Installation et mise en œuvre du module Seth

EOLE 2.6.2



création : Juin 2017 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 : Juin 2017

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

Chapitre 3 - Fonctionnement du module Seth 32
Chapitre 4 - Mise en œuvre du module 36
Chapitre 5 - Installation du module 38
1. Pré-requis 38
2. Médias d'installation 39
3. Déroulement de l'installation 43
4. Partitionnement personnalisé 45
5. Choisir le mode du module 61

Chapitre 6 - Configuration du module Seth 65
1. Configuration généralités 65
1.1. Configuration en mode autonome 66
1.1.1. Accès distant 68
1.1.2. La zone Menu 70
1.1.3. La zone Onglet 73
1.1.4. La zone Formulaire 74
1.1.5. La zone Validation 77
1.1.6. Enregistrer la configuration 77
1.1.7. Le mode Debug 78
1.1.8. FAQ 80
1.2. Configuration en mode Zéphir 82
2. Configuration en mode basique 91
2.1. Onglet Général 91
2.2. Onglet Services 94
2.3. Onglet Interface-0 95
2.4. Onglet Dhcp : Configuration du serveur DHCP 97
2.5. Onglet Directeur Bareos 99
2.6. Onglet Active Directory 99

2.7. Onglet Messagerie 101
3. Configuration en mode normal 102
3.1. Onglet Général 104
3.2. Onglet Services 107
3.3. Onglet Interface-0 108
3.4. Onglet Clamav : Configuration de l'anti-virus 111
3.5. Onglet Dhcp : Configuration du serveur DHCP 112
3.6. Onglet Onduleur 115
3.7. Onglet Directeur bareos 121
3.8. Onglet Stockage bareos 124
3.9. Onglet Nginx 124
3.10. Onglet Reverse proxy : Configuration du proxy inverse 125
3.11. Onglet Active Directory 129
3.12. Onglet Messagerie 134
4. Configuration en mode expert 135
4.1. Onglet Général 137
4.2. Onglet Services 141
4.3. Onglet Système 141
4.4. Onglet Sshd : Gestion SSH avancée 149
4.5. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système 150
4.6. Onglet Logs : Gestion des logs centralisés 150
4.7. Onglet Interface-0 152
4.8. Onglet Interface-n 157
4.9. Onglet Réseau avancé 162
4.10. Onglet Certificats ssl : gestion des certificats SSL 167
4.11. Onglet Dépôt tiers 173
4.12. Onglet Clamav : Configuration de l'anti-virus 175
4.13. Onglet Dhcp : Configuration du serveur DHCP 178
4.14. Onglet Tftp : Configuration d'un serveur PXE/TFTP 183
4.15. Onglet Onduleur 184
4.16. Onglet Saltstack 190
4.17. Onglet Ead-web : EAD et proxy inverse 190
4.18. Onglet Directeur bareos 191
4.19. Onglet Stockage bareos 194
4.20. Onglet Cups : Configuration du serveur d'impression 195
4.21. Onglet Nginx 197
4.22. Onglet Applications web nginx 198
4.23. Onglet Reverse proxy : Configuration du proxy inverse 198
4.24. Onglet Active Directory 203
4.25. Onglet Messagerie 214
4.26. Onglet Eoleflask 219
5. Configuration du module Seth en tant que contrôleur de domaine principal 220
6. Configuration du module Seth en tant que contrôleur de domaine additionnel 221
7. Configuration du module Seth en tant que serveur membre 223
8. Mise en place de l'agrégation de liens Ethernet (bonding) 224
9. Mise en place du protocole ISCSI sur un module EOLE 225
Chapitre 7 - Instanciation du module 228
1. Principes de l'instanciation 228
2. Lancement de l'instanciation 229
2.1. Les mots de passe 229
2.2. Création d'un deuxième administrateur 230
2.3. Activation automatique de la mise à jour hebdomadaire 231

2.4. Le redémarrage 231
3. Particularités de l'instance du module Seth 231
Chapitre 8 - Administration du module Seth 233
1. Administration généralités 233
1.1. Principes de l'administration 233
1.2. Découverte de GNU/Linux 234
1.2.1. Les Bases 234
1.2.2. Quelques Commandes 240
1.2.3. Les conteneurs 241
1.2.4. La gestion des onduleurs 241
1.2.5. Les manuels 242
1.2.6. L'éditeur de texte Vim 243
1.2.7. Les commandes à distance avec SSH 248
1.2.8. Quelques références 253
1.3. Reconfiguration 254
1.4. L'interface d'administration EAD 255
1.4.1. Principe général 256
1.4.2. Premier pas dans l'administration d'un serveur 260
1.4.3. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur 261
1.4.4. Ajout/suppression de serveurs 262
1.4.5. Surveillance de l'état du serveur 265
1.4.6. Authentification locale et SSO 268
1.4.7. Redémarrer, arrêter et reconfigurer 269
1.4.8. Mise à jour depuis l'EAD 270
1.4.9. Arrêt et redémarrage de services 270
1.4.10. Rôles et association de rôles 273
1.4.11. La console 294
1.4.12. Listing matériel 296
1.4.13. Bande passante 297
1.4.14. Résoudre des dysfonctionnements liés à l'EAD 297
1.5. L'interface d'administration EAD 3 301
1.5.1. Présentation 302
1.5.2. Installation 302
1.5.3. L'application web 302
1.5.4. Généralités sur les actions 306
1.5.5. Créer une nouvelle action 308
1.5.6. Type d'actions 310
1.5.7. Compléments techniques 313
1.6. L'interface d'administration semi-graphique 313
1.7. Les mises à jour 314
1.7.1. Les différents types de mises à jour 316
1.7.2. Les procédures de mise à jour 319
1.7.3. Ajout de dépôts supplémentaires 324
1.7.4. Désactivation temporaire des mises à jour 324
1.8. Installation manuelle de paquets 325
1.9. Les administrateurs locaux à droits restreints 326
1.10. Passage d'une version d'EOLE à une autre 327
1.11. Passage d'une version RC à une version stable 327
2. Joindre le domaine 327
3. Gestion de l'Active Directory Seth en ligne de commande 333
4. Gestion sommaire des GPO depuis le contrôleur de domaine 336

5. Le GPO « eole_script » 340
6. Gestion de l'Active Directory Seth avec les outils RSAT 342
7. Intégration du serveur Scribe dans le domaine AD de Seth : Eole-AD 353
8. Diagnose 361

Chapitre 9 - Personnalisation du module 362
1. Panorama des services 362
1.1. Services liés aux bases de données 362
1.1.1. eole-annuaire 362
1.1.2. eole-client-annuaire 363
1.1.3. eole-db 363
1.1.4. eole-interbase 364
1.1.5. eole-mysql 364
1.1.6. eole-postgresql 364
1.2. Services liés aux serveurs de fichiers 365
1.2.1. eole-ad-dc 365
1.2.2. eole-fichier-primaire 365
1.2.3. eole-fichier-membre 366
1.2.4. eole-cups 367
1.2.5. eole-proftpd 367
1.2.6. eole-dhcp 368
1.2.7. eole-nfs 368
1.3. Services liés au web 369
1.3.1. eole-web 369
1.3.2. eole-reverseproxy 370
1.3.3. eole-wpad 370
1.4. Services liés à la messagerie 371
1.4.1. eole-exim 371
1.4.2. eole-spamassassin 371
1.4.3. eole-courier 372
1.4.4. eole-sympa 372
1.5. Services liés au proxy et à l'authentification 373
1.5.1. eole-proxy 373
1.5.2. eole-radius 374
1.6. Services liés à la virtualisation 374
1.6.1. eole-libvirt 374
1.6.2. eole-one-frontend 375
1.6.3. eole-one-node 375
1.6.4. eole-one-singlenode 376
1.7. Autres services réseau 376
1.7.1. eole-antivirus 376
1.7.2. eole-apt-cacher-ng 377
1.7.3. eole-bareos 377
1.7.4. eole-dns 378
1.7.5. eole-dhcrelay 379
1.7.6. eole-ltsp-server 379
1.7.7. eole-nut 379
1.7.8. eole-open-iscsi 380
1.7.9. eole-pacemaker 380
1.7.10. eole-snmpd 381
1.7.11. eole-vpn 381

2. Personnalisation du serveur à l'aide de Creole 382
2.1. Répertoires utilisés par EOLE 382
2.2. Création de patch Creole 383
2.3. Les dictionnaires Creole 385
2.3.1. Ajouter un en-tête XML 385
2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu 386
2.3.3. Utiliser des familles, variables et des séparateurs 394
2.3.4. Comportement des variables 399
2.3.5. Mettre en place des contraintes 399
2.3.6. Afficher de l'aide 407
2.4. Le langage de template Creole 408
2.4.1. Déclarations du langage Creole 409
2.4.2. Fonctions prédéfinies 413
2.4.3. Utilisation avancée 417
2.4.4. Exemple 418
2.5. Le fichier de configuration Creole 419
2.6. Les scripts Creole 420
2.6.1. CreoleLint et CreoleCat 420
2.6.2. CreoleGet et CreoleSet 422
2.6.3. CreoleRun et CreoleService 425
2.6.4. CreoleLock 426
2.6.5. Indications pour la programmation 427
2.7. Ajout de script exécuté à l'instance ou au reconfigure 430
2.8. Ajout d'un test diagnose 431
2.9. Gestion des noyaux Linux 432
2.10. Gestion des tâches planifiées eole-schedule 433
2.11. Gestion du pare-feu eole-firewall 438
Chapitre 10 - Résolution de problèmes 440
1. Problèmes à la mise en œuvre 440
2. Problèmes à l'exploitation 441
3. Trouver de l'information 446
4. Demander de l'aide / Signaler un problème 449
5. Contribuer au projet EOLE 454
Chapitre 11 - Documentations techniques 456
1. Les dépôts EOLE 456
2. Gestion des journaux systèmes sur EOLE 458
3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation 459
3.1. Contexte juridique 459
3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation 460
Chapitre 12 - Compléments techniques 464
1. Les services utilisés sur le module Seth 464
1.1. eole-ad-dc 464
1.2. eole-dhcp 465
1.3. eole-exim 465
1.4. eole-nut 466
1.5. eole-reverseproxy 466
2. Ports utilisés sur le module Seth 467
3. Administration avancée du module Seth 468
4. Gestion des clients à l'aide de SaltStack 471

Chapitre 13 - Questions fréquentes 472
1. Questions fréquentes communes aux modules 472
2. Questions fréquentes propres au module Seth 492

Glossaire 493

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.496] :
- 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.522].

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.512] ;
  - **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.508] ;

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

- intégration d'Envole[p.500] 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.508] 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.508].

2012

- portage d'Eclair en 2.3 (juillet), repose sur ltsp-cluster, le serveur embarque le logiciel Gaspacho[p.502] ;
- 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.518] 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.518] 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.511].
- 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.508]).

  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.506] 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.508] (SSL interception) ;
  - mise à disposition des paquets `eole-fog` et `eole-lts-server` permettant respectivement la mise en œuvre de FOG[p.501] et d'un seveur LTSP[p.514] sur un module EOLE.

2023

- EOLE 2.9.0 LTS (février)
  - intégration du moteur de conteneur[p.497] Podman[p.513] 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.506].

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.

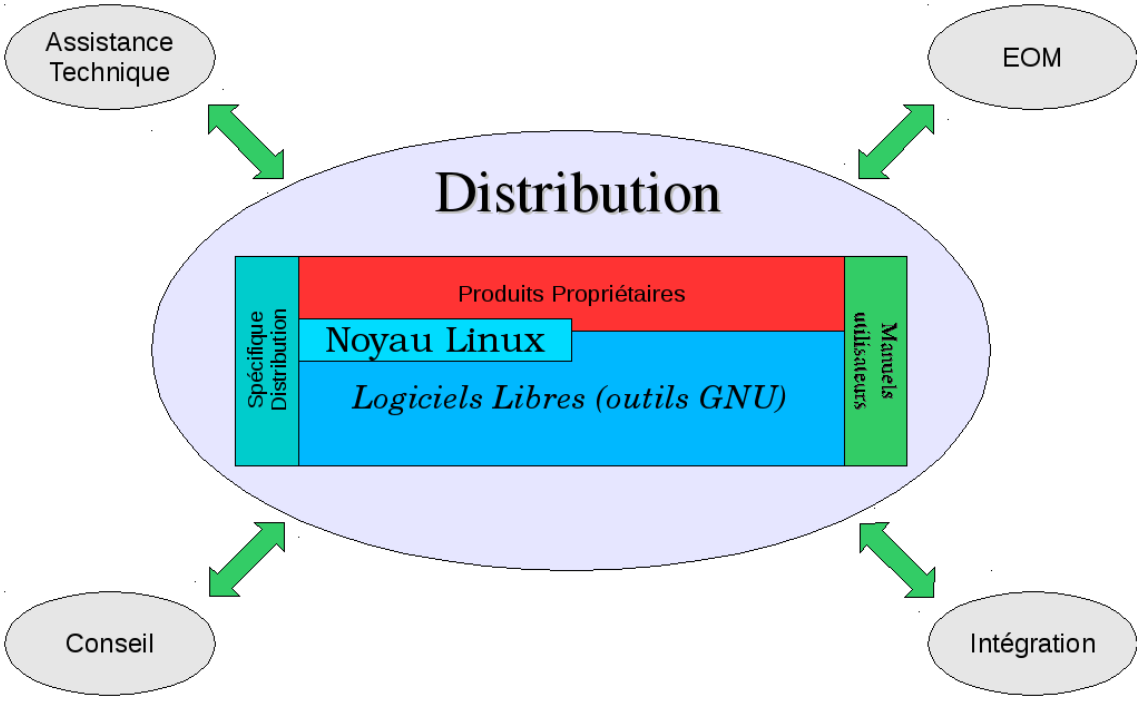
Une distribution GNU/Linux

Une distribution[p.499] GNU/Linux[p.506] 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



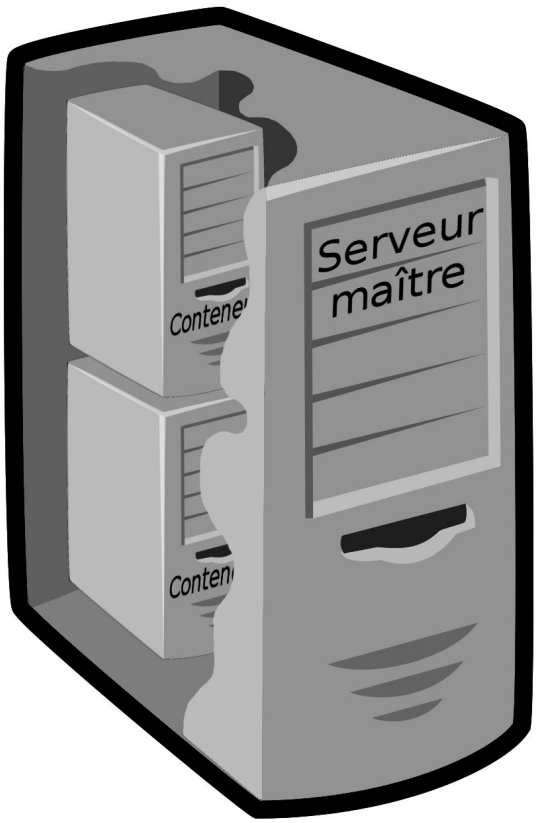
Logo officiel d'Ubuntu par Canonical Ltd

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

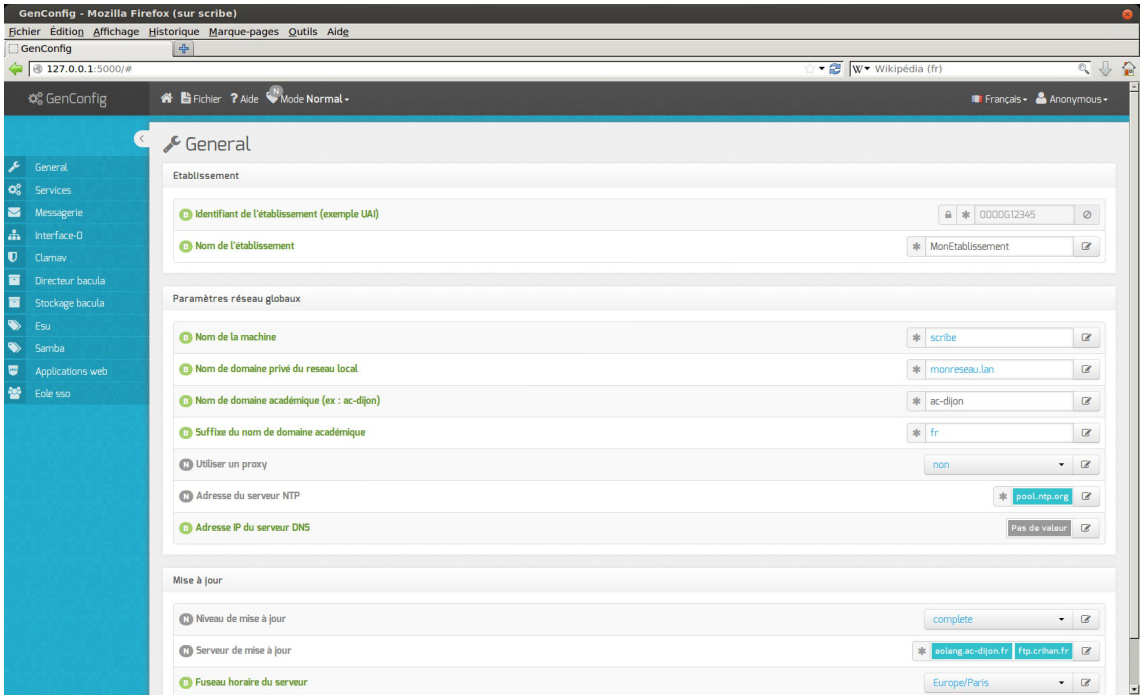
Ubuntu 16.04 LTS est disponible depuis le 21 avril 2016. Portant le label LTS[p.507], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2021. Le Pôle de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2021.

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

Module



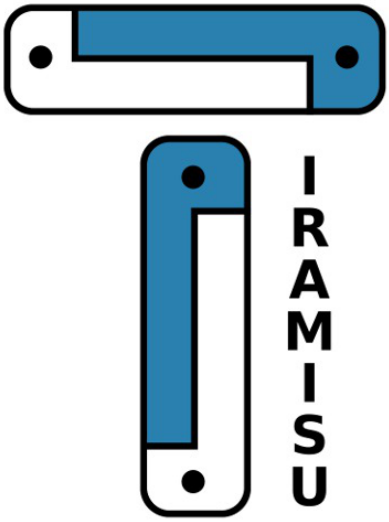
La version 2.6 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule 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.520].



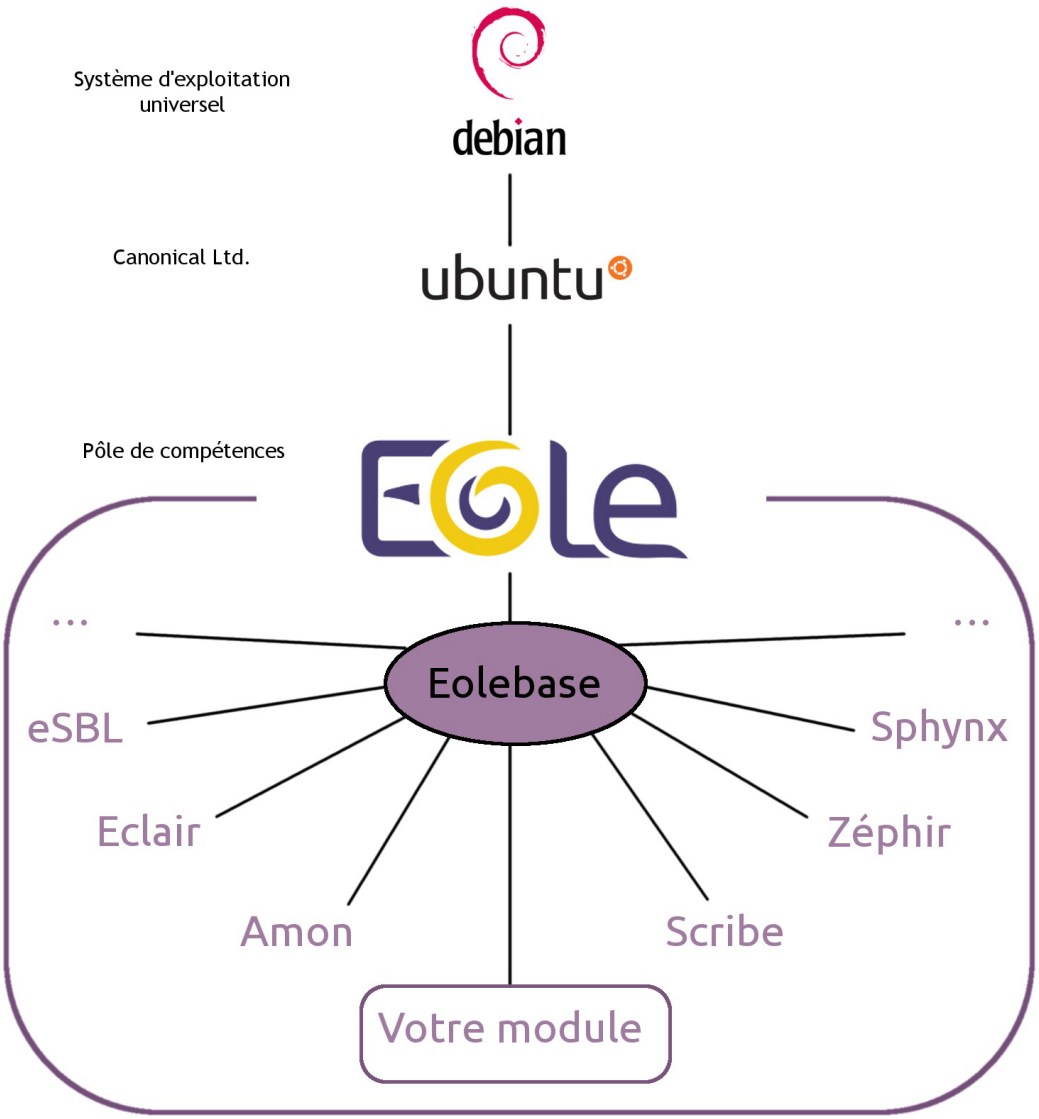
Logo du logiciel Tiramisu

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 Seth

Le module Seth permet de mettre en place un serveur Active Directory basé sur Samba4.

Il peut être configuré soit en tant que :

- contrôleur de domaine (DC) ;
- serveur membre d'un domaine existant.

Il offre les services habituels d'un serveur Active Directory : authentification Kerberos, gestion des machines clientes et des comptes utilisateurs, réplication des contrôleurs de domaine, partage de fichiers, partage d'imprimantes...

1. Qu'est ce que le module Seth ?

Le module Seth est l'intégration dans EOLE du mode Active Directory proposé par le logiciel Samba.

Principales fonctionnalités

Rôles :

- Contrôleur de domaine
- Serveur membre d'un domaine existant

Il offre les services habituels d'un serveur Active Directory :

- annuaire LDAP ;
- serveur DNS ;
- authentification Kerberos ;
- gestion des machines Windows par les GPO ;
- gestion des comptes utilisateurs ;
- gestion des ACLs et des quotas ;
- réplication des contrôleurs de domaine ;
- partage de fichiers et d'imprimantes.

2. À qui s'adresse ce module ?

Le module Seth s'adresse à toutes les structures ayant besoin des fonctionnalités d'un contrôleur de domaine Active Directory afin de gérer un parc de stations clientes GNU/Linux ou Windows :

- entreprises ;
- établissements scolaires ;
- collectivités territoriales;

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

- services départementaux de l'État ;
- services régionaux de l'État ;
- des ministères ;
- etc.

N'importe où dans le monde.

3. Les services Seth

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 Seth

- *Samba-4 AD* : DNS, annuaire, authentification Kerberos[p.505], serveur de fichiers et d'imprimantes, GPO[p.502], gestion des comptes utilisateurs, des droits et des accès, des quotas disque et des ACL[p.493] ;
- *dhcp3-server* : serveur DHCP ;
- *Bind* : serveur DNS ;
- *ClamAV* : anti-virus.

4. Structure des conteneurs

Le module Seth s'installe par défaut en mode non conteneur[p.497].

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

Les ressources de ce module sont fortement dépendantes du nombre d'utilisateurs et dépendent peu du mode dans lequel il est configuré :

- contrôleur de domaine principal ;
- contrôleur de domaine additionnel ;
- serveur membre d'un domaine existant.

Si le module est utilisé dans le mode membre (serveur membre d'un domaine existant) le disque dur doit être dimensionné en conséquence pour accueillir les données utilisateurs.

Nul besoin du support des instructions de virtualisation pour faire fonctionner les conteneurs LXC.

Le module fonctionne avec une seule carte réseau.

La mémoire et la taille du disque dur sont dépendantes du nombre d'utilisateurs et du nombre de services activés.

Les partitions à privilégier sont le `/home` en fonction du nombre d'utilisateurs et des quotas disque fixés et le `/var` selon le nombre d'applications web installées.

Il est indispensable que les stations clientes aient le contrôleur de domaine comme premier serveur DNS.

La solution la plus pratique est d'utiliser le service DHCP.

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

Exemple d'usage du module Seth dans un rectorat :

- un contrôleur de domaine principal ;
  500 comptes
  500 postes clients
  250 connectés en moyenne
  Mémoire 4Go CPU 2 cœurs Disque 40Go
- un contrôleur de domaine additionnel ;
  500 comptes
  500 postes clients
  250 connectés en moyenne
  Mémoire 4Go CPU 2 cœurs Disque 40Go
- plusieurs serveurs membres attachés au domaine et dédiés à différents services du rectorat (DSI, DIRH) ;
  500 comptes
  500 postes clients
  250 connectés en moyenne
  Mémoire 4Go CPU 2 cœurs Disque 1To

6. Les différences entre les versions 2.5 et 2.6

Le module Seth est un nouveau module, il n'est disponible qu'à partir de la version 2.6.0 d'EOLE.

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.507], 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.519] est, dorénavant, la seule méthode valide pour la gestion des services. upstart[p.521] est encore accepté pour assurer la rétrocompatibilité. Cependant, le service est, dans tous les cas, géré par systemd.

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

Interfaces réseau

Sur la nouvelle version d'EOLE les cartes réseau respectent la convention Consistent Network Device Naming[p.496] de udev[p.521] 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.

Installation UEFI

Les nouvelles images ISO générées par EOLE intègrent le support de l'UEFI[p.521].

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.

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.515] de liens Ethernet.

Gestion des certificats Let's Encrypt

L'autorité de certification Let's Encrypt[p.506] 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.

Samba 4.5

À partir de la version 2.6.1 d'EOLE, le module Seth utilise la version 4.5 de Samba. Les paquets associés à la version 4.5 de Samba s'installent à la première mise à jour du module. Cette version de samba permet notamment la prise en compte de plusieurs DNS Forwarders[p.499]. Ainsi, la liste complète des serveurs DNS renseignés dans l'interface de configuration du module est prise en compte (et plus

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

seulement le premier de la liste).

SID du domaine

Dans le cas d'une migration ou d'une réinstallation d'un contrôleur de domaine principal Seth, il est possible de forcer le SID[p.517] à utiliser pour le domaine.

Partages additionnels et corbeille

Il est possible de déclarer des partages additionnels directement dans l'interface de configuration du module et d'activer la corbeille Samba sur les répertoires personnels ainsi que sur certains répertoires partagés.

Archivage et sauvegarde des données de l'Active Directory

Un archivage local est activable et permet d'avoir une copie récente des données du serveur Active Directory.

L'installation complémentaire du logiciel Bareos[p.495] permet la mise en œuvre d'un système de sauvegarde plus complet.

Restrictions d'accès

La déclaration de restrictions et d'autorisations d'accès par service (Samba-AD, LDAP, ...) est possible dans l'interface de configuration du module.

2.6.2

Accès au backend EAD

À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD[p.500] 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.

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.519].

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

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`.

DHCP

Le service DHCP propose maintenant la redondance et la répartition de charge.

La prise en charge de l'API OMAPI[p.511] permet de changer la configuration DHCP à chaud.

Le nommage des plages DHCP facilite leur identification dans l'EAD3.

Composant utilisé pour le service DNS

Sur les contrôleurs de domaine, un service DNS est obligatoirement mis en place.

Le service DNS peut être assuré par un composant interne de Samba (par défaut) ou délégué à Bind9[p.495].

Positionnement du serveur dans un site Active Directory

Il est possible de demander à ce qu'un contrôleur de domaine additionnel soit rattaché à un site Active Directory existant.

Samba 4.7

En version 2.6.2, le module Seth utilise la version 4.7 de Samba. Cette version est la première à supporter officiellement le RODC[p.515].



À partir d'EOLE 2.6.2, l'instance échoue si la version de Samba installée sur le module n'est pas celle attendue.

Les paquets `samba` doivent impérativement être mis à jour via `Maj-Auto` avant l'instance.

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 Seth

Pour jouer son rôle de serveur Active Directory, le module Seth repose principalement sur le projet libre Samba[p.516] en version 4.

Le module propose également un service DHCP[p.498] qui permet aux stations clientes d'obtenir une configuration réseau adaptée.

Le service Samba est paramétrable afin que le module Seth fonctionne dans des modes différents :

- contrôleur de domaine Active Directory ;
- serveur membre d'un domaine existant.

Fonctionnement en mode contrôleur de domaine

Dans ce mode, le module Seth offre tous les services d'un contrôleur de domaine Active Directory.

Les répertoires partagés peuvent être hébergés sur l'un des contrôleurs de domaine ou déportés sur un serveur membre.

La possibilité de faire travailler ensemble plusieurs contrôleurs de domaines Seth (mode multi-DC[p.510]) et d'y adjoindre des serveurs membres rend la solution totalement scalable[p.517].

Fonctionnement en mode membre d'un domaine existant

Ce que ne fait pas un serveur membre

Contrairement au contrôleur de domaine :

- un serveur membre ne traite PAS les ouvertures de session de comptes ;
- un serveur membre ne participe PAS à la réplication Active Directory ;
- un serveur membre ne stocke PAS les informations de stratégie de sécurité de domaine.

Ce que peut faire un serveur membre

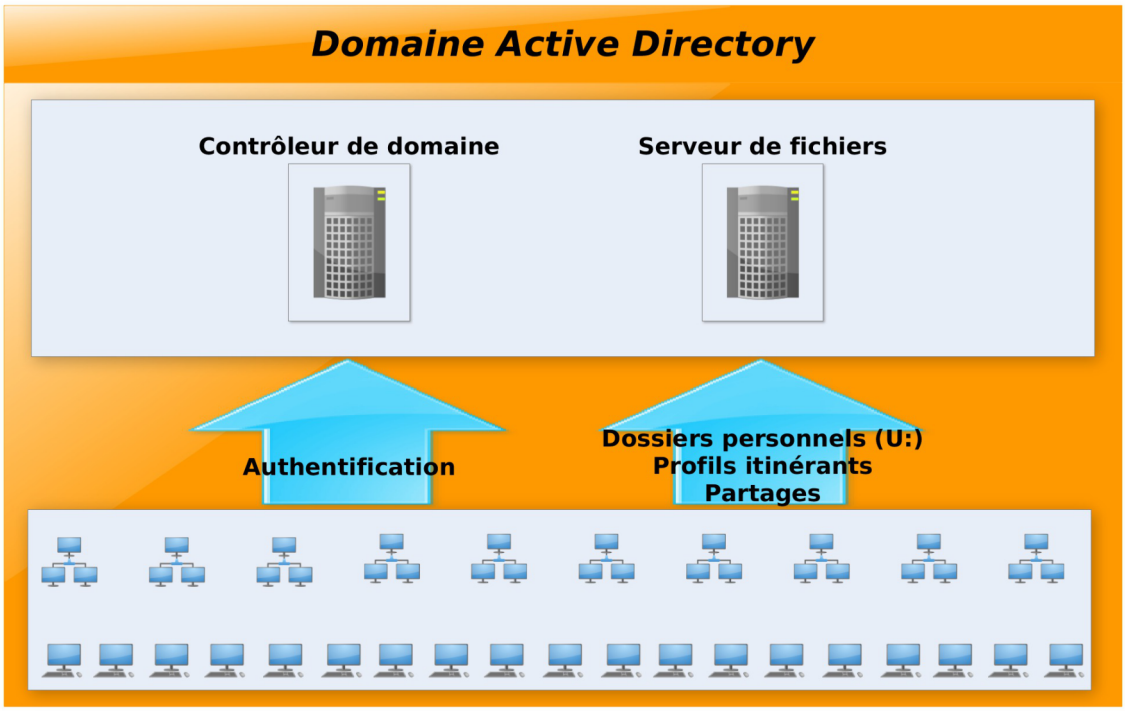
Un serveur membre pourra, par contre, être :

- un serveur de fichiers ;
- un serveur d'impression ;
- un serveur web ;
- un serveur applicatif.

Exemples d'architectures avec des modules Seth

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

Séparation du contrôleur de domaine et du serveur de fichiers



L'architecture repose sur deux serveurs :

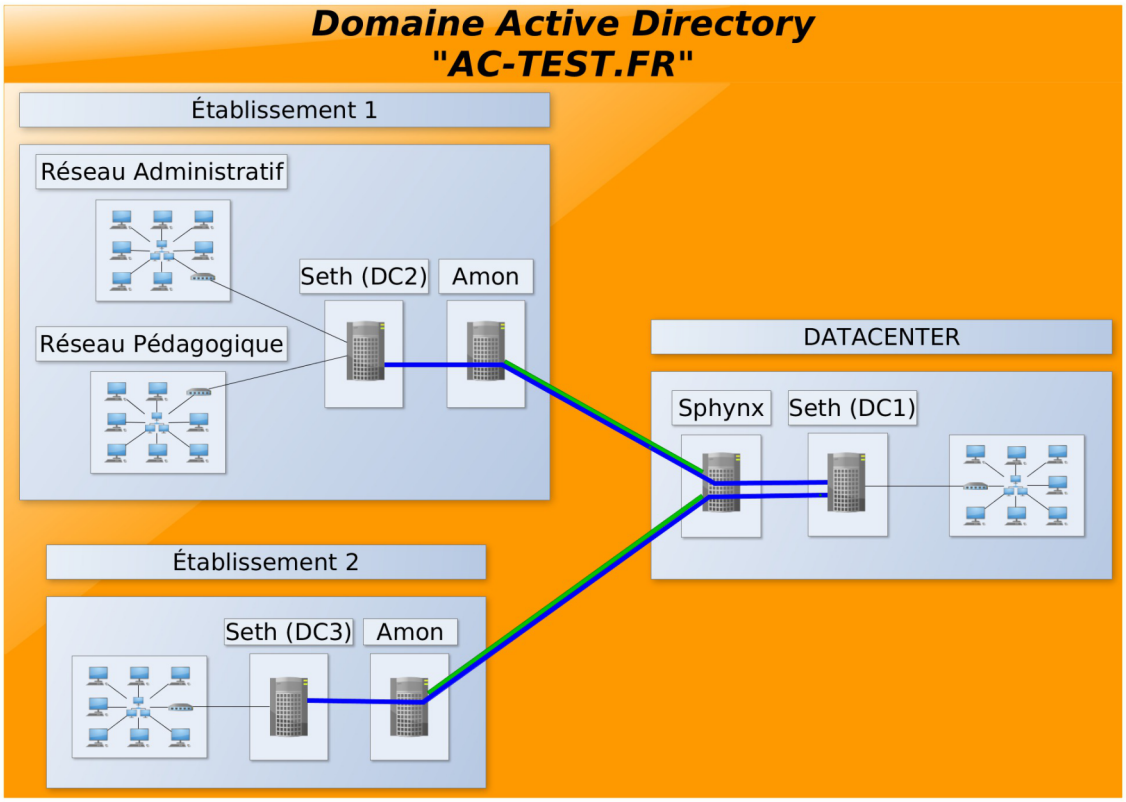
- un contrôleur de domaine réalisant les authentifications ;
- un serveur de fichiers.

Cette architecture permet de répartir la charge et de sécuriser l'ensemble en séparant les données utilisateurs de l'annuaire Active Directory.

En cas de compromission ou de défaillance matérielle, seul une partie des données est concernée.

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

Active Directory centralisé et contrôleurs en établissement

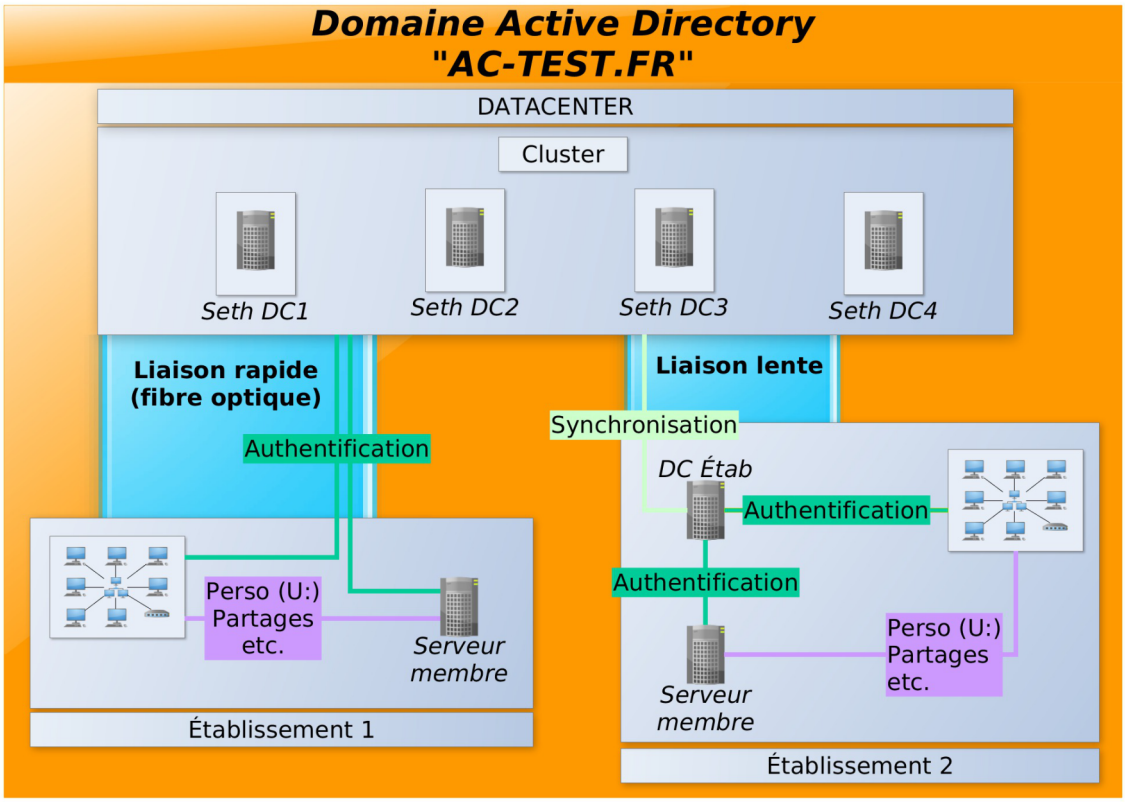


Il est possible d'avoir un seul domaine couvrant plusieurs établissements ou services, voir même une administration entière.

La sécurité de cette infrastructure peut être augmentée en configurant les contrôleurs de domaines des établissements en lecture seule[p.515].

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

Active Directory centralisé et contrôleurs ou serveurs membres en établissement

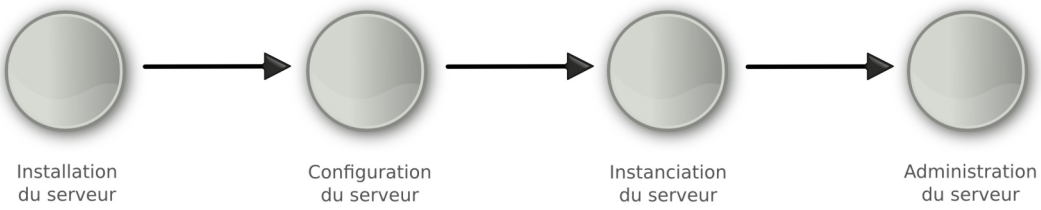


Si les connexions Internet des établissements le permettent, un serveur de fichiers peut suffire par établissement et le contrôleur de domaine peut-être hébergé sur un site distant.

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.504] 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.518], e2guardian[p.500], 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)

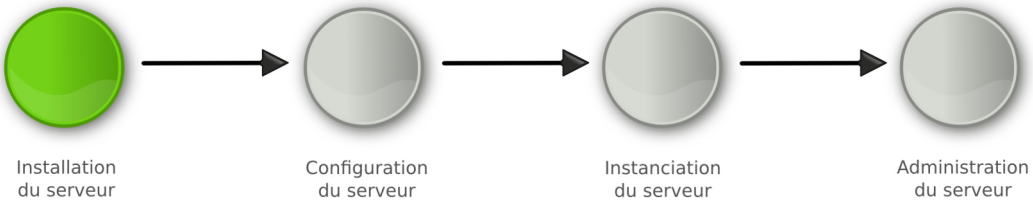
Chaque module possède des fonctionnalités propres, souvent complémentaires.
Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

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.504] 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.521].

Architecture

Depuis la version EOLE 2.6 seule l'architecture 64 bits (AMD64[p.494]) 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.503] :

- 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.508] 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.



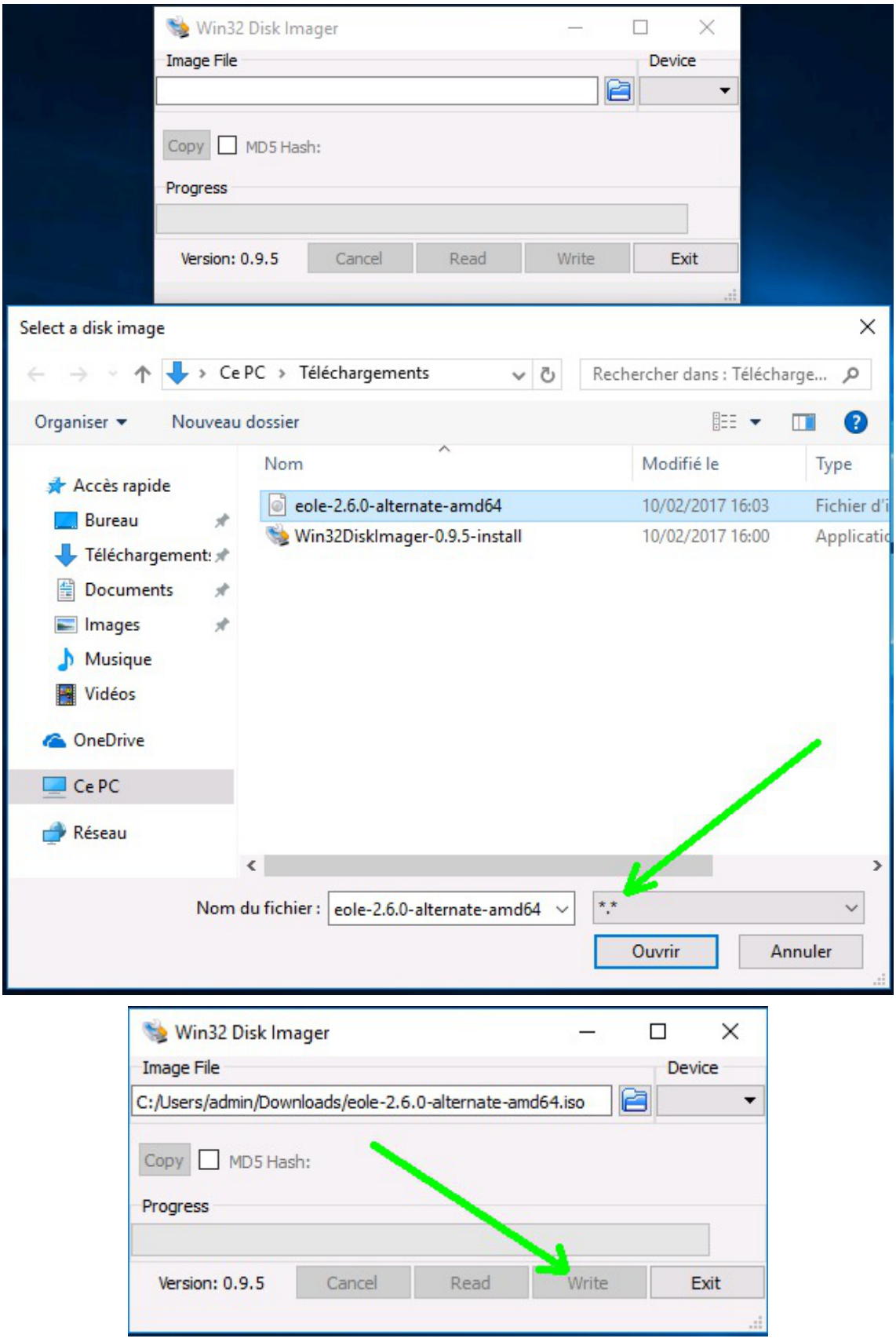
La commande `dd` écrase intégralement le contenu de la clé.

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.514] 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.508] 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.61]

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 :

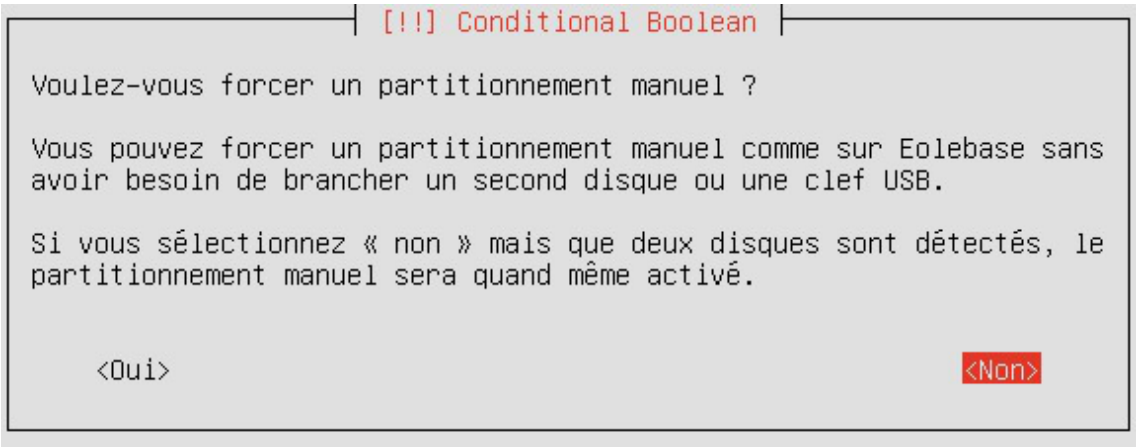
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.508] 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.494]) ;
10. choisir et installer des logiciels ;
11. installation du programme de démarrage GNU GRUB[p.502] ;
12. fin de l'installation.

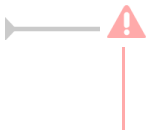
À la fin de l'installation l'écran suivant est affiché.



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.

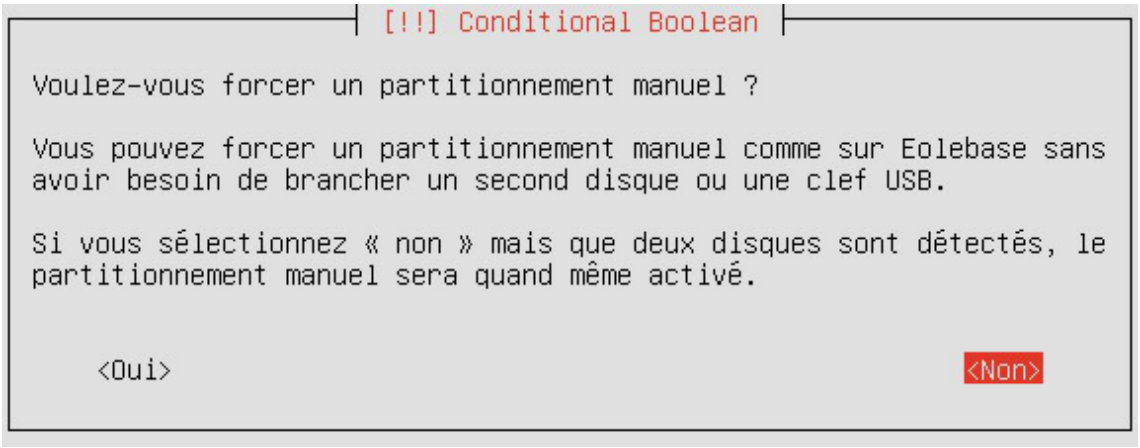
Voir aussi...

Les mots de passe [p.229]

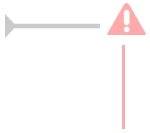
4. Partitionnement personnalisé

Le partitionnement utilise le logiciel LVM[p.508].

- 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

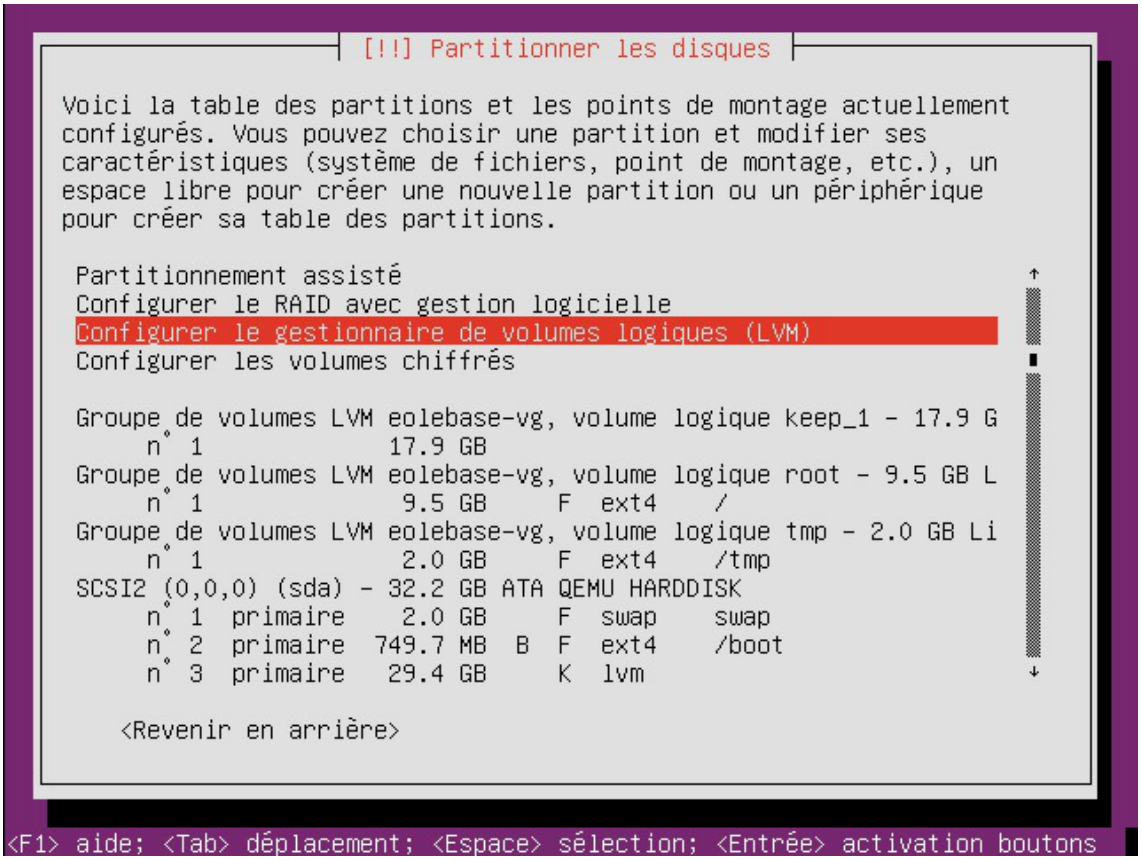
Lorsque le partitionnement manuel est déclenché une fenêtre propose de choisir le disque qu'il faut partitionner pour accueillir le système d'exploitation.



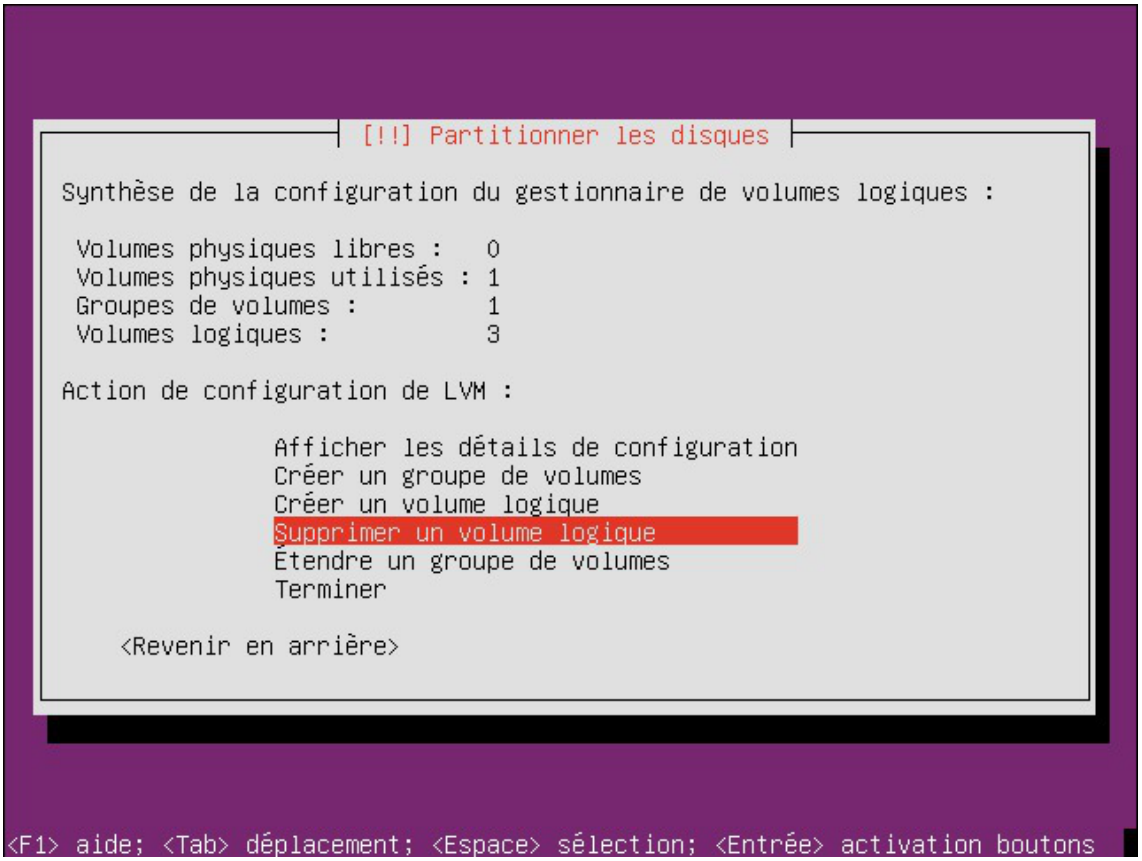
Un volume logique nommé `keep x` sans point de montage et sans système de fichiers contient l'espace qui n'a pas été attribué lors du calcul des autres volumes.
Sur un Eolebase il n'y a pas de volume proposé pour le point de montage `/home`.

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

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

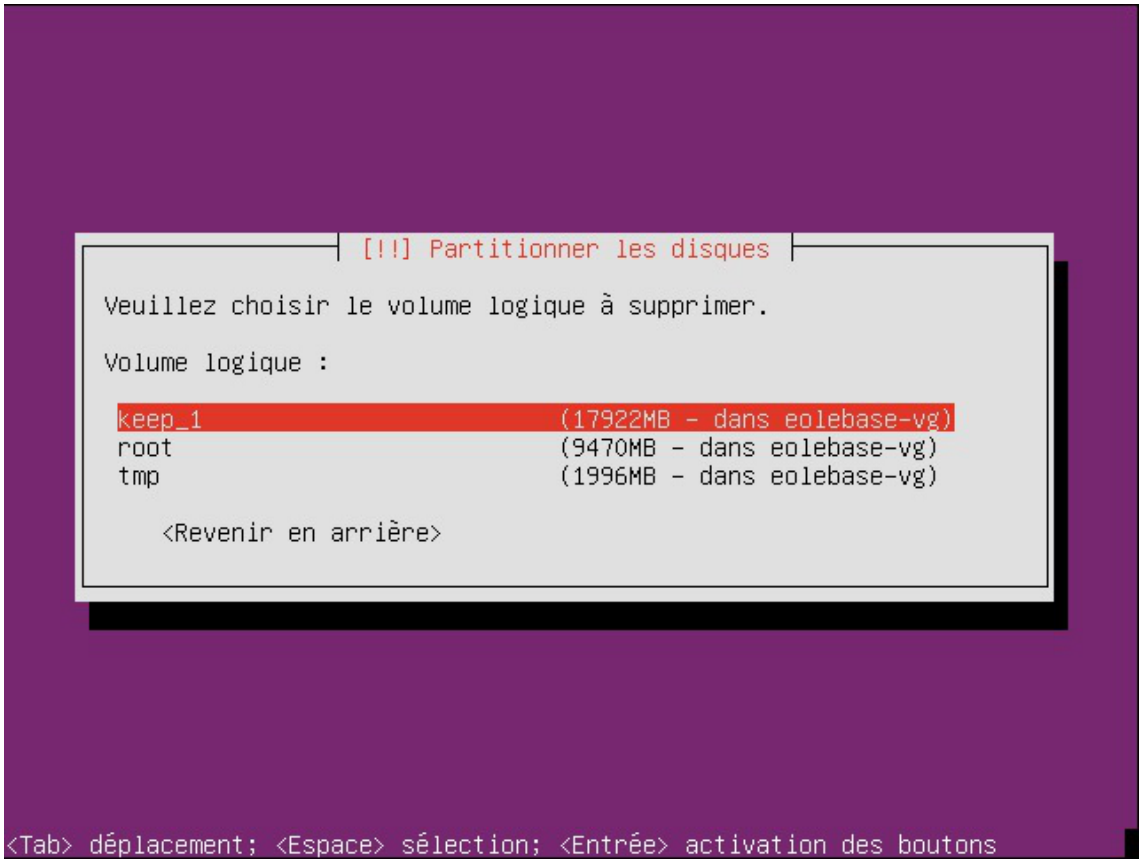


- Sélectionner `Supprimer un volume logique`

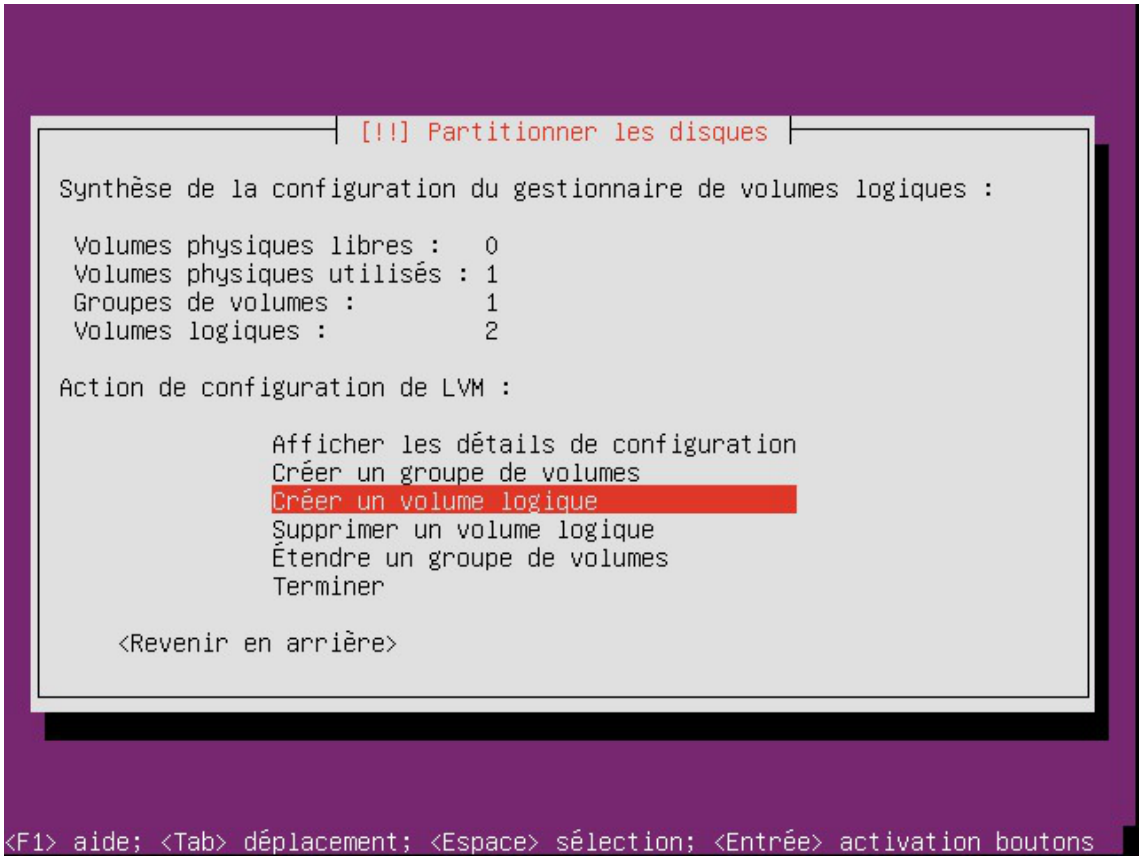


- Sélectionner le volume logique `keep_x`

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

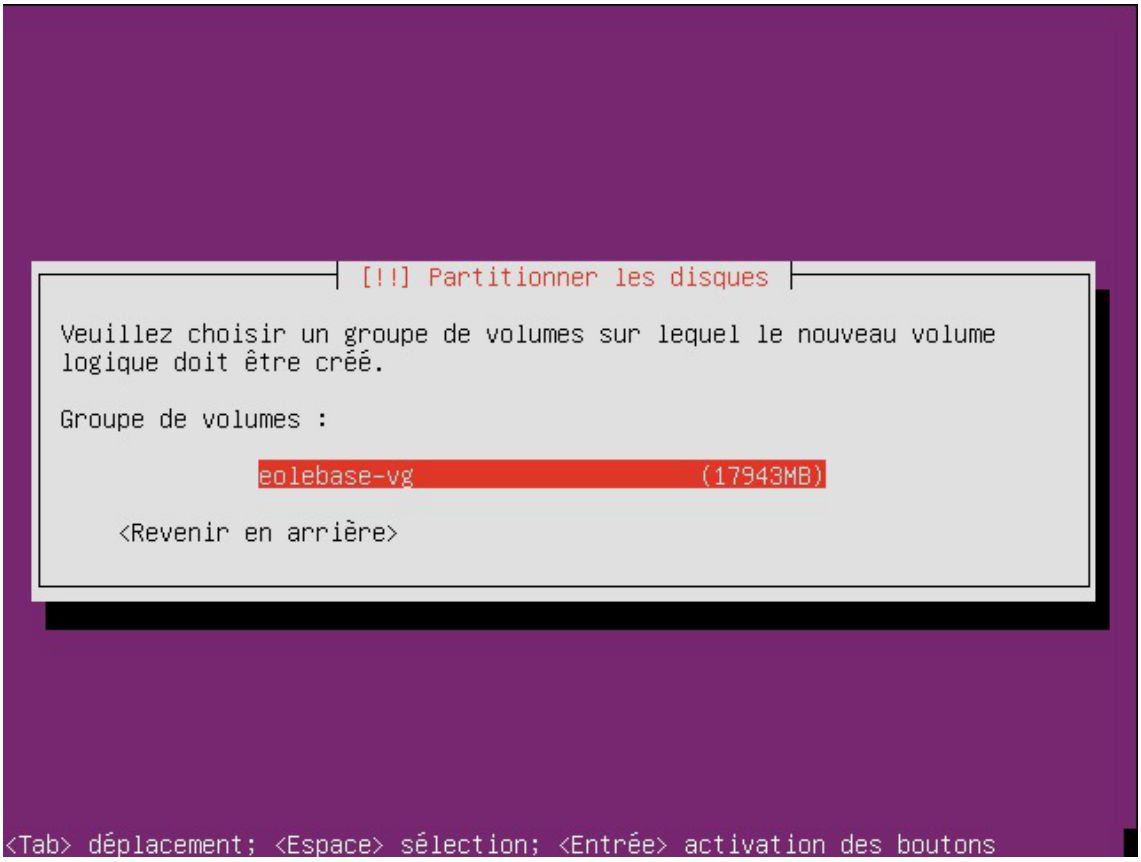


- De retour sur la gestion des volumes logiques, sélectionner `Créer un volume logique`

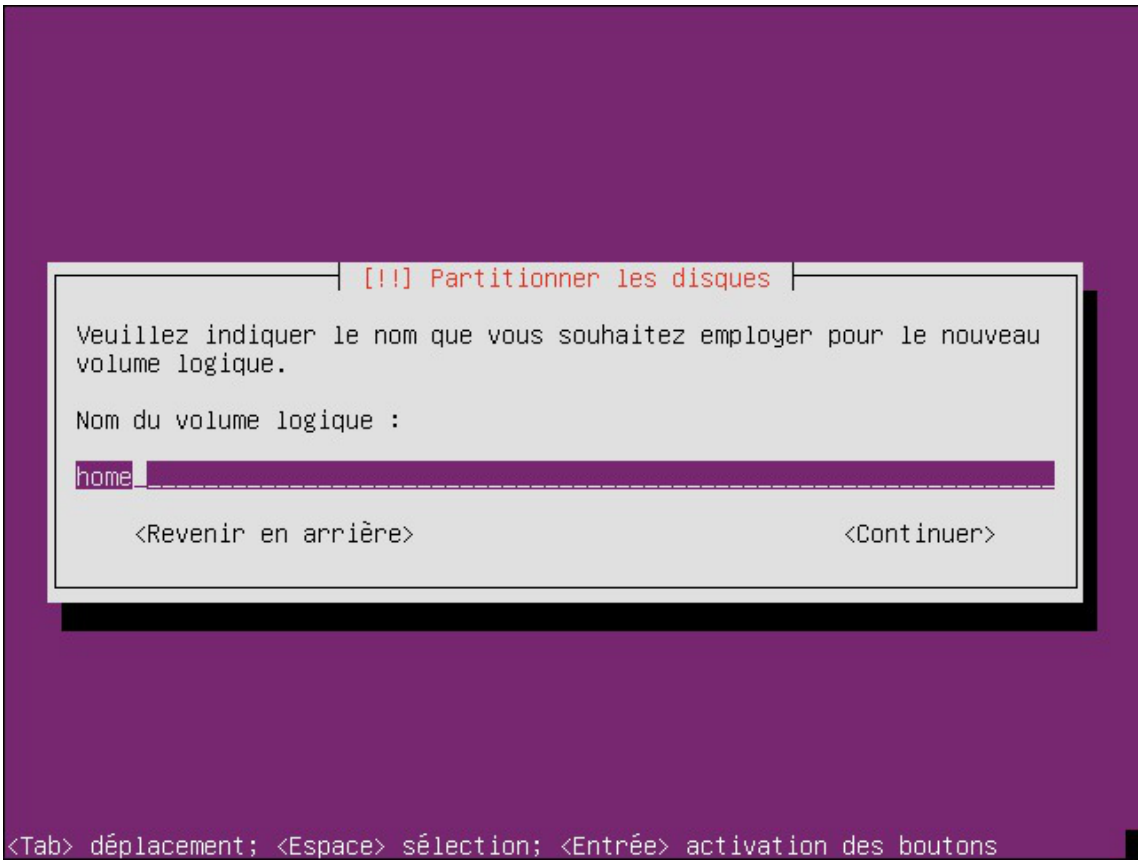


- Valider l'unique `Groupe de volumes` proposé

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

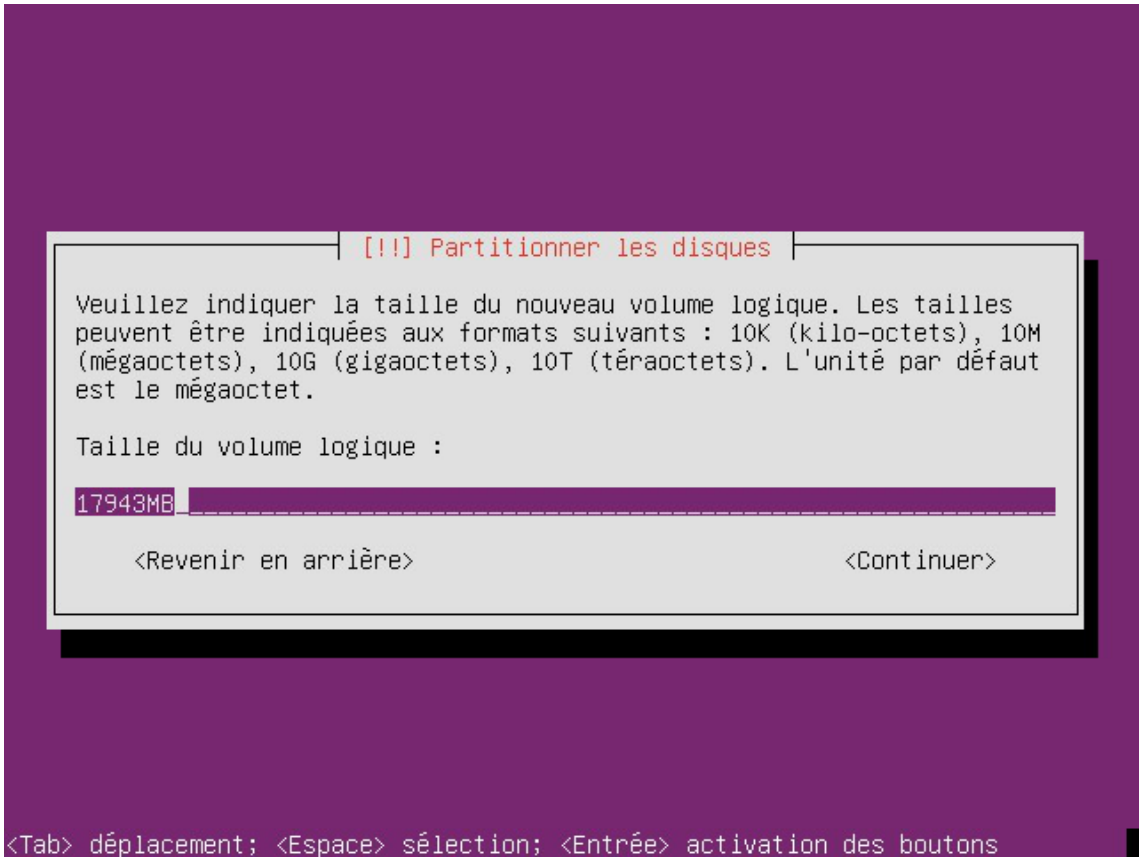


- Choisir le nom du nouveau volume logique

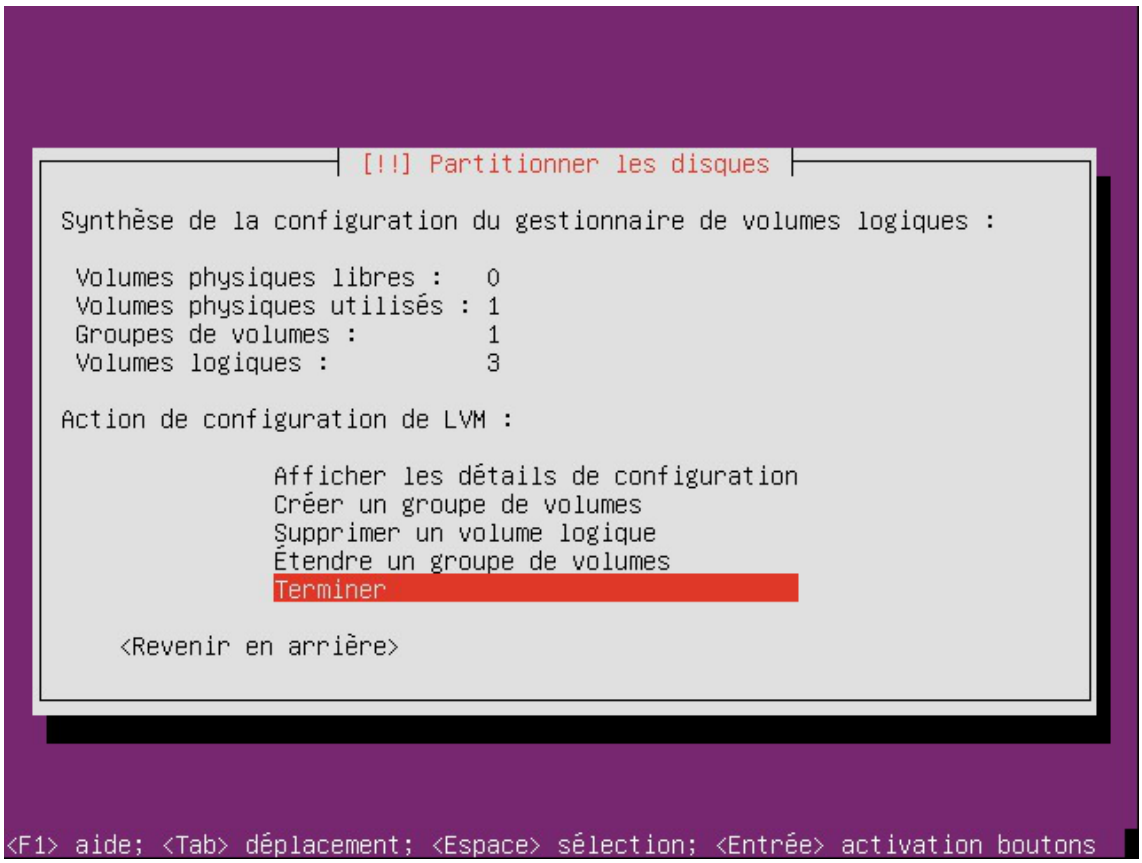


- Puis choisir l'espace à octroyer au nouveau volume, par défaut la taille affichée est la taille maximale

