéphir", "PERSO")
19     sys.exit(1)
20 fonctionseole.zephir("INIT" , "script test_perso en cours d'execution", "PERSO")
21 try:
22     message = sys.argv[1]
23     fonctionseole.zephir("MSG" , "test_perso lancé avec l'argument %s" % message,
   "PERSO")
24 except:
25     fonctionseole.zephir("ERR" , "test_perso lancé sans argument", "PERSO")
26     exit(1)
27 if is_locked(['reconfigure']):
28     fonctionseole.zephir("ERR" , "test_perso stoppé : reconfigure en cours", "PERSO"
   )
29     exit(1)
30 else:
31     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`.

Voir aussi...

Les actions Zéphir sur les serveurs [p.239]

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `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**

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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

A 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

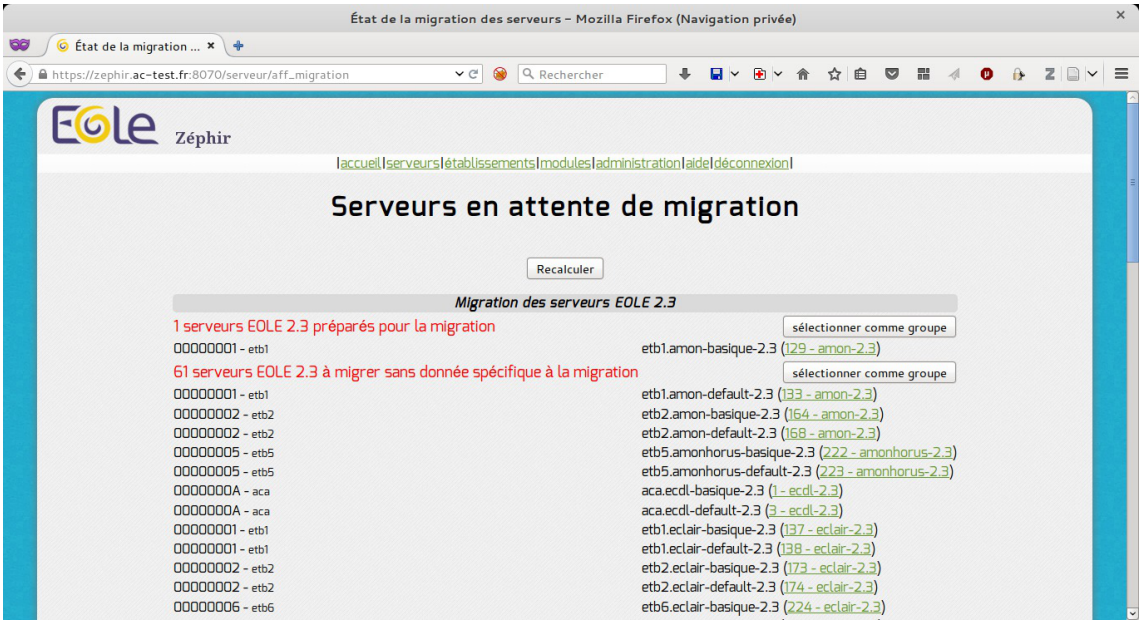
Page de suivi de la migration

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



> 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).

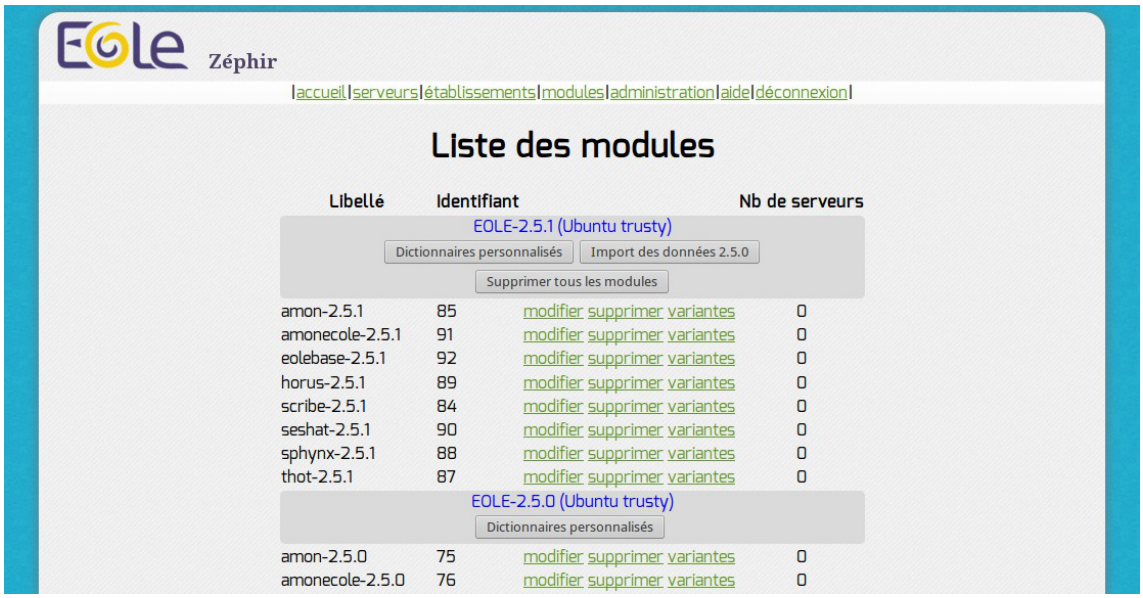


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



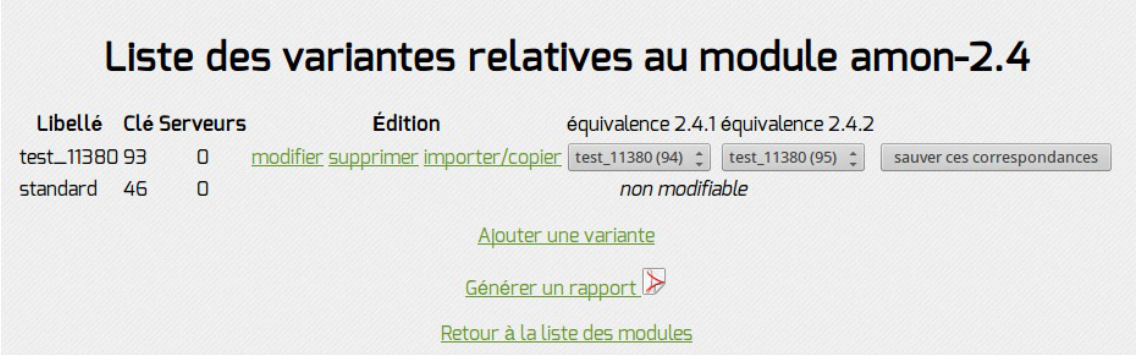
Équivalence des variantes entre deux versions

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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).

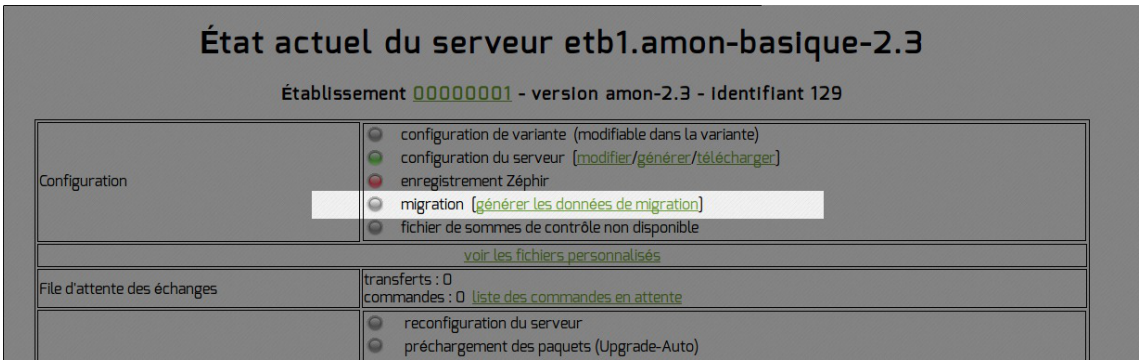
Dans ce cas, il faut renseigner manuellement les équivalences des variantes depuis la page des variantes du module d'origine (par exemple, la page des variantes du module Amon 2.4.0). Zéphir définit les correspondances automatiquement, mais seulement lors de l'import des données entre deux versions mineures 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` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

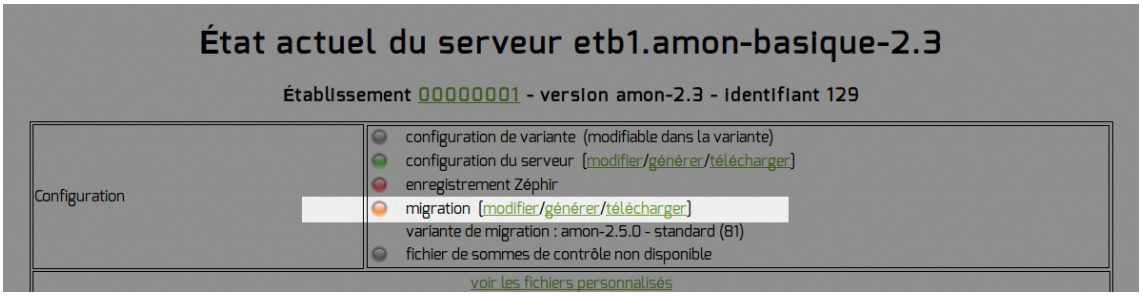


- pour les modules 2.4 et supérieurs, la saisie de configuration passe par l'interface de configuration du module qui a été intégrée au serveur Zéphir, le formulaire interne a été abandonné ;



- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

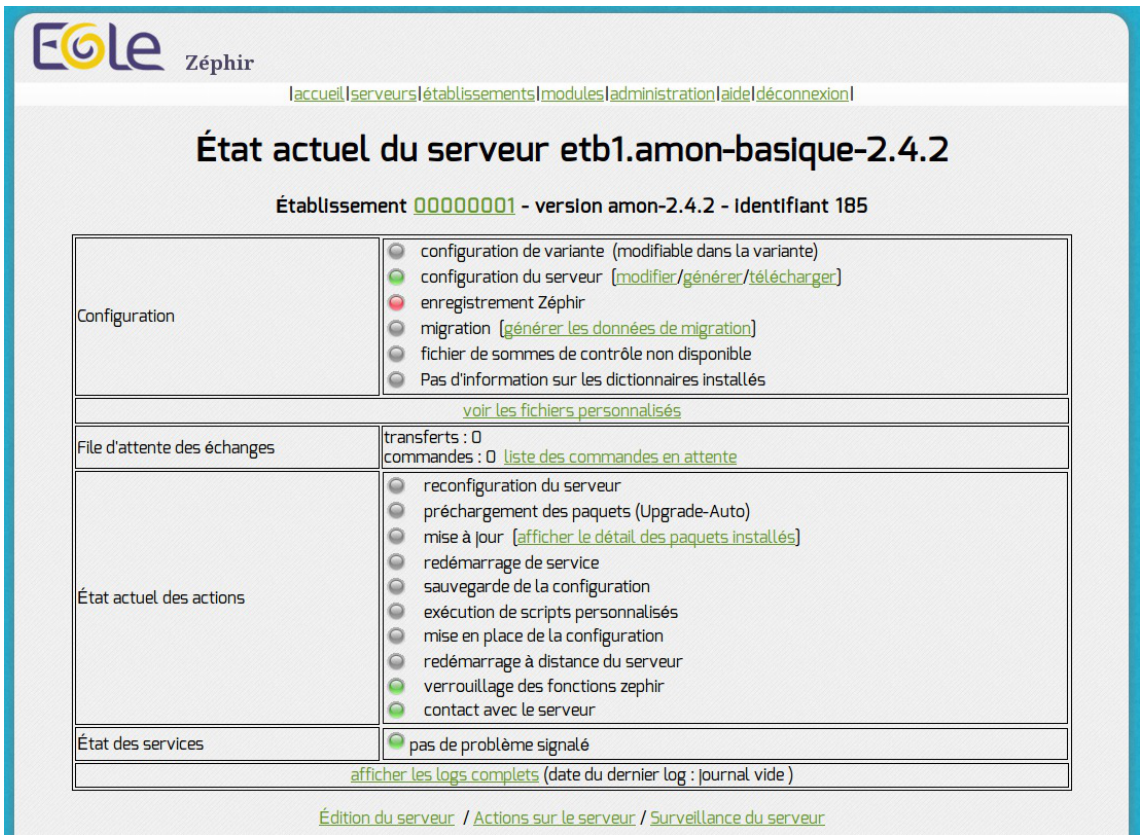
- diode verte : fichier sauvegardé ;
- diode rouge : fichier différent entre Zéphir et le serveur ;
- diode grise : fichier absent.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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[p.465] 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

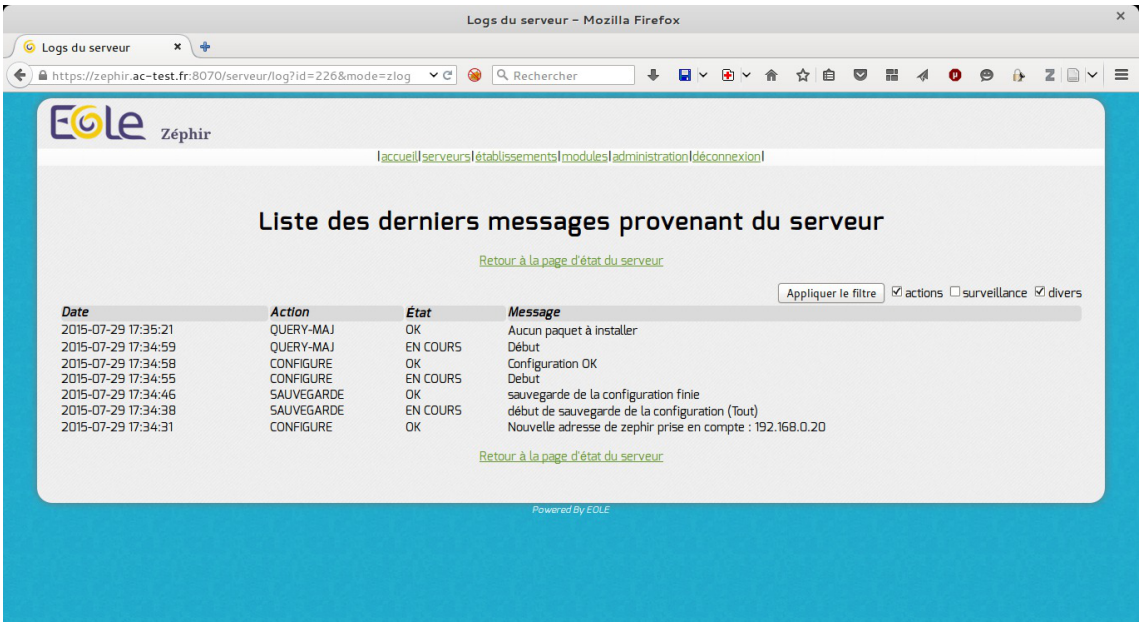
- rouge : indique que l'action s'est terminée de façon anormale (erreur de transfert de fichiers, erreur système, ...) ;
- gris : aucune indication n'est connue pour cette action (elle n'a jamais été lancée ou les logs la concernant ont été effacés).

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.



Si les journaux sont très nombreux l'affichage peut être ralenti. Il peut être nécessaire de procéder à une purge des journaux systèmes.

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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.465] 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.457].

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
===============

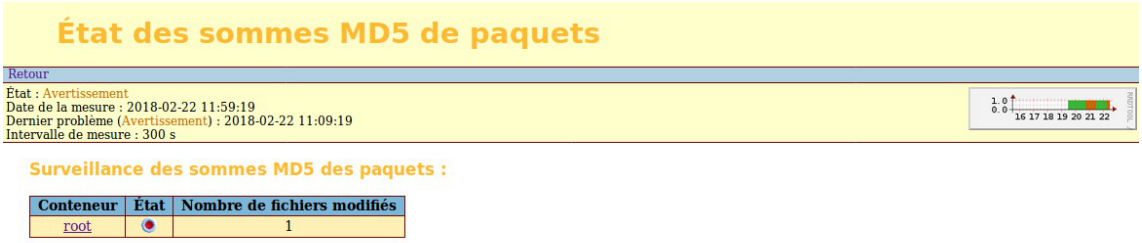
Filename: /var/log/eole-debsums/report.log
Last update: 2018-02-22 11:09:15

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

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

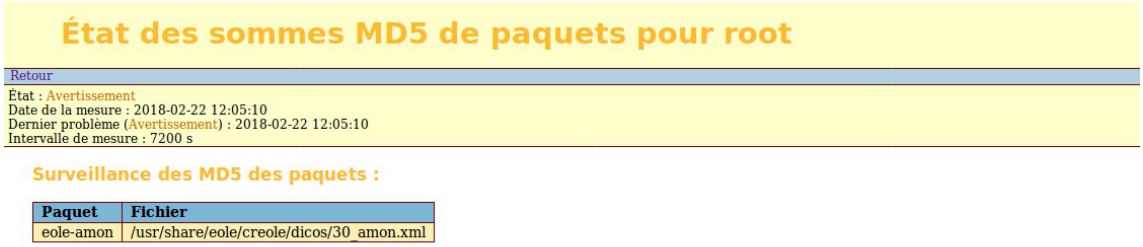
```

Un agent[p.453] de surveillance Zéphir permet de surveiller les sommes MD5 des paquets.



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Exceptions

À partir d'EOLE 2.6.2, il est possible d'ajouter des listes de fichiers à ignorer dans le résultat debsums en les plaçant dans le répertoire : `/etc/eole/debsums-ignore.d` (exemple : `/etc/eole/debsums-ignore.d/academie.conf`).

Les fichiers modifiés par EOLE sont listés dans `/usr/share/eole/debsums/eole-ignores`.

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 :

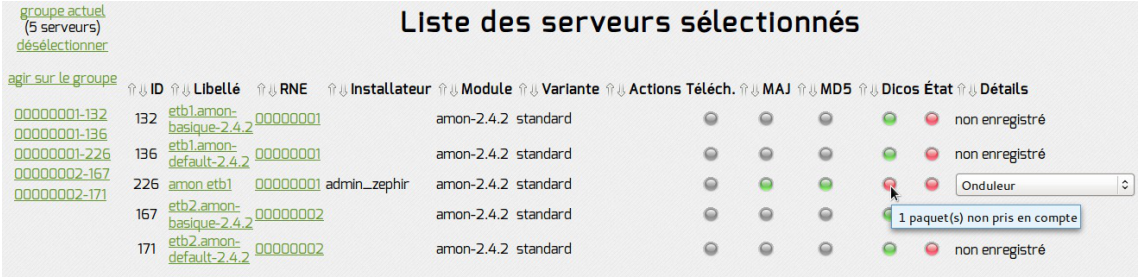
- Statistiques Squid
- Statistiques courrier

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

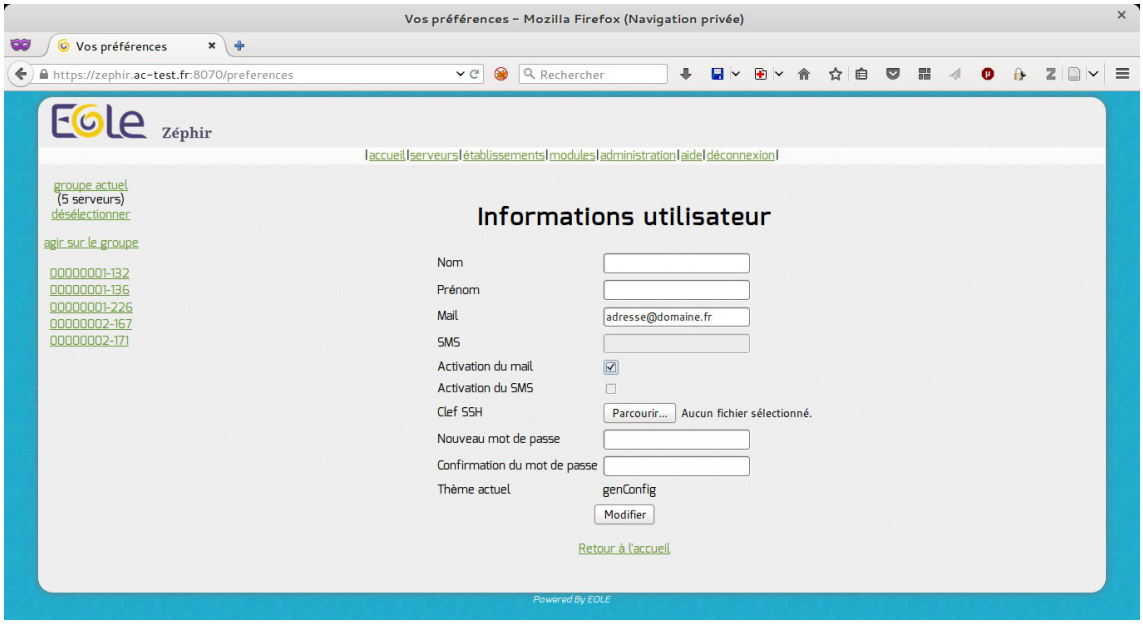
Les différents types d'erreurs possibles sont les suivants :

- 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, ...).

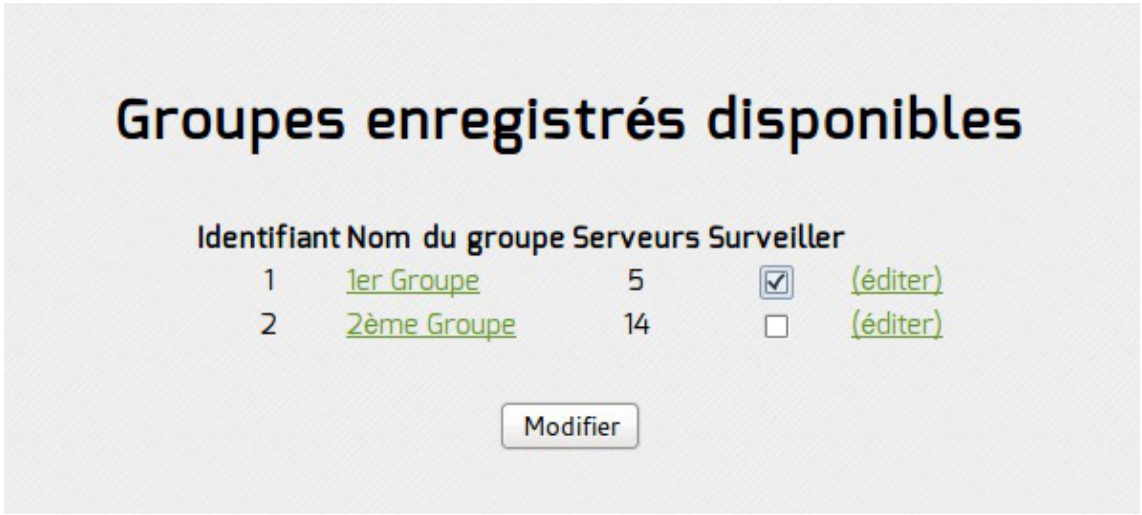
Pour recevoir des courriers électroniques d'alerte, il faut :

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- 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 ;



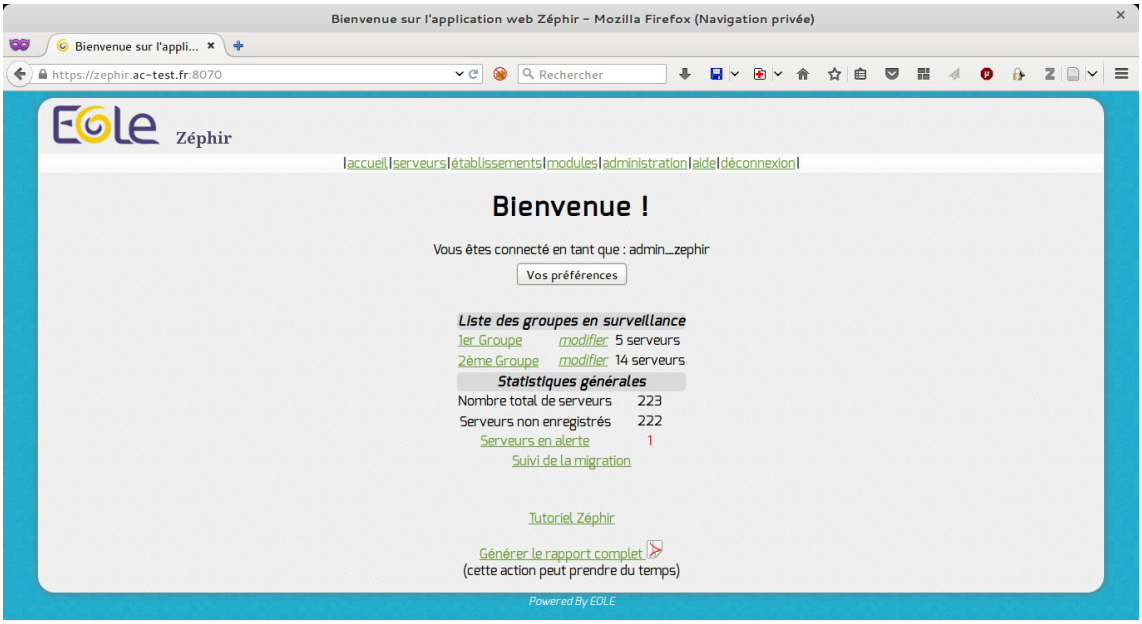
Vous recevrez un courrier électronique en cas de problème sur un serveur et un autre lorsque le serveur retrouvera son état normal.



Exemple d'alerte mail

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

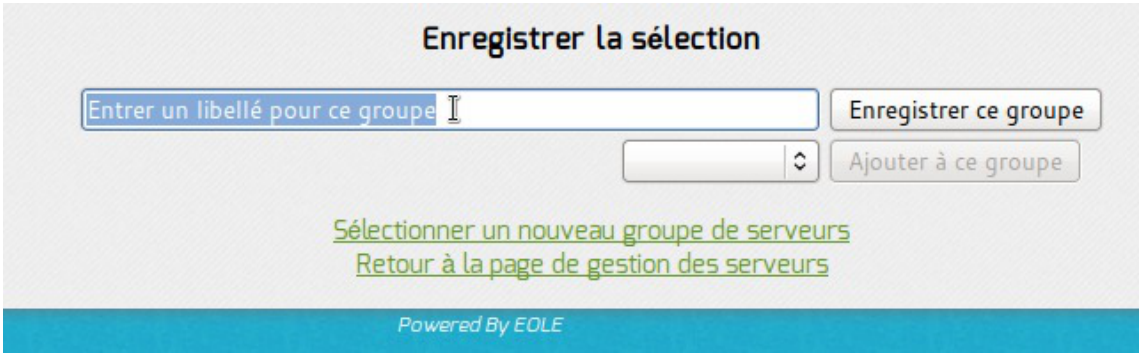


Ajout d'une sélection de serveurs à un groupe existant



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`.

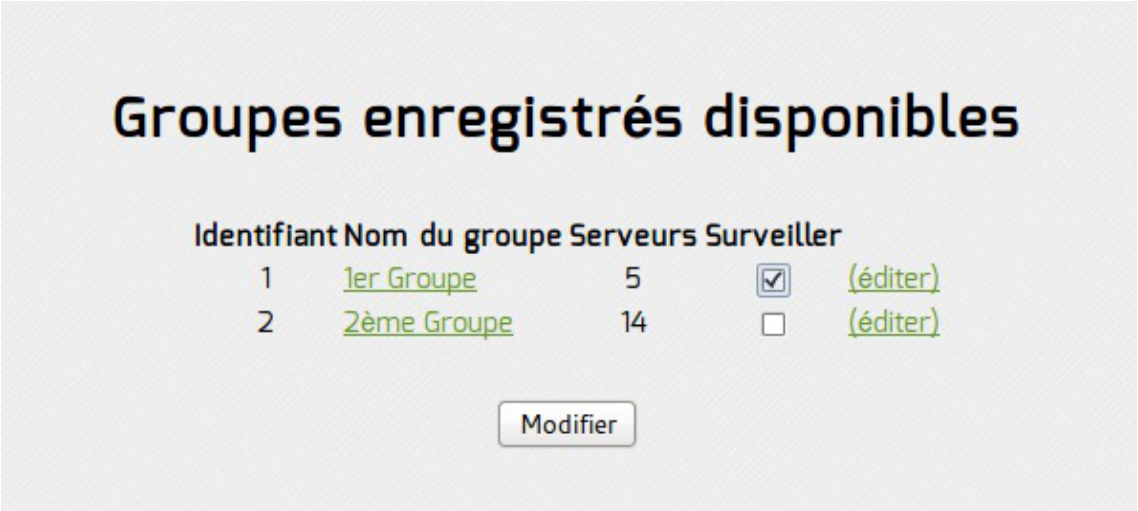


Les groupes enregistrés sont statiques. Si un nouveau serveur entre dans les critères, il faudra le rajouter manuellement.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

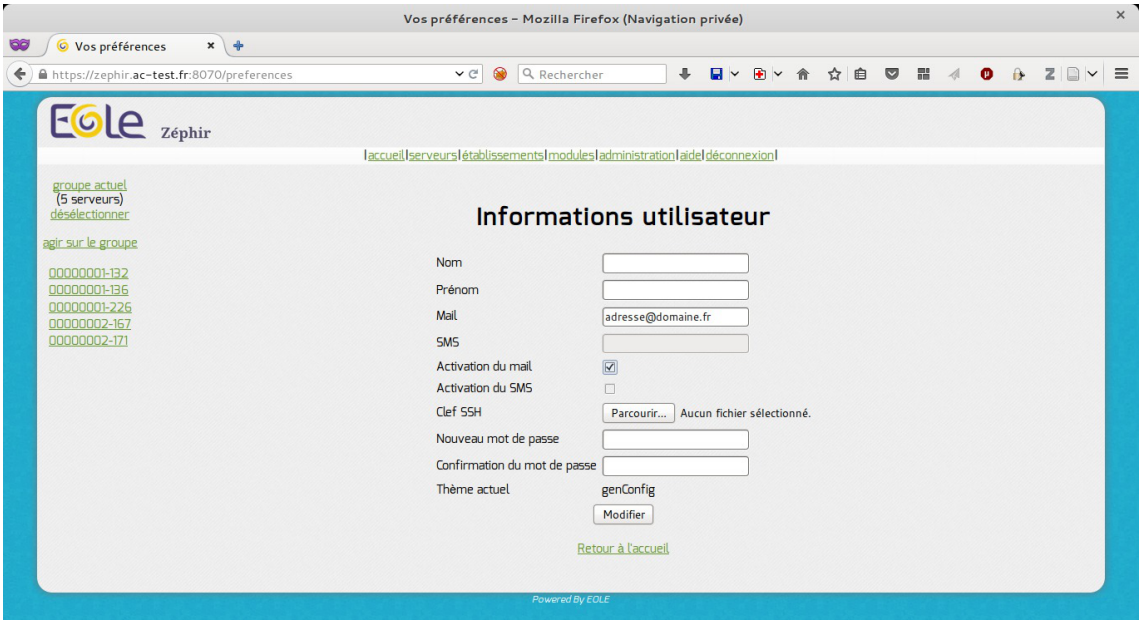
Le serveur Zéphir intègre la possibilité d'envoyer un courrier électronique quand un problème est détecté sur un des serveurs qu'il gère.
Les différents types d'erreurs possibles sont les suivants :

- 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, ...).

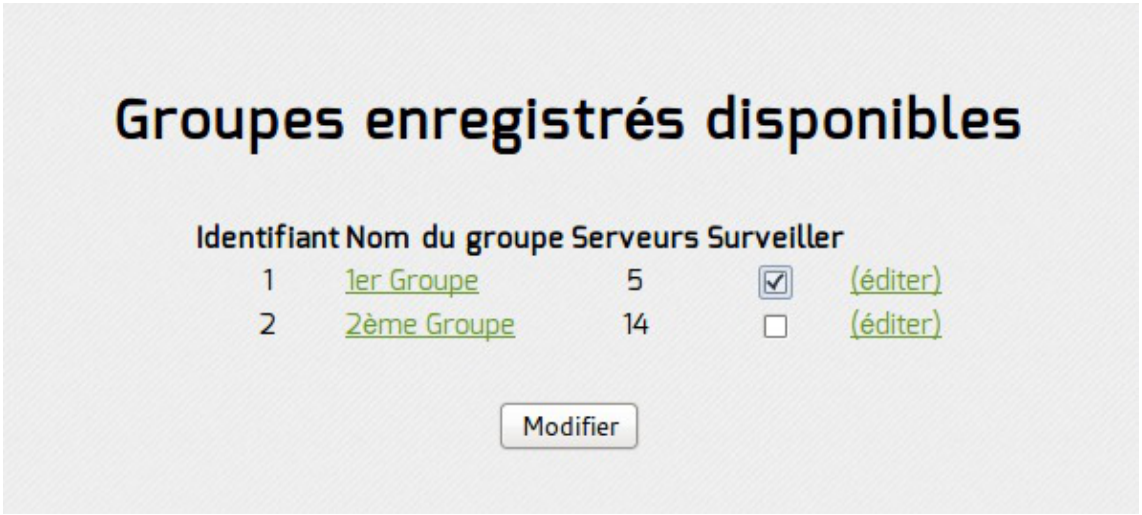
Pour recevoir des courriers électroniques d'alerte, il faut :

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- 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 ;



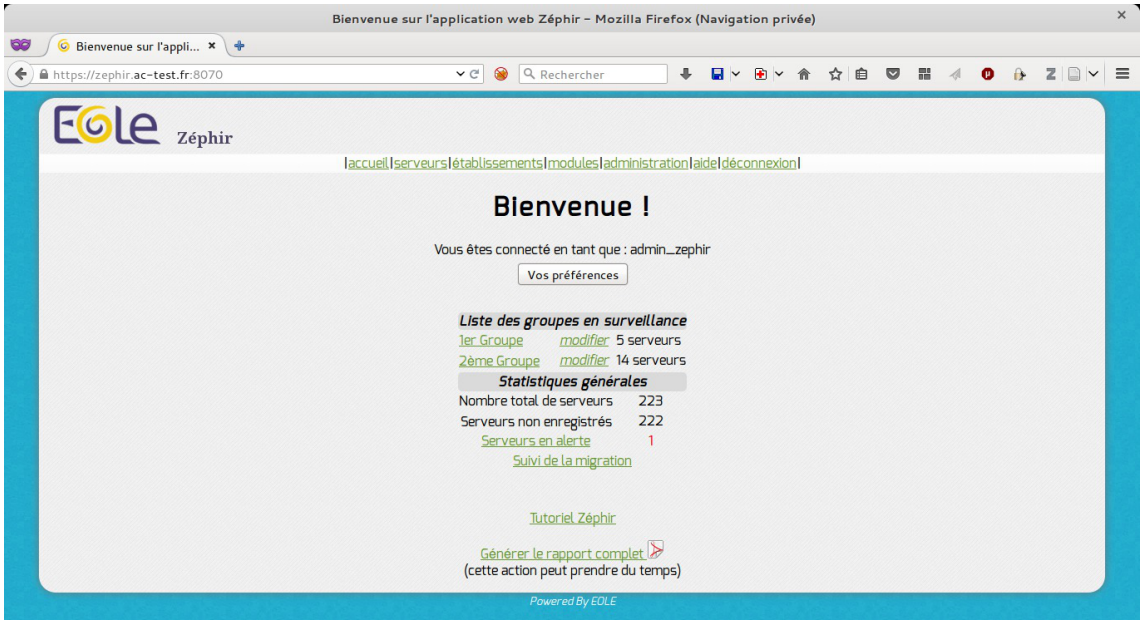
Vous recevrez un courrier électronique en cas de problème sur un serveur et un autre lorsque le serveur retrouvera son état normal.



Exemple d'alerte mail

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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),

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

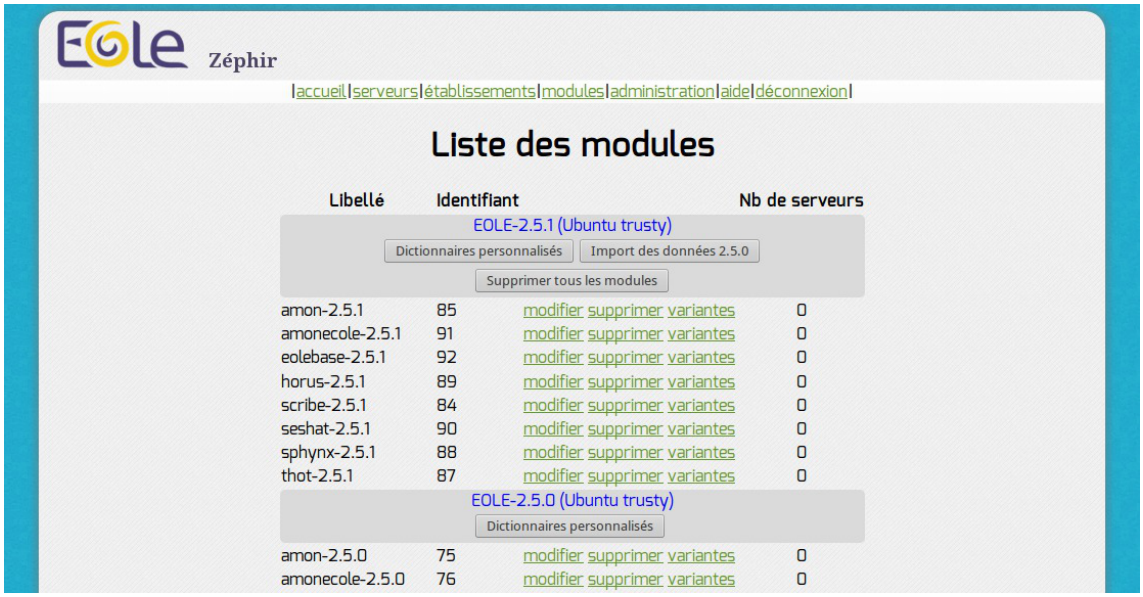
La notion de variante[p.476] est une fonctionnalité majeure de Zéphir. Une variante est une version modifiée d'un module EOLE que l'on veut pouvoir reproduire et déployer à volonté. Modifier une variante permet de modifier l'ensemble des serveurs utilisant cette variante.

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

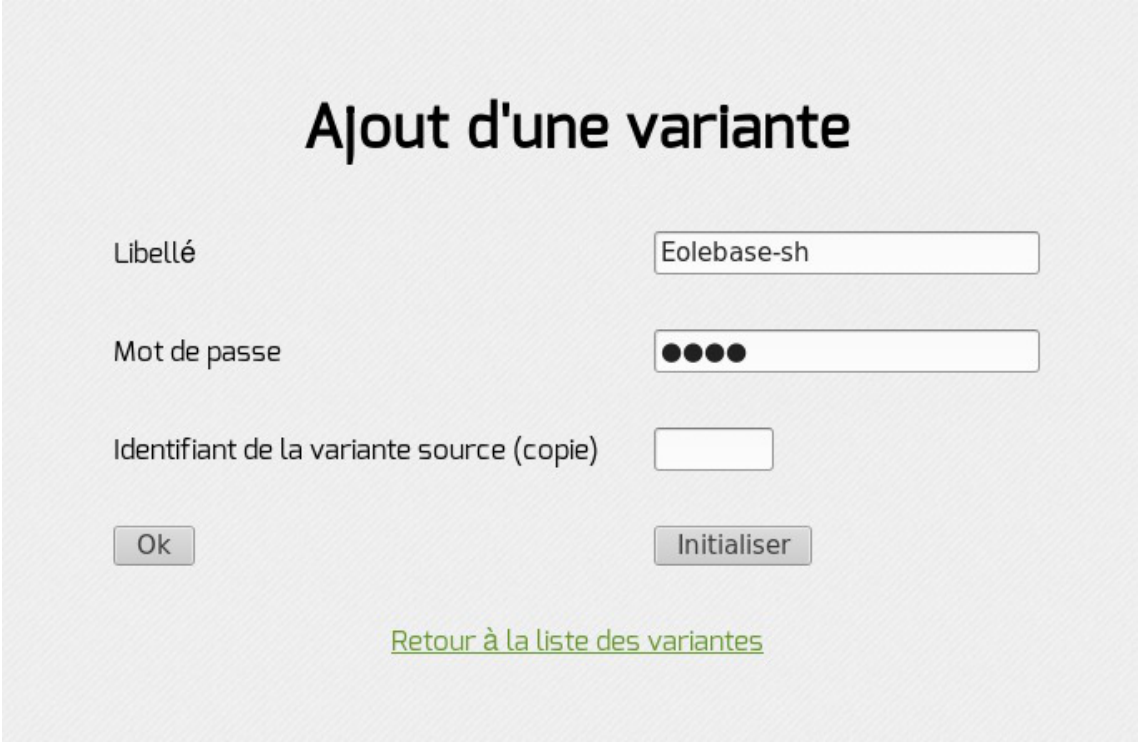
4.11.1. Créer une variante

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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
```

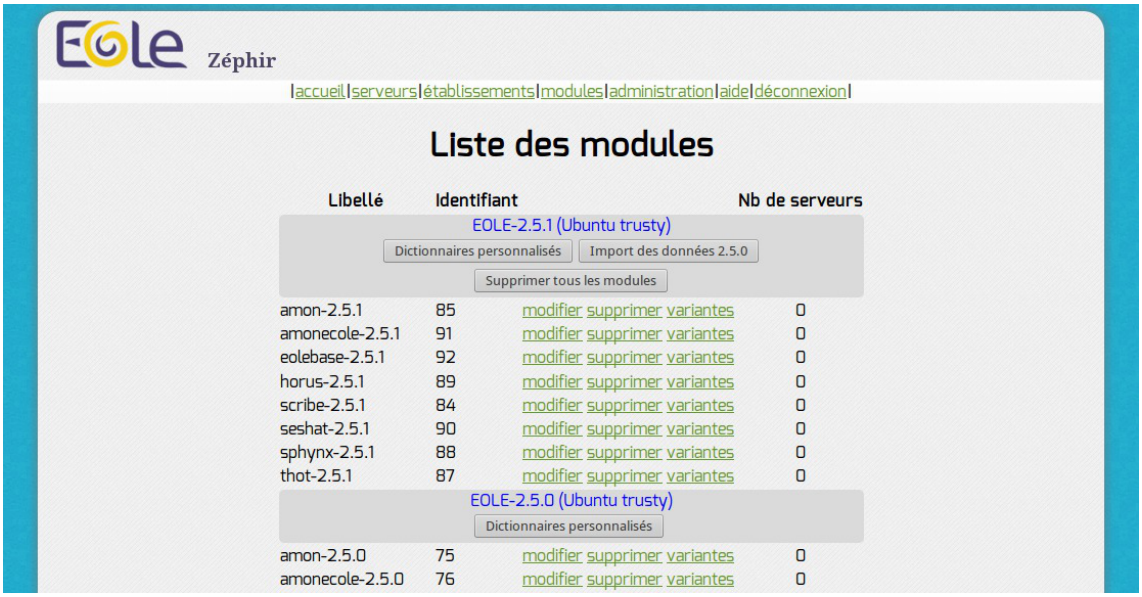

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

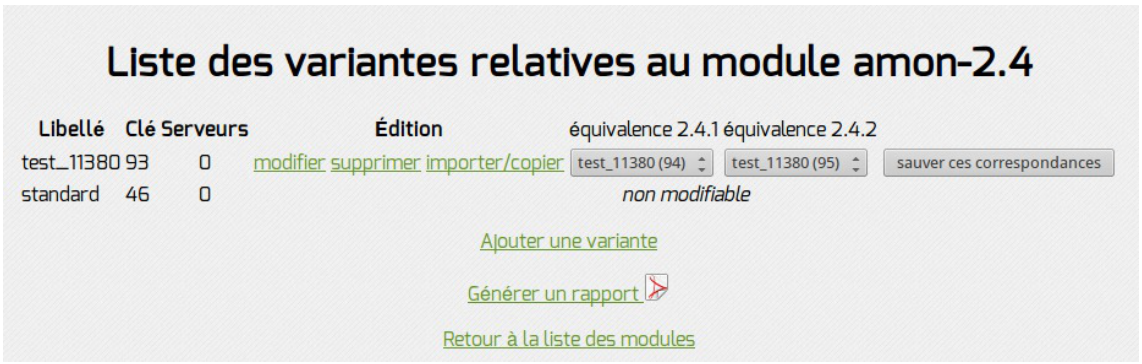
4.11.2. Modifier une variante

Depuis l'interface web

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

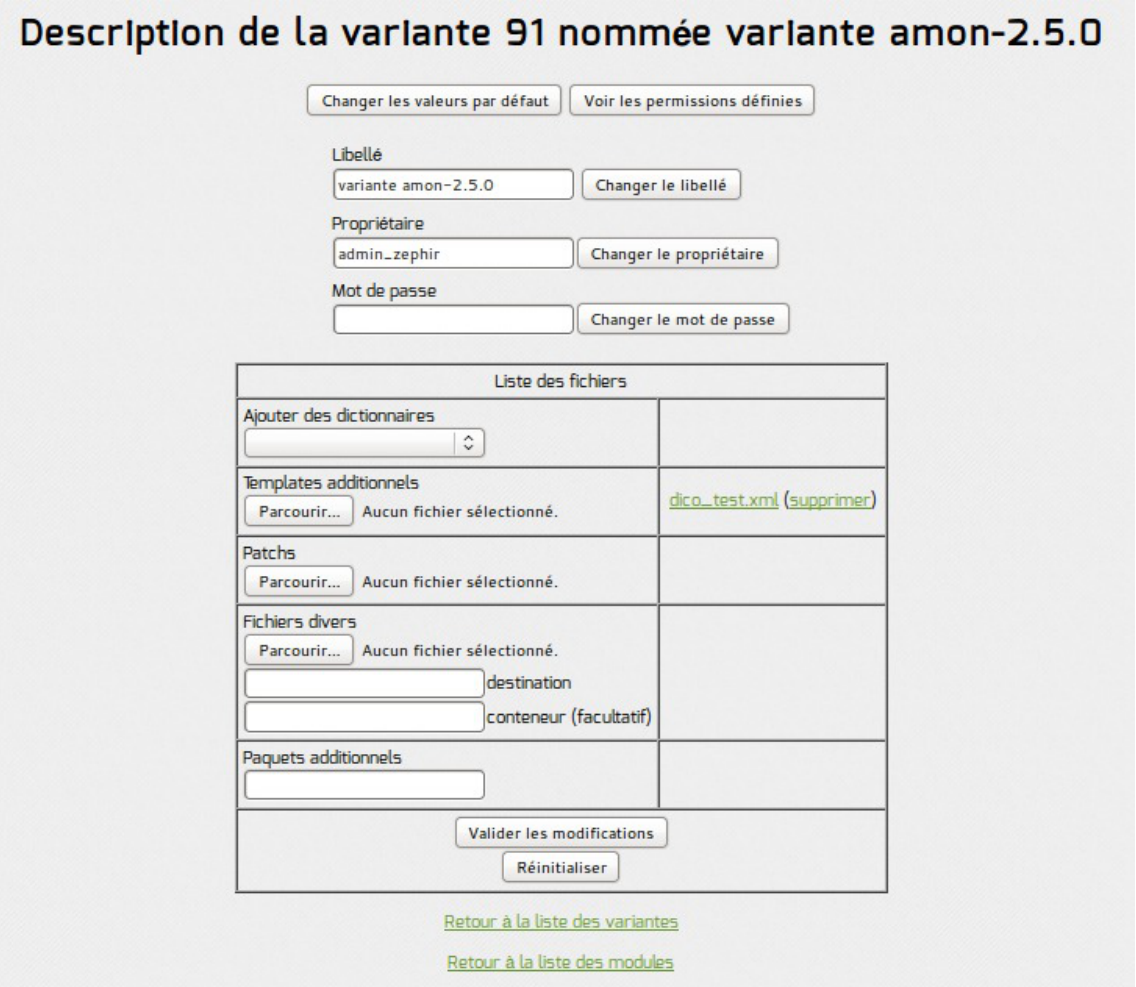


Cliquer sur le bouton `variantes` de la ligne correspondant au module choisi. Une liste des variantes apparaît.



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

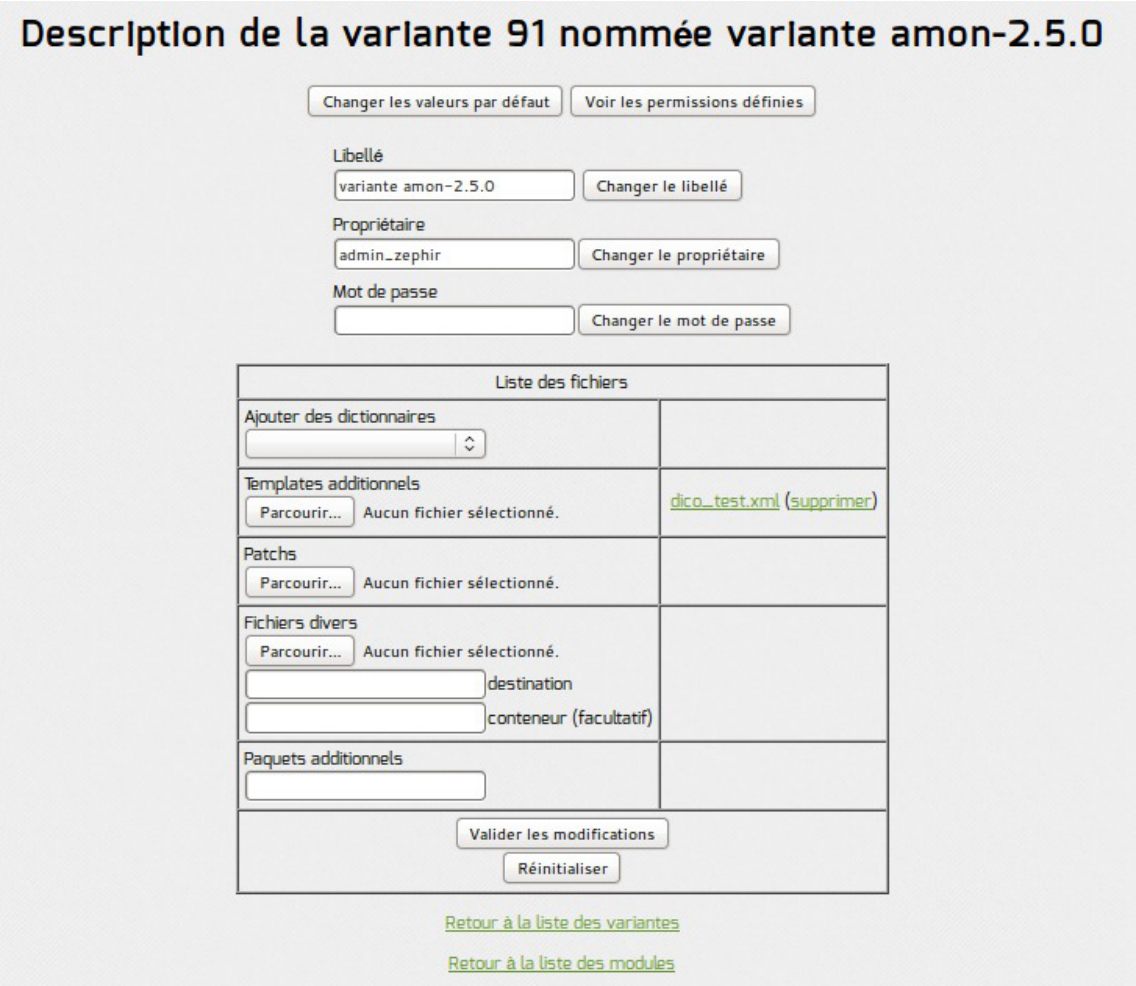
Si vous êtes connecté avec l'utilisateur qui a créé la variante vous pouvez ajouter les fichiers sans avoir à vous soucier du mot de passe. Celui-ci sera demandé si vous ajoutez des fichiers avec un autre utilisateur.

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 :



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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...
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

root@eolebase:~#
```



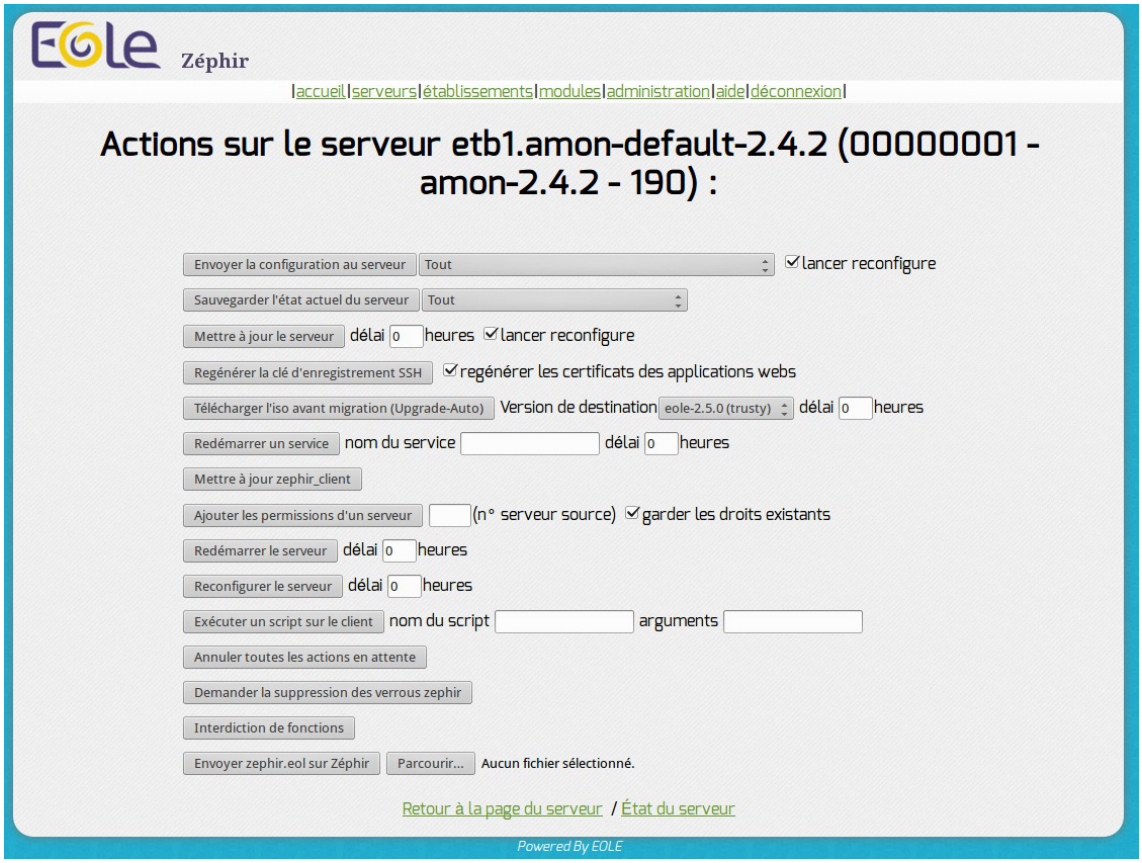
La mise à jour de variante est déconseillée une fois que plusieurs serveurs l'utilisent. En particulier soyez attentifs à d'éventuelles variables obligatoires sans valeur par défaut déclarées dans les dictionnaires.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

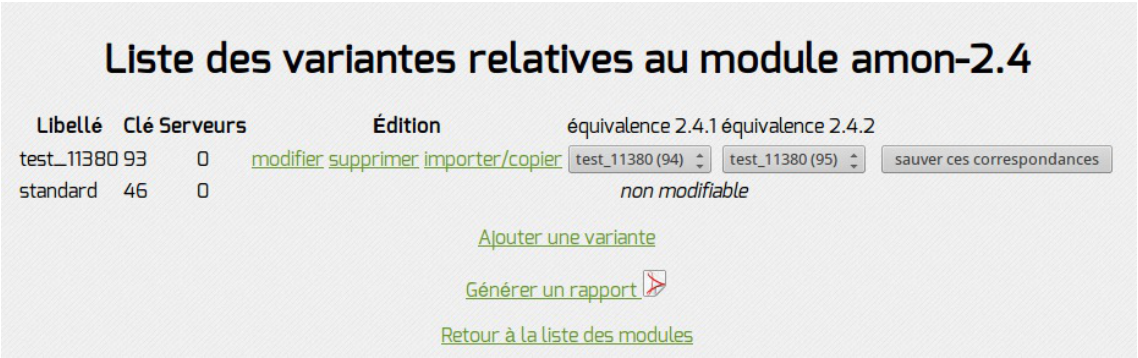
Importer une variante depuis un autre serveur Zéphir

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`.

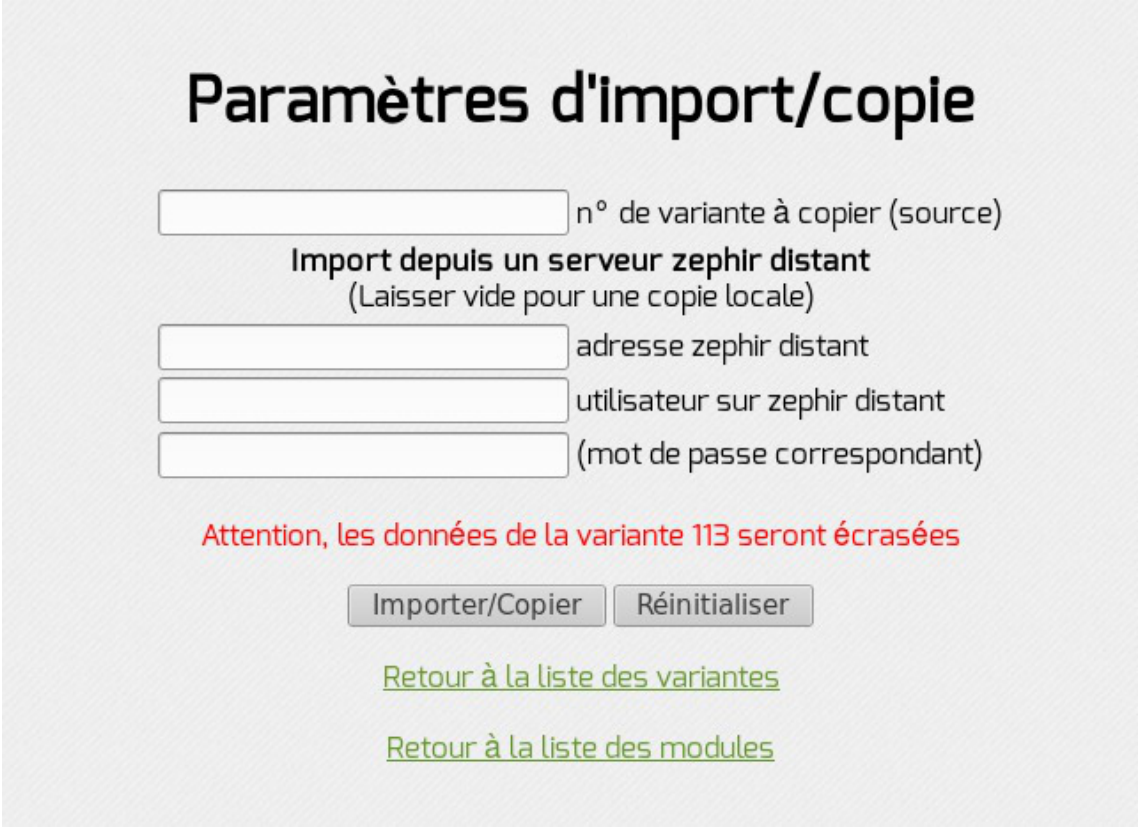


Dans le menu des variantes, cliquer sur `importer/copier` à côté de votre nouvelle variante.



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

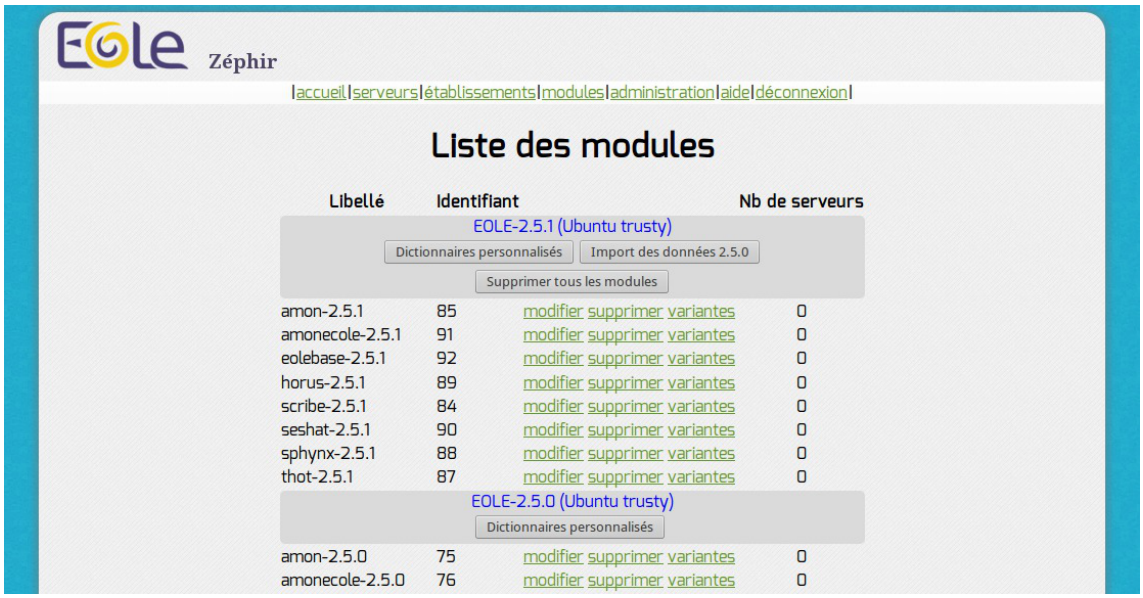
Pour les modules n'utilisant pas ce mode de gestion des dictionnaires (2.3 et antérieurs), le fichier existe mais est vide.

- 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.

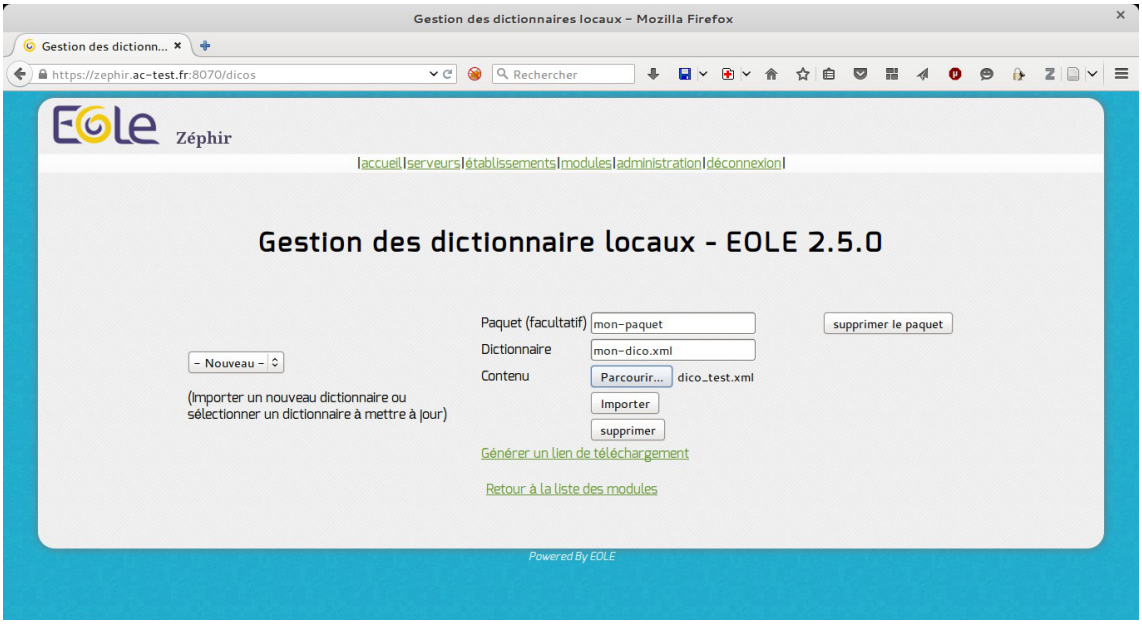
L'accès se fait par l'entrée `modules` du menu et en cliquant sur le bouton `Dictionnaires personnalisés`.



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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

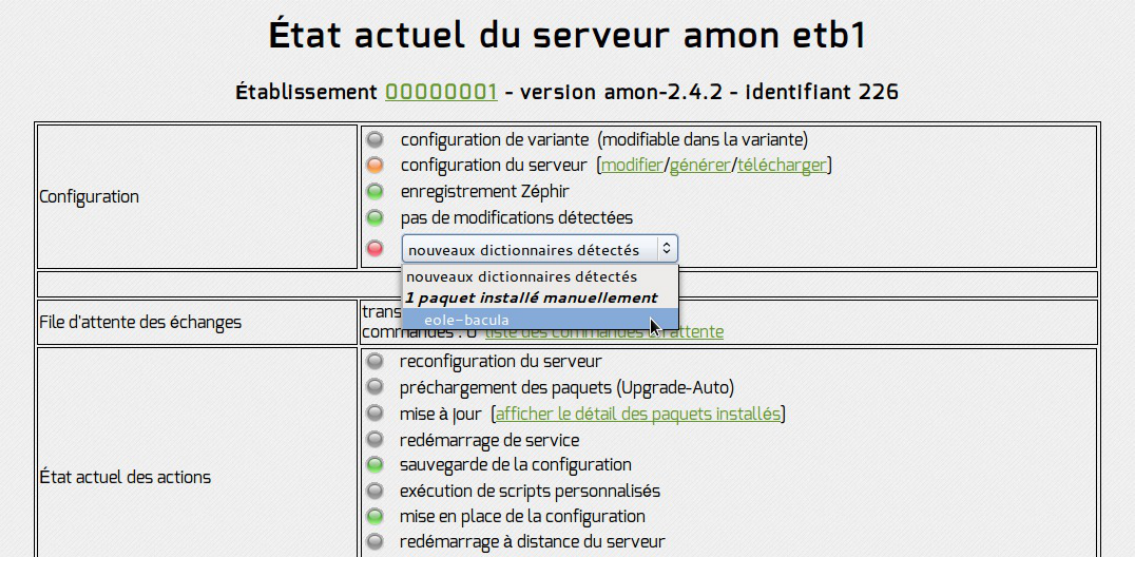
Si un utilisateur installe un paquet contenant des dictionnaires sans passer par le serveur Zéphir, certains problèmes peuvent survenir :

- 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- 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.



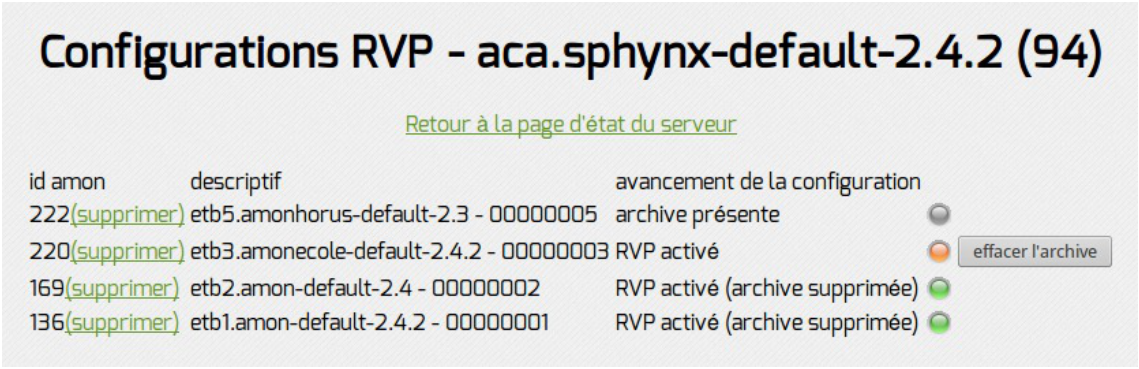
> Un critère de recherche a été ajouté dans l'onglet `serveurs` / `Sélection d'un groupe de serveurs` sous forme de case à cocher ☑ `Serveurs sur lesquels une installation manuelle de dictionnaires est détectée`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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) :
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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.468] génère une archive `tar.gz` par établissement à synchroniser ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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)
```

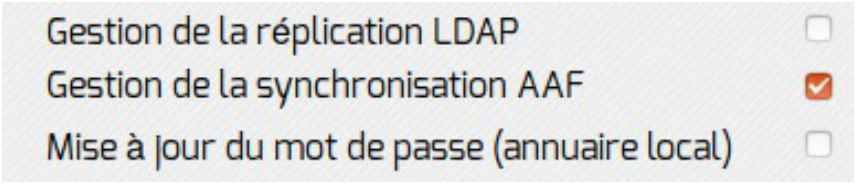
Pour supprimer l'association entre l'archive `0000001A.tar.gz` et le module Scribe :

```
z.aaf.del_file('0000001A.tar.gz')
```

L'utilisateur Zéphir utilisé pour effectuer les manipulations décrites ci-dessus doit posséder le

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

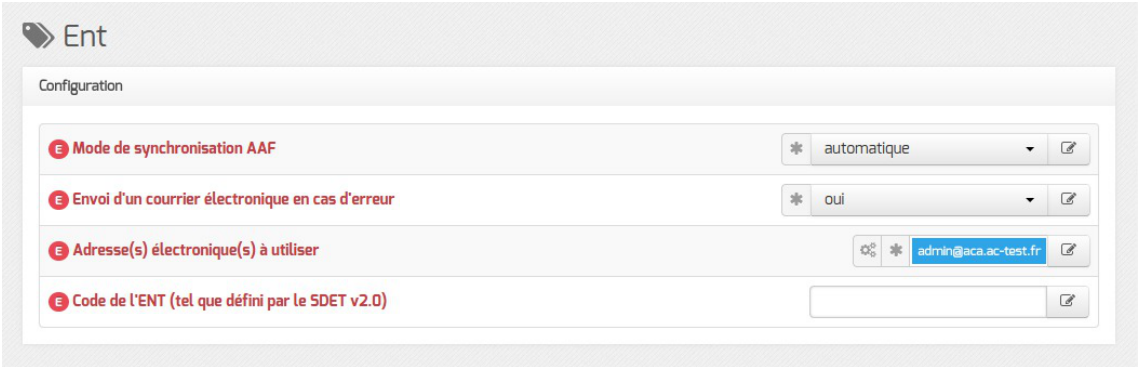
Gestion de l'archive sur le module Scribe

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`).

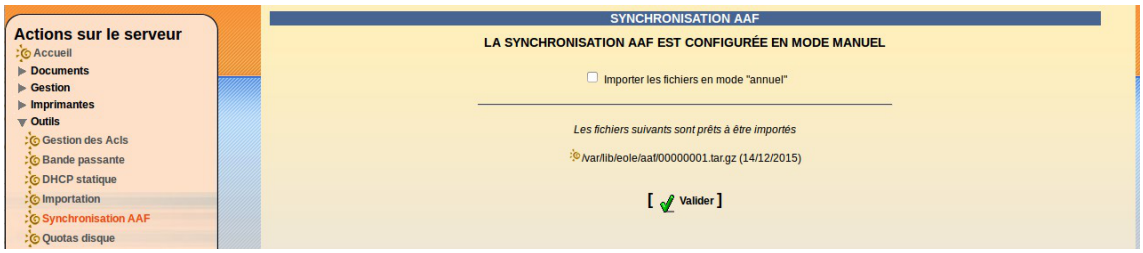
La variable `Envoi d'un courrier électronique en cas d'erreur` active l'envoi d'un

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.454] 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.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.470] 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

4.15. Désinscription d'un serveur

Pour désinscrire un serveur il faut exécuter la commande `enregistrement_zephir` et la désinscription est proposée.

```
root@eolebase:~# enregistrement_zephir

  Procédure d'enregistrement sur le serveur Zéphir


** Ce serveur est déjà enregistré sur le serveur Zéphir **

 - n°identifiant : 454
 - adresse de Zéphir : zephir.ac-test.fr

1 -> Désinscrire ce serveur du serveur Zéphir
2 -> Relancer l'enregistrement
3 -> Ne rien faire

  Entrez le numéro de votre choix : 1

Désinscription auprès du serveur Zéphir terminée

root@eolebase:~#
```

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
11
12 Adresse non envoyée aux serveurs suivants :
13
14   1, 6, 4, 2, 11, 9, 3, 5, 8, 7, 10, 12, 13, 18, 16
15
16 root@zephir:~#
```

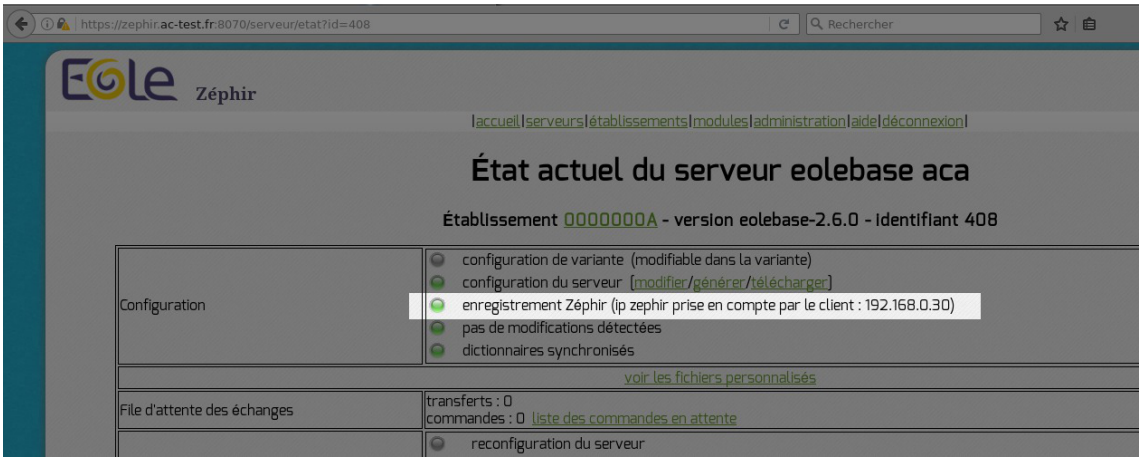
Pendant cette étape, le serveur Zéphir va générer les nouvelles clés et ajouter une action d'envoi de la clé à tous les clients.

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.

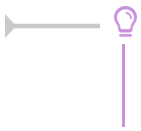
La commande `/usr/share/zephir/utils/prepare_ip.py -p` (ou --purge) permet d'annuler un changement d'adresse IP demandé sur l'ensemble des serveurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



Ce sont ces scripts qu'il faut utiliser pour effectuer un changement de machine ou le changement de version 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 se fait via `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 :
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
 8
 9 29-11-2016-15h36
10
11 Sauvegarde à restaurer (rien pour sortir): 29-11-2016-15h36
12 Arrêt du service Zéphir...
13 Décompression en cours...
14 Vérification des données...
15 Restaurer la base de données (o/n) ? o
16
17  - base PostgreSQL
18  - initialisation de la base
19  - injection des données
20  - régénération du mot de passe
21  - mise à jour du schéma de la base
22  - base LDAP
23  - configuration des serveurs
24  - dictionnaires personnalisés
25  - modules personnalisés
26  - configuration EAD
27  - certificats SSL
28  - configuration EoleSSO
29  - configuration EOLE
30
31 La configuration présente avant restauration a été copiée sous /etc/eole/config.old
32 Pour reprendre cette version, copier ce fichier sur /etc/eole/config.eol
33
34 Reconfigurez le serveur après la fin de la restauration
35
36
37 Système restauré
38
39 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

La restauration sur une nouvelle machine se fait si le serveur est instancié. Le script de restauration propose d'extraire le fichier `config.eol`.

Récupérer l'archive de sauvegarde soit depuis l'ancien serveur Zéphir soit depuis une copie stockée sur un autre support.

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).
Si le serveur n'est pas instancié, le script propose d'extraire le fichier `config.eol`.

```
1 root@zephir:~# /usr/share/eole/restauration.sh
2
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Le serveur doit être instancié pour permettre la restauration.

Si besoin, récupérer le fichier config.eol dans l'archive à restaurer :
# cd /var/lib/zephir_backups
# tar -xzf <nom_archive>.tar.gz
# cd <nom_archive> && tar -xf etc_eole.tar
# cp config.eol /etc/eole/
# cd /root && rm -rf /var/lib/zephir_backups/<nom_archive>

Valider la configuration avec gen_config, puis lancer instance
root@zephir:~#
```

Extraire le fichier `config.eol`.