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

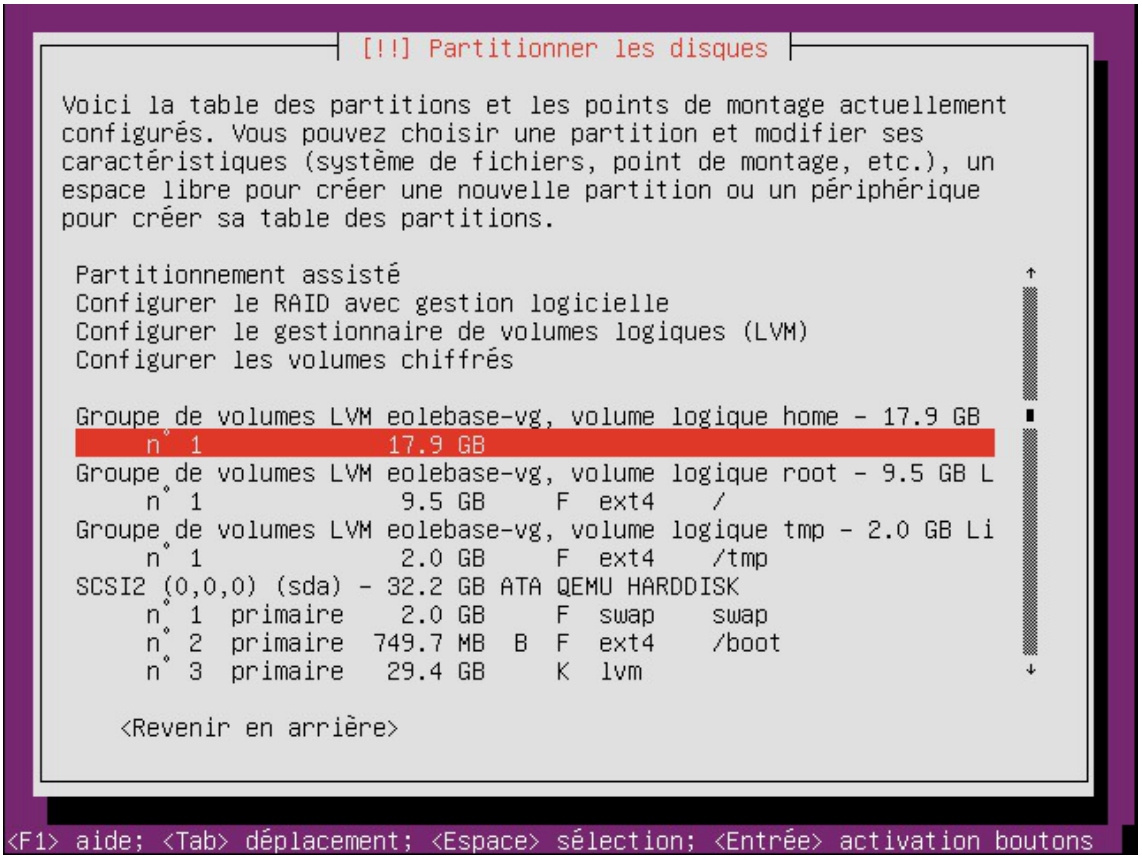


- De retour sur la synthèse de la configuration, sélectionner `Terminer`

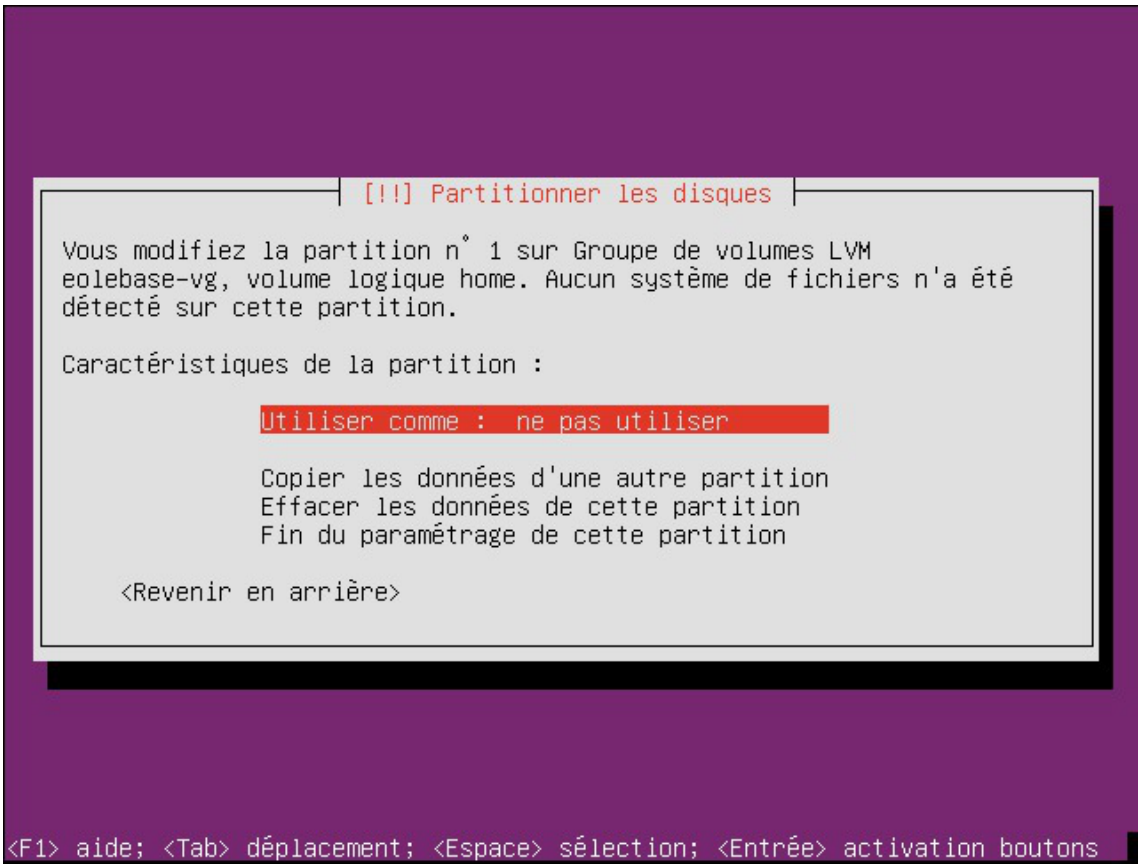


- L'outil de partitionnement affiche maintenant le volume `home`, sélectionner le pour édition

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

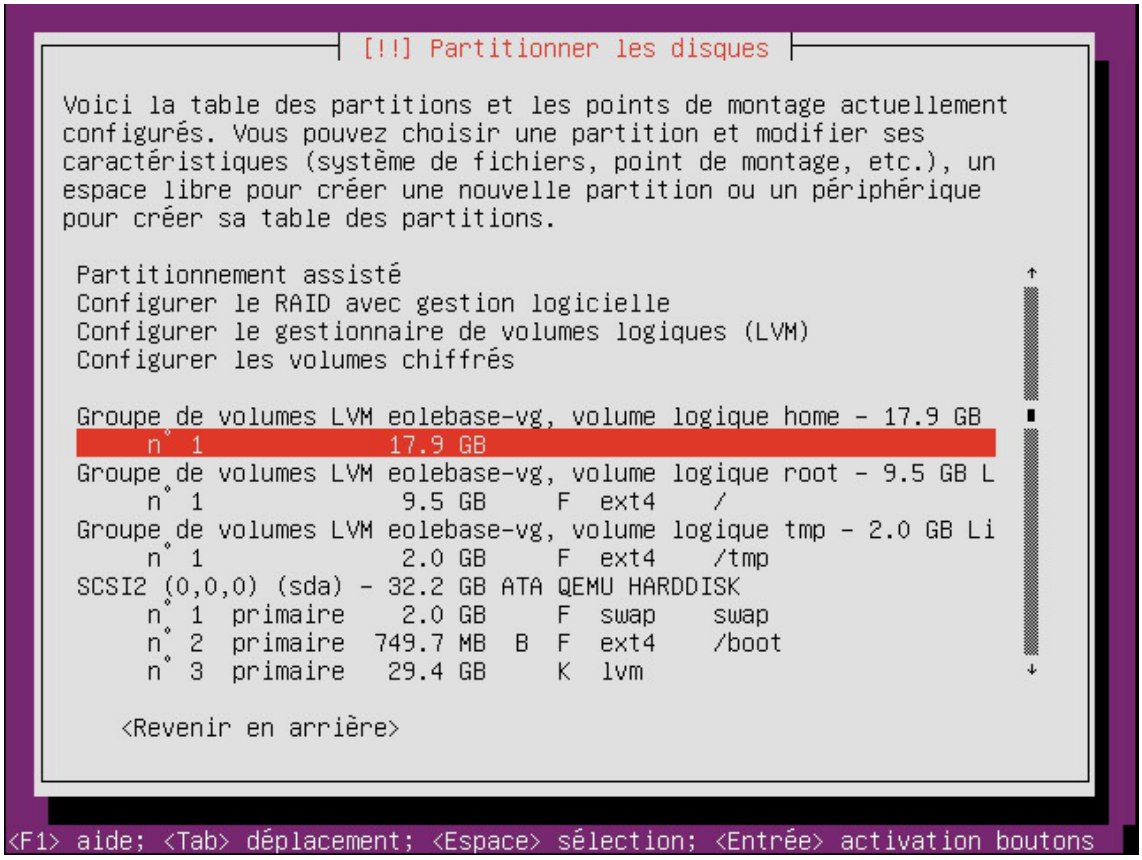


- Sélectionner `Utiliser comme : ne pas utiliser` pour choisir les caractéristiques du volume

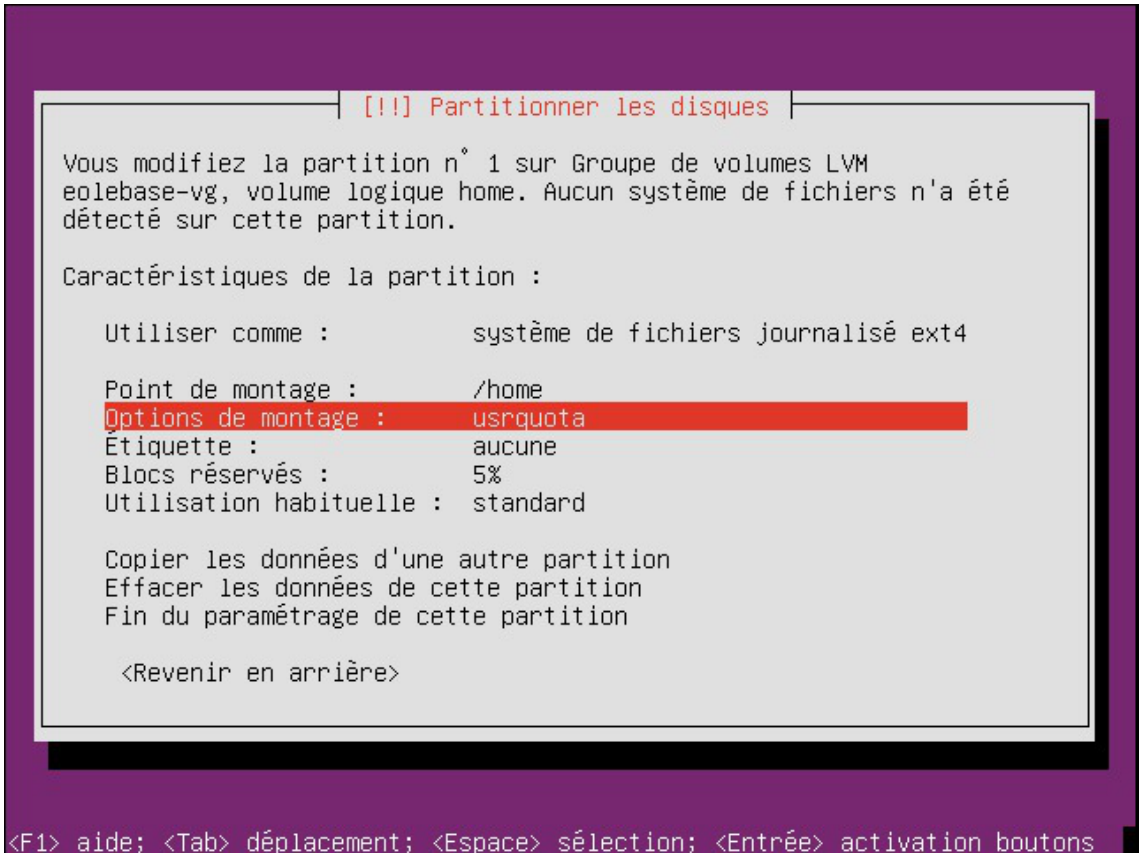


- Sélectionner le type système de fichier

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

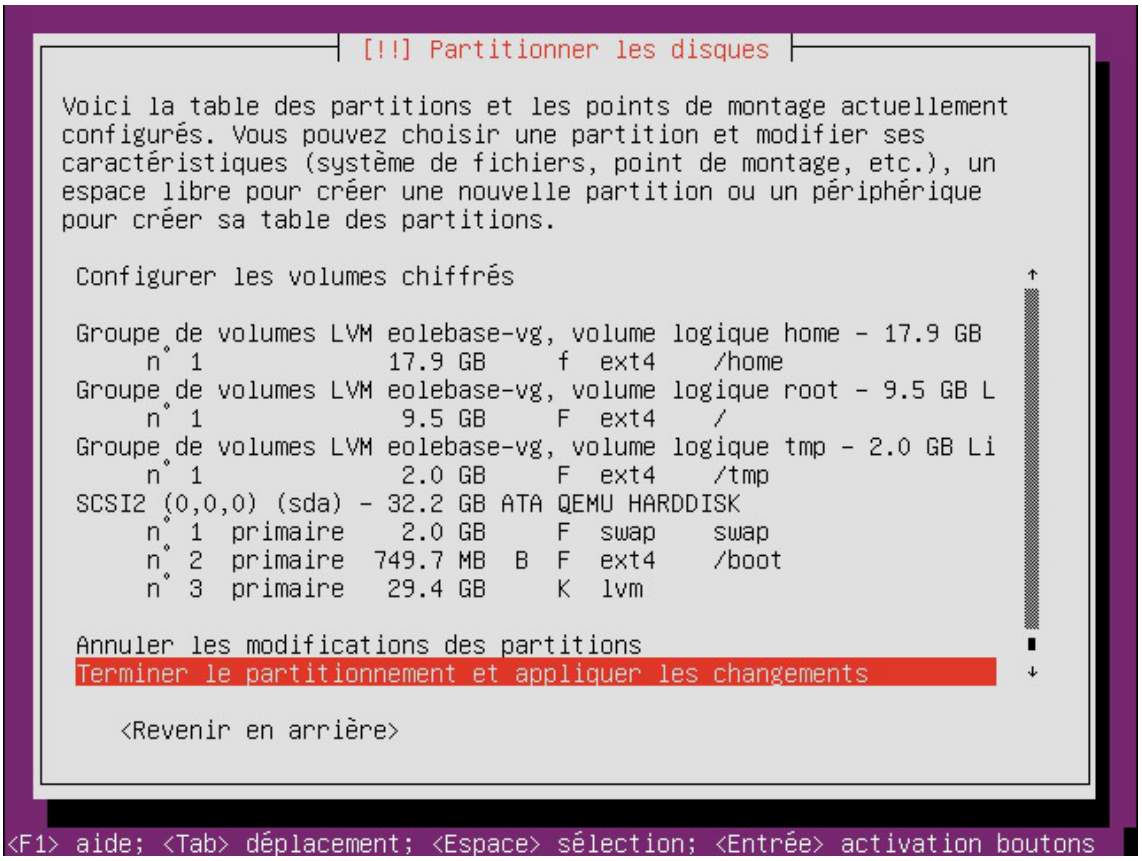


- Puis définir le point de montage et les options de montage

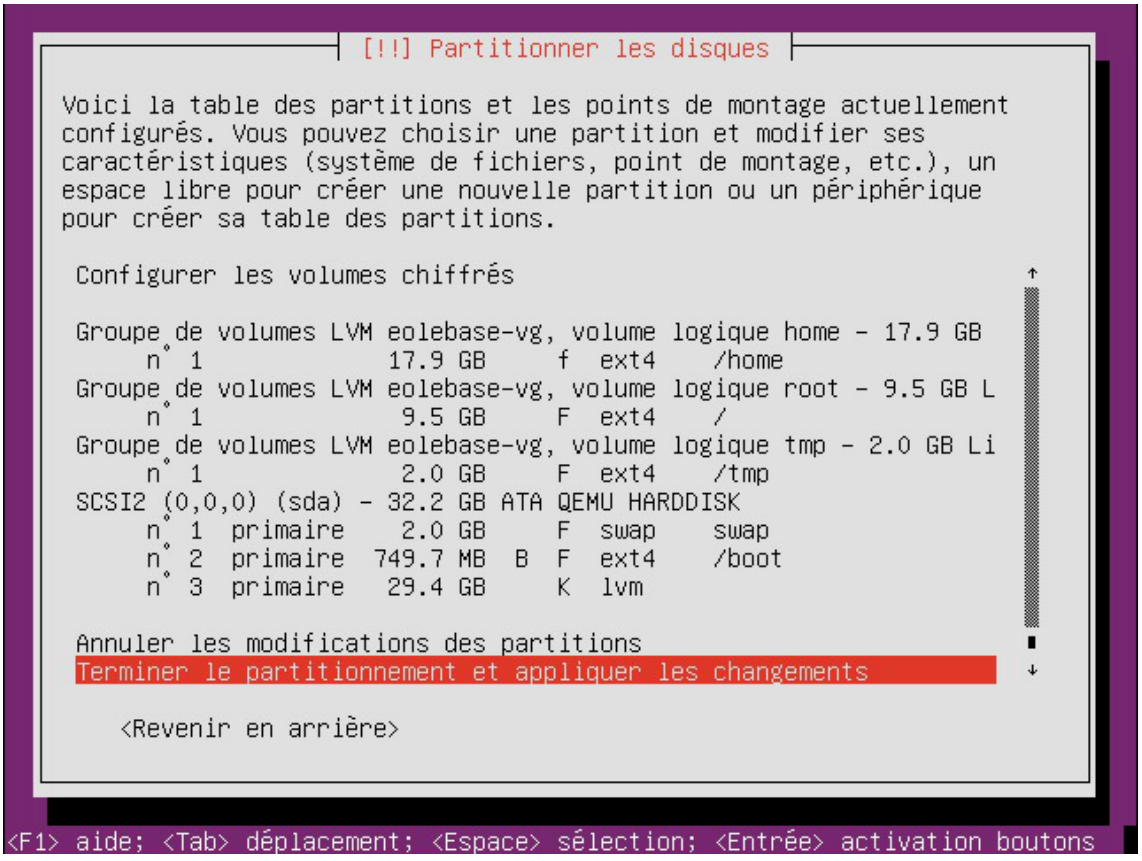


- Sélectionner la `Fin du paramétrage de cette partition`, de retour sur la fenêtre principale du partitionnement

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:~#
```

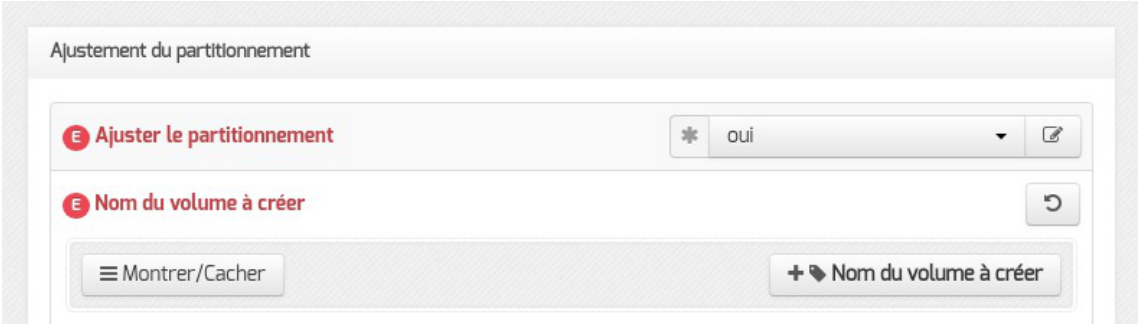
```
root@scribe:~# lvdisplay

  --- 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`.

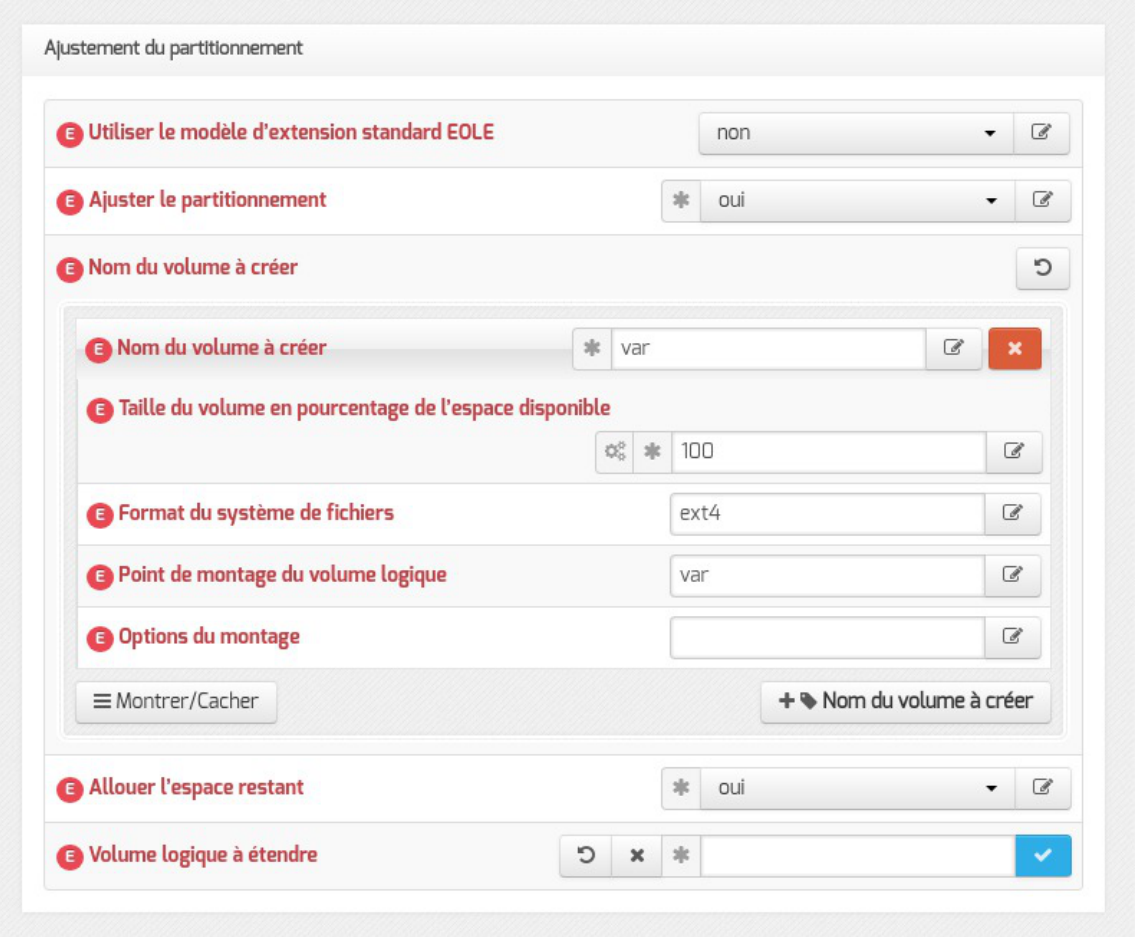
Ajuster le partitionnement sur une version d'EOLE supérieure ou égale à 2.6.2

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).

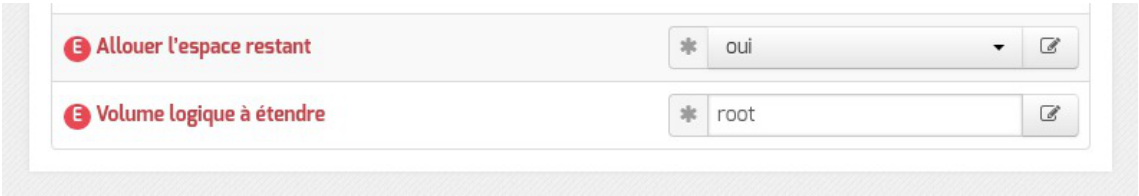
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



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

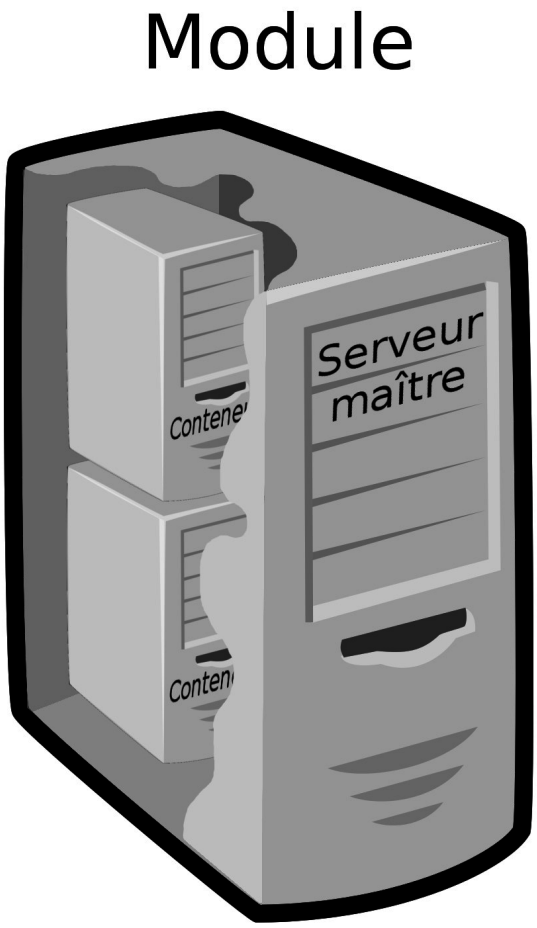
Le paramétrage est effectif après l'instanciation du module.

```
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.497].

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.

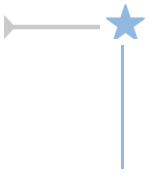
Modules en mode non conteneur

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

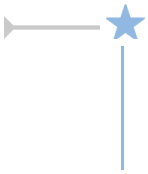
Après l'installation du module, la mise à jour n'est pas obligatoire mais fortement recommandée. Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto`.

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.

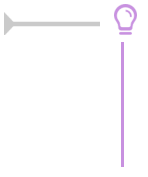
À partir d'un module



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`.

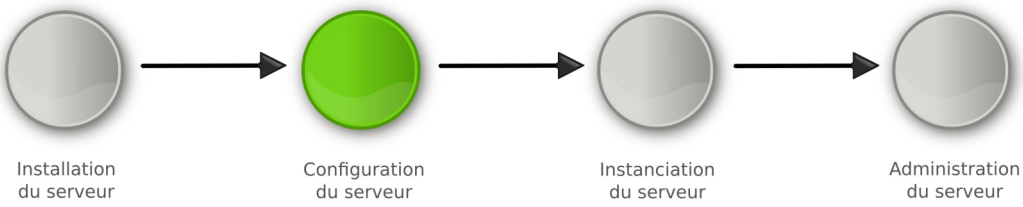
Voir aussi...

Les mises à jour [p.314]

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

Chapitre 6

Configuration du module Seth



Configuration

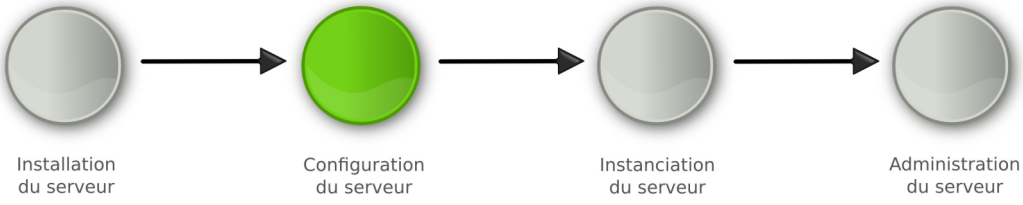
- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config` .

  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.518], e2guardian[p.500], 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.499], l'adresse du serveur de temps NTP[p.511], ...). 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`.

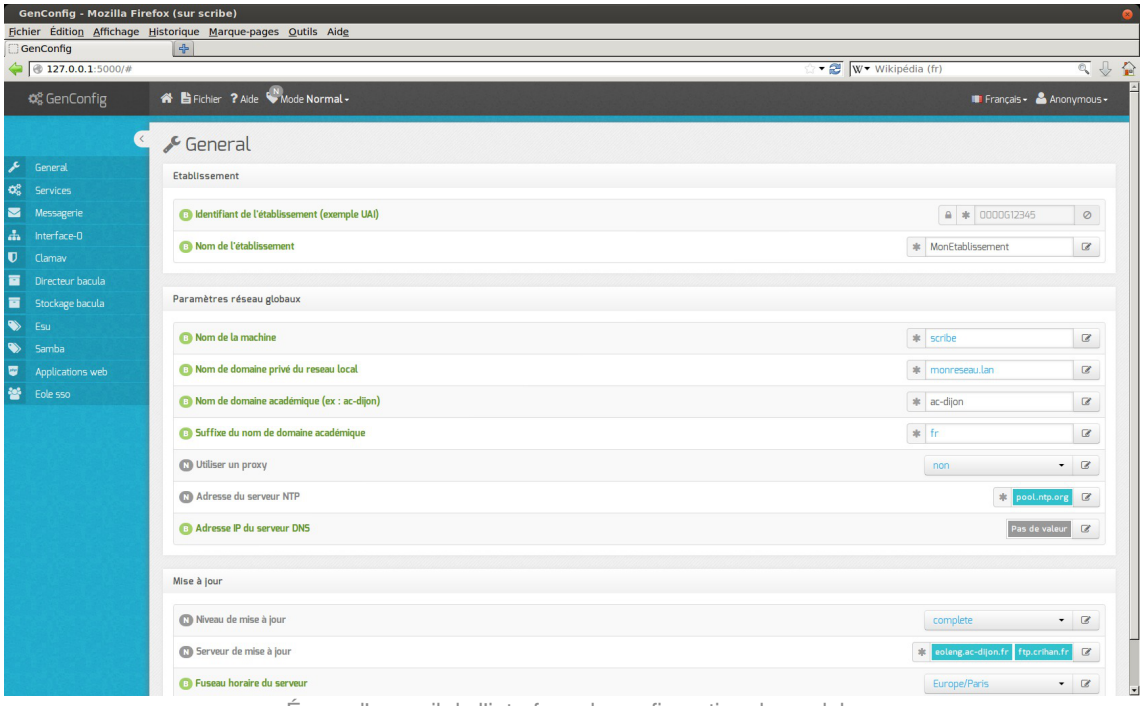
Il est donc possible d'utiliser le fichier `config.eol` d'un serveur en production pour en *instancier* un nouveau.



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

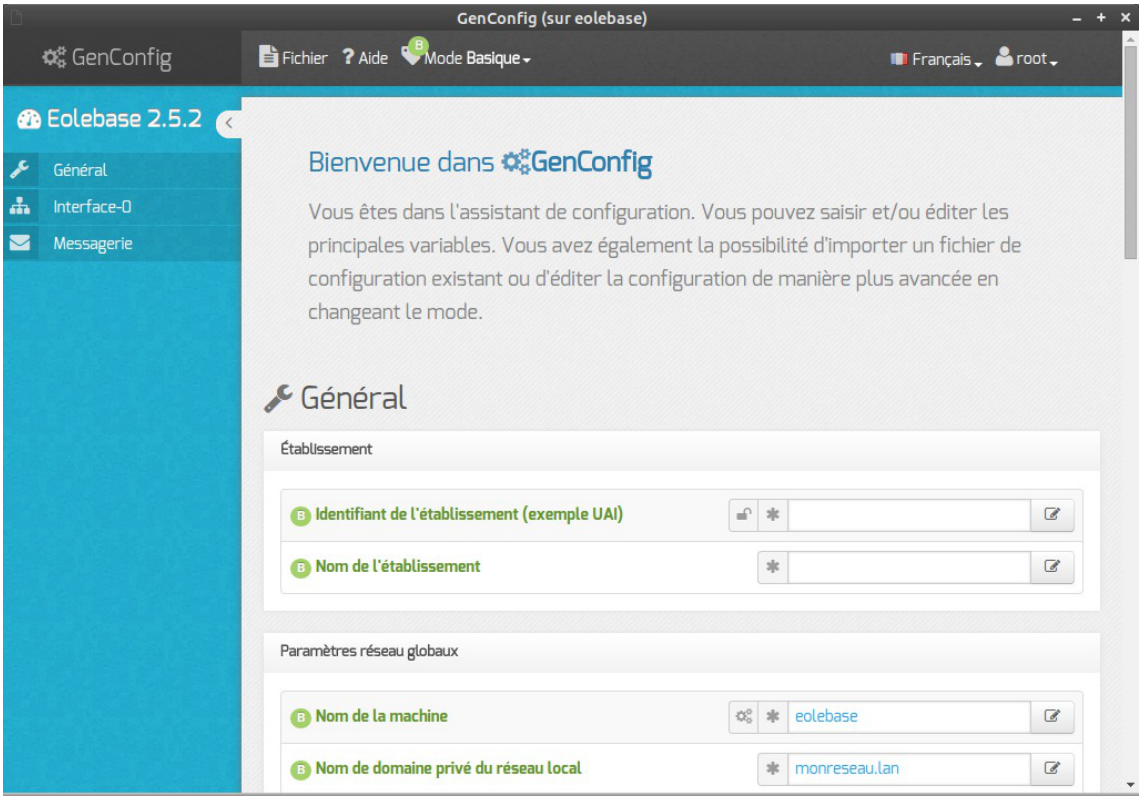
Une fois la commande `gen_config` lancée, comme indiqué dans la mire, vous devez ouvrir une session avec l'utilisateur **root** et le **mot de passe aléatoire** généré à l'installation.



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.

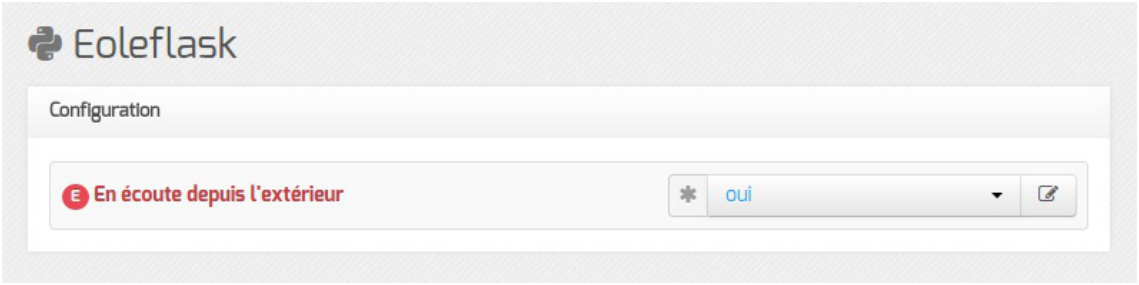
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

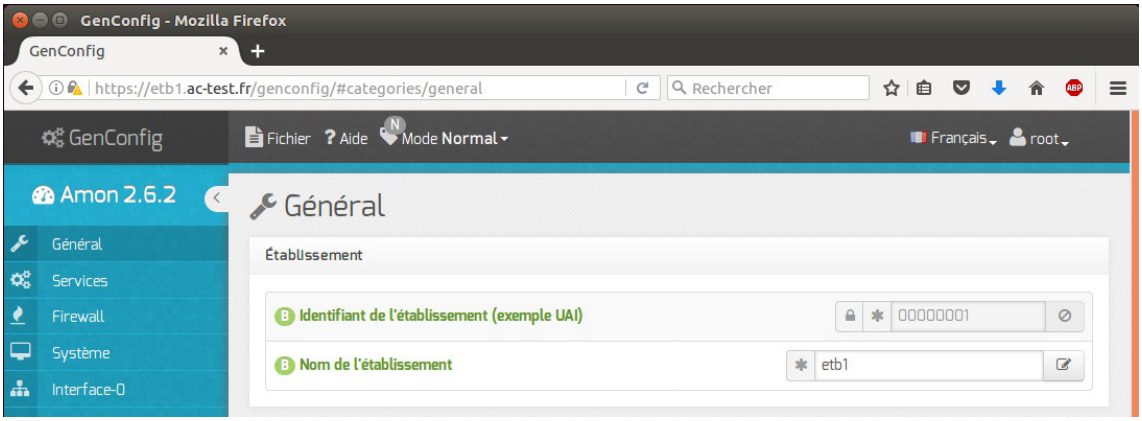
À partir d'EOLE 2.6.1, l'interface est également disponible sur le port 443 si la variable experte `Activer l'interface de configuration du module (GenConfig)` est à `oui` dans l'onglet `Services`. C'est le cas par défaut à partir d'EOLE 2.6.2.

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

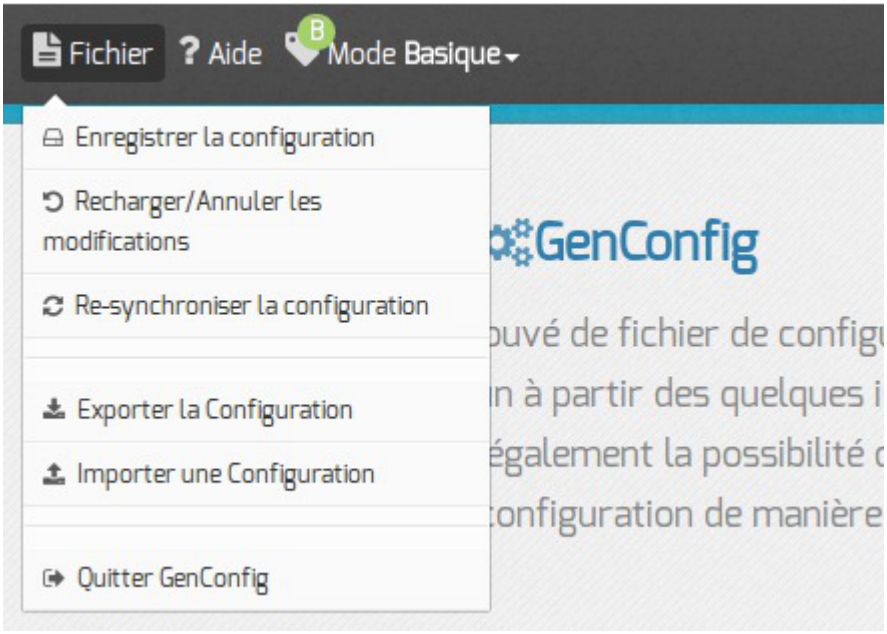
La zone de Menu, en haut de l'interface, propose les items suivants :

- 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.

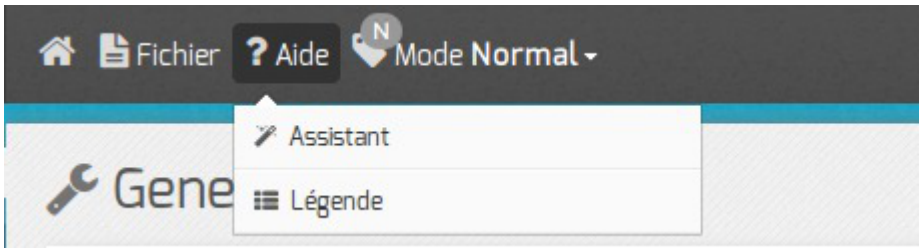
Re-synchroniser la configuration permet de récupérer les informations stockées en session sur le serveur si une coupure arrivait pendant la configuration.

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.

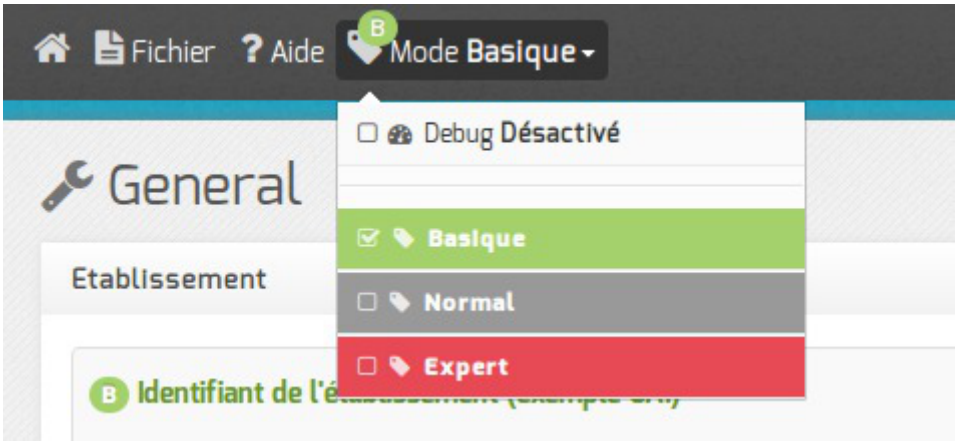
La légende présente un récapitulatif des différentes icônes que l'on peut rencontrer dans l'interface.

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.

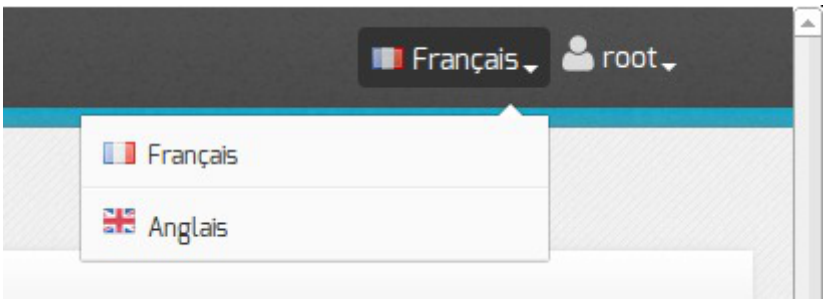
Le mode *Expert* active les onglets et les variables pour une configuration avancée.

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

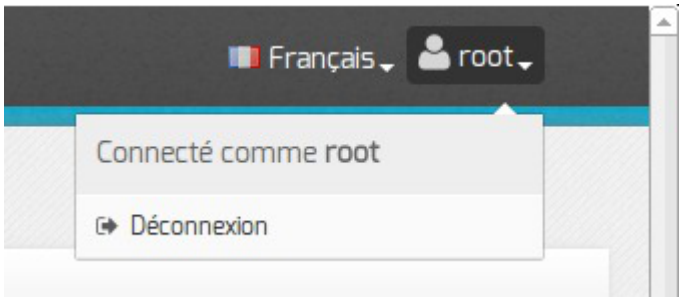


Langue permet de choisir la langue utilisé dans l'interface.

Sous-menu Session

- Connecté comme
- Déconnexion

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



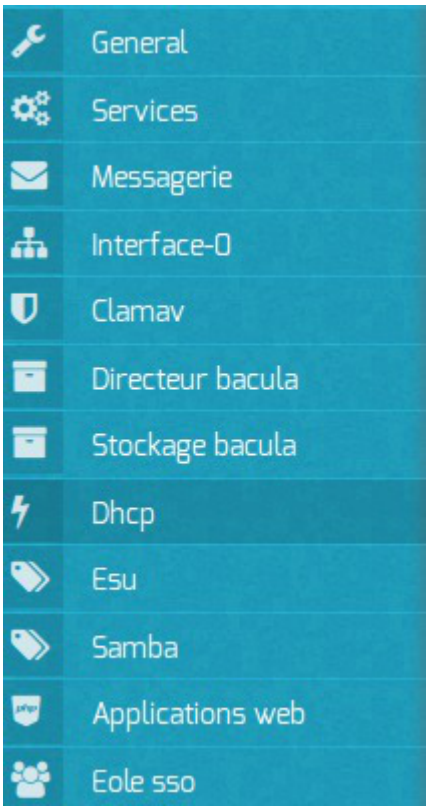
Session permet de connaître l'utilisateur courant et de se déconnecter.

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).



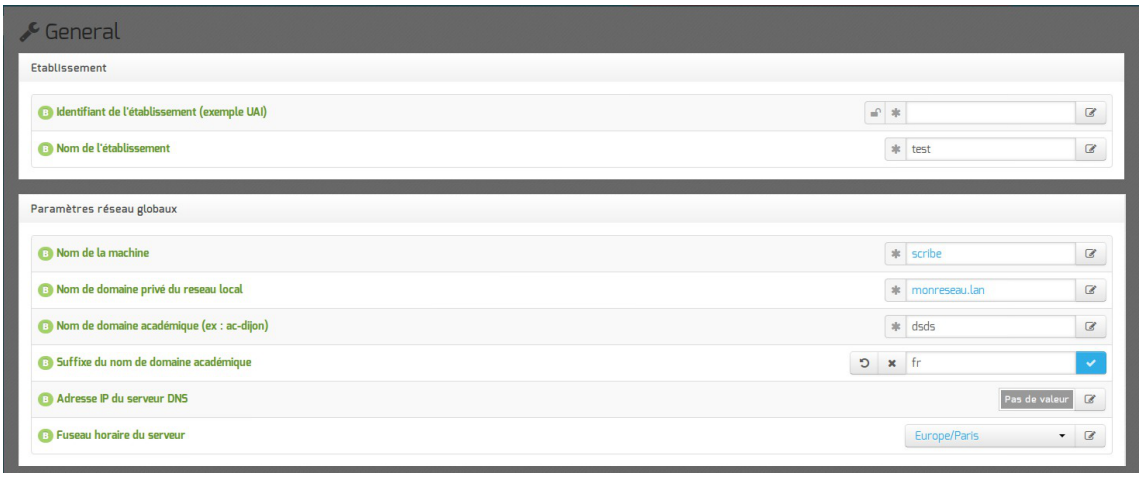
Bouton modifier sur la première ligne à droite, la deuxième ligne a le focus

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.

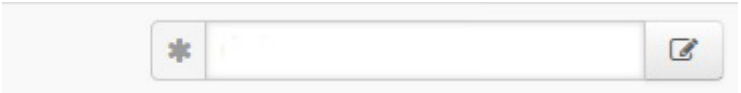


Les blocs thématiques

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

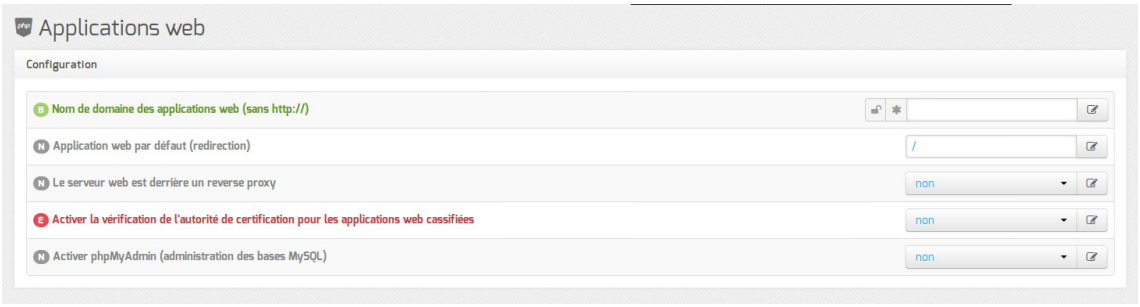
Le mode détermine l'affiche de variable plus ou moins complexes : basiques, normales ou expertes.

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.

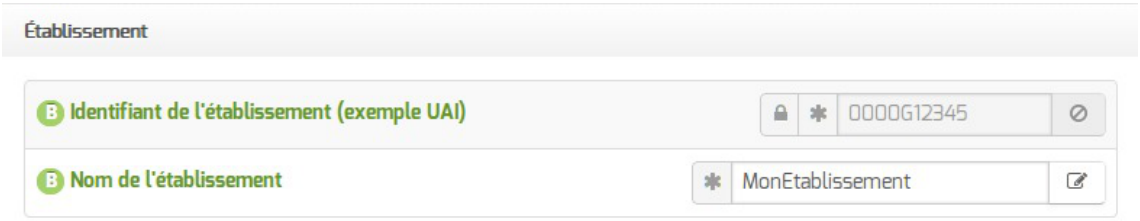


Les variables et leur niveau de complexité

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.



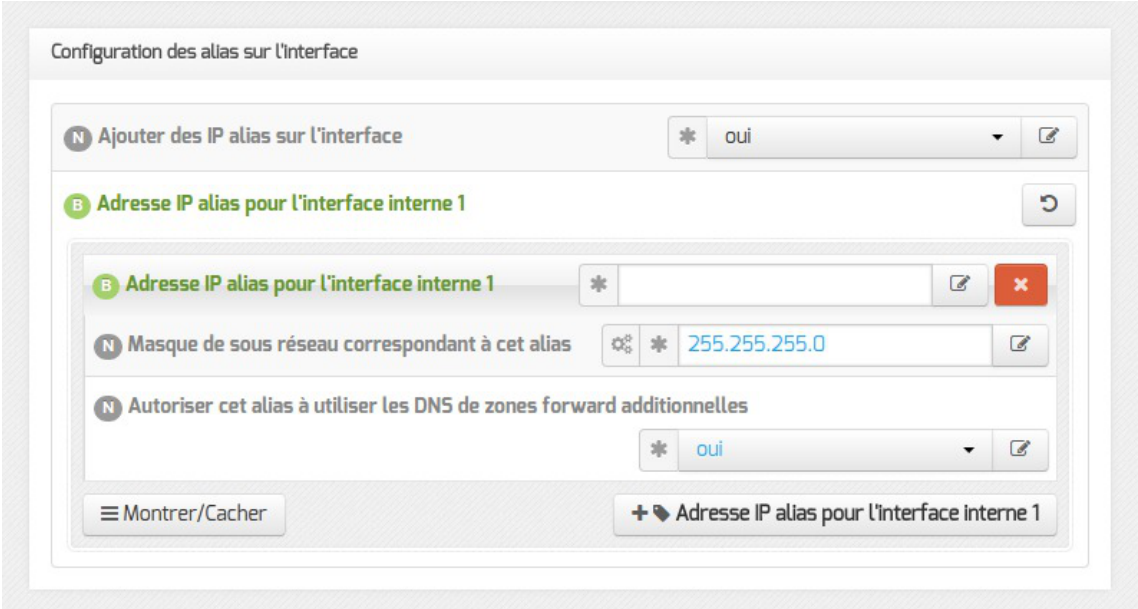
Édition d'une variable multiple

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 :

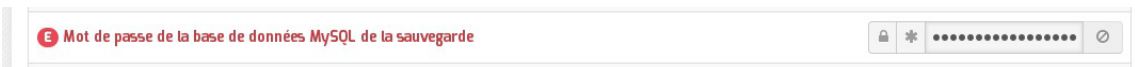
- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée.



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.



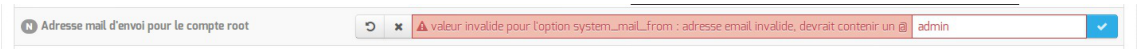
Validation des variables

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.



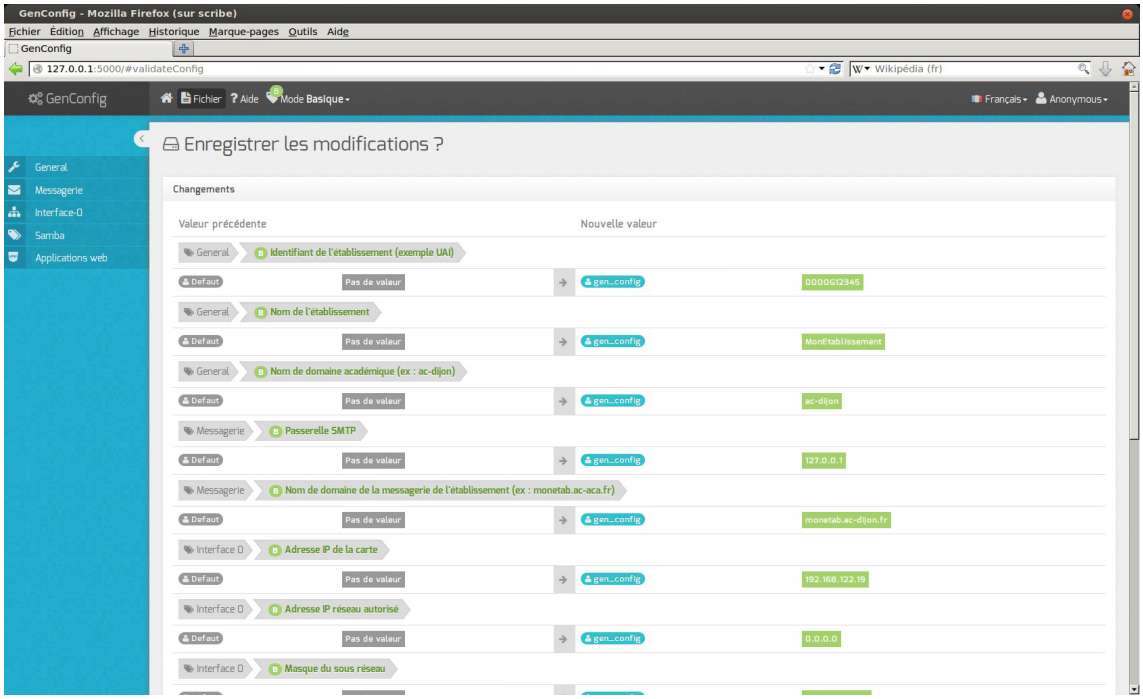
Validation d'une variable

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.

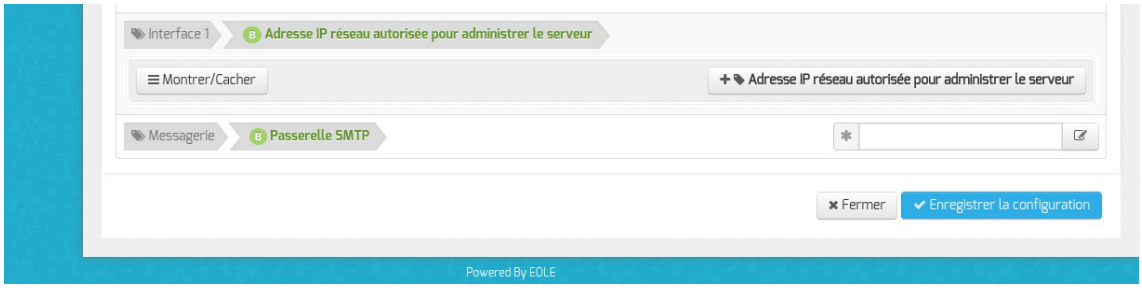
Lors d'une réédition de la configuration cette zone ne montre que les changements qui ont eu lieu.



Zone de validation

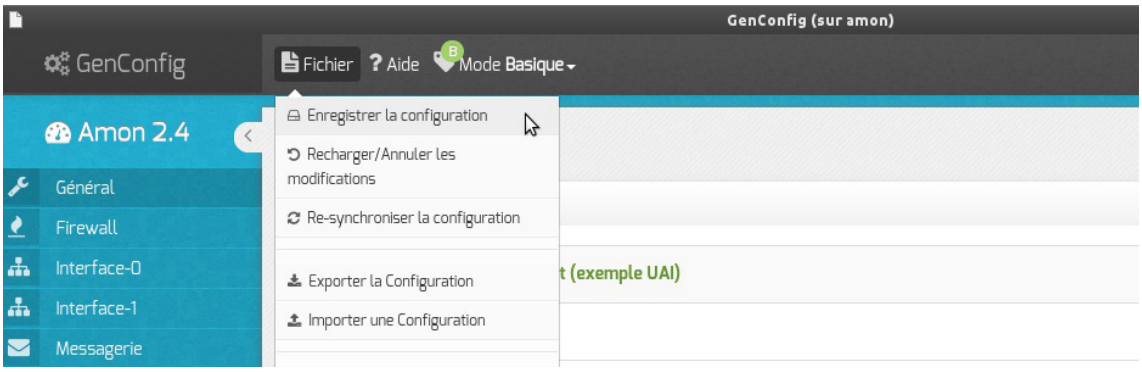
1.1.6. Enregistrer la configuration

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

`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.505] 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.520] 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.503].

> 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.70]

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.520] 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.503].



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

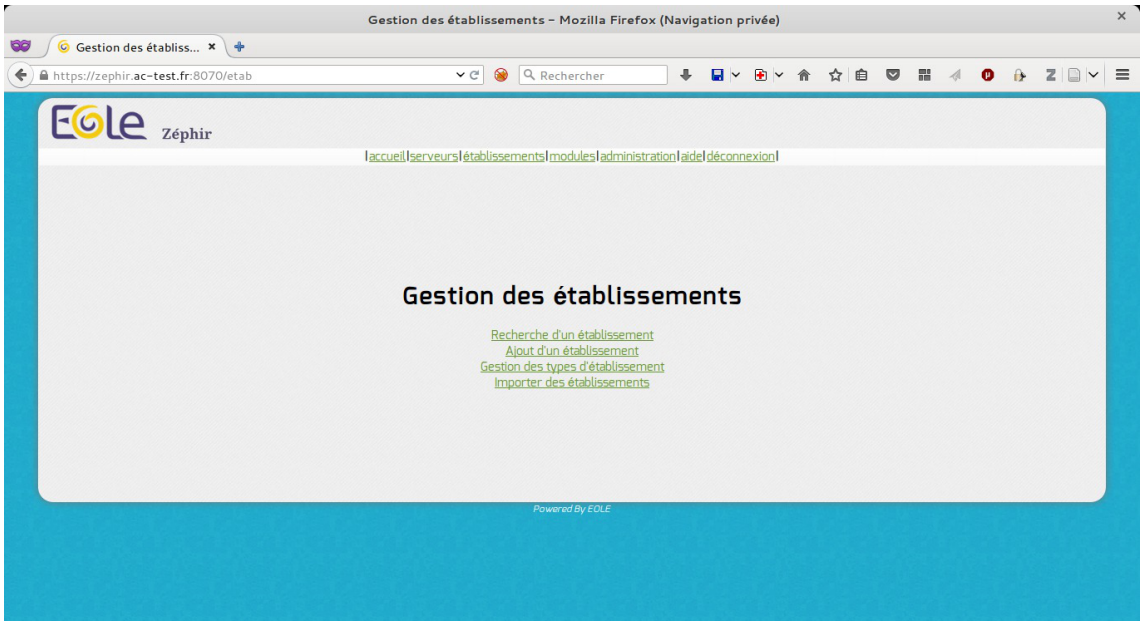
L'établissement d'appartenance du serveur doit déjà exister dans la base des serveurs.



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`.



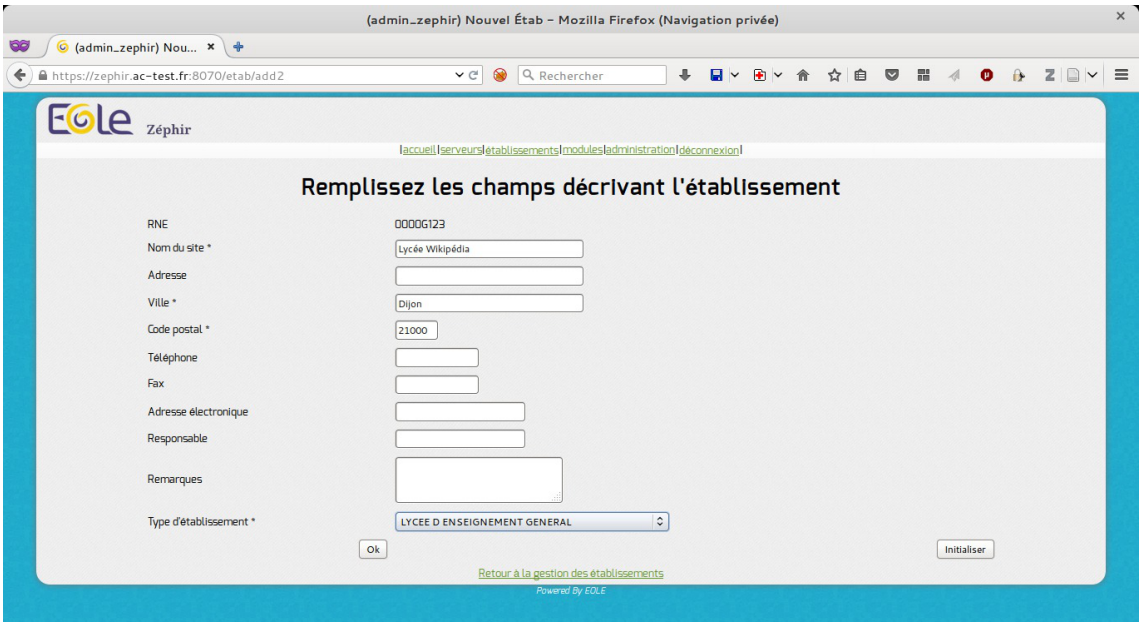
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.514]) CSV[p.498] 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

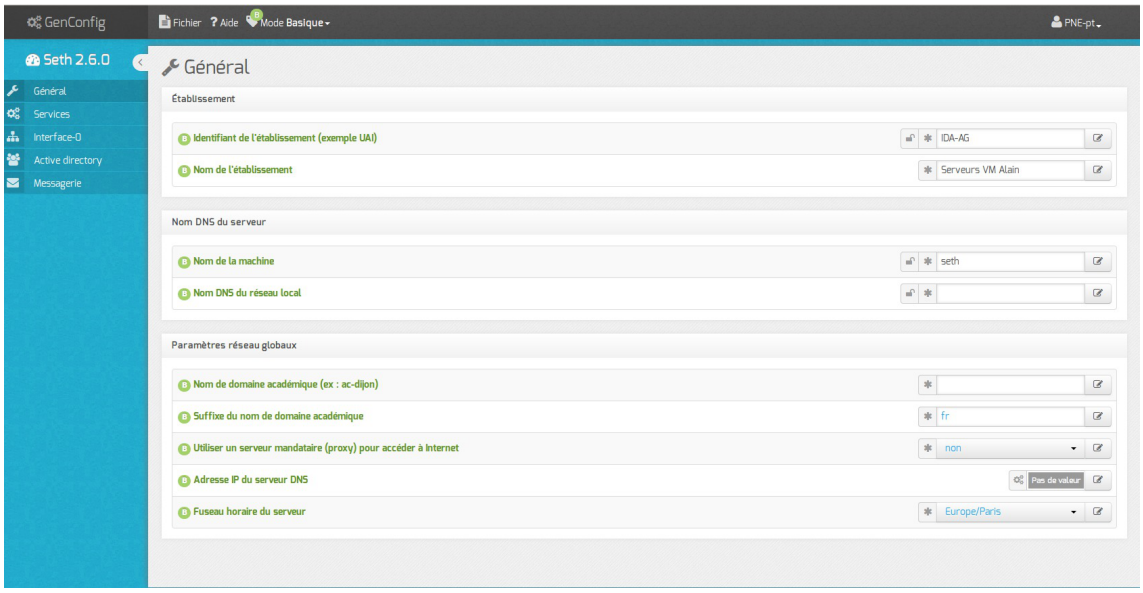
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode normal de l'interface de configuration du module.

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

- `Général` ;
- `Services` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Dhcp` * ;
- `Directeur bareos` ** ;
- `Active Directory` ;
- `Messagerie`.

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

** Certains onglets ne sont disponibles qu'après installation manuelle d'un paquet.

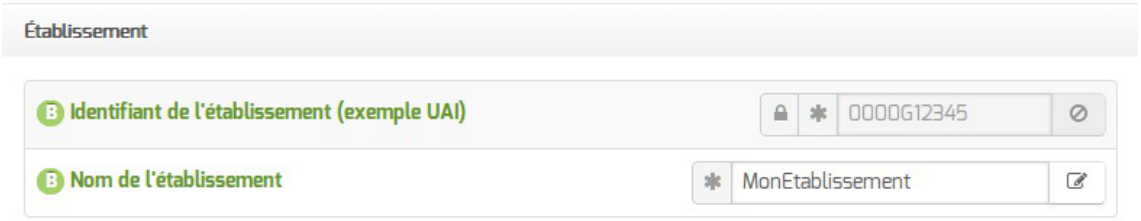


2.1. Onglet Général

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

Informations sur l'établissement

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



Deux informations sont importantes pour l'établissement :

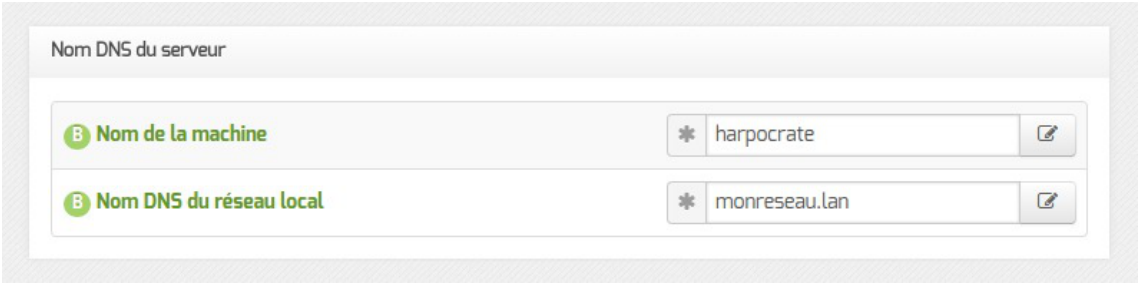
- l'`Identifiant de l'établissement`, qui doit être unique ;
- le `Nom de l'établissement`.

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

Sur les modules fournissant un annuaire LDAP[p.505] 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 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.

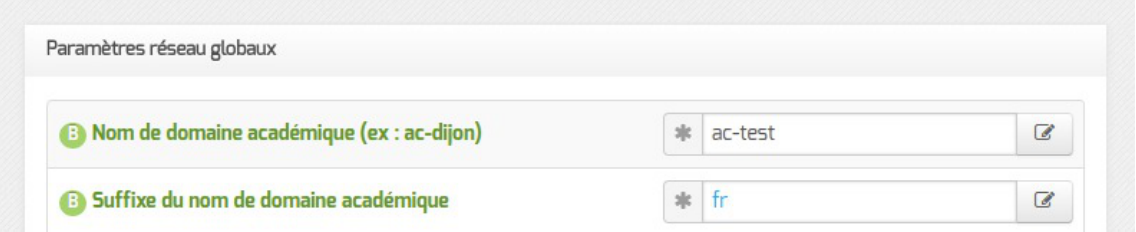
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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

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.

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

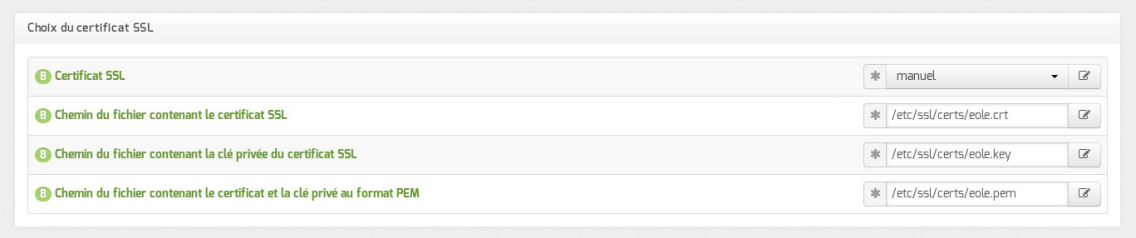
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

IP du ou des serveur(s) de noms DNS[p.499].

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.
>
> 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.520] :

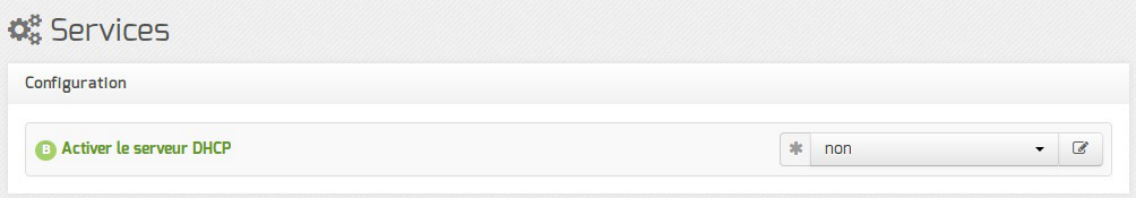
- `autosigné` : le certificat est généré localement et signé par une CA[p.494] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.506] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour se faire, il faut disposer au préalable 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 Services

Configuration

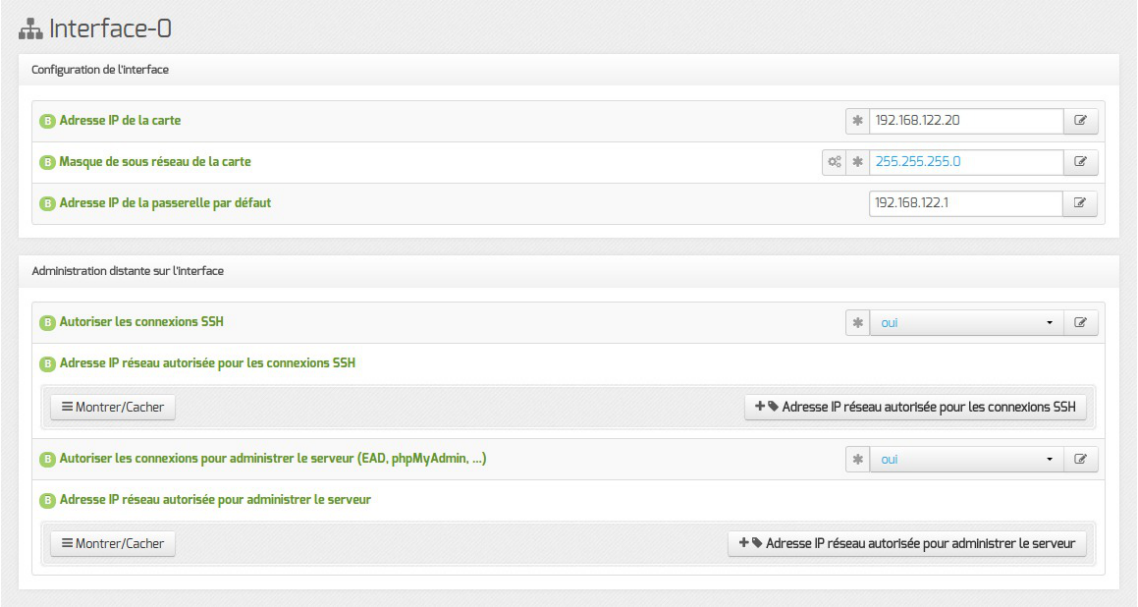
En mode basique seul le service DHCP est activable.



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

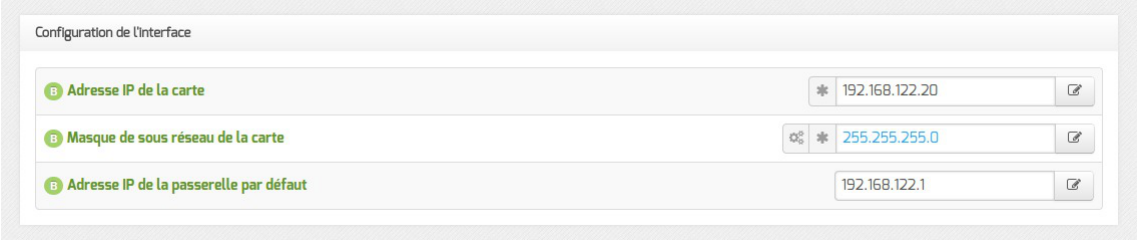
2.3. Onglet Interface-0

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



Vue de l'onglet Interface-n

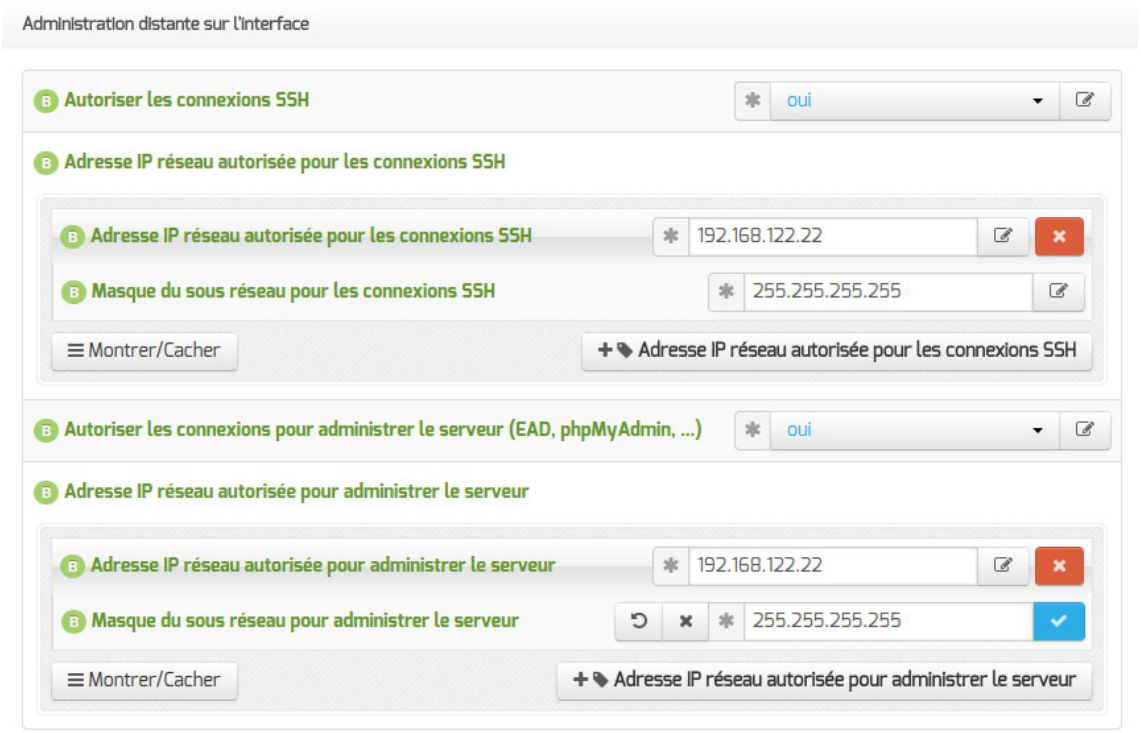
Configuration de l'interface



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

Administration à distance

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

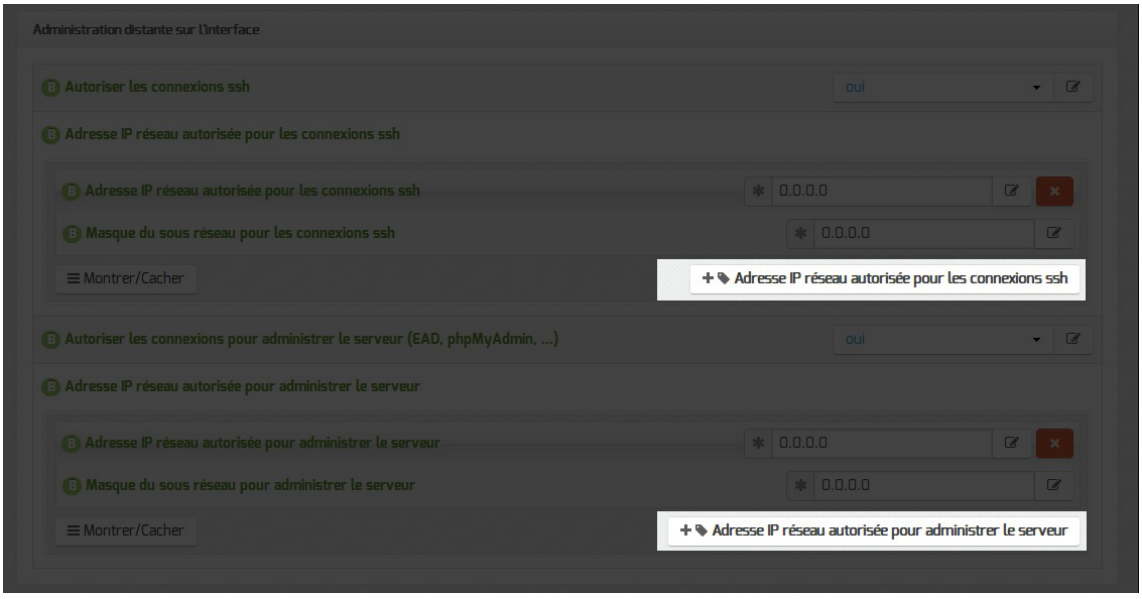


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.518] 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.

2.4. Onglet Dhcp : Configuration du serveur DHCP

Le serveur DHCP[p.498] est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option : `Activer le serveur DHCP`.

L'onglet `Dhcp` apparaît uniquement il le service est activé.

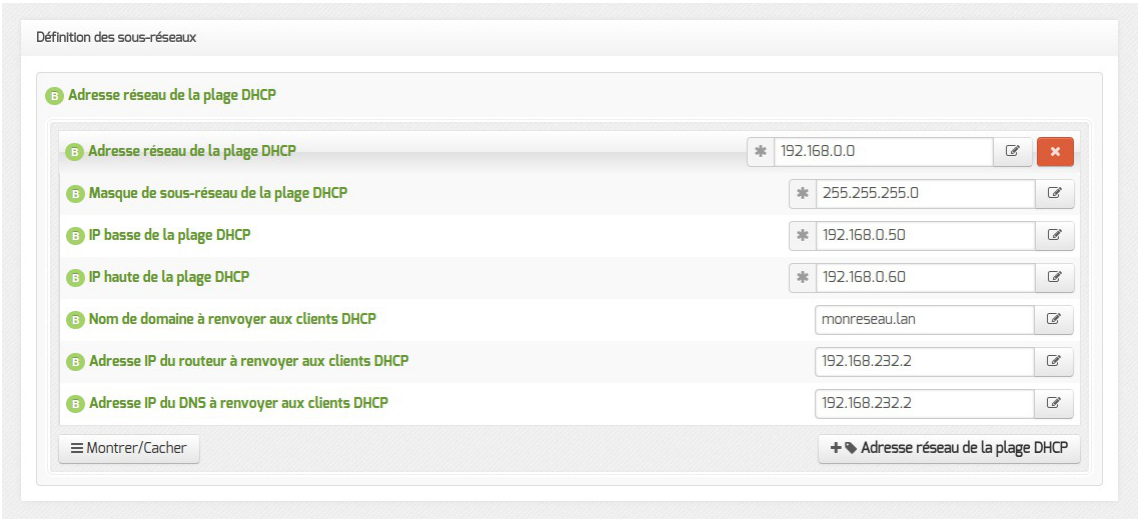
Sur les modules Seth, Horus, Scribe et Eclair (mode une carte), les adresses servies doivent généralement être sur le réseau local (interface 0).

Sur les modules AmonEcole et AmonEcole-Eclair, les adresses servies sont celles du réseau interne (interface 1).

Si le serveur est installé en DMZ, on pourra renseigner des adresses d'un autre réseau mais dans ce cas, il faudra activer le relayage du DHCP[p.515] sur le pare-feu.

Définition des sous-réseaux

Il faut définir une ou plusieurs plages (en anglais range) d'adresses attribuables par le serveur à l'aide du bouton `+ Adresse réseau de la plage DHCP`.



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

La plage DHCP doit contenir au moins autant d'adresses que le nombre de stations susceptibles d'être connectées simultanément sur le réseau.

Les champs `Adresse réseau de la plage DHCP` et `Masque de sous-réseau de la plage DHCP` permettent de définir le réseau sur lequel les adresses doivent être servies.

Le champ `Nom de la plage DHCP`, disponible uniquement à partir de la version 2.6.2, permet d'identifier plus facilement la plage DHCP, notamment dans la nouvelle interface d'administration (EAD3). Pour administrer efficacement le DHCP dans l'interface de configuration, il convient de renseigner des noms de plages pertinents. Dans le cas d'une migration depuis une version antérieure d'EOLE, cette variable est arbitrairement initialisée avec les valeurs "plage0", "plage1"...

Les champs `IP basse de la plage DHCP` et `IP haute de la plage DHCP` doivent être comprise dans le réseau déclaré ci-dessus.

Le champ `IP basse de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus petite.

Le champ `IP haute de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus grande.

Le nombre d'adresses IP servies est déterminé par la différence entre la valeur la plus grande et la valeur la plus petite.

Les champs `Nom de domaine à renvoyer aux clients DHCP`, `Adresse IP du routeur à renvoyer aux clients DHCP` et `Adresse IP du DNS à renvoyer aux clients DHCP` permettent de spécifier des valeurs différentes pour chaque plage déclarée.

Pour la configuration de l'`Adresse IP du routeur à renvoyer aux clients DHCP` :

- dans le mode une carte, l'adresse sera l'adresse IP de la passerelle saisie dans l'onglet `Interface-0` ;
- dans le cas du mode deux cartes, l'adresse IP du routeur sera l'adresse IP de l'`Interface-1` (`eth1`).

L'`Adresse IP du DNS à renvoyer aux clients DHCP` peut être l'adresse IP du DNS de votre FAI[p.501] pour une utilisation sans le module Amon. Il est également possible d'utiliser des serveurs DNS disponibles sur Internet.

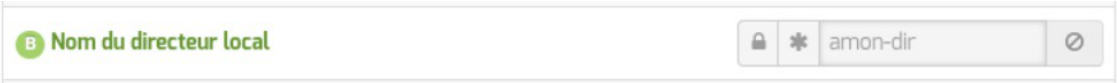
Si vous disposez d'un module Amon ou d'un module AmonEcole, il est conseillé d'utiliser le module comme relais DNS[p.499], L'adresse à préciser dans le cas du mode deux cartes sera l'adresse IP du routeur et donc l'adresse IP de l'`Interface-1` (`eth1`).



Sur le module AmonEcole, l'adresse IP du DNS à renvoyer correspond à celle renseignée dans `Adresse IP pour le proxy (adresse ip eth1 proxy link)` de l'onglet `Interface-1` de l'interface de configuration du module.

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

2.5. Onglet Directeur Bareos



Le nom du directeur est une information importante, il est utilisé en interne dans le logiciel mais, surtout, il est nécessaire pour configurer un client Bareos ou pour joindre le serveur de stockage depuis un autre module.

À l'enregistrement du fichier de configuration il ne sera plus possible de modifier le nom du directeur, en effet cette variable est utilisée dans les noms des fichiers de sauvegarde.

2.6. Onglet Active Directory

La fonctionnalité Active Directory est assurée par le logiciel Samba 4[p.516] en mode Active Directory.

Depuis la version 4.4.6 de Samba, la personnalisation du calcul des identifiants pose problème sur un contrôleur de domaine :

https://wiki.samba.org/index.php/Updating_Samba#Failure_To_Access_Shares_on_Domain_Controllers

À partir de la version 2.6.1 d'EOLE, le module Seth utilise la version 4.5 de Samba.

Cette version de samba permet notamment la prise en compte de plusieurs DNS Forwarders[p.499] :

https://wiki.samba.org/index.php/Samba_4.5_Features_added/changed#Multiple_DNS_Forwarders_on_

Ainsi, la liste complète des serveurs DNS renseignés dans l'interface de configuration du module est prise en compte (et plus seulement le premier de la liste).

À partir de la version 2.6.2 d'EOLE, le module Seth utilise la version 4.7 de Samba.

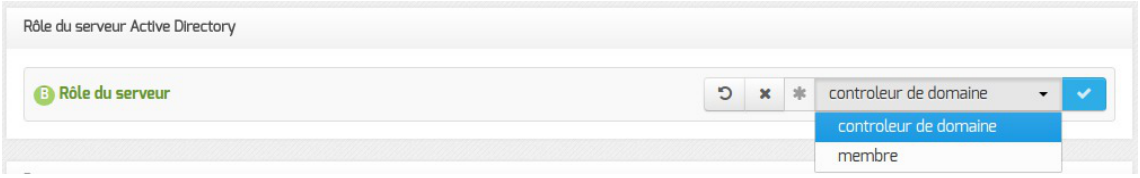
Cette version est la première à supporter officiellement le RODC[p.515]. Pour un contrôleur de domaine additionnel, l'activation de ce paramètre est accessible en mode expert.



À partir d'EOLE 2.6.2, l'instance échoue si la version de Samba installée sur le module n'est pas celle attendue.

Les paquets `samba` doivent impérativement être mis à jour via Maj-Auto avant l'instance.

Rôle du serveur Active Directory



Cette variable permet de choisir le Rôle du serveur :

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

- contrôleur de domaine ;
- serveur membre d'un domaine existant.

Dans le cas où le serveur à mettre en place a le rôle de contrôleur de domaine, il faut définir si celui-ci est le contrôleur de domaine principal ou si il s'agit d'un contrôleur additionnel.

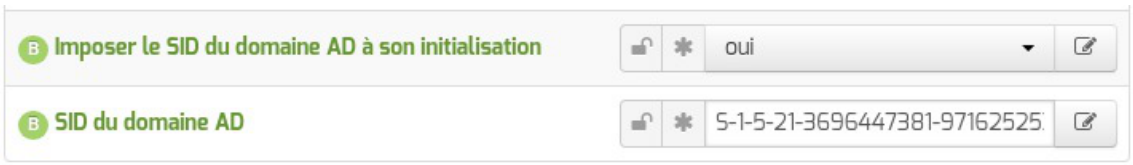


Imposer le SID du domaine AD à son initialisation

Dans le cas d'une migration ou d'une réinstallation d'un contrôleur de domaine principal, il est possible de forcer le SID[p.517] à utiliser pour le domaine.

À partir de la version 2.6.2, forcer le SID s'effectue en deux temps :

- en passant la variable `Imposer le SID du domaine AD à son initialisation` à `oui` ;
- en renseignant la variable `SID du domaine AD`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.

La prise en compte du SID forcé est réalisée lors de l'initialisation de l'annuaire Active Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le SID n'est pas validé au moment de la saisie. Il est nécessaire de s'assurer qu'il est correct avant de sauvegarder.

Forcer le positionnement dans un site AD à l'initialisation

À partir de la version 2.6.2, il est possible de demander à ce qu'un contrôleur de domaine additionnel soit rattaché à un site Active Directory particulier.

Cette demande s'effectue en deux temps :

- en passant la variable `Forcer le positionnement de ce contrôleur de domaine dans un site existant` à `oui` ;
- en renseignant la variable `Site de destination de ce contrôleur de domaine`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.

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

La prise en compte du domaine de rattachement est réalisée lors de l'initialisation de l'annuaire Active Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le site doit impérativement avoir été déclaré au préalable sur le contrôleur de domaine principal.

Si le contrôleur de domaine principal est un module Seth, la déclaration d'un site s'effectue facilement grâce à la fonction bash `samba_update_site` :