```
root@zephir:~# cd /var/lib/zephir_backups
root@zephir:/var/lib/zephir_backups# ll
total 1896
drwxr-xr-x  3 root root    4096 déc.  12 10:46 ./
drwxr-xr-x 51 root root    4096 déc.   1 14:13 ../
drwxr-xr-x  2 root root    4096 déc.  12 10:14 12-12-2016-10h14/
root@zephir:/var/lib/zephir_backups# tar -xzf 12-12-2016-10h14.tar.gz
root@zephir:/var/lib/zephir_backups# ll
total 1896
drwxr-xr-x  3 root root    4096 déc.  12 10:46 ./
drwxr-xr-x 51 root root    4096 déc.   1 14:13 ../
drwxr-xr-x  2 root root    4096 déc.  12 10:14 12-12-2016-10h14/
-rw-r--r--  1 root root 1927039 déc.  12 10:14 12-12-2016-10h14.tar.gz
root@zephir:/var/lib/zephir_backups# cd 12-12-2016-10h14/
root@zephir:/var/lib/zephir_backups/12-12-2016-10h14# tar -xf etc_eole.tar
root@zephir:/var/lib/zephir_backups/12-12-2016-10h14# cp config.eol /etc/eole/
```

Instancier le serveur à l'aide de la commande `instance`.

```
[...]
*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 Systemd 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 :
[...]
```

Exécuter le script `restauration.sh`.

```
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...
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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:~#
```



Il est alors nécessaire de réinstancier le serveur Zéphir en prenant garde de ne pas écraser la base de données (répondre `non` lorsqu'il est demandé de recréer les données).

7. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

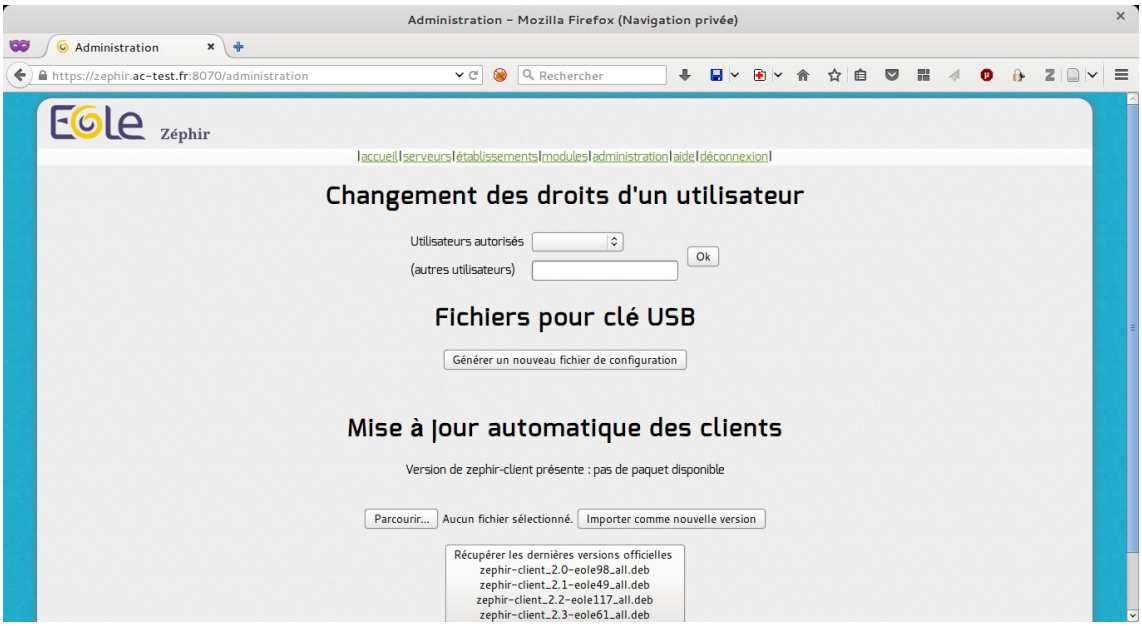
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

8. Divers petits outils

8.1. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

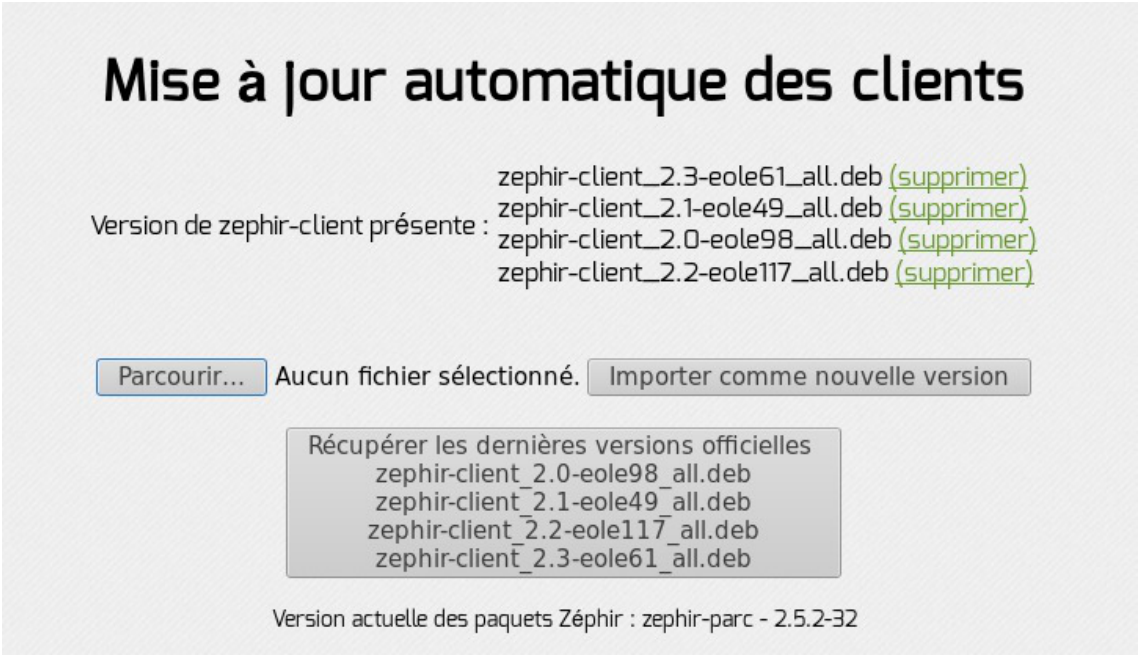
paramètres de connexion au serveur Zéphir.

La clé devra être montée manuellement sur le répertoire `/mnt/removable/` qu'il faut créer.

8.2. 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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 9

Personnalisation du module

Les modules EOLE peuvent être personnalisés et adaptés afin de prendre en compte les spécificités rencontrées en production.

1. Panorama des services

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. Services liés aux bases de données

1.1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un service d'annuaire 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, AmonEcole, 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)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.1.2. 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.

1.1.3. eole-db

Le paquet `eole-db` permet de configurer les bases de données utilisées sur un module EOLE.

Logiciels et services

Le paquet `eole-db` permet de configurer l'outil EoleDB.

Historique

EoleDB est une re-implémentation de l'ancien gestionnaire des bases de données EOLE (eole-sql).

Il est disponible depuis la version 2.5.2 d'EOLE.

Il est désormais utilisé par la majorité des applications web empaquetés par EOLE et Envole (OCS, GLPI, Roundcube, POSH, WordPress, Cdt, Taskfreak...).

De ce fait, il est automatiquement installé sur les serveurs possédant au moins l'une des applications utilisant cet outil.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.1.4. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de base de données Interbase[p.462].

Logiciels et services

Le paquet `eole-interbase` s'appuie principalement sur le service xinetd.

Historique

Historiquement ce service est uniquement utilisé sur le module Horus.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `interbase (id=16)`.
En mode conteneur, il est installé dans le groupe de conteneurs : `bdd (id=50)`

1.1.5. eole-mysql

Le paquet `eole-mysql` permet la mise en place d'un serveur de base de données MySQL[p.467].

Logiciels et services

Le paquet `eole-mysql` s'appuie principalement sur le service mysql-server.

http://www.mysql.fr/

Historique

Utilisé à la base sur les modules Horus, Scribe et Sentinelle, le paquet `eole-mysql` est installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mysql (id=14)`.
Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.1.6. eole-postgresql

Le paquet `eole-postgresql` permet la mise en place d'un serveur de base de données PostgreSQL [p.469].

Logiciels et services

Le paquet `eole-postgresql` s'appuie principalement sur le service postgresql.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

1.2. Services liés aux serveurs de fichiers

1.2.1. eole-ad-dc

Le paquet `eole-ad-dc` permet la mise en place d'un serveur Samba Active Directory[p.453] pouvant être soit contrôleur de domaine, soit membre d'un domaine existant.

Logiciels et services

Le paquet `eole-ad-dc` permet de gérer les services suivants :

- samba-ad-dc en mode contrôleur de domaine ;
- smbd, nmbd et winbind en mode serveur membre.

http://www.samba.org/

Historique

Le service a été créé spécifiquement pour le nouveau module 2.6 nommé Seth.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.2.2. eole-fichier-primaire

Le paquet `eole-fichie-primaire` permet la mise en place d'un serveur de fichiers PDC[p.469] complet.

Logiciels et services

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le paquet `eole-fichie-primaire` permet de gérer les services suivants :

- smbd, nmbd (serveur de fichiers) ;
- nscd (cache).

http://www.samba.org/

Historique

Les services fournis sont spécifiques aux modules Horus et Scribe.

Grâce au paquet `eole-fichier-primaire`, la configuration de base est identique sur les deux modules bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)`.

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.3. eole-fichier-membre

Le paquet `eole-fichier-membre` permet la mise en place d'un serveur de fichiers membre d'un domaine existant.

Logiciels et services

Le paquet `eole-fichier` permet de gérer les services suivants :

- smbd, nmbd (serveur de fichiers) ;
- nscd (cache) ;
- winbind.

http://www.samba.org/

Historique

Les services fournis sont spécifiques au module eSBL.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)` .



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse ip fichier link`).

1.2.4. eole-cups

Le paquet `eole-cups` permet la mise en place d'un serveur d'impression.

Logiciels et services

Le paquet `eole-cups` permet de gérer le service cups (serveur d'impression).

http://www.cups.org/

Historique

Les services fournis sont spécifiques aux modules Horus, Scribe et eSBL.

Grâce au paquet `eole-fichier`, la configuration de base est identique sur tous les modules bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)`.

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.



> En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse ip fichier link`).

1.2.5. eole-proftpd

Le paquet `eole-proftpd` permet la mise en place d'un serveur FTP[p.460].

Logiciels et services

Le paquet `eole-proftpd` permet de gérer le service proftpd (serveur FTP).

http://www.proftpd.org/

Historique

Les services fournis sont spécifiques aux modules Horus, Scribe et eSBL.

Conteneurs

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le service est configuré pour s'installer dans le conteneur : `ftp (id=25)`.
Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.



En mode conteneur, couplé à l'un des paquets `eole-fichier`, l'accès à ce service nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

Remarques

L'accès au service FTP peut être facilité par la mise en œuvre du gestionnaire de fichiers en ligne Pydio.

Voir aussi...

Pydio : gestionnaire de fichiers

1.2.6. eole-dhcp

Le paquet `eole-dhcp` permet la mise en place d'un serveur DHCP[p.457] local et/ou d'un serveur PXE[p.470].

Logiciels et services

Le paquet `eole-dhcp` s'appuie sur les services dhcp3-server et tftpd-hpa.

http://www.isc.org/software/dhcp

Historique

A la base, les services DHCP et TFTP étaient pré-installés uniquement sur les serveurs de fichiers (modules Scribe et Horus) ainsi que sur le serveur de clients légers Eclair, ceci avec des configurations hétérogènes et très limitées.
La mise en commun des configurations permet de bénéficier de toutes les options sur chaque module.
Ce paquet peut désormais être installé sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dhcp (id=17)`.
Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.

Remarques

Ne pas confondre ce paquet avec le paquet `eole-dhcrelay` qui est pré-installé sur le module Amon.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.2.7. eole-nfs

Le paquet `eole-nfs` permet la mise en place d'un serveur NFS[p.467] (partage de fichiers en réseau).

Logiciels et services

Le paquet `eole-nfs` s'appuie sur le service nfs-kernel-server.

http://nfs.sourceforge.net/

Historique

L'installation et l'activation de ce service sur le module Scribe, Horus ou AmonEcole est obligatoire si l'on souhaite accéder aux partages par le biais d'un serveur Eclair.

Conteneurs

Le service s'installe sur système hôte (maître) et non dans un conteneur.

Remarques

Le protocole NFS étant peu sécurisé, il est recommandé de ne pas ouvrir ce service sur l'intégralité du réseau.

1.3. Services liés au web

1.3.1. eole-web

Le paquet `eole-web` permet la mise en place d'un serveur web.



L'installation d'`eole-web` entraîne celle d'`eole-mysql`.

Logiciels et services

Le paquet eole-web s'appuie principalement sur le service apache2.

http://httpd.apache.org/

Il permet également d'activer l'application phpMyAdmin.

http://www.phpmyadmin.net/

Historique

À la base uniquement disponible sur les modules Scribe/AmonEcole, le paquet `eole-web` est désormais installable sur n'importe quel module EOLE.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `web (id=15)`.

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Ce paquet sert de brique de base pour toutes les applications web empaquetées par les équipes des projets EOLE et Envole.

1.3.2. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, Nginx[p.467], peut également faire office de serveur web.

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Initialement conçu pour les modules Amon et AmonEcole, ce service est pré-installé sur tous les modules à partir de la version 2.6.1 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.3.3. eole-wpad

Le paquet `eole-wpad` permet la mise en place du service de découverte automatique du proxy par les navigateurs (WPAD[p.476]).

Le logiciel utilisé, Nginx[p.467], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ce service étaient auparavant inclus dans le paquet `eole-reverseproxy`. Il peut désormais être installé de façon indépendante.
Le paquet `eole-wpad` est pré-installé sur les modules Amon et AmonEcole.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.4. Services liés à la messagerie

1.4.1. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP[p.472] Exim[p.460].

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, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.2. eole-spamassassin

Le paquet `eole-spamassassin` permet la mise en place d'un serveur anti-spam.

Logiciels et services

Le paquet `eole-spamassassin` s'appuie principalement sur le service spamassassin.

http://spamassassin.apache.org/

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-spamassassin` est désormais

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.
Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.3. eole-courier

Le paquet `eole-courier` permet la mise en place d'un serveur POP[p.469] / IMAP[p.462].

Logiciels et services

Le paquet `eole-courier` s'appuie principalement sur les services courier-imap et courier-pop.

http://www.courier-mta.org/

Historique

Historiquement ces services sont uniquement utilisés sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.
Sur le module AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Le greffon `authProg` fourni par le paquet `courier-eolecas` permet au serveur IMAP d'être compatible avec une authentification CAS.
L'accès au service IMAP peut être facilité par la mise en œuvre de la messagerie web Roundcube.

Voir aussi...

> Roundcube : interface pour le courrier électronique

1.4.4. eole-sympa

Le paquet `eole-sympa` permet la mise en place d'un serveur de listes de diffusion.

Logiciels et services

Le paquet `eole-sympa` s'appuie principalement sur le service sympa.
Son interface d'administration nécessite un serveur web apache2.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

http://www.sympa.org/

Historique

Historiquement ce service est uniquement utilisé sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.
Sur le module AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

1.5. Services liés au proxy et à l'authentification

1.5.1. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les logiciels et services suivants :

- Squid[p.473] : proxy cache ;
- e2guardian[p.458] : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM[p.467] ou Kerberos[p.463].

http://www.squid-cache.org/
http://e2guardian.org
http://lightsquid.sourceforge.net/

Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.
Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `internet (id=53)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse ip proxy link`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Remarques

Afin d'assurer les authentifications en mode NTLM/Kerberos, ce paquet fournit des configurations Samba incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

1.5.2. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur RADIUS[p.470].

Logiciels et services

Le paquet `eole-radius` s'appuie sur le projet FreeRADIUS.

http://freeradius.org/

Historique

Ce paquet est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6. Services liés à la virtualisation

1.6.1. eole-libvirt

Le paquet `eole-libvirt` permet la mise en place de la gestion de la virtualisation.

Logiciels et services

Le paquet `eole-libvirt` s'appuie sur le service libvirt[p.464].

http://libvirt.org/

Historique

Utilisé à la base sur les modules Hâpy et Hâpy Node, le paquet `eole-libvirt` est installable sur n'importe quel module EOLE.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.2. eole-one-frontend

Le paquet `eole-one-frontend` permet la mise en place de l'interface de gestion des machines virtuelles, OpenNebula Sunstone[p.474].

Logiciels et services

Le paquet `eole-one-frontend` s'appuie sur le service opennebula-sunstone.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy , le paquet `eole-one-frontend` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.3. eole-one-node

Le paquet `eole-one-node` permet la mise en place de la gestion d'un nœud de calcul (nœud de travail).

Logiciels et services

Le paquet `eole-one-node` s'appuie sur le service opennebula-node.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy et Hâpy Node, le paquet `eole-one-node` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.6.4. eole-one-singlenode

Le paquet `eole-one-singlenode` permet la mise en place de l'interface de gestion des machines virtuelles.

Logiciels et services

Le paquet `eole-one-singlenode` s'appuie sur le service opennebula-node.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy , le paquet `eole-one-singlenode` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7. Autres services réseau

1.7.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.



Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro.

http://dev-eole.ac-dijon.fr/projects/eole-antivir

http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon et clamav-freshclam.

http://www.clamav.net/

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

contenu), ...
La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirales (freshclam) s'installe sur le maître.
Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.
Sur le module AmonEcole, le service clamav-daemon est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.

C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>eole-antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.7.2. eole-apt-cacher-ng

Le paquet `eole-apt-cacher-ng` permet d'installer et de configurer un service de mise en cache des paquets Debian.

Logiciels et services

Le paquet `eole-apt-cacher-ng` s'appuie sur le service apt-cacher-ng.

https://www.unix-ag.uni-kl.de/~bloch/acng/

Historique

Ce service est pré-installé et obligatoire sur le module AmonEcole où il est utilisé par le maître et les conteneurs LXC.
Il est envisageable de l'installer sur n'importe quel module, afin, par exemple de fournir un service de mise en cache des paquets au niveau d'un établissement.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.7.3. eole-bareos

Le paquet `eole-bareos` permet d'installer et de configurer la solution de sauvegarde Bareos[p.454].

La gestion des sauvegardes fait l'objet d'une documentation dédiée : Sauvegardes.

Logiciels et services

Le paquet `eole-bareos` s'appuie sur les services :

- bareos-dir (service directeur)
- bareos-fd (service de lecture/écriture)
- bareos-sd (service de stockage)

http://www.bareos.org [http://net-snmp.sourceforge.net/]

Historique

Ce service est pré-installé sur les modules hébergeant un serveur de fichiers (Horus, Scribe, AmonEcole).
Il est utilisable sur tous les modules EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.4. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS[p.458] local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.454].

http://www.isc.org/downloads/bind/

Historique

À la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dns (id=18)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.7.5. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP[p.457].

Logiciels et services

Le paquet `eole-dhcrelay` s'appuie sur le service dhcp3-relay.

http://www.isc.org

Historique

Ce service est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.6. eole-ltsp-server

Le paquet `eole-ltsp-server` permet la mise en place d'un serveur de clients légers LTSP[p.470].

Logiciels et services

Le paquet `eole-ltsp-server` s'appuie sur les service NBD[p.467] et LDM[p.463].

http://ltsp.org/

Historique

Ce paquet, initialement conçu pour le module Eclair 2.3 intègre désormais les fonctionnalités apportées par l'ancien paquet `eole-ltsp-fichier`.

Conteneurs

Contrairement à la version proposée sur EOLE 2.3, le service s'installe sur le système hôte (maître).

1.7.7. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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).

1.7.8. eole-open-iscsi

Le paquet `eole-open-iscsi` permet de mettre en œuvre l'accès à un réseau de stockage SAN[p.472].

Logiciels et services

Le paquet `eole-open-iscsi` s'appuie sur les services open-iscsi et multipath.

http://www.open-iscsi.com

Historique

Ce service n'est pré-installé sur aucun module.

Initié grâce à une contribution de Karim Ayari de l'académie de Lyon, a été repris par l'équipe EOLE pour répondre à des besoins exprimés par le ministère de l'écologie.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.9. eole-pacemaker

Le paquet `eole-pacemaker` permet la mise en place d'un service de haute disponibilité[p.461].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync[p.456].

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

http://clusterlabs.org/

Historique

A la base, le service de haute disponibilité était uniquement disponible sur le module Sphynx via le service Heartbeat. Celui-ci se fait maintenant via les logiciels Corosync et Pacemaker. Le service a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.10. eole-snmpd

Le paquet `eole-snmpd` permet d'installer et de configurer un serveur SNMP[p.472].

Logiciels et services

Le paquet `eole-snmpd` s'appuie sur le service snmpd.

http://net-snmp.sourceforge.net/

Historique

Ce service n'est pré-installé sur aucun module.
Il a été créé et mis à disposition pour répondre à un besoin exprimé par plusieurs académies.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.11. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN[p.471].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.473].

http://www.strongswan.org/

Historique

Ce paquet est pré-installé sur les modules Amon et AmonEcole ainsi que sur le module Sphynx.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Conteneurs

Le service s'installe sur le serveur maître.

2. Personnalisation du serveur à l'aide de Creole

Creole[p.457] est un ensemble d'outils permettant de mettre en œuvre un serveur suivant une configuration définie.

Il offre des possibilités de personnalisation, permettant à l'utilisateur d'ajouter des fonctionnalités sur le serveur sans risquer de créer une incohérence avec la configuration par défaut et qui ne seront pas écrasées par les futures mises à jour.

Pour personnaliser un serveur, les outils suivants sont à disposition :

- le **patch[p.469]** : permet de modifier un template[p.475] fourni par EOLE ;
- le **dictionnaire[p.457] local** permet d'ajouter des options à l'interface de configuration, d'installer de nouveaux paquets ou de gérer de nouveaux services ;
- le **template**[p.475] reprend le fichier de configuration d'une application avec, éventuellement, une personnalisation suivant des choix de configuration.

2.1. Répertoires utilisés par EOLE

Répertoires liés au logiciel Creole

Dictionnaires

- `/usr/share/eole/creole/dicos/` : contient les dictionnaires fournis par la distribution ;
- `/usr/share/eole/creole/dicos/local/` : contient les dictionnaires créés localement pour le serveur ;
- `/usr/share/eole/creole/dicos/variante/` : contient les dictionnaires fournis par une variante Zéphir.

Templates

- `/usr/share/eole/creole/distrib/` : contient tous les templates (distribution, locaux et issus de variantes) ;
- `/usr/share/eole/creole/modif/` : répertoire à utiliser pour créer des patch avec l'outil `gen patch` ;
- `/usr/share/eole/creole/patch/` : contient les patch réalisés localement (avec ou sans l'outil `gen patch`) ;
- `/usr/share/eole/creole/patch/variante/` : contient les patch fournis par une variante Zéphir ;
- `/var/lib/eole/` : répertoire recommandé pour le stockage des fichiers templatisés nécessitant un traitement ultérieur ;
- `/var/lib/creole/` : contient la copie des templates après la phase de patch (traitement interne à Creole).

Autres répertoires spécifiques

- `/etc/eole/` : contient les fichiers de configuration majeurs du module ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `/var/lib/eole/config/` : contient les fichiers de configuration de certains outils internes ;
- `/var/lib/eole/reports/` : contient des fichiers de rapport (pour affichage dans l'EAD, par exemple) ;
- `/usr/lib/eole/` : librairies shell EOLE (remplacent *FonctionsEoleNg*) ;
- `/usr/share/eole/sbin/` : scripts EOLE ;
- `/usr/share/eole/diagnose/` : scripts *diagnose*.

2.2. Création de patch Creole

Si le fait de renseigner correctement les options de configuration n'offre pas une souplesse suffisante, il faut envisager des adaptations complémentaires.

Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à chaque `instance` / `reconfigure`.

Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch.

L'outil `gen_patch` vous permet de générer facilement un nouveau patch. Pour ce faire il suffit de copier le fichier de configuration depuis `/usr/share/eole/creole/distrib/` vers `/usr/share/eole/creole/modif/`, de le modifier et de lancer la commande `gen_patch`.



Copie du fichier du template d'origine :

```
root@scribe:~#     cp     /usr/share/eole/creole/distrib/php.ini
/usr/share/eole/creole/modif/
```

Changement des paramètres :

```
root@scribe:~# vim /usr/share/eole/creole/modif/php.ini
```

Exécution de la commande `gen_patch` :

```
root@scribe:~# gen_patch
** Génération des patches à partir de modif **
Génération du patch php.ini.patch
** Fin de la génération des patch **
root@scribe:~#
```

Une fois le patch créé, il faut lancer la commande `reconfigure` pour que les nouvelles options soient prises en compte.

La commande diagnose renvoie un diagnostic sur les patch :

```
[…]
*** Patches
. patches => Ok
[…]
```



Le nom du patch doit impérativement être celui du nom du fichier template à modifier suivi de

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'extension `.pacth`.

Exemple : `smb.conf.patch`

Sont concernés par la procédure de patch uniquement les fichiers déjà présents dans le répertoire des templates et référencés dans les dictionnaires fournis par l'équipe EOLE.

Pour les autres fichiers, l'utilisation de dictionnaires locaux et de templates personnalisés est recommandée.

Le répertoire `/usr/share/eole/creole/` contient les répertoires suivants :

- **./distrib/** : templates originaux fournis principalement par le paquet conf d'un module ;
- **./modif/** : endroit où doivent être copiés et modifiés les templates souhaités ;
- **./patch/** : fichiers patch générés à partir des différences entre les deux répertoires précédents.

Le répertoire `/var/lib/creole/` comprend les templates finaux, c'est à dire les templates initiaux avec éventuellement des patchs.

Pour désactiver un patch, il suffit de supprimer ou de déplacer le fichier patch.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptible d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

2.3. Les dictionnaires Creole

En cas d'ajout de templates[p.475] et de variables supplémentaires, il est nécessaire de créer un dictionnaire local.

Ce dictionnaire peut également comprendre des noms de paquet supplémentaire à installer ainsi que des services à gérer.

Un dictionnaire local est un dictionnaire personnalisé permettant d'ajouter des options à Creole.

Un dictionnaire Creole contient un en-tête XML suivi d'une balise racine **<creole></creole>**.

Structure générale d'un dictionnaire XML Creole

```
<?xml version='1.0' encoding='utf-8'?>
<creole>
    <files>
    </files>
    <containers>
    </containers>
    <variables>
    </variables>
    <constraints>
    </constraints>
    <help>
    </help>
</creole>
```

> Il est toujours intéressant de regarder dans les dictionnaires déjà présents sur le module pour comprendre les subtilités des dictionnaires Creole.

> Vous pouvez également vous référer à la DTD[p.458] :
> https://dev-eole.ac-dijon.fr/projects/creole/repository/revisions/master/entry/data/creole.dtd

2.3.1. Ajouter un en-tête XML

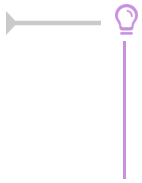
L'en-tête est standard pour tous les fichiers XML :

```
<?xml version="1.0" encoding="utf-8"?>
```

Cet en-tête est nécessaire pour que le fichier soit reconnu comme étant au format XML.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Afin d'éviter les problème d'encodage, il est conseillé de créer le fichier sur un module EOLE (avec l'éditeur de texte vim).



Ajouter la configuration suivante en bas de votre fichier pour forcer l'indentation :

```
<!-- vim: ts=4 sw=4 expandtab
-->
```

Voir aussi...

L'éditeur de texte Vim

2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu

Maître ou conteneur : <files> ou <containers>

Creole propose un système de conteneurs permettant d'isoler certains services du reste du système.

C'est dans le dictionnaire que les conteneurs sont définis et associés à des services.

Si le conteneur n'est pas spécifié, les services seront installés sur le serveur hôte, le maître.

Pour distinguer les fichiers templates, les paquets et les services de l'hôte de ceux mis dans le conteneur, il faut utiliser deux balises différentes.

Sur le serveur hôte, les fichiers templates, les paquets et les services sont dans une balise **<files>**.

Dans le cas des conteneurs, il faut spécifier un ensemble de balises **<container>** à l'intérieur d'une balise **<containers>**. L'utilisation de la balise **<all>** permet d'appliquer des balises à tous les **<container>**. En mode non conteneur cette balise s'applique sur le maître. Pour inhiber ce comportement il faut rajouter l'attribut **instance_mode='when_container'**.

La balise **<container>** doit obligatoirement contenir l'attribut **name** pour renseigner le nom du conteneur.

Lors de la première déclaration d'un conteneur l'attribution d'un identifiant unique (attribut **id**) est obligatoire.

La valeur de cet identifiant permettra de calculer l'adresse IP du conteneur.

Les groupes de conteneurs permettent de réunir des services afin de limiter le nombre de conteneurs.

Ils se déclarent de la même manière que les autres conteneurs. L'affectation d'un conteneur existant à un groupe de conteneurs s'effectue en utilisant l'attribut **group**.

Les ID de groupes de conteneurs de 50 à 99 sont réservés pour les groupes de conteneurs EOLE.

ID	Nom du groupe conteneur	Conteneurs inclus (AmonEcole/Eclair)
50	bdd	annuaire, mysql
51	reseau	web, mail
52	partage	fichier, dhcp, ftp
53	internet	proxy, dns

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

54	ltspserver	dhcp, ltsp
55	ltspapps	application

Les identifiants de conteneur supérieurs à 100 sont utilisables par les contributeurs.

La liste des identifiants des conteneurs et des groupes de conteneurs déjà affectés est actuellement maintenue sur le wiki EOLE à l'adresse :

http://dev-eole.ac-dijon.fr/projects/creole/wiki/ContainersID

```
<creole>
    <files>
    </files>
    <containers>
        <all>
            <host hostlist='web' name='web_url' ip='adresse_ip_br0' instance_mode='when_container' comment="Serveur web sur l'IP de l'interface 0" />
            <file filename='/etc/fichier_cible' instance_mode='when_container' />
        </all>
        <container name='web' id='15'>
            [...]
        </container>
        <container name='reseau' id='51'/>
        <!-- affectation du conteneur web au groupe de conteneurs reseau -->
        <container name='web' group='reseau'/>
    </containers>
    [...]
```

Paquets : <package>

Creole permet de spécifier les paquets à installer pour profiter d'un nouveau service.

A l'instanciation de la machine, les paquets spécifiés seront installés.

Pour cela, il faut utiliser la balise **<package>** avec comme contenu le nom du paquet.

Les attributs de la balise <package>

- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : *when_container*, *when_no_container*, *always* (par défaut).

Pour spécifier plusieurs paquets, il faut obligatoirement écrire une balise **<package>** par paquet.

Fichiers templates : <file>

Les fichiers templates sont définis dans la balise **<file>**.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les attributs de la balise <file>

- l'attribut **name** (obligatoire) indique l'emplacement où sera copié le fichier ;
- l'attribut **source** permet d'indiquer un nom de fichier source différent de celui de destination ;
- l'attribut **mode** permet de spécifier des droits à appliquer au fichier de destination ;
- l'attribut **owner** permet de forcer le propriétaire du fichier ;
- l'attribut **group** permet de forcer le groupe propriétaire du fichier ;
- l'attribut **filelist** permet de conditionner la génération du fichier suivant des contraintes ;
- si l'attribut **rm** vaut *True*, le fichier de destination sera supprimé si il est désactivé via une *filelist* ;
- si l'attribut **mkdir** vaut *True*, le répertoire destination sera créé si il n'existe pas ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : *when_container*, *when_no_container*, *always* (par défaut) ;
- l'attribut **del_comment** engendre la suppression des lignes vides et des commentaires dans le fichier cible afin d'optimiser sa templatisation (exemple : `del_comment='#'`).

Renommage d'un template

L'attribut **name** contient toujours le chemin complet du fichier de destination (par exemple `/etc/hosts`).

Par défaut, le fichier template doit s'appeller de la même façon que le fichier de destination (ici : `hosts`).

Si deux templates ont le même nom, il faudra spécifier le nom du template renommé avec l'attribut **source**.

Services : <service>

Les dictionnaires Creole intègrent un système de gestion de services GNU/Linux (scripts d'init) qu'il est possible d'utiliser pour activer/désactiver des services non gérés par le module EOLE installé.

Services non gérés : services non référencés dans le système de gestion des services de Creole. Ils ne sont jamais modifiés. Ils restent dans l'état dans lequel Ubuntu les a installés ou dans celui que leur a donné l'utilisateur. Les services non gérés sont généralement les services de base Ubuntu (rc.local, gpm, ...) et tous ceux pour lesquels le module ne fournit pas de configuration spécifique (mdadm, ...).

Services désactivés : services systématiquement arrêtés et désactivés lors des phases d'instance et de reconfigure. Les services concernés sont généralement liés à une réponse à "non" dans l'interface de configuration du module.

Services activés : services systématiquement activés et (re)démarrés lors des phases d'instance et de reconfigure. Les services concernés sont ceux nécessaires au fonctionnement du module.

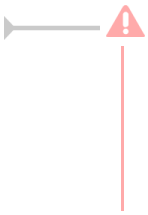
Les services à activer/désactiver se définissent dans le dictionnaire grâce à la balise **<service>.**

Les attributs de la balise <service>

- l'attribut **servicelist** (chaîne de caractères alphanumériques) permet de conditionner le démarrage ou l'arrêt d'un service suivant des contraintes ;
- l'attribut **method** permet de définir la façon de gérer les services : systemd (par défaut), apache et network ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'attribut **hidden** (booléen) indique si le service doit être activé ou non, cet attribut est particulièrement utile lors de la redéfinition d'un service, en particulier pour forcer sa désactivation ;
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir un service déjà défini dans un autre dictionnaire ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence ou non du mode conteneur : when_container, when_no_container, always (par défaut).



systemd est, dorénavant, la seule méthode valide pour la gestion des services. *upstart* est encore accepté pour assurer la rétrocompatibilité. Cependant, le service est, dans tous les cas, géré par *systemd*. Les anciens attributs *start_level*, *stop_level* et *pty='False'*, sans effet, ont été supprimés.

La balise service peut également être utilisée pour activer/désactiver des configurations de site web apache2 (commandes : `a2ensite` / `a2dissite`).
Comme pour les services système, l'activation d'un site peut être conditionnée par une `servicelist`.
On peut ainsi gérer le lien symbolique suivant : `/etc/apache2/sites-enabled/monsite` avec :

```
<service method='apache' servicelist='siteperso'>monsite</service>
```

Le fichier de configuration `monsite` étant stocké dans `/etc/apache2/sites-available/`.



Pour spécifier plusieurs services, il faut obligatoirement écrire une balise **<service>** par service.



Une règle `eole-firewall` peut être liée à un service, ainsi quand un service sera désactivé la règle le sera également.

Hôtes : <host>

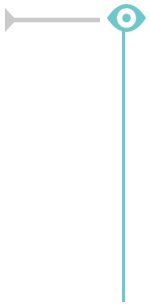
La balise **<host>** permet de déclarer des hôtes à ajouter dans le fichier `/etc/hosts` du maître et/ou des conteneurs.

Les attributs de la balise <host>

- l'attribut **name** contient le nom d'une variable contenant des noms d'hôtes (FQDN), simple ou multi, obligatoire ;
- l'attribut **ip** contient le nom d'une variable contenant les adresses IPs associées aux noms, obligatoire ;
- l'attribut **hostlist** permet d'exclure cette entrée suivant des contraintes, optionnel ;
- l'attribut **crossed** combine toutes les adresses avec tous les noms d'hôtes. L'utilisation de False génère une association 1 nom d'hôte/1 adresse IP. Doit être False dans le cas d'utilisation de variables ayant une relation maître/esclave, False, True (par défaut) ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : when_container, when_no_container, always (par défaut) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'attribut **comment** permet l'ajout d'une ligne de commentaire avant la(les) entrée(s), optionnel.



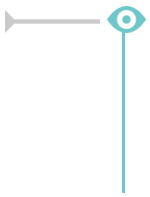
```
<containers>
    <container name="proxy" id='20'>
        <package>eole-proxy-pkg</package>
        <service>squid</service>
        <host hostlist='auth_smb' name='nom_serveur_smb' ip=
'ip_serveur_smb' instance_mode='when_container' crossed='False' comment=
"serveurs d'authentification SMB"/>
    </container>
</containers>
```

Montage d'une partition <disknod>

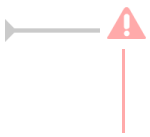
La balise **<disknod>** permet de le montage d'une partition du maître à l'intérieur d'un conteneur.
Par exemple, le montage de la partition `/home` dans le conteneur fichier.

Les attributs de la balise <disknod>

La balise **<disknod>** ne possède pas d'attribut spécifique.



```
<containers>
    <container name='fichier' id='12'>
        <disknod>/home</disknod>
    </container>
</containers>
```



Pour être pris en compte il faut nécessairement arrêter le conteneur avec la commande `CreoleService lxc stop` avant de faire un `gen_conteneurs`.

Montage d'un répertoire <fstab>

La balise **<fstab>** sert à déclarer le montage d'un répertoire (qui n'est pas une partition) à l'intérieur d'un conteneur.
Par exemple, le montage du répertoire `/home/mail/` du maître dans le conteneur mail.

Les attributs de la balise <fstab>

- l'attribut **name** contient le chemin du répertoire à monter ou le nom d'une variable fournissant cette information ;
- si l'attribut **name_type** vaut *SymLinkOption* cela indique que le chemin sera défini dans la variable indiquée dans l'attribut **name** ;
- l'attribut optionnel **mount_point** permet de définir le point de montage à l'intérieur du conteneur, par défaut c'est la valeur de l'attribut **name** ;
- si l'attribut **mount_point_type** vaut SymLinkOption cela indique que le chemin sera défini dans la variable indiquée dans l'attribut **mount_point** ;
- l'attribut optionnel **options** permet de définir les options de montage ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'attribut **fstablist** (chaîne de caractères alphanumériques) permet de conditionner le montage du répertoire suivant des contraintes.

```
<containers>
    <container name='mail' id='13'>
        <fstab name='/home/mail'/>
    </container>
</containers>
```

Pour être pris en compte il faut nécessairement arrêter le conteneur avec la commande `CreoleService lxc stop` avant de faire un `gen_conteneurs`.

Autorisations pour le pare-feu eole-firewall : <service_access> et <service_restriction>

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper[p.474] et l'activation de modules noyau.

eole-firewall et ERA

Pour les modules Amon et AmonEcole, les règles d'`eole-firewall` ne s'appliquent pas. Seules les règles ERA du modèle choisi s'appliquent.

Les doublons

S'il y a plusieurs règles sur une interface/port, c'est la dernière règle qui est appliquée .

Par exemple, dans le dictionnaire `20_apache.xml`, on redirige le port `80` dans le conteneur mais dans `25_nginx.xml`, on ouvre le port `80`. Si ces deux dictionnaires sont installés simultanément, c'est l'ouverture du port qui est appliquée.

L'activation des règles

Si le nom du service correspond a un service déclaré dans le conteneur et que celui-ci est désactivé, alors les accès/restrictions ne s'appliquent pas.

Si `ip` est une variable et que cette variable n'existe pas ou qu'elle est désactivée, la règle ne s'applique pas.

De la même façon pour un port/tcpwrapper avec une variable qui n'existe pas, aucune règle ne s'applique.

Malgré son nom, l'attribut `service` des balises `service_access` et `service_restriction` doit être renseigné avec le nom de la `servicelist` associée au service et non avec le nom du service lui-même.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Si aucune `servicelist` permettant de désactiver le service n'existe, l'attribut peut être rempli librement.

Autoriser un port (XXX) pour un service donné (YYY) :

```
<service access service='YYY'>
  <port>XXX</port>
</service access>
```

Dans la balise `port` il est également possible de spécifier le protocole (par défaut c'est TCP).

Par exemple :

```
<service access service='ntp'>
  <port protocol='udp'>123</port>
</service access>
```

Avec tcpwrapper :

```
<tcpwrapper>YYY</tcpwrapper>
```

Port avec variable (ZZZ) :

```
<port port type="SymLinkOption">ZZZ</port>
```

List (WWW) pour port/tcpwrapper :

```
<port service accesslist="WWW">XXX</port>
<tcpwrapper service accesslist="WWW">YYY</tcpwrapper>
```

Règles `eole-firewall` extraites du dictionnaire `/usr/share/eole/creole/dicos/01_network.xml`. pour le service `sshd`

```
<service_access service='sshd'>
    <port>22</port>
    <tcpwrapper>sshd</tcpwrapper>
</service_access>
<service_restriction service='sshd'>
    <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
    <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
    <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
    <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
    <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
</service_restriction>
```

Si on ne définit que les `service_access`, le port est ouvert pour tout le monde sur toutes les interfaces.

Pour ajouter des restrictions il faut mettre :

```
<service_restriction service='YYY'>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`  <ip interface='eth0'>1.1.1.1</ip>`

`<service_restriction>`

Dans ce cas, seule l'adresse IP `1.1.1.1` peut accéder à ce service.

Il est possible d'utiliser des variables :

`<ip interface='auto' ip type='SymLinkOption'>variable</ip>`

Il est possible d'utiliser un netmask :

`<ip interface='eth0' netmask="255.255.255.0" ip type='SymLinkOption'>variable</ip>`

`<ip interface='eth1' netmask="variable_netmask" netmask type='SymlinkOption' ip type='SymLinkOption'>variable</ip>`

Le paramètre `interface` peut être :

- `ethX` (pour une interface donnée) ;
- `all` (pour toutes les interfaces) ;
- `auto` (calcule de l'interface via la route) ;
- une variable (avec l'ajout de `interface type="SymlinkOption"`).

Il est aussi possible d'ajouter une `service restrictionlist` aux balises `ip`.

Règles `eole-firewall` extraites du dictionnaire `/usr/share/eole/creole/dicos/01_network.xml` pour le service `genconfig`

```
<service_access service='genconfig'>
    <port>7000</port>
</service_access>
<service_restriction service='genconfig'>
    <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
    <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
    <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
    <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
    <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
</service_restriction>

```

Complément sur les attributs

instance_mode

L'attribut instance_mode remplace les anciens attributs in_container et container_only.

Une ressource, qu'elle soit sur le maître ou dans un conteneur, peut n'être à générer que si le mode conteneur est activé ou désactivé :

instance_mode	mode conteneur	mode non conteneur
when_container	✓	

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

when_no_container		✓
always (default)	✓	✓

Les balises acceptant l'attribut instance_mode sont actuellement :

- package ;
- file ;
- service ;
- host ;
- fstab.

Exemple récapitulatif

Fichiers templates, paquets et services locaux ou dans un conteneur

```
<containers>
  <!-- dans le conteneur mon_reverseproxy -->
  <container name="mon_reverseproxy" id='101'>
    <package>nginx</package>
    <service servicelist="myrevprox">nginx</service>
    <file filelist='myrevprox' name='/etc/nginx/sites-enabled/default' source='nginx.default'/>
    <file filelist='myrevprox' name='/var/www/nginx-default/nginx.html' rm='True'/>
  </container>
</containers>
<files>
<!-- sur le maître-->
  <service>ntp</service>
  <file name='/etc/ntp.conf/>
  <file name='/etc/default/ntpdate' owner='ntp' group='ntp' mode='600'/>
  <file name='/etc/strange/host' source='strangehost.conf' mkdir='True'/>
</files>
```

Voir aussi...

Choisir le mode du module [p.58]

2.3.3. Utiliser des familles, variables et des séparateurs

Variables : <variables>

L'ensemble des familles et, ainsi, des variables sont définies dans un nœud **<variables></variables>**.

Familles : <family>

Un conteneur famille permet d'avoir des catégories de variables. Celle-ci correspond à un onglet dans l'interface. Les familles sont incluses obligatoirement dans une balise *<variables>*.

Une famille `Squid` pour gérer toutes les variables relatives a *Squid*.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les attributs de la balise *family* sont les suivants :

- l'attribut **name** (obligatoire) est à la fois le nom et l'identifiant de la famille ;
- l'attribut **mode** permet de définir le mode d'affichage de la famille :
  - mode basique par défaut ;
  - mode normal ;
  - mode expert.
- l'attribut **icon** définit une image associée à l'onglet ;
- l'attribut **hidden** indique si la famille doit être affichée ou non, sa valeur pouvant être modifiée via une condition (voir plus bas).



Une famille dont toutes les variables sont cachées (hidden) ou désactivées (disabled) ne sera pas affichée sauf en mode debug.



Les icônes utilisés proviennent des bibliothèques de polices et d'icônes libres :

- Font Awesome : http://fortawesome.github.io/Font-Awesome/icons ;
- Font Mfizz : http://fizzed.com/oss/font-mfizz.

Pour choisir une icône, il faut se rendre sur les pages ci-dessus et recopier le nom de l'icône. Pour la font Mfizz il faut enlever le préfixe `icon-`.



```
<family name='messagerie' mode='basic' icon='envelope'>
<variable name='system_mail_from' type='mail' description="Adresse électronique d'envoi pour le compte root"/>
</family>
```

Variable : <variable>

Une variable contient une description et, optionnellement, une valeur EOLE par défaut.

Les variables peuvent être à valeur unique ou multi-valuées.

Les balises **<variable>** sont incluses obligatoirement dans une balise **<family>**.

Les attributs de la balise *variable* sont les suivants :

- l'attribut **name** (obligatoire) est le nom de la variable ;
- l'attribut **type** (obligatoire) permet d'utiliser un type EOLE avec des vérifications automatiques (fonctions de vérifications associées a chaque type de variable) ;
- l'attribut **description** permet de définir le libellé à afficher dans l'interface de configuration du module ;
- l'attribut **multi** permet de spécifier qu'une variable pourra avoir plusieurs valeurs (par exemple pour un DNS, on aura plusieurs adresses IP de serveurs DNS) ;
- l'attribut **mode** permet de définir le mode d'affichage de la variable (*basic, normal* ou *expert*) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- si l'attribut **hidden** vaut *True*, la variable ne sera pas affichée dans l'interface de configuration (on peut par exemple souhaiter masquer des variables dont la valeur est calculée automatiquement) ;
- si l'attribut **disabled** vaut *True*, la variable sera déclarée comme désactivée.
- si l'attribut **mandatory** vaut *True*, la variable sera considérée comme obligatoire, cet attribut remplace l'ajout d'un *check obligatoire* au niveau des conditions :
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir une variable déjà définie dans un autre dictionnaire ;
- si l'attribut **exists** vaut *False*, cela permet de définir une variable si et seulement si elle n'a pas déjà été définie dans un autre dictionnaire.
- si l'attribut **remove_check** vaut *True* pour une variable redéfinie, alors toutes les validations (*check*) associées à cette variable sont réinitialisées ;
- si l'attribut **remove_condition** vaut *True* pour une variable redéfinie, alors toutes les conditions associées à cette variable sont réinitialisées (attention, **remove_condition** n'est disponible qu'à partir de la version **EOLE 2.5.2**) ;
- si l'attribut **auto_freeze** vaut *True*, la variable devient à verrouillage automatique. Sa valeur est verrouillée dès le premier enregistrement de la configuration. Dans l'interface de configuration du module, ces variables sont identifiées par la présence d'un cadenas. Ce dernier apparaît verrouillé une fois le serveur instancié ;
- si l'attribut **auto_save** vaut *True*, la variable devient à enregistrement obligatoire. Sa valeur est obligatoirement enregistrée dans le fichier de configuration et elle n'est donc pas automatiquement modifiée si sa valeur par défaut change au niveau des dictionnaires. On retrouve ainsi un fonctionnement équivalent à celui disponible sur EOLE 2.3.

Les principaux types de variables Creole sont les suivants :

- *number* : la valeur de la variable doit être du type "int". La fonction python `int(value)` ne doit pas retourner d'erreur ;
- *string* : la valeur de la variable doit être du type "unicode" ;
- *ip* : valeur de type IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *local_ip* : la même chose que IP, sauf que les adresses réservées et privées soulèvent un warning (voir *IPy* pour des informations sur les adresses réservées et privées) ;
- *netmask* : adresse de masque réseau. La valeur doit passer ce test : `IPy.IP('0.0.0.0/{0}'.format(value))` ;
- *network* : adresse réseau. La valeur doit passer ce test : `IPy.IP(value)` ;
- *broadcast* : adresse de broadcast. : La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *netbios* : alphanumérique autorisé sauf pour le 1er caractère qui doit forcement être du type alpha, minimum 2 et maximum 15 caractères ;
- *domain* :
  - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`

  ou

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

  - alphanumérique et '.' autorisé sauf pour le 1er caractère qui doit forcement être du type alpha. Le '.' est obligatoire. Minimum 2 et maximum 255 caractères ;
- *domain_strict* : nom DNS uniquement (adresse IP interdite) ;
- *unix_user* : nom d'utilisateur ou de groupe Unix ;
- *web_address* : adresse Internet. Doit débuter par `http://` ou `https://` ;
- *hostname* :
  - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`

  ou
  - alphanumérique autorisé sauf pour le 1er caractère qui doit forcement être du type alpha.Minimum 2 et maximum 63 caractères ;
- *hostname_strict* : nom d'hôte uniquement (adresse IP interdite) ;
- *mail* : adresse e-mail ;
- *port* : entier compris entre 1 et 65535 ;
- *filename* : tout chemin Unix (fichier ou répertoire) ;
- *oui/non* : seules valeurs possibles : "oui" et "non" ;
- *yes/no* : seules valeurs possibles : "yes" et "no" ;
- *on/off* : seules valeurs possibles : "on" et "off" ;
- *password* : la valeur de la variable est masquée dans l'interface une fois le champ validé. Elle est affichée en clair lorsque le champ est édité. Aucune contrainte n'est associée à ce type de variable.

Comportement avec redefine='True' et remove_check='False'

- si la nouvelle variable fournit une valeur par défaut, elle remplace l'ancienne ;
- si la nouvelle variable fournit un ou plusieurs des attributs suivants : *description*, *hidden*, *mandatory*, *auto_freeze*, *mode*, les valeurs des nouveaux attributs remplacent les anciennes ;
- les attributs *type* et *multi* ne sont pas modifiables ;
- si un nouveau *valid_enum* est défini dans les fonctions *checks*, il remplace l'ancien ;
- si de nouveaux *disabled_if(_not)_in* sont définis, ils remplacent les anciens ;
- les autres conditions et contraintes sont ajoutées à celles qui étaient déjà définies.

Valeur : <value>

A l'intérieur d'une balise **<variable>**, il est possible de définir une balise **<value>** permettant de spécifier la valeur par défaut de la variable.

Séparateurs : <separators> et <separator>

Les séparateurs permettent de définir des barres de séparation au sein d'une famille de variable dans l'interface de configuration.

Les séparateurs définis dans un dictionnaire sont placés dans la balise **<separators></separators>** dans la balise **<variables>**.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

A l'intérieur de la balise **<separators>** il faut spécifier autant de balises **<separator>** que de séparateurs souhaités.

Les attributs de la balise *separator* sont les suivants :

- l'attribut **name** (obligatoire) correspond au nom de la variable suivant le séparateur ;
- si l'attribut **never_hidden** vaut *True*, le séparateur sera affiché même si la variable associée est masquée.

Dans le cas où il n'y a aucune variable à afficher dans le bloc défini par le séparateur, celui-ci est forcément masqué.

Exemple

Variables, familles et séparateurs

```
<variables>
  <family name='services'>
    <variable name='activer_esu' type='oui/non' description="Utiliser le logiciel ESU" hidden='True'>
      <value>oui</value>
    </variable>
  </family>
  <family name='esu'>
    <variable name='esu_proxy' type='oui/non' description="Activer le proxy ESU">
      <value>non</value>
    </variable>
    <variable name='esu_proxy_server' type='domain' description='Adresse du proxy ESU' mandatory='True'/>
    <variable name='esu_proxy_port' type='port' description='Port du proxy ESU' mandatory='True'>
      <value>3128</value>
    </variable>
    <variable name='esu_proxy_bypass' type='string' description='Ne pas utiliser le proxy ESU pour' multi='True'>
      <value>127.0.0.1</value>
    </variable>
  </family>
  <separators>
    <separator name='esu_proxy'>Proxy ESU</separator>
  </separators>
</variables>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3.4. Comportement des variables

En plus des propriétés décrites explicitement dans les dictionnaires Creole, certaines variables se voient ajouter des contraintes ou des modifications de propriétés en fonction de certains paramètres.

Les variables possédant la propriété `auto freeze='True'` sont obligatoirement affichées en mode basique lors de la saisie initiale, ceci afin d'attirer l'attention de l'utilisateur sur le fait qu'elles ne seront plus modifiables ultérieurement.
Une exception a été ajoutée à cette règle, si la propriété `expert='True'` est explicitement ajoutée sur la variable, celle-ci apparaîtra uniquement dans le mode expert.

Les variables obligatoires (`mandatory='True'`) ne possédant pas de valeur par défaut (calculée ou non) sont obligatoirement affichées en mode basique, puisque l'utilisateur devra forcément les renseigner.

Les variables non obligatoires (`mandatory='False'`) possédant une valeur par défaut (balise `<value>`) deviennent obligatoires.

2.3.5. Mettre en place des contraintes

Des fonctions (contraintes) peuvent être utilisées pour grouper / tester / remplir / conditionner des variables.
L'ensemble des contraintes d'un dictionnaire se place à l'intérieur d'un nœud XML **<constraints></constraints>**.

Lien entre variables : <group>

Il est possible de lier des variables sous la forme d'une relation maître-esclave(s).
La variable maître doit obligatoirement être multi-valuée (`multi='True'`).
Elle se définit dans l'attribut **master**.
Les variables esclaves sont définies entre les balises **<slave>**.
Les variables esclaves deviennent automatiquement multi-valuées.

```
<group master='adresse_ip_eth0'>
    <slave>adresse_netmask_eth0</slave>
    <slave>adresse_network_eth0</slave>
</group>
```

Calcul automatique modifiable <fill> ou non <auto>

Le calcul automatique permet d'associer automatiquement (par le calcul) une valeur par défaut à une variable.
Cette valeur peut être :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- éditable par l'utilisateur : balise *<fill>* ;
- non éditable par l'utilisateur (exemple : l'IP d'un serveur en DHCP) : balise *<auto>*.



Contrairement aux versions précédentes si l'utilisateur a choisi de conserver la valeur par défaut d'une variable affectée par un *fill*, le calcul de la valeur sera réalisé à chaque fois, comme pour les variables *auto* sauf si la variable possède l'attribut `auto_save='True'`.



Les calculs *auto* ne sont pas compatibles avec les variables à verrouillage automatique (`auto_freeze`) ou à enregistrement obligatoire (`auto_save`).

L'attribut *name* correspond au nom de la fonction qui sera utilisée pour le calcul.

Les fonctions utilisées peuvent être :

- des fonctions natives de Tiramisu[p.475] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

L'attribut de la balise *param* : *optional='True'* : indique que le paramètre sera ignoré si la variable associée n'existe pas. Cela permet de contourner les erreurs du type : `Utilisation de la variable <param var_name> non présente dans un calcul`

L'attribut de la balise *param* : *hidden='False'* : indique que le paramètre sera ignoré si la variable possède des propriétés incompatibles avec le calcul (variable désactivée, variable obligatoire sans valeur, ...). Cela permet de contourner les erreurs du type : `impossible d'effectuer le calcul, l'option <target var_name> a les propriétés : ['disabled'] pour : <param var_name>`

Les principales fonctions de calcul utilisables avec les balises fill et auto sont les suivantes :

- *calc_network* : calcule l'adresse réseau par défaut à partir d'une IP et d'un masque de sous-réseau

```
<fill name='calc_network' target='my_network'>
    <param type='eole' name='ip'>my_ip</param>
    <param type='eole' name='netmask'>my_netmask</param>
</fill>
```

- *calc_broadcast* : calcule l'adresse de broadcast à partir d'une adresse IP et d'un masque de sous-réseau

```
<fillname='calc_broadcast' target='my_broadcast'>
    <param type='eole' name='ip'>my_ip</param>
    <param type='eole' name='netmask'>my_netmask</param>
</fill>
```

- *calc_val* : renvoie la valeur passée en paramètre (généralement la valeur d'une autre variable)

```
<fill name='calc_val' target='nom_machine'>
    <param type='eole' name='valeur'>eole_module</param>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
</fill>
```

- *calc_val_first_value* : renvoie la valeur de la première variable définie

```
<fill name='calc_val_first_value' target='eolesso_adresse'>
    <param type='eole' optional='True' hidden='False'>web_url</param>
    <param type='eole'>adresse_ip_eth0</param>
</fill>
```

- *calc_multi_val* : renvoie les valeurs passées en paramètre en supprimant les doublons

```
<fill name='calc_multi_val' target='ssl_organization_unit_name'>
    <param>110_043_015</param>
    <param type='eole'>nom_academie</param>
    <param type='eole'>numero_etab</param>
</fill>
```

  Si l'une des valeurs passées à la fonction est vide, elle renverra une liste vide.

  À partir d'EOLE 2.6.2, il est possible de modifier ce comportement en ajoutant la balise suivante : `<param name='allow_none'>True</param>`.

- *concat* : concaténation de plusieurs valeurs

```
<fill name="concat" target='bacula_dir_name'>
    <param type='eole' name='valeur1'>nom_machine</param>
    <param name='valeur2'>-dir</param>
</fill>
```

- *calc_multi_condition* : la valeur est déterminée en fonction d'une ou de plusieurs autres variables. Le résultat peut être une chaîne de caractères ou la valeur d'une autre variable multi ou non (si type='eole')

```
<auto name='calc_multi_condition' target='variable_calculee'>
    <param>oui</param>
    <param type='eole' name='condition_1'>activer_logiciel1</param>
    <param type='eole' name='condition_2' hidden='False'>activer_logiciel2</param>
    <param name='match'>oui</param>
    <param name='mismatch' type='eole'>variablemiss</param>
    <param name='default_mismatch'>valeur_si_variablemiss_disabled</param>
</auto>
```

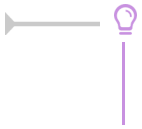
  Il est possible d'utiliser des *calc_multi_condition* avec des variables non déclarées ou désactivées mais uniquement si toutes les variables testent la même condition.

  A contrario, il est possible de spécifier une condition différente pour chacune des variables en en fournissant la liste dans la première balise param : `<param>['non', 'oui']</param>`. Dans ce cas, il faut exactement le bon nombre de variables et que celles-ci soient accessibles.

Validation et/ou liste de choix : <check>

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La valeur renseignée pour une variable est validée par une fonction.



La déclaration de nombreuses validations peut être évitée en affectant un type adapté à chacune des variables.

L'attribut *name* correspond au nom de la fonction qui sera utilisée pour le calcul.

Les fonctions utilisées peuvent être :

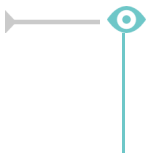
- des fonctions natives de Tiramisu[p.475] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

L'attribut de la balise *param* : *optional='True'* : indique que le paramètre sera ignoré si la variable associée n'existe pas. Cela permet de contourner les erreurs du type : `Utilisation de la variable <param var name> non présente dans un calcul`

L'attribut de la balise *param* : *hidden='False'* : indique que le paramètre sera ignoré si la variable possède des propriétés incompatibles avec le calcul (variable désactivée, variable obligatoire sans valeur, ...). Cela permet de contourner les erreurs du type : `impossible d'effectuer le calcul, l'option <target var name> a les propriétés : ['disabled'] pour : <param var name>`

La présence de l'attribut **level="warning"** indique que le test de validation n'est pas bloquant.

En cas d'échec de la validation un message d'alerte apparaîtra mais la valeur sera tout de même acceptée.



```
1 <check name="valid_ipnetmask" target="adresse_netmask_eth0" level=
  "warning">
2     <param type='eole'>adresse_ip_eth0</param>
3 </check>
```

Les principales fonctions de validation disponibles sont les suivantes :

- *valid_enum* : la valeur doit être choisie parmi celles de la liste, si *checkval* est à False, l'utilisateur est autorisé à entrer la valeur de son choix (liste ouverte)

  ```
  <check name="valid_enum" target="lettre">
      <param>['a','b','c']</param>
      <param name="checkval">False</param>
  </check>
  ```

- *valid_regexp* : la valeur doit être conforme à une expression rationnelle

  ```
  <check name='valid_regexp' target='code_ent'>
      <param>^[A-Z][0-9]$</param>
      <param name='err_msg'>L'identifiant doit etre compose d'une lettre et d'un chiffre</param>
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
</check>
```

- *valid_differ* : la valeur doit être différente de celle passée en paramètre

```
<check name='valid_differ' target='smb_workgroup'>
    <param type='eole' hidden='False'>smb_netbios_name</param>
</check>
```

- *valid_entier* : la valeur doit être un entier sur lequel on peut définir un minimum et/ou un maximum

```
<check name='valid_entier' target='nombre'>
    <param name='mini'>0</param>
    <param name='maxi'>50</param>
</check>
```

- *valid_networknetmask* : vérifie la cohérence entre une variable de type *network* et la variable de type *netmask* associée

```
<check name="valid_networknetmask" target="netmask_ssh_eth0">
    <param type='eole'>ip_ssh_eth0</param>
</check>
```

- *valid_ipnetmask* : vérifie la cohérence entre une variable de type *ip* et la variable de type *netmask* associée

```
<check name="valid_ipnetmask" target="adresse_netmask_eth0" level="warning">
    <param type='eole'>adresse_ip_eth0</param>
</check>
```

- *valid_in_network* : vérifie la cohérence entre une variable de type *ip* et les variables de type *network* et *netmask* associées

```
<check name="valid_in_network" target="adresse_ip_gw">
    <param type='eole'>adresse_network_eth0</param>
    <param type='eole'>adresse_netmask_eth0</param>
</check>
```

Autre fonction de validation disponible mais non utilisée dans les dictionnaires livrés :

- *valid_broadcast*

Contrainte entre variables : <condition> disabled_if_in et disabled_if_not_in

Les conditions *disabled_if_in* et *disabled_if_not_in* permettent :

- d'activer/désactiver une variable (*type='variable'*)
- d'activer/désactiver une famille (*type='family'*)
- d'activer/désactiver des services (*type='servicelist'*)
- d'activer/désactiver des règles de pare-feu (type='*service_accesslist*')
- d'activer/désactiver la templatisation de fichiers (*type='filelist'*)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

en fonction d'un ensemble de conditions.

```
<condition name='disabled_if_not_in' source='port_rpc'>
    <param>0</param>
    <param>7080</param>
    <target>ip_eth0</target>
    <target type='family' optional='True'>net</target>
    <target type='filelist'>ldap</target>
    <target type='servicelist'>ldap</target>
</condition>
```

La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la variable source est renseignée ou non.

hidden_if_in et hidden_if_not_in

Les anciennes conditions *hidden_if_in* et *hidden_if_not_in* sont toujours supportées mais leur comportement est désormais calqué sur celui des *disabled_if_in* et *disabled_if_not_in* par lesquelles elles doivent être remplacées.

Gestion des variables inexistantes ou désactivées

Si l'attribut **optional** de la balise target vaut **'True'**, la cible sera ignorée si elle n'existe pas.

Cela permet de contourner les erreurs du type : `Variable <target_var_name> inexistante mais avec condition`

Si l'attribut **fallback** de la balise condition vaut **'True'**, les cibles seront automatiquement désactivées si le calcul de la condition est impossible (variable source inconnue ou désactivée).

Cela permet de contourner les erreurs du type : `Variable <src_var_name> inexistante mais utilisée dans une condition`

Son utilisation évite d'avoir à déclarer explicitement la variable source avec l'attribut *exists='False'* dans le dictionnaire courant.

```
<condition name='disabled_if_in' source='activer_spamassassin' fallback=
'True'>
    <param>non</param>
    <target type='variable'>exim_spam_score</target>
</condition>
```

Désactivation de variables entre esclaves du même groupe

À partir de la version 2.6.1 d'EOLE, il est possible de gérer la désactivation d'une variable esclave en fonction de la valeur d'une autre variable esclave du même groupe.

Dans les versions précédentes, il était possible de désactiver totalement une variable esclave mais pas de le faire pour une seule de ses valeurs.

Dictionnaire avec conditions de désactivation entre variables esclaves

```
<?xml version="1.0" encoding="utf-8"?>
<creole>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
    <files/>
    <variables>
        <family name='famille_demo'>
            <variable name='ma_master' type='string' description='Je suis une variable maitre' multi="True"/>
            <variable name='ma_slave1' type='oui/non' description='Je suis une variable esclave qui cache'>
                <value>oui</value>
            </variable>
            <variable name='ma_slave2' type='string' description='Je suis une variable esclave qui peut être caché'/>
            <variable name='ma_slave3' type='string' description='Je suis une variable esclave qui peut être caché aussi'/>
        </family>
    </variables>
    <constraints>
        <group master='ma_master'>
            <slave>ma_slave1</slave>
            <slave>ma_slave2</slave>
            <slave>ma_slave3</slave>
        </group>
        <condition name='disabled_if_in' source='ma_slave1'>
            <param>non</param>
            <target type='variable'>ma_slave2</target>
        </condition>
        <condition name='disabled_if_in' source='ma_slave1'>
            <param>oui</param>
            <target type='variable'>ma_slave3</target>
        </condition>
    </constraints>
    <help/>
</creole>
```

Template associé au dictionnaire

```
%for %%master in %%ma_master
pour %%master :
%if %%master.ma_slave1 == 'oui'
* ma_slave2 : %%master.ma_slave2
%else
* ma_slave3 : %%master.ma_slave3
%end if
%end for
```

frozen_if_in et frozen_if_not_in

Les conditions *frozen_if_in* et *frozen_if_not_in* permettent de passer une variable en mode automatique (valeur non modifiable par l'utilisateur) en fonction d'un ensemble de conditions.

```
<condition name='frozen_if_not_in' source='eth0_method'>
    <param>statique</param>
    <target type='variable'>adresse_ip_eth0</target>
    <target type='variable'>adresse_netmask_eth0</target>
    <target type='variable'>adresse_ip_gw</target>
</condition>
```

La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> variable source est renseignée ou non.

Gestion des variables inexistantes ou désactivées

Si l'attribut **optional** de la balise target vaut **'True'**, la cible sera ignorée si elle n'existe pas.

Cela permet de contourner les erreurs du type : `Variable <target var name> inexistante mais avec condition`

Si l'attribut **fallback** de la balise condition vaut **'True'**, les cibles seront automatiquement désactivées si le calcul de la condition est impossible (variable source inconnue ou désactivée).

Cela permet de contourner les erreurs du type : `Variable <src var name> inexistante mais utilisée dans une condition`

Son utilisation évite d'avoir à déclarer explicitement la variable source avec l'attribut *exists='False'* dans le dictionnaire courant.

mandatory_if_in et mandatory_if_not_in

Les conditions *mandatory_if_in* et *mandatory_if_not_in* permettent passer une variable en mode obligatoire (une valeur doit être renseignée par l'utilisateur) en fonction d'un ensemble de conditions.

```
1 <condition name='mandatory_if_not_in' source='mode_zephir'>
2     <param>non</param>
3     <target type='variable'>nom_carte_eth0</target>
4     <target type='variable'>nom_zone_eth0</target>
5 </condition>
```

> La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la variable source est renseignée ou non.

Gestion des variables inexistantes ou désactivées

Si l'attribut **optional** de la balise target vaut **'True'**, la cible sera ignorée si elle n'existe pas.

Cela permet de contourner les erreurs du type : `Variable <target var name> inexistante mais avec condition`

Si l'attribut **fallback** de la balise condition vaut **'True'**, les cibles seront automatiquement désactivées si le calcul de la condition est impossible (variable source inconnue ou désactivée).

Cela permet de contourner les erreurs du type : `Variable <src var name> inexistante mais utilisée dans une condition`

Son utilisation évite d'avoir à déclarer explicitement la variable source avec l'attribut *exists='False'* dans le dictionnaire courant.

Ajout de fonctions personnalisées

Il est possible d'ajouter des librairies de fonctions personnalisées dans le répertoire `/usr/share/creole/funcs`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les librairies doivent posséder l'extension `.py` et contenir des fonctions python.

```
# -*- coding: utf-8 -*-
def to_iso(data):
""" encode une chaine en ISO"""
try:
    return unicode(data, "UTF-8").encode("ISO-8859-1")
except:
    return data
```

Si vous devez importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptible d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3.6. Afficher de l'aide

Il est possible d'afficher de l'aide dans l'interface :

- affichée au survol de l'onglet : **<family>** ;
- affichée au survol du libellé de la variable : **<variable>**.

L'ensemble des aides d'un dictionnaire est dans la balise **<help>**.



```
<help>
  <variable name='adresse_ip_eth0'>
    Adresse IP de la premiere carte réseau (ex: 10.21.5.1)
  </variable>
</help>
<help>
  <family name='messagerie'> Paramétrage du serveur de messagerie (MTA) Exim :
    - Paramétrage d'Exim selon 5 modèles ;
    - Paramétrage du domaine de messagerie suivant le modèle Exim ;
    - Paramétrage des réécritures d'adresses ;
    - Paramétrage des logs Exim ;
    - Paramétrage du relais des mails ;
    - Paramétrage d'activation de spamassassin ;
    - Paramétrage d'activation de Sympa.
  </family>
</help>
```

2.4. Le langage de template Creole

Les variables du dictionnaire Creole sont accessibles en les préfixant par la chaîne de caractères : `%%`.

Si dans le dictionnaire Creole :

`adresse_ip_eth0` vaut `192.168.170.1`

Et qu'on a dans un template source le contenu suivant :

```
bla bla bla %%adresse_ip_eth0 bla bla bla
```

Après instanciation, le fichier cible contiendra :

```
bla bla bla 192.168.170.1 bla bla bla
```



Dans les cas où une variable est susceptible d'être confondue avec le texte qui l'entoure, il est possible d'encadrer son nom par des accolades :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `%%{adresse ip eth0}` est identique à `%%adresse ip eth0`.

2.4.1. Déclarations du langage Creole

Creole fournit un langage de template complet.

Il est possible de créer des boucles, des tests, de gérer les lignes optionnelles, de réaliser des inclusions répétées, ...

La déclaration de test : if

Syntaxe :

`%if EXPRESSION |code if %else |code else %end if`

Dans les tests il est possible d'utiliser les opérateurs du langage python : `==`, `!=`, `>`, `<`, `>=`, `<=`, `not`, `and`, `or`, ...



```
%if %%size > 500
c'est grand
%elif %%size >= 250
c'est moyen
%else
c'est petit
%end if
```



```
%if %%toto == 'yes' and ( %%titi != "" or %%tata not in ['a','b','c'] ) :
la condition a été validée
%end if
```

La déclaration d'itération : for

Syntaxe :

```
%for %%iterateur in EXPRESSION
CODE avec %%iterateur
%end for
```

La boucle `%%for` est particulièrement intéressante lorsque l'on souhaite effectuer des traitements sur une **variable multi-valuée**.



```
%for %%i in range(4)
itération %%i
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
%end for
%for %%valeur in %%variable_multivaluee
%%valeur
%end for
```



Pour des traitements simples, la fonction prédéfinie `%%custom_join` (voir section suivante) peut avantageusement éviter la mise en place d'une boucle `%for`.

La notation pointée

Si une variable Creole est **multivaluée** et **maître** *(master d'un groupe de variable)* alors, il est possible de faire appel à ses variables **esclaves** à l'intérieur de la boucle `%for`.

Si `netmask_admin_eth0` est esclave de `ip_admin_eth0` alors, il est possible d'appeler cette variable en notation pointée.

Par exemple : dans le dictionnaire Creole figurent les variables suivantes.

`ip_admin_eth0` est la variable maître et :

- `ip_admin_eth0 = ['1.1.1.1', '2.2.2.2']`
- `netmask_admin_eth0 = ['255.255.255.255', '255.255.255.255']`

Le template suivant :

```
%for %%ip_admin in %%ip_admin_eth0
%%ip_admin/%%ip_admin.netmask_admin_eth0
%end for
```

donnera comme résultat :

```
1.1.1.1/255.255.255.255
2.2.2.2/255.255.255.255
```

Il est également possible aussi d'accéder à l'index (la position dans la liste) de la variable en cours de boucle :

```
%for %%idx, %%val in %%enumerate(%%ip_admin_eth0)
L'index de %%val est : %%idx
%end for
```

Le template généré sera le suivant :

```
l'index de : 1.1.1.1 est : 0
l'index de : 2.2.2.2 est : 1
```

Il est également possible (mais déconseillé) d'utiliser une "notation par item" (notation entre crochets).

Par exemple pour accéder à l'item numéro 5 d'une variable, il faut écrire :

```
variable[5]
```

La variable doit être évidemment être **multivaluée** et comporter au minimum *(item+1)* valeurs.

```
ip_admin_eth0 = ['1.1.1.1', '2.2.2.2', '3.3.3.3']
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

et si un template a la forme suivante :

```
bla bla
%%ip admin eth0[2]
bla bla
```

alors l'instanciation du template donnera comme résultat :

```
bla bla
3.3.3.3
bla bla
```

.value et .index

Les attributs *.value* et *.index* ne sont plus supportés et ne doivent plus être utilisés dans les templates.

Les déclarations spéciales echo et set

L'instruction `%echo` permet de déclarer une chaîne de caractères afin que celle-ci apparaisse telle quelle dans le fichier cible.

Cela est utile lorsqu'il y a des caractères spéciaux dans le template source et, en particulier, les caractères `%` et `\` qui sont susceptibles d'être interprétés par le système de template.

```
%echo "- deux barres obliques : \\\\\n- un pourcentage : %"
```

L'utilisation de l'instruction `%echo` ne rend pas les templates très lisibles d'autant plus que, généralement, on souhaite intercaler des variables au milieu des caractères spéciaux.

En pratique, il est donc préférable de passer par des variables locales que l'on peut déclarer avec `%set`.

```
%set %%slash='\\'
%set %%double_slash='\\\\'
%%double_slash%%machine%%{slash}partage
```

Autres déclarations

La déclaration while

Syntaxe : `%while EXPR contenu`

`%end while`

Exemple :

```
%while %someCondition('arg1', %%arg2)
The condition is true.
%end while
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La déclaration repeat

Syntaxe : `%repeat EXPR`

```
%end repeat
```

La déclaration unless

```
%unless EXPR
%end unless
```

peut être utile si une variable est dans le dictionnaire Creole pour "'ne pas"' executer une action :

```
%unless %%alive
do this
%end unless
```

La syntaxe d'inclusion

il est possible d'inclure des fichiers à l'aide de la déclaration suivante :

```
%include "includeFileName.txt"
```

ou bien à partir du nom long du fichier à inclure (le nom de fichier étant ici renseigné dans une variable Creole :

```
%include source=%%myParseText
```

Effacement des retours chariots : slurp

Exemple d'utilisation :

```
%for %%i in range(15)
%%i-%slurp
%end for
```

donnera :

```
1-2-3-4-5-6...
```

sur une seule ligne (gobe les retours chariots)

remarquons que dans ce cas là, `slurp` n'est pas nécessaire et il est possible d'écrire le end sans sauter de ligne :

```
%for %%i in range(15)
%%i-%end for
```

exemple 2 :

```
%if %%dns_nameservers != ['']
dns_nameservers %slurp
%for %%name_server in %%dns_nameservers %%name_server %slurp
%end for
%end if
#
```

générera :

```
dns_nameserver toto titi #
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.4.2. Fonctions prédéfinies

Il est possible d'accéder à des fonctions prédéfinies, provenant du module : `eosfunc.py`.

Ces fonctions peuvent être utilisées dans un template de la manière suivante (exemple) :

[...] `%%fonction_predefinie(%%variable)` [...]

Variable "optionnelle" : is_defined

Il peut arriver qu'on ne soit pas sûr que la variable que l'on souhaite tester soit définie dans les dictionnaires présents sur le module ou que la variable soit désactivée.

C'est le cas lorsque l'on veut traiter un cas particulier dans un template qui est commun à plusieurs modules.

Hors, si une variable est utilisée dans le template cible sans avoir été définie, le processus d'instanciation sera stoppé.