```
. /usr/lib/eole/samba4.sh
samba_update_site monsite 10.1.1.0/24
```

Partage de fichiers

Les partages utilisateur et les autres répertoires partagés peuvent être locaux et/ou hébergés sur d'autres serveurs Active Directory.

Sur le serveur local, il est possible d'activer ou non l'hébergement des partages « homes » et « profiles » des utilisateurs.



2.7. Onglet Messagerie

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

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

- `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.

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.

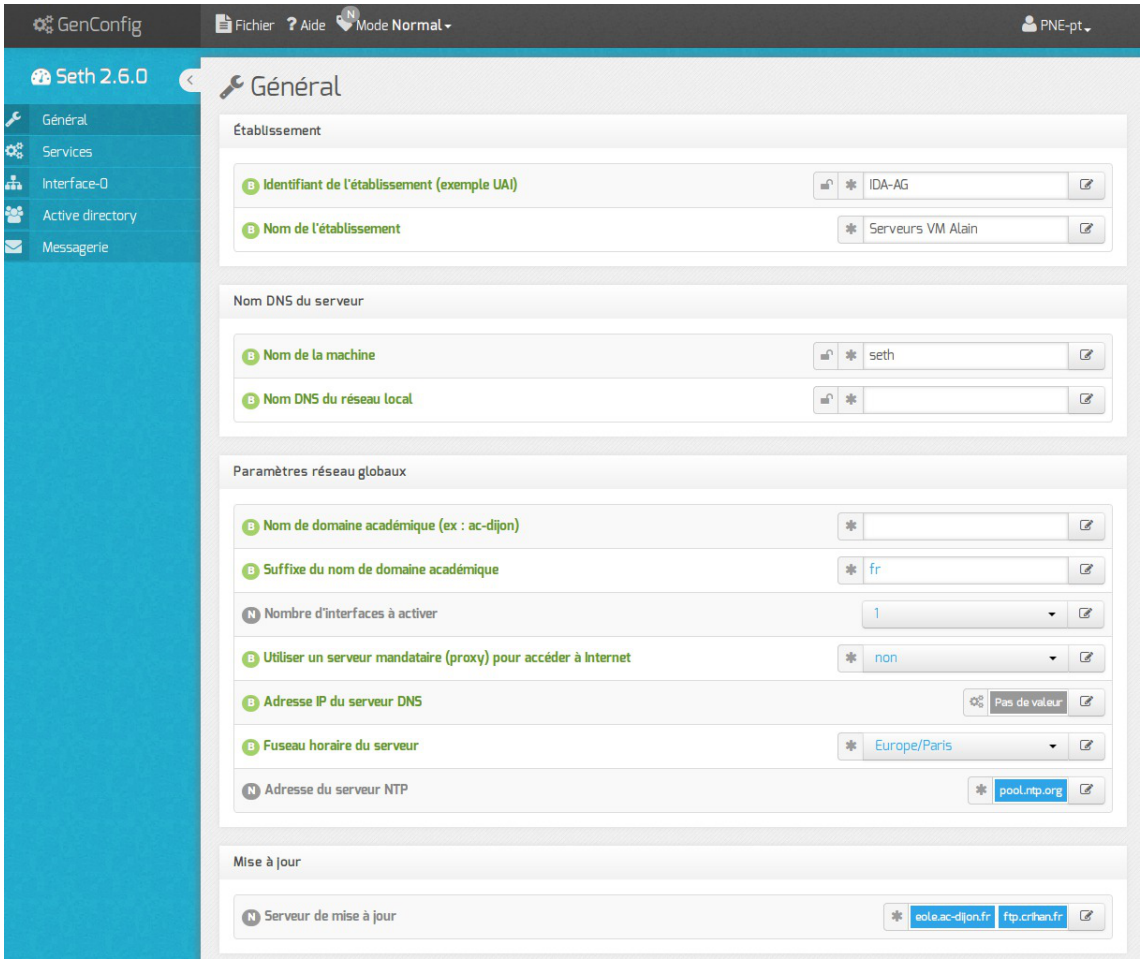
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

- Général ;
- Services ;
- Interface-0 (configuration de l'interface réseau) ;
- Clamav ** ;
- Dhcp * ;
- Onduleur * ;
- Directeur bareos ** ;
- Stockage bareos ** ;
- Nginx ;
- Reverse proxy * ;
- Active Directory ;
- Messagerie.

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

** Certains onglets ne sont disponibles qu'après installation manuelle d'un paquet.

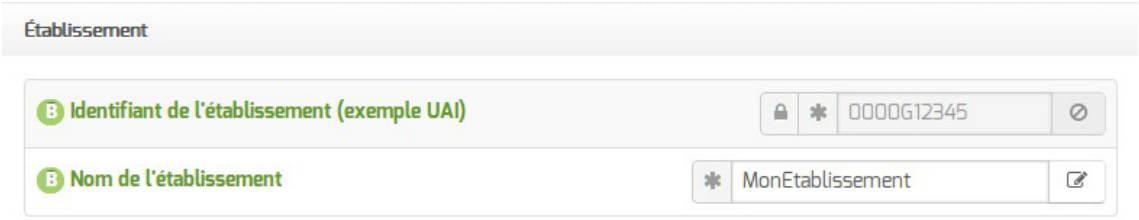


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

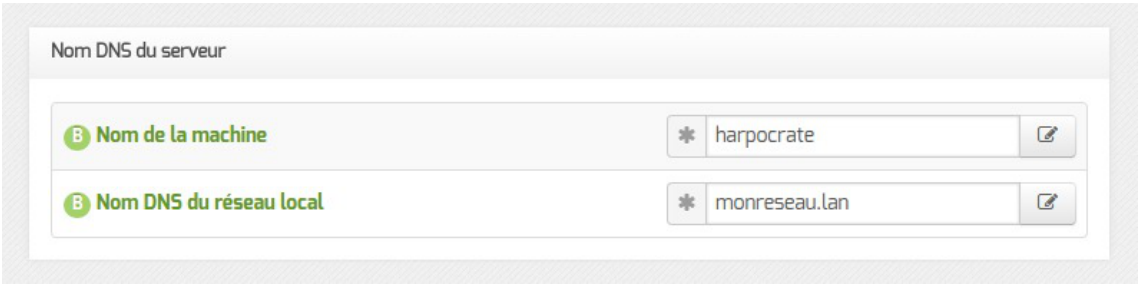
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.505] 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.

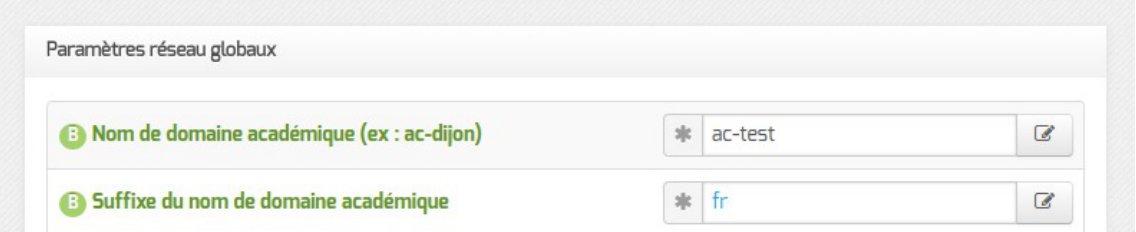
Les domaines de premier niveau `.com`, `.fr` sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

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



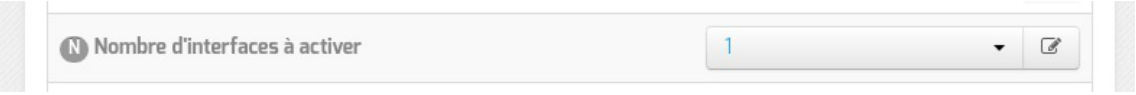
En deuxième lieu, il convient de configurer les noms de domaine de la machine.

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`.



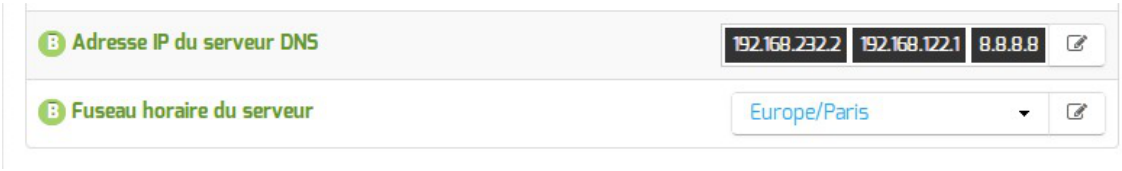
Il devient alors possible de saisir la configuration du serveur proxy :

- 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.

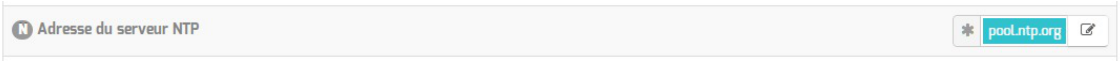
DNS et fuseau horaire



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.499].

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

NTP

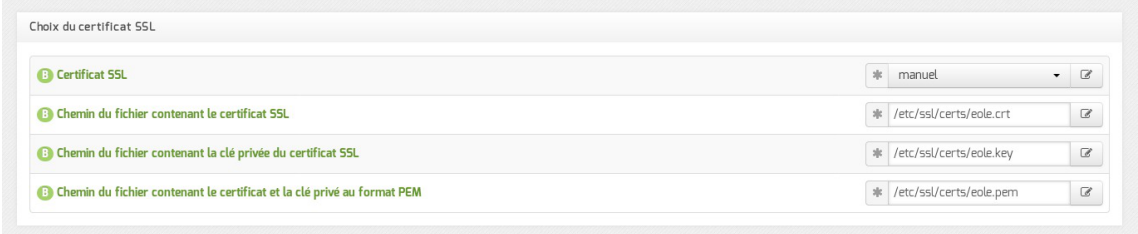


Une valeur par défaut est attribuée pour le serveur de temps NTP[p.511]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

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)

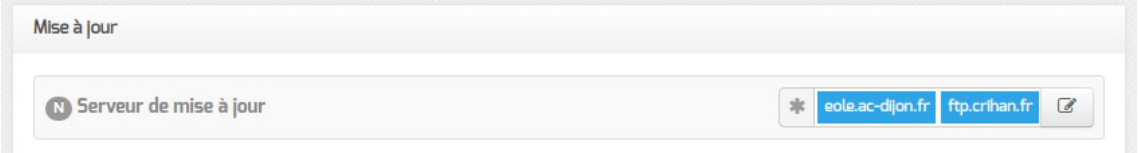
Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.520] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.494] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.506] ;
- `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 [p.316]

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.

Configuration

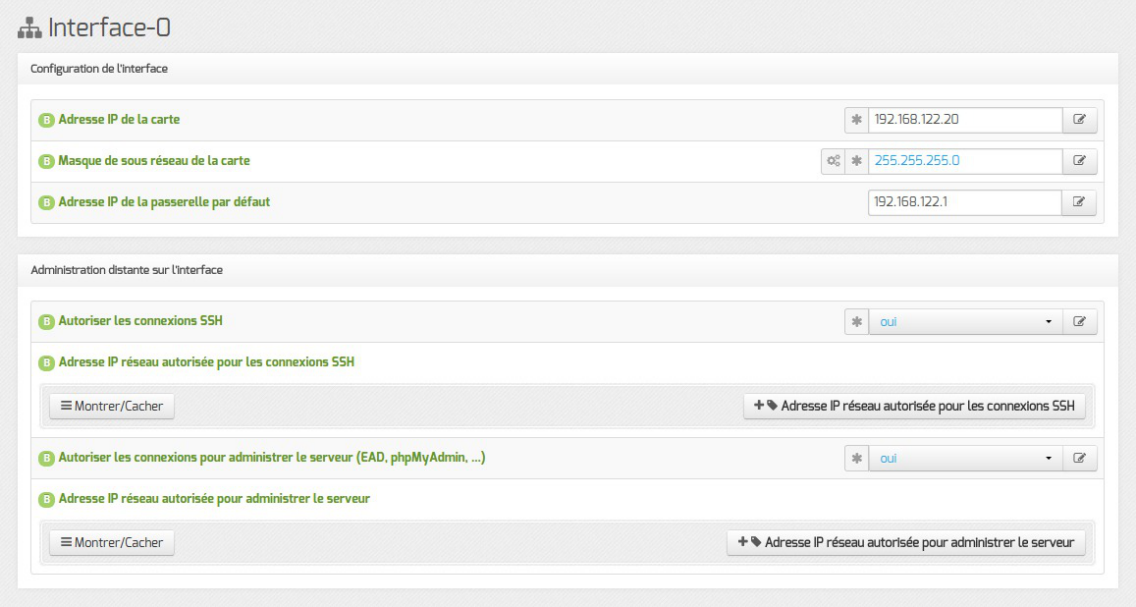


En mode normal, le service de gestion des onduleurs est présent, Celui-ci est commun à tous les modules.

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

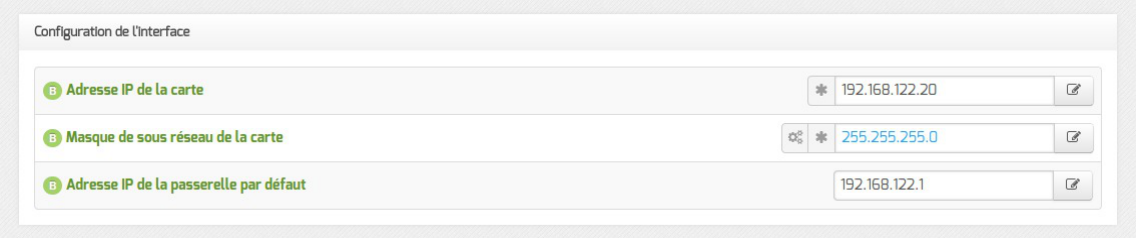
3.3. Onglet Interface-0

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



Vue de l'onglet Interface-n

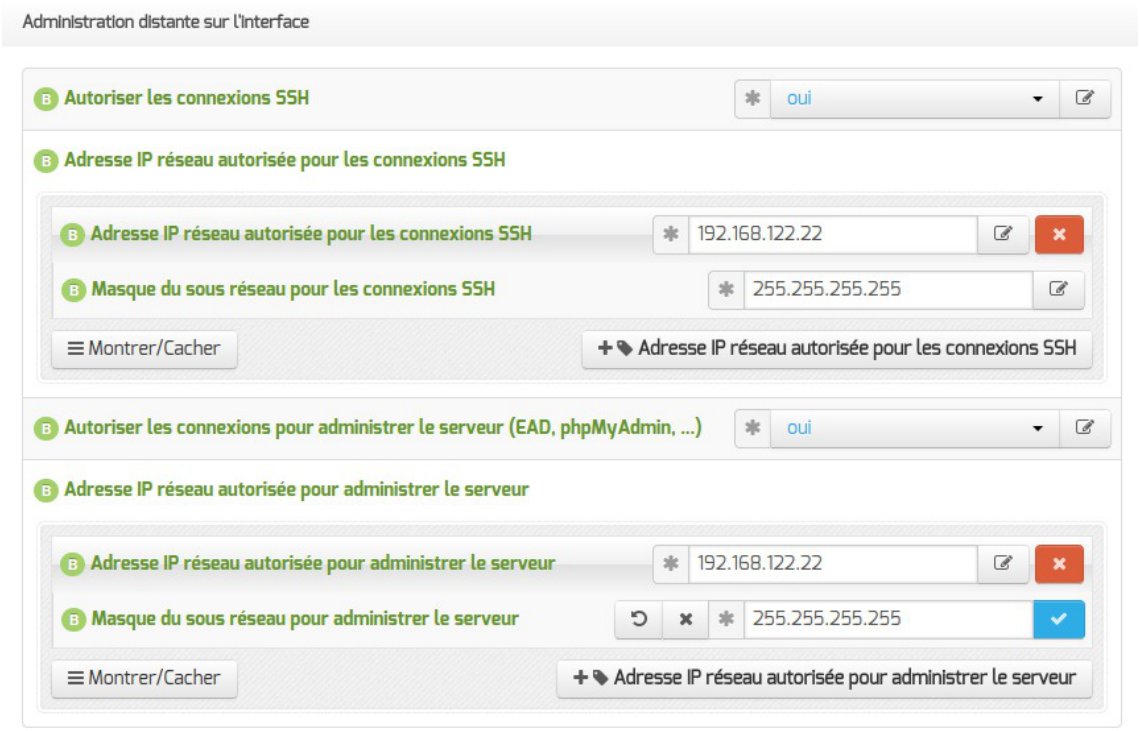
Configuration de l'interface



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

Administration à distance

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

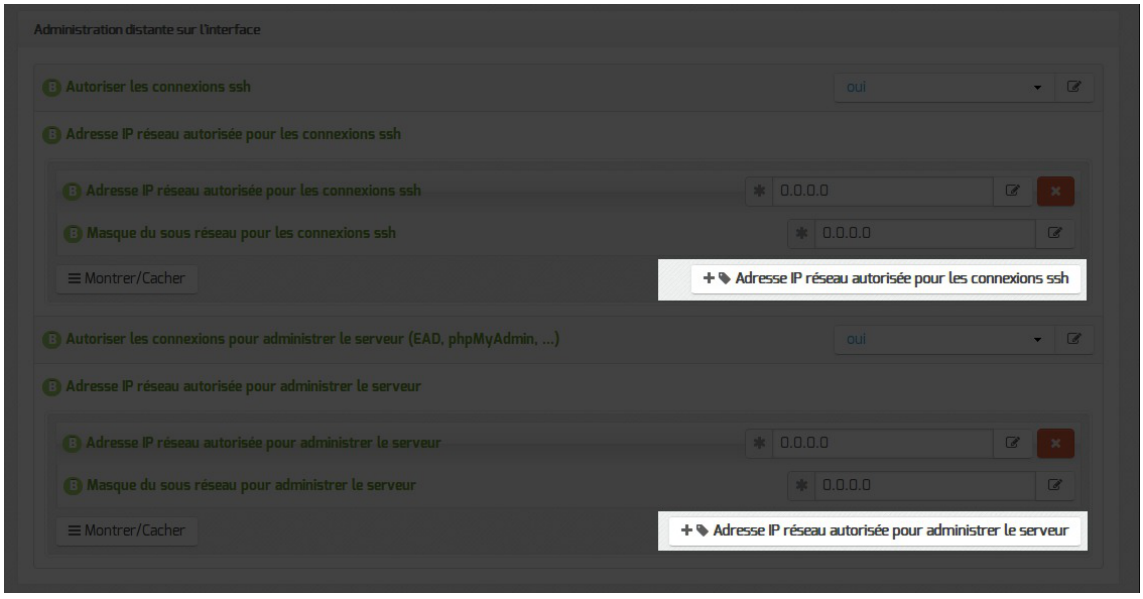


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.518] 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)

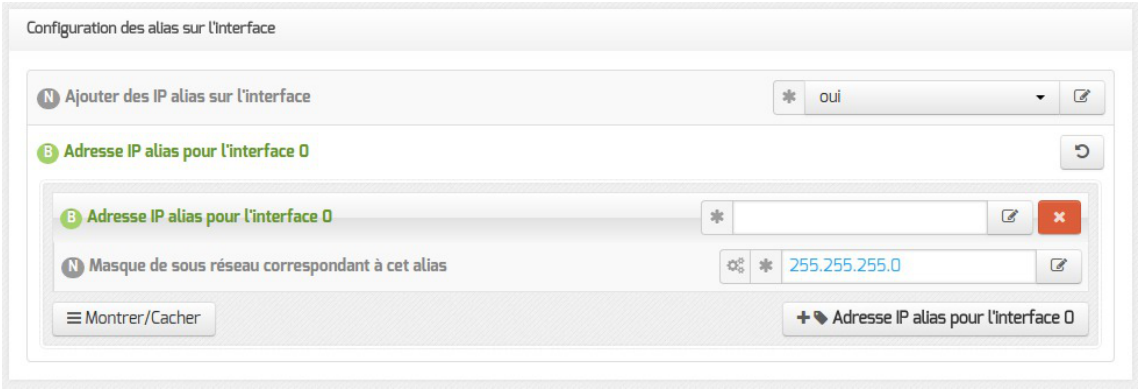
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

> 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.



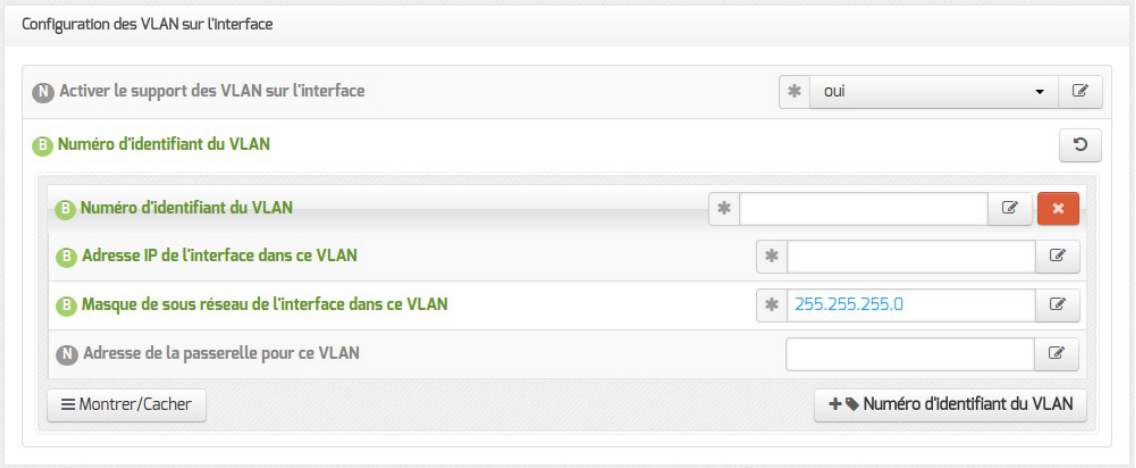
Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

> 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.522] (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.

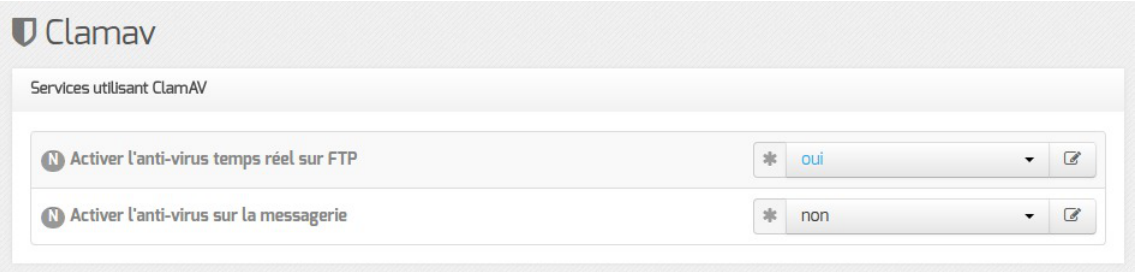
Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.

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

3.4. Onglet Clamav : Configuration de l'anti-virus

EOLE propose un service anti-virus réalisé à partir du logiciel libre ClamAV.
http://www.clamav.net

Activation de l'anti-virus



Par défaut, le service est activé sur le module et l'anti-virus est actif sur certains services :

- le service FTP ;
- le service de messagerie.

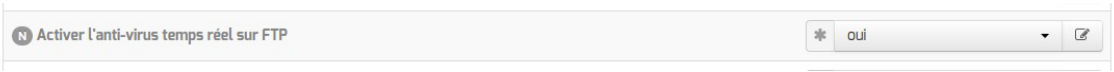
Si aucun service n'utilise l'anti-virus, il est utile de le désactiver dans l'onglet `Services`. Il faut

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

> passer la variable `Activer l'anti-virus ClamAV` à `non`. L'onglet `Clamav` n'est alors plus visible.

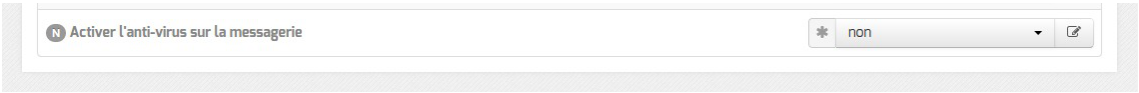
Activation de l'anti-virus sur FTP

Pour désactiver l'anti-virus en temps réel sur les fichiers mis en ligne par FTP il faut passer la variable `Activer l'anti-virus temps réel sur FTP` à `non` dans l'onglet `Clamav`.



Activation de l'anti-virus sur la messagerie

Pour désactiver l'anti-virus sur la messagerie il faut passer la variable `Activer l'antivirus sur la messagerie` à `non` dans l'onglet `Clamav`.



Contribuer

La base de données de virus est mise à jour avec l'aide de la communauté.
Il est possible de faire des signalements :

- signaler de nouveaux virus qui ne sont pas détectés par ClamAV ;
- signaler des fichiers propres qui ne sont pas correctement détectés par ClamAV (faux-positif).

Pour cela il faut utiliser le formulaire suivant (en) : http://www.clamav.net/contact#reports
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.
En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.

> Il ne faut pas signaler des PUA[p.514] comme étant des faux positifs.

3.5. Onglet Dhcp : Configuration du serveur DHCP

Le serveur DHCP[p.498] est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option : `Activer le serveur DHCP`.
L'onglet `Dhcp` apparaît uniquement il le service est activé.

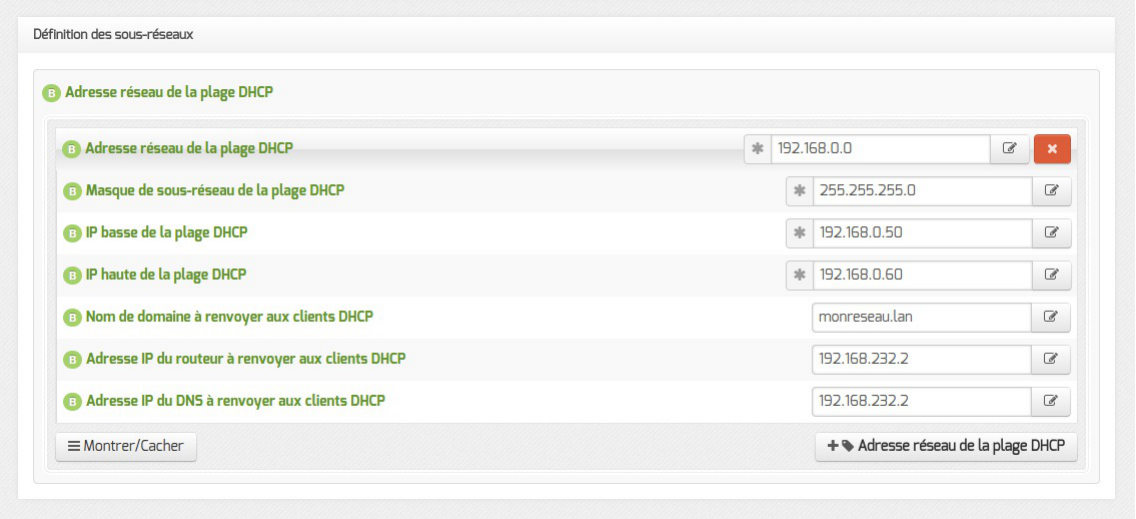
Sur les modules Seth, Horus, Scribe et Eclair (mode une carte), les adresses servies doivent généralement être sur le réseau local (interface 0).
Sur les modules AmonEcole et AmonEcole-Eclair, les adresses servies sont celles du réseau interne (interface 1).

Si le serveur est installé en DMZ, on pourra renseigner des adresses d'un autre réseau mais dans ce cas, il faudra activer le relayage du DHCP[p.515] sur le pare-feu.

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

Définition des sous-réseaux

Il faut définir une ou plusieurs plages (en anglais range) d'adresses attribuables par le serveur à l'aide du bouton `+ Adresse réseau de la plage DHCP`.



La plage DHCP doit contenir au moins autant d'adresses que le nombre de stations susceptibles d'être connectées simultanément sur le réseau.

Les champs `Adresse réseau de la plage DHCP` et `Masque de sous-réseau de la plage DHCP` permettent de définir le réseau sur lequel les adresses doivent être servies.

Le champ `Nom de la plage DHCP`, disponible uniquement à partir de la version 2.6.2, permet d'identifier plus facilement la plage DHCP, notamment dans la nouvelle interface d'administration (EAD3). Pour administrer efficacement le DHCP dans l'interface de configuration, il convient de renseigner des noms de plages pertinents. Dans le cas d'une migration depuis une version antérieure d'EOLE, cette variable est arbitrairement initialisée avec les valeurs "plage0", "plage1"...

Les champs `IP basse de la plage DHCP` et `IP haute de la plage DHCP` doivent être comprise dans le réseau déclaré ci-dessus.

Le champ `IP basse de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus petite.

Le champ `IP haute de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus grande.

Le nombre d'adresses IP servies est déterminé par la différence entre la valeur la plus grande et la valeur la plus petite.

Les champs `Nom de domaine à renvoyer aux clients DHCP`, `Adresse IP du routeur à renvoyer aux clients DHCP` et `Adresse IP du DNS à renvoyer aux clients DHCP` permettent de spécifier des valeurs différentes pour chaque plage déclarée.

Pour la configuration de l'`Adresse IP du routeur à renvoyer aux clients DHCP` :

- dans le mode une carte, l'adresse sera l'adresse IP de la passerelle saisie dans l'onglet `Interface-0` ;
- dans le cas du mode deux cartes, l'adresse IP du routeur sera l'adresse IP de l'`Interface-1` (`eth1`).

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

L'`Adresse IP du DNS à renvoyer aux clients DHCP` peut être l'adresse IP du DNS de votre FAI[p.501] pour une utilisation sans le module Amon. Il est également possible d'utiliser des serveurs DNS disponibles sur Internet.

Si vous disposez d'un module Amon ou d'un module AmonEcole, il est conseillé d'utiliser le module comme relais DNS[p.499], L'adresse à préciser dans le cas du mode deux cartes sera l'adresse IP du routeur et donc l'adresse IP de l'`Interface-1` (`eth1`).



Sur le module AmonEcole, l'adresse IP du DNS à renvoyer correspond à celle renseignée dans `Adresse IP pour le proxy (adresse ip eth1 proxy link)` de l'onglet `Interface-1` de l'interface de configuration du module.

Configurer la continuité de service

À partir de la version 2.6.2, il est possible de mettre en place de la continuité de service pour le DHCP.

Elle permet à deux serveurs DHCP d'opérer sur les mêmes sous-réseaux et mêmes pools d'adresses IP.

Il faut donc un serveur DHCP primaire et un serveur DHCP secondaire.



Les ports d'écoute et de contact du serveur primaire doivent être inversés pour le serveur secondaire. Il est également possible d'utiliser le port 647 partout, c'est à dire en écoute et en contact aussi bien sur le serveur primaire que sur le serveur secondaire.

Paramétrage du serveur primaire

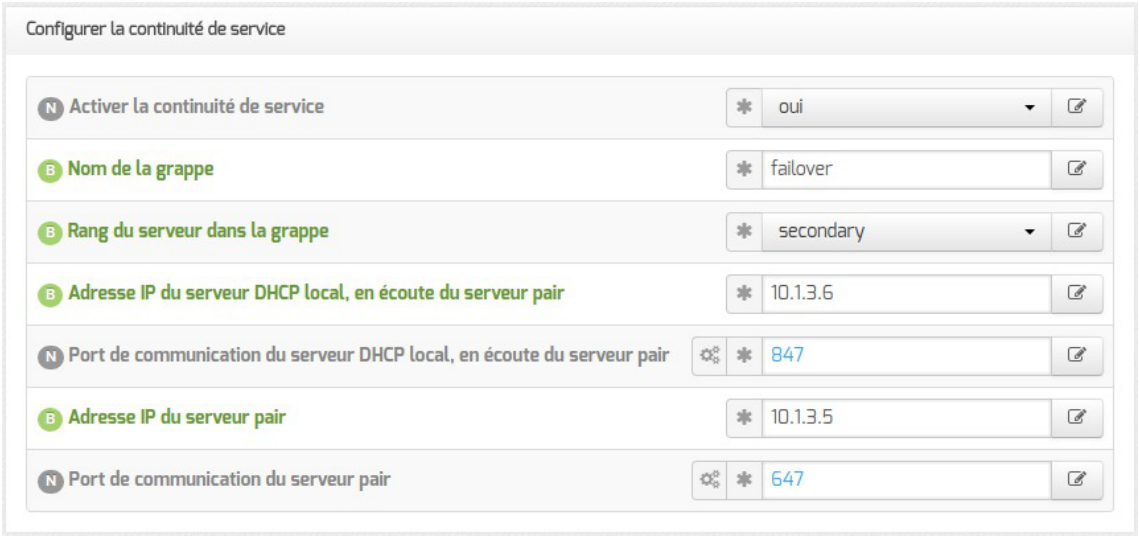


- `Nom de la grappe` : le nom de la grappe devra être le même sur le serveur primaire (local) et sur le serveur secondaire (pair) ;
- `Rang du serveur dans la grappe` : choisir `primary` pour le serveur primaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de l'interface sur laquelle écoute le service DHCP local (IP de l'Interface-0 dans la plupart des cas) ;

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

- `Port de communication du serveur DHCP local, en écoute du serveur pair` : le port par défaut pour un serveur primaire est `647` ;
- `Adresse IP du serveur pair` : saisir l'adresse IP du serveur secondaire (pair) ;
- `Port de communication du serveur pair` : le port par défaut est `847`.

Paramétrage du serveur secondaire



Pour un serveur secondaire, les variables à paramétrer sont :

- `Nom de la grappe` : le nom de la grappe doit être le même que pour le serveur primaire (local) ;
- `Rang du serveur dans la grappe` : choisir `secondary` pour le serveur secondaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de l'interface sur laquelle écoute le service DHCP local (IP de l'Interface-0 dans la plupart des cas) ;
- `Port de communication du serveur DHCP local, en écoute du serveur pair` : le port par défaut pour un serveur secondaire est `847` ;
- `Adresse IP du serveur pair` : saisir l'adresse IP du serveur secondaire (pair) ;
- `Port de communication du serveur pair` : le port par défaut est `647`.

3.6. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.511]. 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)

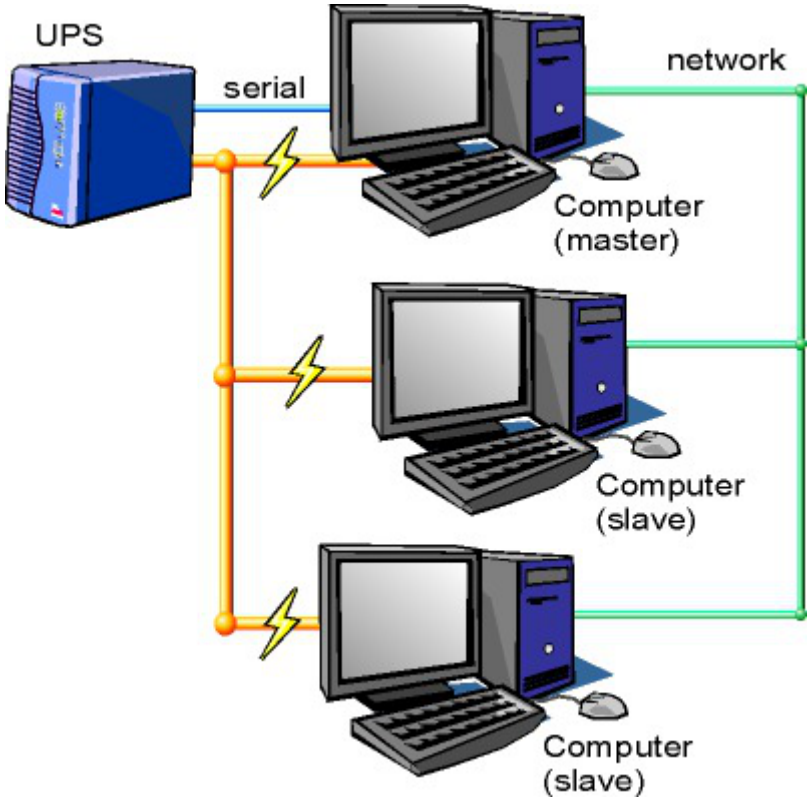


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

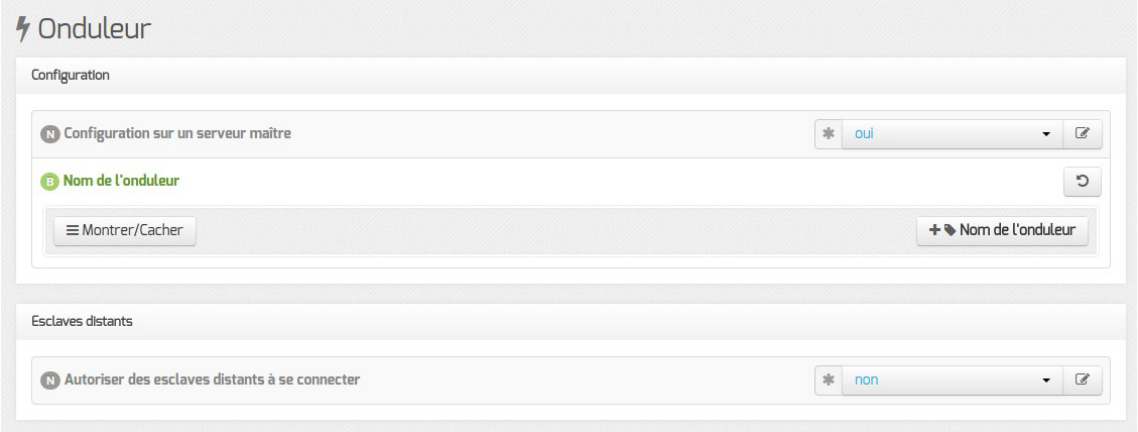
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

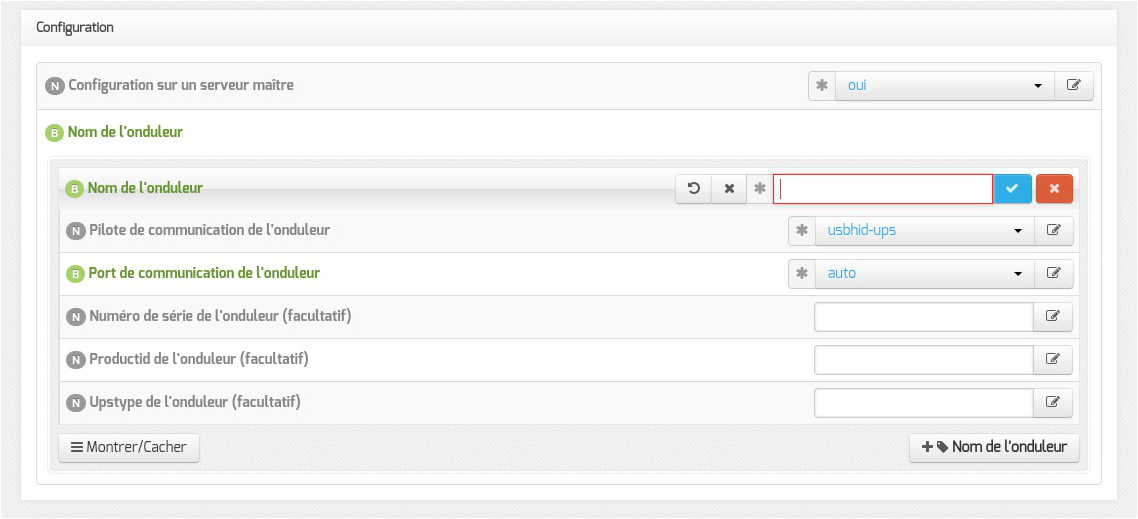
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

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)

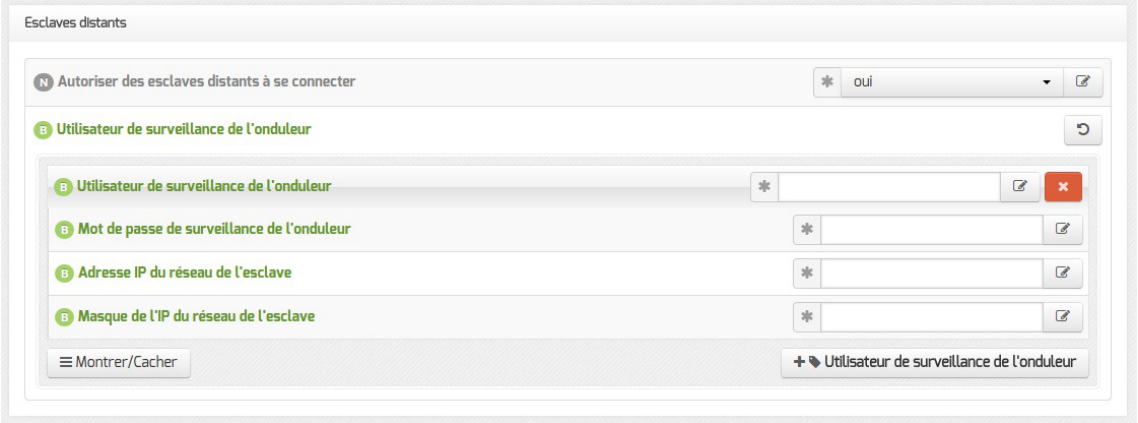
- Port de communication de l'onduleur : `auto`.

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`.

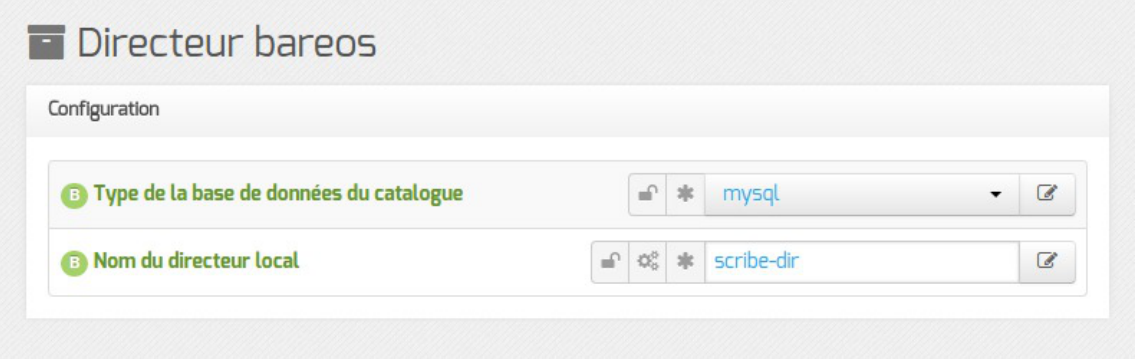
Sur le serveur esclave :

- 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`.

3.7. Onglet Directeur bareos



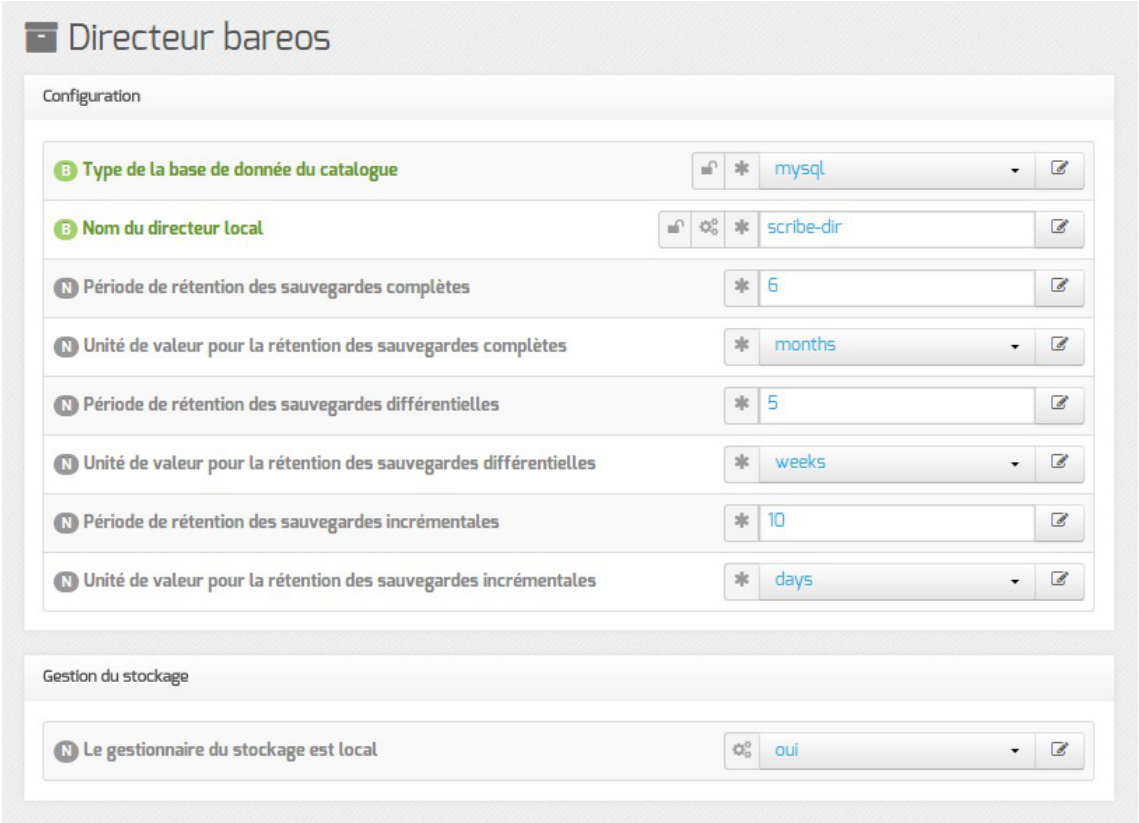
Le type de base de données permet de choisir si l'enregistrement du catalogue se fait dans MySQL ou dans SQLite. Il ne sera plus possible de modifier ce paramètre après l'enregistrement de la configuration.

Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

Le nom du directeur est une information importante, il est utilisé en interne dans le logiciel mais, surtout, il est nécessaire pour configurer un client Bareos ou pour joindre le serveur de stockage depuis un autre module.

À l'enregistrement du fichier de configuration il ne sera plus possible de modifier le nom du directeur, en effet cette variable est utilisée dans les noms des fichiers de sauvegarde.

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



Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention[p.499] des différents espaces de stockage (totale, différentielle et incrémentale).

La durée de rétention des fichiers détermine le temps de conservation avant l'écrasement.

Plus les durées de rétention sont importantes, plus l'historique sera important et plus l'espace de stockage nécessaire sera important.

Il peut être intéressant de conserver un historique long mais avec peu d'états intermédiaires.

Pour cela, voici un exemple de configuration :

- 6 mois de sauvegardes totales ;
- 5 semaines de sauvegardes différentielles ;
- 10 jours de sauvegardes incrémentales.

Avec la politique de sauvegarde suivante :

- une sauvegarde totale par mois ;
- une sauvegarde différentielle par semaine ;
- une sauvegarde incrémentale du lundi au vendredi.

Dans l'historique, il y aura donc une sauvegarde par jour de conservée pendant 10 jours, une sauvegarde par semaine pendant 5 semaines et une sauvegarde mensuelle pendant 6 mois.

Une modification de la durée de rétention en cours de production n'aura aucun effet sur les

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

sauvegardes déjà effectuées, elles seront conservées et recyclées mais sur la base de l'ancienne valeur, stockée dans la base de données.

Afin de prendre en compte la nouvelle valeur pour les sauvegardes suivantes, il faut utiliser les outils Bareos pour mettre à jour la base de données :

```
# bconsole
*update
*2
*<numéro du pool de volumes de sauvegarde>
```

Une autre solution consiste à vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et à ré-initialiser la base de données Bareos avec la commande :

```
# bareosregen.sh
La regénération du catalogue de bareos va écraser l'ancienne base, confirmez-vous ? [oui/non]
[non] : oui
```

Configuration du stockage

Le stockage peut être local ou distant, il est local par défaut.

Dans ce cas aucun paramètre n'est à configurer dans l'onglet `Directeur Bareos`.

Par contre des paramètres vous permettant éventuellement d'autoriser des directeurs à se connecter au présent stockage dans l'onglet `Stockage bareos`.



Vue de l'onglet Directeur Bareos

Dans le cas d'un serveur distant (`Activer le serveur de stockage localement` à `non`), il faut configurer l'adresse IP et le mot de passe du serveur de stockage distant.

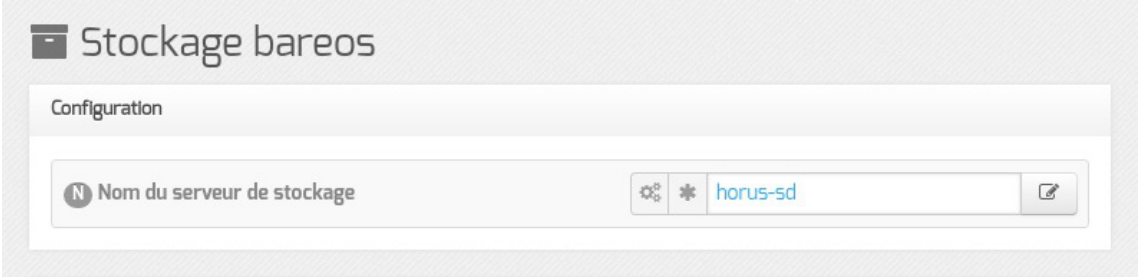
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

Le déport du service `bareos-sd` sur un autre serveur que `bareos-dir` ne permet pas de gérer correctement les verrous des tâches d'administration sur ce serveur : `bareos-dir` ne permet pas de signaler efficacement à `bareos-sd` qu'une sauvegarde est lancée et qu'il doit poser un verrou empêchant les autres tâches d'administration.

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

3.8. Onglet Stockage bareos

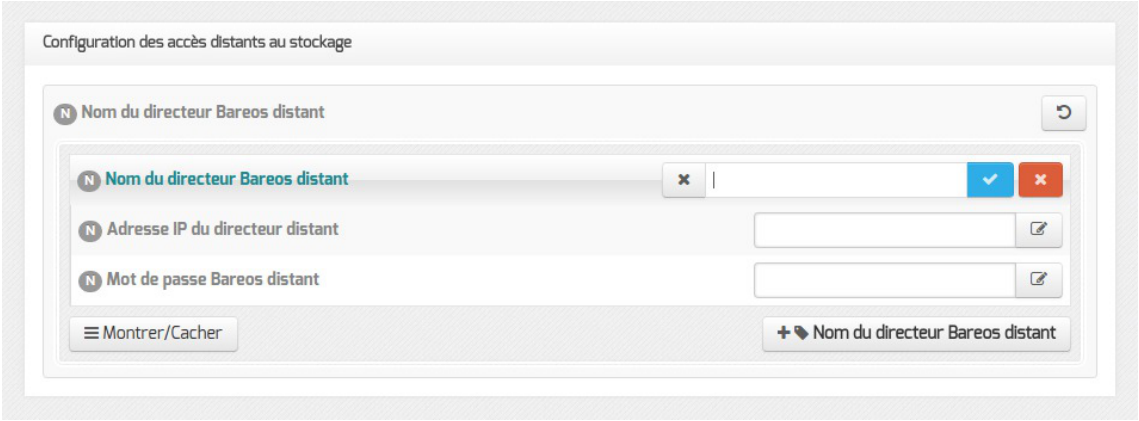
Dans l'onglet Stockage bareos il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur Nom du directeur Bareos distant, le détail de l'autorisation s'affiche.

Pour ce faire il faut se munir des paramètres du directeur distant :

- son nom ;
- son adresse IP ;
- son mot de passe.



Autoriser des clients Bareos distants à se connecter au directeur

Les sauvegardes sont des informations sensibles. Il ne faut pas utiliser de mot de passe facilement déductible.

Voir aussi...

Les mots de passe [p.229]

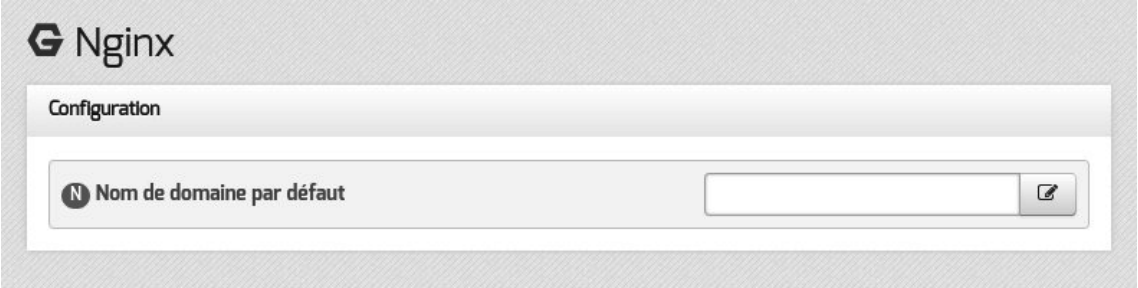
3.9. Onglet Nginx

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.

3.10. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.510].

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.499] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.518].

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.504]*/DNAT*.

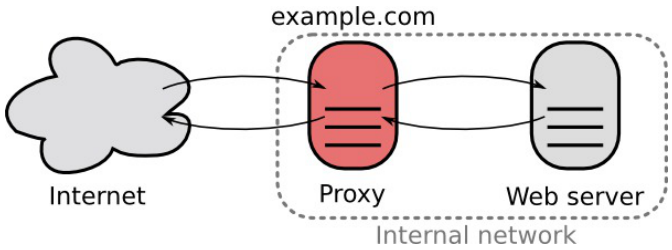
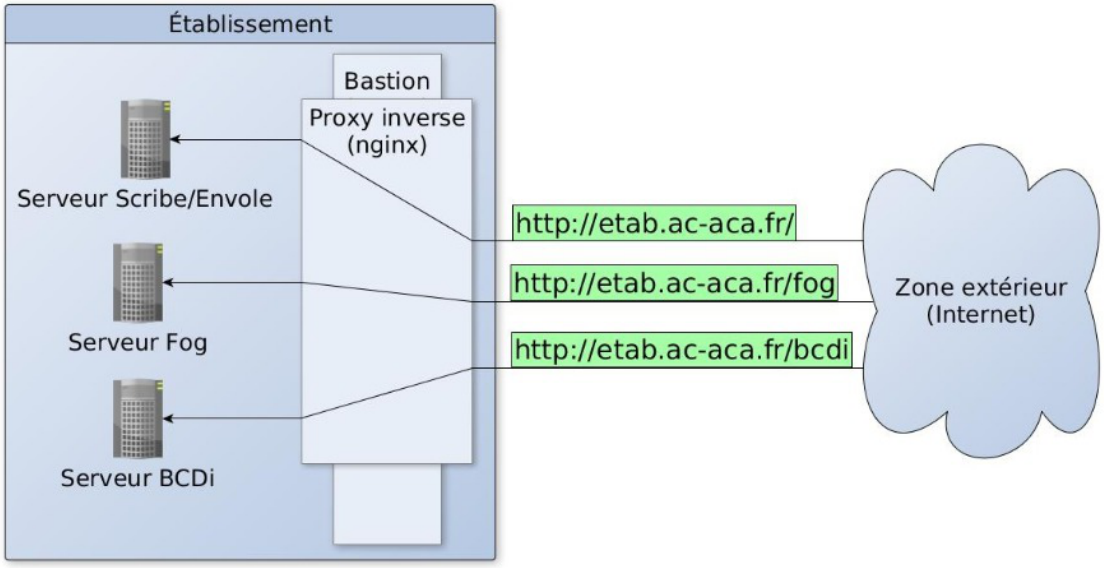


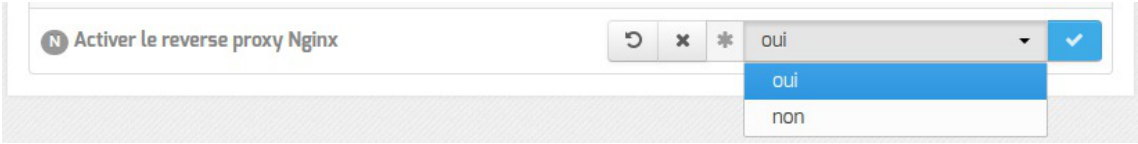
Diagramme d'un proxy inverse - Licence CC0

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

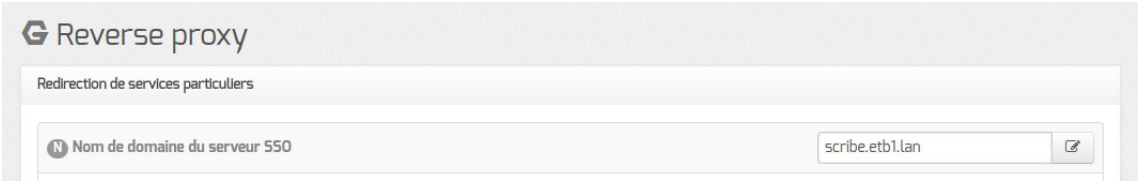
- serveur EoleSSO ;
- outil d'administration EAD[p.500] ;
- application EOP ;
- protocole HTTP[p.503] ;
- protocole HTTPS[p.503].



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

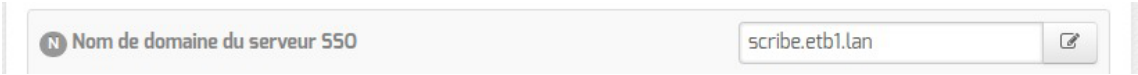


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

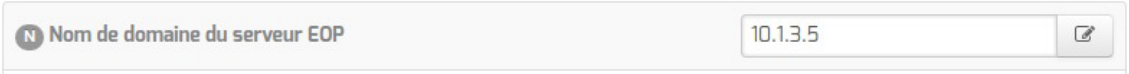
Redirection du service EoleSSO



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.522]).

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).

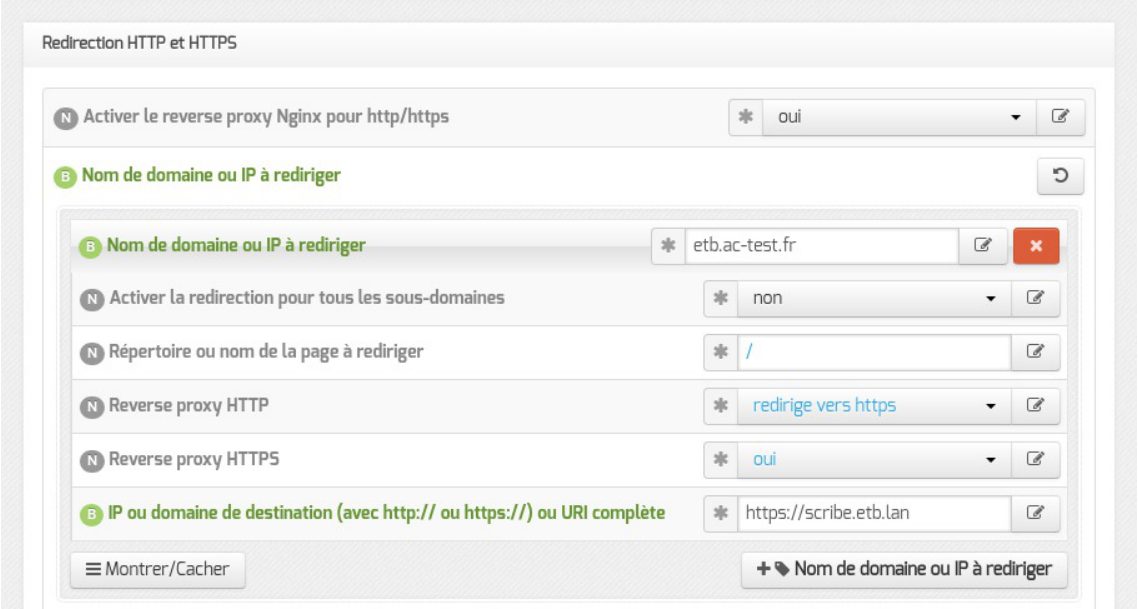
Redirection de l'interface d'administration EAD



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



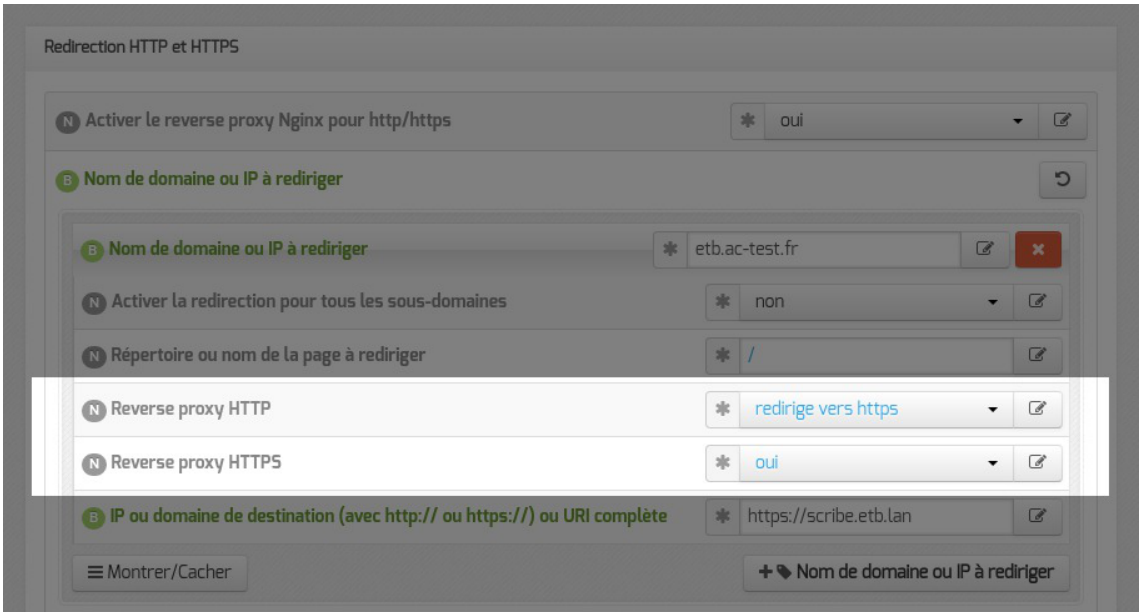
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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.521] (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.).

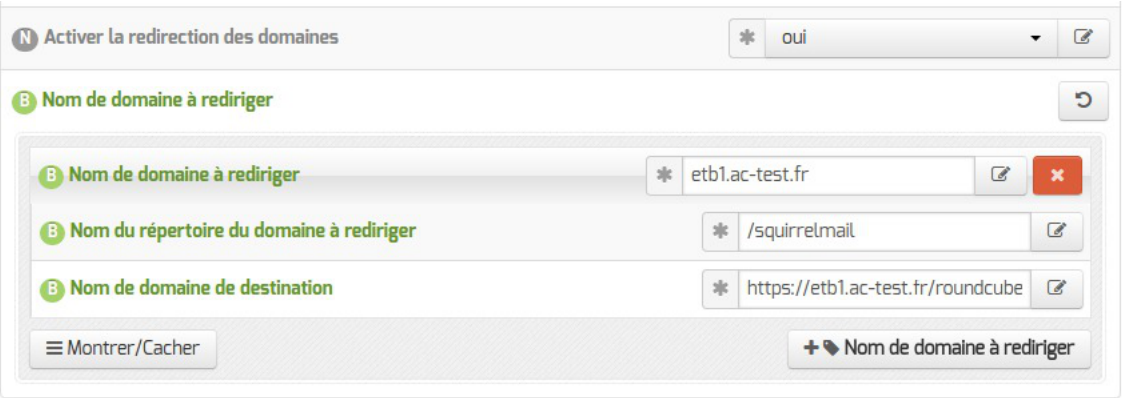
Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

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.514], `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/`.

3.11. Onglet Active Directory

La fonctionnalité Active Directory est assurée par le logiciel Samba 4[p.516] en mode Active Directory.

Depuis la version 4.4.6 de Samba, la personnalisation du calcul des identifiants pose problème sur un contrôleur de domaine :

https://wiki.samba.org/index.php/Updating_Samba#Failure_To_Access_Shares_on_Domain_Controllers

À partir de la version 2.6.1 d'EOLE, le module Seth utilise la version 4.5 de Samba.

Cette version de samba permet notamment la prise en compte de plusieurs DNS Forwarders[p.499] :

https://wiki.samba.org/index.php/Samba_4.5_Features_added/changed#Multiple_DNS_Forwarders_on_

Ainsi, la liste complète des serveurs DNS renseignés dans l'interface de configuration du module est prise en compte (et plus seulement le premier de la liste).

À partir de la version 2.6.2 d'EOLE, le module Seth utilise la version 4.7 de Samba.

Cette version est la première à supporter officiellement le RODC[p.515]. Pour un contrôleur de domaine additionnel, l'activation de ce paramètre est accessible en mode expert.



À partir d'EOLE 2.6.2, l'instance échoue si la version de Samba installée sur le module n'est pas celle attendue.

Les paquets `samba` doivent impérativement être mis à jour via Maj-Auto avant l'instance.

Rôle du serveur Active Directory

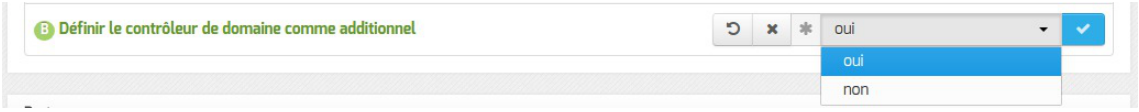
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Cette variable permet de choisir le Rôle du serveur :

- contrôleur de domaine ;
- serveur membre d'un domaine existant.

Dans le cas où le serveur à mettre en place a le rôle de contrôleur de domaine, il faut définir si celui-ci est le contrôleur de domaine principal ou si il s'agit d'un contrôleur additionnel.

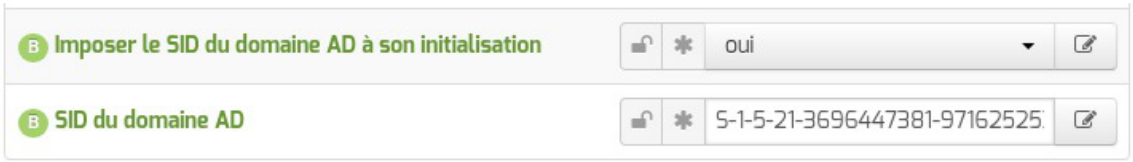


Imposer le SID du domaine AD à son initialisation

Dans le cas d'une migration ou d'une réinstallation d'un contrôleur de domaine principal, il est possible de forcer le SID[p.517] à utiliser pour le domaine.

À partir de la version 2.6.2, forcer le SID s'effectue en deux temps :

- en passant la variable `Imposer le SID du domaine AD à son initialisation` à `oui` ;
- en renseignant la variable `SID du domaine AD`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.

La prise en compte du SID forcé est réalisée lors de l'initialisation de l'annuaire Active Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le SID n'est pas validé au moment de la saisie. Il est nécessaire de s'assurer qu'il est correct avant de sauvegarder.

Forcer le positionnement dans un site AD à l'initialisation

À partir de la version 2.6.2, il est possible de demander à ce qu'un contrôleur de domaine additionnel soit rattaché à un site Active Directory particulier.

Cette demande s'effectue en deux temps :

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

- en passant la variable `Forcer le positionnement de ce contrôleur de domaine dans un site existant` à `oui` ;
- en renseignant la variable `Site de destination de ce contrôleur de domaine`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.

La prise en compte du domaine de rattachement est réalisée lors de l'initialisation de l'annuaire Active Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le site doit impérativement avoir été déclaré au préalable sur le contrôleur de domaine principal.

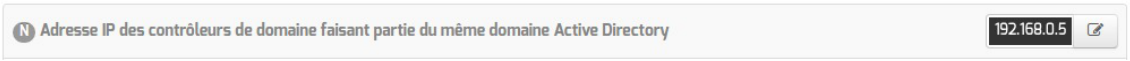
Si le contrôleur de domaine principal est un module Seth, la déclaration d'un site s'effectue facilement grâce à la fonction bash *`samba_update_site`* :