Pour tester si une variable est définie, il faut utiliser la fonction `%%is_defined`.



```
%if %%is_defined('ma_variable')
%%ma_variable
%else
la variable n'est pas définie
%end if
```

Contrairement à toutes les autres fonctions, *is_defined* nécessite comme argument le nom de la variable fourni sous forme d'une **chaîne de caractères**.

Si une variable non définie est placée dans un bloc qui n'est pas traité (conditionné par une fonction ou d'autres variables), ça n'est pas bloquant.



Dans de nombreux cas, la fonction *is_defined* peut avantageusement être remplacée par la fonction *getVar* à laquelle on aura pris soin d'indiquer une valeur par défaut à renvoyer en cas d'indisponibilité de la variable (voir ci-dessous).

Variable "vide" : is_empty

Il n'est pas toujours évident, en particulier lorsque l'on manipule des variables multi-valuées, de trouver le test adéquat afin de déterminer si une variable est vide.

Pour tester si une variable est vide, il est désormais recommandé d'utiliser la fonction `%%is_empty`.



```
%if not %%is_empty(%%ma_variable)
%%ma_variable[0]
%else
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
la variable est vide
%end if
```

Concaténation des éléments d'une liste : custom_join

La fonction `%%custom join` permet de concaténer facilement les éléments d'une variable multi-valuée.
Cela permet d'éviter le recours à une boucle `%for` et l'utilisation du l'instruction `%slurp` qui est souvent source d'erreurs.
Il est possible de spécifier le séparateur à utiliser en le passant comme paramètre à la fonction.
En l'absence de ce paramètre, le séparateur utilisé est l'espace.



```
%%custom join(%%ma variable, ':')
```

Si ma_variable vaut ['a', 'b', 'c'], cela donnera :

```
a:b:c
```

Variable "dynamique" : getVar

Une variable dynamique prend comme nom (ou partie du nom) la valeur d'une autre variable.



```
%for %%interface in range(0, %%int(%%nombre interfaces))
L'interface eth%%interface a pour adresse %%getVar('adresse ip eth'+str(%%interface))
%end for
```

La fonction *getVar* peut également être utilisée lorsque l'on n'est pas certain qu'une variable est disponible car il est possible de lui spécifier une valeur par défaut à renvoyer en cas d'indisponibilité.



```
%if %%getVar("activer_mon_logiciel", "non") == 'oui'
Activation du logiciel
%end if
```

Variable esclave "dynamique" : getattr

Lorsque le nom de la variable esclave doit être calculé, on peut utiliser `%%getattr` à la place de la notation pointée.



```
%set %%num='0'
%for %%ip_ssh in %%getVar('ip_ssh_eth'+%%num)
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
SSH est autorisé pour %%ip ssh/%%getattr(%%ip_ssh,
'netmask ssh eth'+%%num)
%end for
```

La fonction *getattr* peut également être utilisée lorsque l'on n'est pas certain qu'une variable esclave est disponible (inexistante ou désactivée) car il est possible de lui spécifier une valeur par défaut à renvoyer en cas d'indisponibilité.



```
%for %%iterator in %%var master
%%getattr(%%iterator, 'var slave', 'default')
%end for
```

Autres fonctions

Fonctions de traitement des chaînes de caractères

- transformation d'une chaîne en majuscules : `%%upper(%%ma_chaine)` ;
- transformation d'une chaîne en minuscules : `%%lower(%%ma_chaine)` ;
- encodage d'une chaîne en ISO-8859-1 (au lieu d'UTF-8) : `%%to_iso(%%ma_chaine)` ;
- transformation d'un masque réseau (ex : *255.255.255.0*) en classe d'adresse (ex : *24*) : `%%calc_classe(%%mask)` ;

Fonctions de tests

- vérification que la variable est une adresse IP (et pas un nom DNS) : `%%is_ip(%%variable)` ;
- vérification de l'existence d'un fichier : `%%is_file(%%fichier)`.

Déclaration de fonctions locales

Pour un traitement local et répétitif, il peut être pratique de déclarer une fonction directement dans un template avec `%def` et `%end def`.

Cependant, la syntaxe à utiliser dans ces fonctions est assez complexe (on ne sait jamais quand mettre le caractère `%` !) et ce genre de déclaration ne facilite pas la lisibilité du template.

Les fonctions déclarées localement s'utilisent de la même façon que les fonctions déjà prédéfinies.



```
%def nombre_points(chaine)
    %return chaine.count('.')
%end def
Il y a %%nombre_points(%%ma_variable) points dans ma variable.
```

Ajout de fonctions personnalisées

Il est possible d'ajouter des librairies de fonctions personnalisées dans le répertoire

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`/usr/share/creole/funcs`.

Les librairies doivent posséder l'extension `.py` et contenir des fonctions python.

```
# -*- coding: utf-8 -*-
def to_iso(data):
""" encode une chaine en ISO"""
try:
    return unicode(data, "UTF-8").encode("ISO-8859-1")
except:
    return data
```

Si vous devez importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptible d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.4.3. Utilisation avancée

Modification des méta-caractères utilisés

Dans le cas où il y a trop de % dans le template, il est possible de changer carrément de méta-caractères, en ajoutant une section `compiler-settings` en en-tête du template.

Cette méthode est, par exemple, utilisée pour la génération du fichier de configuration du logiciel `eJabberd` qui est en déclaré en Erlang[p.459].

Utilisation de @ et @@ à la place de % et %%

```
%compiler-settings
directiveStartToken = @
cheetahVarStartToken = @@
%end compiler-settings
```

Utilisation de creole_client

Les fonctionnalités de *creole_client* sont utilisables directement dans les templates.

Il est par exemple possible de lister toutes les variables et leurs valeurs :

```
%for %%var, %%value in %%creole_client.get_creole().items()
 %%var : %%value 
%end for
```

Donnera le résultat suivant (notez que le nom des variables esclaves est précédé de celui de la variable maître associée) :

```
ssl_organization_name : Ministere Education Nationale (MENESR) 
https_port : 
check_passwd_min_len_two_type : 9 
container_ip_proxy : 127.0.0.1 
nom_cache_pere_zone.options_cache_pere_zone : [] 
nom_cache_pere : [] 
ignore_expect_100 :
off eolesso_adresse : 192.168.230.205 
activer_dhcprelay : non
[ ... ]
```

Plus généralement, il est possible d'accéder à toutes les informations décrites dans les dictionnaires comme celles concernant les conteneurs, les services et les tâches programmées.

```
Liste des conteneurs :
%for %%container in %%creole_client.get_containers()
* %%container['name']
%end for
Liste des services actifs :
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
%for %%srv in %%creole_client.get_services()
%if %%srv.has_key('activate')
* %%srv['name']
 %end if
%end for
%set %%sched = %%creole_client.get('schedule.schedule')
Les tâches programmées sont exécutées à %%{sched['hour']}h%%{sched['minute']}
```

2.4.4. Exemple

Templatiser un nouveau fichier

Nous voulons templatiser le fichier `toto.conf` à l'aide des mécanismes Creole afin de rajouter l'`adresse ip eth0` (variable existante) ainsi que l'adresse de l'établissement (nouvelle variable).

- Ajouter un dictionnaire local

  Dans `/usr/share/eole/creole/dicos/local/`

  ajouter un fichier `.xml`

- Ajouter votre fichier template

  Notre fichier `toto.conf` sera placé dans `/usr/share/eole/creole/distrib/`

  Il faut ajouter les variables à l'aide de la syntaxe Creole.

  exemple : l'adresse est %%adresse_ip_eth0 et l'adresse est %%adresse_etablissement

- Entrer l'adresse de l'établissement

  - Aller dans l'interface de configuration du module
  - Dans l'onglet `Perso` renseigner l'adresse de l'établissement
  - Enregistrer

- Reconfigurer

  Le mécanisme de configuration a écrit votre fichier `/etc/toto.conf` avec les variables.

Commentaires généraux

Les variantes Zéphir

Cette procédure décrit comment ajouter des spécifications locales.

Dans le cadre d'un développement massif, le module Zéphir propose un mécanisme de variantes semblable.

Instancier un template avec CreoleCat

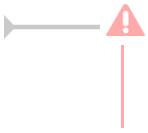
CreoleLint et CreoleCat [p.371]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.5. Le fichier de configuration Creole

Le fichier de configuration principal d'un module EOLE est enregistré dans `/etc/eole/config.eol`.

Ce fichier est au format JSON[p.463].



Bien que ce fichier semble simple et lisible, il est fortement déconseillé de l'éditer sans passer par l'interface de configuration du module.

Version du fichier

Depuis EOLE 2.4, le numéro de sous-version du module EOLE sur lequel a été enregistré le fichier de configuration est stocké dans celui-ci.

Il est associé au mot-clé réservé : **___version___**.

Exemple : `"___version___": "2.6.1"`.

Représentation des variables et des valeurs associées

Seules les variables modifiées par l'utilisateur et celles faisant l'objet d'un enregistrement obligatoire sont stockées dans le fichier sous forme d'un dictionnaire.

Les noms des différentes variables Creole sont les mot-clés du dictionnaire.

La valeur associée est elle-même un dictionnaire qui contient le propriétaire (stocké dans le mot-clé **owner**) et la valeur de la variable (stockée dans le mot-clé **val**).

En fonction du type Creole de la variable, la valeur représentée peut-être :

- une chaîne de caractère : `"numero_etab": {"owner": "gen_config", "val": "0000000A"}` ;
- un entier (si type='number') : `"vm_swappiness": {"owner": "creoleset", "val": 0}` ;
- aucune valeur (possible pour certaines variables à enregistrement obligatoire) : `"test_autosave": {"owner": "forced", "val": null}` ;
- une liste (si multi='True') : `"ip_admin_eth0": {"owner": "gen_config", "val": ["192.168.230.0", "194.18.20.0"]}`.

Depuis la version EOLE 2.6, les valeurs des variables esclaves sont indexées :

`"netmask_admin_eth0": {"owner": {"1": "gen_config", "0": "gen_config"}, "val": {"1": "255.255.255.0", "0": "255.255.255.0"}`

Origine des valeurs enregistrées

Le nom de l'application et/ou de l'action ayant modifié en dernier la valeur de l'une des variable est associé au mot-clé : **owner**.

Exemple : `"serveur_maj": {"owner": "gen_config", "val": ["test-eole.ac-dijon.fr"]}`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `default` : valeur par défaut et/ou calculée (n'est jamais enregistrée dans le fichier config.eol) ;
- `forced` : valeur par défaut enregistrée d'office pour les variables à verrouillage automatique (**auto_freeze**) ou à enregistrement obligatoire (**auto_save**) ;
- `gen_config` : valeur modifiée par l'interface de configuration du module ;
- `creoleset` : valeur modifiée avec la commande CreoleSet ;
- `zephir` : valeur modifiée pour un serveur donné dans l'interface web de Zéphir ;
- `variante` : valeur par défaut de la variante Zéphir ;
- `module` : valeur par défaut du module dans Zéphir ;
- `import` : valeur récupérée depuis un fichier de configuration importé dans l'interface de configuration du module ;
- `zephir_import` : valeur récupérée depuis un fichier de configuration importé dans l'interface web de Zéphir ;
- `upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE ;
- `zephir_upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE dans l'interface web de Zéphir.

2.6. Les scripts Creole

Creole fournit également un ensemble de scripts destinés à faciliter l'administration du serveur :

- CreoleLint permettant de faire des vérifications sur un dico ou sur un template ;
- CreoleCat permettant d'instancier un seul template indépendamment des commandes instance et reconfigure ;
- CreoleGet et CreoleSet permettant de lire et de modifier la valeur d'une variable Creole.
- CreoleRun et CreoleService permettant de lancer des commandes système et de gérer les services sur les modules EOLE, y compris à l'intérieur des conteneurs[p.456] ;
- CreoleLock permettant de placer, enlever ou vérifier les verrous Creole.

2.6.1. CreoleLint et CreoleCat

CreoleLint et CreoleCat sont des utilitaires permettant de faciliter les tests sur les dictionnaires et les templates :

- CreoleLint permet de valider la syntaxe des dictionnaires et des templates ;
- CreoleCat permet d'instancier un seul template indépendamment des commandes instance et reconfigure.

Vérifier les dictionnaires et templates avec CreoleLint

La commande CreoleLint permet de valider la syntaxe des dictionnaires et des templates.

L'outil effectue une série de tests dans le but de détecter des erreurs dans la déclaration et l'utilisation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

des variables.

Sur un module installé, il est possible de lancer l'application sans option particulière :

```
# CreoleLint
```

Cette commande permet également :

- de valider un seul template avec l'option `-t` : `CreoleLint -t hostname`
- de ne lancer qu'un seul des tests lint avec l'option `-n nomDuTest` : `CreoleLint -n valid_dtd`
- de ne lancer que la validation des dictionnaires avec l'option `-d` : `CreoleLint -d`

Les tests lint disponibles sont les suivants :

- `valid_dtd` : validation syntaxique des dictionnaires ;
- `tabs_in_dicos` : recherche de tabulation dans les dictionnaires ;
- `hidden_if_in_dicos` : recherche des conditions dépréciées `hidden_if_in` et `hidden_if_not_in` ;
- `condition_without_target` : recherche des conditions sans cible associée (EOLE >=2.6.2) ;
- `obligatoire_in_dicos` : recherche du validateur déprécié `obligatoire` ;
- `valid_slave_value` : recherche les variables esclaves avec une liste en valeur défaut (EOLE >= 2.5.2) ;
- `wrong_dicos_name` : validation du nom des dictionnaires ;
- `valid_var_label` : vérification des libellés des variables ;
- `valid_separator_label` : vérification des libellés des séparateurs ;
- `valid_help_label` : vérification des libellés de l'aide en ligne ;
- `activation_var_without_help` : vérification des variables d'activation sans balise d'aide (EOLE >= 2.5.2) ;
- `family_without_help` : vérification des familles sans balise d'aide ;
- `family_without_icon` : vérification des familles sans icône spécifique ;
- `old_fw_file` : recherche des anciens fichiers eole-firewall ;
- `valid_parse_tmpl` : validation de tous les templates.



L'option `-l` permet de choisir le niveau des messages (info, warning ou error).

La commande `CreoleLint` suivie du paramètre `-h` permet d'obtenir de l'aide. Un manuel est également disponible :

```
# man CreoleLint
```

Instancier un template avec CreoleCat

La commande `CreoleCat` permet d'instancier un seul template indépendamment des commandes `instance` et `reconfigure`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette commande permet :

- d'instancier un seule template existant sur le module en utilisant la ou les destinations déclarées dans le dictionnaire :
  `# CreoleCat -t hostname`
- d'instancier un template existant sur le module en redirigeant le résultat dans un fichier spécifique :
  `# CreoleCat -t hostname -o /tmp/hostname.txt`
- d'instancier un fichier template spécifique en redirigeant le résultat dans un fichier spécifique :
  `# CreoleCat -s /tmp/test.tmpl -o /tmp/test.txt`
- d'instancier un fichier template spécifique en affichant le résultat sur la console *(EOLE >= 2.5.2)* :
  `# CreoleCat -s /tmp/test.tmpl`



L'option `-l` permet de choisir le niveau des messages (info, warning ou error).

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande CreoleCat suivie du paramètre `-h` permet d'obtenir de l'aide.



```
root@scribe:~# CreoleCat -d -t sympa.auth.conf
Instanciation du fichier '/etc/sympa/auth.conf' depuis '/var/lib/creole/sympa.auth.conf'
Copy template: '/usr/share/eole/creole/distrib/sympa.auth.conf' -> '/var/lib/creole'
Cheetah processing: '/var/lib/creole/sympa.auth.conf' -> '/etc/sympa/auth.conf'
Changing properties: chown sympa:sympa /etc/sympa/auth.conf
Changing properties: chmod 0644 /etc/sympa/auth.conf
```


Dans le cas d'un template renommé, c'est le nom du template (défini dans l'attribut *source*) qu'il faut utiliser.

2.6.2. CreoleGet et CreoleSet

CreoleGet et **CreoleSet** sont des utilitaires permettant de lire et de modifier la valeur d'une variable Creole.

Récupérer la valeur d'une variable avec CreoleGet

CreoleGet est un utilitaire très pratique pour récupérer la valeur d'une variable Creole.

Il s'utilise tout simplement en lui donnant le nom de la variable souhaitée en argument :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`CreoleGet mavariable`

La commande `CreoleGet --list` permet d'obtenir la liste complète des variables.
La commande `CreoleGet` supporte l'autocomplétion à partir de la version 2.5.2 d'EOLE.

```
# CreoleGet --list | grep release
eole_release="2.6.1"
```

CreoleGet permet également de récupérer la liste des groupes de conteneurs :
`CreoleGet --groups`
Sur un serveur en mode non conteneur, cette commande renvoie uniquement `root`.

Dans le cas où l'on n'est pas certain que la variable soit disponible (variable inconnue ou désactivée), il est possible d'indiquer une valeur par défaut à renvoyer en cas d'erreur :
`CreoleGet activer_logiciel non`
Dans le cas contraire, une erreur pourra apparaître.

Pour accéder à une variable esclave, il faut connaître la variable maître :
`CreoleGet lamaster.lesclave`

Les valeurs multiples sont séparées par un saut de ligne (`\n`) :

```
root@eolebase:~# CreoleGet serveur_maj
eole.ac-dijon.fr
ftp.crihan.fr
```

L'option `-h` ou `--help` ou la commande `man CreoleGet` permettent d'obtenir de l'aide.

Lister les services gérés par Creole avec CreoleGet

La commande suivante permet d'obtenir la liste des services qui sont gérés par CreoleService sur le module :

```
CreoleGet .containers.services |grep \.name=
```

```
1 root@eolebase:~# CreoleGet .containers.services|grep \.name=
2 service0.name="networking"
3 service1.name="cron"
4 service10.name="exim4"
5 service11.name="eoleflask"
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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:~#
```

Recharger les variables et/ou la configuration creoled avec CreoleGet

À partir de la version EOLE 2.6.1, deux nouvelles options permettent de demander le rechargement du service creoled[p.457].

- `CreoleGet --reload` : recharge toute la configuration Creole (dictionnaires et valeurs) ;
- `CreoleGet --reload-eol` : recharge uniquement les valeurs de configuration Creole.

Modifier la valeur d'une variable avec CreoleSet

CreoleSet est un utilitaire très pratique pour modifier la valeur d'une variable Creole.
Il s'utilise tout simplement en lui donnant le nom de la variable et sa valeur en argument :
`CreoleSet mon_ip 10.10.10.55`



L'option `--default` permet de réinitialiser une variable à sa valeur par défaut :
`CreoleSet --default serveur_ntp`
La commande `CreoleSet` supporte l'autocomplétion à partir de la version 2.5.2 d'EOLE.

Les valeurs multiples doivent être séparées par un saut de ligne (`\n`) :

```
root@eolebase:~# CreoleSet serveur_maj "eole.ac-toto.fr
ftp.crihan.fr"
```



La modification d'une variable possédant des dépendances fortes avec d'autres variables ou familles ne sera généralement pas possible car cela cassera la consistance des données.



L'option `-h` ou `--help` ou la commande `man CreoleSet` permettent d'obtenir de l'aide.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.6.3. CreoleRun et CreoleService

CreoleRun et **CreoleService** sont des utilitaires permettant de lancer des commandes système et de gérer les services sur les modules EOLE, y compris à l'intérieur des conteneurs[p.456].

Exécuter une commande avec CreoleRun

CreoleRun est un utilitaire très pratique pour exécuter une commande dans un conteneur (depuis le maître).

Le script s'utilise de la façon suivante :

```
CreoleRun "<command>" <container>
```



Si le mot clé `all` est utilisé à la place du nom du conteneur, alors la commande sera lancée dans tous les conteneurs (rien ne sera exécuté en mode non conteneur).

La commande gère un troisième argument qui si il vaut `yes` exécutera la commande uniquement si l'environnement est un conteneur (ie : si l'utilisation de SSH est nécessaire).

Gérer les services avec CreoleService

CreoleService permet de gérer les services déclarés dans les dictionnaires Creole.

Le script s'utilise de la façon suivante :

```
CreoleService [-c <container>] <service> <action>
```

Les actions possible sont :

- *configure* : configure le lancement automatique du service au démarrage du serveur en fonction de la configuration Creole du serveur ;
- *enable* : active le lancement automatique du service au démarrage du serveur ;
- *disable* : désactive le lancement automatique du service au démarrage du serveur ;
- *apply* : démarre ou arrête le service en fonction de la configuration Creole du serveur ;
- *start* : démarre le service ;
- *stop* : arrête le service ;
- *restart* : redémarre le service ;
- *reload* : recharge le service ;
- *status* : vérifie l'état du service.



L'option, `-f` (ou `--force`) permet de forcer le démarrage ou redémarrage d'un service même si celui-ci est désactivé au niveau de la configuration Creole du serveur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.6.4. CreoleLock

CreoleLock est un utilitaire permettant de placer, enlever ou vérifier les verrous Creole.

Il peut gérer deux niveaux (level) de verrouillage distincts.

La plupart des outils de base EOLE utilisent de verrous de niveau "système".

Verrou "normal"

Ce type de verrou permet d'éviter qu'une même application soit exécutée deux fois en parallèle. Il s'agit donc d'un verrou isolé.

En mode normal (`--level=normal`), les fichiers lock sont écrits dans le répertoire `/var/lock/eole` et il est possible d'exécuter plusieurs applications différentes en même temps tant qu'elles ne posent pas un lock ayant le même nom.

Verrou "système"

Contrairement au mode normal, les verrous "système" (`--level=system`) sont exclusifs. Cela permet d'éviter que deux applications concurrentes sont exécutées en même temps. Par exemple, il ne faut pas qu'un reconfigure soit exécuté en même temps qu'une sauvegarde : ces deux procédures utilisent des verrous "système".

Dans ce mode, mes fichiers lock sont écrits dans le sous-répertoire `/var/lock/eole/eole-system`.

Nom d'un fichier lock

Le nom d'un fichier lock est de la forme `prefixe.suffixe`, avec :

- un préfixe invariant fourni par le programme (généralement le nom de l'application) ;
- un suffixe représentant le PID[p.469] de l'application.

Poser un verrou avec CreoleLock

Pour poser un verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock acquire --name toto
```

Si un verrou existe déjà, la commande affichera un message d'erreur et ne renverra pas le code `0`.

Vérifier la présence d'un verrou avec CreoleLock

Pour vérifier la présence du verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock is_locked --name toto
```

Cette commande retournera le code `0` si le verrou est présent.

Supprimer un verrou avec CreoleLock

Pour supprimer un verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock release --name toto
```

Cette commande retournera le code `0` en cas de succès.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Seul le programme (y compris la console si la commande est lancée en console) qui a posé le verrou a le droit de le supprimer.

API python

La librairie `pyeole.lock` permet de gérer les verrous Creole directement en python.

Elle fournit notamment les fonctions `acquire`, `is locked` et `release`.

L'option `-h` permet d'afficher les paramètres de la commande CreoleLock :

```
# CreoleLock -h
usage:      /usr/bin/CreoleLock      [acquire|release|is_locked]
[options|--help]
```

2.6.5. Indications pour la programmation

Certaines fonctions ont été intégrées sur les modules afin que les scripts puissent être écrits en tenant compte des spécificités des modules EOLE, que sont les variables et le mode conteneur.

Programmation bash

- obtenir la valeur d'une variable (variables de conteneur comprises) :
  `CreoleGet <variable_name>`
- obtenir la valeur d'une variable ou une valeur prédéfinie en cas d'erreur :
  `CreoleGet <variable_name> <default_value>`
- modifier la valeur d'une variable :
  `CreoleSet <variable_name> <new_value>`
- exécution d'une commande dans un conteneur :
  `CreoleRun "<command>" <container>`
- redémarrage d'un service dans un conteneur :
  `CreoleService -c <container> <service_name> restart`

Petit script bash

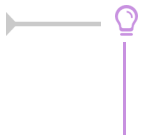
```
1 #!/bin/bash
2 echo "mon adresse IP est $(CreoleGet adresse_ip_eth0)"
3 echo "La base Ldap est stockée dans $(CreoleGet container_path_annuaire)
  /var/lib/ldap"
4 echo "Le conteneur annuaire a l'adresse : $(CreoleGet
  container_ip_annuaire)"
5 CreoleRun "ls /var/lib/ldap" annuaire
6 CreoleService slapd restart -c annuaire
```

Script compatible EOLE 2.3/2.4/2.5

```
1 #!/bin/bash
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
if [ -f /usr/bin/ParseDico ];then
  RunCmd=RunCmd
  . /usr/bin/ParseDico
  . /etc/eole/containers.conf
  . /usr/share/eole/FonctionsEoleNg
else
  RunCmd=CreoleRun
  # récupération des variables nécessaires
  container_path_web=$(CreoleGet container_path_web)
  nom_machine=$(CreoleGet nom_machine)
fi
touch ${container_path_web}/etc/${nom_machine}.conf
$RunCmd "chown www-data /etc/${nom_machine}.conf" web
```



`CreoleGet` permet également d'accéder aux variables "extra" :

`CreoleGet schedule.schedule.hour`

Programmation Python

- obtenir la valeur d'une variable (variables de conteneur comprises) :

  ```
  from creole.client import CreoleClient
  CreoleClient().get_creole('<variable_name>')
  ```

- obtenir la valeur d'une variable ou une valeur prédéfinie en cas d'erreur :

  ```
  from creole.client import CreoleClient
  CreoleClient().get_creole('<variable_name>', '<default_value>')
  ```

- obtenir l'ensemble des variables dans un dictionnaire :

  ```
  from creole.client import CreoleClient
  dico = CreoleClient().get_creole()
  adresse_ip_eth0 = dico['adresse_ip_eth0']
  # cas particulier: pour les variables 'esclaves' d'un groupe, préfixer par la variable maître
  sso_first_base_ldap = dico['eolesso_ldap.eolesso_base_ldap'][0]
  ```

- obtenir la valeur d'une esclave correspond à une master :

  ```
  master = client.get_creole('master')
  slave = client.get_creole('slave')
  for idx, var in enumerate(master):
  print "master : {0}, slave : {1}".format(var, slave[idx])
  ```

- exécution d'une commande dans un conteneur (affichage à l'écran) :

  ```
  from pyeole.process import system_code
  system_code([<commande sous forme de liste>], container='<conteneur>')
  ```

- exécution d'une commande dans un conteneur (sorties dans un tuple) :

  ```
  from pyeole.process import system_out
  system_out([<commande sous forme de liste>], container='<conteneur>')
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- redémarrage d'un service dans un conteneur (avec affichage à l'écran)

  `from pyeole.log import init_logging`

  `from pyeole.service import manage_service`

  `init_logging(level='info')`

  `manage_service('restart', '<service>', '<conteneur>')`

Petit script Python

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-
from creole.client import CreoleClient
creole_client = CreoleClient()
print "mon adresse IP est {0}".format(creole_client.get_creole(
'adresse_ip_eth0'))
print "La base Ldap est stockée dans {0}/var/lib/ldap".format(
creole_client.get_creole('container_path_annuaire'))
print "Le conteneur annuaire a l'adresse : {0}".format(creole_client.
get_creole('container_ip_annuaire'))
from pyeole.process import system_code
system_code(['ls', '/var/lib/ldap'], container='annuaire')
from pyeole.log import init_logging
from pyeole.service import manage_service
init_logging(level='info')
manage_service('restart', 'slapd', 'annuaire')
```

Script compatible EOLE 2.3/2.4/2.5

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-
from pyeole.process import system_code
try:
    from creole import parsedico
    from creole.eosfunc import load_container_var
    variables = parsedico.parse_dico()
    variables.update(load_container_var())
except:
    from creole.client import CreoleClient
    variables = CreoleClient().get_creole()
fichier = open('{0}/etc/{1}.conf'.format(variables['container_path_web'],
variables['nom_machine']), 'a')
fichier.close()
system_code(['chown', 'www-data', '/etc/{0}.conf'.format(variables[
'nom_machine'])], container='web')
```

Modification de variables

Du fait des dépendances entre variables certaines modifications ne sont pas réalisables avec la commande `CreoleSet`.

C'est notamment le cas pour les variables groupées qui doivent impérativement posséder le même nombre d'éléments au moment de l'enregistrement ou pour des variables de type `oui/non` qui permettent de débloquer des variables à caractère obligatoire.

L'exemple qui suit montre comment activer l'autorisation des connexion SSH pour un couple adresse IP / masque de sous-réseau.

```
#!/usr/bin/env python
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# -*- coding: UTF-8 -*-
from creole.loader import creole_loader, config_save_values
config = creole_loader(rw=True)
config.creole.interface_0.ssh_eth0 = u'oui'
config.creole.interface_0.ip_ssh_eth0.ip_ssh_eth0[0] = u'192.168.1.1'
config.creole.interface_0.ip_ssh_eth0.netmask_ssh_eth0[0] =
u'255.255.255.255'
config_save_values(config, 'creole')
```

Pour accéder à une variable esclave, il faut connaître le nom de sa famille et celui de la variable maître associée.

Les valeurs doivent être saisies en Unicode[p.475], qui en python se traduit par l'ajout du caractère **u** devant la chaîne de caractères.

Cette obligation ne concerne pas les variables de type `number` qui attendent un nombre entier :

```
config.creole.systeme.bash_tmout = 3600
```

2.7. Ajout de script exécuté à l'instance ou au reconfigure

Il est parfois nécessaire d'ajouter un script qui sera exécuté à l'instanciation ou au reconfigure du module.

EOLE met en place des mécanismes permettant d'exécuter des scripts avant ou après l'instanciation ou la reconfiguration.

Ces scripts doivent être dans l'un des répertoires suivants :

- `/usr/share/eole/preservice` : exécution avant l'arrêt des services ;
- `/usr/share/eole/pretemplate` : exécution avant la templatisation des fichiers ;
- `/usr/share/eole/postemplate` : exécution entre la templatisation des fichiers et le redémarrage des services ;
- `/usr/share/eole/postservice` : exécution après le redémarrage des services.

Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.

L'ensemble de ces scripts se jouent de façon alphanumérique.

Les scripts fournit par EOLE sont préfixés par des chiffres et un tiret :

```
root@scribe:/usr/share/eole/preservice# ll
total 28
drwxr-xr-x  2 root root 4096 sept. 28 10:24 ./
drwxr-xr-x 29 root root 4096 sept. 28 10:24 ../
-rwxr-xr-x  1 root root  387 sept. 28 09:16 00-anetwork*
-rwxr-xr-x  1 root root  464 sept.  7 15:08 00-bareoswebui*
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
-rwxr-xr-x  1 root root  500 juin  26  2015 00-save-sid*
-rwxr-xr-x  1 root root  702 sept.  7 15:36 00-web*
-rwxr-xr-x  1 root root  235 sept. 28 09:16 99-ifupdown*
root@scribe:/usr/share/eole/preservice#
```

Le type d'appel (instance ou reconfigure) est envoyé au script sous la forme d'un argument :

```
#!/bin/bash
if [ "$1" == "instance" ]; then
    echo "ce code n'est exécuté qu'à l'instance"
elif [ "$1" = "reconfigure" ] ;then
    echo "ce code n'est exécuté qu'au reconfigure"
fi
```



Si le script quitte avec un autre code de retour que `0`, l'instance ou le reconfigure s'arrête immédiatement.

Il est donc préférable que le script soit de la forme :

```
#!/bin/bash
# <<< SCRIPT >>>
exit 0
```

Voir aussi...

Indications pour la programmation [p.378]

2.8. Ajout d'un test diagnose

Les scripts diagnose personnalisés peuvent être placés dans le répertoire `/usr/share/eole/diagnose`

Ces fichiers sont généralement écrits en bash et permettent de se connecter au service voulu pour tester l'état de celui-ci.



Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.

Un certain nombre de fonctions sont disponibles dans les librairies EOLE, mais vous pouvez créer vos propres fonctions pour vos besoins spécifiques.

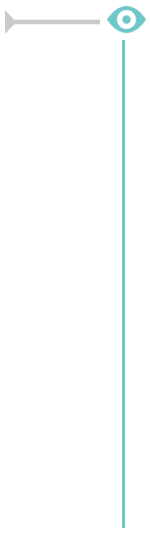
Généralement, le test affiche *Ok* si le service est fonctionnel et *Erreur* en cas de problème.

Voici quelques fonctions disponibles dans la librairie `/usr/lib/eole/diagnose.sh` :

- *TestIP* et *TestIP2* : testent si une IP répond au ping ;
- *TestARP* : teste si l'adresse MAC associée à une IP répond ;
- *TestService* : teste la connexion TCP sur une IP et un numéro de port ;
- *TestUDP* : teste si un port est ouvert localement en UDP ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- *TestPid* : teste la présence du PID d'une application locale ;
- *TestDns* : teste la résolution de nom sur un serveur DNS particulier ;
- *TestNTP* : teste un serveur NTP ;
- *TestHTTPPage* : teste l'ouverture d'une session HTTP ;
- *TestWeb* : teste le téléchargement d'une page HTTP ;
- *TestCerts* : teste des valeurs du certificat TLS/SSL.



```
#!/bin/bash
# utilisation des fonctions EOLE
. /usr/lib/eole/diagnose.sh
# teste si le serveur web local est fonctionnel
# en vérifiant la variable Creole "activer apache"
# et en utilisant la fonction TestHTTPPage
if [ $(CreoleGet activer_apache) = "oui" ];then
            TestHTTPPage   "Web   local"   "http://$(CreoleGet
adresse ip eth0)/"
fi
```

Voir aussi...

Indications pour la programmation [p.378]

2.9. Gestion des noyaux Linux

Noyau Linux utilisé

Les modules EOLE 2.6 utilisent par défaut le noyau le plus récent de la distribution Ubuntu.
Si le noyau utilisé est différent du noyau conseillé, les commandes `instance` et `reconfigure` vous proposeront de redémarrer le serveur ou le redémarreront automatiquement en fonction de la situation.



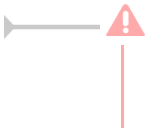
Sur les dernières versions d'Ubuntu 16.04, le noyau utilisé est `linux-image-generic-lts-xenial`.
Pour plus d'informations, consulter la page : http://doc.ubuntu-fr.org/ltsenablementstack

La commande `uname -r` permet de connaître le noyau en cours d'utilisation.

En-tête du noyau

Plusieurs outils nécessitent la présence des en-têtes du noyau (headers) sur le serveur.
Les en-têtes du noyau courant sont pré-installés sur les modules.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Les en-têtes des anciens noyaux sont purgés automatiquement lorsque le noyau associé est supprimé.

Purge des anciens noyaux

Tous les noyaux sont purgés à l'`instance` et au `reconfigure` à l'exception :

- du noyau en cours d'utilisation ;
- du noyau précédent le noyau utilisé ;
- du noyau le plus récent installé ;
- d'un éventuel noyau personnalisé (voir ci-dessous).

Personnalisation du noyau

Dans certains cas (prise en charge de matériels, tests,...), il peut être nécessaire d'utiliser un autre noyau (compilé ou non par vos soins) que le noyau courant.

Créer le fichier `/usr/share/eole/noyau/local` avec le numéro de version du noyau à utiliser permet de forcer l'utilisation d'un noyau antérieur ou d'un noyau compilé.



Pour utiliser le noyau **linux-image-4.4.0-112-generic** il faut ajouter le numéro de version du noyau 4.4.0-112 dans le fichier `/usr/share/eole/noyau/local` :

```
# echo 4.4.0-112 > /usr/share/eole/noyau/local
```

Mettre à jour Grub :

```
# update-grub
```

Pour réutiliser le noyau courant il faut supprimer le fichier `/usr/share/eole/noyau/local` et mettre à jour Grub à l'aide de la commande `update-grub`.



Cette facilité est à utiliser à titre exceptionnel.

Aucun signalement lié à l'utilisation d'un noyau différent de celui préconisé par EOLE ne sera pris en compte.

2.10. Gestion des tâches planifiées eole-schedule

Présentation

Sur les modules EOLE, les tâches planifiées (comme par exemple les mises à jour, les sauvegardes, la purge de certaines informations, l'exportation de l'annuaire, des bases de données et des quotas disque ou encore les mises à des listes noires pour le filtrage proxy) sont gérées par `eole-schedule`.

Contrairement à l'utilisation de cron, `eole-schedule` permet de maîtriser les tâches planifiées même si la sauvegarde est activée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Depuis la version 2.5 d'EOLE, `eole-schedule` est géré depuis Tiramisu[p.475].

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est cron[p.457] qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bareos[p.454] qui lance `eole-schedule`.

Il existe 4 types de tâches planifiées :

- les tâches journalières : *daily* ;
- les tâches hebdomadaires : *weekly* ;
- les tâches mensuelles : *monthly* ;
- les tâches uniques : *once*.

Ces tâches sont découpées en *pre*-sauvegarde et *post*-sauvegarde.

Si aucune sauvegarde n'est prévue : le *cron* lance *pre* puis *post* à l'heure qui a été tirée au hasard.

Si une sauvegarde est prévue : Bareos lance *pre* avant la sauvegarde et *post* à l'heure qui a été tirée au hasard (sauf si celle-ci est prévue avant la sauvegarde ou si la sauvegarde n'est pas terminée, dans ce cas les tâches *post* sont exécutées après la sauvegarde).

Les sauvegardes "post" sont obligatoirement marquées en `Full` même si cela ne correspond à rien (pas de sauvegarde, exécution des scripts uniquement). Elles sont réalisées à l'heure qui a été tirée au hasard.

Par contre, les sauvegardes "pre" sont bien lancées à l'heure des sauvegardes définie par l'administrateur.

Différences par rapport à Schedule 2.3

La liste des scripts à activer est décrite dans un fichier XML[p.477] (dictionnaire). 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 ce qui est à la fois plus simple et plus sûr.

La description n'est plus dans le script. Elle est directement dans le fichier XML.

Les scripts pre/post sont maintenant mélangés dans le répertoire `/usr/share/eole/schedule/scripts`.