```
. /usr/lib/eole/samba4.sh
samba_update_site monsite 10.1.1.0/24
```

Environnement réseau

Adresse des contrôleurs du même domaine

Si plusieurs contrôleurs de domaine doivent être mis en place, il est impératif qu'ils se connaissent les uns les autres.

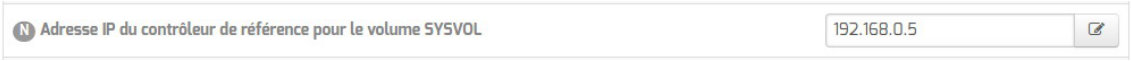


La variable `Adresse IP des contrôleurs de domaine faisant partie du même domaine Active Directory` permet de déclarer les adresses IP des autres contrôleurs du domaine.

Sur EOLE 2.6.2, cette variable est intitulée : `Adresse IP des contrôleurs de domaine en relation avec ce contrôleur de domaine Active Directory`.

Contrôleur de référence pour le volume SYSVOL

Dans le cas de la mise en œuvre d'un contrôleur de domaine additionnel, il est recommandé de déclarer le contrôleur de domaine principal en tant référence pour le volume SYSVOL.



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

Dans le monde Microsoft, les contrôleurs de domaine sont habituellement tous au même niveau. Ceci est possible grâce à la réplication de l'annuaire Active Directory et à l'utilisation d'un système de fichiers distribué (DFS[p.498]).

À l'heure actuelle, la réplication du partage SYSVOL[p.519] n'est pas supportée par Samba. De ce fait, la mise en œuvre d'une architecture multi-DC[p.510] avec le module Seth nécessite de définir un contrôleur de domaine principal qui héberge les fichiers SYSVOL de référence et des contrôleurs de domaine additionnels sur lesquels ces fichiers sont synchronisés à intervalle régulier via rsync[p.516].

Pages relatives au support DFS sur le Wiki Samba

- https://wiki.samba.org/index.php/Distributed_File_System_(DFS)
- https://wiki.samba.org/index.php/SysVol_replication_(DFS-R)

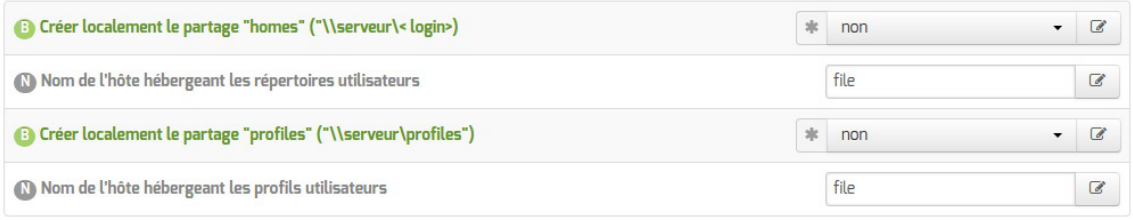
Partage de fichiers

Les partages utilisateur et les autres répertoires partagés peuvent être locaux et/ou hébergés sur d'autres serveurs Active Directory.

Sur le serveur local, il est possible d'activer ou non l'hébergement des partages « homes » et « profiles » des utilisateurs.



Dans le cas où l'on ne souhaite pas héberger ces répertoires localement, il est possible d'indiquer le nom d'hôte d'une machine du domaine (un serveur membre par exemple) sur lesquels ils seront stockés.



Archivage et sauvegarde des données

Un problème de corruption de la base Active Directory peut nécessiter de restaurer une sauvegarde sur le contrôleur de domaine principal et de relancer la synchronisation de tous les autres contrôleurs.

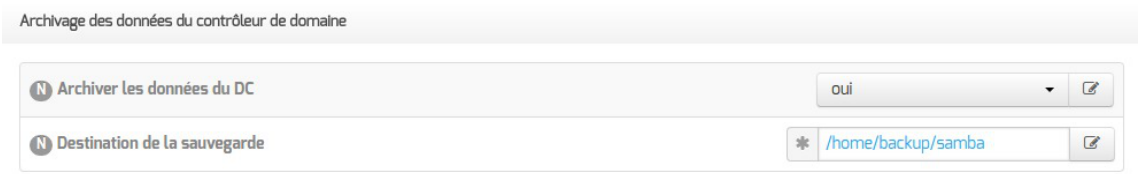
Il est primordial de disposer d'une archive ou d'une sauvegarde récente des données du serveur Active Directory.

Archivage local

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

La variable `Archiver les données du DC` permet d'activer l'exécution quotidienne d'un script d'archivage local et de choisir la destination de stockage de l'archive.

Les données du serveur Active Directory sont ainsi régulièrement sauvegardée (par défaut 1 fois par jour) dans le répertoire spécifié dans `Destination de la sauvegarde`.



Les éléments concernés par cette archive sont les suivants :

- la configuration de Samba (`/etc/samba`) ;
- le répertoire SYSVOL[p.519] (`/home/sysvol`) ;
- les bases TDB[p.520] de Samba (`/var/lib/samba/private`).

> Le script utilisé pour l'archivage des données est inspiré d'un script mis à disposition par les développeurs du logiciel Samba : https://wiki.samba.org/index.php/Back_up_and_Restoring_a_Samba_AD_DC.

Sauvegarde locale ou distante

Il est possible de mettre œuvre un système de sauvegarde complet en installant le logiciel Bareos[p.495] sur le serveur.

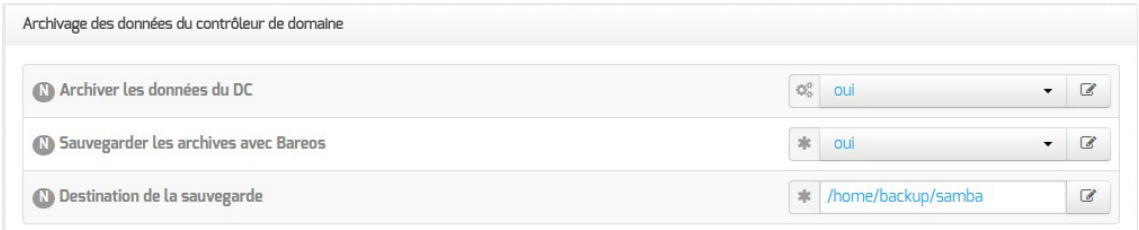
La mise en place de cet outil s'effectue manuellement à l'aide de la commande suivante :

```
# apt-eole install eole-bareos
```

Après installation des paquets, la configuration du service de sauvegarde se fait dans l'interface de configuration du module à plusieurs endroits.

L'archivage du DC soit activé dans l'onglet : `Archiver les données du DC` doit être à `oui`.

Par défaut la sauvegarde Bareos est activée (`Activer la sauvegarde du serveur` à `oui` dans l'onglet `Services`) et la tâche de sauvegarde des données du serveur Active Directory est prise en compte (`Sauvegarder les archives avec Bareos` à `oui` dans l'onglet `Active Directory`).



Dans cette configuration, les éléments suivants sont directement sauvegardés par Bareos avec le support des ACL :

- la configuration de Samba (`/etc/samba`) ;
- le répertoire SYSVOL[p.519] (`/home/sysvol`).

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

L'export des bases TDB est quant à lui géré par eole-schedule[p.501] avant l'exécution des sauvegardes.

La configuration à proprement parler des sauvegardes (distante, locale, durée de rétention, taux de compression…) se fait dans les onglets `Directeur bareos` et `Stockage bareos`.

Voir aussi...

- Onglet Directeur bareos [p.121]
- Onglet Stockage bareos [p.124]

3.12. 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.



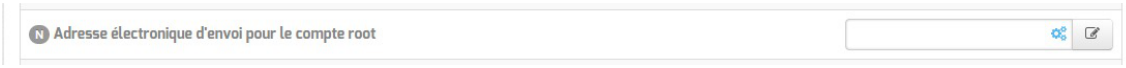
Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

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

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

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.

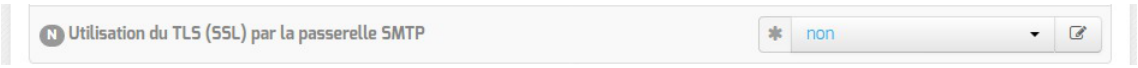
Relai des messages



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.520] pour l'envoi de message. Si la passerelle SMTP[p.517] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.518] (port 25) ou non (port 465).

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 Seth :

- `Général` ;
- `Services` ;
- `Système` ;
- `Sshd` ;

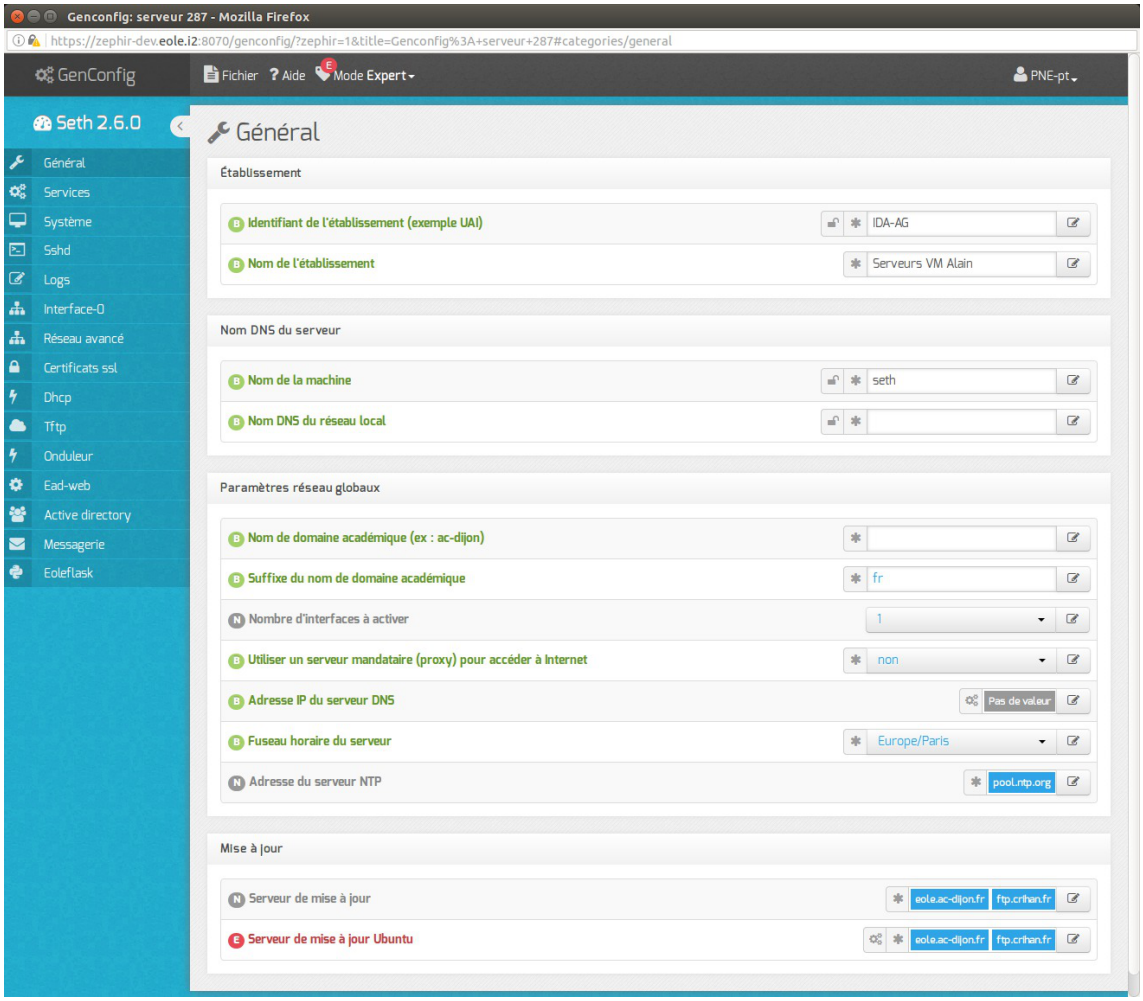
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Ntp` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-n` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificats ssl` ;
- `Dépôt tiers` ;
- `Clamav` ** ;
- `Dhcp` * ;
- `Tftp` *;
- `Onduleur` * ;
- `Saltstack` * ;
- `Ead-web` * ;
- `Directeur bareos` ** ;
- `Stockage bareos` ** ;
- `Cups` ** ;
- `Nginx` ;
- `Applications web nginx` * ;
- `Reverse proxy` * ;
- `Active Directory` ;
- `Messagerie` ;
- `Eoleflask`.

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

** Certains onglets ne sont disponibles qu'après installation manuelle d'un paquet.

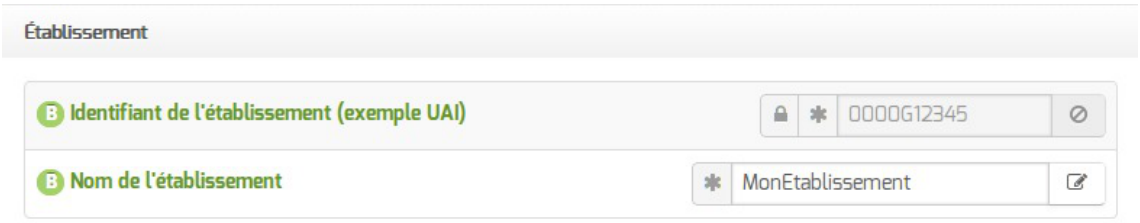
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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`.

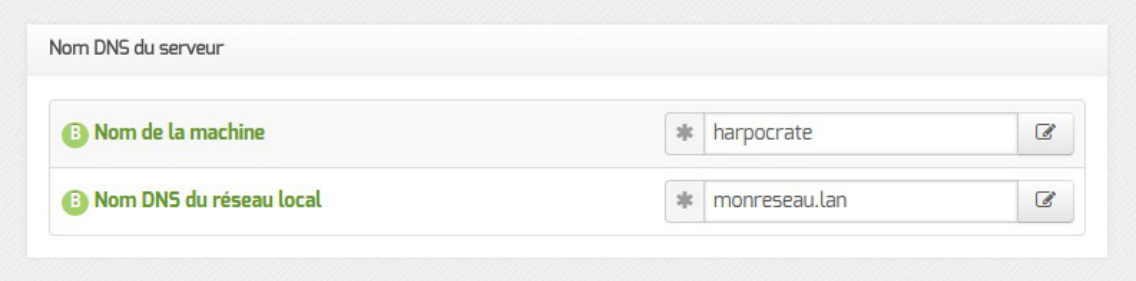
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.505] 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.

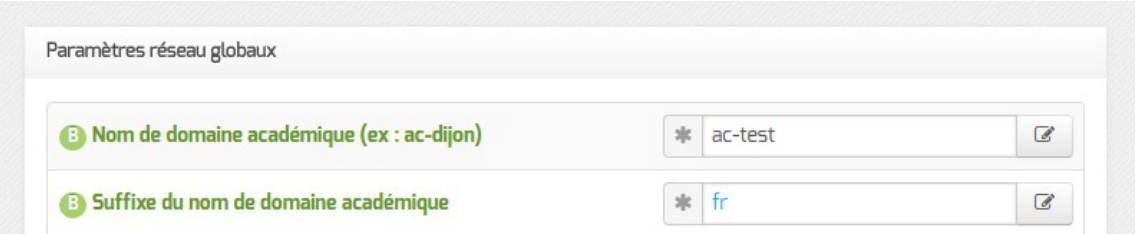
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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)



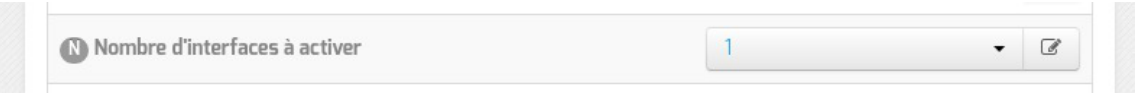
En deuxième lieu, il convient de configurer les noms de domaine de la machine.

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.

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 :

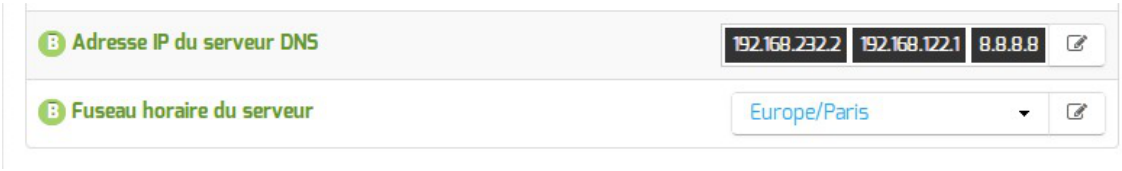
- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.



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

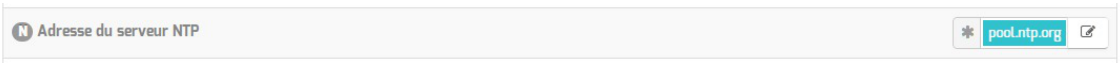
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.499].

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

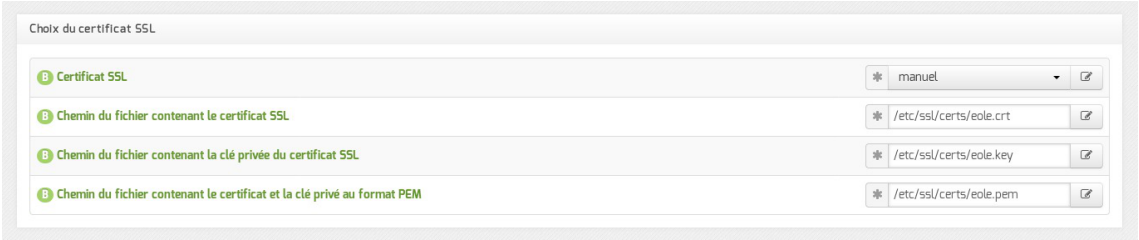
NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.511]. 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.



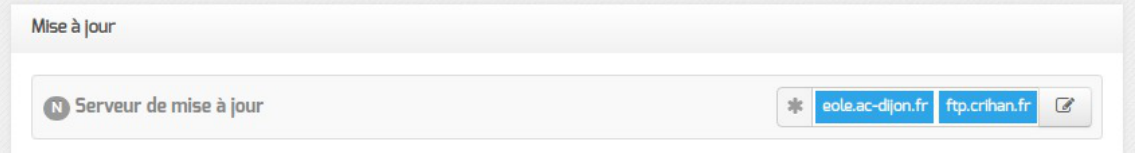
Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.520] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.494] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.506] ;
- `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.

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

Mise à jour



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



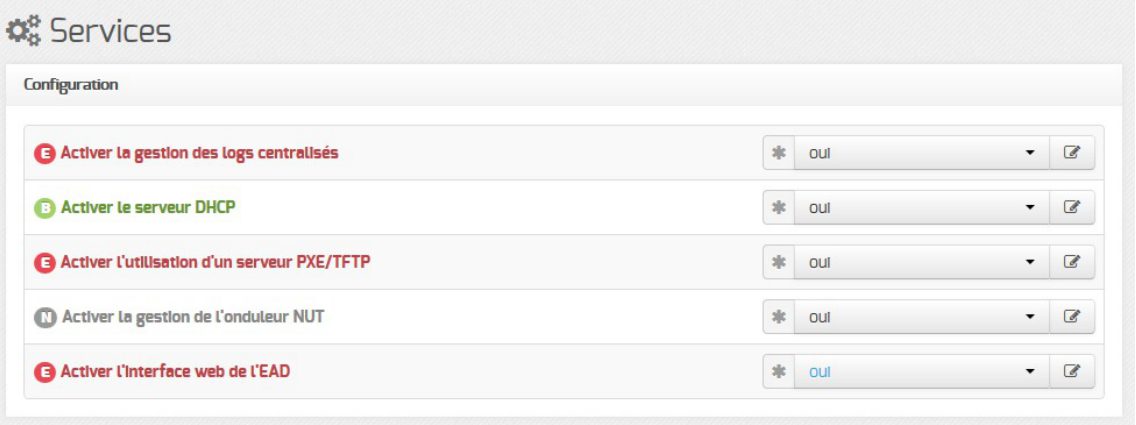
Il est possible de définir d'autres adresses pour le serveur de mise à jour Ubuntu que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Voir aussi...

Les différents types de mises à jour [p.316]

4.2. Onglet Services

Configuration



En mode « Expert » sont présentes de plus la gestion des logs centralisés, l'activation d'un serveur PXE/TFTP et l'activation de l'interface web EAD.

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

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



- `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



- `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)
```


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

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
- `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

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

- `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.s`o 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 ;
- 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.

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

> 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
  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
```

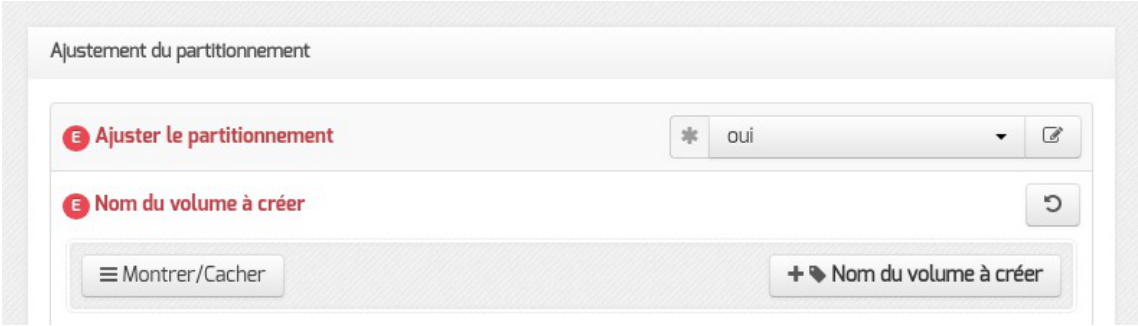

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  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.



- 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`.

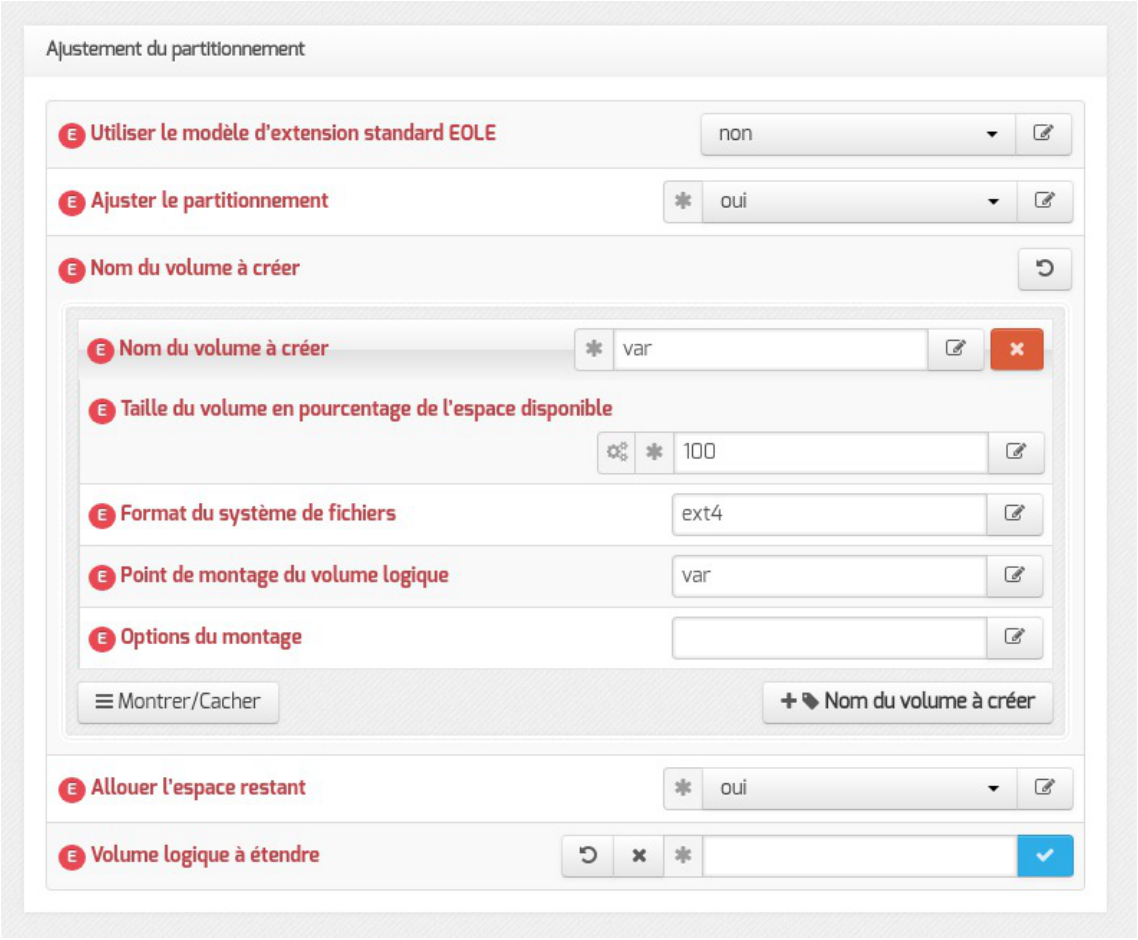


Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

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.



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.

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).

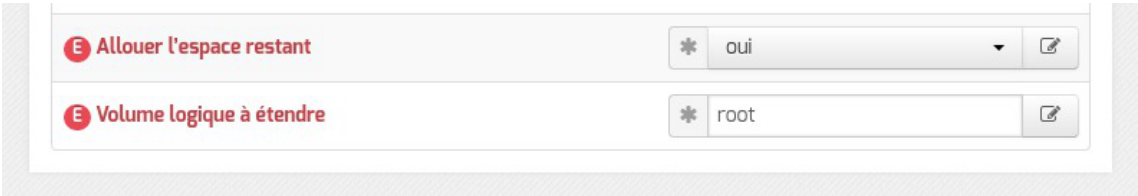
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



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

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% /
```


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

```
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.229]

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`).

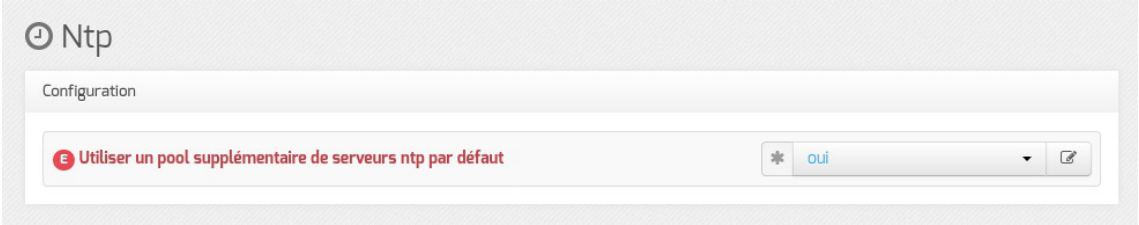
Par défaut, les groupes Unix autorisés sont `root` et `adm`.

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

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`).

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`).

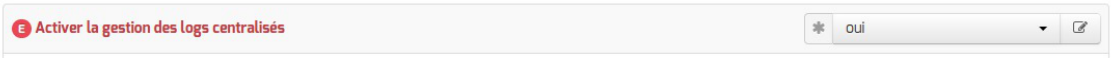
Par défaut, l'utilisation du pool est activée.

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

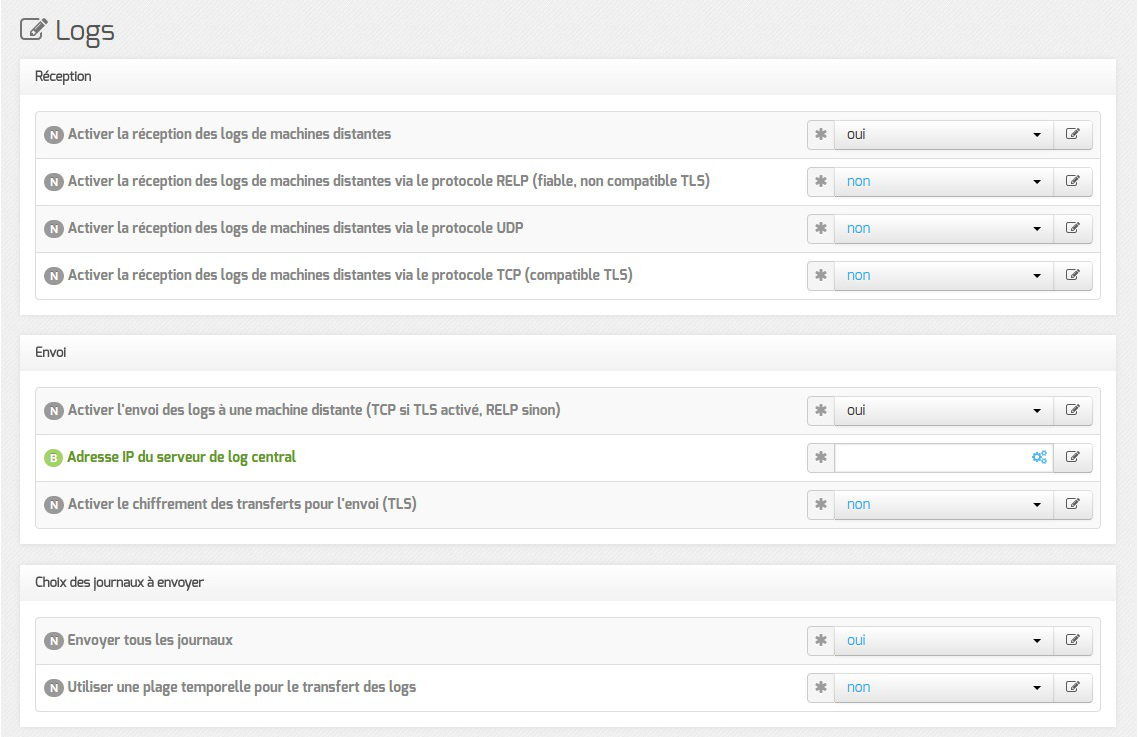
La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.523]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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)



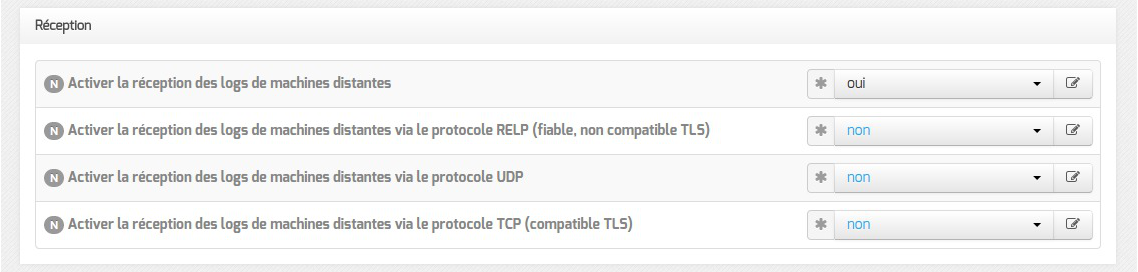
Vue de l'onglet Logs

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.520] ou RELP[p.515]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.520]) ;
- 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.494].

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.

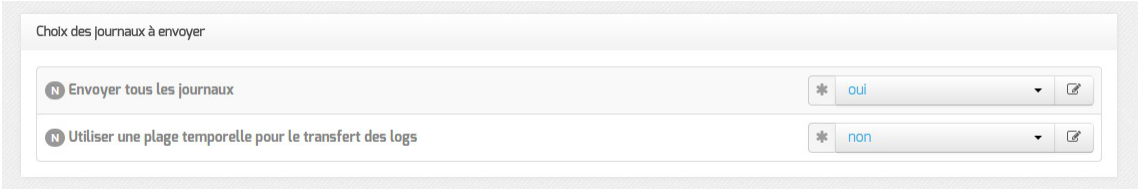


Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.494].

Choix des journaux à envoyer

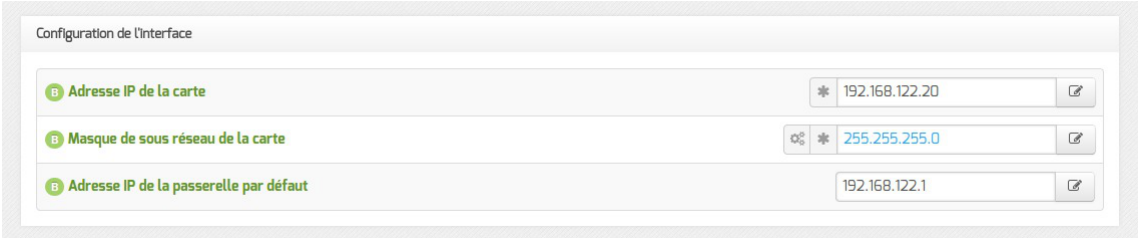
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



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

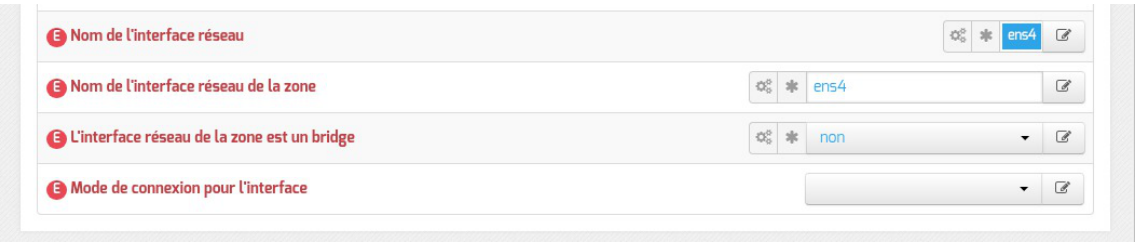
Configuration de l'interface



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.496], 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.493] 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.494].

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.

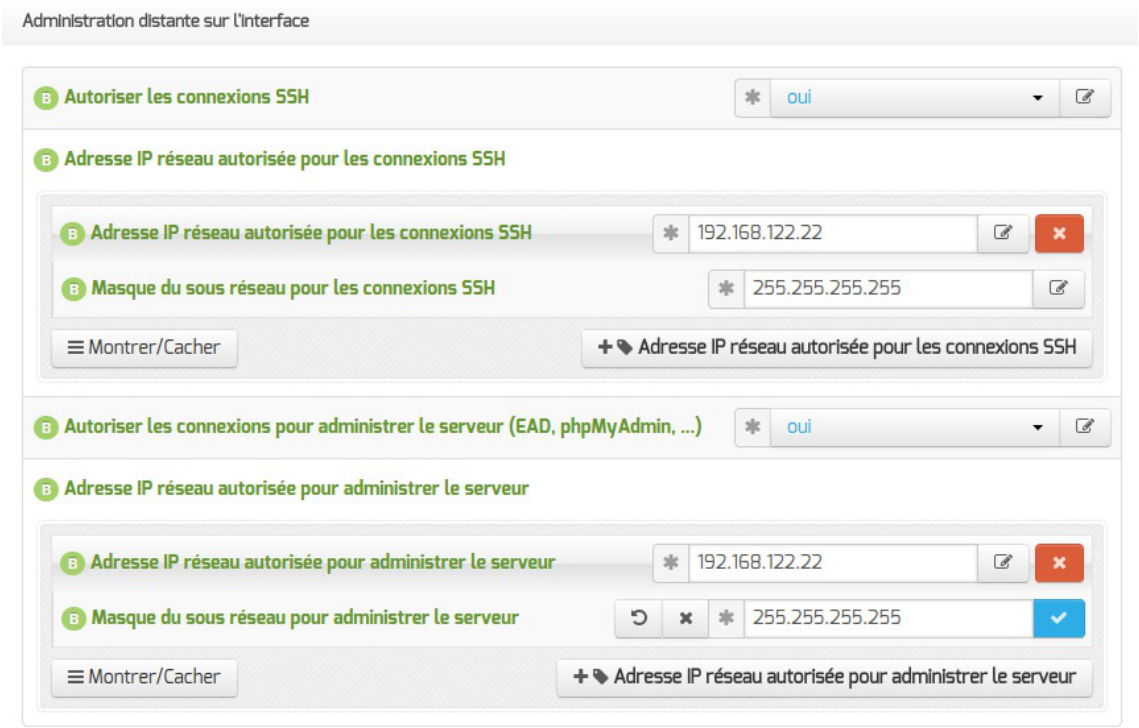
Liste des valeurs possibles :

- `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



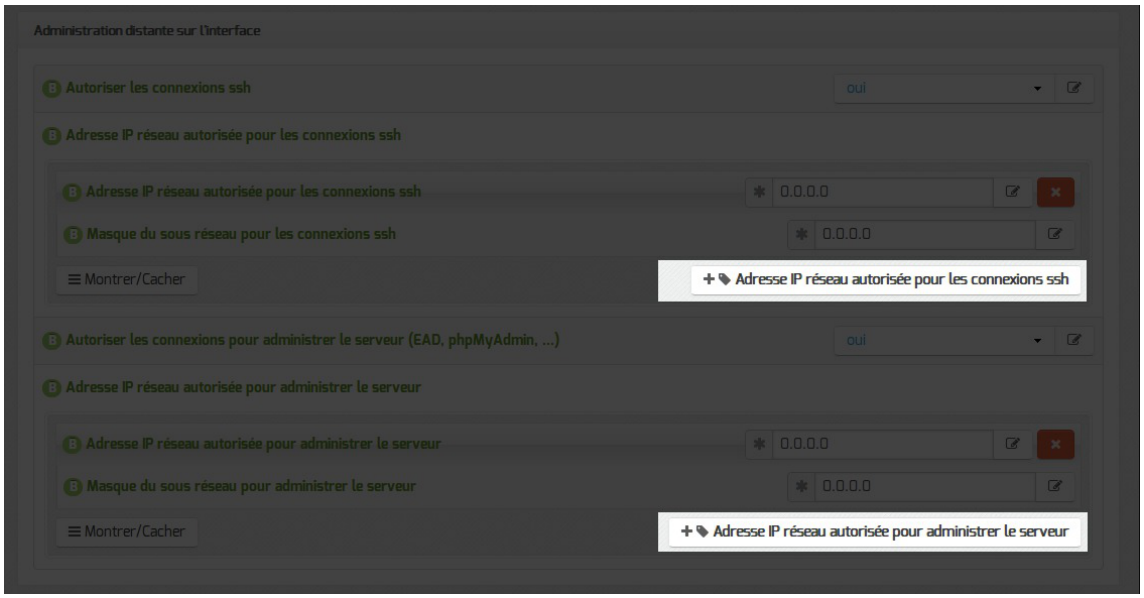
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.518] 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.

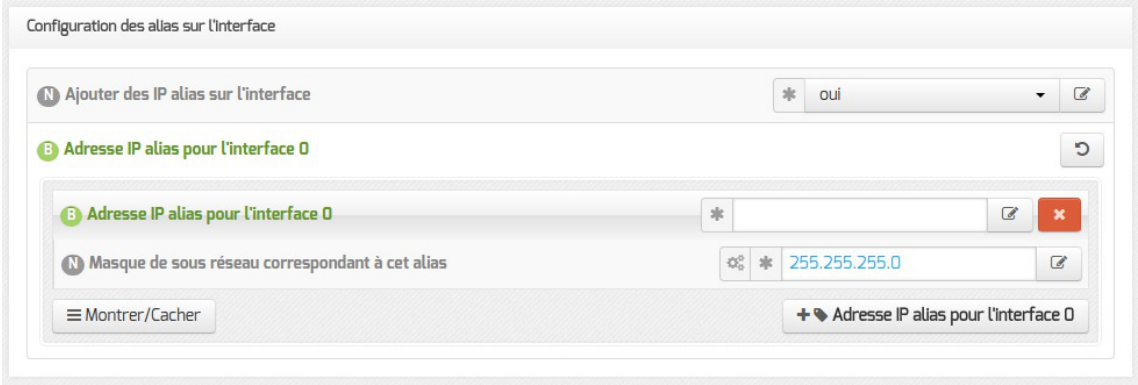
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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)

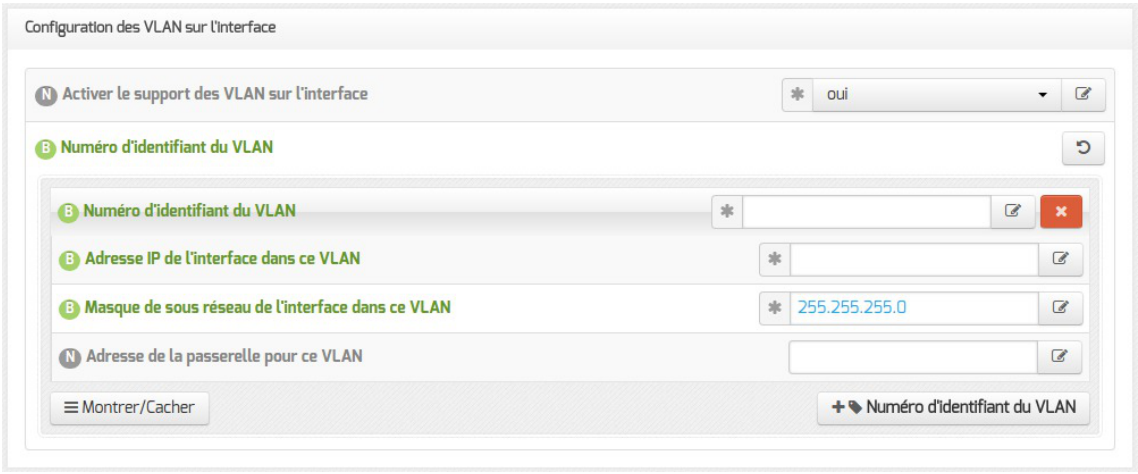


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

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.522] (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 :

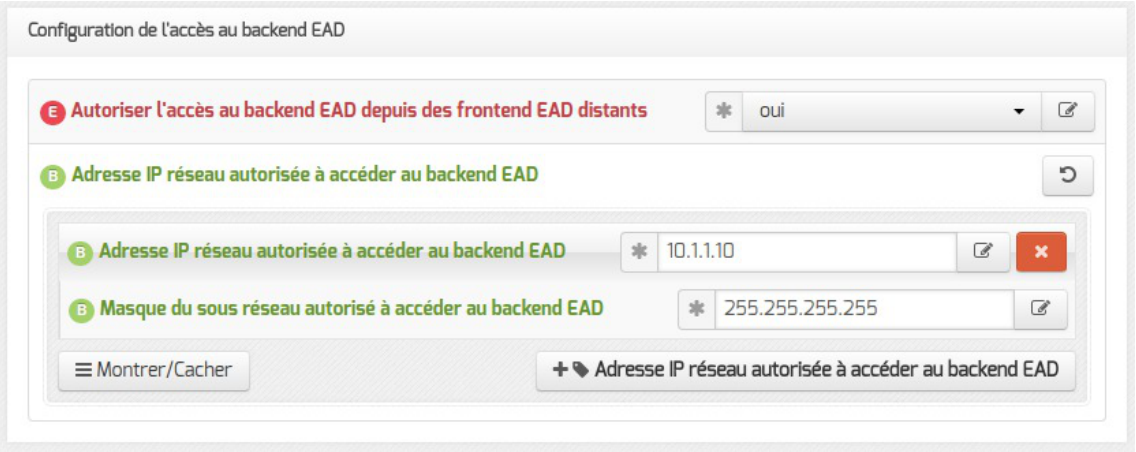
- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

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.500] 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.224]

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.

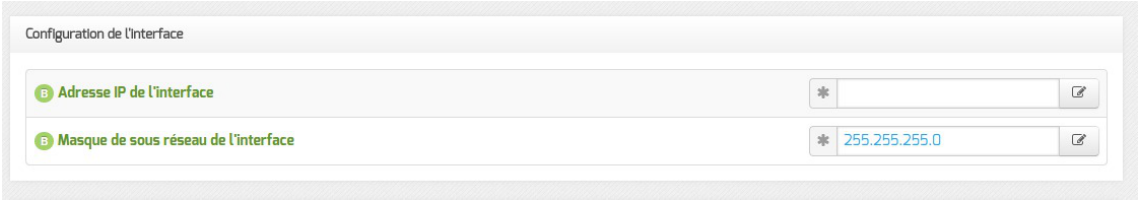


Cela ajoute autant d'onglet `Interface-n` que le nombre d'interfaces à activer choisi.

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

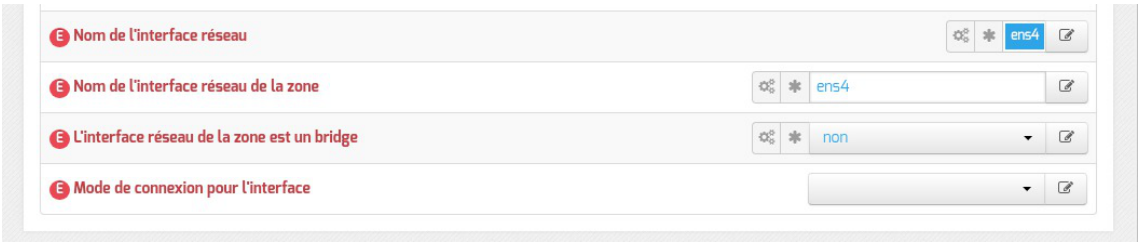
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.496], 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.493] 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.494].

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 :

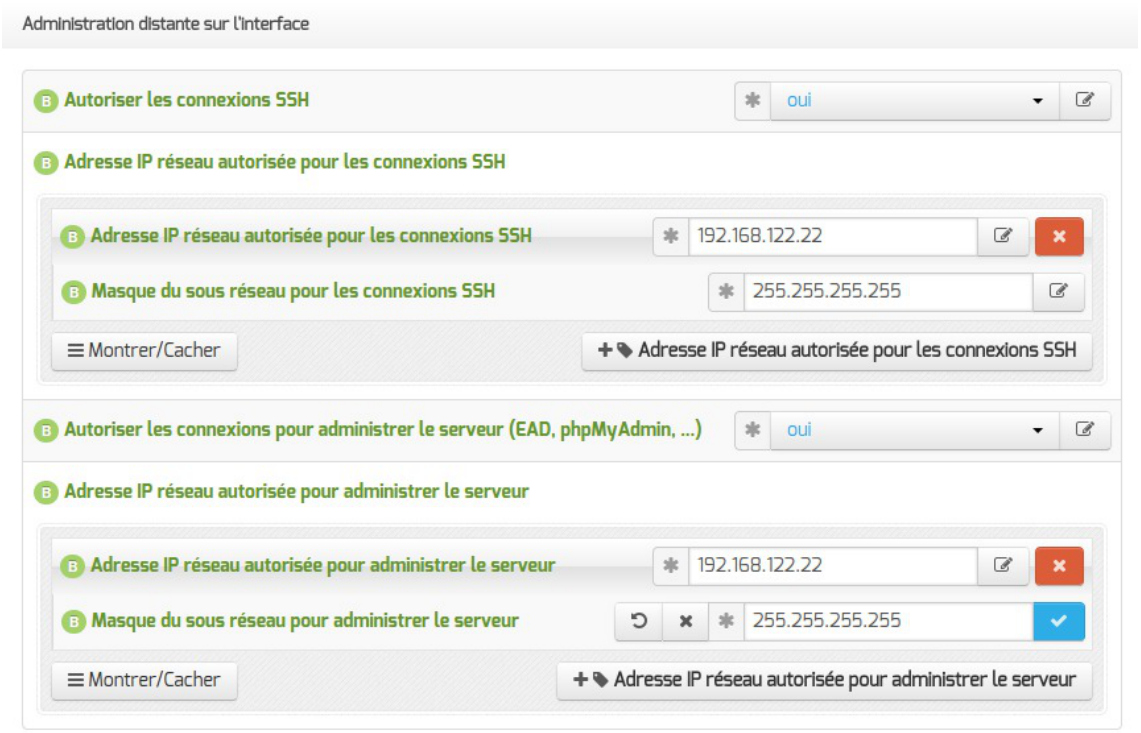
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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

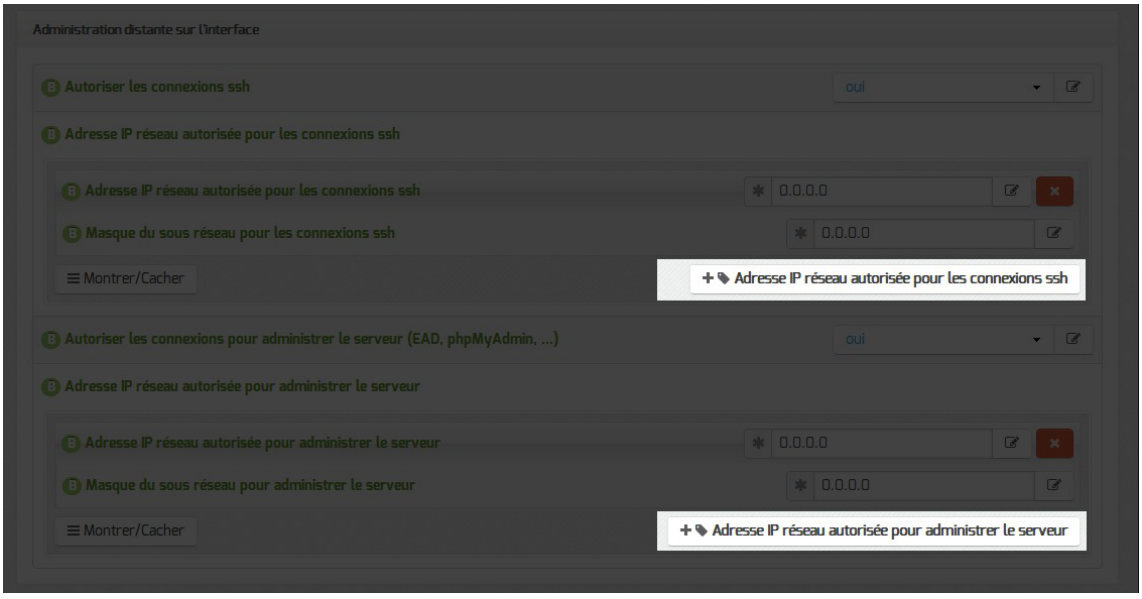


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.518] 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)

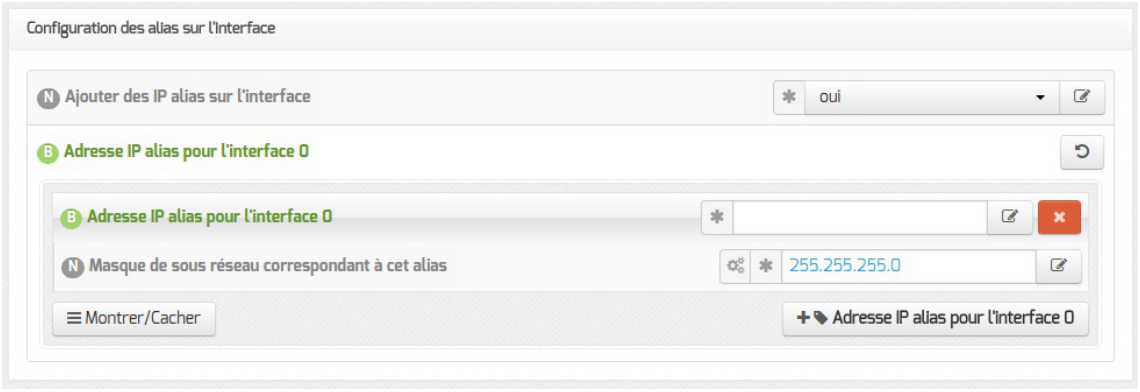
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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.

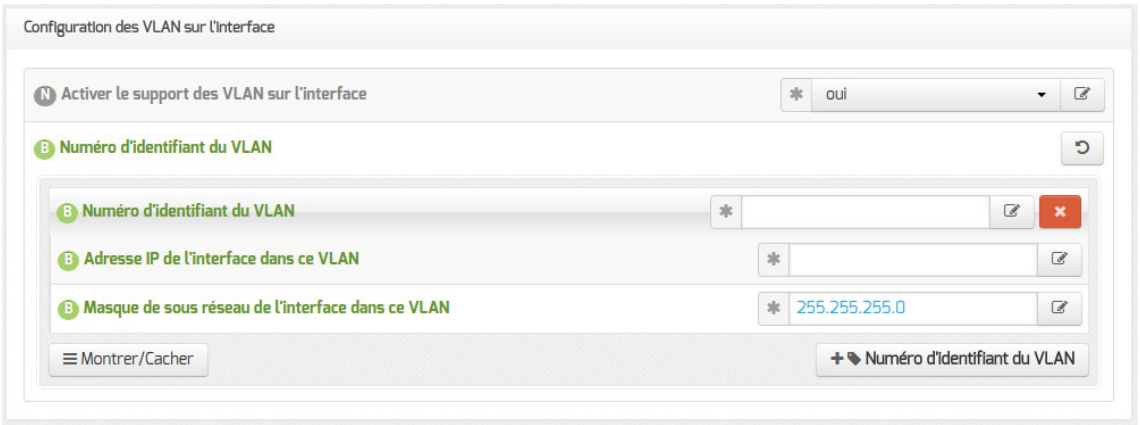


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

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.522] (réseau local virtuel) sur une interface déterminée du module.



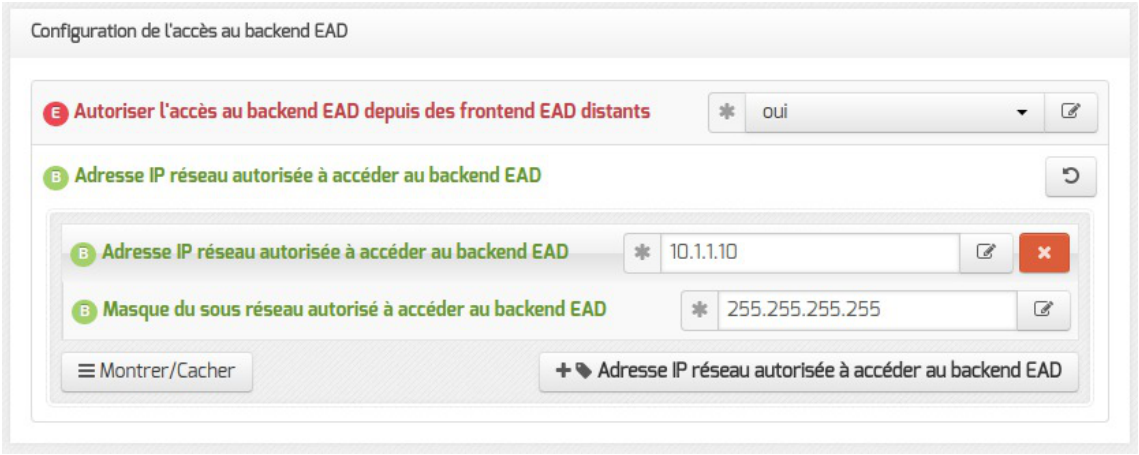
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.500] 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...

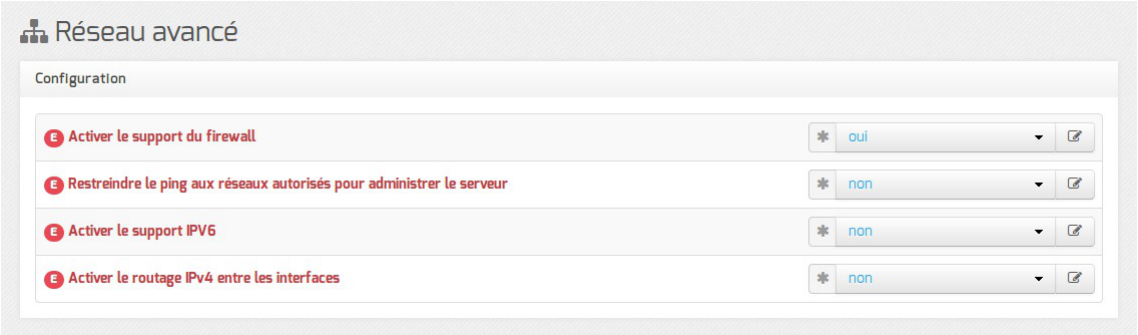
Mise en place de l'agrégation de liens Ethernet (bonding) [p.224]

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.504] 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`).

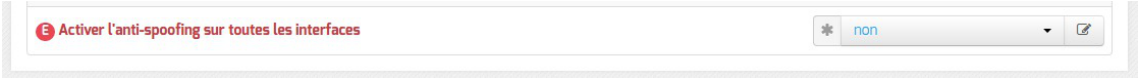
Sécurité



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)

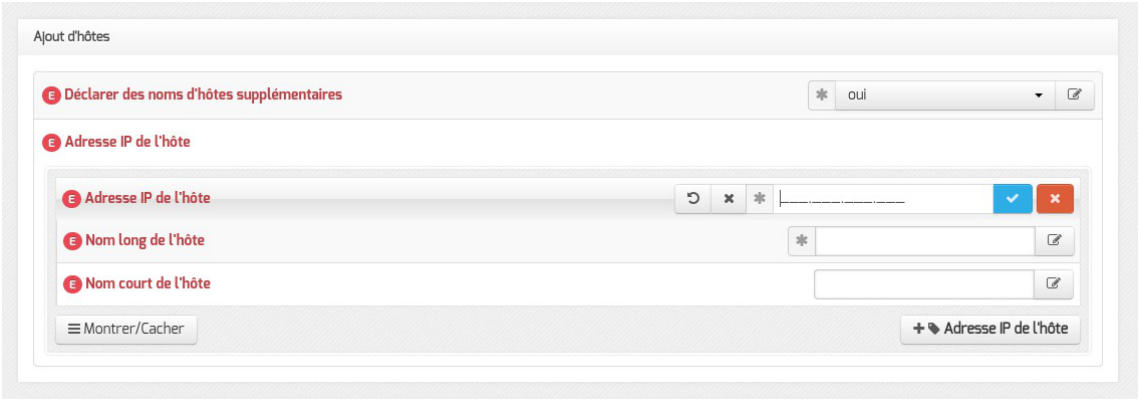
utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.494] 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.

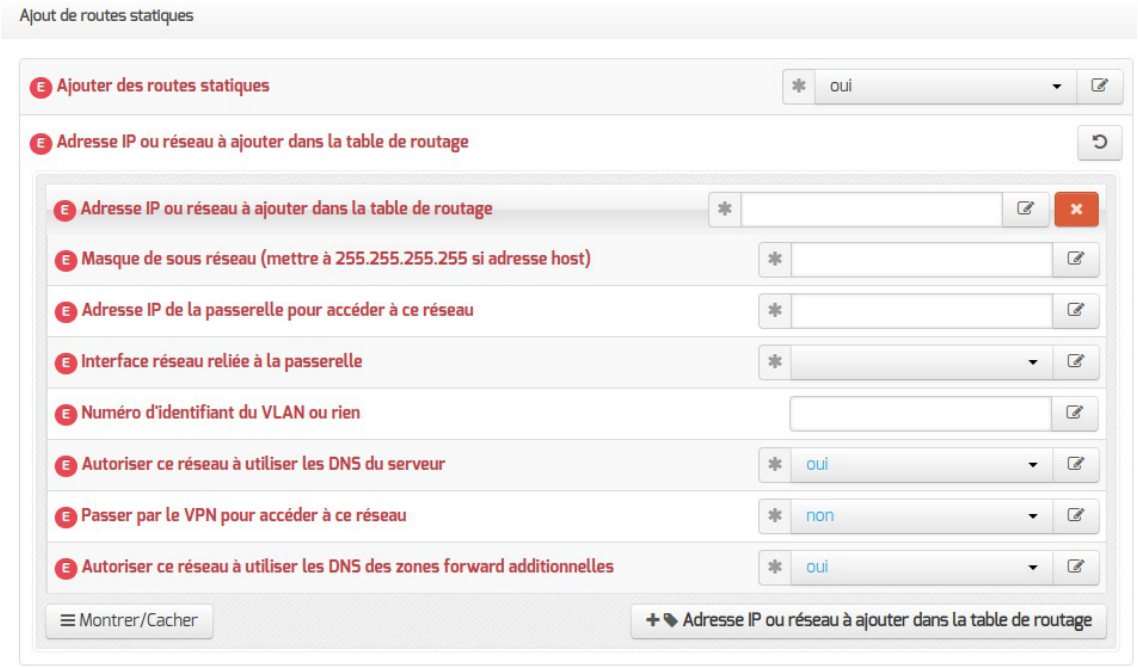


Sur les serveurs EOLE faisant office de serveur DNS, comme les modules Amon et AmonEcole, pour que le logiciel BIND[p.495] puisse résoudre un nom, il faut que le suffixe DNS de ce nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

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 :

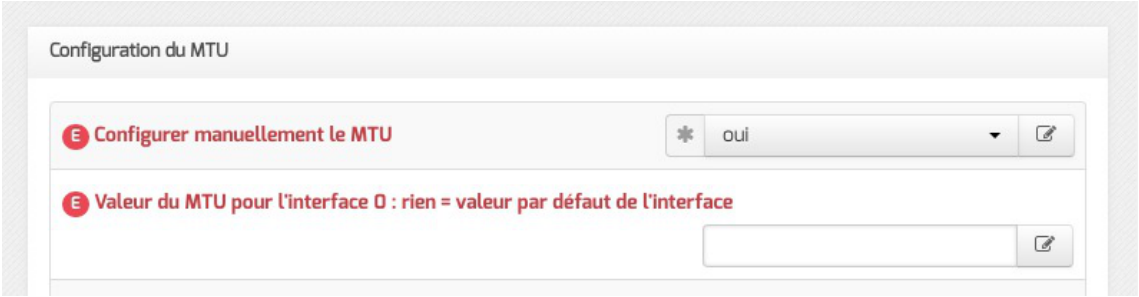
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

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.510] (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.503] 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.510] 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).

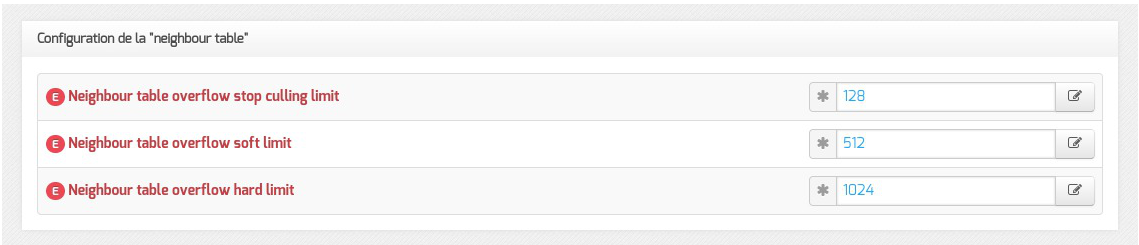
Si l'interface externe est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le champ : `Valeur du MTU pour l'interface 0`.



Si l'interface externe d'un module Amon ou AmonEcole est de type PPPoE[p.514] 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"

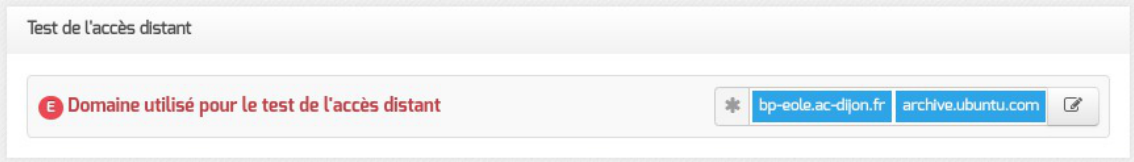


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.506] permet de mettre en place, gratuitement, des certificats dont la distribution et le renouvellement sont automatisés.

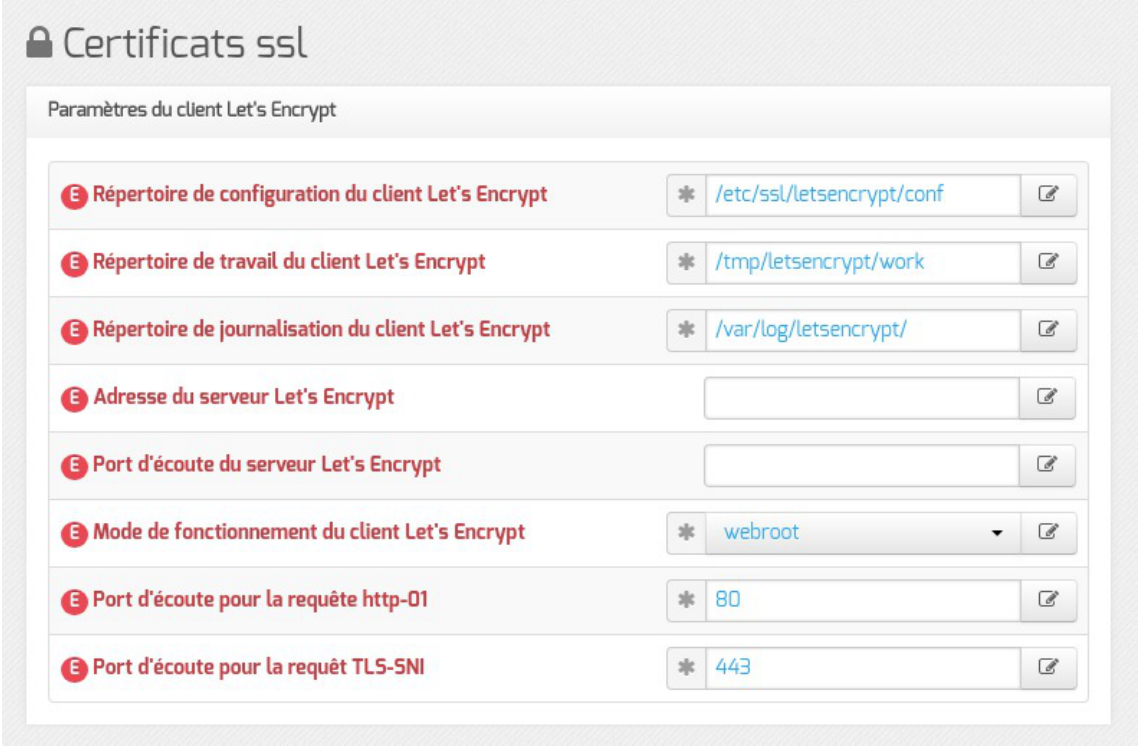
Vous pouvez à présent gérer des certificats Let's Encrypt pour des serveurs accessibles depuis Internet ou au travers d'un proxy inverse.

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.

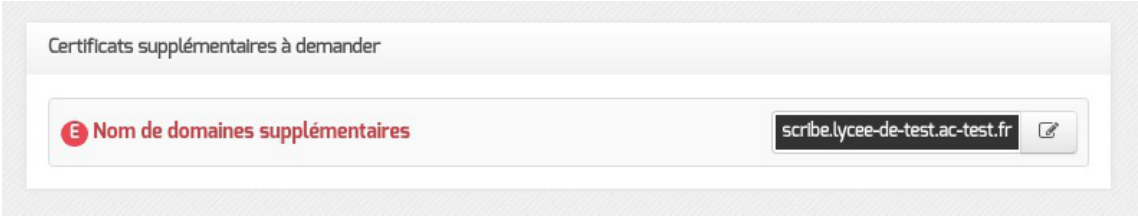
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 `webroo`t.

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)

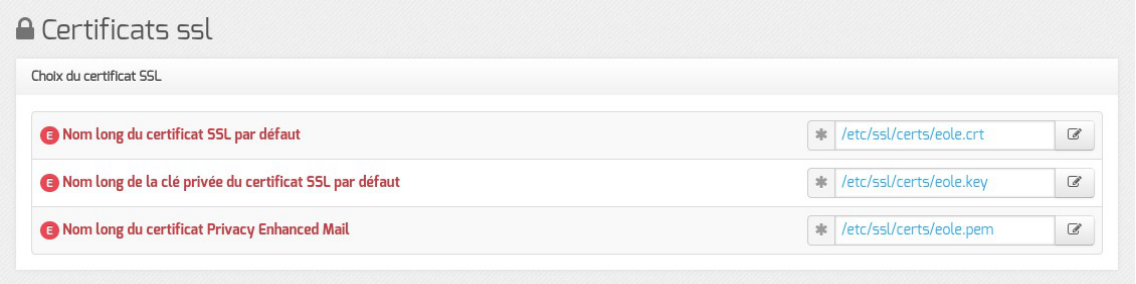
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un 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.512] 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.499]) 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.521] 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.496] 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.500] 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...

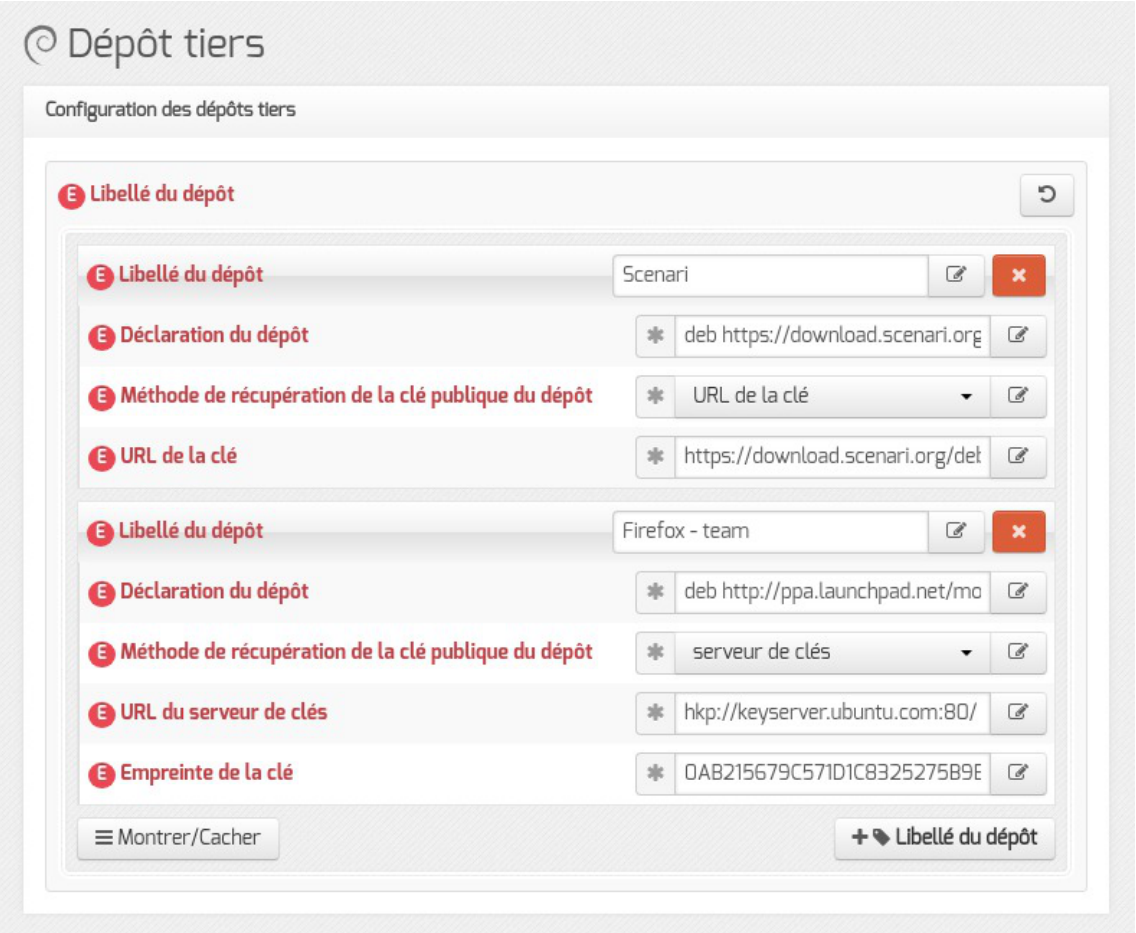
Intégration d'un certificat et d'une chaîne d'authentification

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)

```
Aucun paquet à installer.
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`.



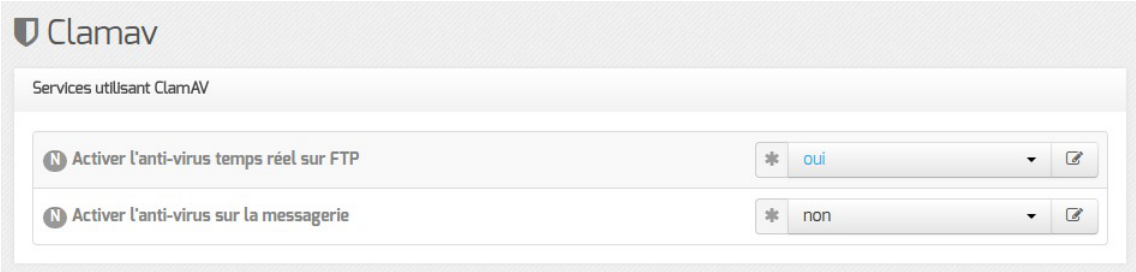
La variable `upgrade auto meta release repo` permet de définir où est téléchargé le fichier `meta-release-lts`.

4.12. Onglet Clamav : Configuration de l'anti-virus

EOLE propose un service anti-virus réalisé à partir du logiciel libre ClamAV.

http://www.clamav.net

Activation de l'anti-virus



Par défaut, le service est activé sur le module et l'anti-virus est actif sur certains services :

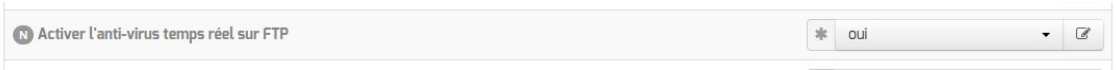
- le service FTP ;
- le service de messagerie.



Si aucun service n'utilise l'anti-virus, il est utile de le désactiver dans l'onglet `Services`. Il faut passer la variable `Activer l'anti-virus ClamAV` à `non`. L'onglet `Clamav` n'est alors plus visible.

Activation de l'anti-virus sur FTP

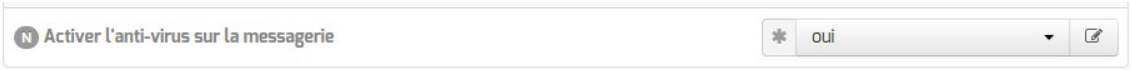
Pour désactiver l'anti-virus en temps réel sur les fichiers mis en ligne par FTP il faut passer la variable `Activer l'anti-virus temps réel sur FTP` à `non` dans l'onglet `Clamav`.



Activation de l'anti-virus sur la messagerie

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

Pour activer l'anti-virus sur la messagerie il faut passer la variable `Activer l'antivirus sur la messagerie` à `oui` dans l'onglet `Clamav`.



Forcer l'activation du service clamd

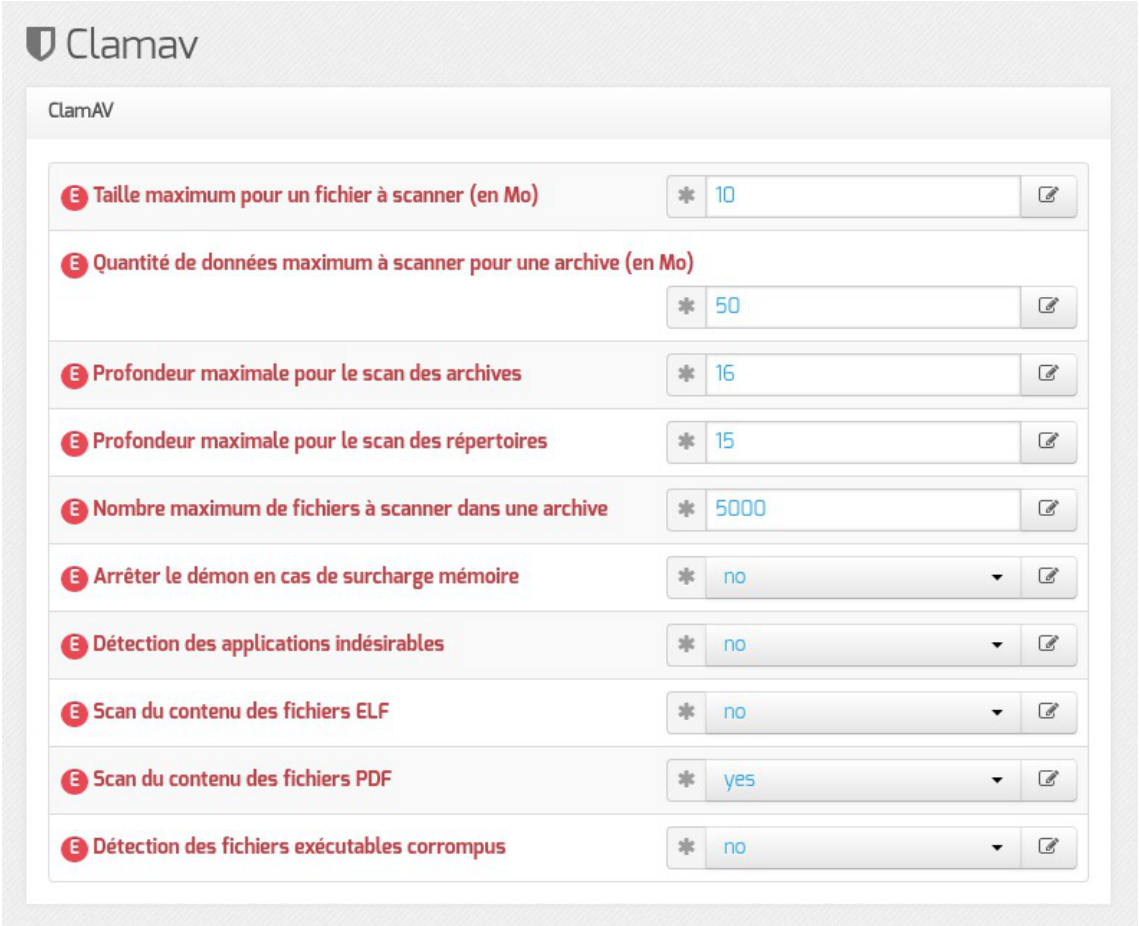
Si `Activer l'anti-virus ClamAV` est à `oui` dans l'onglet `Service` mais qu'aucun service EOLE ne l'utilise alors seul le service de mise à jour de la base de signatures (freshclam) sera actif sur le serveur.