Gestion des tâches planifiées

Lister ce qui est programmé

```
# manage_schedule -l
```

Ajouter une tâche planifiée

```
# manage_schedule -a daily -s majblacklist -m post
```

Supprimer une tâche planifiée

```
# manage_schedule -d majblacklist
```

Appliquer la configuration (génération des liens symboliques)

```
# manage_schedule --apply
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'ajout et la suppression n'appliquent pas la configuration. Il faut :

- soit l'appliquer à la main (`manage schedule --apply`) ;
- soit effectuer un `reconfigure`.

À partir d'EOLE 2.6.1, l'option `-m` (ou `--mode`) est obsolète.

Le mode (`pre` ou `post`) utilisé pour un script est forcément celui qui a été déclaré dans le dictionnaire extra.

Les commandes actuelles sont toujours fonctionnelles mais sont susceptibles d'afficher des avertissements.

Gestion des tâches uniques (once)

Les scripts lancés pour une nuit sont gérés totalement différemment et les informations associées ne sont pas conservées dans Tiramisu.

Ajouter une une tâche planifiée unique

```
# manage_schedule -a once -s majauto -m post
```

Supprimer une une tâche planifiée unique

```
# manage_schedule -d once -s majauto -m post
```

La prise en compte des tâches uniques est instantanée.

L'appel à la méthode `--apply` n'est donc pas nécessaire.

À partir d'EOLE 2.6.1, l'option `-m` (ou `--mode`) est obsolète.

Le mode (`pre` ou `post`) utilisé pour un script est forcément celui qui a été déclaré dans le dictionnaire extra.

Les commandes actuelles sont toujours fonctionnelles mais sont susceptibles d'afficher des avertissements.

Exemple de fichier XML

Les fichiers XML décrivant les tâches planifiées ont un format proche de celui des dictionnaires[p.457] Creole.

Exemple du fichier : `/usr/share/eole/creole/extra/schedule/01_majauto.xml`

```
1 <?xml version="1.0" encoding="utf-8"?>
2
3 <creole>
4     <variables>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
        <family name='majauto'>
            <variable name="description" type="string"><value>Mise à jour
du serveur</value></variable>
            <variable name="day" type="schedule"><value>weekly
</value></variable>
            <variable name="mode" type="schedulemod"><value>post
</value></variable>
        </family>
    </variables>
</creole>
```

Gestion des mises à jour avec Creole et eole-schedule

La mise à jour hebdomadaire consiste en un script `eole-schedule` nommé `majauto`. Il est configuré pour être lancé une fois par semaine (`weekly`) après la sauvegarde (`post`).

Sa gestion dans les scripts python est facilitée par la librairie `creole.maj`.

Savoir quand est prévue la mise à jour

```
# python -c "from creole import maj; print maj.get_maj_day()"
```

Activer/désactiver la mise à jour hebdomadaire

Activation de la mise à jour hebdomadaire :

```
# manage_schedule -a weekly -s majauto -m post
```

ou :

```
# python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
# manage_schedule -d majauto
```

ou :

```
# python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

À partir d'EOLE 2.6.1, l'option `-m` (ou `--mode`) est obsolète.

Le mode (`pre` ou `post`) utilisé pour un script est forcément celui qui a été déclaré dans le dictionnaire extra.

Les commandes actuelles sont toujours fonctionnelles mais sont susceptibles d'afficher des avertissements.

Forcer l'exécution des tâches planifiées

Il est possible de forcer l'exécution des tâches planifiées avec la commande `/usr/share/eole/schedule/schedule cron`.

```
root@amon:~# /usr/share/eole/schedule/schedule cron
Démarrage de pre schedule daily
pre schedule daily accompli
Démarrage de post schedule daily
.  Test de http://eole.orion.education.fr/maj/blacklists => Ok
Téléchargement des bases
Rien à faire pour blacklists.tar.gz
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Rien à faire pour le fichier weighted
eole-schedule - run-parts: executing
 /usr/share/eole/schedule/daily/post/majblacklist daily
post schedule daily accompli
Démarrage de pre schedule once
pre schedule once accompli
Démarrage de post schedule once
post schedule once accompli
root@amon:~#
```

Lire les journaux de l'exécution des tâches planifiées

Les journaux de l'exécution des tâches planifiées se trouvent dans le répertoire `/var/log/rsyslog/local/eole-schedule/`.

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:~#
```

À partir d'EOLE 2.7.0, il est possible de fixer le jour et l'heure de la mise à jour hebdomadaire à l'aide de la commande `CreoleSet`.



Pour paramétrer la mise à jour hebdomadaire le mercredi matin à 3h30, il faut exécuter les commandes suivantes :

```
root@eole:~# CreoleSet .schedule.schedule.weekday 3
root@eole:~# CreoleSet .schedule.schedule.hour 3
root@eole:~# CreoleSet .schedule.schedule.minute 30
```

Le jour choisi devra cependant être différent de celui choisi pour le "Jour des tâches mensuelles la première semaine du mois" (`.schedule.schedule.monthday`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.11. Gestion du pare-feu eole-firewall

Introduction

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper[p.474] et l'activation de modules noyau.

`eole-firewall` ne gère que des "autorisations", des règles en INPUT sur un port déterminé.

Les flux sont bloqués en entrée depuis l'extérieur. En interne (entre le maître et les conteneurs et entre conteneurs) il n'y a pas de restriction.

Si un conteneur possède une seconde interface (variable du type : *adresse_ip_link*), les flux sont bloqués en entrée.

eole-firewall avec ERA

Pour les modules avec ERA, Amon et AmonEcole, les règles d'`eole-firewall` ne s'appliquent pas. Seules les règles ERA du modèle choisi s'appliquent.

eole-firewall sans ERA

`eole-firewall` ne gère que des "autorisations", des règles en INPUT sur un port déterminé. Ces autorisations peuvent être affinées avec des "restrictions".



Les flux sont bloqués en entrée depuis l'extérieur. En interne (entre le maître et les conteneurs et entre conteneurs) il n'y a pas de restriction.

Si un conteneur possède une seconde interface (variable du type : *adresse_ip_link*), les flux sont bloqués en entrée.

Pour gérer les "autorisations" il faut créer des dictionnaires personnalisés. Pour cela il faut se référer à la rubrique traitant des dictionnaires dans la personnalisation du module à l'aide de Creole.

Pour des cas particuliers et exceptionnels il est possible de décrire des règles de pare-feu dans des fichiers placés dans le répertoire `/usr/share/eole/bastion/data/`.

Ces fichiers de règles doivent respecter les critères suivants :

- commencer par #!/bin/bash ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- être exécutable ;
- ne pas contenir d'extension ;
- son code retour doit être 0.

La création de règles par cette méthode doit rester exceptionnelle.

Fichier `/usr/share/eole/bastion/data/40-icmp_static_rules` sur le module Scribe

```
#!/bin/bash
/sbin/iptables -A eth0-root -p icmp --icmp-type destination-unreachable -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type network-unreachable -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type source-quench -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type fragmentation-needed -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type time-exceeded -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type parameter-problem -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type echo-reply -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type echo-request -j ACCEPT
```

Créer des dictionnaires personnalisés pour gérer les règles du pare-feu eole-firewall

Utiliser des fichiers templates, paquets, services et règles de pare-feu [p.337]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 10

Résolution de problèmes

Sur les modules EOLE quelques outils sont disponibles pour aider à la résolution de problèmes. L'outil de diagnostic `diagnose` et la lecture des logs permettent l'identification de la plupart des problèmes. L'outil de génération de rapport aidera à rassembler des informations en vue d'une analyse.

1. Problèmes à la mise en œuvre

Erreur lors du partitionnement

L'outil de partitionnement affiche la question suivante : "partitionner le disques > Nom de volume déjà utilisé" :

Cela indique juste que des partitions LVM[p.465] (issues d'une installation antérieure) ont été détectées sur le disque dur.

Vous pouvez cliquer sur "oui" pour continuer l'installation.

Erreur lors de l'installation des paquets

L'installeur s'arrête ou affiche un message d'erreur lors de l'étape : "choisir et installer des logiciels" :

C'est peut-être uniquement parce que le CD-ROM utilisé est mal gravé ou abîmé.

Pour connaître la nature exacte du problème, vous pouvez réaliser les manipulations suivantes :

- `ctrl F2` (affiche la console de débogage)
- `nano /var/log/syslog` (édite le fichier de log)
- `ctrl W`, `ctrl V` (va à la fin du fichier)

puis utilisez la *flèche du haut* pour remonter dans le fichier jusqu'à trouver les lignes contenant des erreurs.

La présence de l'expression "I/O Error" indique qu'il y a eu des erreurs de lecture, dans ce cas, il faut graver un nouveau CD.

Erreur lors de la création des conteneurs

Il est possible de suivre le processus d'installation des conteneurs dans le journal d'activité `/var/log/isolation.log`

Problèmes lors de la configuration

Pour détecter les problèmes de configuration, il faut utiliser la commande `diagnose`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Avant de chercher un éventuel problème, il est recommandé de lancer une reconfiguration du module à l'aide de la commande `reconfigure`.

2. Problèmes à l'exploitation

La commande diagnose

Lors de la mise en œuvre d'un module, un outil de diagnostic permet de valider que la configuration est correcte et fonctionnelle.

la commande `diagnose` valide donc les points clés de la configuration des services.

L'état des services est indiqué clairement par un code couleur vert/rouge.

```
Last login: Wed Jan 27 11:15:15 2016 from 192.168.230.146
root@horus:~# diagnose

*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Cartes réseau
eth0: Link detected: yes

*** Interfaces
horus:           192.168.0.25 => Ok

*** Services distants
.      Passerelle 192.168.0.1 => Ok
.           DNS 192.168.232.2 => Ok
.            NTP pool.ntp.org => Ok
.               Accès distant => Ok

Sur l'interface réseau eth0
.                          SSH => Ok
.                   EAD Server => Ok
.                      EAD Web => Ok

*** Pare-feu
.       Génération des règles => Ok (22:42:30 26/01/16)
.                    Pare-feu => Ok

*** Validité du certificat
.                    eole.crt => Ok
```

Les points importants de l'état du serveur sont vérifiés :

- la version du module installé ;
- la connectique réseau et sa configuration ;
- l'état des principaux services.

S'il apparaît que certaines sections sont en erreur, il faut revoir la configuration dans l'interface dédiée et reconfigurer le serveur.

Le diagnose, mode étendu

Si le diagnostic précédent n'est pas suffisant pour comprendre d'éventuelles erreurs, un mode étendu avec l'option `-L` permet d'obtenir plus d'informations :

```
# diagnose -L
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Configuration matérielle du serveur

Type  :
Standard PC (i440FX + PIIX, 1996) - QEMU

Processeur :
  QEMU Virtual CPU version 2.0.0

Carte réseau :
    Virtio

Disques :
       DVD reader

 Appuyez sur Entrée pour continuer ...
```

Le premier écran détaille l'aspect matériel du serveur.

```
Sys. de fichiers           Taille Utilisé Dispo Uti% Monté sur
udev                         486M    4,0K  486M   1% /dev
tmpfs                        100M    5,3M   95M   6% /run
/dev/mapper/horus--vg-root   3,4G    2,0G  1,2G  64% /
none                         4,0K       0  4,0K   0% /sys/fs/cgroup
none                         5,0M       0  5,0M   0% /run/lock
none                         497M       0  497M   0% /run/shm
none                         100M       0  100M   0% /run/user
/dev/mapper/horus--vg-home    18G     75M   17G   1% /home
/dev/mapper/horus--vg-tmp    1,8G    3,4M  1,7G   1% /tmp
/dev/vda2                    688M     69M  570M  11% /boot
/dev/mapper/horus--vg-var     14G    603M   13G   5% /var

Inode disques  :
Sys. de fichiers           Inœuds IUtil. ILibre IUti% Monté sur
udev                         122K    476   121K    1% /dev
tmpfs                        125K    470   124K    1% /run
/dev/mapper/horus--vg-root   220K   116K   105K   53% /
none                         125K      2   125K    1% /sys/fs/cgroup
none                         125K      5   125K    1% /run/lock
none                         125K      1   125K    1% /run/shm
none                         125K      2   125K    1% /run/user
/dev/mapper/horus--vg-home   1,2M     90   1,2M    1% /home
/dev/mapper/horus--vg-tmp    120K    152   119K    1% /tmp
/dev/vda2                     45K    304    45K    1% /boot
/dev/mapper/horus--vg-var    888K   5,9K   883K    1% /var

 Appuyez sur Entrée pour continuer ...
```

Le deuxième écran détaille les disques reconnus, leur partitionnement, et le taux d'occupation des partitions affichées.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
*** Paquets installés

Noyau linux : Linux 4.2.0-25-generic

Vérification des paquets installés : OK

Vérification des mises à jour...
Mise à jour le jeudi 28 janvier 2016 11:04:10
*** horus 2.5.2 (0000000A) ***

Configuration du dépôt Ubuntu avec la source test-eole.ac-dijon.fr
Configuration du dépôt EOLE avec la source test-eole.ac-dijon.fr
Action update pour root
Action list-upgrade pour root
0 nouveau, 11 mis à jour, 0 à enlever
Paquets à mettre à jour :
    apache2 (2.4.7-1ubuntu4.9) (root)
    apache2-bin (2.4.7-1ubuntu4.9) (root)
    apache2-data (2.4.7-1ubuntu4.9) (root)
    apt (1.0.1ubuntu2.11) (root)
    apt-transport-https (1.0.1ubuntu2.11) (root)
    apt-utils (1.0.1ubuntu2.11) (root)
    curl (7.35.0-1ubuntu2.6) (root)
    libapt-inst1.5 (1.0.1ubuntu2.11) (root)
    libapt-pkg4.12 (1.0.1ubuntu2.11) (root)
    libcurl3 (7.35.0-1ubuntu2.6) (root)
    libcurl3-gnutls (7.35.0-1ubuntu2.6) (root)

 Appuyez sur Entrée pour continuer ...
```

L'écran suivant affiche ensuite le nom du module, sa version, ainsi que l'état des mises à jour. Si comme ici, il en existe, il est conseillé de les installer pour vérifier si le problème rencontré est corrigé dans les nouveaux paquets.

```
Dernières actions Creole

2016-01-26T22:44:15.856124+01:00 horus.ac-test.lan zephir: INSTANCE => FIN : Configuration terminée
2016-01-28T11:04:10.400319+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T11:05:02.602131+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : 11 paquets à mettre à jour
2016-01-28T11:28:10.989084+01:00 horus.ac-test.lan zephir: MAJ => INIT : Début en devel
2016-01-28T11:28:12.422925+01:00 horus.ac-test.lan zephir: MAJ => MSG : Mise à jour en devel forcée par l'utilisateur
2016-01-28T11:30:44.113397+01:00 horus.ac-test.lan zephir: MAJ => FIN : 30 paquets mis à jour en devel
2016-01-28T11:30:44.117192+01:00 horus.ac-test.lan zephir: MAJ => MSG : Reconfiguration du serveur à planifier
2016-01-28T11:36:41.877030+01:00 horus.ac-test.lan zephir: RECONFIGURE => INIT : Début de configuration
2016-01-28T11:40:04.902914+01:00 horus.ac-test.lan zephir: RECONFIGURE => FIN : Configuration terminée
2016-01-28T11:56:25.998182+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T11:57:23.416706+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer
2016-01-28T14:37:48.275191+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T14:38:27.340008+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer
2016-01-28T14:42:33.432867+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T14:43:13.145804+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer

 Appuyez sur Entrée pour continuer ...
```

Le dernier écran affiche la liste des dernières actions Creole réalisées sur le serveur (mise à jour, reconfigure, Query-Auto, etc.).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Last login: Wed Jan 27 11:15:15 2016 from 192.168.230.146
root@horus:~# diagnose

*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Cartes réseau
eth0: Link detected: yes

*** Interfaces
horus:          192.168.0.25 => Ok

*** Services distants
.      Passerelle 192.168.0.1 => Ok
.           DNS 192.168.232.2 => Ok
.            NTP pool.ntp.org => Ok
.               Accès distant => Ok

Sur l'interface réseau eth0
.                         SSH => Ok
.                  EAD Server => Ok
.                     EAD Web => Ok

*** Pare-feu
.       Génération des règles => Ok (22:42:30 26/01/16)
.                   Pare-feu => Ok

*** Validité du certificat
.                   eole.crt => Ok
```

Enfin, on retrouve l'affichage standard de l'outil avec l'état des services.

Les journaux système

Lorsque des problèmes surviennent en exploitation, les journaux système (ou journaux de bord, fichiers de log, fichiers de journalisation) constituent une source incomparable d'informations. Ils contiennent la succession des événements ou des actions qui sont survenus sur un système informatique donné.

Ces fichiers sont au format texte, et sont généralement stockés en local dans le répertoire `/var/log`

L'outil de log utilisé par EOLE est `rsyslogd` et la configuration se trouve dans `/etc/rsyslog.conf`

Ce fichier définit les messages à enregistrer et le fichier cible, cela permet éventuellement de filtrer (ou répartir) les messages, par leur source et leur degré d'importance.

La plupart des logiciels disposent d'un paramètre "*log level*" permettant de régler la verbosité des informations journalisées.

En cas de problème, il est conseillé d'augmenter le niveau de journalisation du logiciel incriminé.

Les fichiers les plus couramment utilisés sont :

- `/var/log/messages` : contient tous les messages d'ordre général concernant la plupart des services et démons.
- `/var/log/syslog` : est plus complet que `/var/log/messages`, il contient tous les messages, hormis les connexions des utilisateurs.
- `/var/log/auth` : contient les connexions des utilisateurs.
- `/var/log/mail.log` : contient les envois et réception de mails.
- `/var/log/cron` : fichier log du service cron (planificateur système).



Il est possible de lire le contenu d'un fichier avec la commande `less` :

```
# less /var/log/syslog
```

Pour n'afficher que les dernières ligne d'un fichier, utiliser la commande `tail` :

```
# tail -n 50 /var/log/syslog
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La commande `tail` permet également d'afficher en temps réelle les nouvelles entrées dans un fichier. Pour cela, ajouter l'option `-f` :

```
# tail -f /var/log/syslog
```

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
18 [...]
```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

3. Trouver de l'information

Plusieurs sources d'information sont disponibles pour répondre de manière autonome aux questions que l'on se pose :

- équipes d'assistance académiques ;
- les documentations EOLE ;
- la FAQ des documentations ;
- aide sur les commandes ;
- les archives des listes de discussion ;
- les listes de discussion ;
- la documentation externe ;
- les wikis de la forge.

La documentation officielle EOLE

La documentation officielle EOLE est accessible depuis la page du module sur le site internet du projet EOLE dans la rubrique Documentation ou directement à l'adresse http://eole.ac-dijon.fr/documentations/

La documentation EOLE est publiée en HTML et en PDF, elle est divisée sous forme :

- de documentation par module ;
- de documentation transversale et thématique.

Les questions les plus fréquentes - FAQ

Les problèmes rencontrés fréquemment ont souvent déjà trouvés une solution, des FAQ sont proposées dans la documentation de chaque module, elles recensent les interrogations les plus courantes. Ces rubriques évolues régulièrement.



Une documentation thématique dédiée réuni les FAQ de tous les modules.

Aide sur les commandes

N'oubliez pas de consulter les pages de manuel installées sur le système avec la commande `man` :

```
# man nomDeLaCommande
```



```
# man man
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`# man setfacl` (`q` pour sortir)

Sur un serveur les différents commandes offrent de l'aide avec l'option `--help` :

```
# nomDeLaCommand --help
```



`# man --help`

Certains logiciels libres manquent encore de documentation ou ne sont pas documentés du tout. Dans ce cas, pensez à consulter le contenu de leur fichier de configuration. Certains commentaires donnent des indications voire remplacent une documentation externe.

Commandes utiles sous Linux

Voici quelques commandes qui peuvent vous aider à vous faire une idée plus précise de l'état du serveur. Voici une liste de quelques commandes utiles :

- `top -d1` (`q` pour sortir, `h` pour aide)
- `mc` (éditeur de texte)
- `links` (navigateur texte que l'on peut exécuter via SSH directement sur le serveur)
- `tcpdump` (examinateur de paquets)
- `nmap` (scanneur de ports)
- `tcpcheck` (testeur de port)

Les archives des listes de discussion

Les listes de discussion du projet sont archivés et mettent à disposition un moteur de recherche.

Rares sont les fils de discussion (threads ou topics) évoquant un questionnement ou un problème sans évoquer la réponse ou la solution.

https://pcll.ac-dijon.fr/listes

Les listes de discussion

Les listes de diffusions sont un espace d'échange qui est source d'aide et d'informations. Chaque module EOLE possède sa propre liste. Pour échanger sur les listes il faut préalablement être inscrit.

https://pcll.ac-dijon.fr/listes



Avant de poser une question sur une liste de discussion ou avant d'y répondre il faut s'assurer qu'elle n'a pas déjà trouvée réponse.



- Gardez toujours à l'esprit que beaucoup de gens vont lire ce que vous écrivez : ne postez jamais d'informations confidentielles sur une liste de diffusion.
- N'activer pas de répondeur sur une liste de discussion ;-).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- N'écrivez pas en privée aux membres de l'équipe, préférez exposer remarques publiquement ;
- Ne modifiez pas le champ "Répondre à" afin que les réponses soient envoyés à la liste et non à votre adresse personnel. Consultez cet explication pour Thunderbird : http://blogzinet.free.fr/index.php?2005/02/16/536-thunderbird-repondre-a-recurrent-dans-c
- Pour écrire à la liste n'utilisez pas un ancien message pour en modifier le sujet, le fil de discussion serait endommagé, il faut ouvrir un nouveau fil de discussion avec un sujet parlant.
- La Nétiquette décrit un certains nombre de règles lors de l'envoie de messages sur une liste de discussion, merci de les respecter.

  http://fr.wikipedia.org/wiki/Nétiquette

Documentation externe

La plupart des logiciels fournit avec les modules EOLE sont largement utilisés en dehors de l'Éducation nationale.

Des documentations plus spécifiques à l'utilisation de la plupart des logiciels utilisés sont disponibles sur Internet (ex. http://doc.ubuntu-fr.org/cups).

Dans le cas de la mise en place d'une configuration avancée de l'un des logiciels, il est tout à fait indiqué de consulter sa documentation officielle (ex. http://www.cups.org/documentation.php).



Les documentations externes peuvent faire état de commandes systèmes à exécuter.

Il n'est pas forcément judicieux de suivre ces instructions car les modules EOLE disposent d'un système d'auto-configuration (Creole[p.457]) qui risque d'écraser vos modifications ou même de ne plus fonctionner correctement.



En cas de doute, n'hésitez pas à demander à l'équipe.

Les wikis de la forge

Les wiki de la forge peuvent contenir des notes diverses comme des documentations techniques, des pistes de réflexion et des informations sur la diffusion, l'évolution et le développement des logiciels et des modules.



Les notes les plus importantes sont régulièrement intégrées à la documentation.

Les annonces

La publication des paquets fait l'objet d'annonces officielles :

- publication d'une annonce dans la forge : https://dev-eole.ac-dijon.fr/projects/modules-eole/news ;
- reprise de l'annonce dans les flux RSS du site officiel du projet : http://pcll.ac-dijon.fr/eole/ ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- envoi d'un message sur les principales listes de diffusion du projet : https://pcll.ac-dijon.fr/listes ;
- publication d'un message sur le compte Twitter du pôle de compétences : https://twitter.com/poleeole ;
- publication d'un message sur le compte Mastodon de l'équipe EOLE : https://mastodon.etalab.gouv.fr/@EOLE.

Le détail des paquets disponibles est indiqué dans les journaux des versions mineures concernées (exemple : https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Journaux262 pour EOLE 2.6.2).

Quelques références

- Site officiel du Pôle de Compétences Logiciels Libres : https://pcll.ac-dijon.fr ;
- Site web officiel de la distribution : https://pcll.ac-dijon.fr/eole/ ;
- Le blog : http://pcll.ac-dijon.fr/eole/blog/ ;
- Les listes de discussion : https://pcll.ac-dijon.fr/listes ;
- La forge : http://dev-eole.ac-dijon.fr/ ;
- Les annonces
  - Sur la forge : http://dev-eole.ac-dijon.fr/news
  - Flux Atom : http://dev-eole.ac-dijon.fr/news.atom
- La documentation : http://eole.ac-dijon.fr/documentations/

4. Demander de l'aide / Signaler un problème

Les problèmes rencontrés ont fréquemment déjà trouvés une solution, il existe diverses sources d'informations à disposition :

- les documentations ;
- la FAQ des documentations ;
- les archives des listes de diffusion.

Avant de demander de l'aide

- Avez-vous consulté la documentation du projet ?
- Avez-vous consulté la FAQ ?
- Avez-vous consulté les archives des listes de discussion ?
- Avez-vous effectué un reconfigure sur le serveur ?
- Avez-vous répondu oui aux 4 questions listées ci-dessus ?

Collecte d'informations

RGPD
Si vous souhaitez échanger des données avec le Pôle de Compétences à des fins d'expertise, vous pouvez être amené à transférer des journaux, des mots de passe, des fichiers confidentiels qui

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

contiennent beaucoup d'informations concernant les utilisateurs (personnels administratif, enseignants, élèves, parents d'élèves).

Nous attirons votre attention sur les informations nominatives suivantes : nom, prénom, date de naissance, email, coordonnées des responsables.

Il est de votre responsabilité de vérifier tous les contenus et de les anonymiser.

Vous devez avoir l'aval du Responsable des données de votre organisation avant d'effectuer l'envoi.

Si vous utilisez la procédure `gen_rpt` présentée ci-dessous, l'archive sera chiffrée avec une clé détenue par le seul PCLL.

Cette procédure, vous permet de transférer d'autres fichiers en les incluant dans l'archive.

Le PCLL et le Ministère de l'Éducation nationale ne peuvent être tenus responsables de la mauvaise application de cette procédure.

Il faut collecter des informations permettant la compréhension et le contexte du problème rencontré. Par contre il faut trouver un juste milieu entre trop peu d'information et trop d'information.

Voici des informations qui selon le contexte vont être utile à la description du problème :

- La version précise du module utilisé ainsi que le niveau des mises à jour (stable, candidat, développement) ;
- Résultat de la commande de diagnostic diagnose (`diagnose -L` pour un diagnostic étendu) ;
- Les différentes étapes permettant de reproduire le problème rencontré ;
- Les extraits de fichiers de journalisation ;
- Toutes informations connexes ayant un rapport avec votre problème (les adaptations locales, patch, dictionnaires additionnels, logiciels supplémentaires, etc.) ;
- Joindre des copier/coller et/ou des captures d'écran ;
- Générer un rapport avec la commande `gen_rpt` ;

La commande `gen_rpt` permet de générer une archive incluant :

- les fichiers de configuration EOLE du serveur ;
- le diagnostic étendu ;
- la liste des processus en cours sur le serveur ;
- les règles de pare-feu appliquées sur le système ;
- l'historique des commandes système ;
- la liste des paquets installés ;
- plusieurs fichiers de journalisation ;
- le rapport d'extraction (selon le module) ;
- le rapport de sauvegarde (selon le module) ;
- le contenu du répertoire `/root/gen_rpt` (à partir de la version 2.7.2).

Le répertoire /root/gen_rpt peut être utilisé pour ajouter à l'archive des fichiers complémentaires utiles au diagnostic.

La commande `gen_rpt` crée les archives dans le répertoire courant.

L'archive nommée <module>-<numéro-etab>.tar.gz, non chiffrée, peut être envoyée à n'importe qui.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

À partir de la version 2.7.2, une archive chiffrée nommée `<module>-<numéro-etab>.tar.gz.gpg` est également générée. Seule l'équipe EOLE possède la clé nécessaire pour déchiffrer cette archive. Si vous voulez envoyer le rapport à l'équipe EOLE, envoyez cette archive chiffrée nommée `<module>-<numéro-etab>.tar.gz.gpg`.

Si une passerelle de courrier a été définie sur le serveur, il est possible d'envoyer l'archive par courriel.

Celui-ci pourra être immédiatement envoyée à l'équipe EOLE (merci de ne pas en abuser) ou à l'adresse de votre choix.

À partir de la version 2.7.2, l'envoi immédiat à l'équipe EOLE utilise la version chiffrée de l'archive. Dans le cas d'un envoi vers une autre adresse, il faut choisir quelle version de l'archive envoyer : normale ou chiffrée (mais dans ce dernier cas, uniquement lisible par l'équipe EOLE).

Si aucune passerelle de courrier n'a été définie sur le serveur, les deux versions de l'archive sont créées. Vous avez alors le choix de la version à récupérer pour un envoi depuis un autre poste.

Dans la collecte d'informations peuvent se trouver des informations sensibles, attention à leur diffusion sur des médias publics : IRC, liste de discussion, demande sur la forge…

Formuler une demande d'aide

Lorsque vous posez une question, gardez à l'esprit que ceux qui la liront n'auront que votre message pour se représenter votre demande. Essayez de donner une description précise du problème. Les informations précédemment collectées vous aiderons à fournir des détails.

- Écrivez dans un langage clair et concis, pas de langage SMS, soignez la grammaire et l'orthographe, cela permet d'éviter certains quiproquos ;
- Soyez précis et explicite sur le contexte du problème ou de l'aide demandée.

  Ne dites pas *Quand je clique sur la disquette ça marche pas.* mais dites plutôt *Dans LibreOffice, quand je clique sur l'icône en forme de disquette j'obtiens l'erreur suivante : "copiez le texte intégral de l'erreur ou faites une capture d'écran" ;*
- Décrivez les symptômes du problème, évitez les suppositions ou les interprétations.

  Préférez dire *Le fond d'écran ne s'affiche pas* plutôt que *Un firewall doit sûrement bloquer mon fond d'écran* ;
- Décrivez la chronologie des événements et/ou des symptômes de votre problème ;
- Décrivez le but à atteindre, le comportement attendu ;
- Le volume d'information n'a rien avoir avec la précision des informations attendues ;
- Ne dites jamais que votre problème est URGENT même si c'est le cas, personne n'aime se sentir contraint par le caractère urgent de la demande ;
- Ne posez votre question qu'une seule fois, même si la réponse se fait attendre. Il est par

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

exemple possible que la réponse nécessite des recherches et donc du temps.

La Nétiquette décrit un certain nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

http://fr.wikipedia.org/wiki/Nétiquette

Vous trouverez le développement intégral des différents points évoqués ci-dessus dans le document présent à cette adresse : http://www.gnurou.org/writing/smartquestionsfr

Les listes de discussion

Les listes de diffusions sont un espace d'échange qui est source d'aide et d'informations. Chaque module EOLE possède sa propre liste. Pour échanger sur les listes il faut préalablement être inscrit.

http://eole.orion.education.fr/listes

La liste de diffusion est un bon endroit pour poser votre question. Cependant la quantité des messages et leur contenu demande une certaine organisation de tous afin que les échanges restent cohérents, efficaces et cordiaux.

Voici quelques points à suivre lors de l'envoie d'un message :

- Utilisez un sujet le plus explicite et le plus adapté possible ;
- Envoyez vos messages dans des formats lisibles par tous les clients de messagerie : le texte brut est très apprécié, le HTML et les images animées beaucoup moins ;
- Si votre courrier comporte une énorme pièce jointe, préférez utiliser la compression ou l'utilisation d'un dépôt de fichiers externe ;
- Ne postez jamais d'informations confidentielles sur une liste de diffusion ;
- Nouveau sujet est équivalent à un nouveau fil de discussion. N'utilisez pas la fonction `Répondre à` un ancien message en en modifiant l'objet pour lancer un nouveau sujet. Créez vraiment un `Nouveau message`. Sinon, en classant par fils de discussion votre message sera confondu avec un autre sujet et risque de ne pas être vu.
- Laissez l'historique de la conversation dans votre réponse, pour ceux qui vous aide et qui n'ont pas votre problème en tête cela constitue un aide-mémoire et permet de se replacer rapidement dans le contexte.
- N'activer pas de répondeur (message d'absence) sur une liste de discussion ;
- N'écrivez pas en privée aux membres de l'équipe, préférez exposer vos remarques publiquement pour le bénéfice de tous ;
- Ne modifiez pas le champ "Répondre à" afin que les réponses soient envoyés à la liste et non à votre adresse personnel. Consultez cet explication pour Thunderbird : http://blogzinet.free.fr/index.php?2005/02/16/536-thunderbird-repondre-a-recurrent-dans-c
- Pour écrire à la liste n'utilisez pas un ancien message pour en modifier le sujet, le fil de

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

discussion serait endommagé, il faut ouvrir un nouveau fil de discussion avec un sujet parlant.

- La Nétiquette décrit un certain nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

  http://fr.wikipedia.org/wiki/Nétiquette

Discussion relayée par Internet

Internet Relay Chat ou IRC sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion, mais peut aussi être utilisé pour de la communication de un à un.

Vous pouvez nous rejoindre sur le canal `#eole` hébergé sur irc://irc.oftc.net:6667 ou grâce à l'interface https://webchat.oftc.net.



- Il est demandé de mettre son nom réel dans les paramètres du client. ;
- La Nétiquette décrit un certain nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

  http://fr.wikipedia.org/wiki/Nétiquette

Le Pôle de Compétences Logiciels Libres utilisait Freenode depuis 2008 comme réseau IRC. Suite aux changements des conditions d'usages de Freenode, la gestion du canal `#eole` nous a été enlevé sans préavis. Vous avez pu constater que les lignes d'accueil ont disparu. Maintenant, les utilisateurs doivent créer un compte (SSO) pour accéder à notre canal.

Faire un signalement sur la forge

Il est possible de faire des remonter aux travers des différents listes de discussion du projet EOLE mais pour une bonne prise en charge il vous sera demandé de saisir une demande dans la forge.

Il est possible de demander des évolutions, de l'aide ou de signaler des erreurs directement sur la forge à l'adresse suivante : http://dev-eole.ac-dijon.fr/projects/modules-eole/issues/new



Pour se faire il est recommandé de regarder avant si la demande n'existe pas déjà à l'adresse :

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



Lorsque vous renseignez un signalement, veillez à suivre ces quelques recommandations :

- Soyez clairs, donnez des explications claires de façon à ce que d'autres puissent reproduire le dysfonctionnement ;
- Séparez clairement les faits des suppositions ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> - S'il n'ont rien à voir, faites un signalement par dysfonctionnement rencontré ;
> - Si vous avez des informations susceptibles d'aider à résoudre le problème ou si vous avez la solution, n'hésitez pas à les joindre à votre demande.

Quelques références

- Site officiel du Pôle de Compétences Logiciels Libres : http://pcll.ac-dijon.fr ;
- Site web officiel de la distribution : http://eole.orion.education.fr ;
- Le blog : http://pcll.ac-dijon.fr/eole/blog/ ;
- Les listes de discussion : http://eole.orion.education.fr/listes [http://eole.orion.education.fr/] ;
- La forge : http://dev-eole.ac-dijon.fr/ ;
- Les annonces
  - Sur la forge : http://dev-eole.ac-dijon.fr/news
  - Flux Atom : http://dev-eole.ac-dijon.fr/news.atom
- La documentation : http://eole.ac-dijon.fr/documentations/

5. Contribuer au projet EOLE

Il est possible de contribuer au projet EOLE de différentes manières. Les contributions seront intégrées au fur et à mesure en fonction de ce qui est prioritaire dans les cycles de publication.

Les contribution peuvent aller du partage de l'astuce la plus simple jusqu'à des développements plus complexes en passant par la relecture, l'enrichissement de la documentation, l'écriture de tutoriels, le test des versions candidates, l'écriture d'un rapport de bug, la revue de code, la réponse aux demandes d'aide sur les listes de discussions…

Vous pouvez manifester votre désir de contribuer à des développements il faut s'inscrire et le signaler sur la liste dev-eole@listeseole.ac-dijon.fr.

Si votre contribution est complexe, une documentation expliquant son fonctionnement est toujours la bienvenue. Soit directement dans votre message, soit sous forme d'un fichier indépendant.

Pour permettre aux utilisateurs d'accéder à votre contribution vous pouvez :

- demander son intégration et sa diffusion directement par l'équipe ;
- fournir des ressources que nous pourrons intégrer à la documentation ou à l'espace contribution.

Demander des évolutions ou signaler des erreurs

Il est possible de faire des remonter aux travers des différents listes de discussion du projet EOLE mais pour une bonne prise en charge il vous sera demandé de saisir une demande dans la forge.

Il est possible de demander des évolutions, de l'aide ou de signaler des erreurs directement sur la forge à l'adresse suivante : http://dev-eole.ac-dijon.fr/projects/modules-eole/issues/new

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Pour se faire il est recommandé de regarder avant si la demande n'existe pas déjà à l'adresse :

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 11

Documentations techniques

1. Les dépôts EOLE

Architecture des dépôts EOLE

Un miroir des dépôts Ubuntu est disponible à l'adresse suivante :

http://eole.ac-dijon.fr/ubuntu

Le miroir propose pour chaque version de la distribution Ubuntu plusieurs catégories de paquets (les fichiers *.deb[p.460]) :

- **<version>-backports** : paquets contenant les évolutions fonctionnelles d'une version supérieure d'Ubuntu portées sur une version inférieure ;
- **<version>-proposed** : paquets candidats qui sont éligibles pour passer en version stable après validation totale (dysfonctionnement, régression, etc.) ;
- **<version>-updates** : paquets contenants des mises à jour correctives non critiques ;
- **<version>-security** : paquets contenants des mises à jour de sécurité ;
- **<version>** : paquets de la distribution Ubuntu tels que livrés sur la première image ISO de la version majeure, aucun paquet n'y est ajouté après la publication.

La synchronisation s'effectue chaque nuit.