À partir de la version 2.5.2 d'EOLE, il est possible de forcer l'activation du service anti-virus (clamd) en passant la variable du mode expert `Forcer l'activation du démon clam sur le serveur` à `oui` dans l'onglet `Clamav`.



Configuration avancée du service anti-virus

En mode expert, l'onglet `Clamav` comporte de nombreuses variables qui permettent d'affiner la configuration du service anti-virus ClamAV.



- `Taille maximum pour un fichier à scanner (en Mo)` ;

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

- `Quantité de données maximum à scanner pour une archive (en Mo)` ;
- `Profondeur maximale pour le scan des archives` ;
- `Profondeur maximale pour le scan des répertoires` ;
- `Nombre maximum de fichiers à scanner dans une archive` ;
- `Arrêter le démon en cas de surcharge mémoire` ;
- `Détection des applications indésirables` ;
- `Scan du contenu des fichiers ELF` *[p.500] ;
- `Scan du contenu des fichiers PDF` ;
- `Scan des fichiers courriels` ;
- `Détection des fichiers exécutables corrompus`.

Configuration avancée du service de mise à jour de l'anti-virus

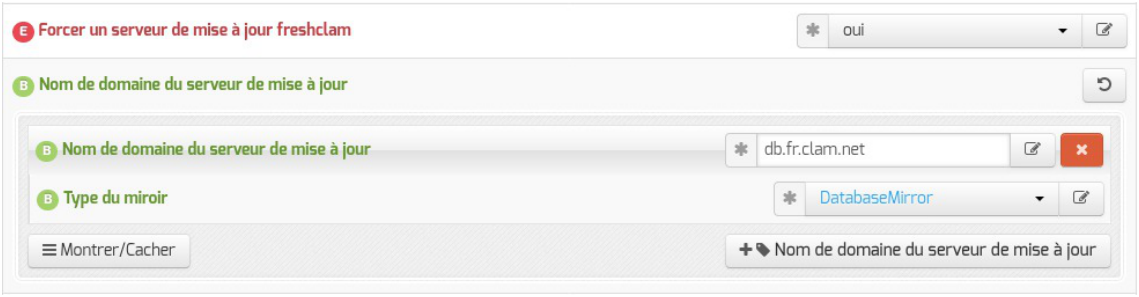
En mode expert, l'onglet `Clamav` comporte des variables qui permettent d'affiner la configuration de Freshclam, le service de mise à jour de la base de signatures.



- `Nom de domaine du serveur DNS de mise à jour` permet de spécifier un miroir interne pour les signatures ;
- `Forcer un serveur de mise à jour freshclam` permet d'ajouter un ou plusieurs miroirs pour les signatures ;
- `Code IANA pour la mise à jour de la base de signature` permet de sélectionner le miroir le plus proche en se saisissant un code pays dans le cas où on n'ajoute pas manuellement de miroirs ;
- `Nombre de tentatives de mise à jour par miroir` permet de réduire le nombre de tentatives de mise à jour, en effet des fichiers sont récupérés systématiquement à chaque tentative ;
- `Nombre de mises à jour quotidiennes` permet de réduire le nombre de mises à jour quotidiennes.

Passer `Forcer un serveur de mise à jour freshclam` à **oui** donne accès à un groupe de deux variables supplémentaires permettant de renseigner le nom de domaine d'un miroir et son type.

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



Lorsqu'un miroir est ajouté manuellement, il est nécessaire d'indiquer quel est son type : **DatabaseMirror** ou **PrivateMirror**. La distinction porte sur le protocole utilisé pour établir la connexion avec le miroir. **DatabaseMirror** implique l'utilisation du protocole **https** alors que **PrivateMirror** implique l'utilisation du protocole **http**.

L'établissement d'une connexion avec le protocole **https**, impliqué par le type **DatabaseMirror**, suppose que le certificat identifiant le miroir soit valide.

Contribuer

La base de données de virus est mise à jour avec l'aide de la communauté.

Il est possible de faire des signalements :

- signaler de nouveaux virus qui ne sont pas détectés par ClamAV ;
- signaler des fichiers propres qui ne sont pas correctement détectés par ClamAV (faux-positif).

Pour cela il faut utiliser le formulaire suivant (en) : http://www.clamav.net/contact#reports

L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.

Il ne faut pas signaler des PUA[p.514] comme étant des faux positifs.

4.13. Onglet Dhcp : Configuration du serveur DHCP

Le serveur DHCP[p.498] est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option : `Activer le serveur DHCP`.

L'onglet `Dhcp` apparaît uniquement il le service est activé.

Sur les modules Seth, Horus, Scribe et Eclair (mode une carte), les adresses servies doivent généralement être sur le réseau local (interface 0).

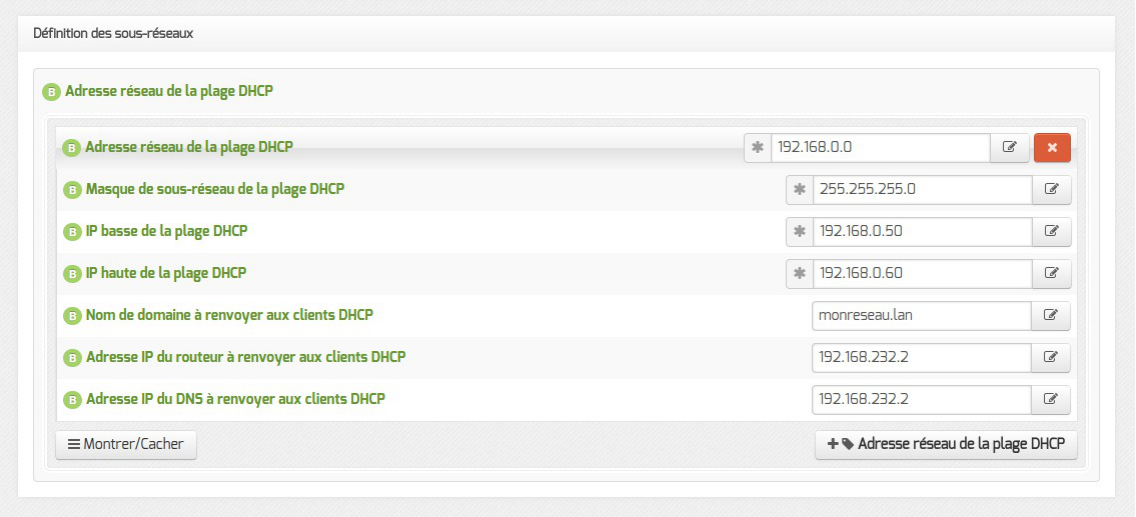
Sur les modules AmonEcole et AmonEcole-Eclair, les adresses servies sont celles du réseau interne (interface 1).

Si le serveur est installé en DMZ, on pourra renseigner des adresses d'un autre réseau mais dans ce cas, il faudra activer le relayage du DHCP[p.515] sur le pare-feu.

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

Définition des sous-réseaux

Il faut définir une ou plusieurs plages (en anglais range) d'adresses attribuables par le serveur à l'aide du bouton `+ Adresse réseau de la plage DHCP`.



La plage DHCP doit contenir au moins autant d'adresses que le nombre de stations susceptibles d'être connectées simultanément sur le réseau.

Les champs `Adresse réseau de la plage DHCP` et `Masque de sous-réseau de la plage DHCP` permettent de définir le réseau sur lequel les adresses doivent être servies.

Le champ `Nom de la plage DHCP`, disponible uniquement à partir de la version 2.6.2, permet d'identifier plus facilement la plage DHCP, notamment dans la nouvelle interface d'administration (EAD3). Pour administrer efficacement le DHCP dans l'interface de configuration, il convient de renseigner des noms de plages pertinents. Dans le cas d'une migration depuis une version antérieure d'EOLE, cette variable est arbitrairement initialisée avec les valeurs "plage0", "plage1"...

Les champs `IP basse de la plage DHCP` et `IP haute de la plage DHCP` doivent être comprise dans le réseau déclaré ci-dessus.

Le champ `IP basse de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus petite.

Le champ `IP haute de la plage DHCP` correspond, dans un réseau de classe C, à l'adresse IP dont le dernier octet a la valeur la plus grande.

Le nombre d'adresses IP servies est déterminé par la différence entre la valeur la plus grande et la valeur la plus petite.

Les champs `Nom de domaine à renvoyer aux clients DHCP`, `Adresse IP du routeur à renvoyer aux clients DHCP` et `Adresse IP du DNS à renvoyer aux clients DHCP` permettent de spécifier des valeurs différentes pour chaque plage déclarée.

Pour la configuration de l'`Adresse IP du routeur à renvoyer aux clients DHCP` :

- dans le mode une carte, l'adresse sera l'adresse IP de la passerelle saisie dans l'onglet `Interface-0` ;
- dans le cas du mode deux cartes, l'adresse IP du routeur sera l'adresse IP de l'`Interface-1` (`eth1`).

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

L'`Adresse IP du DNS à renvoyer aux clients DHCP` peut être l'adresse IP du DNS de votre FAI[p.501] pour une utilisation sans le module Amon. Il est également possible d'utiliser des serveurs DNS disponibles sur Internet.

Si vous disposez d'un module Amon ou d'un module AmonEcole, il est conseillé d'utiliser le module comme relais DNS[p.499], L'adresse à préciser dans le cas du mode deux cartes sera l'adresse IP du routeur et donc l'adresse IP de l'`Interface-1` (`eth1`).



Sur le module AmonEcole, l'adresse IP du DNS à renvoyer correspond à celle renseignée dans `Adresse IP pour le proxy (adresse ip eth1 proxy link)` de l'onglet `Interface-1` de l'interface de configuration du module.

Paramètres globaux et surcharge

En mode expert, les champs `Nom de domaine à renvoyer aux clients DHCP`, `Adresse IP du routeur à renvoyer aux clients DHCP`, `Adresse IP du DNS à renvoyer aux clients DHCP` et `Adresse IP du DNS secondaire à renvoyer aux clients DHCP` permettent de spécifier des valeurs pour les paramètres globaux. Ils peuvent être surchargés pour un sous-réseau spécifique.



Un certain nombre de paramètres peuvent être spécifiés ou modifiés dans les paramètres globaux et/ou pour les sous-réseaux.



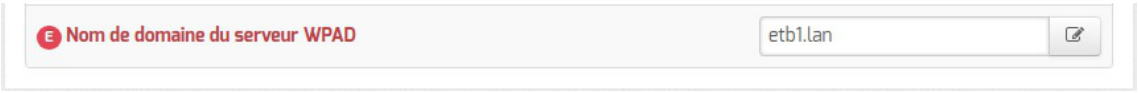
Il est possible de spécifier les adresses IP de Wins primaire et secondaire à renvoyer aux clients.

L'adresse d'un serveur de temps à renvoyer aux clients peut être spécifié : `Adresse IP du serveur NTP à renvoyer aux clients`.

Passer `Interdire cette zone aux hôtes inconnus` à `oui` permet d'activer l'option `deny unknown-clients` qui interdit l'attribution d'une adresse IP à une station dont l'adresse MAC est inconnue du serveur (gestion des adresses MAC connues au travers de l'EAD).

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

Il est possible de modifier les durées du bail DHCP : `Temps du bail par défaut (sec)` et `Temps maximum du bail (sec)`.



Le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.

Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.

Pour les postes de travail Windows c'est la valeur du champ `Nom de domaine du serveur WPAD` qui sera utiliser pour accéder au fichier WPAD tandis que pour des postes de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.

Configurer la continuité de service

À partir de la version 2.6.2, il est possible de mettre en place de la continuité de service pour le DHCP.
Elle permet à deux serveurs DHCP d'opérer sur les mêmes sous-réseaux et mêmes pools d'adresses IP.
Il faut donc un serveur DHCP primaire et un serveur DHCP secondaire.

Les ports d'écoute et de contact du serveur primaire doivent être inversés pour le serveur secondaire. Il est également possible d'utiliser le port 647 partout, c'est à dire en écoute et en contact aussi bien sur le serveur primaire que sur le serveur secondaire.

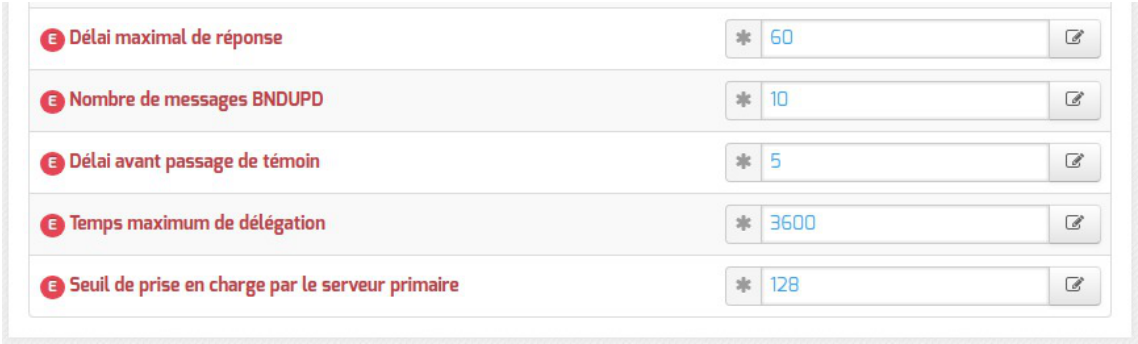
Paramétrage du serveur primaire



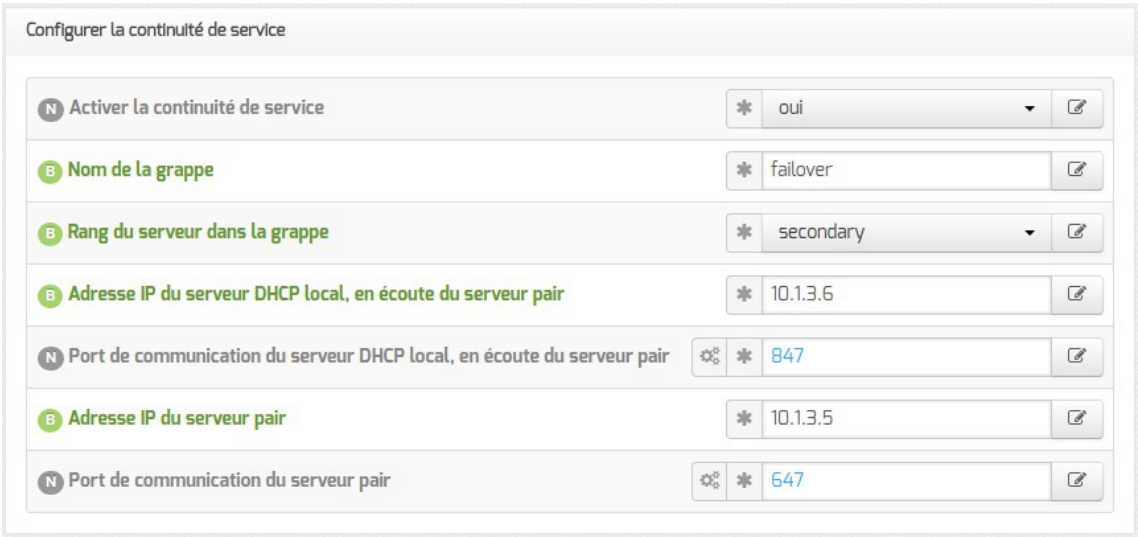
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Nom de la grappe` : le nom de la grappe devra être le même sur le serveur primaire (local) et sur le serveur secondaire (pair) ;
- `Rang du serveur dans la grappe` : choisir `primary` pour le serveur primaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de l'interface sur laquelle écoute le service DHCP local (IP de l'Interface-0 dans la plupart des cas) ;
- `Port de communication du serveur DHCP local, en écoute du serveur pair` : le port par défaut pour un serveur primaire est `647` ;
- `Adresse IP du serveur pair` : saisir l'adresse IP du serveur secondaire (pair) ;
- `Port de communication du serveur pair` : le port par défaut est `847`.

En mode expert, un certain nombre de variables permettent d'ajuster finement la configuration du failover et de la répartition de charge.



Paramétrage du serveur secondaire



Pour un serveur secondaire, les variables à paramétrer sont :

- `Nom de la grappe` : le nom de la grappe doit être le même que pour le serveur primaire (local) ;
- `Rang du serveur dans la grappe` : choisir `secondary` pour le serveur secondaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de l'interface sur laquelle écoute le service DHCP local (IP de l'Interface-0 dans la plupart des cas) ;
- `Port de communication du serveur DHCP local, en écoute du serveur pair` : le port par défaut pour un serveur secondaire est `847` ;

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

- `Adresse IP du serveur pair` : saisir l'adresse IP du serveur secondaire (pair) ;
- `Port de communication du serveur pair` : le port par défaut est `647`.

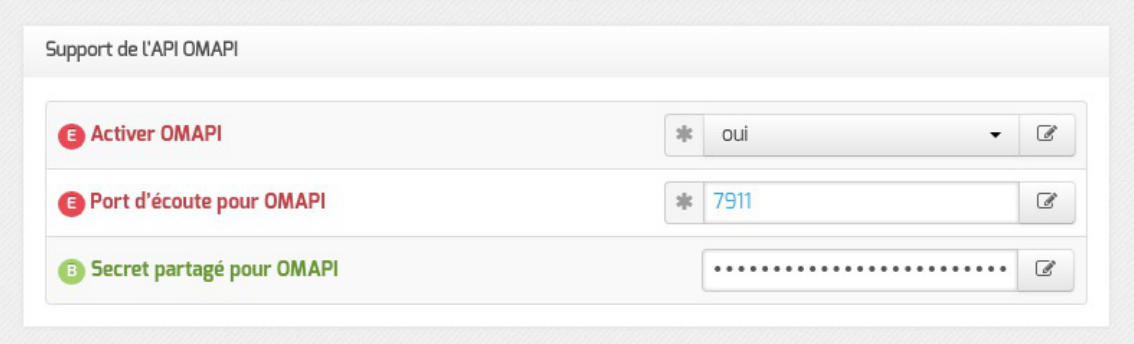
En mode expert, un certain nombre de variables permettent d'ajuster finement la configuration du failover.



Support de l'API OMAPI

Le serveur DHCP offre la possibilité de modifier une partie de sa configuration en cours d'exécution, sans l'arrêter, de modifier ses fichiers de base de données et de la redémarrer. Cette capacité est actuellement fournie en utilisant OMAPI[p.511], une API pour manipuler les objets distants.

Activer le support OMAPI affiche les variables permettant de configurer le service.



Le port d'écoute déclaré peut être modifié et est pris en compte par bastion[p.495].
La clé secrète sera à utiliser pour que les clients du service s'authentifient.

Voir aussi...

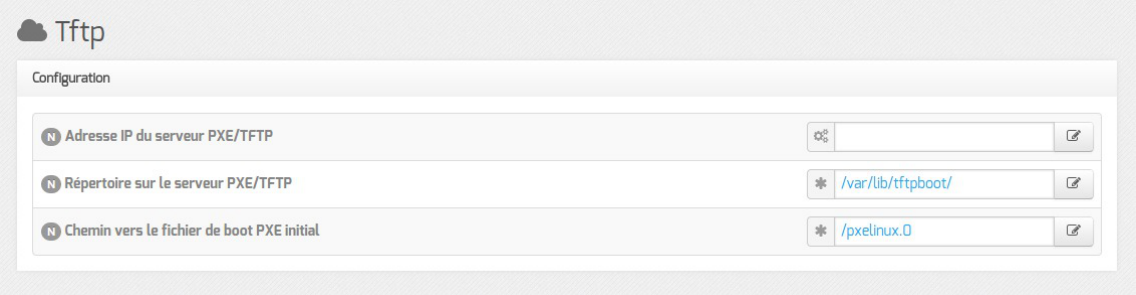
> Configurer la découverte automatique du proxy avec WPAD

4.14. Onglet Tftp : Configuration d'un serveur PXE/TFTP

Il est possible d'activer un service d'amorçage PXE sur le module. Une station de travail pourra alors démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur.

La configuration du serveur PXE/TFTP se trouve dans l'onglet `Tftp`, celui-ci n'est disponible qu'en mode expert après activation du service dans l'onglet `Services`.

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



Vue de l'onglet Tftp

L'adresse IP du serveur PXE/TFTP proposée par défaut est celle de l'interface 0 précédemment configurée.

Si le service DHCP local est activé et que l'adresse d'un serveur TFTP distant est saisie, le service DHCP renverra les stations qui le demandent vers ce serveur (directive : `next-server`).

Si le serveur TFTP est local, la variable `Répertoire sur le serveur PXE/TFTP` définit le répertoire dans lequel se trouve le ou les fichiers de boot PXE.

Si le service DHCP local est activé, la variable `Chemin vers le fichier de boot PXE initial` définit le nom du fichier de boot PXE initial renvoyé par le service DHCP (directive : `filename`).

Cette fonctionnalité permet notamment la mise en place d'un logiciel de clonage permettant de restaurer des images sauvegardées de poste clients.

Exemple d'OSCAR[p.512], outil de clonage édité par le CRDP de Lyon (http://oscar.crdp-lyon.fr) :

- Un procédure pour la mise en place d'OSCAR est disponible sur la forge EOLE à l'adresse : http://dev-eole.ac-dijon.fr/projects/oscar/wiki
- Une documentation sur l'utilisation d'OSCAR est disponible à l'adresse : http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/scribe/formationadminscribeoscar

4.15. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.511]. 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)

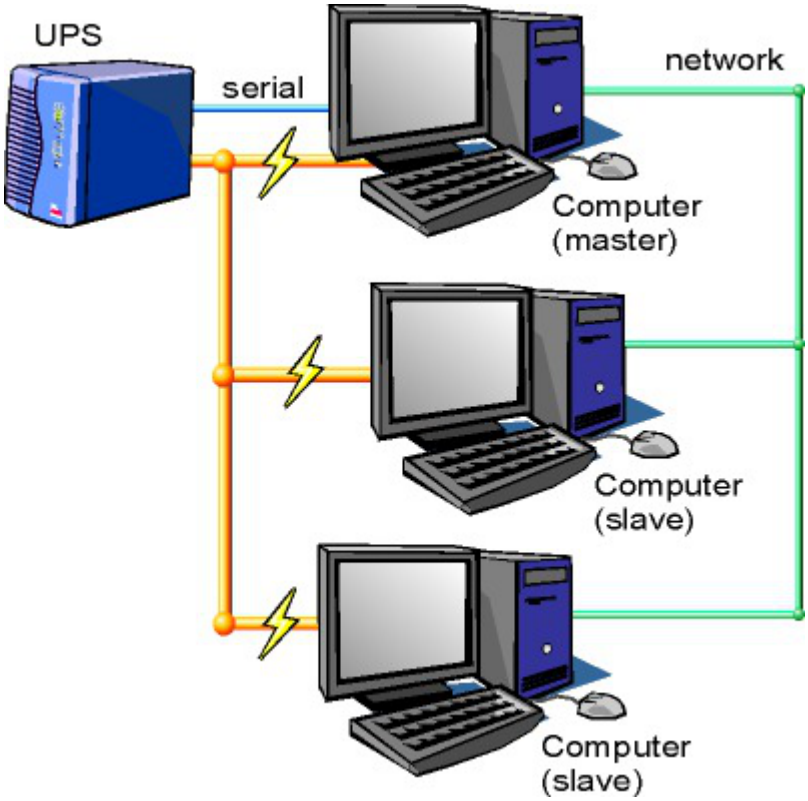


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

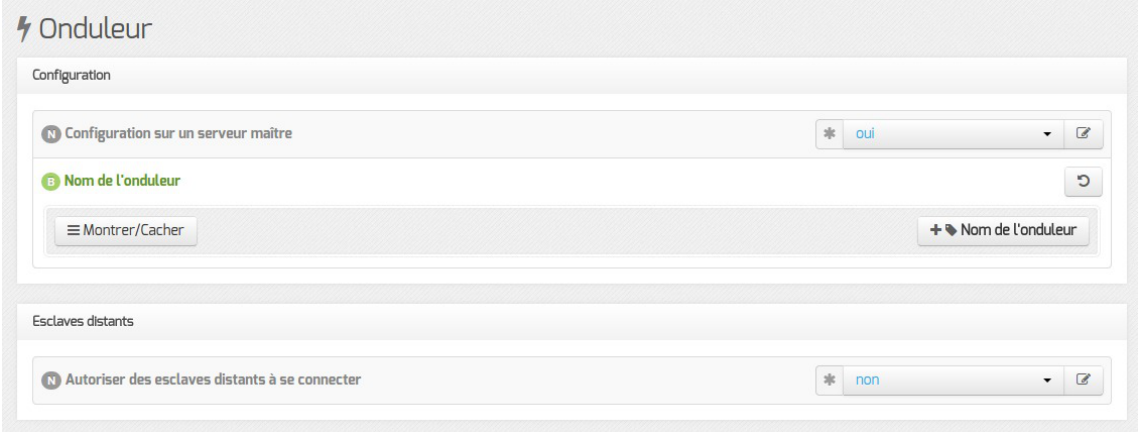
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

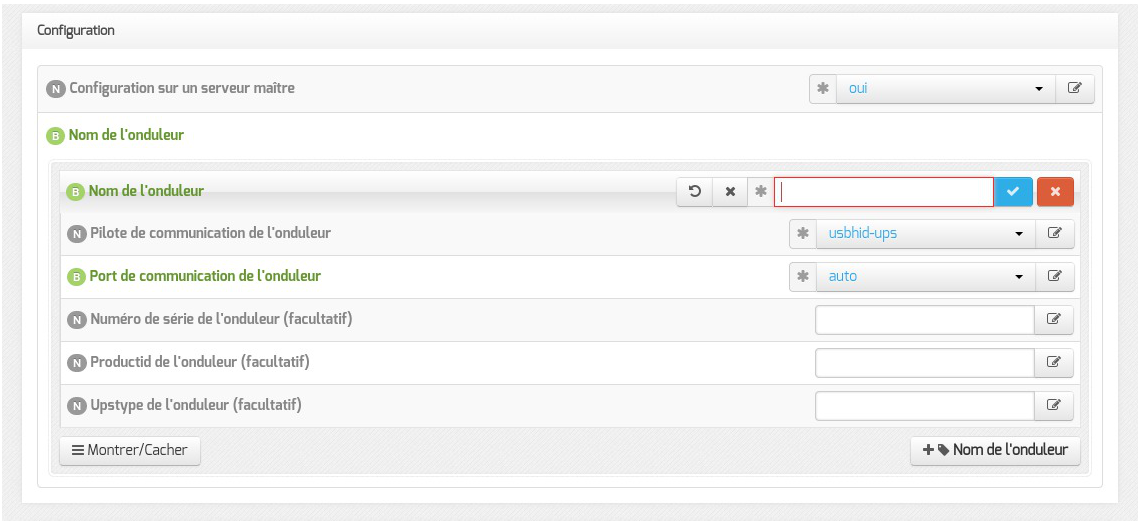
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

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)

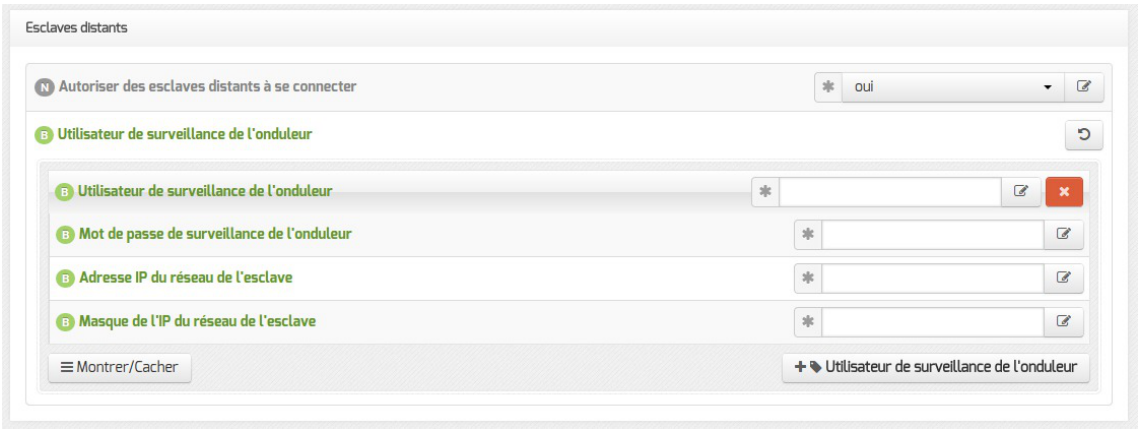
- Port de communication de l'onduleur : `auto`.

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` ;

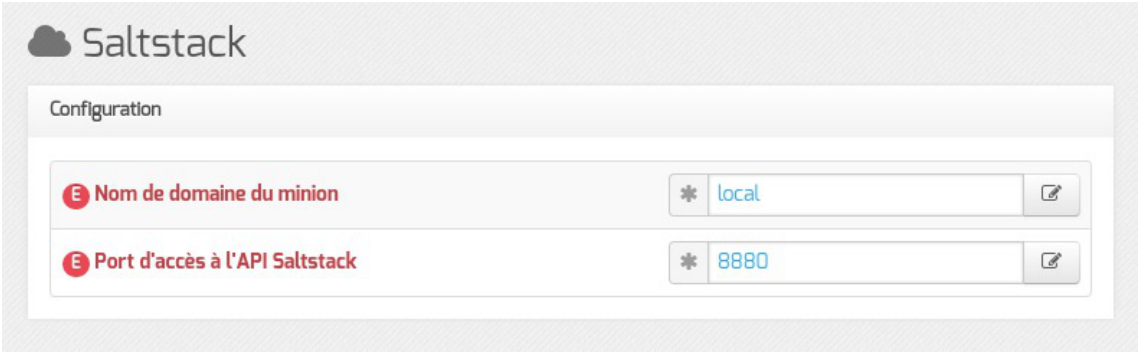
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

4.16. Onglet Saltstack

L'onglet `Saltstack` permet de personnaliser la configuration de Saltstack[p.516].

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.

4.17. Onglet Ead-web : EAD et proxy inverse

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



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

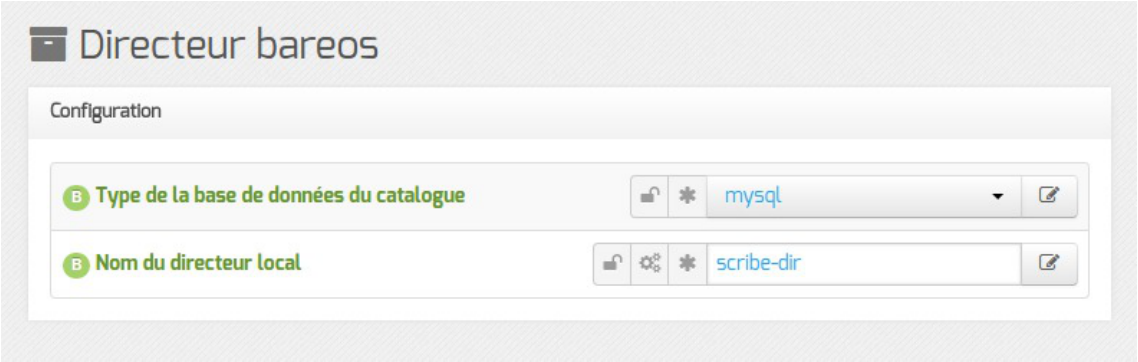
Si la variable est passée à `oui`, le port proposé pour accéder à l'EAD depuis l'extérieur est par défaut 4203.

Voir aussi...

> Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur [p.261]

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

4.18. Onglet Directeur bareos

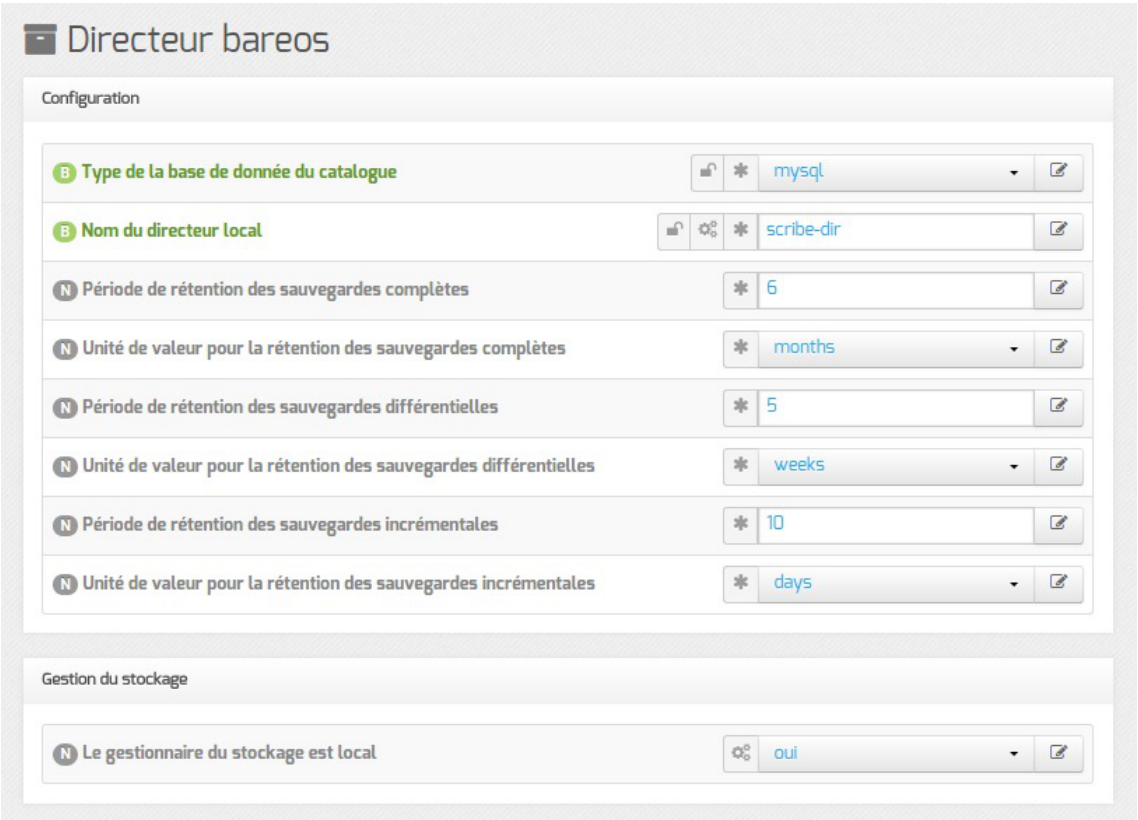


Le type de base de données permet de choisir si l'enregistrement du catalogue se fait dans MySQL ou dans SQLite. Il ne sera plus possible de modifier ce paramètre après l'enregistrement de la configuration.

Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

Le nom du directeur est une information importante, il est utilisé en interne dans le logiciel mais, surtout, il est nécessaire pour configurer un client Bareos ou pour joindre le serveur de stockage depuis un autre module.

À l'enregistrement du fichier de configuration il ne sera plus possible de modifier le nom du directeur, en effet cette variable est utilisée dans les noms des fichiers de sauvegarde.



Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention[p.499] des différents espaces de stockage (totale, différentielle et incrémentale).

La durée de rétention des fichiers détermine le temps de conservation avant l'écrasement.

Plus les durées de rétention sont importantes, plus l'historique sera important et plus l'espace de stockage nécessaire sera important.

Il peut être intéressant de conserver un historique long mais avec peu d'états intermédiaires.

Pour cela, voici un exemple de configuration :

- 6 mois de sauvegardes totales ;
- 5 semaines de sauvegardes différentielles ;
- 10 jours de sauvegardes incrémentales.

Avec la politique de sauvegarde suivante :

- une sauvegarde totale par mois ;
- une sauvegarde différentielle par semaine ;
- une sauvegarde incrémentale du lundi au vendredi.

Dans l'historique, il y aura donc une sauvegarde par jour de conservée pendant 10 jours, une sauvegarde par semaine pendant 5 semaines et une sauvegarde mensuelle pendant 6 mois.

Une modification de la durée de rétention en cours de production n'aura aucun effet sur les sauvegardes déjà effectuées, elles seront conservées et recyclées mais sur la base de l'ancienne valeur, stockée dans la base de données.

Afin de prendre en compte la nouvelle valeur pour les sauvegardes suivantes, il faut utiliser les outils Bareos pour mettre à jour la base de données :

```
# bconsole
*update
*2
*<numéro du pool de volumes de sauvegarde>
```

Une autre solution consiste à vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et à ré-initialiser la base de données Bareos avec la commande :

```
# bareosregen.sh
La regénération du catalogue de bareos va écraser l'ancienne base, confirmez-vous ? [oui/non]
[non] : oui
```

Configuration du stockage

Le stockage peut être local ou distant, il est local par défaut.

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

Dans ce cas aucun paramètre n'est à configurer dans l'onglet `Directeur Bareos`.

Par contre des paramètres vous permettant éventuellement d'autoriser des directeurs à se connecter au présent stockage dans l'onglet `Stockage bareos`.

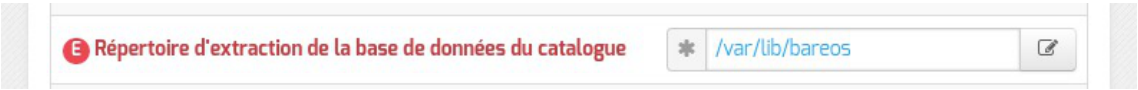


Vue de l'onglet Directeur Bareos

Dans le cas d'un serveur distant (`Activer le serveur de stockage localement` à `non`), il faut configurer l'adresse IP et le mot de passe du serveur de stockage distant.

> Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.
>
> Le déport du service `bareos-sd` sur un autre serveur que `bareos-dir` ne permet pas de gérer correctement les verrous des tâches d'administration sur ce serveur : `bareos-dir` ne permet pas de signaler efficacement à `bareos-sd` qu'une sauvegarde est lancée et qu'il doit poser un verrou empêchant les autres tâches d'administration.

En mode expert, il est possible de modifier le répertoire utilisé par défaut pour l'extraction de la base de données du catalogue. Ce changement permet éventuellement de ne pas surcharger l'espace occupé dans `/var`.



Il est également possible de définir manuellement le mot de passe de la base de donnée MySQL, le délai accordé à l'exécution de la sauvegarde ainsi que l'algorithme de compression utilisé pour le stockage.



Vue de l'onglet Directeur Bareos



Type de compression et délai alloué

La durée maximale pour l'exécution complète d'une sauvegarde permet d'arrêter le job après un temps d'exécution fixé en seconde, par défaut le job est limité à 86 400 secondes soit 24 heures (la valeur 0 lève cette limite de temps).

Plus l'algorithme est efficace, moins il nécessite d'espace mais plus il alourdit la charge système et

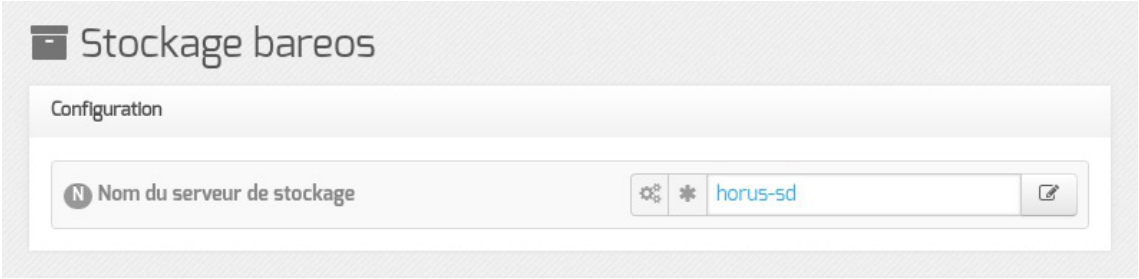
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

allonge la durée du processus de sauvegarde. Le taux de compression est exprimé par un chiffre de 1 à 9, proportionnel. Au delà de 6, le gain en place est faible par rapport aux niveaux immédiatement inférieurs, tandis que la durée de traitement s'allonge sensiblement.

Le champ `Mot de passe du directeur` contient le mot de passe à transmettre aux applications distantes pour leur permettre de s'authentifier auprès du directeur.

4.19. Onglet Stockage bareos

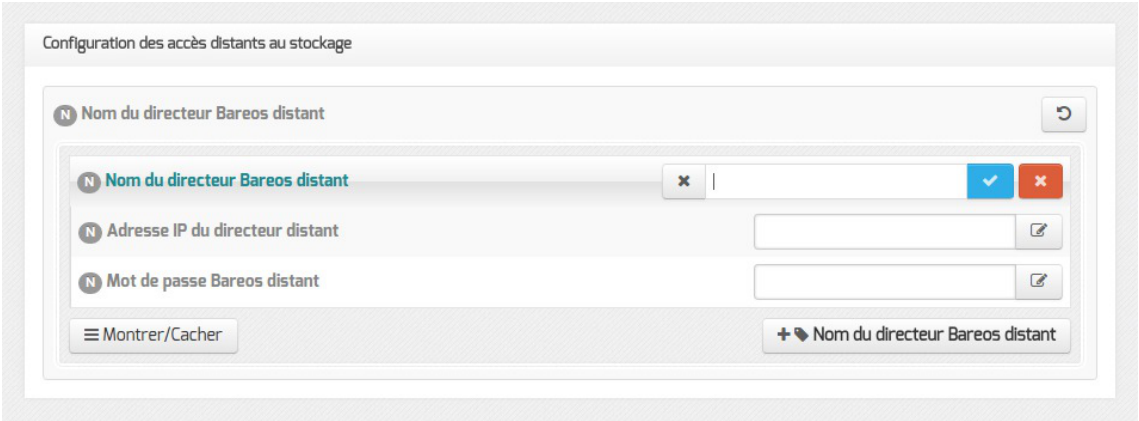
Dans l'onglet `Stockage bareos` il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur `Nom du directeur Bareos distant`, le détail de l'autorisation s'affiche.

Pour ce faire il faut se munir des paramètres du directeur distant :

- son nom ;
- son adresse IP ;
- son mot de passe.



Autoriser des clients Bareos distants à se connecter au directeur

Les sauvegardes sont des informations sensibles. Il ne faut pas utiliser de mot de passe facilement déductible.

Voir aussi...

Les mots de passe [p.229]

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

4.20. Onglet Cups : Configuration du serveur d'impression

CUPS, pour Common Unix Printing System, est un système modulaire d'impression informatique pour les systèmes d'exploitation Unix et assimilés. Ce serveur d'impression accepte des documents envoyés par des ordinateurs clients, les traite, et les envoie à l'imprimante qui convient.

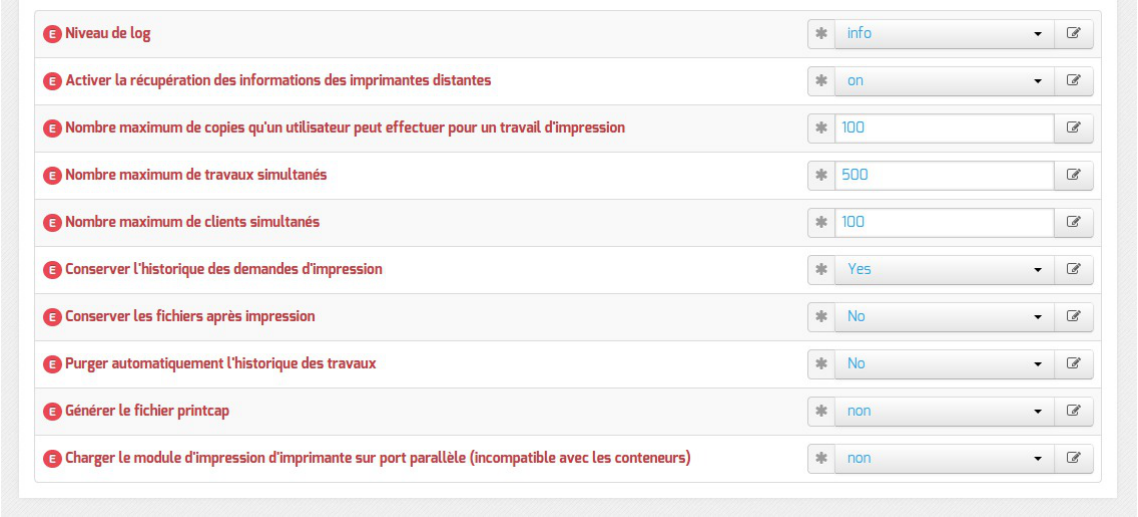
Le serveur d'impression est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option : `Activer le serveur d'impression CUPS`.

L'onglet `Cups` apparaît en mode expert uniquement si le service est activé.

L'onglet expert `Cups` permet de configurer l'imprimante virtuelle PDF.



Il est possible de désactiver l'imprimante virtuelle PDF, de changer son nom et de ne pas la partager.



L'onglet expert `Cups` permet de modifier et de fixer une sélection de paramètres disponibles dans le fichier de configuration : `/etc/cups/cupsd.conf`.



Le nom des paramètres en question est utilisé dans le nom des variables Creole. Ils sont généralement préfixés par la chaîne "`cups_`".

Pour les faire apparaître il faut activer le mode debug de l'interface de configuration du module.

Niveau de log

Le niveau de journalisation est par défaut à `warn`. Celui-ci peut être modifié afin d'obtenir plus ou moins

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

de verbosité.

Activer la récupération des informations des imprimantes distantes

Indique si oui ou non les imprimantes partagées doivent être annoncés.

Nombre maximum de copies qu'un utilisateur peut effectuer pour un travail d'impression

Indique le nombre maximum de copies qu'un utilisateur peut imprimer de chaque travail.

Nombre maximum de travaux simultanés

Indique le nombre maximum de travaux simultanés supportés.

Nombre maximum de clients simultanés

Indique le nombre maximum de clients simultanés supportés.

Conserver l'historique des demandes d'impression

Indique s'il faut ou non préserver l'historique des demandes d'impression.

Conserver les fichiers après impression

Indique s'il faut ou non conserver les fichiers de travail après leur impression.

Purger automatiquement l'historique des travaux

Indique s'il faut ou non purger automatiquement l'historique des travaux lorsqu'il n'est plus utilisé pour la gestion des quotas.

Générer le fichier printcap

Cette variable permet de générer un fichier `printcap`.

Le fichier /var/run/cups/printcap contient la configuration pour vos imprimantes. Chaque entrée définit une imprimante, lui donne un nom pour vous et pour les utilisateurs. Vous pouvez avoir plusieurs imprimantes dans ce fichier qui correspondent à la même imprimante physique, mais qui utilisent des fonctionnalités différentes. Il y a au minimum une entrée `printcap` par imprimante physique présente sur votre système.

Charger le module d'impression d'imprimante sur port parallèle (incompatible avec les conteneurs)

Active / désactive le chargement du module permettant le support d'imprimante parallèle au démarrage du service CUPS.



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

```
# man cupsd.conf
```

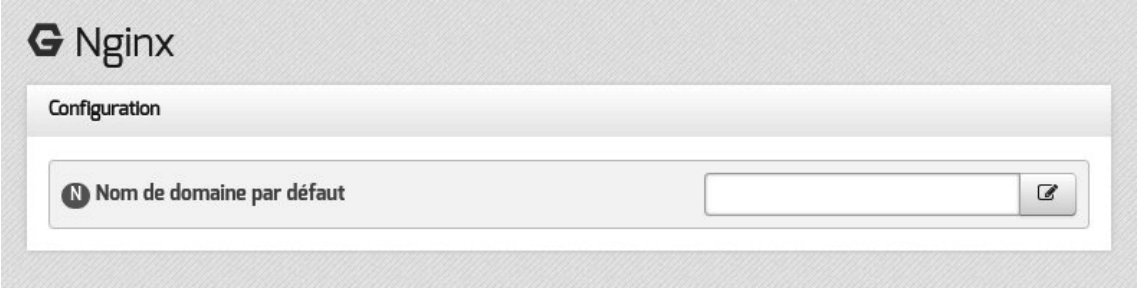
ou en visitant la page suivante : http://manpages.ubuntu.com/manpages/xenial/en/man5/cupsd.conf.5.html

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

4.21. 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` ;
- `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

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

> `server_names_hash_bucket_size: 32`
>
> Nginx Optimization : http://nginx.org/en/docs/http/server_names.html#optimization

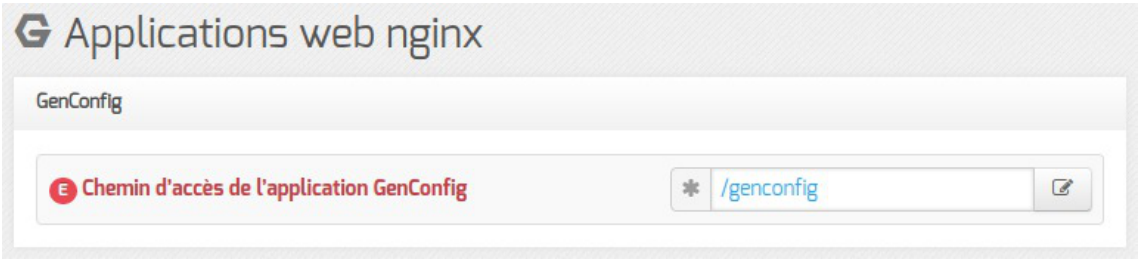
Taille maximale des données reçues par la méthode POST

L'option `Taille maximale des données reçues par la méthode POST (en Mo)` permet 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.

4.22. 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.

4.23. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.510].

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.499] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.518].

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.504]*/DNAT*.

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

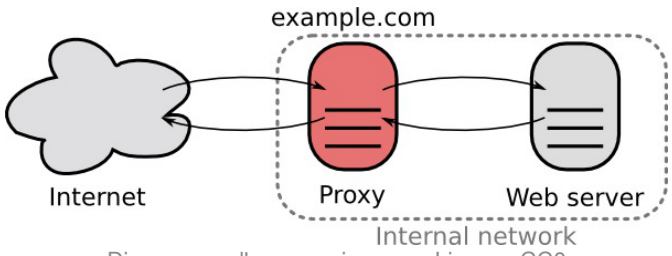
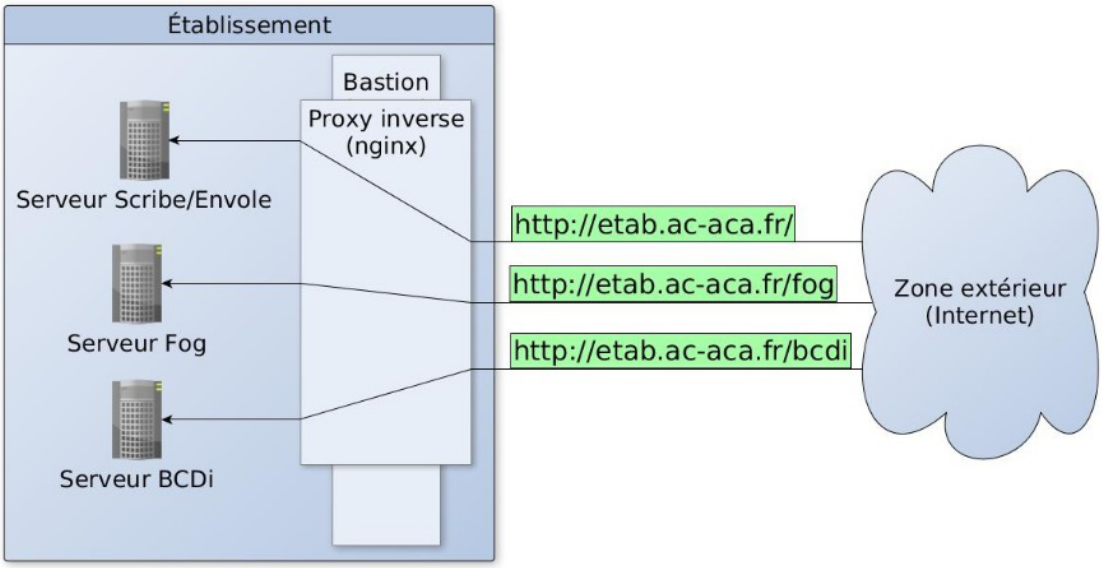


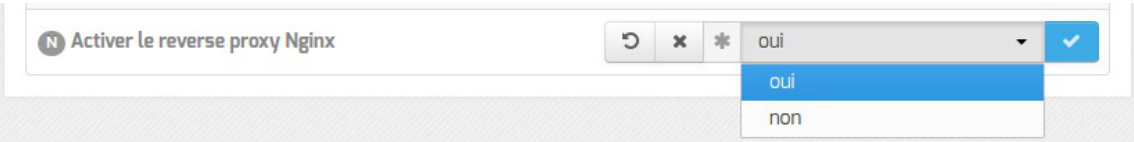
Diagramme d'un proxy inverse - Licence CC0

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

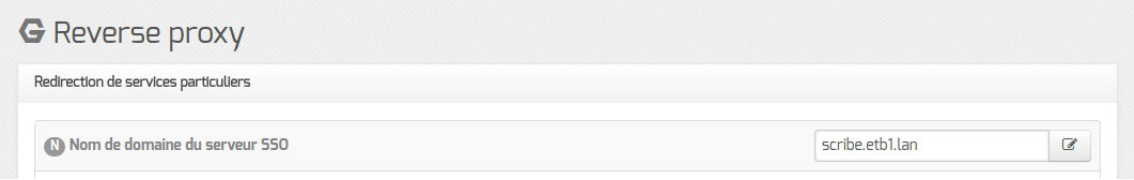
- serveur EoleSSO ;
- outil d'administration EAD[p.500] ;
- application EOP ;
- protocole HTTP[p.503] ;
- protocole HTTPS[p.503].



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

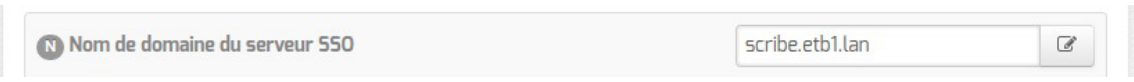


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

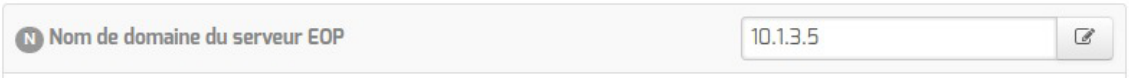
Redirection du service EoleSSO



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.522]).

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

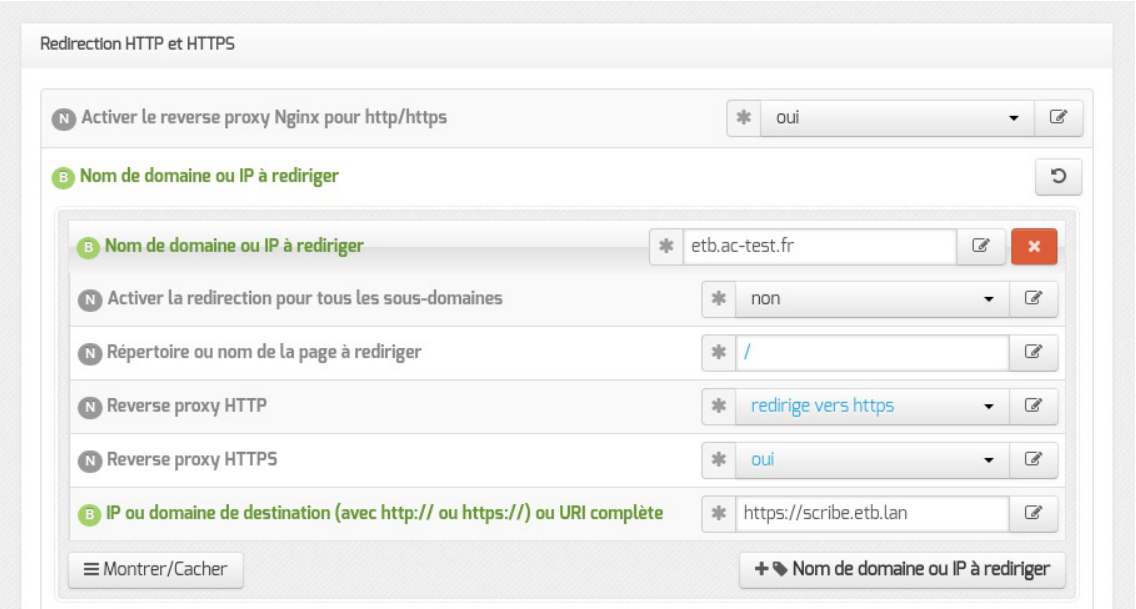


Pour accéder de manière sécurisée à l'EAD d'un serveur depuis l'extérieur de l'établissement, il est recommandé :

- 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

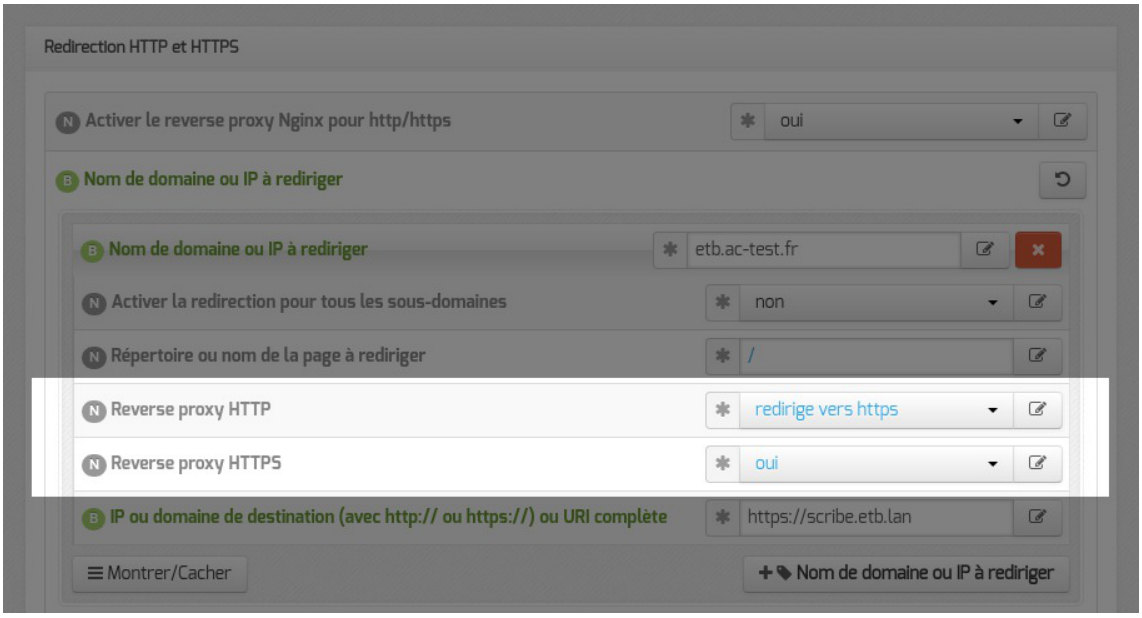
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 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.521] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.

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



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`.

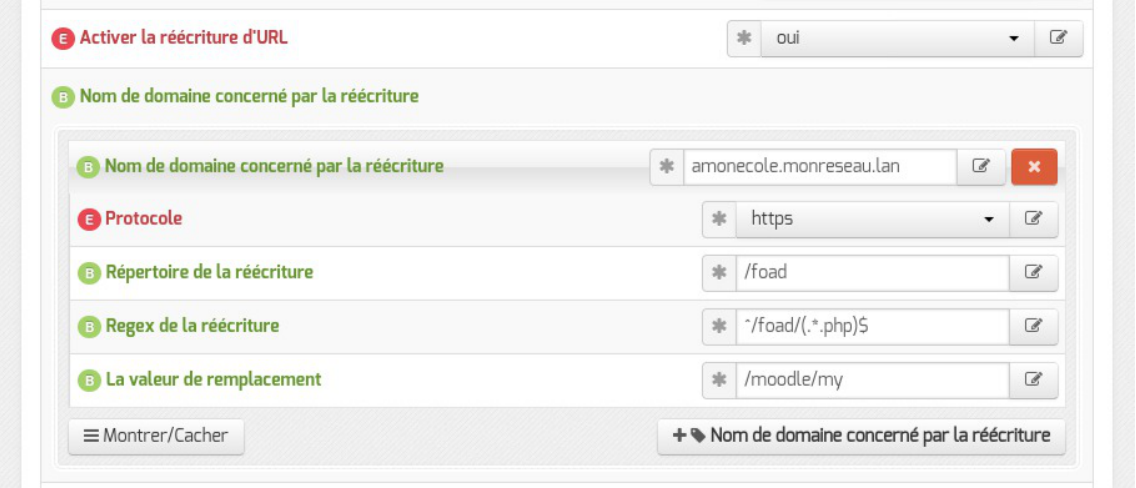


Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.514], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Réécriture d'URL

L'activation de la réécriture d'URL permet d'ajouter une expression rationnelle et une valeur de remplacement.

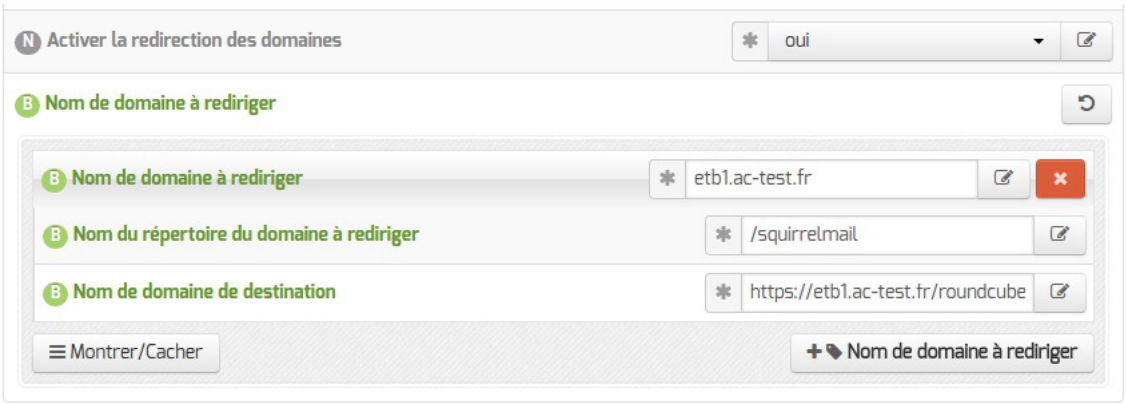
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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/`.

4.24. Onglet Active Directory

La fonctionnalité Active Directory est assurée par le logiciel Samba 4[p.516] en mode Active Directory.

Depuis la version 4.4.6 de Samba, la personnalisation du calcul des identifiants pose problème sur un contrôleur de domaine :

https://wiki.samba.org/index.php/Updating_Samba#Failure_To_Access_Shares_on_Domain_Controllers

À partir de la version 2.6.1 d'EOLE, le module Seth utilise la version 4.5 de Samba.

Cette version de samba permet notamment la prise en compte de plusieurs DNS Forwarders[p.499] :

https://wiki.samba.org/index.php/Samba_4.5_Features_added/changed#Multiple_DNS_Forwarders_on_

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

Ainsi, la liste complète des serveurs DNS renseignés dans l'interface de configuration du module est prise en compte (et plus seulement le premier de la liste).

À partir de la version 2.6.2 d'EOLE, le module Seth utilise la version 4.7 de Samba.

Cette version est la première à supporter officiellement le RODC[p.515]. Pour un contrôleur de domaine additionnel, l'activation de ce paramètre est accessible en mode expert.



À partir d'EOLE 2.6.2, l'instance échoue si la version de Samba installée sur le module n'est pas celle attendue.

Les paquets `samba` doivent impérativement être mis à jour via Maj-Auto avant l'instance.

Rôle du serveur Active Directory



Cette variable permet de choisir le Rôle du serveur :

- contrôleur de domaine ;
- serveur membre d'un domaine existant.

Dans le cas où le serveur à mettre en place a le rôle de contrôleur de domaine, il faut définir si celui-ci est le contrôleur de domaine principal ou si il s'agit d'un contrôleur additionnel.

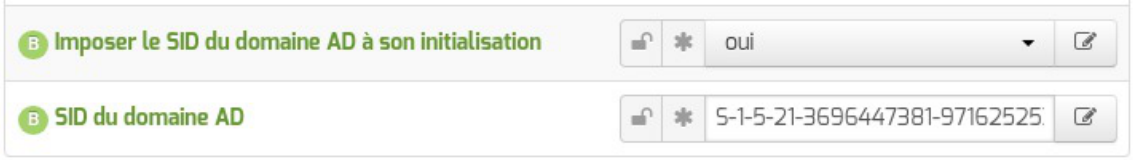


Imposer le SID du domaine AD à son initialisation

Dans le cas d'une migration ou d'une réinstallation d'un contrôleur de domaine principal, il est possible de forcer le SID[p.517] à utiliser pour le domaine.

À partir de la version 2.6.2, forcer le SID s'effectue en deux temps :

- en passant la variable `Imposer le SID du domaine AD à son initialisation` à `oui` ;
- en renseignant la variable `SID du domaine AD`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.



La prise en compte du SID forcé est réalisée lors de l'initialisation de l'annuaire Active

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

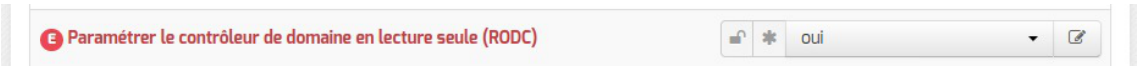
Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le SID n'est pas validé au moment de la saisie. Il est nécessaire de s'assurer qu'il est correct avant de sauvegarder.

Contrôleur de domaine en lecture seule

Dans le cas d'un contrôleur de domaine additionnel, il est possible de préciser si celui-ci est en lecture seule (RODC[p.515]) ou non.

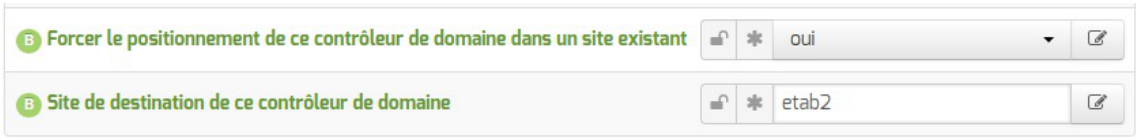


Forcer le positionnement dans un site AD à l'initialisation

À partir de la version 2.6.2, il est possible de demander à ce qu'un contrôleur de domaine additionnel soit rattaché à un site Active Directory particulier.

Cette demande s'effectue en deux temps :

- en passant la variable `Forcer le positionnement de ce contrôleur de domaine dans un site existant` à `oui` ;
- en renseignant la variable `Site de destination de ce contrôleur de domaine`.



Après sauvegarde et instance, ces deux variables sont verrouillées et ne peuvent plus être modifiées.

La prise en compte du domaine de rattachement est réalisée lors de l'initialisation de l'annuaire Active Directory.

Cette variable n'a plus d'utilité une fois le module instancié.

Le site doit impérativement avoir été déclaré au préalable sur le contrôleur de domaine principal.

Si le contrôleur de domaine principal est un module Seth, la déclaration d'un site s'effectue facilement grâce à la fonction bash `samba_update_site` :

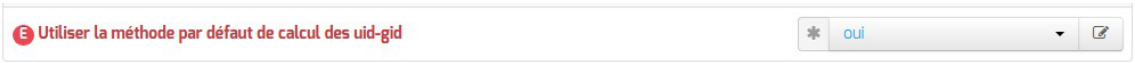
```
. /usr/lib/eole/samba4.sh
samba_update_site monsite 10.1.1.0/24
```

Méthode de calcul des uid-gid

Dans le cas d'un serveur membre d'un domaine existant, il est possible de personnaliser la méthode de calcul des UID / GID (IDMAP[p.503]) en passant la variable `Utiliser la méthode par défaut de`

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

`calcul des uid-gid` à `non`.



Plusieurs domaines cibles avec des limites haute et basse d'adresse IP et des méthodes de calcul différentes (rid, autorid, ad, ldpa, tdb, nss) peuvent être déclarés.

Depuis la version 4.4.6 de Samba, la personnalisation du calcul des identifiants pose problème sur un contrôleur de domaine.

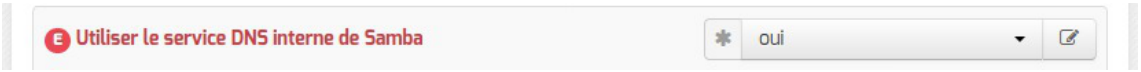
https://wiki.samba.org/index.php/Updating_Samba#Failure_To_Access_Shares_on_Domain_

Mise en œuvre du service DNS

Sur les contrôleurs de domaine, un service DNS[p.499] est obligatoirement mis en place.

Le service DNS peut être assuré par un composant interne de Samba (par défaut) ou délégué à Bind9[p.495].

Le choix du composant à utiliser s'effectue à l'aide de la variable : `Utiliser le service DNS interne de Samba`.



En laissant à `oui`, le choix par défaut, le service DNS est assuré par le composant interne de Samba. En passant à `non`, Bind9 est activé et la configuration mise en place pour le lien entre Samba et Bind9.

Le comportement des deux services est similaire. L'utilisation de Bind9 ne change pas la manière d'ajouter les machines à la base de données DNS de Samba qui en garde la gestion. Bind9 interroge cette base via un greffon.

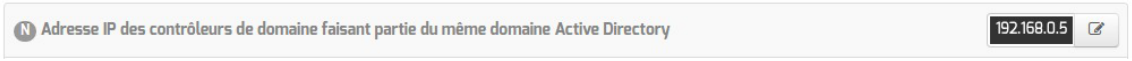
Dans une infrastructure mettant en œuvre plusieurs contrôleurs de domaine et la synchronisation des données de l'AD, il est impératif de mettre en œuvre le même type de service DNS pour tous les contrôleurs de domaine.

Dans le cas contraire, la réplication avec la commande `samba-tool drs` provoquera une erreur.

Environnement réseau

Adresse des contrôleurs du même domaine

Si plusieurs contrôleurs de domaine doivent être mis en place, il est impératif qu'ils se connaissent les uns les autres.



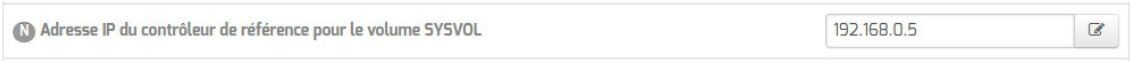
La variable `Adresse IP des contrôleurs de domaine faisant partie du même domaine Active Directory` permet de déclarer les adresses IP des autres contrôleurs du domaine.

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

Sur EOLE 2.6.2, cette variable est intitulée : `Adresse IP des contrôleurs de domaine en relation avec ce contrôleur de domaine Active Directory`.

Contrôleur de référence pour le volume SYSVOL

Dans le cas de la mise en œuvre d'un contrôleur de domaine additionnel, il est recommandé de déclarer le contrôleur de domaine principal en tant référence pour le volume SYSVOL.



Dans le monde Microsoft, les contrôleurs de domaine sont habituellement tous au même niveau. Ceci est possible grâce à la réplication de l'annuaire Active Directory et à l'utilisation d'un système de fichiers distribué (DFS[p.498]).

À l'heure actuelle, la réplication du partage SYSVOL[p.519] n'est pas supportée par Samba. De ce fait, la mise en œuvre d'une architecture multi-DC[p.510] avec le module Seth nécessite de définir un contrôleur de domaine principal qui héberge les fichiers SYSVOL de référence et des contrôleurs de domaine additionnels sur lesquels ces fichiers sont synchronisés à intervalle régulier via rsync[p.516].

Pages relatives au support DFS sur le Wiki Samba

- https://wiki.samba.org/index.php/Distributed_File_System_(DFS)
- https://wiki.samba.org/index.php/SysVol_replication_(DFS-R)

Restrictions d'accès réseau

Le bon fonctionnement d'une infrastructure basée sur un serveur Active Directory nécessite un certain nombre d'interactions avec d'autres serveurs et les postes clients.

Les ports suivants sont concernés par ces interactions :

- 53 (DNS)
- 5353 (broadcast DNS)
- 123 (NTP)
- 88 (Kerberos)
- 445 (SMB CIFS)
- 135 (MSRPC)
- 3268 (Global Catalog)
- 3269 (Global Catalog)
- 464 (kpasswd)
- 389 (ldap)
- 636 (ldaps)

Les ports suivants peuvent être ouverts si nécessaires mais concernent un protocole obsolète :

- 137 (NetBIOS)

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

- 138 (NetBIOS)
- 139 (NetBIOS)

Restriction d'accès

En mode expert, il est possible de restreindre l'accès réseau sur les services Samba et LDAP à des sources spécifiques.

> Sur un module Seth, l'accès aux services Samba et LDAP est ouvert à toutes les sources par défaut.

Restriction d'accès en 2.6.1

En 2.6.1, la restriction d'accès n'est effective que si les différentes variables d'autorisations d'accès sont saisies.



Ces différentes variables supplémentaires donnent la possibilité de restreindre les accès à des ensembles de machines potentiellement différentes pour des ensembles de services.

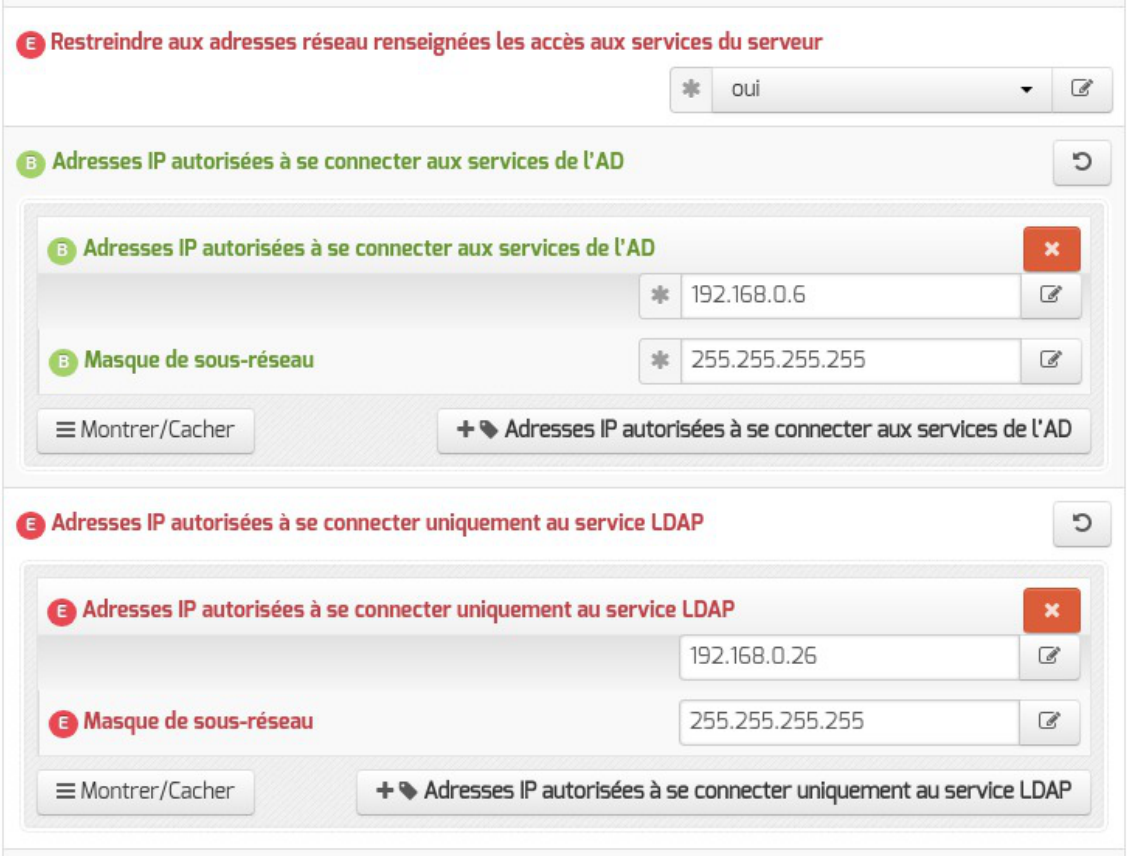
Les clients et serveurs du domaine doivent accéder aux services de samba-ad. D'autres machines peuvent avoir besoin d'accéder à l'annuaire Active Directory (LDAP).

Restriction d'accès en 2.6.2

À partir d'EOLE 2.6.2, ne subsiste qu'une liste unique pour les sources pouvant accéder à tous les services.

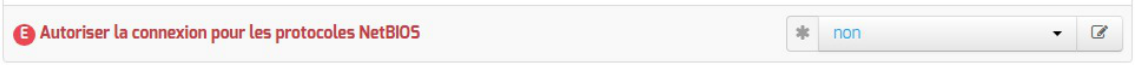
La liste pour les sources ne nécessitant uniquement un accès au service LDAP est conservée.