Les dépôts EOLE 2.6 sont disponibles à l'adresse suivante :

http://eole.ac-dijon.fr/eole [http://eole.ac-dijon.fr/eole]

Les dépôts proposent pour chaque version d'EOLE plusieurs catégories de paquets (les fichiers *.deb) :

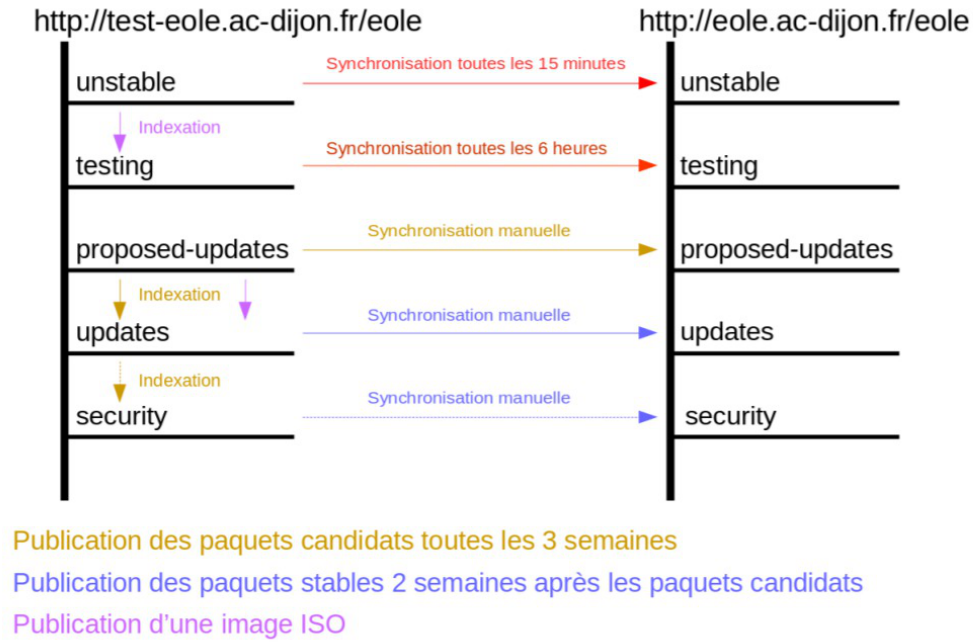
- **eole-2.6-unstable** : paquets de développement pouvant contenir des évolutions fonctionnelles, des corrections de sécurité ou de dysfonctionnement ;
- **eole-2.6-testing** : paquets candidats (correspondant aux images RC de la distribution) qui sont éligibles pour passer en version stable après validation ;
- **eole-2.6.x-proposed-updates** : paquets candidats qui sont éligibles pour passer en version update après validation (dysfonctionnement, régression, etc.) ;
- **eole-2.6.x-updates** : paquets contenant des mises à jour correctives non critiques ;
- **eole-2.6.x-security** : paquets contenant des mises à jour de sécurité ;
- **eole-2.6.x** : paquets EOLE tels que livrés sur la première image ISO de la version majeure, aucun paquet n'y est ajouté après la publication.

Politique de publication des paquets

Les mises à jour sont composées de paquets dépendants les uns des autres. Avant toute publication sur le site de référence http://eole.ac-dijon.fr/eole et sur les miroirs académiques (ex. : ftp://ftp.crihan.fr), les

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

paquets sont copiés sur le dépôt http://test-eole.ac-dijon.fr. Ce dépôt est réservé aux développeurs et aux contributeurs. Il permet d'avoir les paquets à disposition tels qu'ils le seront lors de la publication officielle. Ils sont utilisés durant le développement et lors des tests de mises à jour avant diffusion.



Le délai de synchronisation des paquets entre les 2 dépôts varie en fonction du type de paquet :

- **eole-2.6-unstable** : dépôt synchronisé toutes les 15 minutes ;
- **eole-2.6-testing** : dépôt synchronisé toutes les 6 heures ;
- **eole-2.6.x-proposed-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.6.x-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.6.x-security** : synchronisation manuelle avec annonce préalable ;
- **eole-2.6.x** : aucune modification sur ce dépôt.

Les miroirs académiques sont en principe synchronisés toutes les nuits.

Architectures supportées

Depuis la version 2.6, seule l'architecture 64 bits[p.453] (x86_64) est supportée par EOLE. Pour un paquet spécifique à une architecture le nom de celle-ci apparaît dans le nom du paquet :

- **all** : paquets compatibles avec toutes les architectures ;
- **amd64** : paquets compilés spécifiquement pour l'architecture 64 bits.

Signature des paquets EOLE

La clé GPG[p.461] publique de la clé signant les paquets EOLE est disponible à l'adresse : http://eole.ac-dijon.fr/eole/project/eole-2.6-repository.key

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Gestion des journaux systèmes sur EOLE

Architecture cible

Dans un souci d'harmonisation et de centralisation de l'information, la quasi totalité des logs est désormais rassemblée sur le maître dans le répertoire : `/var/log/rsyslog/local`

Par défaut, les logs des services installés dans un conteneur et qui utilisent rsyslog sont remontés sur le maître (fichiers de configuration : `/etc/rsyslog.d/99-aggregation.conf` dans les conteneurs).

L'utilisation de rsyslog laisse la possibilité de réaliser une configuration spécifique pour chaque service.

C'est déjà le cas pour `squid` par exemple (template : `80-squid.conf`).

Le répertoire `/var/log/rsyslog/remote` est quant à lui prévu pour recevoir les journaux de serveurs distants dans le cas de la mise en place d'un serveur de log centralisé (l'équivalent du serveur 2.2 : `ZéphirLog`).

Exceptions connues

A l'heure actuelle, plusieurs services ne sont pas directement pris en charge par rsyslog :

- les logs de `Samba` sont toujours stockés dans le répertoire : `/var/log/samba` et ne sont pas remontés sur le maître ;
- les logs de `ltsp-cluster-lbagent` et `ltsp-cluster-lbserver` sont toujours stockés dans le répertoire `/var/log` et ne sont pas remontés sur le maître.

Un lien symbolique permet toutefois d'accéder directement aux fichiers depuis le maître.

Rotation des logs

Les programmes dont les logs sont centralisés sur le maître doivent avoir une configuration *logrotate* avec les chemins adaptés sur le maître.



Si le service est susceptible d'être installé dans un conteneur et qu'il doit être redémarré, il faut penser à adapter les commandes.

La commande `CreoleService` permet, par exemple, de gérer un service y compris si celui-ci est dans un conteneur :

```
CreoleService -c <conteneur> <service> restart
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation

Note technique de l'ANSSI du 02/12/2013

Cette note technique détaille les prérequis nécessaires à la mise en œuvre d'un système de journalisation efficace et sécurisé et présente les bonnes pratiques permettant de bâtir une architecture de gestion de journaux pérenne, quelle que soit la nature du système d'information.

http://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journ

Note technique de l'ANSSI[p.453] du 02/12/2013 au format PDF :

http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf

3.1. Contexte juridique

Aspects juridiques et réglementaires

- les éléments juridiques doivent être pris en compte dans le cadre de la conception technique ;
- la réglementation pose un principe général d'effacement ou d'anonymisation des données de connexion ;
- il existe plusieurs régimes juridiques distincts en fonction de la nature de celui qui opère la journalisation ou du cadre dans lequel les éléments de journalisation sont générés.

Valeur probatoire des éléments de journalisation

- objectifs :
  - permettre la traçabilité de l'activité d'un réseau et d'apporter la preuve de cette activité (utilisation ou non-utilisation d'une application ou d'un service par un utilisateur, accès illégitime, etc) ;
  - être en capacité à identifier directement ou indirectement un individu ou un équipement ayant participé à cette activité.
- afin d'être opposable en cas de contentieux, leur mise en œuvre doit respecter les règles relatives à l'administration de la preuve et les principes directeurs des procès civils et pénaux

Traces nominatives

Régime général de protection des données à caractère personnel

- les éléments de journalisation peuvent contenir des données à caractère personnel (données relatives à une personne identifiable directement ou indirectement) ;
- une adresse courriel, une URL ou une adresse IP sont régulièrement considérées par la CNIL comme des données à caractère personnel.

Le traitement d'éléments de journalisation impose le plus souvent le respect des dispositions notamment de la loi du 6 janvier 1978 et en particulier :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- formalités préalables auprès de la CNIL (déclaration, autorisation, etc.) ;
- définir une politique claire adaptée aux données traitées et aux finalités ;
- définir le cycle de vie des éléments de journalisation (processus de création, de conservation, de destruction, etc.) ;
- respecter les exigences relatives aux droits de la personne.

Accès au traces nominatives

Jurisprudence CNIL

- seules des personnes spécifiquement habilitées peuvent accéder aux éléments de journalisation ;
- les personnes habilitées doivent être soumises à des obligations de confidentialité particulières ;
- l'accès doit être strictement limité à la finalité poursuivie, de la manière la moins intrusive possible pour les données à caractère personnel ;
- le personnel habilité ne doit subir aucune contrainte quant au dévoilement des informations, notamment par son employeur, sauf si la loi en dispose autrement (dans le cadre d'une procédure judiciaire) ;
- les éléments de journalisation ne peuvent être conservés que pour un temps limité ;
- les activités liées à la gestion des éléments de journalisation doivent être strictement limitées au but poursuivi ;
- les procédures liées à la gestion des éléments de journalisation doivent être décrites dans des documents de référence, permettant ainsi de s'assurer que les données à caractère personnel ne sont pas conservées de manière illégitime.

Régimes particuliers relatifs à la conservation des éléments de journalisation

- conservation des éléments de journalisation au minimum durant un an par les fournisseurs d'accès à Internet (FAI) et par les hébergeurs ;
- conservation des éléments de journalisation des opérateurs de communications électroniques.

3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation

Règles de conception technique

La prise en compte de la fonction de journalisation est primordiale et doit se faire lors de toute démarche de conception et de développement.

Les événements doivent être horodatés

- pour l'ensemble des événements et ce afin de permettre une meilleure exploitation des journaux ;
- les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles.

Dimensionnement

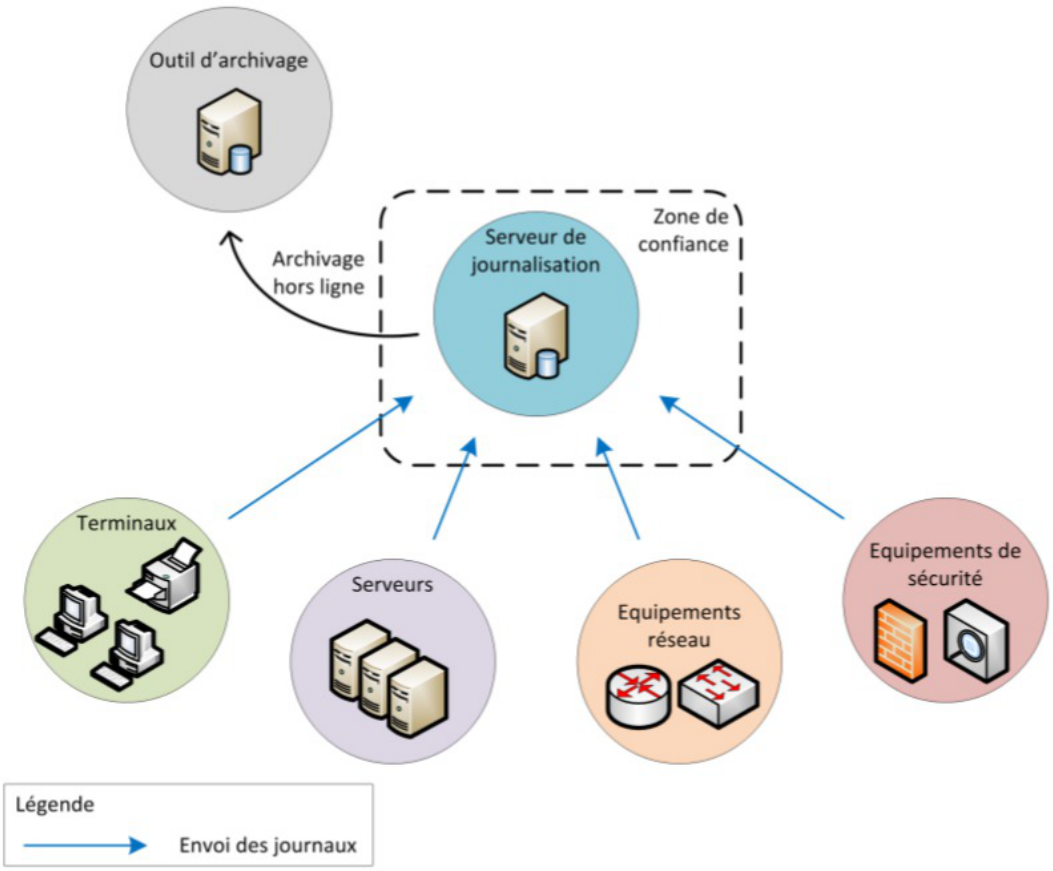
- l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux doit être prise

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

en compte dans le dimensionnement des équipements,

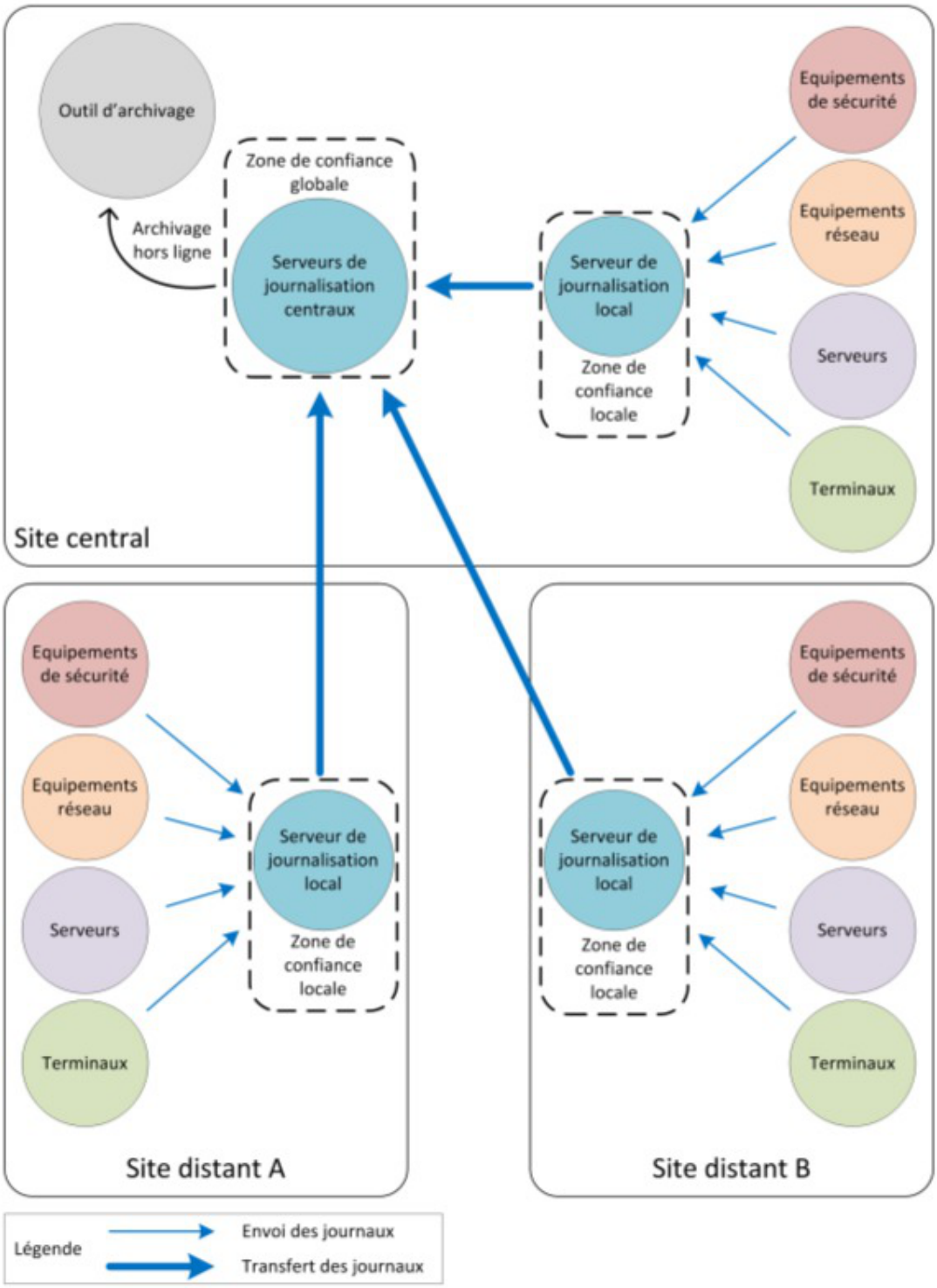
Recommandations d'architecture et de conception

- Les journaux doivent être automatiquement exportés sur une machine physique différente de celle qui les a générés ;
- centralisation des journaux journaux de l'ensemble des équipements du système d'information sur des serveurs dédiés ;
- redondance nécessaire du serveur central en cas de volume de journaux important ou selon le nombre de sites de collecte de journaux ;
- selon la taille ou la typologie du système d'information mise en place d'une approche hiérarchique pour l'organisation des serveurs de collecte.



Exemple d'architecture de journalisation simple (image du document officiel de l'ANSSI)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Exemple d'architecture de journalisation multi-sites (image du document officiel de l'ANSSI)

Protection des données échangées

- privilégier un transfert en temps réel des journaux sur les serveurs centraux ;
- ne pas effectuer de traitement sur les journaux avant leur transfert (peut conduire à dénaturer les événements et induire des pertes d'information).

Fiabilisation du transfert des journaux

- il est recommandé d'utiliser des **protocoles d'envoi de journaux basés sur TCP** pour fiabiliser le

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

transfert de données entre les machines émettrices et les serveurs centraux.

Sécurisation du transfert des journaux

- utiliser des protocoles de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes ;
- contrôler la bande passante des flux réseau utilisée pour transférer les journaux d'événements ;
- en cas de besoin de sécurité, le transfert des journaux doit se faire sur un réseau d'administration dédié ;
- placer les serveurs de journalisation dans un réseau spécifique non exposé directement à des réseaux qui ne sont pas de confiance.

Stockage

- dédier une partition disque au stockage des journaux d'événements ;
- prendre en compte les durées réglementaires de stockage.

Protection des journaux

- l'accès aux journaux doit être limité en écriture à un nombre restreint de comptes ayant le besoin d'en connaître ;
- les processus de journalisation et de collecte doivent être exécutés par des comptes disposant de peu de privilèges ;
- un outil spécifique doit être utilisé pour une meilleure exploitation des journaux présents sur les serveurs centraux ;
- les comptes ayant accès à l'outil de consultation centralisée des journaux doivent être associés à des rôles prédéterminés.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 12

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 service d'annuaire 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, AmonEcole, 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 le module AmonEcole, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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[p.472] Exim[p.460].

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, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 [p.469].

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)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

À ce jour, aucun module EOLE n'implémente l'utilisation de ce service en mode conteneur.

1.6. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.
Le logiciel utilisé, Nginx[p.467], peut également faire office de serveur web.

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Initialement conçu pour les modules Amon et AmonEcole, ce service est pré-installé sur tous les modules à partir de la version 2.6.1 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 123/udp : ntpd
- 465/tcp : smtps (Exim4)
- 514/udp : rsyslogd (réception des journaux distants)
- 3493/tcp : nut (gestion des onduleurs)
- 4505/tcp : saltstack EAD3 (publisher)
- 4506/tcp : saltstack EAD3 (request server)
- 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
- 8880/tcp : saltsatck EAD3 (salt-api)
- 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

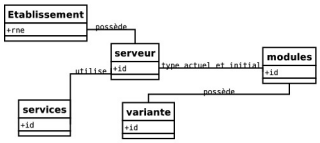
Les répertoires des serveurs contiennent les données suivantes :

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.477].

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```python
#!/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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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)
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
    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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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[p.459] 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# 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 [p.384]
- Restauration partielle

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 13

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.



1. Questions fréquentes communes aux modules

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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`# 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

Il faut ajouter le nom alternatif dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet `Certificats ssl` en mode expert il faut remplir les champs `Nom DNS/IP alternatif 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`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

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`.

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.476] 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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.

```
1 root@eole:~# manage_schedule -l
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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:~#
```

À partir d'EOLE 2.7.0, il est possible de fixer le jour et l'heure de la mise à jour hebdomadaire à l'aide de la commande `CreoleSet`.

Pour paramétrer la mise à jour hebdomadaire le mercredi matin à 3h30, il faut exécuter les commandes suivantes :

```
root@eole:~# CreoleSet .schedule.schedule.weekday 3
root@eole:~# CreoleSet .schedule.schedule.hour 3
root@eole:~# CreoleSet .schedule.schedule.minute 30
```

Le jour choisi devra cependant être différent de celui choisi pour le "Jour des tâches mensuelles la première semaine du mois" (`.schedule.schedule.monthday`).

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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:~#
```

Questions propres au partitionnement

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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% /
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  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` :

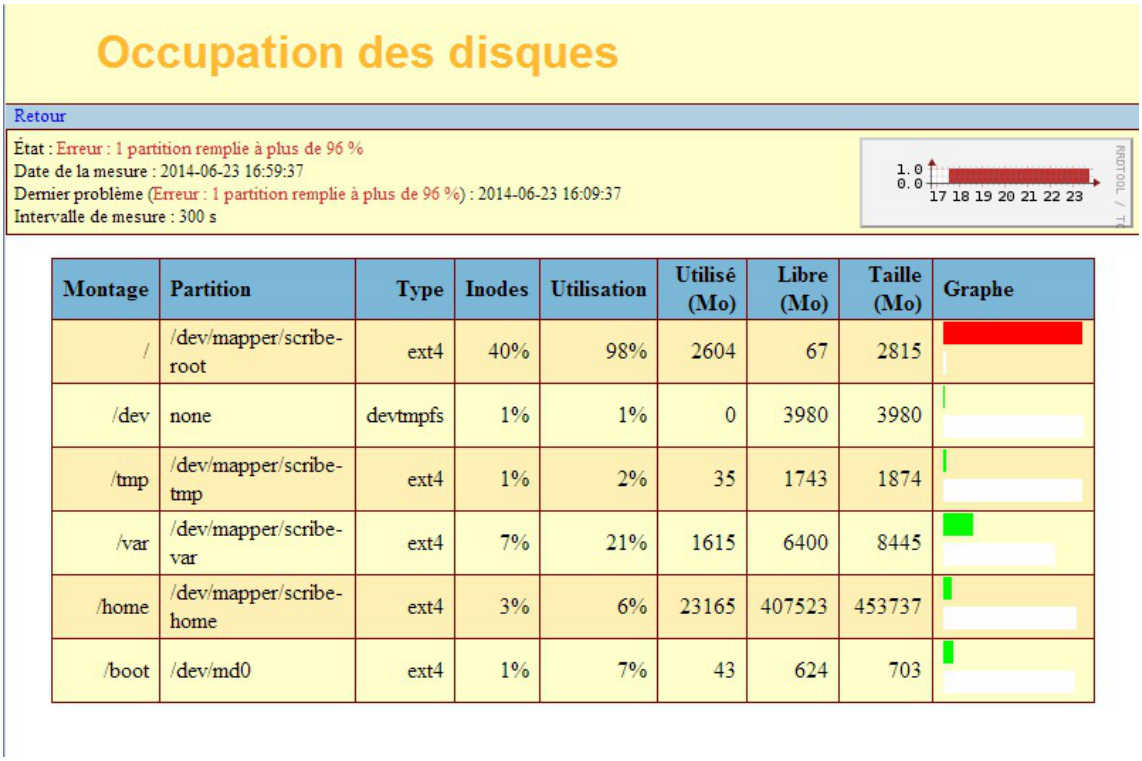
```
# mount /var/home
```



Pensez à redémarrer les services qui ont précédemment été arrêtés.

Partition saturée

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

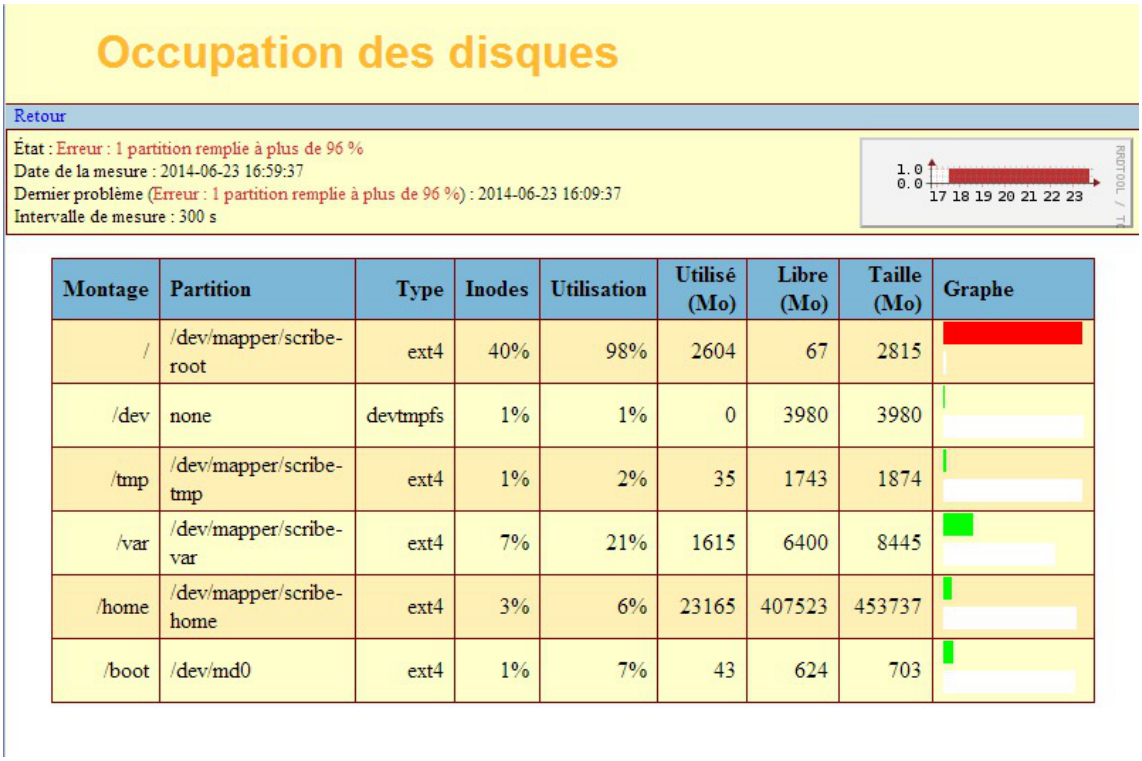
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	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	

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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. 465]).

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. 465]).

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

Questions propres à l'EAD

Problème d'accès à l'EAD avec un nom de domaine incorrect

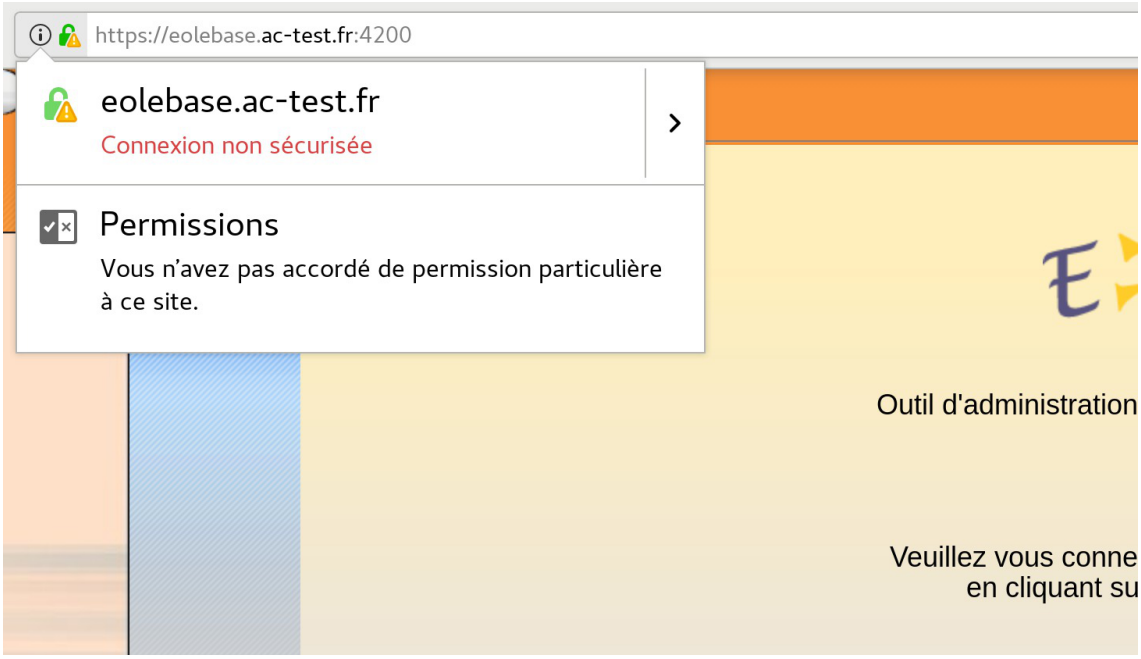
Pour avoir accès à l'EAD il faut impérativement que le nom de domaine soit présent dans le certificat SSL.

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

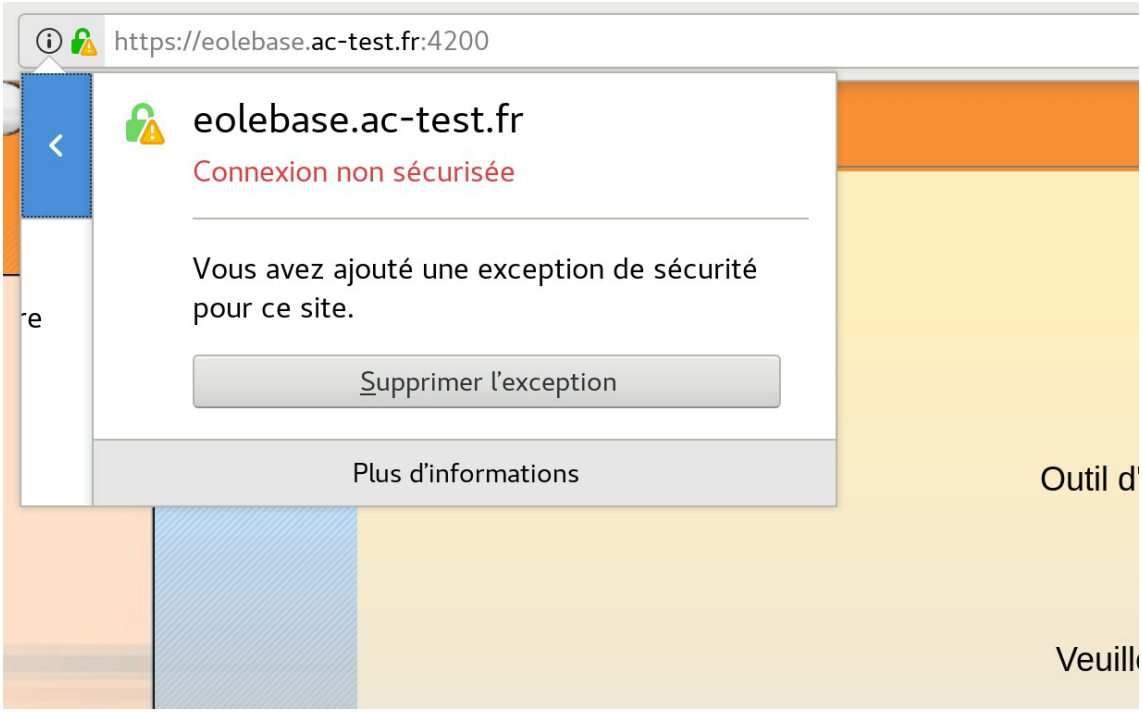
Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

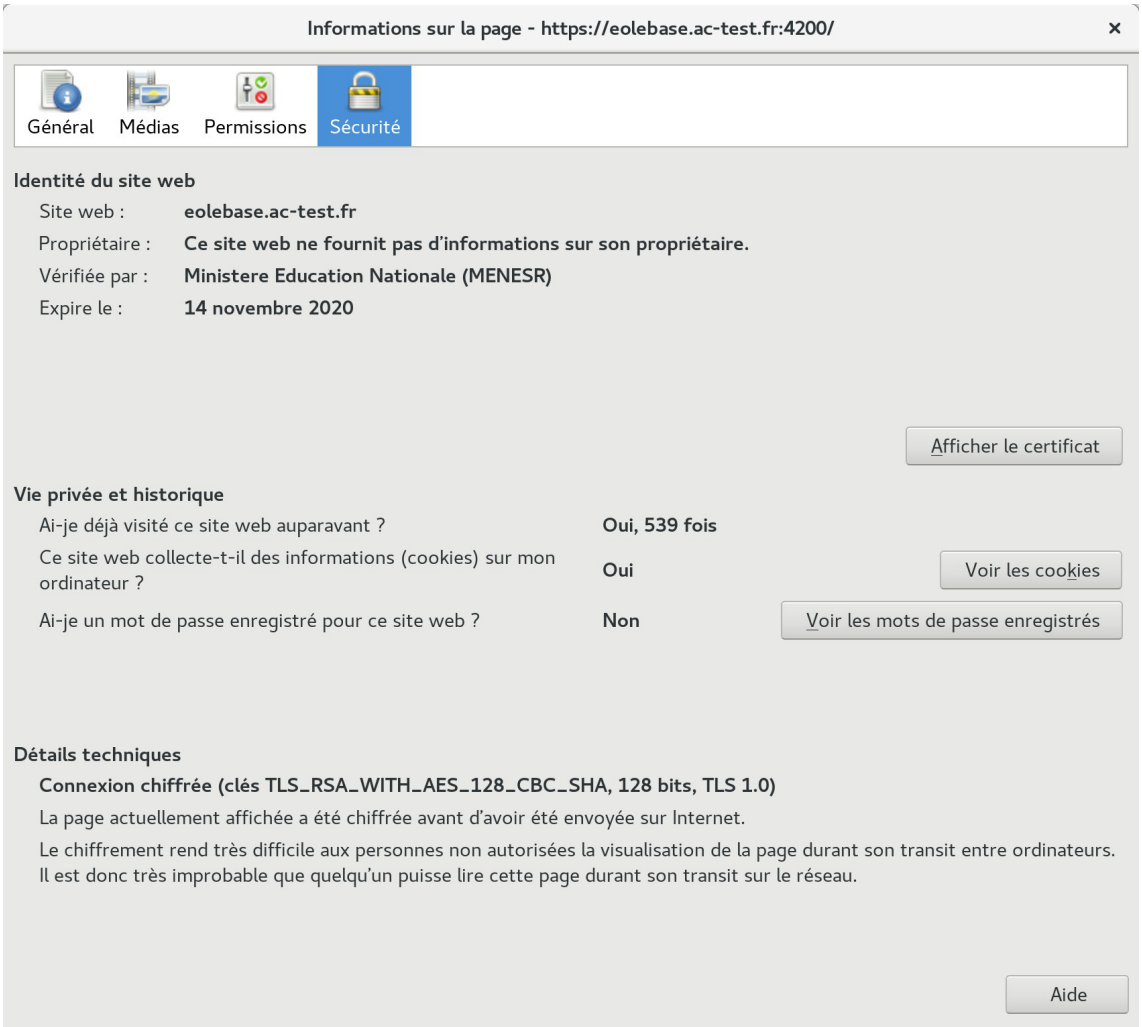


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



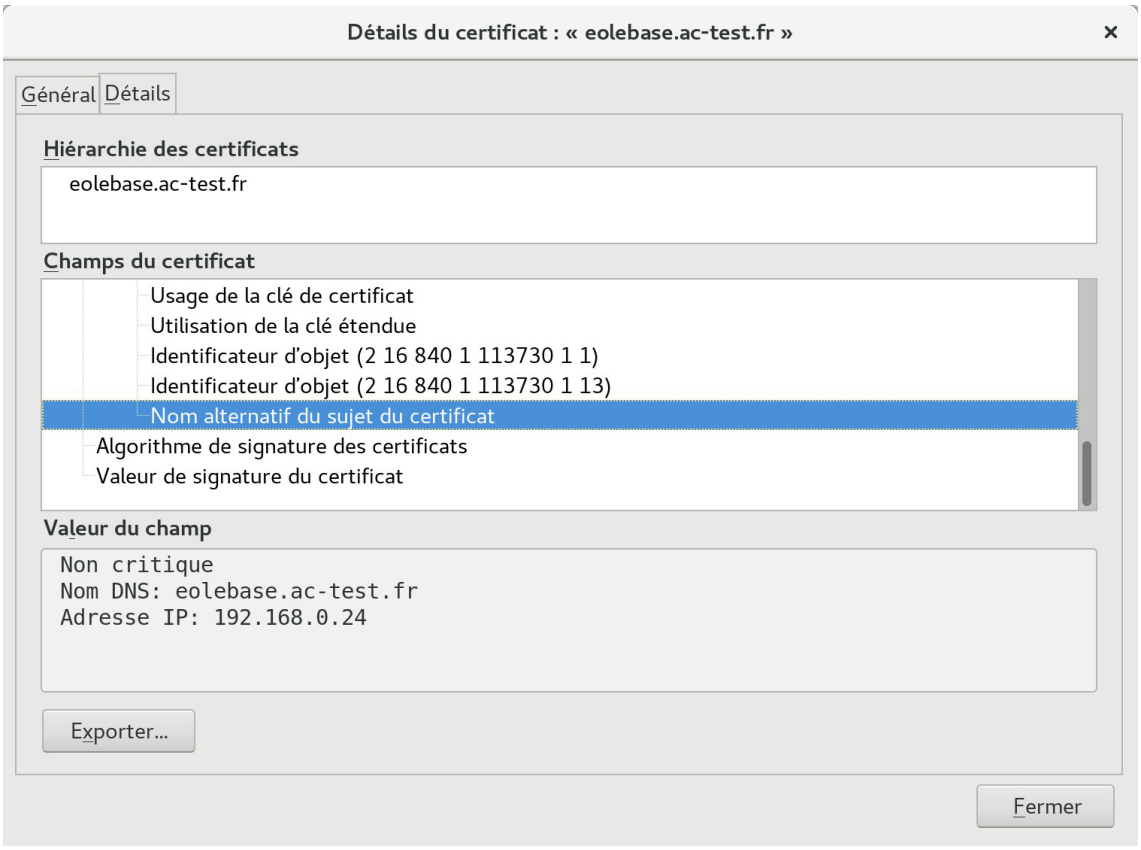
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- Il est possible que des noms alternatifs soient renseignés dans le certificat. Pour les retrouver, cliquer sur le bouton `Afficher le certificat`, puis sur l'onglet `Détails` et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.



Attention, même si la bonne adresse IP apparaît dans le certificat, elle ne sera pas prise en compte.

Si le nom de domaine n'apparaît pas et que le certificat est de type autosigné, il faut le rajouter dans l'onglet `Certificats ssl` de l'interface de configuration du module en mode expert.

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom d'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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`# 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`

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 des fichiers journaux `/var/log/rsyslog/local/ead-server/ead-server.info.log` et `/var/log/rsyslog/local/ead-web/ead-web.info.log` n'apportent pas d'informations pertinentes, le service peut être exécuté 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, le service peut être exécuté 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.