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



Ports NetBIOS

En mode expert, il est possible d'autoriser ou non l'accès au serveur via les ports NetBIOS.

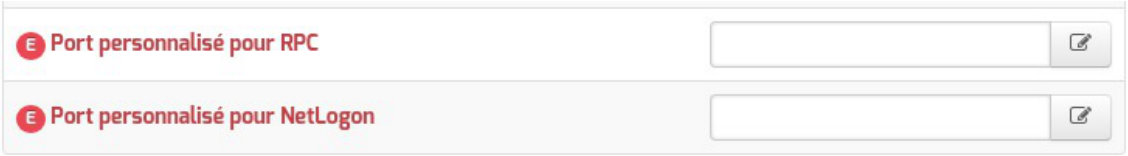


Sur un module Seth, les services historiques NetBIOS[p.510] (ports 137 à 139) sont désactivés par défaut.

Personnalisation des ports RPC

À partir d'EOLE 2.6.2, les ports de communication RPC[p.516] sont personnalisables.

Si ils ne sont pas configurés, le comportement antérieur est conservé par Samba : le premier port libre dans la plage 1024-5000 est utilisée.



Partage de fichiers

Activation du module de prise en charge des corbeilles

Par défaut lorsque l'on supprime un fichier depuis un partage Samba, il est directement supprimé.

L'option `Charger le module recycle pour la prise en charge des corbeilles` paramètre Samba afin que les fichiers supprimés soient déplacés dans un répertoire tampon avant la

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

suppression définitive.



Le nom proposé par défaut, `.corbeille`, définit un répertoire qui sera masqué pour les utilisateurs.

Il est possible de rendre ce répertoire accessible en supprimant le . dans le nom du répertoire.

La durée de conservation des fichiers supprimés est paramétrable.

Les fichiers déplacés dans la corbeille sont inclus dans le calcul de l'espace disque occupé par l'utilisateur. Pour limiter les dépassements de quota disque, il est conseillé de paramétrer une durée de conservation assez courte.

L'activation du module Samba recycle, n'active pas automatiquement la corbeille sur les répertoires partagés.

Pour activer la corbeille sur les répertoires personnels des utilisateurs, il faut passer la variable `Activer la corbeille pour le partage "homes"` à `oui`.

Il est également possible de l'activer sur les répertoires partagés, mais cela s'effectue au cas par cas.

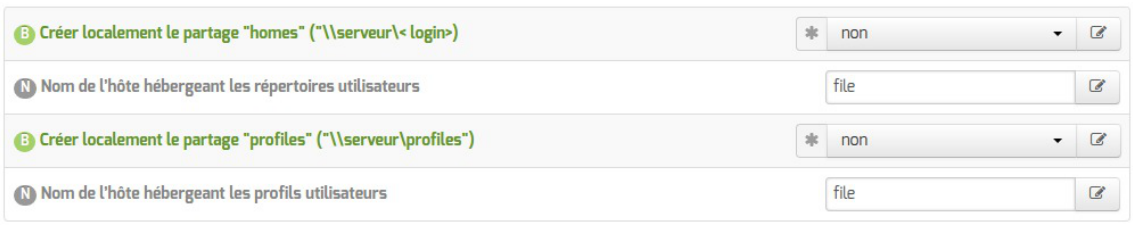
Partages utilisateur

Les partages utilisateur et les autres répertoires partagés peuvent être locaux et/ou hébergés sur d'autres serveurs Active Directory.

Sur le serveur local, il est possible d'activer ou non l'hébergement des partages « homes » et « profiles » des utilisateurs.



Dans le cas où l'on ne souhaite pas héberger ces répertoires localement, il est possible d'indiquer le nom d'hôte d'une machine du domaine (un serveur membre par exemple) sur lesquels ils seront stockés.



En mode expert, si les partages et/ou les profils sont gérés localement, il est possible de personnaliser le répertoire dans lequel ils seront stockés sur le serveur.

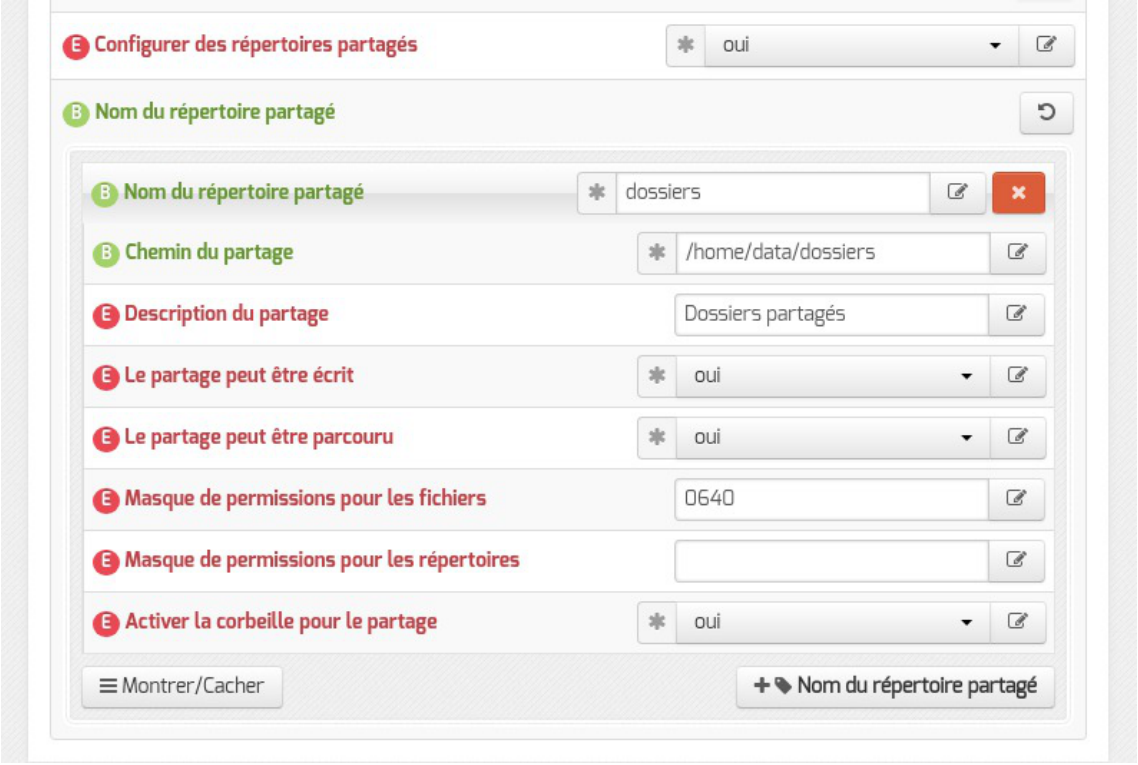
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Si le module `recycle` est activé, il est également possible d'activer la corbeille Samba pour les répertoires personnels des utilisateurs

Répertoires partagés

Passer la variable `Configurer des répertoires partagés` à `oui` permet de déclarer un ou plusieurs partages additionnels. Pour ajouter un ou plusieurs partages il faut cliquer sur le bouton `+ Nom du répertoire partagé`.



Les options à renseigner pour chaque partage supplémentaire sont :

- le `Nom du répertoire partagé` ;
- le `Chemin du partage` : le chemin Unix du répertoire à partager ;
- la `Description du partage` ;
- `Le partage peut être écrit` : le partage peut être défini en lecture/écriture ou en lecture seule (option `writeable`) ;
- `Le partage peut être parcouru` : le partage est visible dans le voisinage réseau ou non (option `browseable`) ;
- le `Masque de permissions pour les fichiers` (optionnel) : masque par défaut des fichiers créés (option `create mask`) ;

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

- le `Masque de permissions pour les répertoires` (optionnel) : masque par défaut des répertoires créés (option `directory mask`) ;
- la possibilité d'`Activer la corbeille pour le partage` (proposé uniquement si le module `recycle` est activé).

Les répertoires déclarés sont pris en compte et créés sur le disque lors de l'instanciation ou la reconfiguration du module.

Partages manuels

Le fichier de configuration `/etc/samba/smb.conf` est re-généré à chaque reconfiguration du serveur (commande `reconfigure`).

Il est possible de déclarer des partages supplémentaires manuellement en plaçant un fichier (possédant l'extension `.conf`) décrivant le partage dans le répertoire `/etc/samba/conf.d/`.

Sa prise en compte nécessite un `reconfigure`.

Archivage et sauvegarde des données

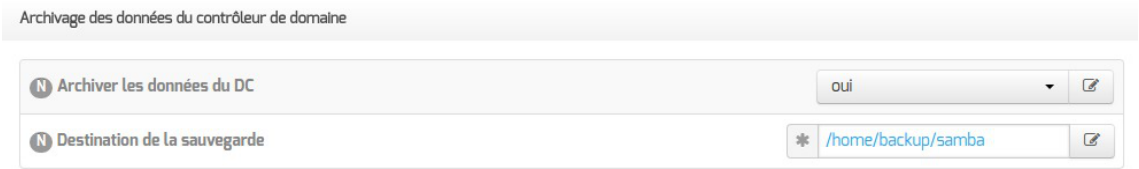
Un problème de corruption de la base Active Directory peut nécessiter de restaurer une sauvegarde sur le contrôleur de domaine principal et de relancer la synchronisation de tous les autres contrôleurs.

Il est primordial de disposer d'une archive ou d'une sauvegarde récente des données du serveur Active Directory.

Archivage local

La variable `Archiver les données du DC` permet d'activer l'exécution quotidienne d'un script d'archivage local et de choisir la destination de stockage de l'archive.

Les données du serveur Active Directory sont ainsi régulièrement sauvegardée (par défaut 1 fois par jour) dans le répertoire spécifié dans `Destination de la sauvegarde`.



Les éléments concernés par cette archive sont les suivants :

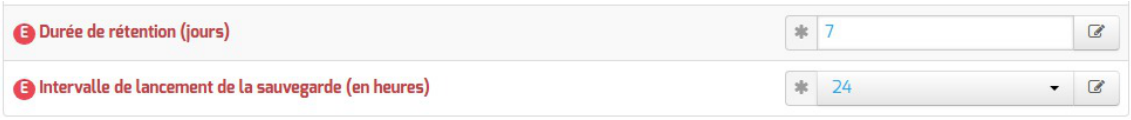
- la configuration de Samba (`/etc/samba`) ;
- le répertoire SYSVOL[p.519] (`/home/sysvol`) ;
- les bases TDB[p.520] de Samba (`/var/lib/samba/private`).

Le script utilisé pour l'archivage des données est inspiré d'un script mis à disposition par les développeurs du logiciel Samba :

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

> https://wiki.samba.org/index.php/Back_up_and_Restoring_a_Samba_AD_DC.

En mode expert, il est possible de spécifier la périodicité et la durée de rétention[p.499] de la sauvegarde locale.



Sauvegarde locale ou distante

Il est possible de mettre œuvre un système de sauvegarde complet en installant le logiciel Bareos[p.495] sur le serveur.

La mise en place de cet outil s'effectue manuellement à l'aide de la commande suivante :

```
# apt-eole install eole-bareos
```

Après installation des paquets, la configuration du service de sauvegarde se fait dans l'interface de configuration du module à plusieurs endroits.

L'archivage du DC soit activé dans l'onglet : `Archiver les données du DC` doit être à `oui`.

Par défaut la sauvegarde Bareos est activée (`Activer la sauvegarde du serveur` à `oui` dans l'onglet `Services`) et la tâche de sauvegarde des données du serveur Active Directory est prise en compte (`Sauvegarder les archives avec Bareos` à `oui` dans l'onglet `Active Directory`).



Dans cette configuration, les éléments suivants sont directement sauvegardés par Bareos avec le support des ACL :

- la configuration de Samba (`/etc/samba`) ;
- le répertoire SYSVOL[p.519] (`/home/sysvol`).

L'export des bases TDB est quant à lui géré par eole-schedule[p.501] avant l'exécution des sauvegardes.

Lorsque la sauvegarde des archives avec Bareos est activée la durée de rétention configurable en mode expert ne concerne que le script d'export des bases TDB de Samba.



La configuration à proprement parler des sauvegardes (distante, locale, durée de rétention, taux de compression…) se fait dans les onglets `Directeur bareos` et `Stockage bareos`.

Voir aussi...

> Onglet Directeur bareos [p.191]

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

Onglet Stockage bareos [p.124]

4.25. 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 :

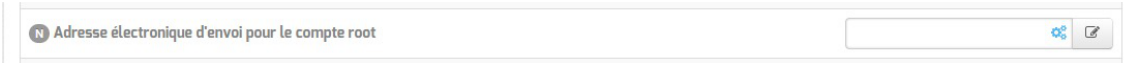
- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer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

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

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 configuration définie dans `/etc/mailname`
- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs[p. 497] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

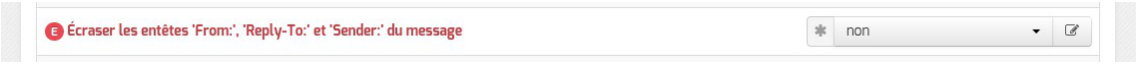
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

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

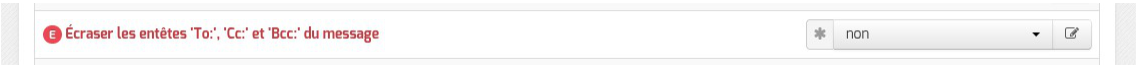
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

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 :

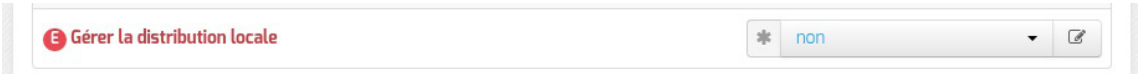
	system_mail_from_for_headers = non	system_mail_from_for_headers = oui
MAIL FROM	system_mail_from	system_mail_from
From :	user@conteneur.machine.domaine	system_mail_from
Reply-To :	user@conteneur.machine.domaine	system_mail_from
Sender :	user@conteneur.machine.domaine	system_mail_from

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

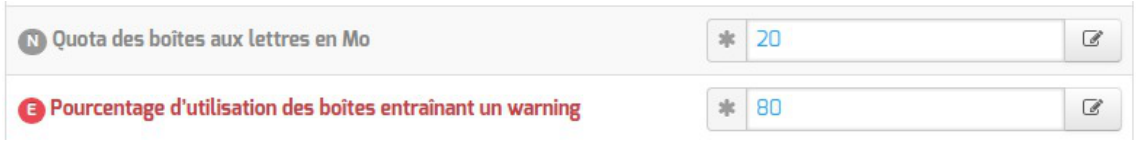
Réécriture du destinataire :

	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

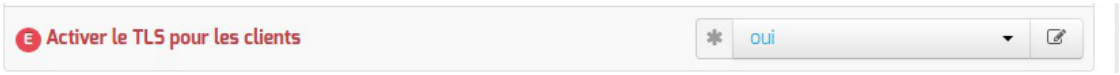
Par défaut, la distribution locale des messages est désactivée, sauf sur les modules Scribe et AmonEcole sur lesquels cette variable est masquée.



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.520] pour l'envoi de message est activé par défaut. La commande StartTLS[p.518] 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

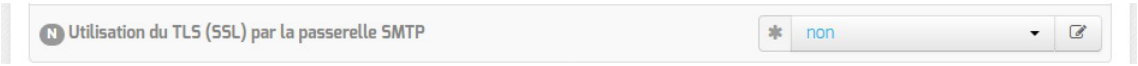


La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.

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

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.520] pour l'envoi de message. Si la passerelle SMTP[p.517] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.518] (port 25) ou non (port 465).

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



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`

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

Nom de domaine ajouté aux adresses :

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

- `Envoyer les logs à rsyslog`

  Permet de désactiver l'envoi des logs.

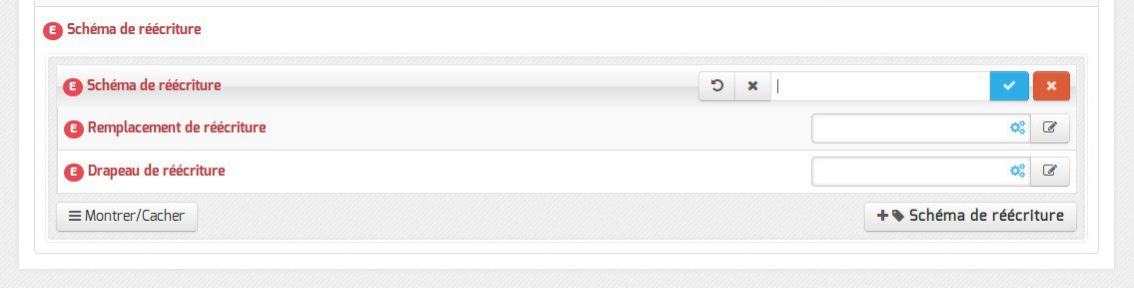
- `Dupliquer les logs dans des fichiers`

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

- `Activer les règles de réécriture étendue`

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

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



Les trois variables à saisir sont :

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

Fermeture de la messagerie

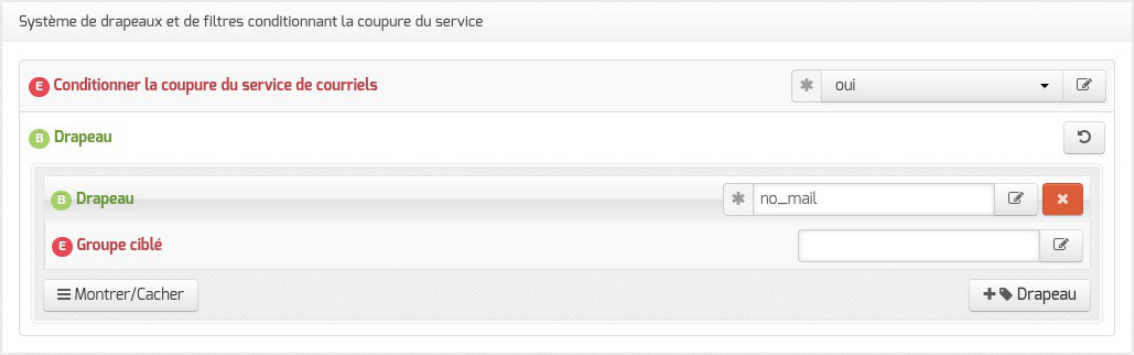
Le service de messagerie peut-être coupé sur la base de la présence d'un drapeau (fichier sur le système de fichiers).

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`.

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



- `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.

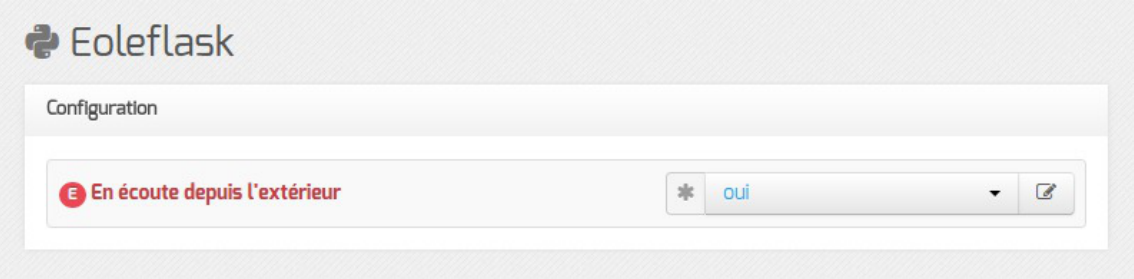


Sur EOLE 2.6.2, la création du drapeau n'est pas gérée automatiquement et le dossier `/var/run/eole/flags` n'existe pas par défaut.

Il est nécessaire de créer ce répertoire en cas d'activation de la fonctionnalité.

4.26. 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)

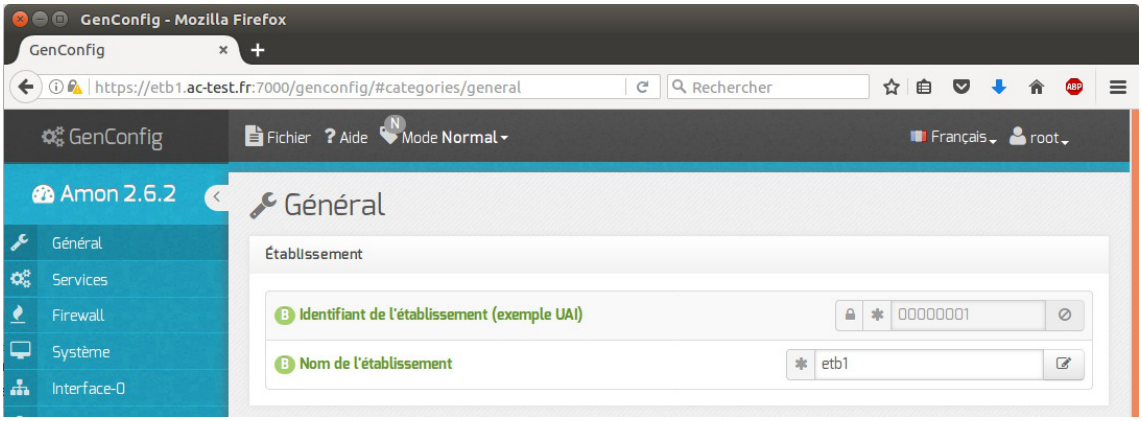
Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

`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.

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



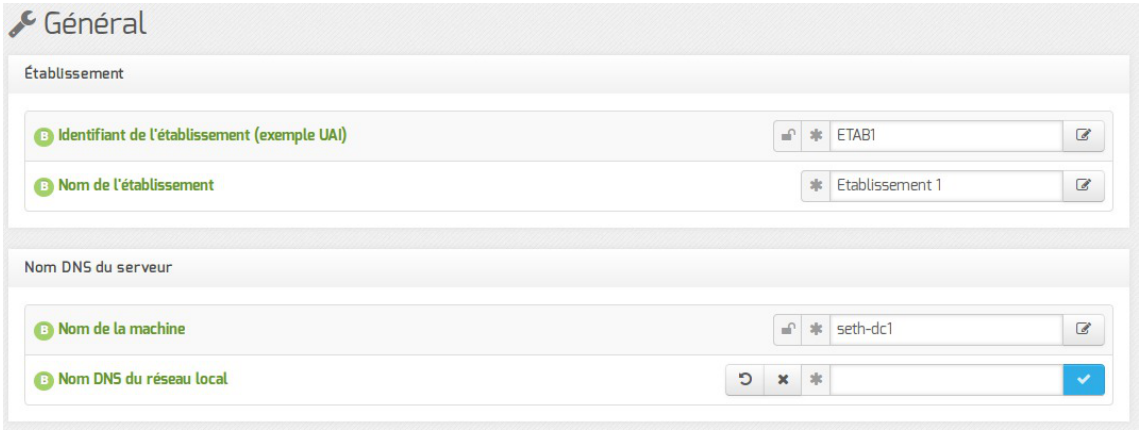
Vue de l'interface de configuration au travers d'un navigateur web (port 7000)

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`.

5. Configuration du module Seth en tant que contrôleur de domaine principal

Onglet général

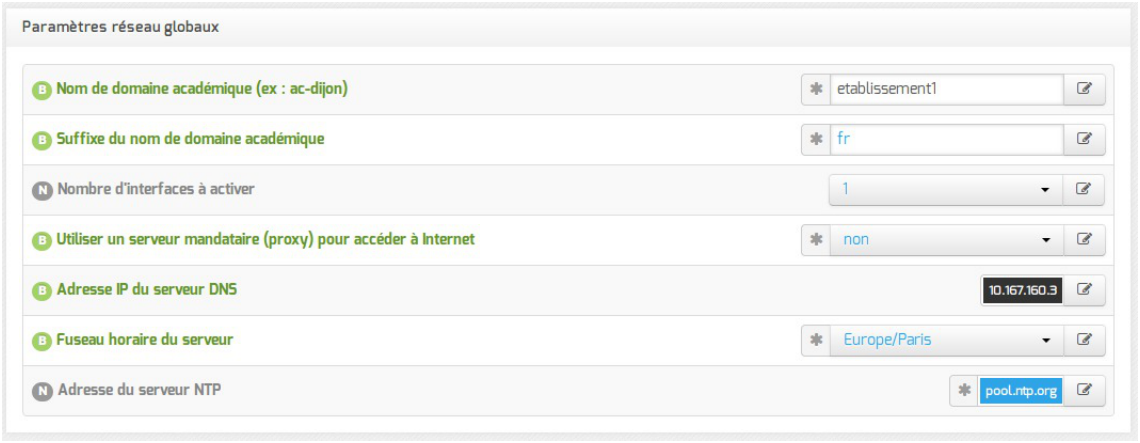
Établissement



La variable `Nom DNS du réseau local` doit être renseignée avec le realm[p.515]

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

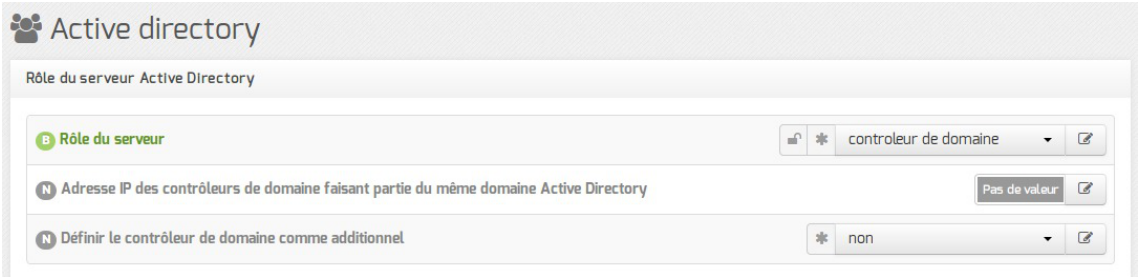
Paramètres réseau globaux



La variable `Adresse IP du serveur DNS` doit correspondre à un vrai serveur DNS.

La variable `Nom DNS du réseau local` doit être renseignée avec le realm[p.515]

Onglet Active Directory



La définition du rôle de contrôleur principal est la combinaison de

- la variable `Rôle du serveur` placée à `Contrôleur de domain` ;
- la variable `Définir le contrôleur de domaine comme additionnel` à `Non`.

6. Configuration du module Seth en tant que contrôleur de domaine additionnel

Dans le monde Microsoft, les contrôleurs de domaine sont habituellement tous au même niveau. Ceci est possible grâce à la réplication de l'annuaire Active Directory et à l'utilisation d'un système de fichiers distribué (DFS[p.498]).

À l'heure actuelle, la réplication du partage SYSVOL[p.519] n'est pas supportée par Samba. De ce fait, la mise en œuvre d'une architecture multi-DC[p.510] avec le module Seth nécessite de définir un contrôleur de domaine principal qui héberge les fichiers SYSVOL de référence et des contrôleurs de domaine additionnels sur lesquels ces fichiers sont synchronisés à intervalle régulier via rsync[p.516].

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

Pages relatives au support DFS sur le Wiki Samba

- https://wiki.samba.org/index.php/Distributed_File_System_(DFS)
- https://wiki.samba.org/index.php/SysVol_replication_(DFS-R)

Onglet général

Établissement



Paramètres réseau globaux

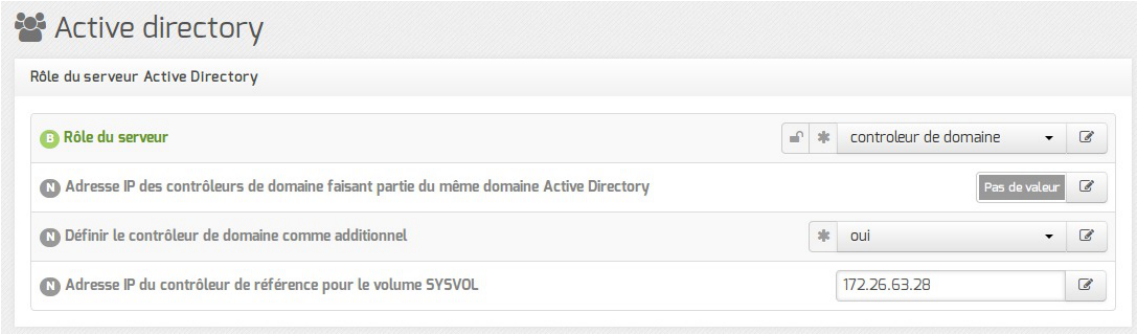


La variable `Adresse IP du serveur DNS` doit prendre la valeur de l'adresse IP du contrôleur de domaine principal.

La variable `Nom DNS du réseau local` doit être renseignée avec le realm[p.515]

Onglet Active Directory

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



La définition du rôle de contrôleur principal est la combinaison de :

- la variable `Rôle du serveur` passée à `Contrôleur de domaine` ;
- la variable `Définir le contrôleur de domaine comme additionnel` à `Oui` ;

La variable `Adresse IP du contrôleur de référence pour le volume SYSVOL` doit prendre la valeur de l'adresse IP du contrôleur de domaine principal.

Instanciation

Un contrôleur de domaine principal doit être installé, fonctionnel et joignable par le contrôleur de domaine additionnel pendant son instanciation.

7. Configuration du module Seth en tant que serveur membre

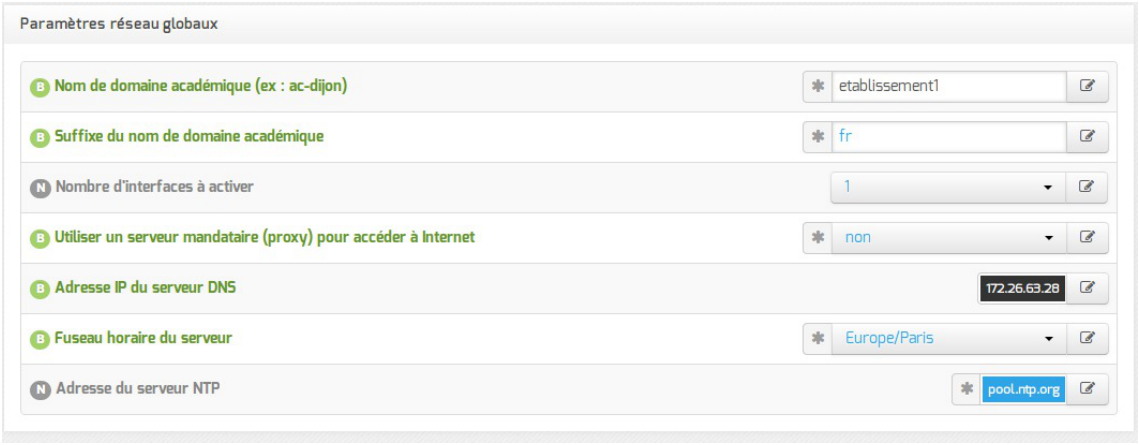
Onglet général

Établissement



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

Paramètres réseau globaux



La variable `Adresse IP du serveur DNS` doit prendre la valeur de l'adresse IP d'au moins un contrôleur de domaine.

La variable `Nom DNS du réseau local` doit être renseignée avec le realm[p.515]

Onglet Active Directory



Le rôle de serveur membre est simplement défini par la variable `Rôle du serveur`.

Instanciation

Un contrôleur de domaine doit être installé, fonctionnel et joignable par le serveur membre pendant son instanciation.

8. Mise en place de l'agrégation de liens Ethernet (bonding)

Activation de l'agrégation de liens Ethernet

L'activation de l'agrégation de liens Ethernet[p.494] s'effectue en déclarant au minimum deux interfaces réseau dans la variable experte `Nom de l'interface réseau` dans un onglet `Interface-n`.

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



L'utilisation de l'agrégation de liens Ethernet[p.494] nécessite de disposer d'un Commutateur réseau[p.496] 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.496] 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.

9. Mise en place du protocole ISCSI sur un module EOLE

Un SAN[p.517], tout comme un NAS[p.510] usant des protocoles NFS[p.510] ou SMB[p.517], permet de partager de l'espace disque via une image disque simulant un disque dur ou d'un disque complet, via le protocole

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

iSCSI[p.505].

La nette différence résulte dans le fait que c'est le système client qui prend en charge le formatage et le système de fichiers de ce dernier, sans compter que les performances seront généralement meilleures que sous les deux autres protocoles, notamment sur de multiples petits fichiers.

Cette technique permet de soulager le serveur en terme de ressources demandées (au détriment du poste client), mais surtout elle permet de lier cet espace disque comme s'il faisait partie intégrante de la machine client.

Source : https://doc.ubuntu-fr.org/iscsi.

Le projet `eole-open-iscsi`, 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.

La fonctionnalité peut désormais être facilement déployée et mise en œuvre sur un module EOLE grâce à un paquet dédié qui permet d'installer et de configurer le service `open-iscsi` (http://open-iscsi.com).

Installation d'eole-open-iscsi

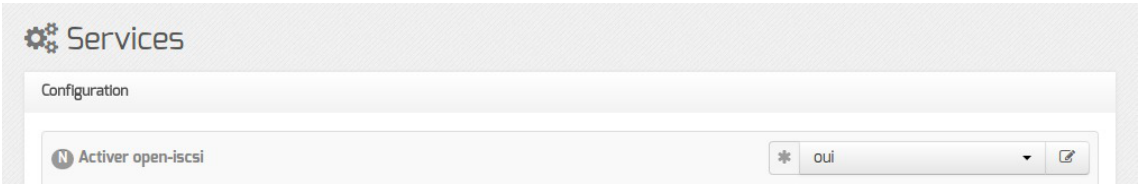
Le paquet `eole-open-iscsi` s'installe manuellement sur un module EOLE :

```
# apt-eole install eole-open-iscsi
```

Configuration d'eole-open-iscsi

Une fois le paquet installé, la configuration du service est à réaliser dans l'interface de configuration du module en mode normal.

L'activation du service open-iscsi s'effectue dans l'onglet `Services`.



Passer la variable `Activer open-iscsi` à `oui` permet d'activer le service.

Une fois le service activé, il est possible d'adapter sa configuration dans l'onglet : `Open-iscsi`.



- Si la variable `Activation du montage automatique des ressources` est à `oui`, le démon *iscsi*, lors de son démarrage, essayera de se connecter à toutes les cibles découvertes ;
- Si la variable `Activation du multipath pour gérer des accès multiples à des ressources` est à `oui`, il sera possible d'accéder à une même ressource via plusieurs liens, ce qui permet d'avoir de la redondance en cas de perte, et éventuellement, une répartition de charge.

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

Configuration du MTU

En fonction du matériel utilisé et de la configuration du réseau local, il peut s'avérer nécessaire de forcer une valeur de MTU[p.510] pour certaines interfaces réseau dans l'onglet Réseau avancé.

Mise en place

Une fois le service configuré, il faut reconfigurer le serveur à l'aide de la commande reconfigure :

```
# reconfigure
```

Voir aussi...

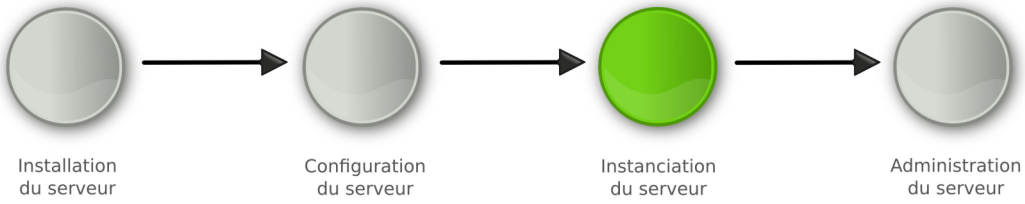
Onglet Réseau avancé [p.162]

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.520] 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.513] 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.382]

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.495] 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.433]

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]
```

3. Particularités de l'instance du module Seth

Au cours de l'instanciation du module Seth certaines questions spécifiques sont posées mais celles-ci différent selon le rôle du serveur.

Instance d'un module Seth - DC principal

Deux utilisateurs Active Directory sont créés à l'instance du contrôleur de domaine principal, il faut leur attribuer un mot de passe :

- `Administrator` : compte avec tous les pouvoirs (administrateur du domaine AD) à privilégier pour toutes les opérations d'administration du serveur ;
- `admin` : compte d'administration à privilégier pour la jonction des clients au domaine et les opérations courantes.

Instance d'un module Seth - DC additionnel

La synchronisation d'un contrôleur de domaine additionnel avec le contrôleur de domaine principal nécessite un échange de clés SSH.

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

De ce fait, le mot de passe root du contrôleur de domaine principal est demandé à l'instance.

Si vous êtes connecté en SSH avec la fonctionnalité transfert d'agent[p.493] (option par défaut de la commande `ssh`) et que la clé privée a été copiée sur le serveur distant, la phrase secrète n'est pas demandée.

Le contrôleur de domaine additionnel doit également être joint au domaine Active Directory. Pour cela, il est nécessaire de disposer :

- d'un contrôleur de domaine principale fonctionnel et joignable par le contrôleur de domaine additionnel à instancier
- du compte d'administration à utiliser (`Administrator` par défaut) et son mot de passe.

Instance d'un module Seth - serveur membre

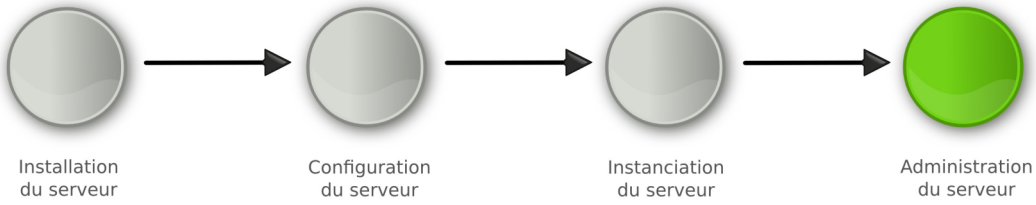
Le serveur membre doit être joint au domaine Active Directory. Pour cela, il est nécessaire de disposer :

- d'un contrôleur de domaine principale fonctionnel et joignable par le serveur membre à instancier
- du compte d'administration à utiliser (`Administrator` par défaut) et son mot de passe.

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

Chapitre 8

Administration du module Seth

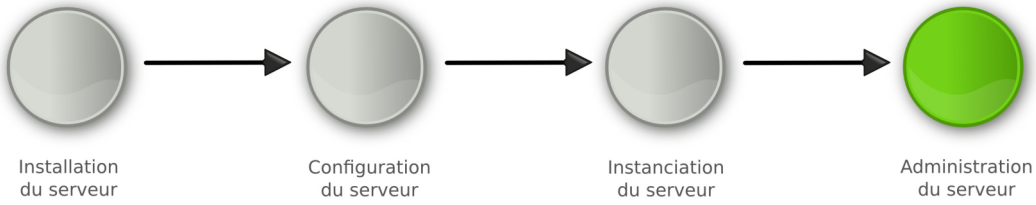


Administration

- 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. Administration généralités

La dernière des quatre phases



Administration

- 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.

1.1. Principes de l'administration

L'administration d'un module est facilitée par plusieurs outils mis à disposition :

- l'interface d'administration web : EAD ;

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

- l'interface d'administration semi-graphique : `manage-eole` ;
- l'interface d'administration du module Zéphir : `Zéphir-Web` ;
- des outils spécifiques à certains modules : `ARV`, `frontend horus`, ...
- des interfaces fournies par les logiciels utilisés : Cups, Sympa, ...
- la procédure de mise à jour ;
- les sauvegardes.

Il est également possible d'utiliser la **ligne de commande**.

Le choix de l'outil à utiliser s'effectue en fonction du type de module, de l'emplacement de ce module dans l'architecture (serveur en établissement ou serveur académique) et du profil de l'administrateur (administrateur académique, relai académique, personne ressource en établissement...).

1.2. Découverte de GNU/Linux





1.2.1. Les Bases

Descriptif sommaire

Une distribution

- un kernel = Linux [p.506]
- des outils périphériques = GNU [p.502]
- un environnement console ou graphique
- un système de fichiers éprouvé, hérité d'UNIX

1.2.1.a. L'arborescence GNU/Linux

L'arborescence GNU/Linux

Pour l'utilisateur, un système de fichiers est vu comme une arborescence : les fichiers sont regroupés dans des répertoires (concept utilisé par la plupart des systèmes d'exploitation). Ces répertoires contiennent soit des fichiers, soit récursivement d'autres répertoires. Il y a donc un répertoire racine et des sous-répertoires. Une telle organisation génère une hiérarchie de répertoires et de fichiers organisés en arbre.

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

Racine de l'arbre

`/` (appelé slash ou root) : racine de l'arborescence sur laquelle sont raccrochés tous les sous-répertoires et fichiers.

Arborescence 1er niveau

- `bin/` : commandes liées au système, exécutables par tous ;
- `boot/` : noyau et initrd nécessaires au démarrage (ou boot) du système ;
- `dev/` : fichiers spéciaux effectuant le lien noyau / périphériques ;
- `etc/` : fichiers de configuration ;
- `home/` : répertoires de connexion (ou home directory) des utilisateurs ;
- `lib/` : librairies essentielles au démarrage et modules du noyau ;
- `mnt/` : contient les sous-répertoires de montage des partitions des autres périphériques ;
- `opt/` : installation des applications autres ;
- `proc/` : pseudo système de fichier représentant le noyau à un instant T ;
- `root/` : répertoire de connexion de root ;
- `sbin/` : commandes réservées à root et utilisées dans les niveaux de démarrage bas ;
- `sys/` : pseudo système de fichier représentant les processus ;
- `tmp/` : répertoire temporaire accessible à tous ;
- `usr/` : commandes utilisées par les utilisateurs (bin), l'administrateur (sbin), mais aussi ensemble du système graphique ;
- `var/` : ensemble des données variables du système (spools, logs, web, bases de données, ...).

Filesystem Hierarchy Standard (« norme de la hiérarchie des systèmes de fichiers », abrégé en **FHS**) définit l'arborescence et le contenu des principaux répertoires des systèmes de fichiers des systèmes d'exploitation GNU/Linux et de la plupart des systèmes Unix.

Fichiers et répertoires

Sous Unix, tout est fichier

Les différents types :

- **fichiers ordinaires** : fichiers éditables
- **fichiers programmes** : fichiers contenant des données compilées
- **répertoires** : fichier contenant les infos sur les fichiers et sous-répertoires contenus (index)
- **fichiers spéciaux** : fichier associé à un périphérique. Ne contient qu'une description relative au driver et type d'interface.

Adresse absolue / adresse relative

Un fichier ou un répertoire peut être défini :

- soit par un chemin relatif à l'endroit où vous vous positionnez au moment T.
- soit par un chemin absolu à partir de la racine de l'arborescence.

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

1.2.1.b. La gestion des droits

Droits de base UNIX

Les droits détaillés ci-après s'appliquent à l'ensemble des composantes de l'arborescence GNU/Linux, à savoir les fichiers et les répertoires.

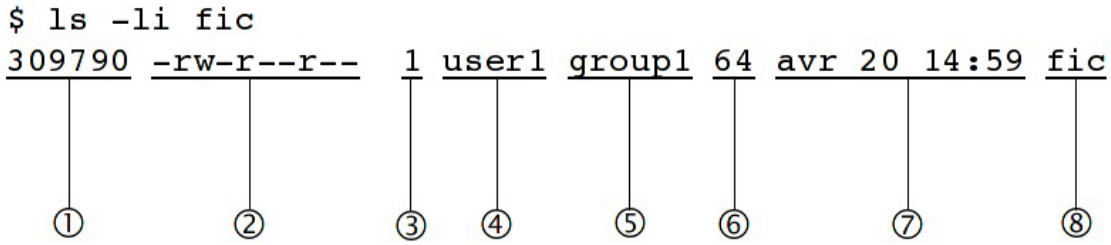
Droits essentiels :

- lecture
- écriture
- exécution

Autres droits :

- sticky bit
- setuid et setgid bits

Description d'un fichier



1. numéro d'inode
2. type & droits sur le fichier (ou répertoire)
3. compteur de liens physiques
4. propriétaire
5. groupe
6. taille
7. date de dernière modification
8. nom du fichier (répertoire)

Représentation du type et des droits des fichiers

Le schéma précédent montre, dans le second bloc, comment sont affichés les droits associés à un fichier (ou répertoire).

Ce bloc se décompose en 4 sous-parties :

- La première, codée sur un caractère, représente le type du fichier
- On trouve ensuite 3 groupes de 3 caractères indiquant les droits de lecture/écriture/exécution.

Le type du fichier peut être un des éléments suivants :

- `d` : répertoire
- `l` : lien symbolique

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

- `c` : périphérique de type caractère
- `b` : périphérique de type bloc
- `p` : pile fifo
- `s` : socket
- `-` : fichier classique



- Fichiers de périphériques :
  - brw-rw---- 1 root disk 8, 0 nov 12 08:17 /dev/sda
  - brw-rw---- 1 root cdrom 3, 0 nov 12 08:17 /dev/hda
  - crw-r----- 1 root kmem 1, 1 nov 12 08:17 mem
  - crw-rw---- 1 root root 4, 0 nov 12 08:17 tty0
- Répertoires :
  - drwxr-xr-x 13 root root 4096 oct 20 10:22 /usr
  - drwxr-xr-x 17 user1 group1 4096 oct 31 09:18 /home/user1
- Fichiers standards :
  - -rw-r--r-- 1 root root 2008 oct 17 19:36 /etc/inittab
  - -rw-r--r-- 1 root root 724 déc 20 2006 /etc/crontab
  - -rwxr-x--1 root root 1024 oct 29 /home/user1/monScript
- Lien symbolique :
  - lrwxrwxrwx 1 root root 31 oct 27 15:00 /var/lib/postgresql/8.3/main/root.crt -> /etc/postgresql-common/root.crt
- Socket :
  - srw-rw-rw- 1 root root 0 nov 12 08:18 /var/run/gdm_socket

Détail des droits standards

Comme énoncé précédemment, les droits sont codés sur 3 jeux de 3 droits.

Cet ensemble de 3 droits sur 3 entités se représente généralement de la façon suivante : on écrit côte à côte les droits **r** (*R*ead/lecture), **w** (*W*rite/écriture) puis **x** (e*X*ecute/exécution) respectivement pour le propriétaire (**u**), le groupe (**g**) et les autres utilisateurs (**o**). Les codes u, g et o (u comme user, g comme group et o comme others) sont utilisés par les commandes UNIX qui permettent d'attribuer les droits et l'appartenance des fichiers.

Lorsqu'un droit est attribué à une entité, on écrit ce droit (r, w ou x), et lorsqu'il n'est pas attribué, on écrit un '-'. Par exemple : `rwxr-xr--`

Droits Spécifiques

SUID Bit

Ce droit s'applique aux fichiers exécutables, il permet d'allouer temporairement à un utilisateur les droits du propriétaire du fichier, durant son exécution.

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

En effet, lorsqu'un programme est exécuté par un utilisateur, les tâches qu'il accomplira seront restreintes par ses propres droits, qui s'appliquent donc au programme.

Lorsque le droit SUID est appliqué à un exécutable et qu'un utilisateur quelconque l'exécute, le programme détiendra alors les droits du propriétaire du fichier durant son exécution.

Bien sûr, un utilisateur ne peut jouir du droit SUID que s'il détient par ailleurs les droits d'exécution du programme. Ce droit est utilisé lorsqu'une tâche, bien que légitime pour un utilisateur classique, nécessite des droits supplémentaires (généralement ceux de root). Il est donc à utiliser avec précaution.

- -r-**s**--x--x 1 root root 15540 jun 20 2004 /usr/bin/passwd

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci : ---**s**------ ou ---**S**------

SGUID Bit

Ce droit fonctionne comme le droit SUID, mais appliqué aux groupes. Il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire.

De plus, ce droit a une tout autre utilisation s'il est appliqué à un répertoire. Normalement, lorsqu'un fichier est créé par un utilisateur, il en est propriétaire, et un groupe par défaut lui est appliqué (généralement users si le fichier a été créé par un utilisateur, et root s'il a été créé par root). Cependant, lorsqu'un fichier est créé dans un répertoire portant le droit SGID, alors ce fichier se verra attribuer par défaut le groupe du répertoire. De plus, si c'est un autre répertoire qui est créé dans le répertoire portant le droit SGID, ce sous-répertoire portera également ce droit.

- -rwxr-sr-x 1 root utmp 319344 avr 21 2008 /usr/bin/xterm

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci : ---**s**------ ou ---**S**------

Sticky Bit

Lorsque ce droit est positionné sur un répertoire, il interdit la suppression des fichiers qu'il contient à tout utilisateur autre que le propriétaire. Néanmoins, il est toujours possible pour un utilisateur possédant les droits d'écriture sur ce fichier de le modifier (par exemple de le transformer en un fichier vide).

Notation : il est représenté par la lettre `t` ou `T`, qui vient remplacer le droit d'exécution `x` des autres utilisateurs que le propriétaire et ceux appartenant au groupe du fichier, de la même façon que les droits SUID et SGID. La majuscule fonctionne aussi de la même façon, elle est présente si le droit d'exécution x caché n'est pas présent : ---------**t** ou ---------**T**

Exemple : le répertoire /tmp

- drwxrwxrw**t** 23 root root 4096 oct 20 14:27 /tmp/

Listes de contrôle d'accès

Une liste de contrôle d'accès ou ACL, permet de définir une liste de permission sur un fichier ou répertoire.

Aux habituels utilisateur, groupe et autre, il est possible d'étendre le nombre d'utilisateurs et de groupes ayant des droits sur un même fichier

Les ACLs s'ajoutent aux droits standards. Lorsqu'on liste les droits d'un fichier, les ACLs sont symbolisées par un "+".

```
-rwxrwx---+ 1 root professeurs 26 2009-05-27 16:37 fic
```


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

Les droits étendus apparaissent de la façon suivante :

```
user::rwx
user:p.nom:rwx
group::---
mask::rwx
other::---
```

Les ACLs d'un dossier père ne sont pas automatiquement repris pour le fichier fils.

Il est possible de modifier ce comportement, à associant des droits par défaut (grâce à l'attribut *default*).

Par exemple :

```
user::rwx
user:p.nom:rwx
group::rwx
mask::rwx
other::--x
default:user::rwx
default:user:p.nom:rwx
default:group::---
default:mask::rwx
default:other::---
```

1.2.1.c. La gestion des processus

Définition d'un processus

Un processus est un programme qui s'exécute en mémoire.

Tout processus lancé :

- se voit attribuer un numéro appelé **PID** (Process Identifier).
- est fils du processus qui l'a lancé. Le fils connaît le PID de son père, et en garde une trace sous la forme d'un numéro appelé **PPID** (Parent Process Identifier).
- appartient à un propriétaire (**UID** - celui qui a lancé le programme et qui pourra interagir avec ce processus)
- détermine son activité par un état : Actif, Exécutable, Endormi, Zombi.

Si un processus disparaît, tous les processus fils disparaissent également, sauf quand un processus est raccroché à `init`. Ainsi donc, à l'instar des fichiers, les processus sont organisés en arbre.

Enfin GNU/Linux est un système multi-tâche, c'est à dire que plusieurs processus peuvent être exécutés en même temps, en réalité, un seul utilise le processeur à la fois, ce dernier ne sachant effectuer qu'une seule instruction à la fois.

Etat d'un processus

Comme évoqué précédemment, un processus peut avoir un état : Actif, Exécutable, Endormi, Zombi.

- **Actif** : le processus utilise le processeur, et est donc en train de réaliser des actions pour lequel il a été conçu.

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

- **Exécutable** : le processus est en exécution mais il est en attente de libération du processus qui est utilisé par un processus actif. Pour l'utilisateur, ceci est invisible car l'opération est très rapide.
- **Endormi** : comme son nom l'indique, le processus est endormi, il ne fait rien. Par exemple, un processus peut attendre un événement pour redevenir *Actif*, comme par exemple, que l'on appuie sur une touche lors de l'affichage d'un message.
- **Zombie** : un processus zombie est un processus terminé, mais le système ou le processus parent n'en a pas été informé. L'état d'un processus peut être modifié par un autre processus, par lui même ou par l'utilisateur.

1.2.2. Quelques Commandes

Actions sur les fichiers et répertoires

Se déplacer dans l'arborescence :

- savoir où je me situe : `pwd` ;
- aller vers : `cd [répertoire]`.

Lister les fichiers et les droits : `ls [-la] [fichier...] [répertoire...]`.

Lister les ACLs : `getfacl [fichier...] [répertoire...]`.

Créer/supprimer un répertoire :

- créer un répertoire : `mkdir [-p] <répertoire...>` ;
- supprimer un répertoire (déjà vide) : `rmdir <répertoire...>`.

Copier, renommer, déplacer :

- copier : `cp [-fr] <source1>... <destination>` ;
- renommer : `mv <source> <destination>` ;
- déplacer : `mv <source1>... <destination>`.

Liens physiques, liens symboliques : `ln [-s] <origine> <destination>`.

Manipuler les droits & les propriétaires :

changer les droits : `chmod [-R] [MODE|MODE-OCTAL] <fichier...> <répertoire...>` ;

changer le propriétaire : `chown [-R] <user>[.<group>] <fichier...> < répertoire...>` ;

changer le groupe : `chgrp [-R] <group> <fichier...> < répertoire...>` ;

changer les ACLs : `setfacl [-R] -m <u|g|o>:<utilisateur|group>:<droit> < répertoire...>`.

Gestion des processus

Voir l'état des processus :

- à un instant T : `ps [auxef...]` ;
- visualisation dynamique : `top`.

Arrêt d'un processus : `kill [-Num_Sig] <PID...>`.

Autres commandes diverses

passwd : permet de changer le mot de passe d'un utilisateur système (il ne permet pas de changer les mots de passe des utilisateurs dans un annuaire LDAP)

`passwd` sans option modifie le mot de passe de l'utilisateur courant.

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

`passwd nom_d_utilisateur` permet de changer le mot de passe d'un autre utilisateur.
Si la commande est exécuté par un utilisateur autre que "root" le mot de passe actuel sera demandé.

sort : trier des lignes en fonction d'une ou plusieurs clés : `sort [-ndtX] [-k num_champs] fichier...`.

grep : rechercher des chaînes de caractère dans un ou plusieurs fichiers : `grep [-vni] chaîne fichier...`.

cut : extraire des colonnes d'un ou plusieurs fichiers : `cut -f <nombre> [options] fichier...`.

wc : déterminer le nombre de lignes, mots ou caractères dans un ou plusieurs fichiers : `wc [-lwc] fichier...`.

tail et head : visualiser les dernières ou les premières lignes d'un fichier :

- `tail [-n] fichier` ;
- `head [-n] fichier`.

screen : multiplexeur de terminaux en mode texte. Il permet de détacher un terminal et de le récupérer en cas de déconnexion. Ce logiciel est particulièrement adapté aux travaux à distance, en cas de coupure réseau il est possible de reprendre la main dessus le serveur. Voici le fonctionnement de base :

- lancer un nouveau terminal : `screen` ;
- détacher ce terminal : `ctrl a d` ;
- re-attacher le terminal : `screen -rd`.

1.2.3. Les conteneurs

Pour gérer les conteneurs, différentes commandes sont disponibles :

- installation d'un paquet dans un conteneur : `apt-eole install-conteneur (nom_du_conteneur) paquet`
- statut de tous les conteneurs : `lxc-status` ;
- arrêt de tous les conteneurs : `service lxc stop` ;
- démarrage de tous les conteneurs : `service lxc start` ;
- arrêt d'un conteneur : `lxc-halt -n (nom_du_conteneur)` ;
- forcer l'arrêt d'un conteneur : `lxc-stop -n (nom_du_conteneur)` ;
- démarrage d'un conteneur : `lxc-start -n (nom_du_conteneur) -d`
- entrer dans un conteneur : `ssh (nom_du_conteneur)` .

Les conteneurs seront installés dans le répertoire `/opt/lxc/`, mais, normalement, il n'est pas nécessaire de modifier les fichiers directement dans ce répertoire.

1.2.4. La gestion des onduleurs

Quelques commandes utiles :

- test d'une installation sans démarrer le service upsd : `upsdrvctl start` ;
- test de l'arrêt du serveur sans avoir à attendre que la batterie soit vide : `upsmon -c fsd` ;
- lister la configuration : `upsc eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur) ;

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

- modifier la configuration : `upsrw eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur).

1.2.5. Les manuels

L'organisation du man

L'ensemble du man est organisé en sections numérotées de 1 à 9 pour les plus courantes :

1. commandes utilisateurs pouvant être exécutées quelque soit l'utilisateur
2. appels systèmes, c'est-à-dire les fonctions fournies par le noyau
3. fonctions des bibliothèques
4. périphériques, c'est-à-dire les fichiers spéciaux que l'on trouve dans le répertoire /dev
5. descriptions des formats de fichiers de configuration (comme par exemple /etc/passwd)
6. jeux
7. divers (macros, conventions particulières, ...)
8. outils d'administration exécutables uniquement par le super utilisateur (root)
9. autre section (spécifique à GNU/Linux) destinée à la documentation des services offerts par le noyau

Lorsque la documentation est interrogée à propos d'un terme présent dans plusieurs sections (ex : `passwd`, à la fois commande et fichier de configuration), si le numéro de section n'est pas précisé, c'est toujours la section de numérotation la moins élevée qui sera affichée.

Contenu d'une page

Chaque page de man est structurée en paragraphes contenant des éléments particuliers.

Intitulé de la commande ou du fichier et section du manuel

Vérifier qu'il s'agit de la documentation attendue.

Exemple :

- `CP(1)  Manuel de l'utilisateur Linux  CP(1)`

documentation pour la commande cp, section 1

- `PASSWD(5)  Manuel de l'administrateur Linux  PASSWD(5)`

documentation pour le fichier passwd, section 5

Nom

comme son nom l'indique, il s'agit du nom de la commande ou du fichier ainsi que d'une description synthétique.

Exemple :

- `NOM`
  `cp - Copier des fichiers.`

Synopsis

Dans ce paragraphe, on retrouve la syntaxe d'une commande, c'est-à-dire l'ensemble des options et

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

arguments disponibles.

Quelques précisions pour bien lire cette syntaxe : si à première vue elle peut paraître rébarbative, elle dit tout au sujet de la manipulation d'une commande.

Exemple :

- `cp [options] fichier chemin`
  `Options GNU (forme courte) : [-abdfilprsuvxPR]`

la commande `cp` accepte des options (introduites par un "-") et des arguments (sans "-").

Les éléments spécifiés entre crochets sont facultatifs pour le fonctionnement de la commande.

Au contraire, les éléments indiqués sans crochets sont obligatoires et, s'ils sont omis, provoqueront une erreur.

Lorsque les options sont indiquées dans les mêmes crochets, elles peuvent être combinées. Dans le cas contraire, elles sont incompatibles et devront être utilisées séparément.

Enfin les options peuvent être abrégées (ex : -f) ou complètes (ex : --force), la signification est la même et elle est développée dans le paragraphe `description`.

Description

Cette section du man détaille la totalité des options et arguments d'une commande, ou les éléments d'un fichiers de configuration.

Fichiers

Dans ce paragraphe, vous trouverez une liste de fichiers intéressants à consulter, en complément d'information pour une commande ou un fichier de configuration.

Voir aussi

(ou "See also")

Comme son nom l'indique, il s'agit d'une liste de commandes, fichiers, appels système... auquel on renvoie le lecteur pour compléter son information

Exemple :

- `VOIR AUSSI`
  `passwd(1), login(1), group(5), shadow(5).`

Cette page propose ici de consulter les commandes `passwd` et `login` dans la section 1 et les fichiers `group` et `shadow` dans la section 5 de la documentation.

Environnement

ici sont spécifiées les variables d'environnement qu'il est possible de configurer pour le fonctionnement de la commande ou du fichier.

1.2.6. L'éditeur de texte Vim

Qu'est ce que Vim ?

Vim est un éditeur de texte libre. Il est à la fois simple est puissant.

Il est néanmoins nécessaire de passer par un temps d'apprentissage pour maîtriser l'outil.

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

Pourquoi Vim ?

L'éditeur est généralement installé de base sur la plupart des distributions. C'est un logiciel stable et éprouvé.

L'éditeur peut être lancé directement sans interface graphique. Il est ainsi possible d'exécuter depuis le serveur.

De plus, Vim est pré-configuré par l'équipe EOLE. Il n'y aura pas de problème de balise de fin de ligne, de nombre d'espace lors de l'indentation, ... Problème qu'il est possible de rencontrer avec d'autres éditeurs.

1.2.6.a. Les modes Vim

Introduction

Vim utilise un système de "modes". Ce concept de base est indispensable pour comprendre le fonctionnement du logiciel.

Vim est un éditeur entièrement accessible au clavier. Un ensemble de commande permet d'accéder à un ensemble de fonctionnalité. Pour que l'éditeur distingue la saisie de commande (le mode "normal") et la saisie de texte (le mode "insertion"), différents modes sont utilisés.

Il existe également le mode "visuel" permettant de sélectionner une zone de texte où sera appliquée un ensemble de commande.

Cette distinction n'existe pas, généralement, dans les autres éditeurs. Ils utilisent alors des entrées dans un menu graphique ou des raccourcis clavier à la place du mode "normal".

Comparé au mode graphique, le mode commande ne nécessite pas l'usage de la souris pour rechercher le bon menu. Par rapport aux raccourcis clavier, le mode commande est souvent plus facile à se rappeler (write pour écrire).

Passage d'un mode à l'autre

Pour passe au mode "normal", il suffit de taper la touche Echap ou Esc.

Pour passer au mode "insertion" (depuis le mode "normal") :

- insérer avant le curseur : i (ou la touche Inser du clavier) ;
- insérer après le curseur : a ;
- insérer en début de ligne : I ;
- insérer en fin de ligne : A ;
- insérer une ligne après : o ;
- insérer une ligne avant : O ;
- supprime pour remplacer un (et un seul) caractère : s ;
- supprime pour remplacer la ligne complète : S ;
- remplacer un caractère : r ;
- remplacer plusieurs caractères : R ;

Pour passer au mode "visuel" (depuis le mode "normal") :

- sélection caractère par caractère : v ;
- sélection ligne par ligne : V ;

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

- sélection colonne par colonne : `ctrl v` .

1.2.6.b. Première prise en main

Exécuter Vim

Pour exécuter Vim, il suffit de taper `vim` dans l'interpréteur de commande. Il est aussi possible d'ouvrir directement un fichier en faisant `vim fichier.txt` .

Ouvrir un fichier

En mode normal, taper : `:edit fichier.txt` (ou `:e fichier.txt`).

Insérer du texte

Passer en mode insertion : `i` et taper votre texte.

Enregistrer le texte

Quitter le mode insertion : `esc` .

Enregistrer le texte : `:write` (ou `:w`).

Quitter l'éditeur

Pour quitter l'éditeur : `:quit` (ou `:q`).

> Vim créé un "buffer" lorsque l'on édite un fichier. Cela signifie que l'on ne modifie pas directement le fichier. Il faut sauvegarder les changements sous peine de perdre les modifications.
>
> Le buffer est sauvegardé de façon fréquente dans un fichier "swap" (généralement `.fichier.txt.swp`). Ce fichier est supprimé lorsqu'on enregistre ou ferme le document.

1.2.6.c. Les déplacements

- se déplacer d'un caractère vers la gauche : `h` ;
- se déplacer de 20 caractères vers la gauche : `20h` ;
- se déplacer d'une ligne vers le bas : `j` ;
- se déplacer de 20 lignes vers le bas : `20j` ;
- se déplacer d'une ligne vers le haut : `k` ;
- se déplacer d'un caractère vers la droite : `l` ;
- se déplacer au début du prochaine mot : `w` ;
- se déplacer au début de deux mots : `2w` ;
- revenir au début du mot précédent : `b` ;
- se déplacer à la fin du prochain mot : `e` ;
- se déplacer à la prochaine phrase : `)` ;
- revenir à la phrase précédente : `(` ;

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

- se déplacer au prochain paragraphe : `}` ;
- revenir au paragraphe précédent: `{` ;
- revenir au début de la ligne : `^` ;
- aller à la fin de la ligne : `$` ;
- remonter d'un écran : `pgup` ;
- descendre d'un écran : `pgdown` ;
- descendre à la fin du fichier : `G` ;
- aller à la ligne 20 : `20G` ;
- aller au début de la page courante : `H` ;
- aller au milieu de la page courante : `M` ;
- aller à la fin de la page courante : `L` ;
- revenir à l'emplacement précédent : `ctrl o` ;
- aller à l'emplacement suivant : `ctrl i` ;
- la troisième occurrence de la lettre "e" : `3fe` ;

Il est possible de "marquer" des positions dans le texte. Cela permet de revenir très facilement à cet emplacement plus tard.

Pour cela, il faut utiliser la commande `m` suivi du nom de la marque (c'est à dire une lettre). Par exemple : `ma`. Pour revenir à la marque, il suffira de taper : `'a`.

1.2.6.d. Recherche et remplacement de texte

Rechercher

- chercher les occurrences EOLE : `/EOLE` ;
- chercher les mots EOLE : `/\<EOLE\>` ;
- chercher l'occurrence suivante : `n` ;
- chercher l'occurrence précédente : `N` ;
- chercher les autres occurrences du mot sous le curseur : `*` ;
- chercher en arrière les autres occurrences du mot sous le curseur : `ctrl #` ;

Remplacement

- remplacer le mot EOLE par Scribe : `:%s/EOLE/Scribe/g`
- remplacer le mot EOLE par Scribe en demande confirmation : `:%s/EOLE/Scribe/gc`
- remplacer le mot EOLE par Scribe sur les 20 première ligne d'un fichier : `:0,20s/EOLE/Scribe/g`

1.2.6.e. Couper, copier et coller

- couper un texte sélectionné : `d` ;
- couper le caractère sélectionné : `x` ;

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

- couper les deux caractères suivants : `d2l` ;
- couper un mot : `dw` ;
- couper la ligne courante : `dd` ;
- couper 2 lignes : `d2` ;
- couper le paragraphe : `d}` ;
- copier un texte sélectionné : `y` ;
- coller le texte après : `p` .
- coller le texte avant : `P` ;

1.2.6.f. Le mode fenêtre

Ouvrir plusieurs fenêtres

Il est possible d'ouvrir plusieurs fichiers en même temps.

Pour cela, il suffit de lancer plusieurs fois la commande `:e nomdufichier` .

Pour passer d'un buffer à un autre, il suffit de taper `:bn` (n étant le numéro du buffer).

Ouvrir plusieurs tabulations

Pour ouvrir le fichier dans une nouvelle tabulation : `:tabedit fichier.txt` .

Pour se déplacer de tabulation en tabulation, il suffit d'utiliser `ctrl alt pgup` et `ctrl alt pgdown` .

Voir plusieurs fichiers

Il est possible de voir plusieurs fichiers dans la même interface.

Pour cela, il faut créer un nouveau buffer en tapant `:new` et ensuite ouvrir le nouveau fichier : `:e fichier.txt` .

Pour se déplacer dans les buffers, il faut utiliser le raccourci `ctrl w` et les touches de déplacement `hjkl` .

Pour se déplacer de buffer en buffer, il est possible également de taper deux fois `ctrl w` .

Il est ensuite possible de déplacer les fenêtres horizontalement et verticalement avec `ctrl w` et les touches de déplacement en majuscule `HJKL` .

Pour fermer une fenêtre, il suffit de faire `:q` .

Voir plusieurs fois le même fichier

Il est possible d'ouvrir plusieurs fois le même buffer en faisant `ctrl w s` . Cela permet de voir simultanément plusieurs parties du même texte.



Dans ce cas, il s'agit du même buffer. Une modification dans une vue sera automatiquement reporter dans les autres vues.

Système de fichiers

Il est possible d'ouvrir une fenêtre de système de fichiers en faisant : `:Sex` ou `:Vex` .

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

1.2.6.g. Autres

Complétion automatique

La complétion permet de compléter un mot automatiquement à partir d'une liste de mot présent dans le texte en court d'écriture. Il est souvent utile pour ne pas faire d'erreur dans le nom des fonctions.

Pour l'utiliser, il suffit de commencer a écrire le début du mot et faire `ctrl n` ou `ctrl p` .

Annuler et refaire

Pour annuler la dernière action : `u` ;

Pour revenir sur l'annulation : `ctrl r` .

Passer un texte en majuscule

Pour passer un texte en majuscule, il suffit de taper `~` ou `maj u` .

Voir la différence entre les fichiers

Vim permet également de voir la différence entre deux textes. Pour cela, il suffit de lancer en ligne de commande :

```
vimdiff nomdufichieroriginal.txt nomdufichiermodifier.txt
```

1.2.6.h. Liens connexes

http://www.vim.org/

http://www.swaroopch.com/notes/Vim_fr:Table_des_Mati%C3%A8res

https://svn.timetombs.org/svn/doc-keymap/doc-keymap-cheat_sheet-vim-azerty_fr.pdf [https://svn.timetombs.org/svn/doc-keymap/doc-keymap-cheat_sheet-vim-azerty_fr.pdf]

1.2.7. Les commandes à distance avec SSH

1.2.7.a. Le protocole SSH

SSH[p.518] (Secure Shell) et un protocole de communication sécurisé. Il permet différentes actions comme l'authentification à distance, l'exécution de commande à distance ou le transfert de fichier.

Le protocole est chiffré par un mécanisme d'échange de clés de chiffrement effectué au début de la connexion.

Le transfert de fichier d'une machine à une autre se fait par un protocole proche de FTP[p.501]. La différence étant que les transferts du client et du serveur se font par un tunnel chiffré.

1.2.7.b. SSH sous GNU/Linux

Connexion à distance

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

Le client SSH est installé par défaut sur la plupart des distributions. Si ce n'est pas le cas, il faut installer un paquet dont le nom est généralement "openssh-client".

Une fois installé, il est possible d'ouvrir une session à distance de la manière suivante :

```
ssh utilisateur@ip_serveur
```

Si vous ne spécifiez pas de nom d'utilisateur, c'est l'utilisateur courant de votre session GNU/Linux qui sera utilisé.

Pour lancer des applications graphiques, il faudra le préciser dans la commande ssh en rajoutant l'option -X :

`ssh -X utilisateur@ip_serveur`.

A la première connexion, le message suivant apparaît :

```
Warning: Permanently added 'xxxxx' (RSA) to the list of known hosts.
```

Cela signifie qu'on ne s'est jamais connecté sur cette station et qu'un identifiant est ajouté à la liste des hôtes connus.

Il peut arriver que le certificat du serveur change (par exemple en cas de réinstallation).

Le message suivant apparaîtra :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
65:6d:9d:c0:78:f7:60:bf:13:86:59:16:53:07:3b:a4.
Please contact your system administrator.
Add correct host key in /home/xxx/.ssh/known_hosts to get rid of this message.
Offending key in /home/xxx/.ssh/known_hosts:12
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
X11 forwarding is disabled to avoid man-in-the-middle attacks. Permission denied (publickey,password).
```

Ce message nous apprend plusieurs choses :

- le serveur ssh a une clef différente de celle de notre dernier passage ;
- le fichier comprenant les hôtes connus est `/home/xxx/.ssh/known_hosts` ;
- l'identifiant de l'hôte est spécifié à la ligne 12 (Offending key in /home/xxx/.ssh/known_hosts:12).

Si vous êtes sûr que l'hôte est le bon, il vous suffira de supprimer la ligne 12 du fichier known_hosts et de relancer une connexion.

Il faudra spécifier le mot de passe de l'utilisateur pour se connecter.

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

Ssh propose également la connexion par échange de clef. Cela permet de se connecter à distance sans connaître le mot de passe de l'utilisateur.

L'échange de clef peut être réalisé par l'intermédiaire d'un serveur Zéphir. Pour plus d'informations, consulter la documentation spécifique à ce module.

Exécution de commande à distance

Une fois connecté à distance, vous pouvez lancer n'importe quelle action comme si vous étiez en local.

Transfert de fichier à distance

Pour envoyer un fichier sur un serveur, il faut faire :

```
scp nom_du_fichier utilisateur@ip_serveur:/repertoire/de/destination/
```

Pour récupérer un fichier d'un serveur :

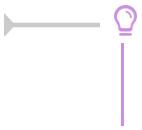
```
scp utilisateur@ip_serveur:/repertoire/source/nom_du_fichier /repertoire/de/destination/
```

Pour récupérer un répertoire d'un serveur :

```
scp -r utilisateur@ip_serveur:/repertoire/ /repertoire/de/destination/
```

Enfin, il est possible d'avoir un shell proche de la commande FTP en faisant :

```
sftp utilisateur@ip_serveur
```



Sur la plupart des gestionnaires de fichier disponibles sous GNU/Linux, il est possible de faire des transferts de fichier avec SSH graphiquement (logiciel Filezilla par exemple).

1.2.7.c. SSH sous Windows

Exécution de commande à distance

Putty est un logiciel libre implémentant un client Telnet[p.520] et SSH[p.518] pour Unix et Windows.

http://www.chiark.greenend.org.uk/~sgtatham/putty/

Dans l'environnement EOLE, il permet de se connecter à un serveur à distance depuis un poste Windows et, ainsi, pouvoir exécuter des commandes.

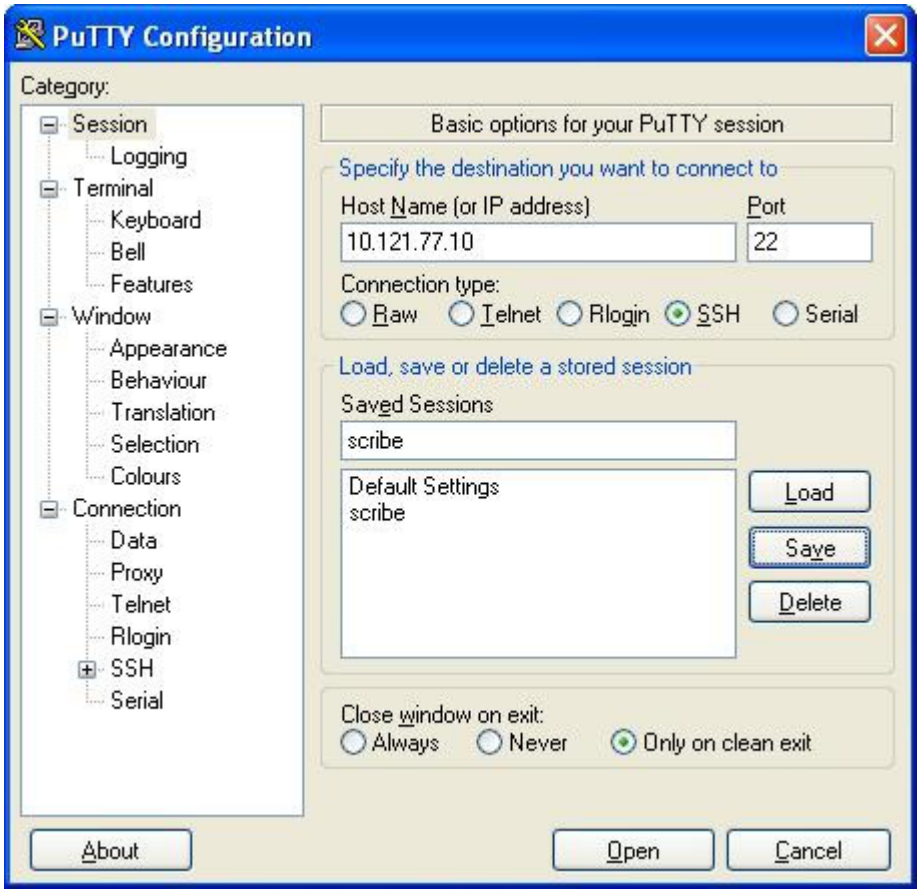
La connexion avec Putty au serveur se fait en utilisant le protocole SSH.

Sur le module Scribe, Putty est pré-installé dans le répertoire personnel d'*admin* (`U:\client\putty.exe`).