La mire de connexion de l'EAD3 n'affiche pas les informations de contexte, il est impossible de se connecter

La mire de connexion s'affiche mais le domaine, le nom du module et de la machine ne s'affiche pas. Il est de plus impossible de se connecter.

Vérifier le certificat et l'acceptation du certificat.

Pour fonctionner la connexion à l'EAD3 a besoin d'un certificat valide et reconnue par la navigateur. Le cache du navigateur peut faire que la mire peut s'afficher alors que le certificat n'est plus reconnu.

Questions propres à l'interface de configuration du module

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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>/genconfig/`

ou : `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.eol.bak` est sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

S'il existe une différence entre `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'a pas encore été appliquée.

Comment modifier la valeur d'une variable verrouillée

Il est vivement recommandé de ne pas éditer manuellement le fichier `config.eol` pour éviter les erreurs de frappe ou de type de données.



Exporter puis importer le fichier de configuration courant permet de passer outre le verrouillage des variables.



Cette astuce demande une bonne maîtrise des implications que peut avoir le changement d'une valeur verrouillée. Et une valeur n'est jamais verrouillée sans raison.

Par exemple, le changement de l'identifiant de l'établissement ne se répercute pas sur l'annuaire dont le schéma n'est construit qu'une fois au moment de l'instance du serveur.



Pour modifier la valeur verrouillée `Identifiant de l'établissement` :

- ouvrir l'interface de configuration du module ;
- importer le fichier de configuration courant : `Fichier` → `Importer une Configuration` → `/etc/eole/config.eol` ;
- modifier la valeur de l'identifiant de l'établissement ;
- enregistrer la configuration : `Fichier` → `Enregistrer la configuration` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- procéder à une reconfiguration du serveur à l'aide de la commande `reconfigure`.

Erreurs de timeout ou erreur 504 avec Nginx

L'utilisation de la nouvelle interface de configuration du module sur une petite configuration peut poser problème.

Cela se traduit par des erreurs de timeout[p.475] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Gunicorn[p.461].



La valeur de timeout peut être changée à la ligne `timeout = '120'` dans le fichier de configuration de eoleflask : `/etc/eole/flask/eoleflask.conf`. Celui-ci n'est pas templatisé et n'est donc pas écrasé en cas de reconfiguration du serveur.

Le changement de valeur doit être suivi d'une relance du service eoleflask :

```
# CreoleService eoleflask restart
```

Interface de configuration en mode console

Impossible de trouver le mode console de l'interface de configuration du module.



Le mode console a été supprimé par contre il est possible :

- d'accéder à distance à l'interface de configuration du module via un navigateur web ;
- d'utiliser la commande CreoleSet pour configurer une variable en ligne de commande.

Consultation des mots de passe dans l'interface de configuration

Sur les versions d'EOLE supérieures à 2.6.0, les valeurs des variables de type *password* sont masquées lorsque le champ n'est pas en mode édition, donc inaccessibles lorsque le champ est verrouillé.



La consultation d'un mot de passe non éditable (stocké dans une variable verrouillée par exemple) est possible en passant en mode Debug. Le mot de passe pouvant malgré tout apparaître tronqué, sa valeur intégrale est accessible dans l'info-bulle qui s'affiche lors du survol du champ.

2. Questions fréquentes propres au module Zéphir

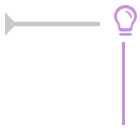
Le serveur Zéphir 2.6.0 ne gère plus les serveurs EOLE 2.3, que faire ?

Le serveur Zéphir 2.6.0 ne gère plus les serveurs EOLE 2.3, si la base est importée dans la nouvelle version de Zéphir, tous les serveurs 2.3 seront supprimés.

Les versions 2.5 du module Zéphir ne prennent pas en charge les modules 2.6. D'une manière générale

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



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 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)
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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. 206].

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.470] 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Glossaire

Active Directory *= AD*	Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Source Wikipédia : https://fr.wikipedia.org/wiki/Active_Directory
adresse MAC *= Media Access Control*	Une adresse MAC, parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés (tablette tactile, smartphone,consoles de jeux). Une adresse MAC est généralement représentée sous la forme hexadécimale en séparant les octets par un double point. Par exemple 5E:FF:56:A2:AF:15. Source Wikipédia : http://fr.wikipedia.org/wiki/Adresse MAC
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.
Agrégation de liens Ethernet *= Bonding*	L'agrégation de liens (niveau 2) est une technique utilisée dans les réseaux informatiques, permettant le regroupement de plusieurs ports réseau et de les utiliser comme s'il s'agissait d'un seul. Le but est d'accroître le débit au-delà des limites d'un seul lien, et éventuellement de faire en sorte que les autres ports prennent le relais si un lien tombe en panne (redondance). Source Wikipedia : https://fr.wikipedia.org/wiki/Agrégation_de_liens [https://fr.wikipedia.org/wiki/Agr%C3%A9gation_de_liens]
AMD64	AMD64 est le nom d'une architecture processeur développée par la société AMD. Cette architecture est compatible avec le standard 32 bits x86 d'Intel.
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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.
APT *= Advanced Packaging Tool*	APT est un ensemble d'outils fondamentaux au cœur de Debian. Il permet : • d'installer des applications ; • de supprimer des applications ; • de garder les applications à jour ; • et encore bien d'autres choses... APT, qui essentiellement résout les problèmes de dépendances et récupère les paquets désirés, fonctionne avec `dpkg`, un autre outil qui réalise l'installation réelle ou la suppression des paquets (applications). APT est très puissant, et est essentiellement utilisé en ligne de commande.
Autorité de Certification *= CA : Certification Authority*	AC est l'acronyme de Autorité de Certification. Une autorité de certification est une société ou un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.
Bareos	Bareos est un ensemble de programmes qui permet de gérer les sauvegardes, les restaurations ou la vérifications de données d'un ordinateur sur un réseau hétérogène. En termes techniques, il s'agit d'un programme de sauvegarde client/serveur. Il est relativement facile d'utilisation et efficace. Il offre de nombreuses fonctions avancées de gestion de stockage qui facilitent la recherche et la restauration de fichiers perdus ou endommagés.
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	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Berkeley Internet Name Domain	http://www.isc.org/downloads/bind/
CERT-FR *= Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*	Le CERT-FR (anciennement CERTA) est une des composantes curatives complémentaires des actions préventives assurées par l'ANSSI. En tant que CERT (Computer Emergency Response Team) national, il est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il assure une permanence de ses activités 24h/24, 7j/7.S Ses principales missions peuvent se décliner ainsi : • détecter les vulnérabilités des systèmes, au travers notamment d'une veille technologique ; • piloter la résolution des incidents, si besoin avec le réseau mondial des CERT ; • aider à la mise en place de moyens permettant de se prémunir contre de futurs incidents ; • organiser la mise en place d'un réseau de confiance. Source : https://www.cert.ssi.gouv.fr/
CETIAD *= Centre d'Études et de Traitements Informatiques de l'Académie de Dijon*	DSI de l'académie de Dijon en charge l'informatisation des services académiques et des établissements des 1er et 2nd degré nommée ainsi jusqu'au déménagement du service de la rue Berbisey à la rue du Général Delaborde dans les nouveaux locaux du rectorat de l'académie de Dijon en novembre 2012.
CN *= Common Name*	Valeur permettant d'identifier le serveur dans le certificat.
Commutateur réseau *= switch*	Un commutateur réseau (en anglais switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage. Dans les réseaux locaux (LAN), il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub) mais peut être configuré pour un accès direct à Internet, ce qui n'est pas possible pour un hub. Il existe aussi des commutateurs pour tous les types de réseau en mode point à point comme pour les réseaux ATM, relais de trames, etc. Source : http://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau
Consistent Network Device Naming	Le nommage des interfaces réseau en ethX n'était pas assez fiable. Si on insérait une carte réseau supplémentaire dans le système, la nouvelle carte réseau pouvait remplacer eth0 et la déplacer en eth1. Le nom des interfaces est fonction de leur attachement au système et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	non plus simplement de l'ordre matériel. Consistent Network Device Naming est une convention pour le nommage des cartes réseau sous GNU / Linux. Cette convention a été implémentée au travers du module kernel biosdevname par la société Dell. Le schéma de nommage de biosdevname respecte les conventions suivantes : • em[1−N] pour les cartes physiques embarquées, le numéro correspond à l'emplacement interne de la carte sur la carte mère (numéro renvoyé par la commande `lspci`) ; • p<numeroEmplacement>p<numeroEmplacementPhysique> pour les cartes PCI, le numéro de l'emplacement physique commençant à 1 ; • un suffixe _vf est ajouté au matériel NPAR et SR-IOV, le numéro dépend du nombre de partitions ou des fonctions de virtualisation utilisées et sur quel port ; • d'autres conventions comme les suffixes vlan et alias sont inchangées et reste applicables. Source : http://en.wikipedia.org/wiki/Consistent_Network_Device_Naming systemd/udev utilisent leur propre schéma de nommage similaire à biosdevname. Les principales différences sont supportées nativement par udev : • carte embarquée et numéro interne de l'emplacement de la carte (numéro renvoyé par la commande `lspci`) (exemple: eno1) ; • carte PCI Express et numéro interne de l'emplacement de la carte (exemple: ens1) ; • carte et localisation du connecteur au niveau du matériel (exemple: enp2s0) ; • carte avec l'adresse MAC (exemple: enx78e7d1ea46da) ; • pour les cartes nommées nativement dans le kernel (exemple: eth0).
Conteneur	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
Corosync Cluster Engine *= Corosync*	Corosync Cluster Engine est un moteur libre de cluster. C'est un système de communication avec des fonctionnalités supplémentaires pour la mise en œuvre de la haute disponibilité dans les applications.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Le projet fournit quatre fonctionnalités principales : • un groupe restreint de processus avec une garantie de synchronisation virtuelle afin de créer des machines à états répliquées ; • un simple gestionnaire de disponibilité qui redémarre les processus d'application lorsqu'ils ont échoués ; • une configuration et des statistiques stockées en base de données dans la mémoire vive permet de définir, de récupérer et de recevoir des notifications concernant les changements d'état ; • un système de notification qui se déclenche lorsque un quorum est atteint ou perdu. Sources : https://fr.wikipedia.org/wiki/Corosync_Cluster_Engine et http://clusterlabs.org/
Creole *= Création EOLE*	Creole gère la personnalisation des options de configuration des modules, le redémarrage des services, l'installation de paquets additionnels, la mise à jour du système. Il a été conçu pour être facilement personnalisable pour l'utilisateur final. Un ensemble d'outils est proposé pour modifier ou étendre les fonctionnalités offerte par EOLE.
creoled	creoled est un service permettant d'effectuer des requêtes sur la configuration Creole depuis la boucle locale sur le maître et dans les conteneurs.
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.
DHCP *= Dynamic Host Configuration Protocol*	Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.
Dictionnaire Creole	Fichier, au format XML, décrivant l'ensemble de variables, de fichiers, de services et de paquets personnalisés en vue de configurer un serveur.
Distribution	Une distribution GNU/Linux est un ensemble cohérent de logiciels rassemblant un système d'exploitation composé d'un noyau Linux et d'applications, la plupart étant des logiciels libres.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

DMZ *= Demilitarized Zone*	En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local. Source Wikipédia : http://fr.wikipedia.org/wiki/Zone démilitarisée (informatique)
DN *= Distinguished Name*	Identifiant unique dans le cadre des annuaires LDAP.
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
DTD *= Document Type Definition*	La Définition de Type de Document, est un document permettant de décrire un modèle de document SGML ou XML. Le modèle est décrit comme une grammaire de classe de documents : grammaire parce qu'il décrit la position des termes les uns par rapport aux autres, classe parce qu'il forme une généralisation d'un domaine particulier, et document parce qu'on peut former avec un texte complet. Une DTD décrit les documents à deux niveaux : • la structure logique, que l'on peut assimiler à la syntaxe abstraite ; • la structure physique, que l'on peut assimiler à la syntaxe concrète. Source : http://fr.wikipedia.org/wiki/Document_Type_Definition
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
EAD *= EOLE ADmin*	L'EAD est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse `https://<adresse module>:4200`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	L'authentification peut être locale et/ou au travers d'EoleSSO (authentification unique). L'EAD est composé de deux parties : • un serveur de commandes (service ead-server), présent et actif sur tous les modules ; • une interface web (service ead-web), présent et actif sur tous les modules. Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, ...) ne disposent que de la version de base qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...). Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.
Envole	Envole est un Espace Numérique Personnel pour l'Éducation. Il propose une interface de type portail Web 2.0 qui permet l'interaction entre un utilisateur et son environnement numérique résultant de l'utilisation de services hétérogènes. Il centralise dans une seule interface l'ensemble des applications de l'utilisateur : mail, agenda, dossier personnel, B2I, blog, gestion de notes, gestion des absences, etc ... Envole est adapté pour mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Établissement (PIE) ou un Espace Numérique de Travail (ENT). http://envole.ac-dijon.fr/
eole-schedule	Sur les modules EOLE, les tâches planifiées (comme par exemple les mises à jour, les sauvegardes, la purge de certaines informations, l'exportation de l'annuaire, des bases de données et des quotas disque ou encore les mises à des listes noires pour le filtrage proxy) sont gérées par `eole-schedule`. Contrairement à l'utilisation de cron, `eole-schedule` permet de maîtriser les tâches planifiées même si la sauvegarde est activée. Sur un module instancié, la commande suivante permet d'obtenir la liste des tâches planifiées : `manage_schedule -l`.
Erlang	Erlang est un langage de programmation, supportant plusieurs paradigmes : concurrent, temps réel, distribué. Son cœur séquentiel est un langage fonctionnel à évaluation stricte, affectation unique, au typage dynamique fort. Sa couche concurrente est fondée sur le modèle d'acteur. Il possède des fonctionnalités de tolérance aux pannes et de mise à jour du code à chaud, permettant le développement d'applications à très haute disponibilité. Erlang est conçu pour s'exécuter sur une machine virtuelle spécifique appelée BEAM. Source Wikipédia :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	http://fr.wikipedia.org/wiki/Erlang_%28langage%29
Exim	Exim est un serveur de messagerie électronique (ou Mail Transfer Agent en anglais) utilisé sur de nombreux systèmes de type UNIX. Il est l'un des serveurs de messagerie électronique (MTA) les plus flexibles et robustes. Exim est hautement configurable : il possède des fonctionnalités manquantes dans les autres serveurs de courriel. http://www.exim.org/
Fichier DEB	Un fichier DEB est un package permettant d'installer une application sous les systèmes Linux Debian. La distribution Debian propose un outil de gestion de package permettant d'automatiser l'installation, la configuration et la mise à jour des logiciels installés par ce biais.
FOG *= Free OpenSource Ghost*	FOG est un logiciel libre de déploiement d'OS. FOG est installable facilement sur le module EoleBase versions 2.8 et supérieures. https://pcll.ac-dijon.fr/eole/installation-de-fog-sur-eolebase-2-8/ https://fogproject.org/
FTP *= File Transfert Protocol*	File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS. FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande). FTP, qui appartient à la couche application du modèle OSI et du modèle ARPA, utilise une connexion TCP. Par convention, deux ports sont attribués (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990. Ce protocole peut fonctionner avec IPv4 et IPv6. (Source : http://fr.wikipedia.org/wiki/File_Transfer_Protocol)
Gaspacho	Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil. Pour le moment il n'existe que la version GNU/Linux du client

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Gaspacho.
GNU GRUB *= GRand Unified Bootloader*	GNU GRUB est un programme d'amorçage de micro-ordinateur. Il s'exécute à la mise sous tension de l'ordinateur, après les séquences de contrôle interne et avant le système d'exploitation proprement dit, puisque son rôle est justement d'en organiser le chargement. Lorsque le micro-ordinateur héberge plusieurs systèmes (on parle alors de multi-amorçage), il permet à l'utilisateur de choisir quel système démarrer. Source : http://fr.wikipedia.org/wiki/GRand_Unified_Bootloader
GPG *= GnuPG*	GPG est l'implémentation GNU du standard OpenPGP. OpenPGP est un format pour l'échange sécurisé de données. http://fr.wikipedia.org/wiki/GNU_Privacy_Guard
Gunicorn *= Green Unicorn (Licorne Verte)*	Gunicorn est un serveur Web HTTP WSGI écrit en Python et disponible pour Unix. Son modèle d'exécution est basé sur des sous-processus créés à l'avance, adapté du projet Ruby Unicorn. Le serveur Gunicorn est compatible avec un large nombre de frameworks Web, repose sur une implémentation simple, légère en ressources et relativement rapide. Source Wikipédia : http://fr.wikipedia.org/wiki/Gunicorn_(HTTP_server)
Haute Disponibilité *= High Availability ou HA*	La haute disponibilité c'est garantir la disponibilité et le bon fonctionnement d'un service ou d'une architecture informatique. Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité : • la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle. Est alors créé un cluster de haute-disponibilité (par opposition à un cluster de calcul) : une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités ; • la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur. ITIL contient de nombreux processus de ce type. Source Wikipédia : http://fr.wikipedia.org/wiki/Haute disponibilité
HTTP *= HyperText Transfer Protocol - protocole de transfert hypertexte*	HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (le S signifiant sécurisé) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS. HTTP est un protocole de la couche application. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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.
IMAP *= Internet Message Access Protocol*	IMAP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Mais contrairement au protocole POP, il permet de laisser les messages sur le serveur, ce qui présente un gros avantage pour consulter sa messagerie depuis plusieurs postes équipés de clients lourds.
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`.
InterBase	InterBase est un moteur de base de données. Il a été choisi par le ministère de l'Éducation nationale pour supporter les bases de données utilisées par les logiciels nationaux (comme GFC et SELENE, par exemple). Source Wikipédia : http://fr.wikipedia.org/wiki/InterBase
iptables	iptables est un logiciel libre grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu dans l'espace noyau composé par des modules Netfilter. Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	d'adresses locales facilitent l'interconnexion de réseaux privés.
JSON *= JavaScript Object Notation*	JSON est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Il permet de représenter de l'information structurée comme le permet XML par exemple. Un document JSON a pour fonction de représenter de l'information accompagnée d'étiquettes permettant d'en interpréter les divers éléments, sans aucune restriction sur le nombre de celles-ci. Un document JSON ne comprend que deux types d'éléments structurels : • des ensembles de paires nom / valeur ; • des listes ordonnées de valeurs. Ces mêmes éléments représentent trois types de données : • des objets ; • des tableaux ; • des valeurs génériques de type tableau, objet, booléen, nombre, chaîne ou null. Source Wikipédia : http://fr.wikipedia.org/wiki/JavaScript_Object_Notation
Kerberos	Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Source Wikipédia : http://fr.wikipedia.org/wiki/Kerberos_(protocole)
Keycloak	Keycloak est un outil libre et moderne de gestion d'identité et des accès (IAM).
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.
LDM *= LTSP Display Manager*	LDM est le gestionnaire d'affichage spécialement écrit pour LTSP.
LemonLDAP *= LemonLDAP::NG*	LemonLDAP::NG est une infrastructure d'authentification unique distribuée (SSO – Single Sign On) avec gestion centralisée des droits. Il se présente sous la forme d'une suite logicielle libre reposant sur le serveur web Apache. Source : http://www.starxpert.fr/lemon-ldap/
Let's Encrypt *= LE*	Let's Encrypt est une autorité de certification qui fournit des certificats gratuits X.509 pour le protocole cryptographique TLS au moyen d'un processus automatisé destiné à se passer du processus complexe actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation des sites internet.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Source Wikipédia : https://fr.wikipedia.org/wiki/Let's_Encrypt
libvirt	libvirt est une bibliothèque, une API, un daemon et des outils en logiciel libre de gestion de la virtualisation. Elle est notamment utilisée par KVM, Xen, VMware ESX, QEMU et d'autres solutions de virtualisation. Elle est notamment utilisée par la couche d'orchestration des hyperviseurs. Source : http://fr.wikipedia.org/wiki/Libvirt
Licence CeCILL	Acronyme pour CEa Cnrs Inria Logiciel Libre. C'est une licence libre de droit français compatible avec la licence GNU GPL.
Linux *= Kernel Linux*	Le noyau Linux est un noyau de système d'exploitation de type Unix. Le noyau Linux est un logiciel libre développé initialement par Linus Torvalds. Il a officiellement vu le jour en 1991. Formellement, « Linux » est le nom du seul noyau, mais dans les faits, on appelle souvent « Linux » l'ensemble du système d'exploitation, aussi appelé « GNU/Linux », voire l'ensemble d'une distribution Linux.
LTS *= Long Term Support*	Certaines versions d'Ubuntu sont estampillées LTS. Ces versions, publiées tous les deux ans au mois d'avril, sont soutenues pour une durée prolongée de 60 mois (5 ans). Le label LTS : • la récupération des paquets de Debian se fait de manière plus conservatrice, synchronisée depuis Debian testing plutôt que Debian unstable ; • la stabilisation de la distribution commence tôt dans le cycle de développement en limitant le nombre de nouveautés. L'équipe d'Ubuntu fait une sélection entre les paquets qui doivent être inclus dans une distribution maintenue sur une durée d'au plus 5 ans et ceux qui pourront être optionnellement installés par les utilisateurs ; • les changements structurels majeurs sont le plus possible évités, comme le changement des applications incluses par défaut dans la distribution, la transition vers d'autres bibliothèques ou les changements des couches basses du système. Une version LTS est : • tournée vers les entreprises : ces versions sont pensées pour le déploiement dans des parcs de serveurs et de postes de travail dont la durée de vie est longue et où les changements sont peu fréquents ; • compatible avec les nouveaux matériels : des révisions sont publiées à intervalles réguliers (une point release) pour ajouter la prise en charge de nouveaux matériels pour serveurs et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	postes de travail ; • davantage testée : la phase de développement alpha est réduite, afin d'étendre davantage la période de stabilisation bêta pour récolter le plus de retours d'expérience et de rapports de bogues et pour stabiliser l'ensemble de la distribution. Clairement, une version LTS n'est pas : • une version incluant de nombreuses nouveautés : l'effort est surtout tourné vers la stabilisation et le renforcement des fonctionnalités existantes. Si des exceptions sont accordées à certains projets, elles sont documentées et leur intégration dans une version LTS doit être complétée pour la version bêta 1 du cycle de développement ; • une version d'avant-garde : plutôt que d'importer les paquets de Debian depuis sa version unstable, ceux-ci sont tirés depuis la version testing de Debian. Même si certaines nouveautés ne sont pas incluses dans ces paquets, il y a plus de bénéfices à importer des paquets testés qui introduisent moins de bogues et moins de régressions.
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.
LXC *= Linux Containers*	LXC, contraction de l'anglais Linux Containers, est un système de virtualisation au niveau système d'exploitation utilisé pour faire fonctionner de multiples environnements Linux isolés les uns des autres sur un seul et même système hôte. Le conteneur LXC n'est pas une machine virtuelle mais uniquement un environnement virtualisé qui dispose de ses propres processus et de son propre réseau (isolés du système physique hôte).
man in the middle *= homme du milieu*	L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. Source Wikipédia : http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Source : https://fr.wikipedia.org/wiki/MD5
MEEM *= Ministère de l'Environnement, de l'Énergie et de la Mer*	Le ministère de l'Environnement, de l'Énergie et de la Mer est l'administration française chargée de préparer et mettre en œuvre la politique du Gouvernement dans les domaines du développement durable, de l'environnement et des technologies vertes, de la transition énergétique et de l'énergie, du climat, de la prévention des risques naturels et technologiques, de la sécurité industrielle, des transports et de leurs infrastructures, de l'équipement et de la mer. Il est dirigé par le ministre de l'Environnement, de l'Énergie et de la Mer, membre du gouvernement français. Né de la fusion, en 2007, du Ministère de l'Environnement et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer il a depuis changé plusieurs fois de nom et de compétences : • Ministère de l'Écologie, du Développement et de l'Aménagement durables (2007-2010) Le ministère de l'Écologie, du Développement et de l'Aménagement durables (MEDAD) naît ainsi de la fusion du Ministère de l'Écologie et du Développement durable et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer. Il intègre également l'énergie, qui relevait alors du ministère de l'économie. • Ministère de l'Écologie, du Développement durable, des Transports et du Logement (2010-2012) Le ministère devient le Ministère de l'Écologie, du Développement durable, des Transports et du Logement (MEDDTL) et perd au passage ses compétences sur l'énergie, exception faite des énergies renouvelables. • Ministère de l'Écologie, du Développement durable et de l'énergie (2012-2016) Le Ministère de l'Écologie, du Développement durable et de l'énergie (MEDDE) assemble des fonctions historiquement séparées dans différents ministères : l'écologie (ministère de l'écologie et du Développement durable) et l'énergie (auparavant rattachée au ministère de l'industrie). • Ministère de l'Environnement, de l'Énergie et de la Mer (depuis 2016) Le ministère devient Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM) et est chargée des relations internationales sur le climat. Source Wikipédia : http://fr.wikipedia.org/wiki/Minist%C3%A8re_de_l'Environnement,_de_l http://fr.wikipedia.org/wiki/Liste_des_ministres_fran%C3%A7ais_des_T
MTU	Le MTU définit la taille maximum d'un paquet (en octets) pouvant être

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Maximum Transmission Unit	transmis sur le réseau sans fragmentation. Source Wikipédia : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit
MySQL	MySQL est un système de gestion de base de données (SGBD). Il fait partie des logiciels de gestion de base de données les plus utilisés au monde. C'est un serveur de bases de données relationnelles SQL développé dans un souci de performances élevées en lecture, il est davantage orienté vers le service de données déjà en place plutôt que vers celui de mises à jour fréquentes et fortement sécurisées. Il est multi-thread et multi-utilisateur.
NBD *= Network Block Devices*	Network Block Devices (NBD) est un composant du kernel permettant de monter un fichier distant via ethernet, en TCP, comme s'il s'agissait d'un périphérique de bloc local.
NFS *= Network File System*	NFS est est un protocole développé par Sun Microsystems qui permet à un ordinateur d'accéder à des fichiers via un réseau. Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Des implémentations existent pour Macintosh et Microsoft Windows. NFS est compatible avec IPv6 sur la plupart des systèmes.
Nginx *= Engine-x*	Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions. Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.
NTLM *= NT Lan Manager*	NTLM est un protocole d'identification utilisé dans diverses implémentations des protocoles réseau Microsoft. Il est aussi utilisé partout dans les systèmes de Microsoft comme un mécanisme d'authentification unique SSO.
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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	• 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.
OpenNebula	OpenNebula est un projet libre et européen qui fournit un ensemble de fonctionnalités permettant de gérer un nuage informatique. OpenNebula organise le fonctionnement d'un ensemble de serveurs physiques, fournissant des ressources à des machines virtuelles. Il orchestre et gère le cycle de vie de toutes ces machines virtuelles. http://opennebula.org/
OpenSSL	OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, openssl. Source : https://fr.wikipedia.org/wiki/OpenSSL
OpenVZ	OpenVZ est une technique de virtualisation de niveau système d'exploitation basée sur le noyau Linux. Cette technique de virtualisation de niveau système d'exploitation est souvent appelée conteneurisation et les instances sont appelées conteneur. OpenVZ permet à un serveur physique d'exécuter de multiples instances de systèmes d'exploitation isolés, qualifiées de serveurs privés virtuels (VPS) ou environnements virtuels (VE). Source Wikipédia : https://fr.wikipedia.org/wiki/OpenVZ
OTP	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= One-time password	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
Patch	Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à l'instance ou à chaque reconfigure. Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch. La procédure pour réaliser des patchs est expliquée dans la rubrique **Personnalisation du serveur à l'aide de Creole** dans les documentations complètes ou dans la documentation partielle dédiée nommée **PersonnalisationEOLEAvecCreole**.
PDC *= Primary Domain Controller*	Un contrôleur principal de domaine appartient à une technologie d'annuaire et de réseau pour Windows NT. C'est un serveur qui dans un domaine (un groupe d'ordinateur appelé aussi «forêt») Windows gère et contrôle l'accès à une variété de ressources. Le contrôleur principal de domaine a un compte d'administration générale qui a le contrôle total des ressources du domaine. Un domaine a au moins un contrôleur de domaine principal et a souvent un ou plusieurs contrôleurs de domaine de sauvegarde (BDC). Si un contrôleur de domaine principal tombe en panne, l'un des contrôleurs secondaires peuvent ensuite être promu pour prendre sa place.
PID *= Process IDentifier*	L'identifiant de processus ou PID est un code unique attribué sur les systèmes Unix ou Windows à tout processus lors de son démarrage. Il permet ainsi d'identifier le processus dans la plupart des commandes s'appliquant sur un processus donné (comme kill). Wikipédia : https://fr.wikipedia.org/wiki/Identifiant_de_processus
Podman	Podman est un logiciel libre permettant de lancer des applications dans des conteneurs logiciels. Il s'agit d'une alternative à Docker, qui permet de lancer les commandes sans les permissions root. https://fr.wikipedia.org/wiki/Podman
POP *= Post Office Protocol*	POP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. C'est cette dernière qui a cours actuellement.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

PostgreSQL	PostgreSQL est un système de gestion de base de données relationnelle et objet (SGBDRO). Il est fondé sur une communauté mondiale de développeurs et d'entreprises.
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.
PPPoE *= Point-to-Point Protocol over Ethernet*	PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP et du contrôle de la connexion (débit, etc.), sur un réseau 802.3. Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers, bien qu'une connexion utilisant un pont Ethernet-Ethernet soit souvent plus stable et plus performante. Il pose également des problèmes de MTU.
Projet LTSP *= Linux Terminal Server Project*	Linux Terminal Server Project (LTSP) est un ensemble de programmes permettant à plusieurs personnes d'utiliser le même ordinateur. Cela est réalisé par la mise en place d'un réseau informatique composé d'un serveur sous GNU/Linux et de clients légers. http://www.ltsp.org/
Pronote	Pronote est un logiciel privateur de gestion de vie scolaire créé en 1999. C'est au départ un client lourd, mais il existe, depuis 2003, une extension permettant d'utiliser une version Web.
PXE *= Pre-boot eXecution Environment*	L'amorçage PXE permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur. L'amorce par PXE s'effectue en plusieurs étapes : • recherche d'une adresse IP sur un serveur DHCP/BOOTP et recherche du fichier à amorcer ; • téléchargement du fichier à amorcer depuis un serveur Trivial FTP ; • exécution du fichier à amorcer.
RADIUS *= Remote Authentication Dial-In User Service*	RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification. Source : http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Servic
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,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	notamment sa localisation, son code. Caractéristiques techniques : • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
Redondance *= Redondance des matériels*	La redondance consiste à disposer plusieurs exemplaires d'un même équipement ou d'un même processus ou de tout autre élément participant à une solution électronique, mécanique ou industrielle. Selon les circonstances elle est utile : • pour augmenter la capacité totale ou les performances d'un système ; • pour réduire le risque de panne ; • pour combiner ces deux effets.
RELP *= Reliable Event Logging Protocol*	Reliable Event Logging Protocol ou RELP est un protocole définissant un service de journaux d'événements d'un système informatique. Il est supporté entre autres par Rsyslog.
Réseau virtuel Privé *= RVP ou VPN (Virtual Private Network) en anglais*	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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
SaltStack *= Salt*	Salt ou SaltStack est un logiciel de gestion de configuration écrit en Python, fonctionnant sur le principe client-serveur. SaltStack a pour but de rendre la gestion de configuration simple mais flexible. Il s'agit d'une alternative à Puppet, Ansible et Chef. On utilise les langages informatiques YAML, Jinja2 et Python pour configurer SaltStack. Source Wikipédia : https://fr.wikipedia.org/wiki/Salt_(logiciel) Le vocabulaire SaltStack : • Pillar : Dictionnaire des variables ; • States : Ordres à exécuter ; • Formula : Ensemble de States ; • Grains : Informations que retournent les minions au master-salt. La machine cliente SaltStack est appelé « minion », le serveur est appelé « master ».
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.
SAN *= Storage Area Network*	Un SAN, un réseau de stockage est un réseau spécialisé permettant de mutualiser des ressources de stockage. Un réseau de stockage se différencie des autres systèmes de stockage tels que le NAS (Network attached storage) par un accès bas niveau aux disques. Pour simplifier, le trafic sur un SAN est très similaire aux principes utilisés pour l'utilisation des disques internes (ATA, SCSI). C'est une mutualisation des ressources de stockage. Source Wikipédia : https://fr.wikipedia.org/wiki/R%C3%A9seau_de_stockage_SAN
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.
SNMP	SNMP est un protocole de communication qui permet aux

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Simple Network Management Protocol	administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance. https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol
Socle Interministériel de Logiciel Libre *= SILL*	Le secrétariat général pour la modernisation de l'action publique (SGMAP) relève du Premier ministre. L'un des services du SGMAP, la Direction Interministérielle des Systèmes d'Information et de Communication (DISIC), coordonne les administrations d'État en matière de systèmes d'information. L'instance DISIC en charge des logiciels libres préconise une sélection de logiciels, sous la forme d'un socle interministériel de logiciels libres (SILL). Le SILL propose des logiciels libres répondant aux besoins des administrations françaises. Il est mis à disposition sans garantie de l'État. Il peut être utilisé librement et gratuitement par tous, à titre public, professionnel ou privé. Il peut être copié et diffusé sans restriction. http://references.modernisation.gouv.fr/socle-logiciels-libres
Squid	Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.
SSH *= Secure Shell*	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
StartTLS	Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas, par exemple des protocoles de mails IMAP et SMTP ou LDAP.
strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/
SubjectAltName	OpenSSL respecte la norme X. 509v3 qui permet d'étendre la demande de certificat à l'usage qui en sera fait du dit certificat.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Subject Alternative Name, nom alternatif du sujet du certificat, SAN	Plusieurs extensions sont disponibles dont l'extension Subject Alternative Name. Cette extension permet d'inclure diverses valeurs littérales dans le fichier de configuration : • un email (une adresse de courrier électronique) ; • un URI (un indicateur de ressource uniforme) ; • un DNS (un nom de domaine DNS) ; • un RID (un ID enregistré: OBJECT IDENTIFIER) ; • une adresse IP ; • un dirName (un nom distinctif) ; • ou un otherName (un autre nom distinctif).
sudo *= substitute user do*	La commande sudo permet à un administrateur système d'accorder à certains utilisateurs (ou groupes d'utilisateurs) la possibilité de lancer une commande en tant qu'administrateur, ou comme autre utilisateur, tout en conservant une trace des commandes saisies et des arguments. Source : https://fr.wikipedia.org/wiki/Sudo
Sunstone	Sunstone est une interface graphique permettant de gérer OpenNebula. C'est une application Web qui permet de gérer et d'administrer les machines virtuelles et tout ce qui s'y rapporte. Depuis la version 2.7.2, l'accès à l'interface Sunstone s'effectue en https via un navigateur web : `https://<adresseServeur>`
systemd *= system daemon*	systemd est un système d'initialisation et un daemon qui a été spécifiquement conçu pour le noyau Linux comme alternative à System V. Il a pour but d'offrir un meilleur cadre pour la gestion des dépendances entre services, de permettre le chargement en parallèle des services au démarrage, et de réduire les appels aux scripts shell. Le projet a été lancé par Lennart Poettering en 2010 et publié sous licence GNU LGPL version 2.1. https://fr.wikipedia.org/wiki/Systemd
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.
TCP Wrapper *= tcpd*	TCP Wrapper est une technique, propre à Unix, permettant de contrôler les accès à un service (ou démon) suivant la source. Il se configure grâce au deux fichiers /etc/hosts.allow et /etc/hosts.deny.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Tous les démons ne supportent pas la technique TCP Wrapper.
Template *= Modèle Creole*	Un template est un fichier contenant des variables Creole, qui sera instancié pour générer un fichier cible (typiquement un fichier de configuration serveur).
timeout	Le timeout est la durée de validité d'une donnée avant son expiration.
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.
udev	udev est un gestionnaire de périphériques remplaçant devfs dans le noyau Linux depuis la version 2.6. Sa fonction principale est de gérer les périphériques dans le répertoire /dev. udev s'exécute en mode utilisateur et écoute le socket netlink2 pour communiquer avec le noyau. Source : https://fr.wikipedia.org/wiki/Udev
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
Unicode	Unicode est un standard informatique qui permet des échanges de textes dans différentes langues, à un niveau mondial. Il est développé par le Consortium Unicode, qui vise à permettre le codage de texte écrit en donnant à tout caractère de n'importe quel système d'écriture un nom et un identifiant numérique, et ce de manière unifiée, quelle que soit la plate-forme informatique ou le logiciel. Source Wikipédia : http://fr.wikipedia.org/wiki/Unicode

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Unité organisationnelle *= OU*	Une Unité organisationnelle (Organizational Unit ; OU ; UO) est un objet conteneur, de la norme ldap, qui est utilisé pour hiérarchiser les annuaires.
Upstart	Sous Unix, Upstart est un remplaçant du daemon init qui se base sur les événements. Il a été écrit par Scott James Remnant, un employé de Canonical Ltd. Upstart fonctionne de manière asynchrone. De la même manière qu'il gère le lancement des tâches et daemons au démarrage et leur arrêt à l'arrêt de la machine, il les supervise pendant que le système tourne. Ubuntu remplace Upstart par systemd à partir de la version 15.04 Vivid Vervet. https://fr.wikipedia.org/wiki/Upstart
URI *= Uniform Resource Identifier*	L'URI est une courte chaîne de caractères identifiant une ressource sur un réseau.
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.
VLAN *= Réseau local virtuel*	Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
VNC *= Virtual Network Computing*	VNC est un système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant. Il permet au logiciel client VNC de transmettre les information de saisie du clavier et de la souris à l'ordinateur distant, possédant un logiciel serveur VNC à travers un réseau informatique. Il utilise le protocole RFB pour les communications.
WPAD *= Web Proxy Autodiscovery Protocol*	WPAD définit la façon selon laquelle un navigateur web se connecte à Internet. Ce protocole permet au navigateur d'utiliser automatiquement le proxy approprié à l'URL demandée. WPAD laisse le navigateur découvrir l'emplacement du fichier PAC grâce aux services DHCP et DNS. Un fichier PAC est un fichier texte en JavaScript, qui contient entre autres la fonction FindProxyForURL(url, host). Cette fonction possède deux arguments associés : • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Xen	Xen est un logiciel libre de virtualisation, plus précisément un hyperviseur de machine virtuelle.
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)