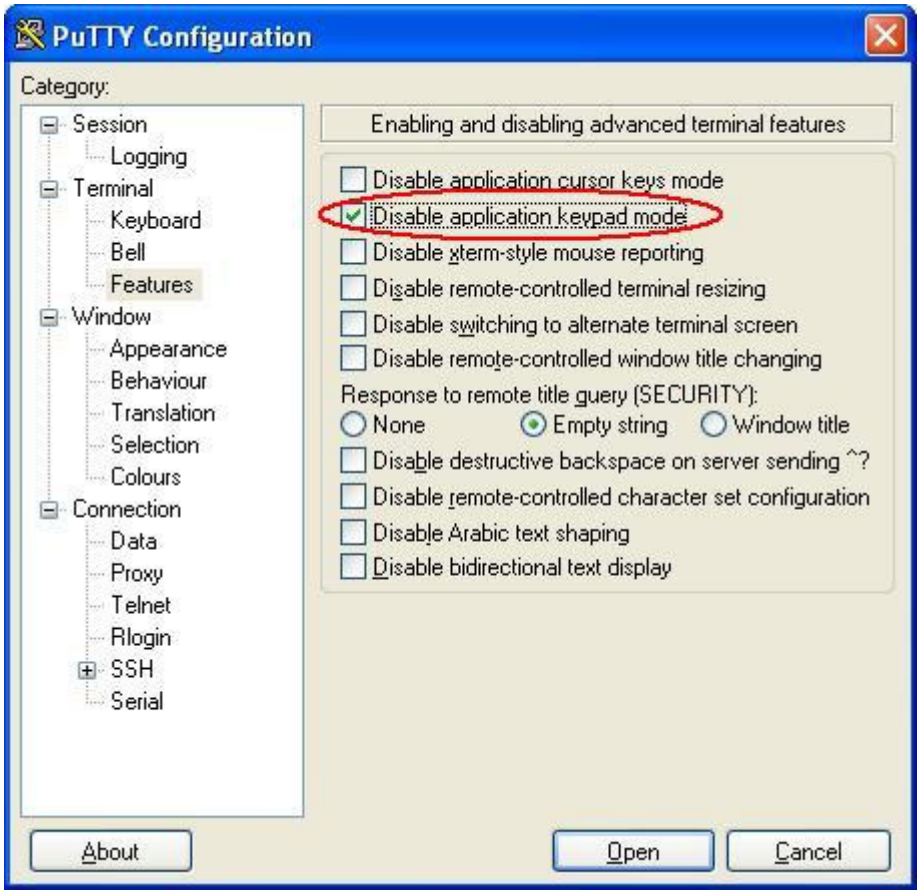
Configuration pour les serveurs EOLE

Pour obtenir un meilleur environnement de travail, la configuration par défaut de Putty doit être modifiée.

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

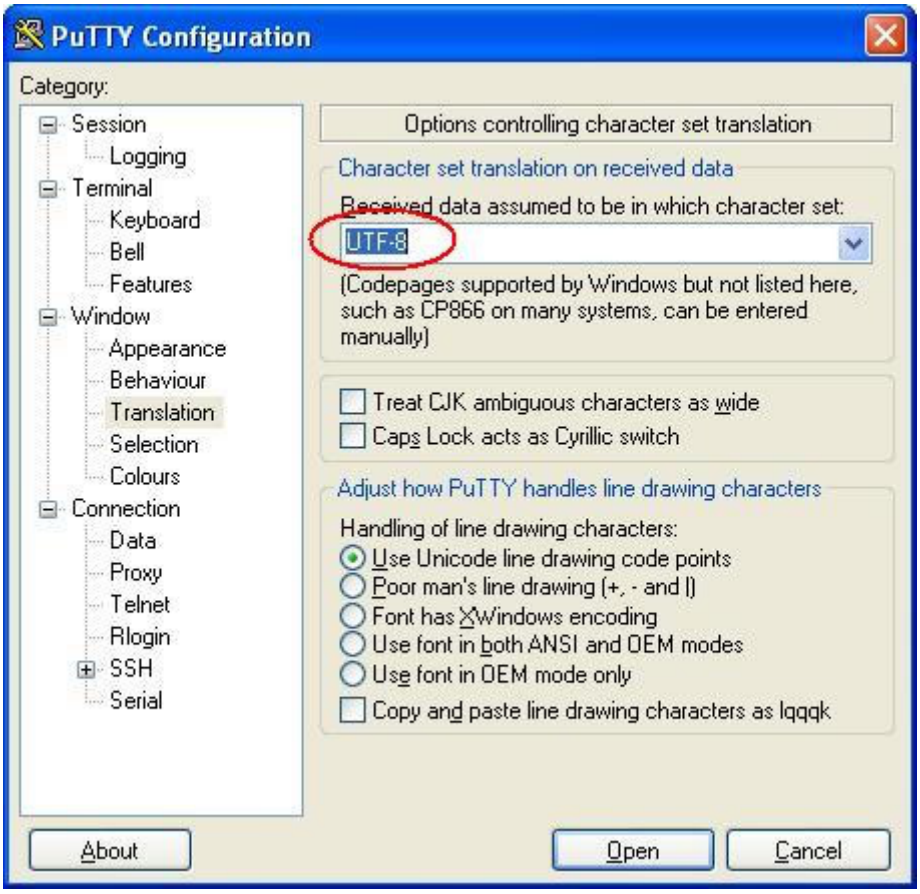


Fenêtre principale

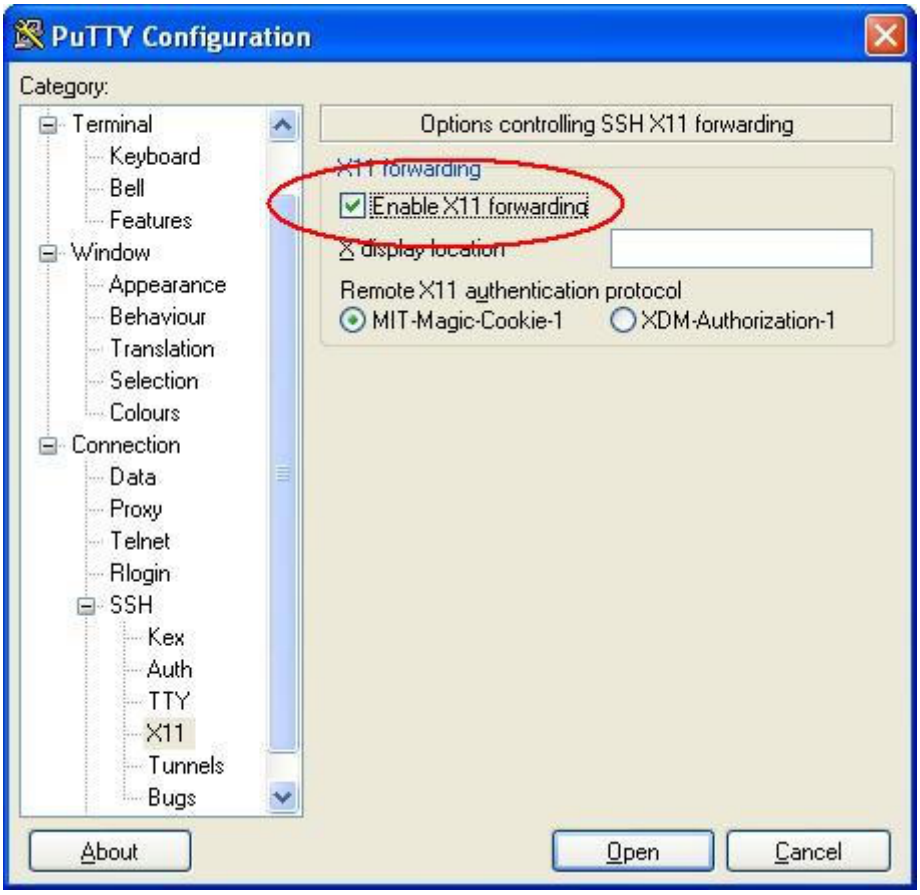


Permettre au pavé numérique de fonctionner correctement (dans "vim" par ex.)

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



Permettre aux accents de s'afficher normalement



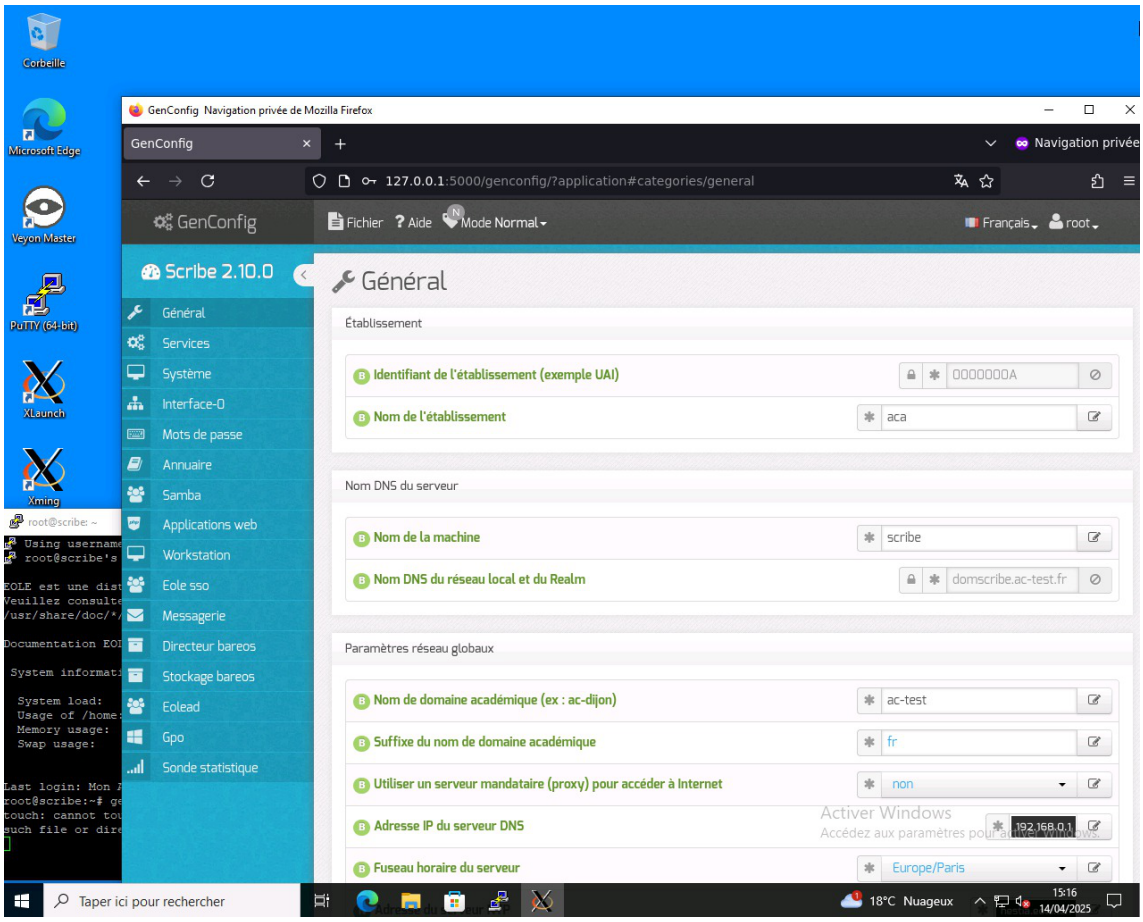
Pouvoir lancer des applications graphique du serveur depuis la station (Ex. "gen_config")

La dernière capture montre comment autoriser la redirection des applications graphiques vers votre poste.

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

Cependant vous devrez utiliser Xming [http://sourceforge.net/projects/xming] .

C'est un logiciel libre permettant d'émuler un serveur X [http://fr.wikipedia.org/wiki/X_Window] vers lequel sera redirigé l'application graphique lancée à travers ssh sur le serveur EOLE.



Lancement de "gen_config" sur un poste Windows

Transfert de fichier à distance

Il existe une interface graphique de transfert de fichier à distance. Il s'agit de WinSCP.

On utilise le logiciel comme un client FTP normal.

1.2.8. Quelques références

- Le site du Kernel Linux : http://www.kernel.org ;
- Le projet GNU : http://www.gnu.org ;
- Site réputé pour ses documentations et son forum d'entraide : http://www.lea-linux.org/ ;
- Guide de survie du débutant : http://www.delafond.org/survielinux/ ;
- Un manuel en ligne (man) : https://www.tldp.org/guides.html ;
- Définitions sur Wikipédia :
  - Noyau Linux : http://fr.wikipedia.org/wiki/Noyau_Linux,
  - Projet GNU :http://fr.wikipedia.org/wiki/GNU,
  - Distribution :http://fr.wikipedia.org/wiki/Distribution_Linux,

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

- Les Permissions Unix : http://fr.wikipedia.org/wiki/Permissions_Unix.

1.3. Reconfiguration

Suite à un diagnostic, à une modification de la configuration ou à une mise à jour, il est nécessaire de reconfigurer le serveur.

On réalise cette opération avec la commande `reconfigure`, plutôt qu'avec la commande `instance`.

Les différentes valeurs attribuées aux variables sont enregistrées dans un fichier `config.eol` au format JSON[p.505] 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.

Reconfigure

Cette commande `reconfigure` sert à appliquer un changement de configuration (par exemple, le changement d'adressage IP) ou à appliquer des changements apportés par la mise à jour d'un ou de plusieurs paquets.

Avec `Maj-Auto`, un message indique s'il est nécessaire de lancer `reconfigure`.

Cette commande :

- ré-applique le SID[p.517] trouvé dans l'annuaire sur les modules Horus et Scribe ;
- supprime des paquets (utilisé pour les noyaux notamment) ;
- exécute les scripts pre et postreconf ;
- met à jour les valeurs par défaut des dictionnaires ;
- recréé le compte `admin` s'il n'a pas été trouvé (modules Scribe et Horus) ;
- copie, patch[p.513] et renseigne les templates ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (redémarrage automatique si mise à jour par EAD) ;
- relance les services.

Lors d'une mise à jour via l'EAD[p.500], `reconfigure` est lancé automatiquement. Si la mise à jour a été effectuée sur la console ou via SSH avec la commande `Maj-Auto` un message indique s'il est nécessaire de lancer reconfigure.

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

reconfigure is not instance : pourquoi reconfigure au lieu d'instance

La commande `instance` est exécutée à l'installation d'un nouveau serveur.
Cette commande :

- initialise les mots de passe des comptes `root`, `eole` et `admin` ;
- propose de créer des comptes d'administration supplémentaires ;
- génère un nouveau SID ;
- génère l'annuaire et les bases MySQL si inexistants ;
- lance des commandes spécifiques à l'instanciation ;
- copie, patch et renseigne les templates ;
- (re)lance les services ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD).



Il existe plusieurs contre-indications à l'utilisation de la commande `instance` sur un serveur déjà instancié :

- les commandes exécutées peuvent être différentes ;
- la commande instance demande une interaction tandis que reconfigure est automatique, il ne pose pas de question et est donc plus rapide ;
- l'interaction est source d'erreur (possibilité d'écrasement de l'annuaire ou des bases de données). Sur les modules Scribe et Horus si l'utilisateur répond oui à la question concernant la re-génération de l'annuaire, tous les comptes utilisateurs et les stations intégrés au domaine sont effacés.

Des comptes d'administration supplémentaires peuvent être ajoutés en dehors de la procédure d'instance grâce à la commande `add_restricted_admin`.

1.4. L'interface d'administration EAD

EOLE offre une interface simplifiée de gestion du serveur : l'interface d'administration EAD.



Accueil EAD outil d'administration

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

Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

1.4.1. Principe général

L'EAD (Eole ADmin) est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible avec un navigateur à l'adresse `https://<adresse_module>:4200`.



Depuis la version EOLE 2.6, il n'est plus possible d'accéder à l'EAD à l'aide de l'adresse IP du serveur, il faut impérativement utiliser un nom de domaine et que celui-ci soit présent dans le certificat SSL.

Cette restriction est notamment due au durcissement du support du protocole HTTPS[p.503] par les navigateurs.

L'EAD est composé de deux parties :

- un serveur de commandes (**ead-server**), présent et actif sur tous les modules ;
- une interface (**ead-web**), désactivable depuis l'interface de configuration du module dans l'onglet `Services` en passant `Activer l'interface web de l'EAD` à `non`.

Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, Sentinelle, ...) 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.



Accueil EAD outil d'administration



Aide

Un point d'interrogation est accessible en bas à droite de certaines pages, il permet d'afficher une aide associée.



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.

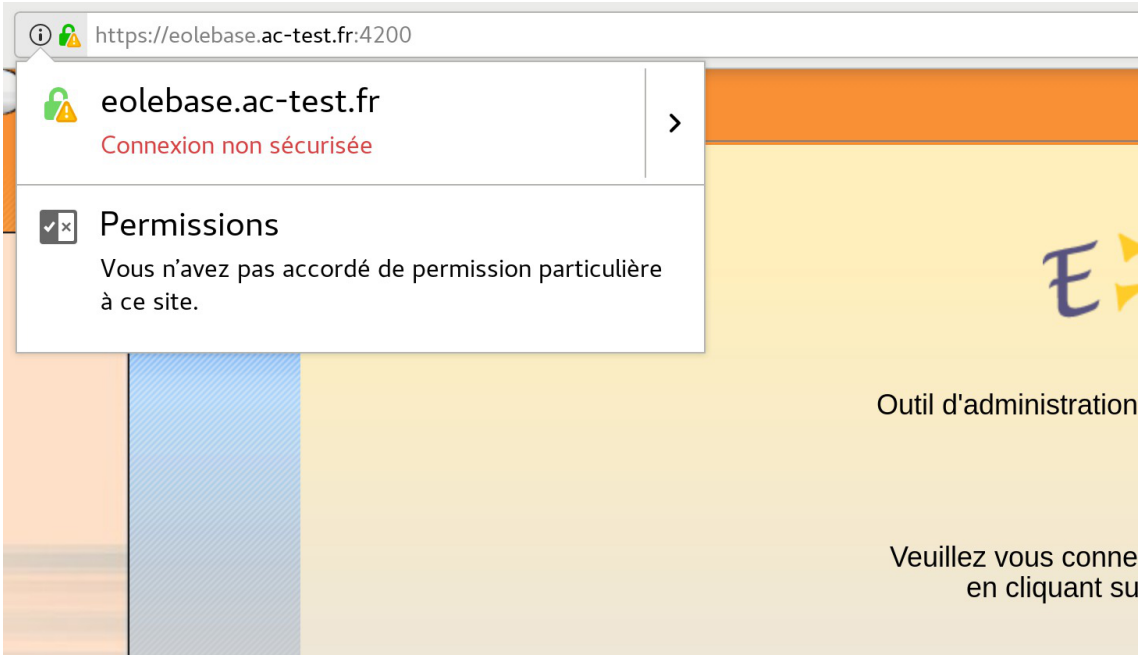
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

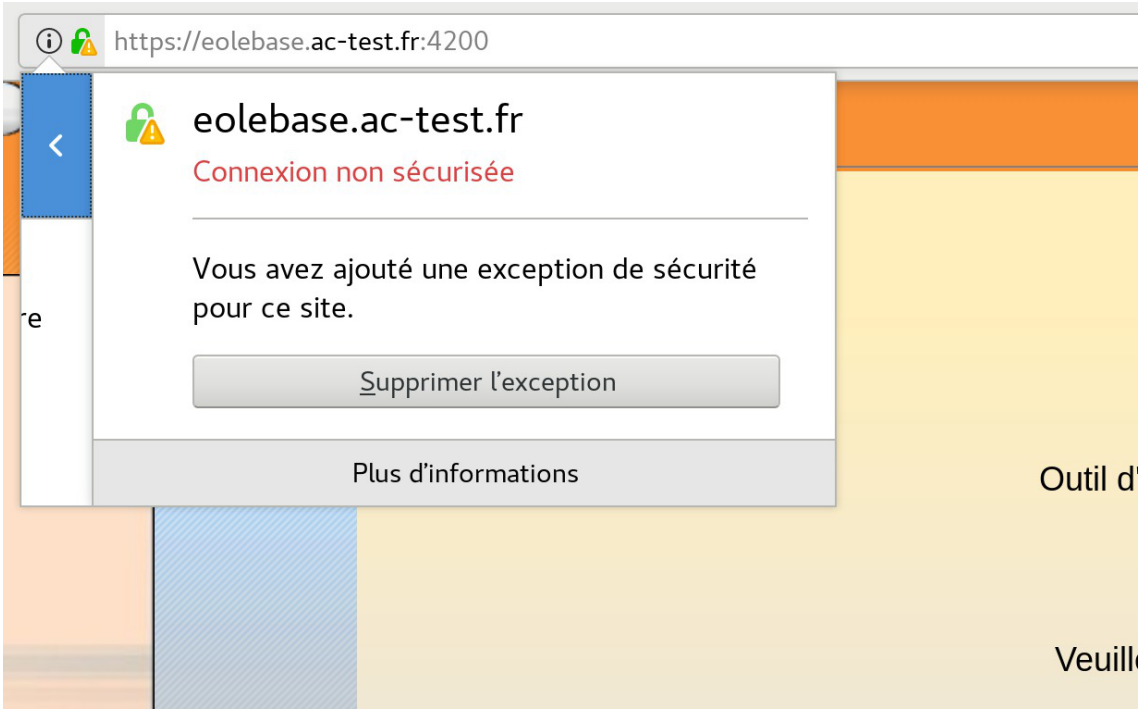
Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

Exemple avec Firefox

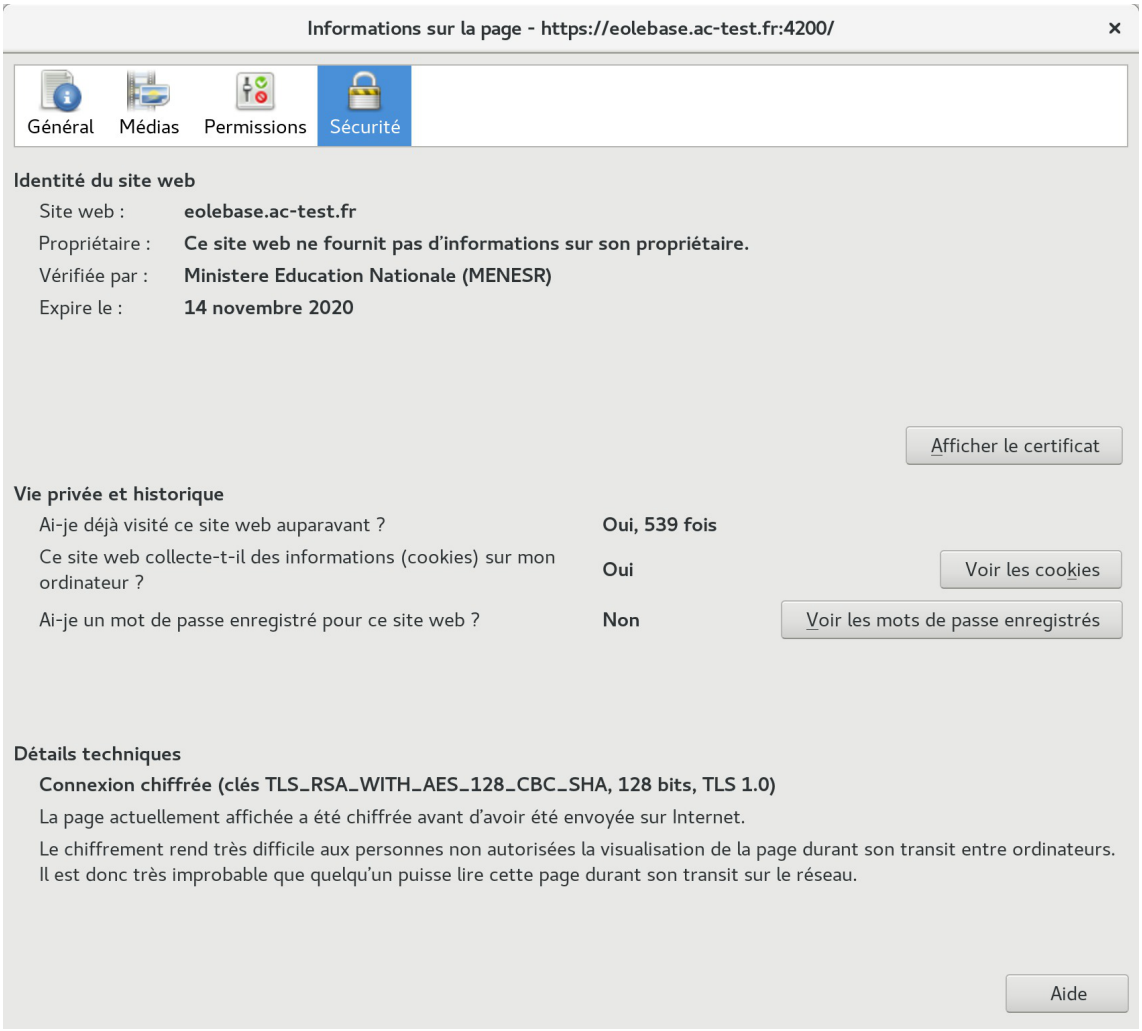
- Cliquer sur le cadenas à côté de l'URL



- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

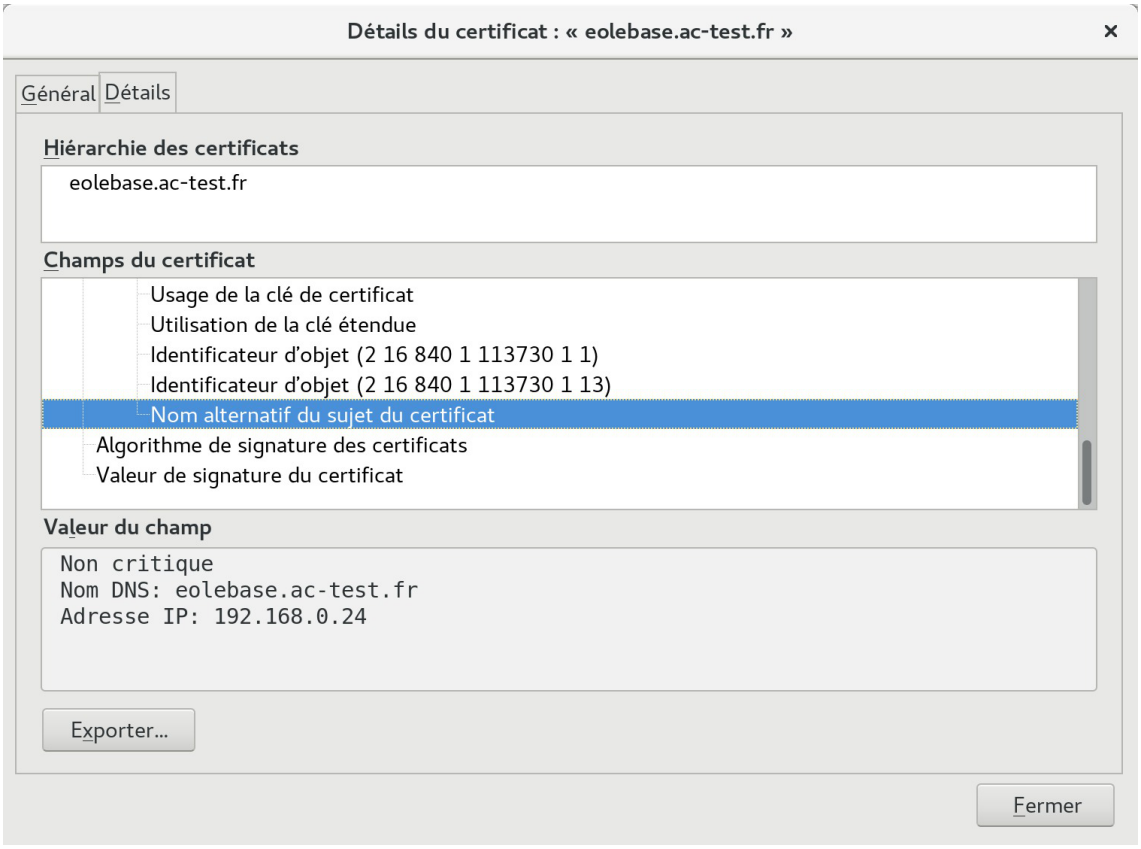


- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- 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 sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.

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



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).

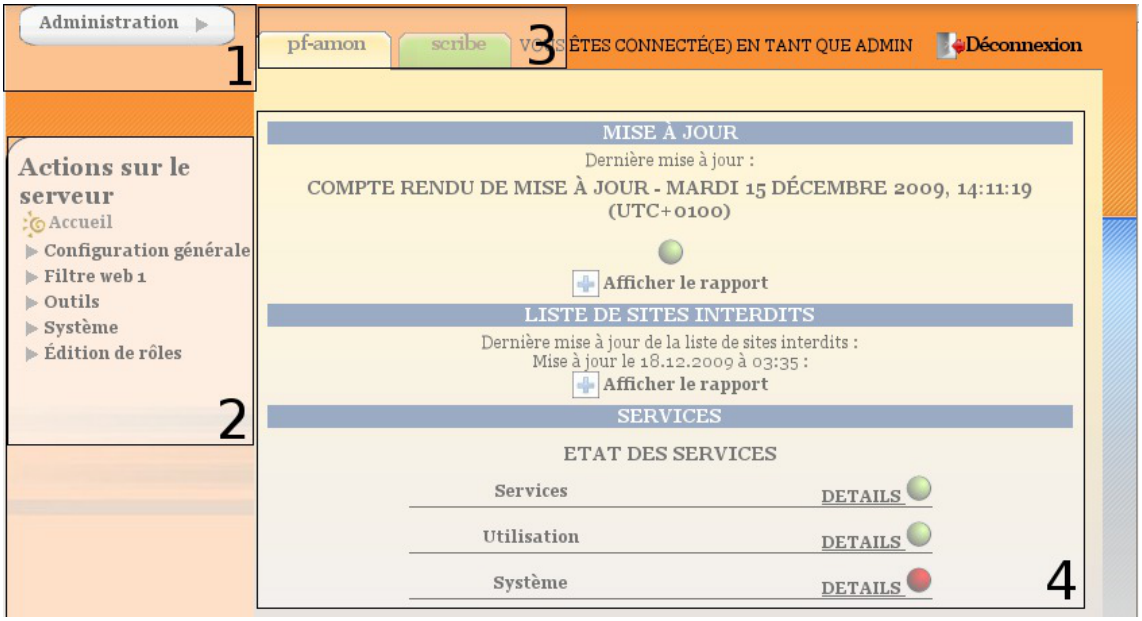
```
# reconfigure
# /usr/share/creole/gen_certif.py -f ou #
```


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

> `/usr/share/creole/gen_certif.py -f nom_du_certificat` pour la régénération d'un certificat en particulier.
>
> `# reconfigure`

1.4.2. Premier pas dans l'administration d'un serveur

Lorsque vous vous êtes connecté sur un serveur de commandes, vous avez quatre éléments :



Page d'accueil lors de la connexion à un serveur

1. la gondole d'administration ;
2. le menu d'action (propose les actions auxquelles vous avez accès) ;
3. les onglets (les serveurs enregistrés sur l'interface) ;
4. la partie centrale ou espace de travail (il s'agit de la partie venant du serveur de commandes).

1 - La gondole d'administration

Elle permet d'accéder aux actions de base de l'interface (ajout/suppression de serveur, déconnexion, retour vers l'accueil, choix de la feuille de style CSS, connexion locale).

2 - Le menu d'action

Il permet d'accéder aux actions disponibles sur le serveur de commandes.

3 - Les onglets (les serveurs enregistrés sur l'interface)

Ils permettent d'accéder aux divers serveurs EOLE enregistrés sur l'interface.

4 - La partie centrale ou espace de travail

Les éléments affichés dans cette partie viennent du serveur de commandes.

C'est un conteneur pour les actions (sous forme de rapport, formulaire ...).

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

La page d'accueil d'un serveur de commandes affiche les rapports de :

- mise à jour (sur tous les modules) ;
- mise à jour de listes de sites interdits sur le module Amon ;
- sauvegarde Bareos sur les modules Horus et Scribe ;
- importation sur le module Scribe.

Elle affiche également les diodes d'état du serveur (agents Zéphir).

Les agents Zéphir peuvent être consultés directement en utilisant l'adresse : `http://<adresse module>:8090`

Voir aussi...

Surveillance de l'état du serveur [p.265]

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

Le serveur Scribe étant derrière un serveur Amon, la configuration des deux modules permet de faire écouter l'EAD du serveur Scribe sur le port 4203 et donc d'y accéder depuis l'extérieur grâce à une redirection Nginx.

Avantages

Cette configuration présente plusieurs avantages par rapport à la méthode consistant à ajouter le serveurs de commandes du module Scribe dans l'interface EAD du serveur Amon :

- elle ne nécessite pas de déclarer le serveur SSO du serveur Scribe comme source d'authentification de l'EAD du serveur Amon ;
- il n'y a pas de problème d'incompatibilité (templates, protocoles obsolètes, ...) dans le cas où les versions des EAD des deux modules sont différentes ;
- elle simplifie la gestion des certificats.

Configuration côté Scribe

Dans l'interface de configuration du module Scribe, en mode expert, aller dans l'onglet `Ead-web` et passer la variable `Activer l'interface web de l'EAD sur un second port` à `oui` et vérifier que le port personnalisé est bien le `4203`.



Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande

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

`reconfigure` est nécessaire afin que l'EAD écoute sur le port `4203`.

Configuration côté Amon

Dans l'interface de configuration du module Amon, aller dans l'onglet `Reverse proxy`, passer la variable `Activer la redirection de l'EAD d'un Scribe` à `oui` puis renseigner l'adresse IP du module Scribe et vérifier que le port renseigné est le `4203`.



Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande `reconfigure` est nécessaire afin que la redirection soit appliquée.

L'autorisation d'accès au port configuré est gérée par ERA via la directive optionnelle cachée [p.498] : `ead scribe`.

Voir aussi...

Onglet Ead-web : EAD et proxy inverse [p.190]

Onglet Reverse proxy : Configuration du proxy inverse [p.125]

1.4.4. Ajout/suppression de serveurs

Il est possible de connecter plusieurs serveurs de commandes à une même interface.

Une seule interface sert alors à administrer l'ensemble des serveurs EOLE d'un établissement.

Depuis la version EOLE 2.6, il n'est plus possible d'accéder à l'EAD à l'aide de l'adresse IP du serveur, il faut impérativement utiliser un nom de domaine et que celui-ci soit présent dans le certificat SSL.

Cette restriction est notamment due au durcissement du support du protocole HTTPS [p.503] par les navigateurs.

Ajout/suppression de serveurs de commandes dans l'interface

L'interface de l'EAD est une coquille vide.

Elle permet de se connecter à des serveurs de commandes qui proposent des actions.

Lors de l'instanciation du serveur, le serveur de commandes du serveur est enregistré auprès de son interface.

La coquille n'est pas laissée vide.

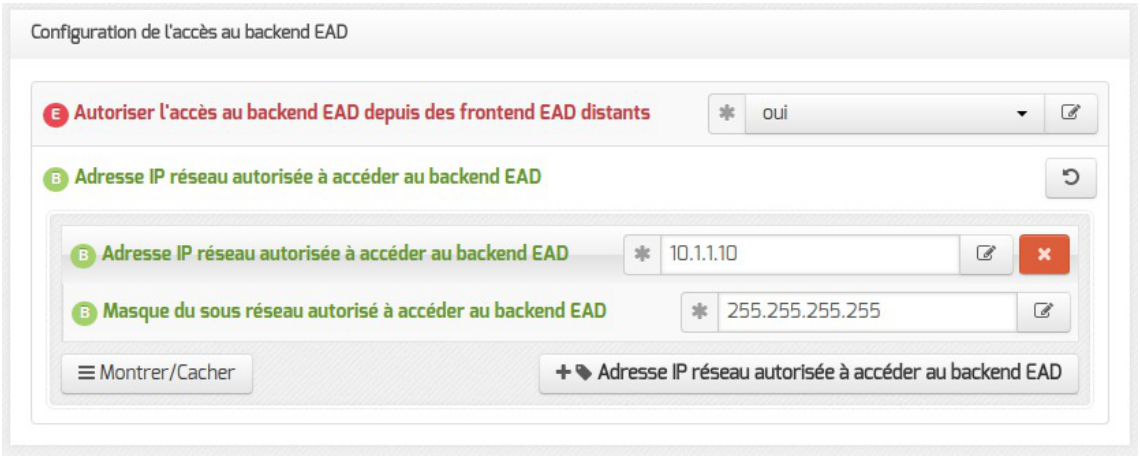
Il est possible d'enregistrer plusieurs serveurs EOLE sur l'interface.

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

On obtient ainsi un point d'entrée unique pour administrer l'ensemble des serveurs d'un établissement.
Une seule interface web dans laquelle chaque onglet représente un des serveurs.
Il est ensuite possible de gérer les accès ainsi que les actions autorisées par utilisateur ou par groupe.

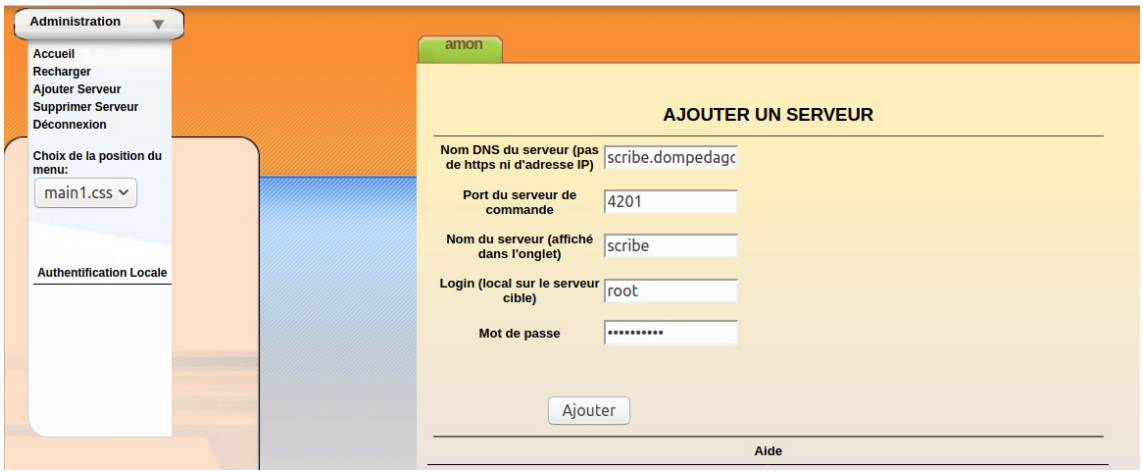
Ajout de serveur

À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD de se connecter à un serveur de commandes EAD distant, il faut, sur le module distant, l'autoriser explicitement pour chaque interface. Cela peut s'effectuer en mode expert dans l'interface de configuration du module, dans l'onglet `Interface-n`.



Dans la gondole d'administration de l'EAD, cliquer sur `Ajouter serveur` et renseigner :

- le nom DNS du serveur ;
- le port du serveur de commandes (4201) ;
- le nom à afficher dans l'onglet ;
- le nom de l'utilisateur `eole` du serveur de commandes à enregistrer ;
- le mot de passe correspondant (sur le serveur à enregistrer).



Depuis la version EOLE 2.6, si le certificat du serveur à ajouter n'est pas signé par une autorité de certification[p.494] connue du serveur hébergeant le frontend EAD, il sera nécessaire de copier sa CA sur ce dernier.

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

L'exemple suivant décrit la copie et l'intégration de la CA d'un module Scribe sur un module Amon :

```
root@amon:~# scp root@scribe:/etc/ssl/certs/ca_local.crt
  /usr/local/share/ca-certificates/
root@amon:~# update-ca-certificates
```

Le compte `root` peut être utilisé à la place du compte `eole` pour toutes les manipulations présentées ici.

Suppression de serveur

Suppression normale

C'est le mécanisme de suppression classique. L'onglet du module est vert et on souhaite le retirer.

Dans la gondole d'administration, cliquer sur `Supprimer Serveur` :

- choisir le serveur à supprimer ;
- entrer le login `eole` du serveur de commandes à désinscrire ;
- entrer le mot de passe ;
- valider.



Suppression d'un serveur

La référence sera supprimée côté interface et côté serveur de commandes.

Suppression forcée

Il ne faut utiliser la suppression forcée du serveur que si l'onglet est rouge ou que le mot de passe du serveur de commandes à supprimer est inconnu.

Il est préférable d'utiliser la suppression normale d'un serveur.

Dans la gondole d'administration, cliquez sur `Supprimer Serveur` :

- choisir le serveur à supprimer ;
- entrer le login (utilisez le compte `eole` du serveur de l'interface et non celui du serveur de commandes à désinscrire) ;
- entrer le mot de passe ;
- cocher la case `☑ Forcer la désinscription` ;

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

- valider.



Suppression forcée d'un serveur

La référence ne sera supprimée que du côté de l'interface.

Désinscription forcée suite à un changement d'adresse IP

Si vous avez modifié l'adresse IP d'un serveur, il est possible que son onglet devienne rouge dans l'EAD.

Il faut alors utiliser la suppression forcée et ré-enregistrer le serveur.

Complément technique

Les interfaces associées au serveur de commandes local sont enregistrées dans le fichier `/usr/share/ead2/backend/config/frontend_keys.ini`

```
[keys]
127.0.0.1 = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Les serveurs de commandes associés à l'interface EAD locale sont enregistrés dans le fichier `/usr/share/ead2/frontend/config/servers.ini`

```
[1]
url = https://127.0.0.1
port = "4201"
comment = u"amon"
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

1.4.5. Surveillance de l'état du serveur

La page d'accueil d'un serveur de commandes affiche les rapports de :

- mise à jour ;

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

- mise à jour de listes de sites interdits sur le module Amon ;
- sauvegarde Bareos sur les modules Horus et Scribe ;
- importation sur le module Scribe.

Elle affiche également les diodes d'état du serveur (agents Zéphir).

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

1.4.5.a. Système

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

- Informations systèmes
- Occupations des disques
- Statistiques réseau
- État des sommes MD5 de paquets

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

- Onduleur

> Surveillance de l'état des sommes MD5 des paquets

L'outil `eole-debsums` permet de surveiller les modifications apportées aux fichiers présents sur les modules EOLE grâce à la vérification des sommes de contrôle MD5[p.508] 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.498].

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:
```

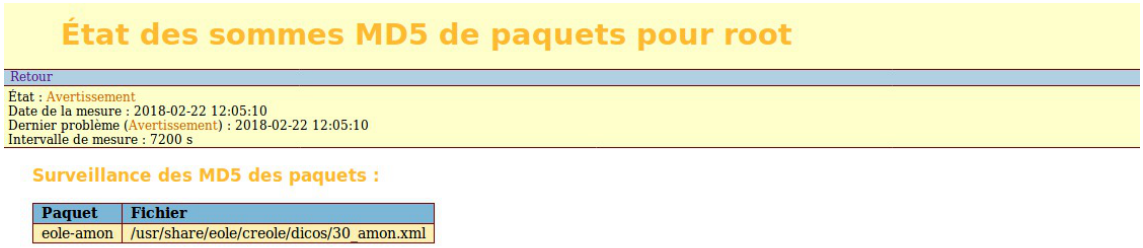

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
    /usr/share/eole/creole/dicos/30_amon.xml

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

```

Un agent[p.493] de surveillance Zéphir permet de surveiller les sommes MD5 des paquets.



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



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`.

1.4.5.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

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

1.4.5.d. Utilisation

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

- Mise à jour

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

- Sauvegarde

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

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

1.4.6. Authentification locale et SSO

Dans l'EAD, il existe deux systèmes d'authentification :

- l'authentification unique (SSO[p.518]) ;
- l'authentification locale (PAM).

Dans le cas de l'authentification SSO, le serveur de commandes et l'interface se connectent à un même serveur d'authentification.

Pour se connecter en tant qu'*administrateur* :

- authentification SSO : l'utilisateur `admin` de l'annuaire associé au serveur sera utilisé ;
- authentification locale : les utilisateurs `root` et `eole` peuvent être utilisés.

1.4.6.a. Authentification locale

L'authentification locale est un mécanisme plus simple mais moins souple que l'authentification SSO. Il utilise les comptes système de la machine hébergeant le serveur de commandes. Le nombre d'utilisateurs et leur gestion est donc plus limitée.

L'authentification locale est systématiquement activée et peut être utilisé conjointement avec l'authentification SSO.

Pour vous authentifier localement, dans la gondole d'administration :

- cliquer sur `authentification locale` ;
- cliquer sur le nom de votre serveur.

Vous accédez alors au formulaire d'authentification locale.

Si le serveur SSO n'est pas activé, vous arriverez sur ce même formulaire en cliquant sur l'onglet.

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



Formulaire d'authentification locale

Il est possible d'utiliser la gestion des rôles pour déléguer une partie de l'administration à d'autres comptes systèmes.

1.4.6.b. L'authentification SSO

Connexion

Entrer l'adresse `https://<adresse_serveur>:4200` dans le navigateur et cliquer sur l'onglet du serveur à administrer.

Une re-direction vers le serveur SSO (`https://<adresse_serveur>:8443/`) est effectuée et le formulaire d'authentification apparaît :



Formulaire d'authentification SSO

L'utilisation d'un serveur SSO permet de centraliser l'authentification. En s'authentifiant une seule fois vous pouvez vous connecter aux différents serveurs de commandes enregistrés dans l'interface (naviguer d'un onglet à l'autre).

Les rôles permettent d'utiliser d'autres comptes pour se connecter (ex : sur Scribe, les professeurs ont un rôle prédéfini).

Pour utiliser l'authentification SSO, il est indispensable que le serveur SSO utilisé par l'interface et par les serveurs de commandes qui y sont inscrits **soit identique**.

1.4.7. Redémarrer, arrêter et reconfigurer

Il est possible de redémarrer, arrêter ou reconfigurer un module EOLE directement depuis l'interface d'administration EAD.

Ces actions sont accessibles depuis `Système/Serveur`.

Ces trois actions vous déconnectent de l'EAD.

Redémarrer un serveur


Action de redémarrage d'un serveur

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

Reconfigurer un serveur



Action de reconfiguration d'un serveur

Arrêter un serveur



Action d'arrêt d'un serveur

1.4.8. Mise à jour depuis l'EAD

Dans `Système` / `Mise à jour`, l'EAD propose une interface de mise à jour du serveur, il est possible de :

- de lister les paquets disponibles pour la mise à jour ;
- de programmer une mise à jour différée (dans 3 heures par exemple, ou dans 0 heure pour le faire tout de suite) ;
- d'activer / désactiver les mises à jour hebdomadaires (le jour et l'heure de la mise à jour automatique sont déterminés aléatoirement).

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.



Rapport de mise à jour

Penser à consulter le rapport de mise à jour et l'état des services sur la page d'accueil.

Reconfiguration et redémarrage automatique

Une mise à jour lancée depuis l'EAD exécute automatiquement une reconfiguration du serveur avec la commande `reconfigure`, il n'est donc pas nécessaire d'en lancer un par la suite comme c'est le cas depuis la console.

Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

1.4.9. Arrêt et redémarrage de services

Dans l'EAD, il existe deux manières d'arrêt ou de redémarrage des services :

- le mode normal ;
- le mode expert.

1.4.9.a. Redémarrer ou arrêter des services (mode normal)

Pour utiliser la fonctionnalité en mode normal il faut dans un premier temps créer des groupes de

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

services.

Création de groupes de services

Le nom des services, au sens système, n'est pas souvent parlant. Par exemple, il faut savoir que le service `apache2` est le nom du serveur web.

Les groupes de services permettent de regrouper un ou plusieurs services sous une dénomination plus claire. Cela permet de regrouper et donc de faciliter le redémarrage/arrêt de services.

Création un groupe de services nommé `web` :

Pour créer un groupe, cliquer sur le bouton `créer groupe` dans `Système/Editeur de services` :

1. entrer le nom du groupe ;
2. choisir les services du groupe (cocher les cases) ;
3. cliquer sur la flèche verte ;
4. valider avec le bouton `Créer`.

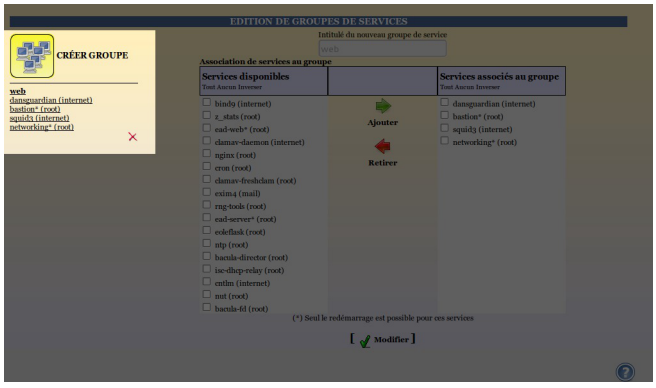


Création d'un groupe de services (1)



Création d'un groupe de services (2)

Une fois créé le groupe de services apparaît sous l'icône CRÉER GROUPE à gauche de l'écran.



Création d'un groupe de services (2)

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

Un groupe de services peut être modifié en cliquant sur son nom dans la liste de gauche sous l'icône CRÉER GROUPE.

Un groupe de services peut être supprimé en cliquant sur la croix rouge sous son descriptif dans la liste de gauche sous l'icône CRÉER GROUPE.

Redémarrer ou arrêter un groupe de services

Une fois créé, un groupe apparaît dans l'onglet `Système/Services (mode normal)`, il est alors possible de redémarrer ou d'arrêter le groupe de services.



Redémarrage d'un groupe de services

La gestion des rôles permet de déléguer l'accès à des actions, on peut ainsi permettre à la documentaliste de l'établissement de redémarrer le logiciel BCDI.

Tous les groupes de services lui seront néanmoins accessibles.

Complément technique

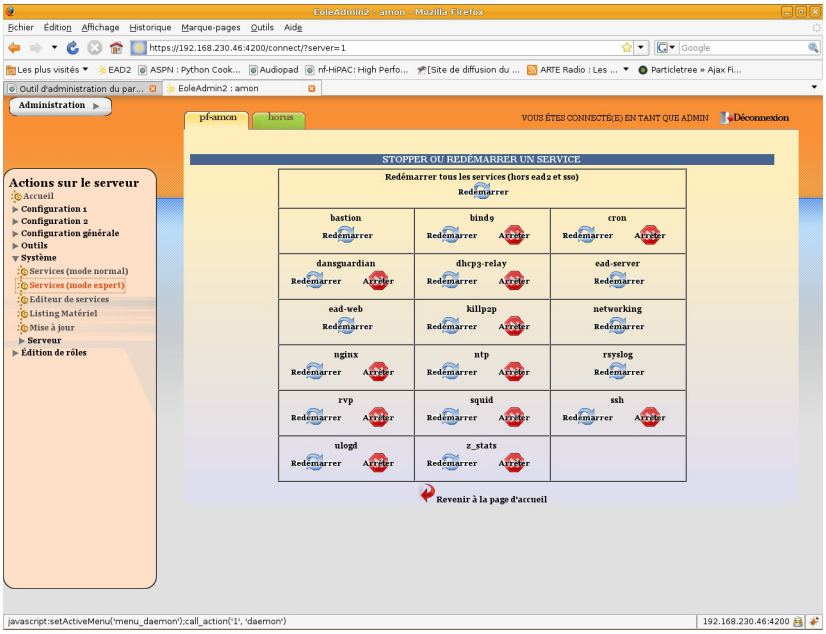
Les groupes de services déclarés dans l'EAD sont enregistrés dans le fichier `/usr/share/ead2/backend/config/simple_services.ini`

```
[amon]
w____e b =
squid3#internet,networking#root,eole-guardian#internet,bastion#root
```

1.4.9.b. Redémarrer ou arrêter des services (mode expert)

Dans `Système/Services (mode expert)`, cliquer sur le bouton `Arrêter` ou `Redémarrer` du service voulu.

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



Actions sur les services (mode expert)

Les services liés au fonctionnement de l'EAD ne sont disponibles qu'en redémarrage. Sinon, vous perdrez tout accès à l'interface.

Pour relancer l'ensemble des services (sauf l'EAD et le serveur SSO) choisir le bouton : `Redémarrer tous les services (hors EAD et SSO)`.

1.4.10. Rôles et association de rôles

L'EAD est composé, d'*actions*. Chaque action ayant un but bien précis.

L'EAD dispose d'un mécanisme de délégation d'*actions* à des utilisateurs déterminés.

Pour affecter certaines actions à un utilisateur, l'EAD utilise une mécanisme interne : les **rôles**.

Par défaut sur les modules EOLE, l'utilisateur **admin** est associé au rôle **administrateur**.

Plusieurs rôles sont prédéfinis sur les différents modules EOLE et certains sont propres à certains d'entre eux :

- administrateur ;
- professeur (utilisé sur le module Scribe) ;
- élève (utilisé sur le module Scribe) ;
- administrateur de classe (utilisé sur le module Scribe) ;
- administratif dans Scribe (utilisé sur le module Scribe) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon) ;
- administrateur du Scribe (utilisé sur le module AmonEcole) ;
- administrateur de l'Amon (utilisé sur le module AmonEcole).

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

1.4.10.a. Déclaration des actions

Les actions de l'EAD sont déclarées dans les fichiers : `/usr/share/ead2/backend/config/actions/actions_*.cfg`

Ces fichiers au format *texte* permettent de déclarer les fichiers python déclarant eux-mêmes des actions EAD à charger.

Ces fichiers sont situés dans `/usr/share/ead2/backend/actions` et ses sous-répertoires.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/actions.cfg` : fichiers des actions de base ;
- ainsi que tout les fichiers `actions_*.cfg` présents dans le répertoire `/usr/share/ead2/backend/config/actions`.

Syntaxe des fichiers

Les fichiers d'action sont déclarés avec leur chemin court depuis `/usr/share/ead2/backend/actions` et sans l'extension ".py".



La déclaration des fichiers d'action suivants :

- `/usr/share/ead2/backend/actions/mes_actions.py`
- `/usr/share/ead2/backend/actions/repertoire/autres_actions.py`

prend la forme suivante dans le fichier `actions_perso.cfg` :

```
$ cat /usr/share/ead2/backend/actions/actions_perso.cfg
mes_actions
repertoire/autres_actions
```

1.4.10.b. Gestion des rôles

Les rôles de l'EAD sont déclarés dans les fichiers : `/usr/share/ead2/backend/config/perms/perm_*.ini`

Ces fichiers au format *ini* permettent d'associer des actions (permissions) à un ou plusieurs rôles.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/perm.ini` : rôles de base ;
- `/usr/share/ead2/backend/config/perm_local.ini` : rôles déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/perm_acad.ini` : rôles déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers `perm_*.ini` présents dans le répertoire `/usr/share/ead2/backend/config/perms`.

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

Syntaxe des fichiers

Les permissions associent un rôle à une ou plusieurs actions.
Les fichiers `perm*.ini` doivent posséder une section `[role]` et une section `[permissions]`.

```
[role]
nom_du_role = libelle_du_role
[permissions]
action1 = nom_du_role
action2 = nom_du_role
```

Création de rôle via l'EAD

L'interface EAD permet de créer des rôles personnalisés.
Ces rôles ne sont, en fait, qu'une liste d'actions regroupées sous un intitulé et un libellé unique.
Il est possible, dans un deuxième temps d'associer ces rôles à des utilisateurs.



La fenêtre d'édition des rôles

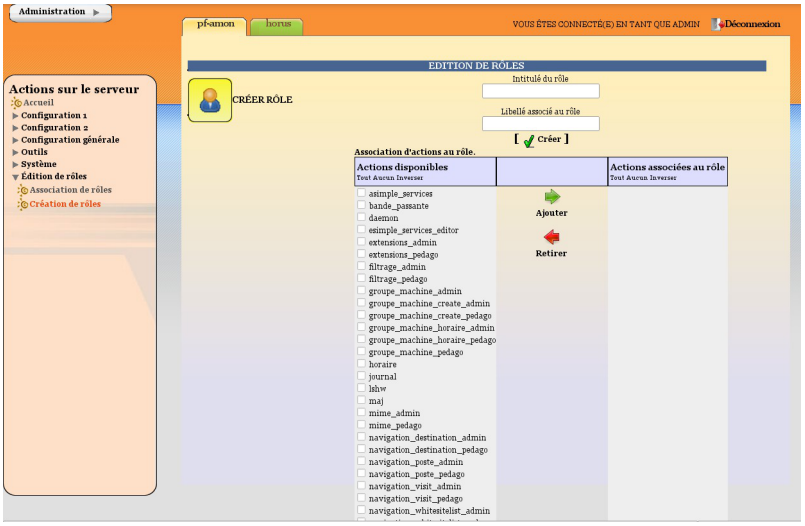
Pour créer un nouveau rôle cliquer sur :

- Édition de rôles/Création de rôles

puis

- Créer rôle
- entrer l'intitulé (le nom) du rôle (sans caractère spécial, sans accent et sans espace) ;
- entrer un libellé (courte description) du rôle ;
- cocher les actions à autoriser ;
- ajouter ;
- créer.

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



Création d'un rôle

Actions obligatoires

Certaines actions doivent être obligatoirement permises pour tous les utilisateurs :

- **help** : utilisé notamment pour l'affichage d'aide ;
- **main_status** : page d'accueil appelée par défaut, elle gère un rôle prof (n'affiche pas les états de services) et un rôle admin ;
- **update_ead** : outil de téléchargement des javascripts, CSS, images spécifiques au module.

Actions communes aux différents modules

- **lshw** : listing matériel ;
- **maj** : action de mise à jour ;
- **daemon** : relancer des services (mode expert) ;
- **simple_services_editor** : éditer des groupes de services pour le mode simplifié ;
- **simple_services** : redémarrer/arrêter les services (mode simplifié) ;
- **server-configure**/**server-reboot**/**server-stop** : redémarrer/arrêter/reconfigurer le serveur ;
- **role_editor** : création de rôles ;
- **role_manager** : association de rôle (appelée par d'autres actions).

Actions spécifiques au module Amon

La modification du système de filtrage sur le module Amon apporte de profondes modifications sur ce module.

Selon les choix effectués lors de la phase de configuration avec l'interface de configuration du module, vous pouvez choisir d'utiliser une ou deux zones de configuration pour le filtrage et les options du pare-feu.

La zone 1 correspond à la réseau admin et la zone 2 correspond au réseau pedago.

- Gestion des postes
  - **navigation_poste_admin** (ou pedago) : action de gestion des postes à interdire ;
  - **navigation_destination_admin** (ou pedago) : interdire des destinations.

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

- Gestion des groupes de machine
  - **groupe_machine_admin** (ou pedago) : action d'entrée pour la gestion des groupes de machine (gère des restrictions pour le rôle prof) ;
  - **groupe_machine_create_admin** (ou pedago) : action de création de groupe de machine (nécessite groupe_machine) ;
  - **groupe_machine_horaire_admin** (ou pedago) : action de gestion des horaires pour les groupes de machine.
- Gestion des utilisateurs
  - **navigation_banned_user_admin** (ou pedago) : action de gestion des utilisateurs à interdire ;
  - **navigation_moderateur_admin** (ou pedago) : action de gestion des modérateurs ;
  - **navigation_whitelist_admin** (ou pedago) : action de gestion des utilisateurs en liste blanche ;
  - **navigation_whitesitelist_admin** (ou pedago) : action de gestion des sites en liste blanche.
- Gestion des sites
  - **opt_filters_admi**n (ou pedago) : gestion des filtres optionnels pour la zone de configuration 1 (ou 2) ;
  - **filtrage_admin** (ou pedago) : gestion du mode de filtrage syntaxique pour la zone de configuration 1 (ou 2) ;
  - **sites_interdits_admin** (ou pedago) : gestion des sites interdits pour la zone de configuration 1 (ou 2) ;
  - **sites_autorises_admin** (ou pedago) : gestion des sites autorisés pour la zone de configuration 1 (ou 2) ;
  - **extensions_admin** (ou pedago) : gestion des extensions interdites pour la zone de configuration 1 (ou 2) ;
  - **mime_admin** (ou pedago) : gestion des types mime interdits pour la zone de configuration 1 (ou 2).
- Gestion des règles du pare-feu
  - **regles** : mode de fonctionnement du pare-feu ;
  - **peertopeer** : autorisation/interdiction du peer to peer ;
  - **horaire** : horaire de fonctionnement du pare-feu.
- Autres actions
  - **navigation_visit** : action de consultation des logs ;
  - **filtrage_bayes** : action d'évaluation d'URL à l'aide du filtrage bayésien ;
  - **bande_passante** : outil de test de bande passante.

Actions spécifiques au module Scribe

- Gestion des utilisateurs
  - **scribe_user_create** : action de création ;
  - **scribe_user_list** : renvoie le formulaire de recherche par critères qui appelle scribe_user_table pour la validation ;

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

  - **scribe_user_table** : action de listing d'utilisateur (gère les rôles prof_admin et admin) appelle scribe_user_modify, scribe_user_delete, scribe_user_modpassword ;
  - **scribe_user_modify** : action de modification d'utilisateur (utilisée par scribe_user_table gère les rôles prof_admin et admin) ;
  - **scribe_user_delete** : action de suppression d'utilisateur (gère les rôles prof_admin et admin) ;
  - **scribe_user_modpassword** : action de modification d'un mot de passe (gère les rôles prof_admin et admin).
- Actions restreintes (créées pour les professeurs, les personnels administratifs et les professeurs admins, gère le rôle de prof et prof_admin)
  - **scribe_prof_preference** : préférences du professeur connecté (mot de passe, inscription aux groupes, mail) ;
  - **scribe_prof_mod_mail** : modifie le mail d'un professeur (nécessite scribe_prof_preference) ;
  - **scribe_user_password** : action de modification de son propre mot de passe (nécessite scribe_prof_preference) ;
  - **scribe_prof_mod_groupe** : Inscription du prof connecté aux groupes ;
  - **scribe_prof_user** : action d'entrée pour la gestion des utilisateurs par les profs lien vers scribe_prof_user_create et scribe_prof_user_modify ;
  - **scribe_prof_user_create** : action de création d'utilisateur (nécessite scribe_prof_user) ;
  - **scribe_prof_user_modify** : action d'entrée pour la modification des utilisateurs (nécessite scribe_prof_user) ;
  - **scribe_grouped_edition** : action d'entrée pour l'édition groupée d'utilisateur (appelle scribe_user_table).
- Gestion des groupes
  - **scribe_group_create** : création de groupes, niveau, classe..., appelle scribe_group_list ;
  - **scribe_group_list** : liste les groupes, appelle scribe_group_delete, appelle scribe_group_create ;
  - **scribe_group_modify** : modification de groupe ;
  - **scribe_group_delete** : suppression de groupe ;
  - **scribe_prof_group** : entrée pour la gestion des groupes par un prof_admin ou un prof, appelle scribe_prof_user_modify et scribe_prof_group_create ;
  - **scribe_prof_group_create** : action de création de groupe par un prof_admin.
- Gestion des partages
  - **scribe_share** : attribution de lettre de lecteur à un partage.
- Gestion des stations et connexions
  - **scribe_station** : action de suppression forcée de station du domaine ;
  - **scribe_extraction** : action d'extraction sconet ;
  - **scribe_connexion_index** : page d'accueil des observations des connexions ;
  - **scribe_connexion_machine** : page d'affichage des machines connectées ;
  - **scribe_connexion_quota** : observation des quotas ;
  - **scribe_connexion_virus** : affiche la liste les virus repérés ;

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

    - **scribe_connexion_history** : affiche l'historique des connexions.
- Autres actions
    - **scribe_devoir_distribuer** / **scribe_devoir_ramasser** / **scribe_devoir_rendre** / **scribe_devoir_supprimer** : gestion des devoirs ;
    - **bareos** : action de programmation de sauvegarde ;
    - **bareos_config** : action de configuration de sauvegarde ;
    - **scribe_sympa** : action renvoyant des liens pour l'interface de gestion de listes de diffusion ;
    - **printers** : action de gestion simplifiée des imprimantes.

Actions spécifiques au module Horus

- Gestion des connexions
    - **isis** : action d'entrée pour l'interface d'observation des connexions, appelle les actions isis ;
    - **isis_stop** : action d'arrêt de toutes les connexions ;
    - **isis_disconnect** : action de déconnexion d'utilisateur connectés au domaine ;
    - **isis_sendmsg** : action d'envoi de message à des utilisateurs connectés ;
    - **isis_machine** : action de listing des machines connectées au domaine (client, maîtres explorateurs...) ;
    - **isis_login** : action d'autorisation des utilisateurs par login ;
    - **isis_quota** : action d'affichage des quotas ;
    - **gestion_index** : action d'entrée vers les gestions d'utilisateur, groupe, partage, appelle les actions gestion.
- Gestion des utilisateurs
    - **gestion_user_modify** : action de modification d'utilisateur ;
    - **gestion_user_create** : action de création d'utilisateur ;
    - **gestion_user_suppr** : action de suppression d'utilisateur.
- Gestion des partages
    - **gestion_share_create** : action de création de partage ;
    - **gestion_share_modify** : action de modification de partage ;
    - **gestion_share_suppr** : action de suppression de partage.
- Gestion des groupes
    - **gestion_group_create** : action de création de groupe ;
    - **gestion_group_modify** : action de modification de groupe ;
    - **gestion_group_suppr** : action de suppression de groupe.
- Autres actions
    - **gestion_account_suppr** : action de suppression forcée de compte ;
    - **extraction_aaf** : action pour l'extraction AAF ;
    - **bareos** : action programmation de sauvegarde ;
    - **bareos_config** : action de configuration de Bareos pour la sauvegarde ;
    - **scripts_admin** : action pour l'exécution de scripts d'administration ;

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

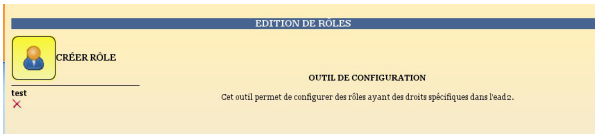
- **printers** : action de gestion des imprimantes.

Actions spécifiques au module Seshat

- Menu Messagerie
  - **routes** : gestion du routage des messages vers les établissements de l'Académie.

Modification et suppression de rôle via l'EAD

- Pour modifier un rôle, il suffit de cliquer sur le nom voulu ;
- pour le supprimer, cliquer sur la croix rouge associée.



Modification/suppression d'un rôle

1.4.10.c. Association des rôles

Les associations de rôle de l'EAD sont déclarées dans les fichiers : `/usr/share/ead2/backend/config/roles/roles_*.ini`

Ces fichiers au format INI[p.504] permettent d'associer des rôles à un ou plusieurs utilisateurs.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/roles.ini` : associations de base (admin, eleve, prof, ...) ;
- `/usr/share/ead2/backend/config/roles_<module>.ini` : associations spécifiques au module installé (ex : `roles_scribe.ini`) ;
- `/usr/share/ead2/backend/config/roles_local.ini` : associations déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/roles_acad.ini` : associations déclarés au niveau académique (via Zéphir).

Syntaxe des fichiers

L'association d'un rôle se fait à partir du login d'un utilisateur système (section `[pam]`) ou de la valeur associée à un attribut ldap (section `[nom attribut]`) de l'annuaire utilisé pour l'authentification SSO sur l'EAD du module.

```
[pam]
scribe2=admin
[uid]
 jean.dupont=prof admin
```


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

```
[user groups]
minedu=admin_horus
```

La clé spéciale `[user groups]` permet d'attribuer un rôle à tous les membres d'un groupe déclaré dans l'annuaire LDAP.

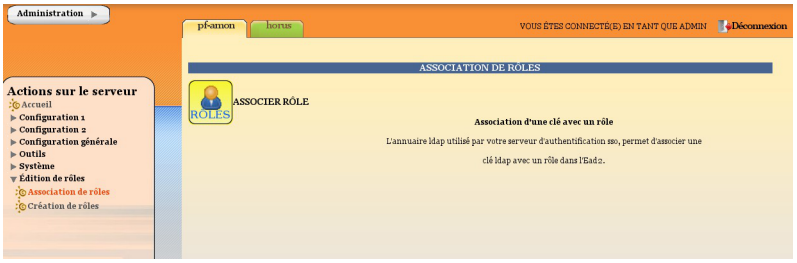
Création d'association via l'EAD

Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

Certaines de ces informations sont utilisées pour lui attribuer des rôles et ainsi lui donner accès à certaines actions.

Pour associer un rôle à des utilisateurs:

- dans `Édition des rôles/Association de rôle` ;
- cliquer sur `Associer Rôle`.



La fenêtre d'association de rôles

- choisir la clef (attribut de l'utilisateur) ;
- renseigner la valeur recherchée pour cet attribut (dans le cas d'une authentification locale on mettra le login de l'utilisateur) ;
- choisir le rôle à associer ;
- valider.



Association d'un rôle

L'intitulé de la clef dépend du système d'authentification utilisé pour se connecter :

Authentification locale :

- le login de l'utilisateur.

Authentification SSO :

- l'élève fait partie de la classe ;
- la valeur de la clé LDAP typeadmin :
  - 0 → enseignant
  - 1 → administrateur
  - 2 → enseignant responsable de classe
  - 3 → personnel administratif

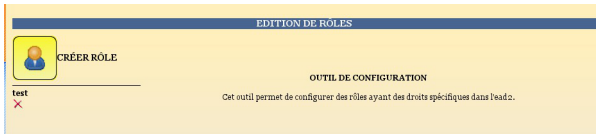
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.

Il est indispensable de redémarrer le service ead-server dans `Système->Services (mode expert)` pour que les modifications soient prises en compte.

Suppression d'une association via l'EAD

Une association de rôle peut par la suite être supprimée en cliquant sur la croix rouge.



Modification/suppression d'un rôle

1.4.10.d. Les rôles sur le module Scribe

L'EAD est accessible :

- en authentification locale aux utilisateurs *root* et *eole* ;
- en authentification SSO au compte *admin* ainsi qu'à tous les *personnels enseignant et administratif*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module Scribe, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions comme par exemples : redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc (valeur de l'attribut LDAP `uid` → admin et comptes locaux root et eole);
- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS (valeur de l'attribut LDAP `typeadmin` → 0) ;
- responsable de classe : en plus des actions "professeur", il peut ré-initialiser le mot de passe des élèves des classes dont il est responsable (valeur de l'attribut LDAP `typeadmin` → 2). Attention, le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable (pour cela il doit être ajouté à l'équipe pédagogique) ;
- personnel administratif : modification des préférences personnelles, gestion des files d'impression CUPS (membres du groupe administratifs).



Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

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

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

Fonctionnalités Scribe

L'EAD du module Scribe, dans son mode le plus complet, présente les fonctionnalités suivantes :

- distribution de devoirs et de documents ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/SIECLE/AAF/ONDES ;
- gestion des ACL ;
- gestion des quotas disque ;
- gestion des listes de diffusion ;
- test de la bande passante du serveur ;
- modification du mode de visualisation des postes élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Professeur"

Un enseignant dispose d'actions lui permettant de :

- configurer ses préférences personnelles ;
- distribuer des documents ;
- gérer les imprimantes.

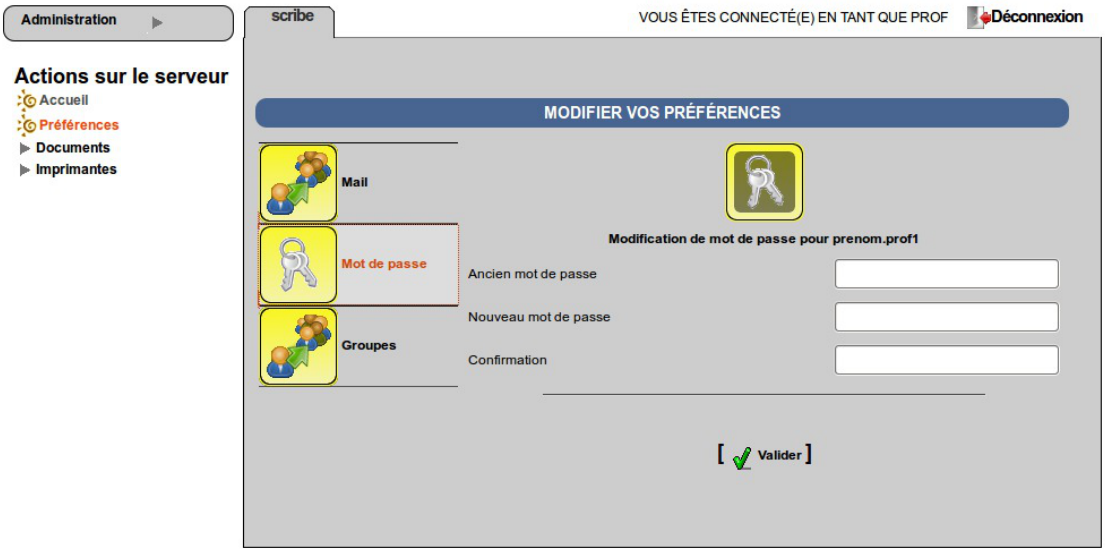


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

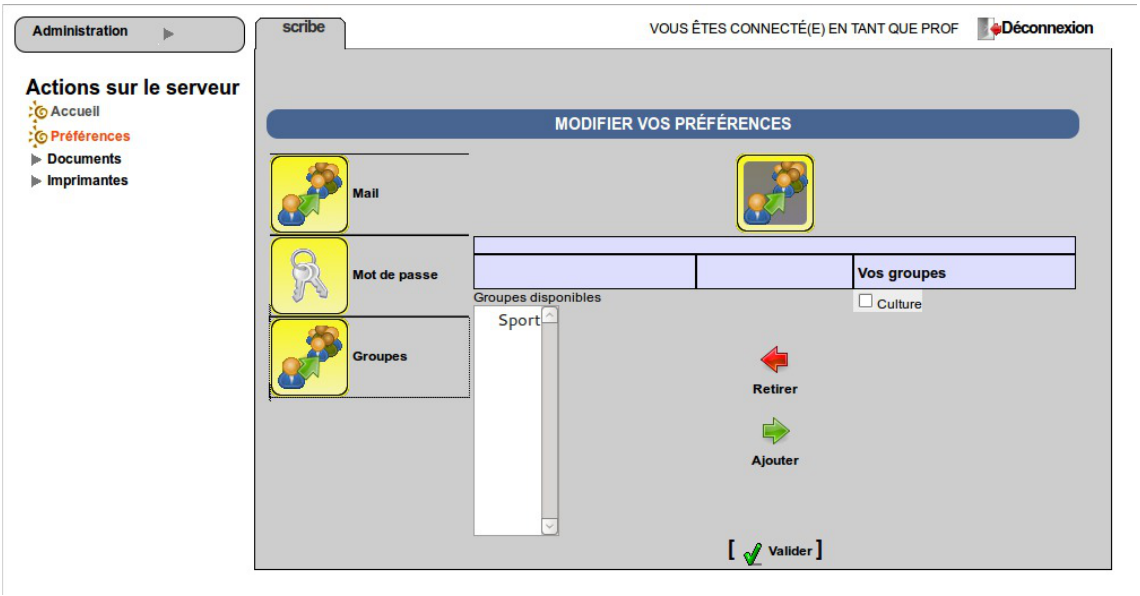
- modifier son mot de passe ;

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



EAD vue enseignant avec thème Envole, changement de mot de passe

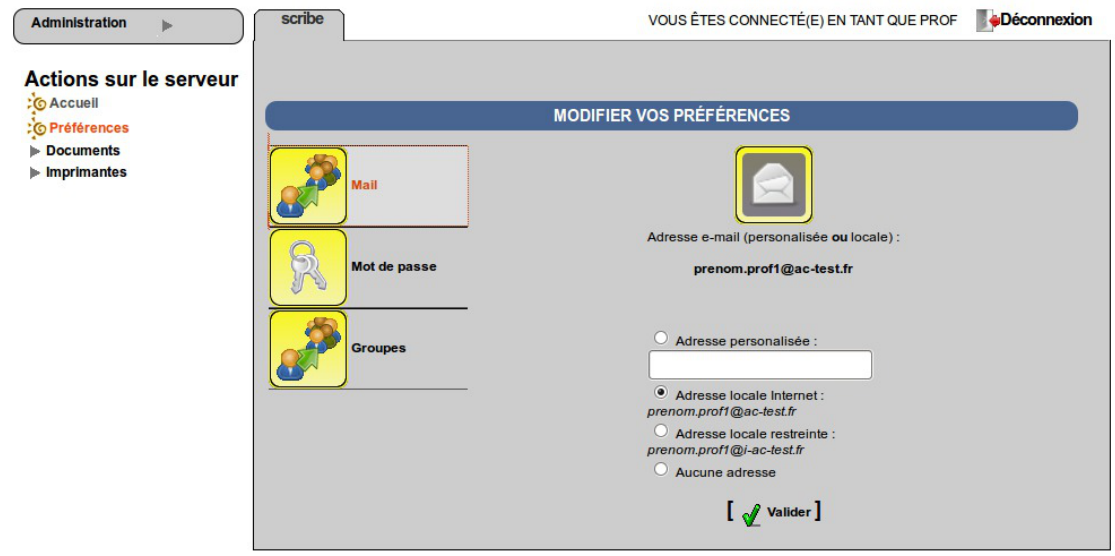
- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.

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



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

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

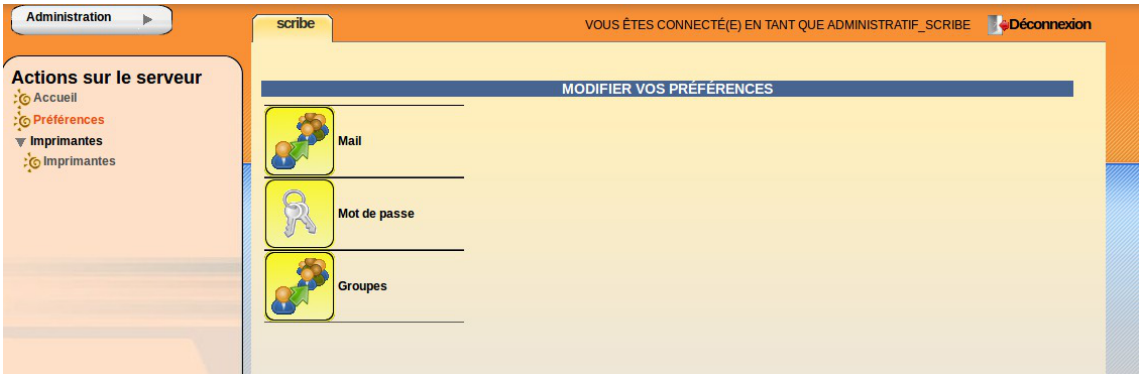
Un professeur peut être responsable de plusieurs classes.

Une classe peut se voir affecter plusieurs responsables.

Le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable, pour cela il doit être ajouté à l'équipe pédagogique.

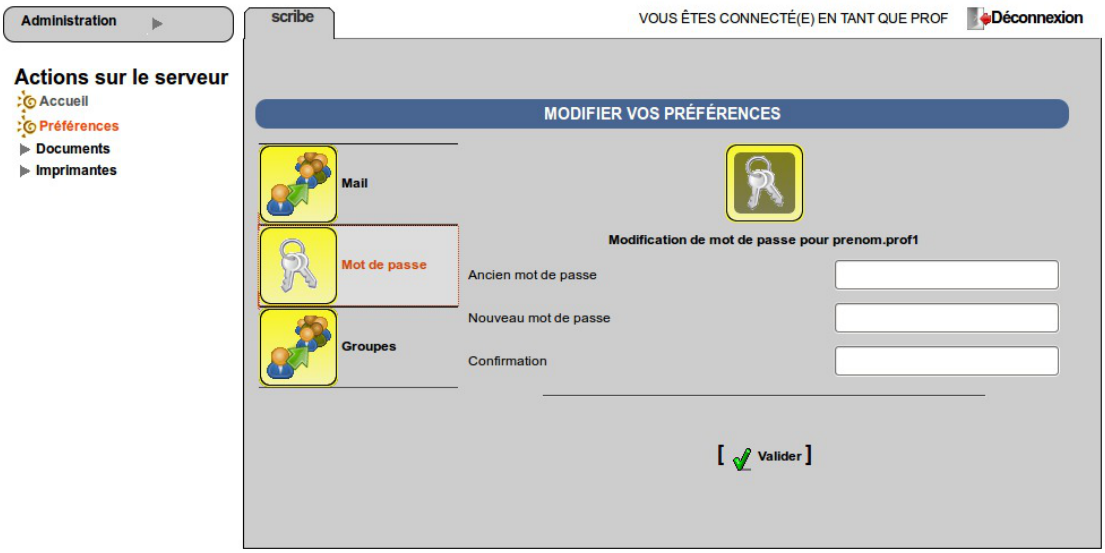
Accès "Administratif du Scribe"

Les personnels administratifs possédant un compte sur le module ont accès à leurs préférences personnelles et à la gestion des imprimantes.



L'item *Préférences* permet à un utilisateur de :

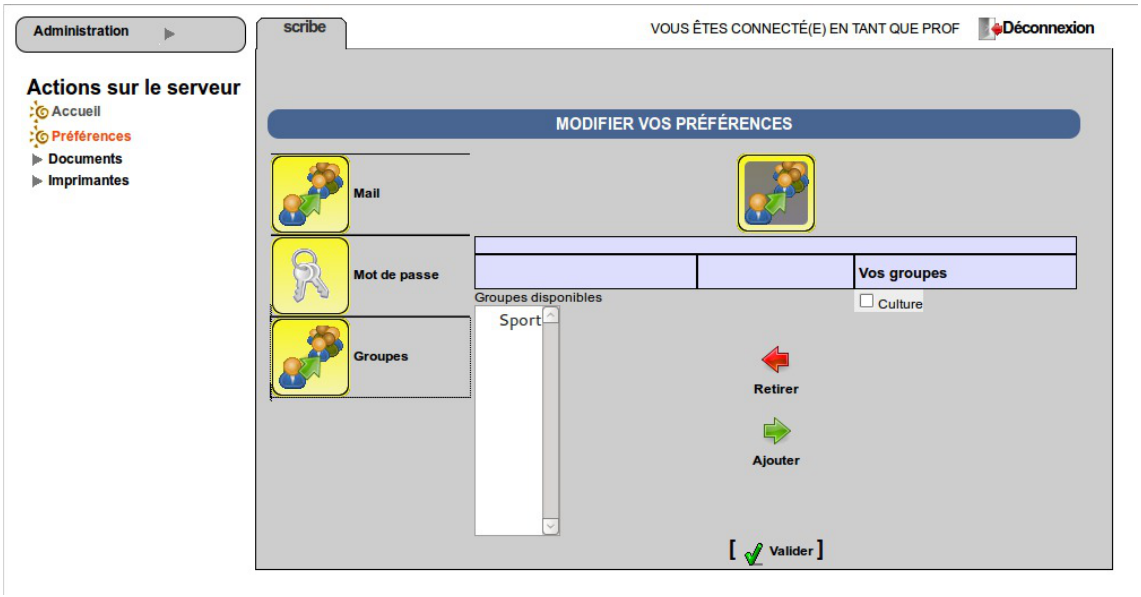
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

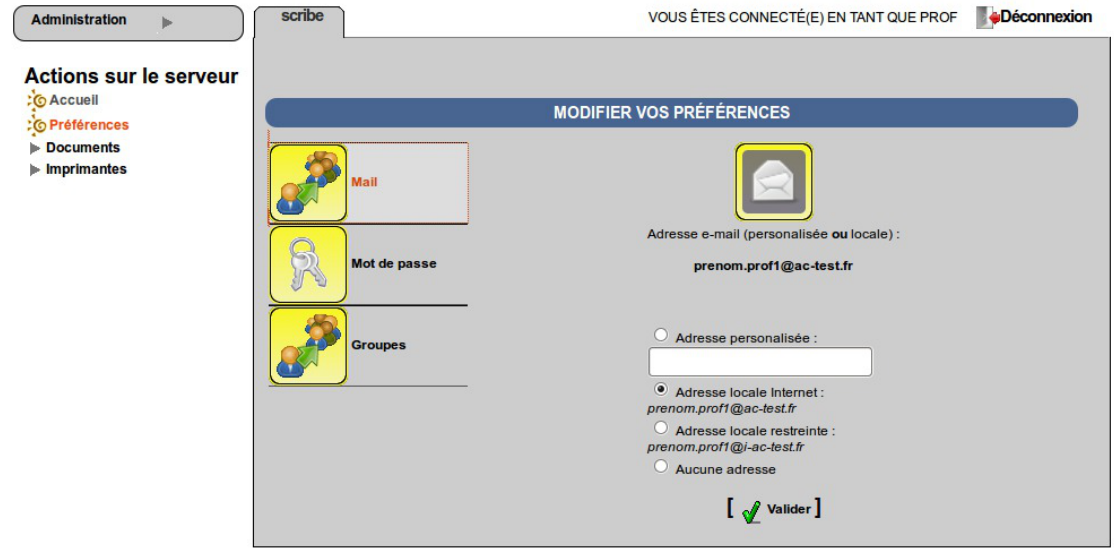
- s'inscrire/se désinscrire d'un groupe ;

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



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

1.4.10.e. Les rôles sur le module Amon

L'EAD est accessible aux utilisateurs locaux *root* et *eole.*

Si l'authentification SSO est configurée, il est également accessible à l'utilisateur *admin*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module Amon, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;

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

- administrateur du réseau pédagogique (utilisé sur le module Amon).

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

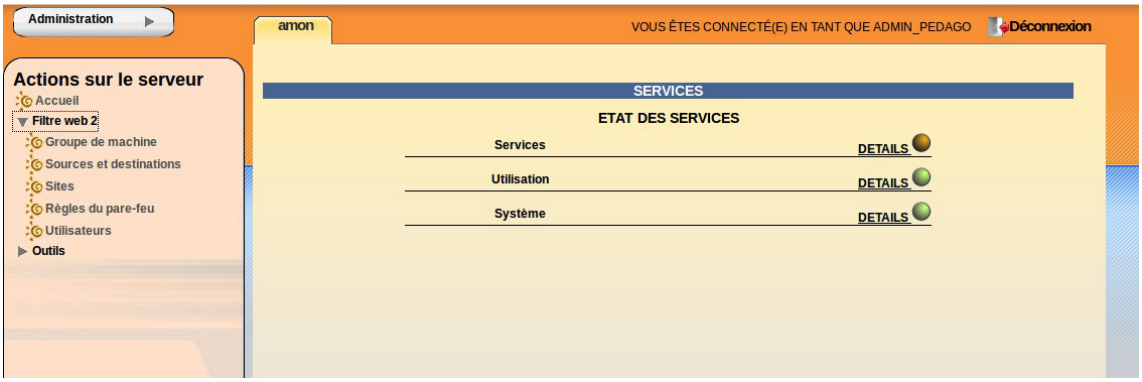
Fonctionnalités Amon

L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques du proxy ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Administrateur du réseau pédago"

Dans le cas où plusieurs filtres web (instances de e2guardian) sont configurés, ce rôle permet de déléguer la gestion des options de filtrage pour le filtre n°2, traditionnellement associé à la zone pédagogique.



1.4.10.f. Les rôles sur le module AmonEcole

L'EAD est accessible :

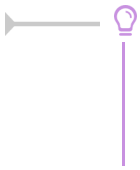
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- en authentification locale aux utilisateurs *root* et *eole* ;
- en authentification SSO au compte *admin* ainsi qu'à tous les *personnels enseignant et administratif*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module AmonEcole, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS ;
- responsable de classe : en plus des actions "professeur", peut ré-initialiser le mot de passe des élèves des classes dont il est responsable ;
- administratif dans Scribe ;
- administrateur du Scribe ;
- administrateur de l'Amon.



Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

Accès "Professeur"

Un enseignant dispose d'actions lui permettant de :

- configurer ses préférences personnelles ;
- distribuer des documents ;
- gérer les imprimantes.

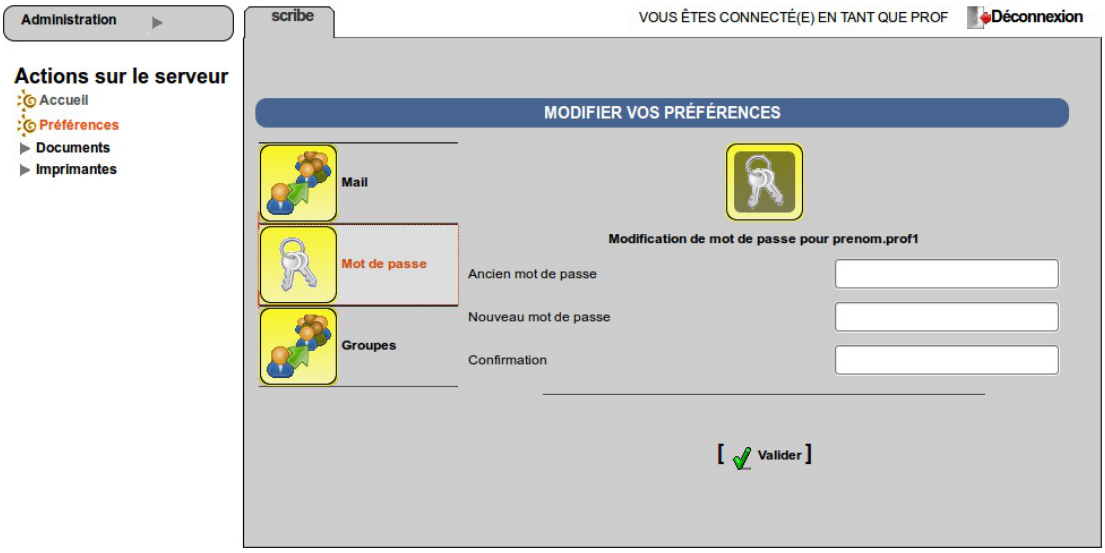


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

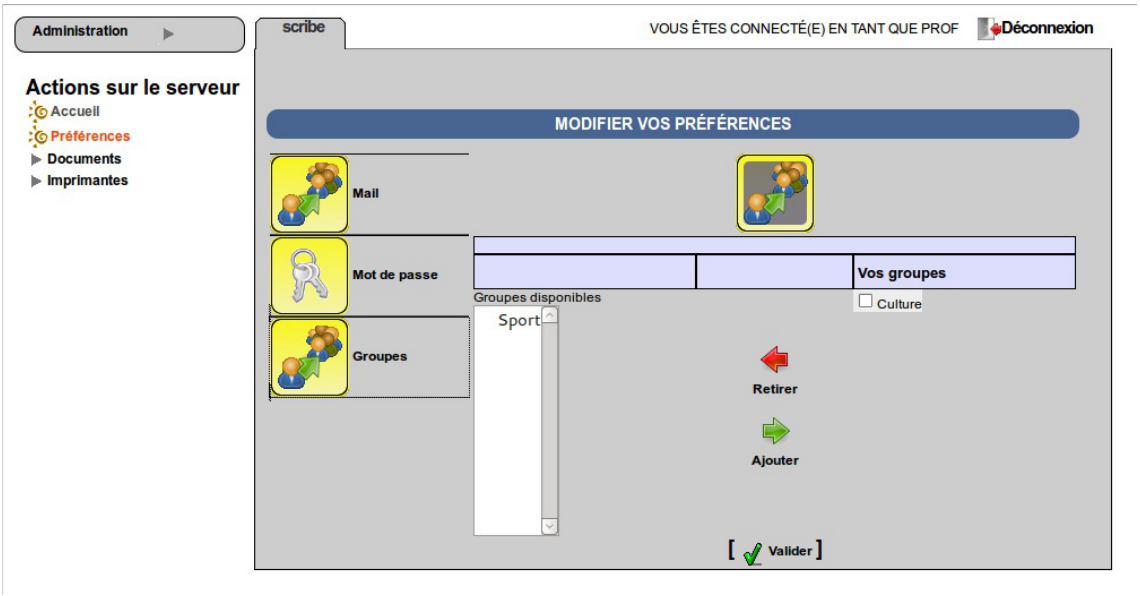
- modifier son mot de passe ;

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



EAD vue enseignant avec thème Envole, changement de mot de passe

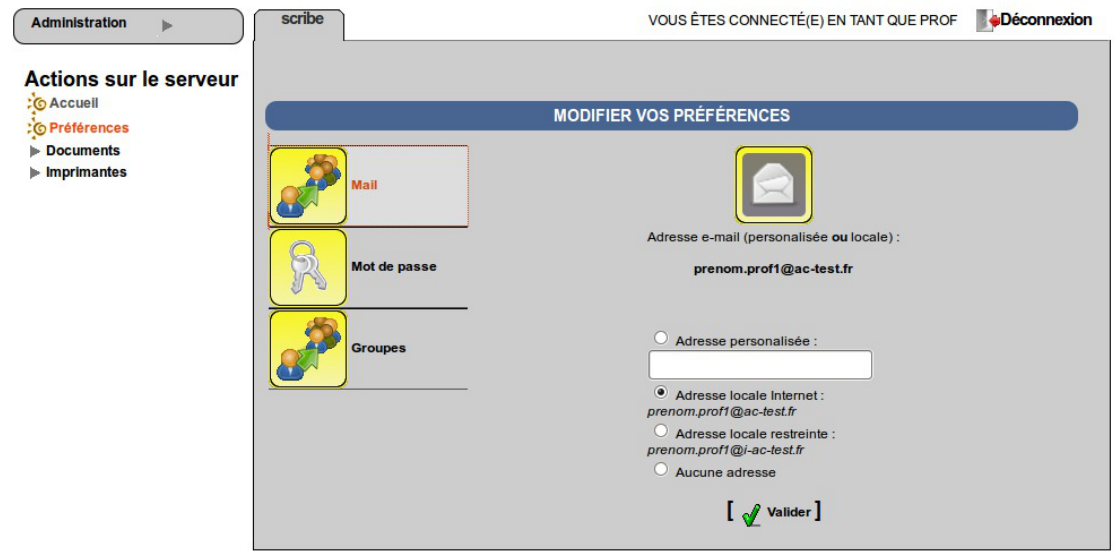
- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.

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



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

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

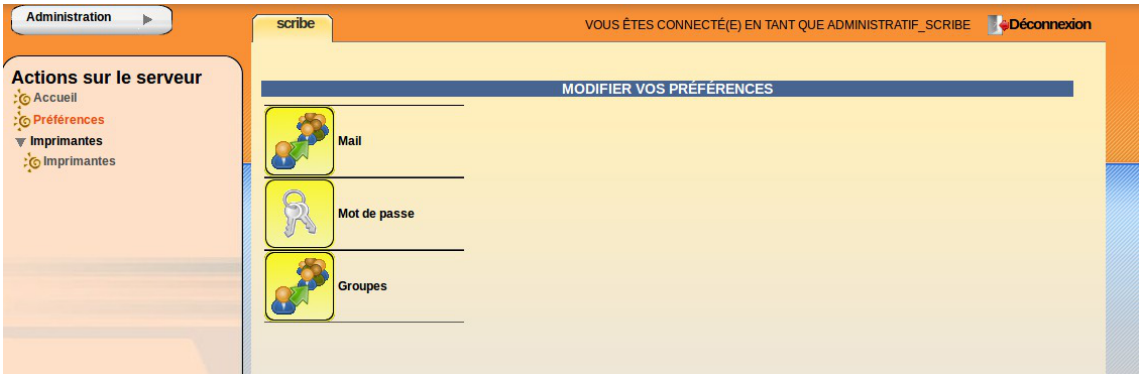
Un professeur peut être responsable de plusieurs classes.

Une classe peut se voir affecter plusieurs responsables.

Le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable, pour cela il doit être ajouté à l'équipe pédagogique.

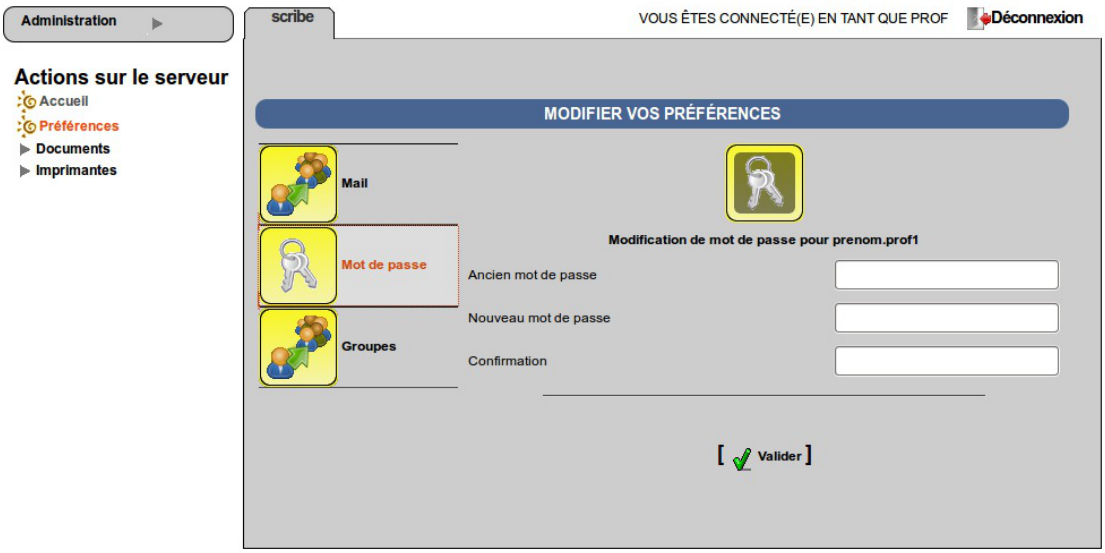
Accès "Administratif du Scribe"

Les personnels administratifs possédant un compte sur le module ont accès à leurs préférences personnelles et à la gestion des imprimantes.



L'item *Préférences* permet à un utilisateur de :

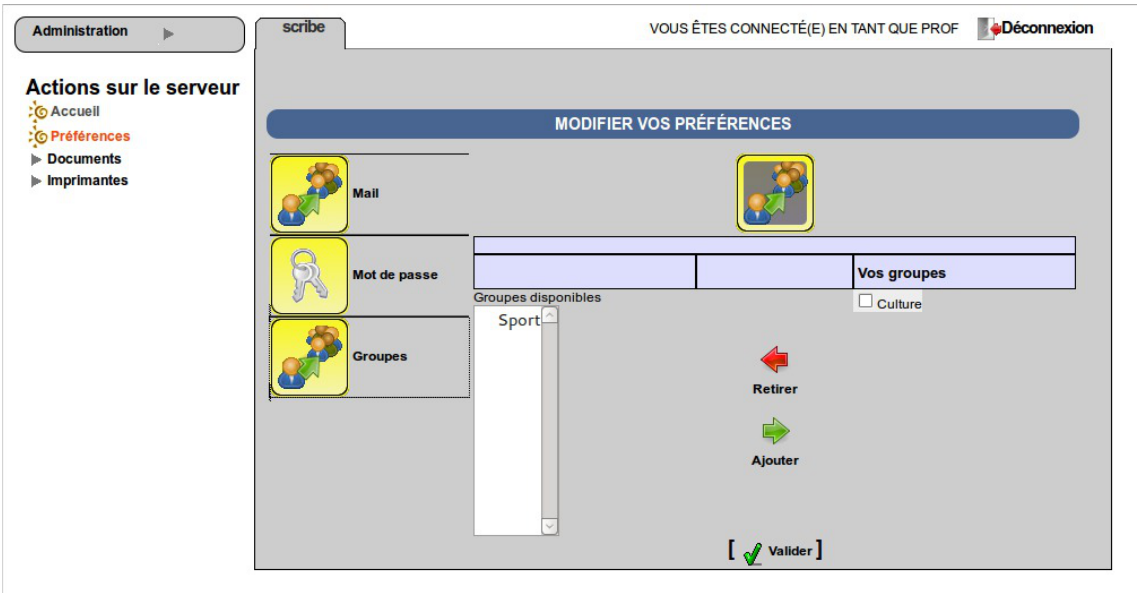
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

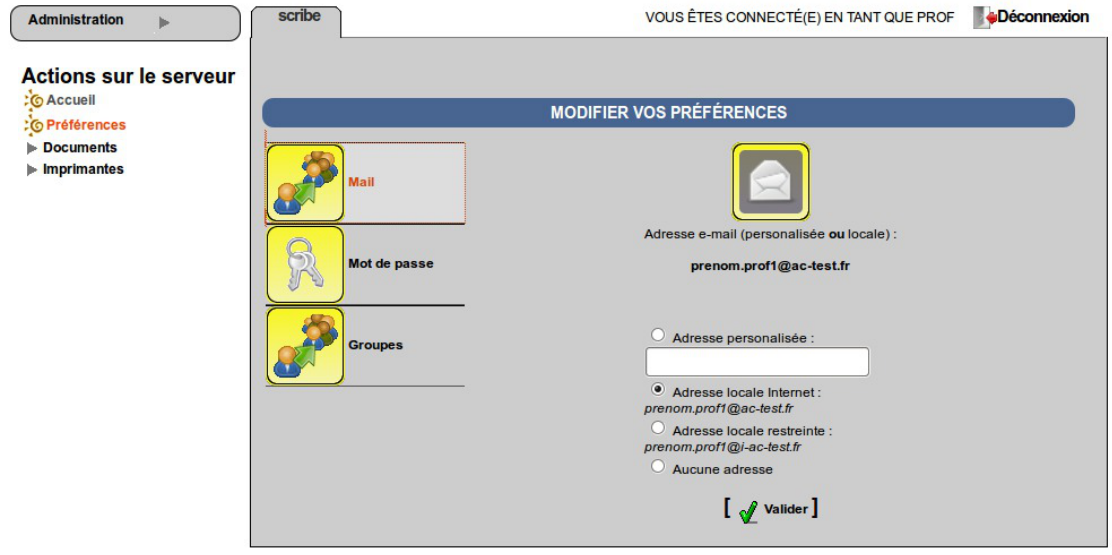
- s'inscrire/se désinscrire d'un groupe ;

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



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "Administrateur du Scribe"

Sur un module AmonEcole, le rôle "Administrateur du Scribe" (admin_scribe) permet de déléguer à un utilisateur les fonctionnalités EAD propres au module Scribe.

Fonctionnalités Scribe

L'EAD du module Scribe, dans son mode le plus complet, présente les fonctionnalités suivantes :

- distribution de devoirs et de documents ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;

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

- importation CSV/SIECLE/AAF/ONDES ;
- gestion des ACL ;
- gestion des quotas disque ;
- gestion des listes de diffusion ;
- test de la bande passante du serveur ;
- modification du mode de visualisation des postes élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Administrateur de l'Amon"

Sur un module AmonEcole, le rôle "Administrateur de l'Amon" (admin_amon) permet de déléguer à un utilisateur les fonctionnalités EAD propres au module Amon.

Fonctionnalités Amon

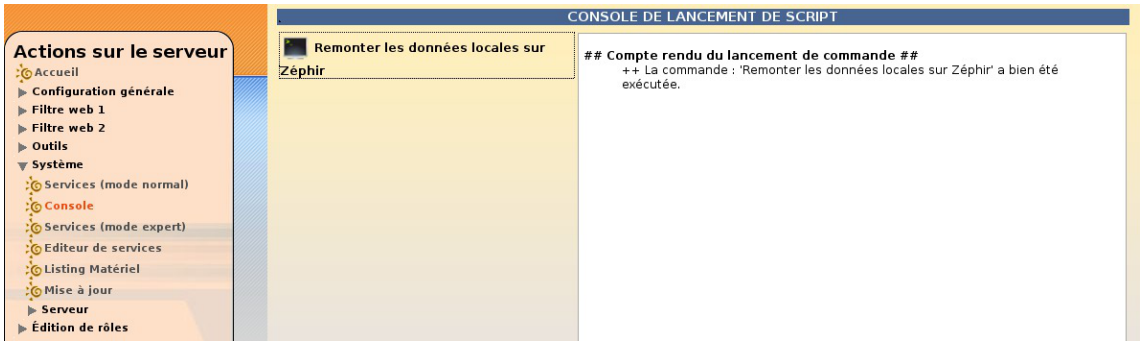
L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques du proxy ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

1.4.11. La console

Cette fonctionnalité permettra d'exécuter des actions et des scripts personnalisés directement dans l'EAD.

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



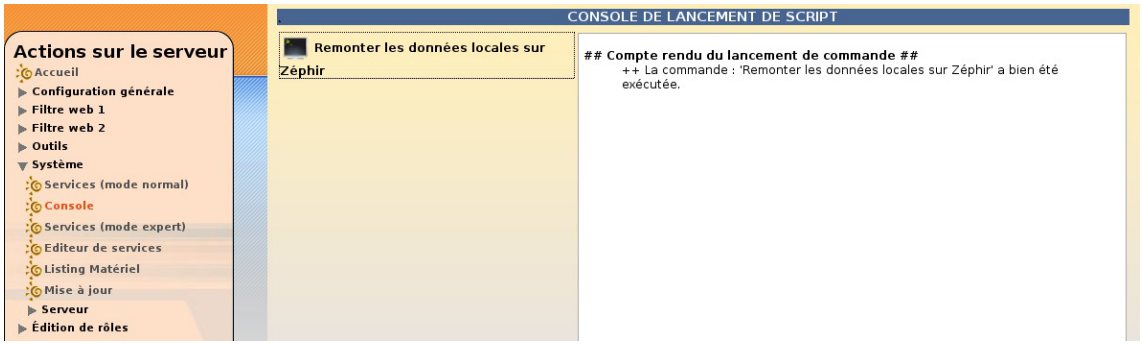
Remontée des données locales sur Zéphir par la console EAD

Seul le script Remonter les données locales sur Zéphir est fourni par défaut.

Cette fonctionnalité n'est pas stabilisée. De plus, les actions et scripts personnalisés seront supprimés à la prochaine mise à jour.

Remonter les données locales sur Zéphir

Cette action permet de déclencher la remontée des données sur le Zéphir (appel de la commande : `zephir_client save_files 3`).



Remontée des données locales sur Zéphir par la console EAD

Écrire des scripts personnalisés

Copier avec un nouveau nom le script existant :

```
# cp /usr/share/ead2/backend/actions/cmd_update_zephir.py /usr/share/ead2/backend/actions/cmd_df.py
```

Éditer le script et renommer la classe, le nom du script, la commande à exécuter et le libellé de la commande :

```
# vim /usr/share/ead2/backend/actions/cmd_df.py
```

```
1  # -*- coding: UTF-8 -*-
2  from ead2.backend.actions.lib.main import Cmd
3
4  class Cmd_Df(Cmd): # renommer la classe
5      """
6      Action du mode commande
7      """
8      name = "cmd_df" # nom du script
9      # propriété de la commande à exécuter
10     cmd_template = "df -h"
```


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

```
11    cmd_libelle = "Occupation disque" # libellé du script dans l'EAD
```

Ajouter le nom du nouveau script au fichier `zstats.cmd` :

```
# vim /usr/share/ead2/backend/config/cmds/zstats.cmd
```

ou

```
# echo "cmd_df" >> /usr/share/ead2/backend/config/cmds/zstats.cmd
```

Déclarer le nouveau script dans le fichier `actions_zstats.cfg` :

```
# vim /usr/share/ead2/backend/config/actions/actions_zstats.cfg
```

ou

```
# echo "cmd_df" >> /usr/share/ead2/backend/config/actions/actions_zstats.cfg
```

Ajouter les droits d'utilisation du script dans le fichier `perm_zstats.ini` :

```
# vim /usr/share/ead2/backend/config/perms/perm_zstats.ini
```

ou

```
# echo "cmd_df=admin" >> /usr/share/ead2/backend/config/perms/perm_zstats.ini
```

Relancer le service :

```
# service ead-server restart
```

L'action est accessible dans le menu de l'EAD. Lorsque la commande réussi un message s'affiche :

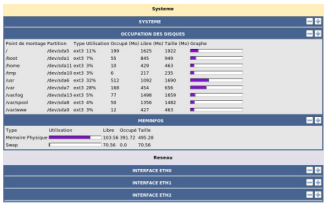
```
++ La commande : 'Occupation disque' a bien été exécutée.
```

Cliquer sur `Afficher le contenu reçu` permet d'afficher le résultat de la commande.

1.4.12. Listing matériel

Le listing matériel permet de visualiser les éléments matériels du serveur.

Il indique notamment l'occupation des disques, de la mémoire vive et de la partition swap.



Listing matériel (lshw)

La mémoire physique (RAM)

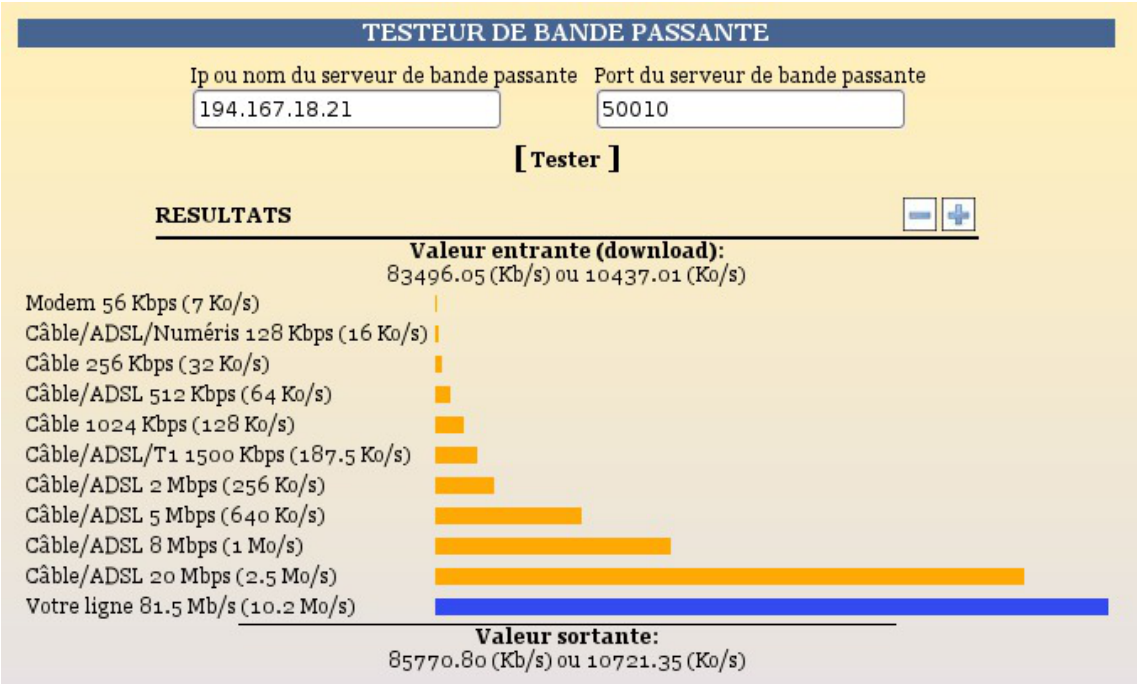
Le noyau Linux[p.506] utilise un système de cache mémoire pour limiter les accès disque. Le chiffre "mémoire physique" comprend ce cache. Cela signifie qu'il n'est pas inquiétant de voir une valeur proche de 100%.

Le critère important étant l'occupation le swap (mémoire virtuelle). Une utilisation du swap indique que le serveur manque de RAM. Il faut alors envisager d'en augmenter la quantité ou chercher à alléger la charge de la machine.

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

1.4.13. Bande passante

Le menu Outils/Bande passante permet de tester la bande passante dont dispose le serveur.



Testeur de bande passante

1.4.14. Résoudre des dysfonctionnements liés à l'EAD

Services et journaux

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.

Problème d'accès à l'EAD avec un nom de domaine incorrect

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

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.

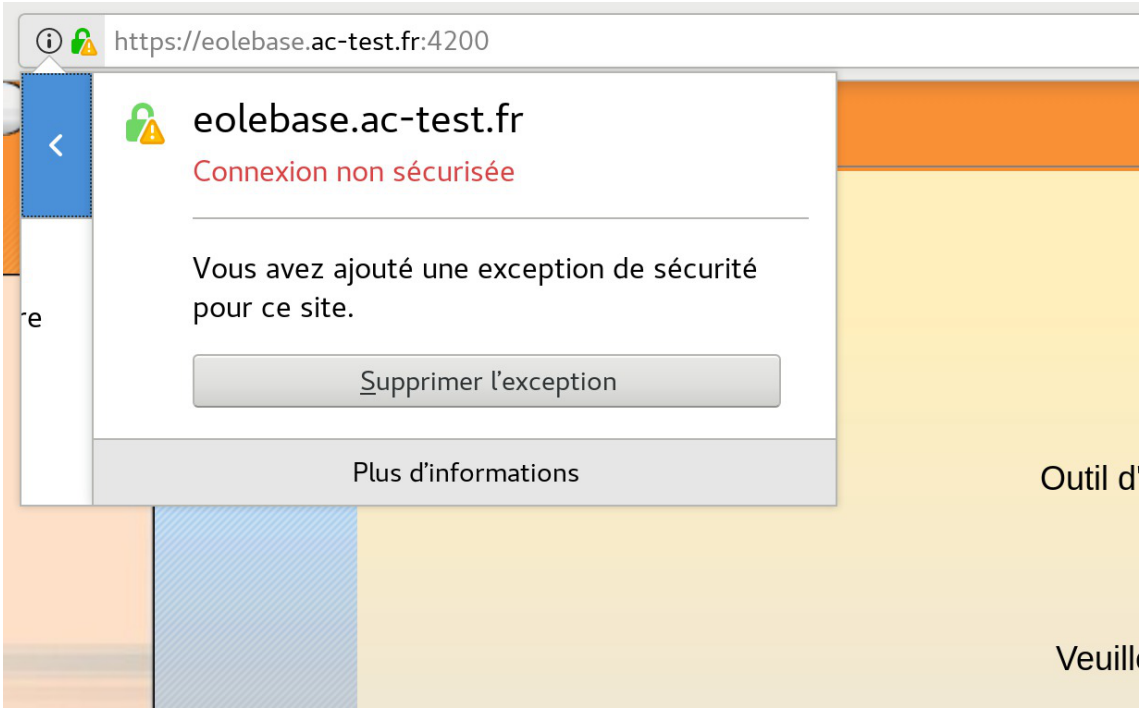
Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

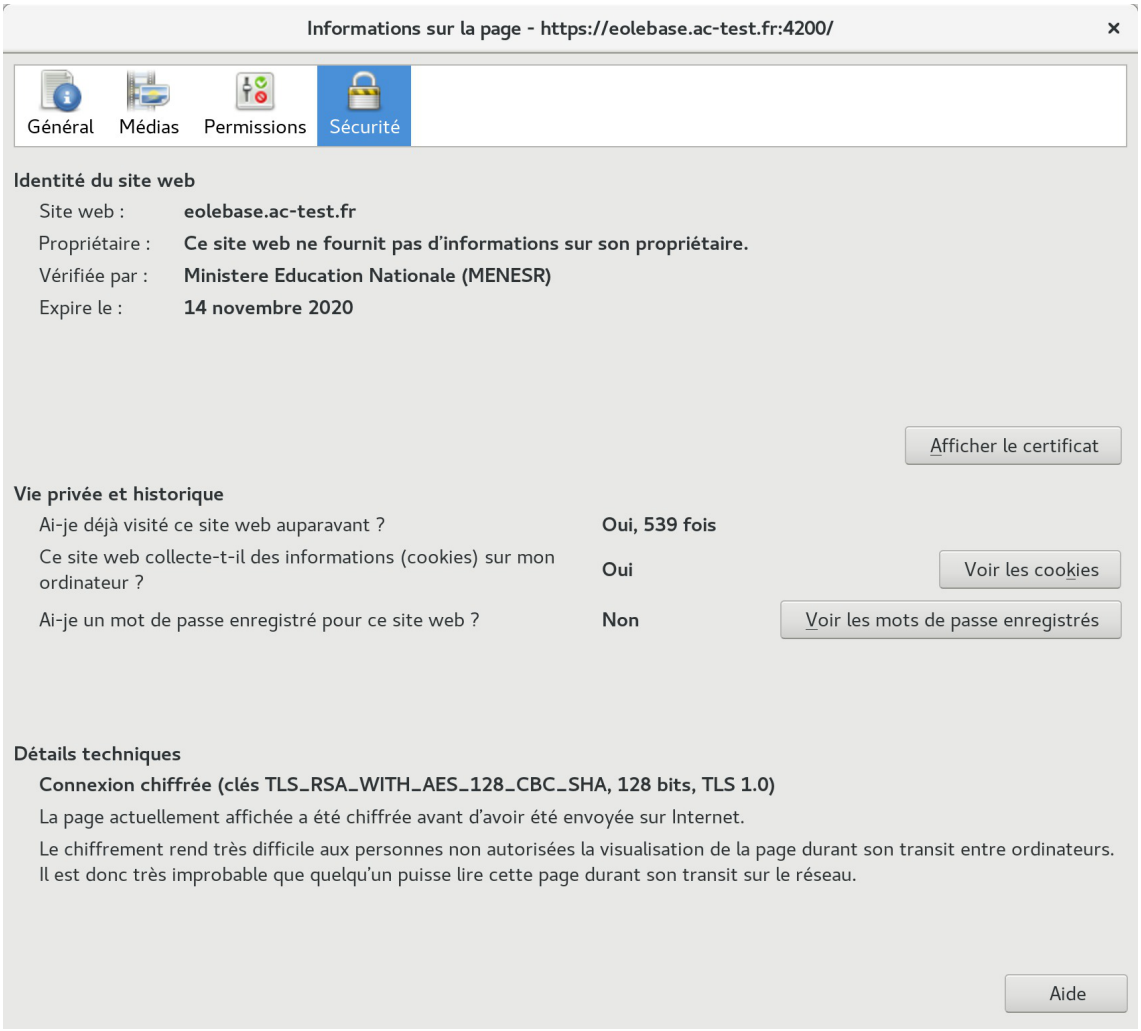


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion



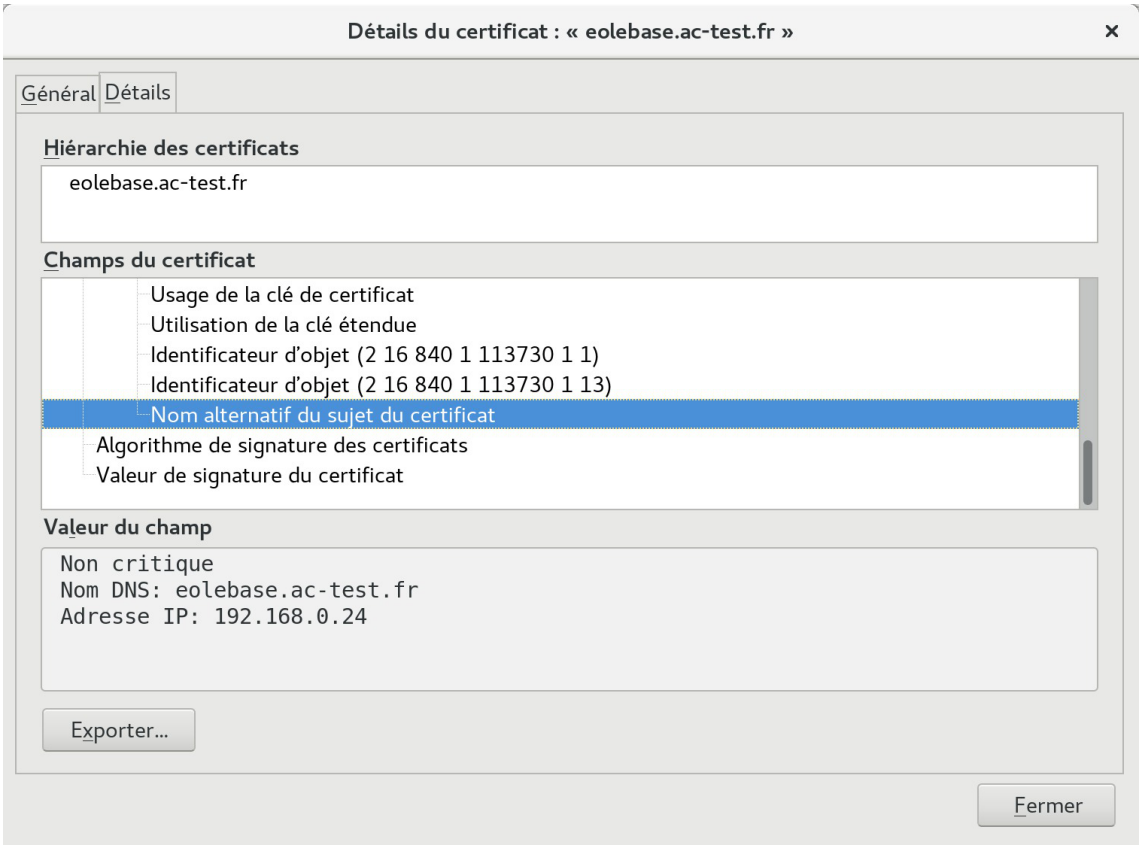
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`

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



- 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 sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.

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



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).

```
# reconfigure
# /usr/share/creole/gen_certif.py -f
```

ou `#`

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

> `/usr/share/creole/gen_certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.
>
> `# reconfigure`

Clés d'enregistrement

Les interfaces associées au serveur de commandes local sont enregistrées dans le fichier `/usr/share/ead2/backend/config/frontend_keys.ini`

```
[keys]
127.0.0.1 = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Les serveurs de commandes associés à l'interface EAD locale sont enregistrés dans le fichier `/usr/share/ead2/frontend/config/servers.ini`

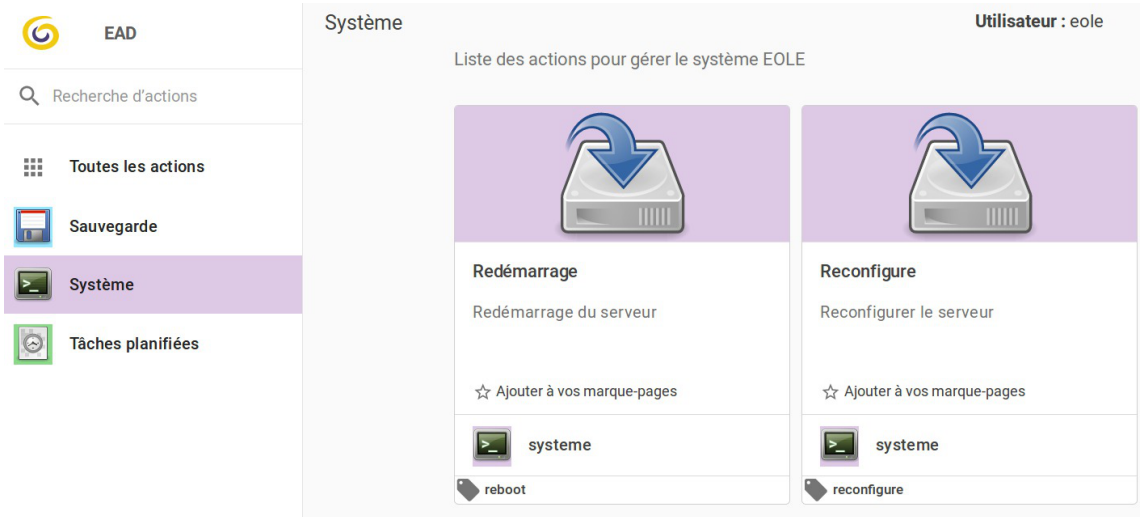
```
[1]
url = https://127.0.0.1
port = 4201
comment = amon
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Si nécessaire, il est possible de réinitialiser ces fichiers à l'aide des commandes suivantes :

```
1 echo '[keys]' > /usr/share/ead2/backend/config/frontend_keys.ini
2 echo '' > /usr/share/ead2/frontend/config/servers.ini
3 reconfigure
```

1.5. L'interface d'administration EAD 3

EOLE offre une nouvelle interface simplifiée de gestion du serveur : l'interface d'administration EAD 3.



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

Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

1.5.1. Présentation

L'EAD3 est préinstallé sur les modules à partir de la version EOLE 2.6.1, mais n'est pas activé.

1.5.2. Installation

Pour découvrir l'EAD3, il est possible d'installer un Eolebase au minimum en version 2.6.1 et de l'activer :

```
# CreoleSet activer_ead3 oui
```

Son activation nécessite la reconfiguration du serveur :

```
# reconfigure
```

1.5.3. L'application web

Pour accéder à l'application EAD3 il faut utiliser l'URL suivante : https://<serveur>/ead/

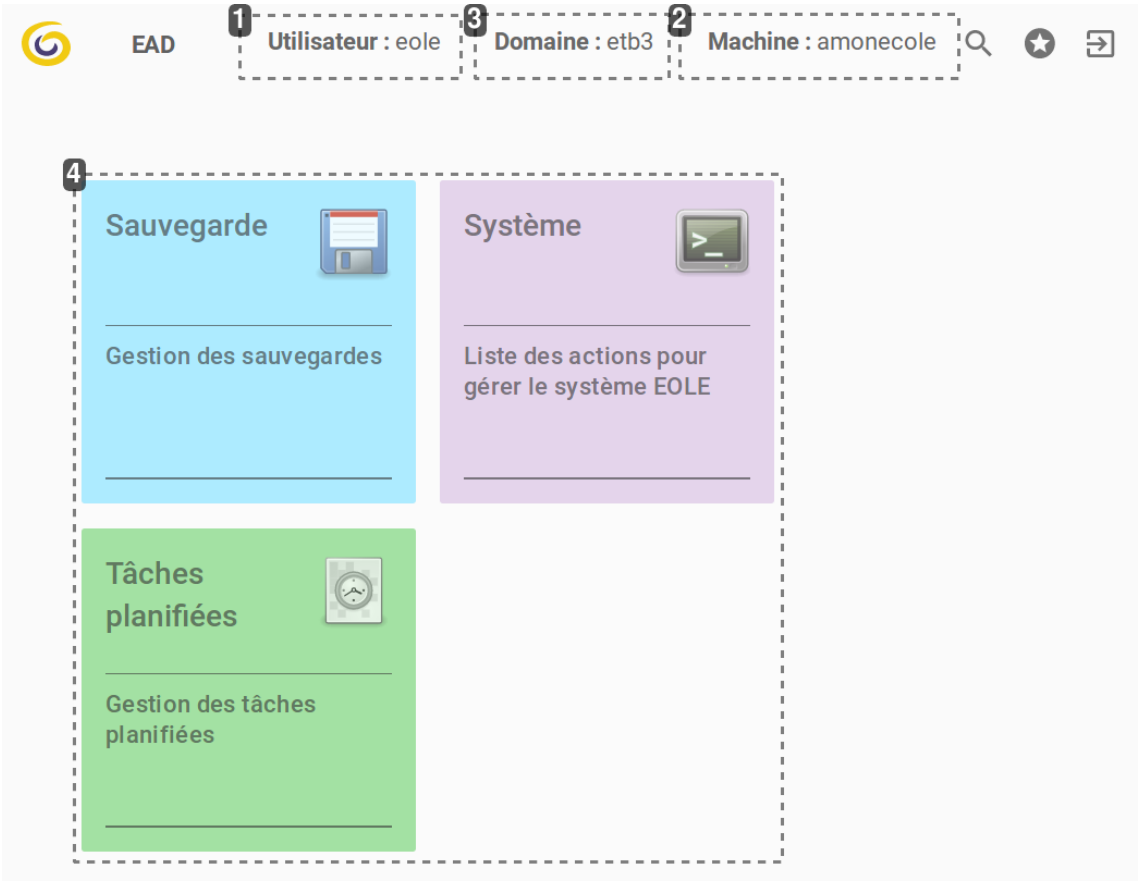
Une mire d'authentification apparaît. Saisir le compte et la clé secrète associée.

Pour le moment l'authentification est réalisée avec PAM[p.512], vous pouvez par exemple utiliser le compte `eole` et le mot de passe défini à l'instanciation du module ou créer un autre compte.

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

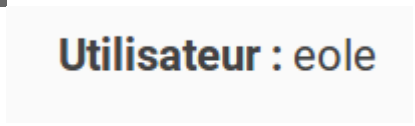


Description des éléments de la page principale



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

1



Compte connecté

2



Nom de machine du serveur que l'application administre.

3



Nom de domaine du serveur que l'application administre.

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

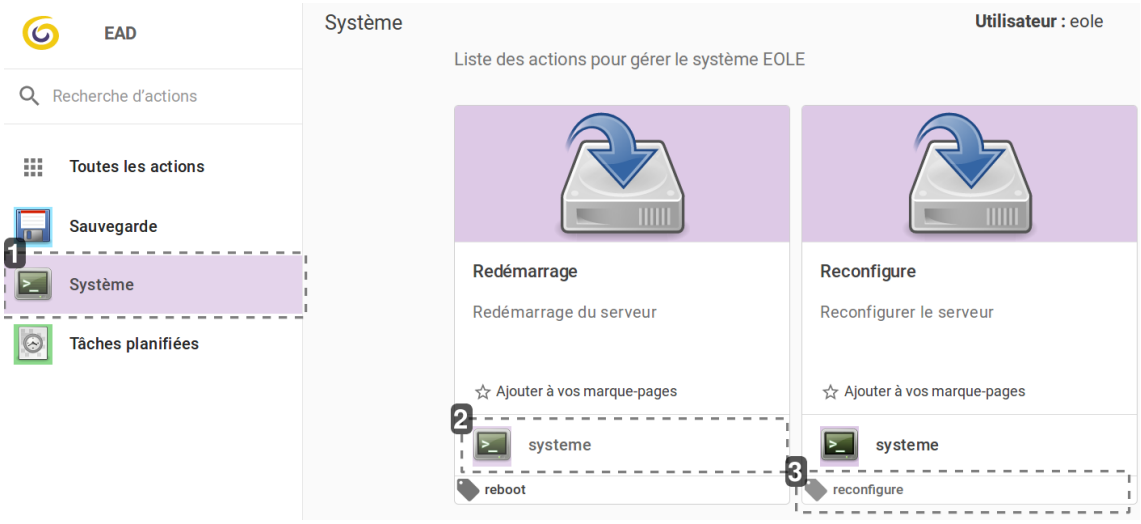
4



Catégories d'actions (exemple : sauvegarde, système…)

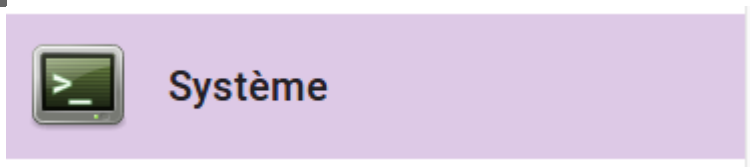
Cliquer sur une catégorie particulière permet d'afficher une vue propre à la catégorie.

Description de la vue par catégorie



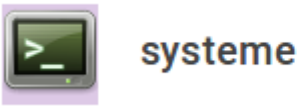
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1



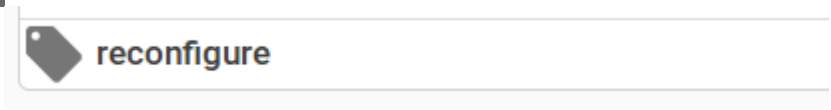
La catégorie choisie est en surbrillance.

2



Chaque action appartient à une catégorie.

3



Les étiquettes ne sont pas liées à une catégorie, elles déterminent un ensemble d'actions.

1.5.4. Généralités sur les actions

Une action est une fonctionnalité de l'EAD3 permettant de réaliser un ou plusieurs traitements sur un ou plusieurs serveurs cibles.

Une action est construite à partir de deux éléments :

- un fichier XML Creole[p.498] permettant de décrire l'action et de définir les variables et/ou les configurations nécessaires pour construire l'interface web ;
- un fichier de recette SaltStack[p.516] (nommé States) permettant d'effectuer l'action demandée sur les serveurs cibles.

Ces fichiers sont stockés sur le serveur dans le répertoire `/usr/share/eole/creole/extra/`.

Un sous-répertoire correspond à une action et son nom est le nom de l'action.

Par exemple, l'action *majreport* est définie à la création du répertoire enfant `/usr/share/eole/creole/extra/majreport/` qui contient le XML Creole, et éventuellement une recette SaltStack.

Si une recette SaltStack est associée à l'action, elle doit obligatoirement être placée dans le répertoire enfant `sls/` de l'action.

```
root@scribe:~# tree /usr/share/eole/creole/extra/backuponce
/usr/share/eole/creole/extra/backuponce
```


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

```
├── 00_action.xml
└── sls
    └── eole
        └── init.sls

2 directories, 2 files
root@scribe:~#
```

Dans les dossiers `sls` des actions déjà existantes, un sous-dossier `eole` est présent. Il contient les recettes SaltStack fournies par EOLE.

Plusieurs recettes SaltStack successives peuvent être appelées. Un fichier `init.sls` permet d'inclure toutes les recettes à appliquer dans un ordre spécifique.

Pour personnaliser le comportement d'une action existante il faut placer les recettes SaltStack directement dans le répertoire parent.

Par exemple pour surcharger le comportement des recettes EOLE de l'action *majonce* il faut placer les recettes personnalisées dans `/usr/share/eole/creole/extra/majonce/sls/`.

Les fichiers personnalisés des recettes SaltStack peuvent être templatisés avec Jinja2[p.505].

Dans ce cas, l'accès aux variables Creole se fait via les pillars[p.516].

Si l'on souhaite accéder à la variable Creole *hour* de la famille *mise_a_jour* de l'action *majonce*, il faut écrire dans la recette : *pillar['majonce.mise_a_jour.hour']*.

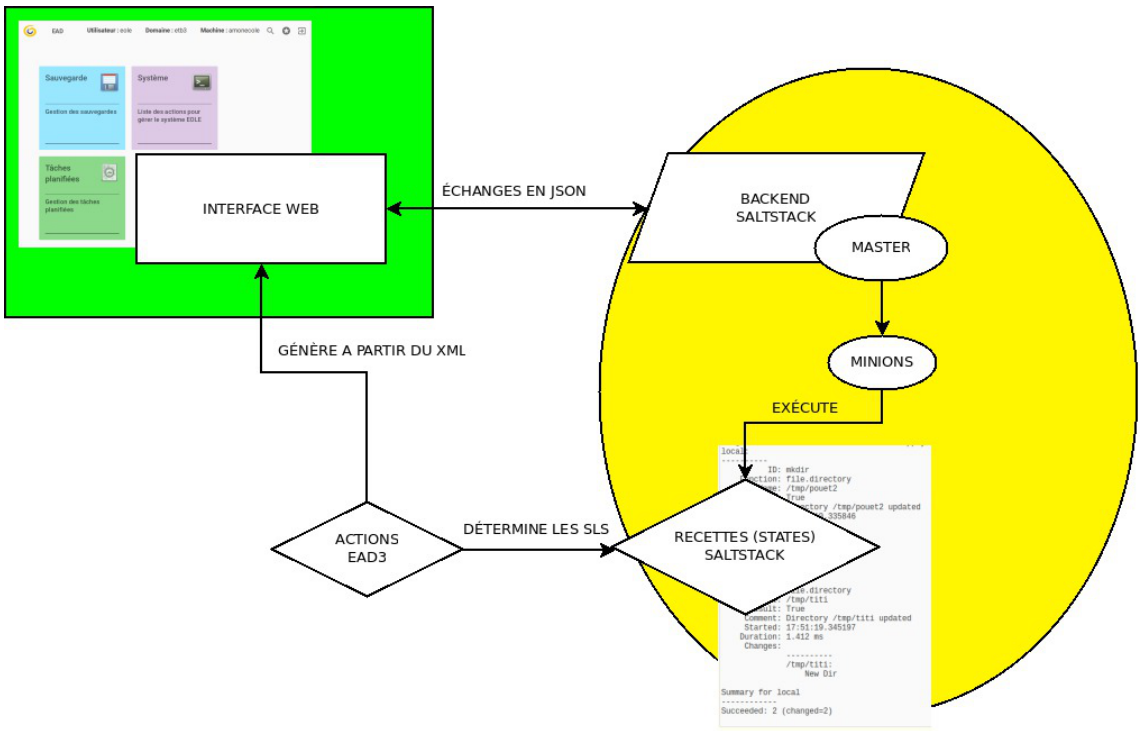


Diagramme de fonctionnement

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

```
<creole>
    <family_action name="Catégorie contenant une ou plusieurs actions">
        <action type="reader"
            title="Nom appraissant dans l'interface web"
            description="Description de l'action apparaissant dans l'interface web"
            image="icons/edit-find.svg">
            <profile>ead_admin</profile>
            <ewtapp>ead</ewtapp>
            <tag>étiquette1</tag>
            <tag>étiquette2</tag>
        </action>
    </family_action>

    <variables>
        <family name="options">
            <variable name="filename" type="filename">
        </family>
    </variables>
</creole>

```

Balises et variables qui permettent de définir l'interface pour une action de type formulaire :

- *<family_action>* : Cette balise est obligatoire, elle permet de définir la catégorie qui contient l'action (si on veut ranger l'action à créer dans une catégorie existante, il suffit de renseigner le nom de la catégorie, si on veut créer une nouvelle catégorie, il suffit de mettre un nouveau nom) ;
- *<action>* : Cette balise est obligatoire, elle définit l'action d'une manière générique ;

  type : Le type de l'action, exemple *reader* pour une action d'affichage, *form* pour une action de type formulaire, *custom* pour une action personnalisée ;

  title : Intitulé de l'action ;

  descriptif : Courte description de l'action ;

  image : Les icônes disponibles sont dans le répertoire : `/usr/share/ewt/static/images/icons/` ;
- <family name="options"><variable name="filename" type="filename"> : Permettent de définir les variables Creole nécessaires au bon fonctionnement de l'action ;
- *<ewtapp>* : Applications dans lesquelles l'action doit apparaître (une balise par application), ici seulement l'EAD ;
- *<profile>* : L'action n'est accessible que pour le profil *ead_admin* ou un profil équivalent ou supérieur ;
- *<tag>* : Permet de déclarer une ou plusieurs étiquettes dans l'interface EAD.

Il est possible, comme dans n'importe quel XML Creole, de mettre en place des contrôles et des conditions sur les variables déclarées.

1.5.5. Créer une nouvelle action

Pour créer une nouvelle action il est possible de prendre modèle sur une action existante :

```
# cp -R /usr/share/eole/creole/extra/majreport/00_action.xml
```


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

`/usr/share/eole/creole/extra/test/00_action.xml`

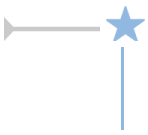
À gauche la copie de l'action de droite

```
<creole>
<creole>
    <family_action name="Test"
     <family_action name="Mise à jour"
                   description="Test"
                    description="Gestion de la mise à jour"
                   color="#0000dd"
                    color="#fca474"
                   image="icons/mail-attachment.svg">
                    image="icons/applications-internet.svg">
    <action type="reader"
     <action type="reader"
           title="Test de lecture"
            title="Rapport de mise à jour"
           description="Afficher le contenu d'un fichier"
            description="Afficher le journal de la dernière mise à jour"
           image="icons/face-angel.svg">
            image="icons/edit-find.svg">
           <profile>ead_admin</profile>
            <profile>ead_admin</profile>
           <ewtapp>ead</ewtapp>
            <ewtapp>ead</ewtapp>
           <tag>lecture</tag>
            <tag>log</tag>
           <tag>fichier</tag>
            <tag>maj</tag>
           <tag>test</tag>
            <tag>maj-auto</tag>
       </action>
            <tag>mise à jour</tag>
    </family_action>
        </action>
    <variables>
     </family_action>
        <family name="options"
     <variables>
                description="Contenu du fichier  ">
        <family name="options"
           <variable name="filename" type="filename">
                description="Dernière mise à jour">
               <value>/usr/share/eole/creole/extra/test/00_action.xml
</value>            <variable name="filename" type="filename">
           </variable>
                <value>/var/lib/eole/reports/rapport-maj.log</value>
           <variable name="language" type="string">
            </variable>
              <value>prolog</value>
            <variable name="language" type="string">
           </variable>
                <value>prolog</value>
       </family>
            </variable>
    </variables>
         </family>
    <constraints>
     </variables>
    </constraints>
     <constraints>
    <help/>
     </constraints>
</creole>
     <help/>

</creole>
```


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

Pour que la nouvelle action soit prise en compte il faut reconfigurer le serveur à l'aide de la commande `reconfigure` ou appliquer les commandes suivantes :

```
# /usr/share/eole/postservice/00-actions reconfigure
# CreoleCat -t ext_auth.conf
# service salt-api restart
```



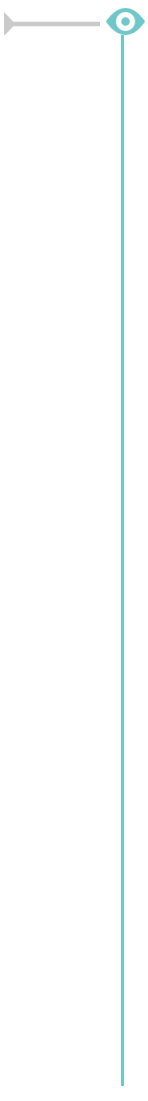
Dans un cas comme dans l'autre il est préférable de se déconnecter et se reconnecter à l'EAD.

Pour supprimer une action :

```
# rm -r /usr/share/eole/creole/extra/test/
# reconfigure
```

1.5.6. Type d'actions

1.5.6.a. Les actions d'affichage



```
<creole>
    <family_action name="Tâches planifiées">
        <action type="reader"
        title="Rapport de mise à jour"
        description="Visualisation du fichier de log de MajAuto"
        image="icons/edit-find.svg">
        <profile>ead_admin</profile>
        <ewtapp>ead</ewtapp>
        <tag>log</tag>
        <tag>maj</tag>
        <tag>maj-auto</tag>
        <tag>mise à jour</tag>
        </action>
    </family_action>

    <variables>
        <family name="options">
        <variable name="filename" type="filename">
        <value>/var/lib/eole/reports/rapport-maj.log</value>
        </variable>
        <variable name="language" type="string">
        <value>prolog</value>
        </variable>
        </family>
    </variables>

<constraints>
</constraints>

<help/>

</creole>
```


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

33

Balises et variables qui permettent de définir l'interface pour une action de type affichage :

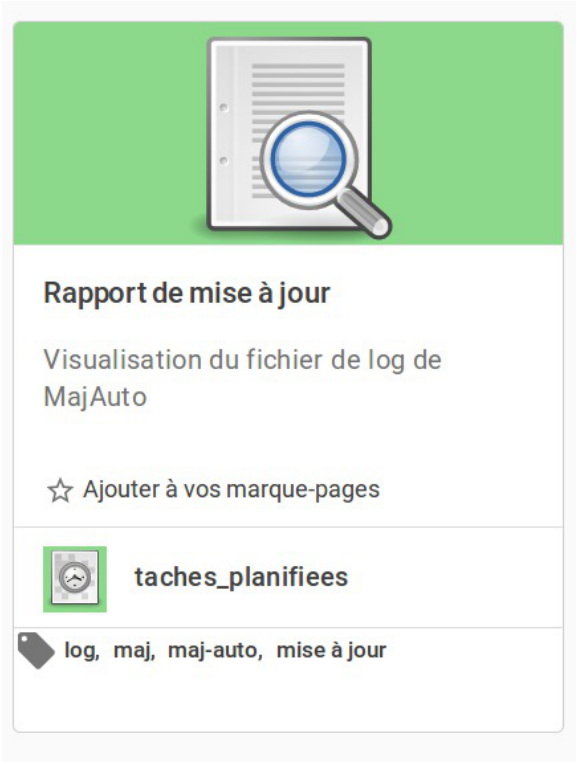
- *<family_action>* et *<action>* : permettent de définir l'action d'une manière générique ;

Des variables Creole sont définies dans la rubrique *familly* et sont utiles pour le fonctionnement de l'action :

- la variable *filename* contient le nom long du fichier à afficher ;
- la variable *language* est optionnelle, elle contient le mode de coloration syntaxique utilisé pour afficher le fichier en couleur.

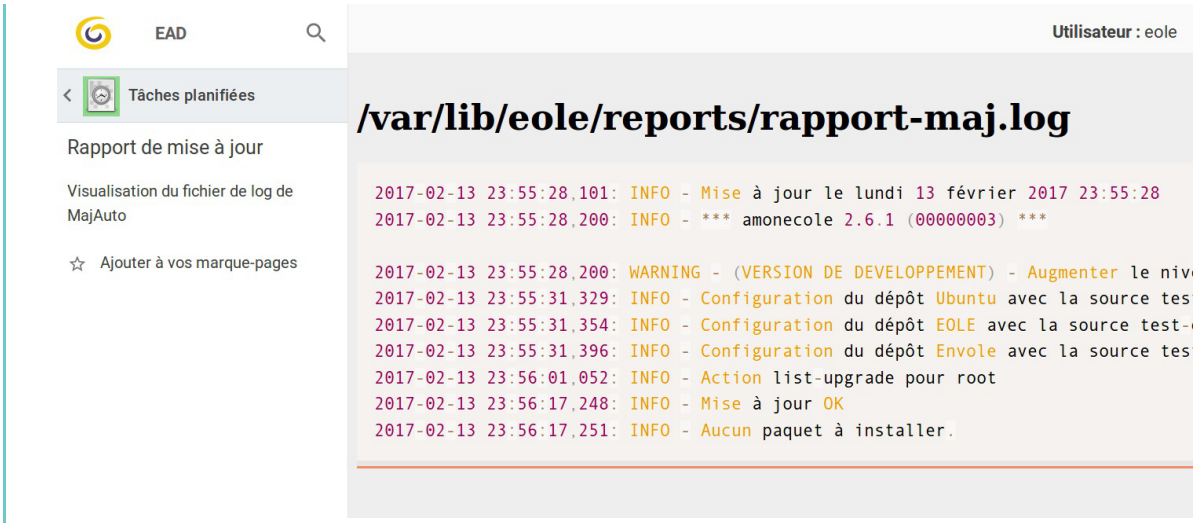
Ces variables sont des variables Creole chargée en mémoire vives, si on veut qu'elles soient enregistrées il faut renseigner l'attribut *save=True* et elles leurs nouvelles valeurs seront stockées dans un `config.eol` (qui n'est pas le `/etc/config.eol` principal de Creole).

L'action d'affichage est de type *filename* et est préexistante. Elle ne nécessite aucune recette SaltStack particulière. Donc seul le fichier XML Creole est présent.



L'action Rapport de mise à jour

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



Rapport de mise à jour

1.5.6.b. Les actions de type formulaire

Les actions de type formulaire sont des actions qui ont besoin de paramètres pour pouvoir être lancées.

Dans ce cas, il faut faire apparaître un formulaire pour renseigner les variables nécessaires au fonctionnement de l'action.

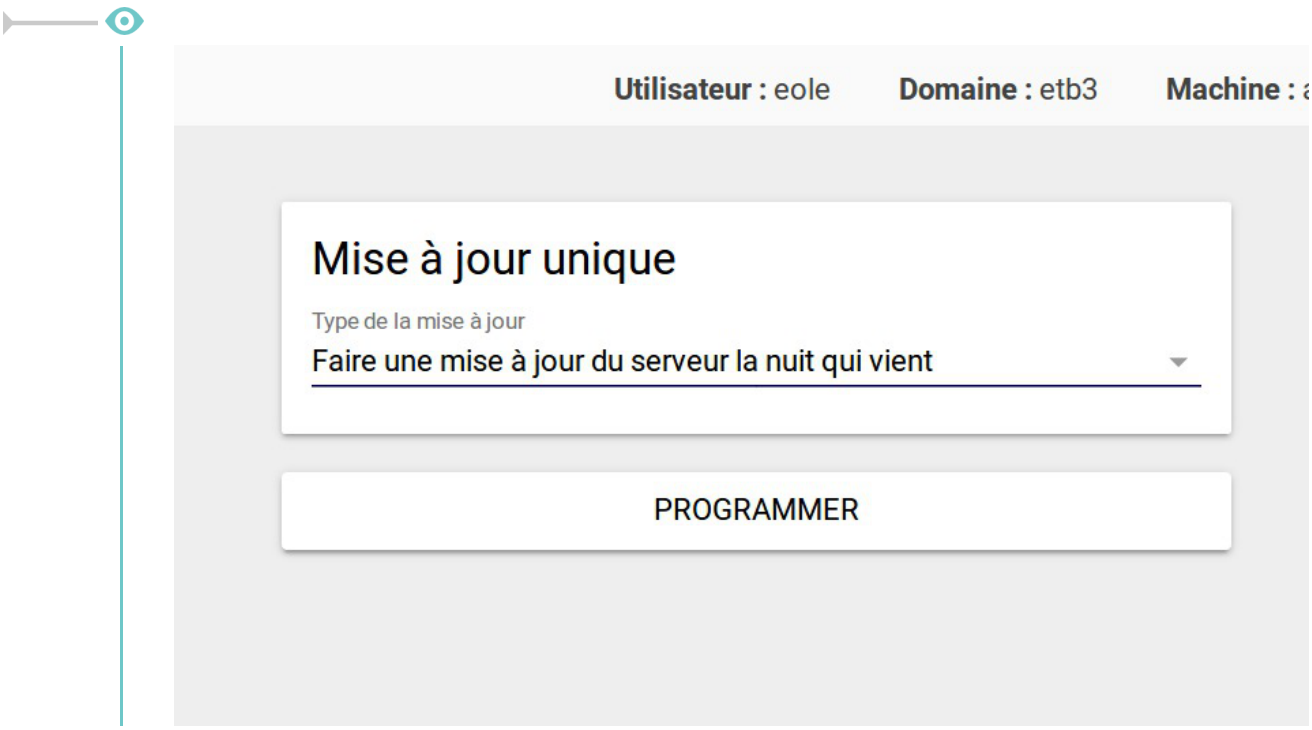
Ce formulaire est généré automatiquement à partir de la définition de variables dans le XML Creole.

```
<variables>
    <family name='Mise à jour'>
    <variable description="Type de la mise à jour" type="string" name="typemaj">
    <value>Faire une mise à jour du serveur la nuit qui vient</value>
    </variable>
    <variable description="Choisir les options de mise à jour" type="string" name="majoption">
    <value>Mise à jour, reconfigure et redémarrage du serveur</value>
    </variable>
    <variable description="Heure" name='hour' type='number'/>
    <variable description="Minute" name='minute' type='number'/>
    <variable description="Jour" name='day' type='date'/>
    </family>
</variables>

```

La définition de variables de type *string* ou de type *number* va générer un formulaire dans l'espace réservé à afficher l'action (widget).

- *<input>Programmer</input>*
  permet de définir un bouton de validation
- *<variable description="Type de la mise à jour" type="string" name="typemaj">*
  <value>Faire une mise à jour du serveur la nuit qui vient</value>
  </variable>
  fait apparaître une liste déroulante avec un item

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



1.5.7. Compléments techniques

Relancer l'EAD3

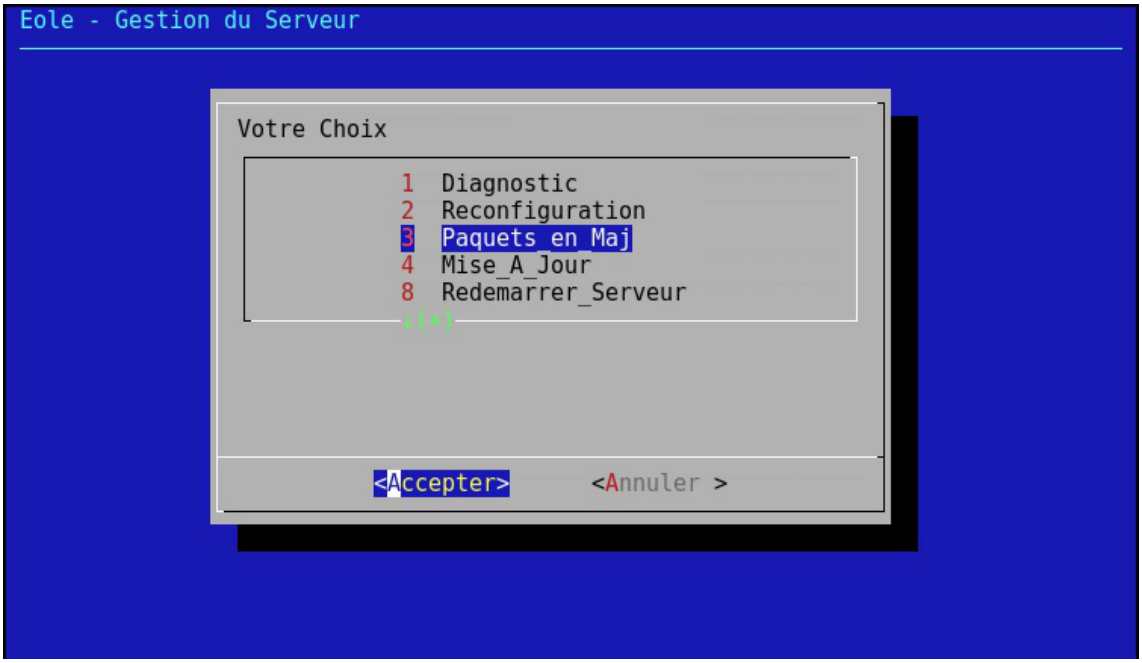
```
root@scribe:~# service salt-api status
● salt-api.service - The Salt API
   Loaded: loaded (/lib/systemd/system/salt-api.service; enabled; vendor preset:
enabled)
   Active: active (running) since mer. 2017-03-01 11:31:49 CET; 4min 22s ago
 Main PID: 9193 (salt-api)
   CGroup: /system.slice/salt-api.service
           ├─9193 /usr/bin/python /usr/bin/salt-api
           └─9614 /usr/bin/python /usr/bin/salt-api

mars 01 11:31:48 scribe systemd[1]: Starting The Salt API...
mars 01 11:31:49 scribe systemd[1]: Started The Salt API.
root@scribe:~#
```

1.6. L'interface d'administration semi-graphique

En plus de l'EAD, une interface semi-graphique est disponible.

Cette interface (`manage-eole`) permet d'exécuter quelques tâches simples d'administration du serveur : diagnostique, mise à jour, liste des paquets en mise à jour, etc.

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



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ... créés à l'instance, et pour les administrateurs à droits restreints qui peuvent être créés avec la commande `add_restricted_admin` en dehors de la procédure d'instance.

1.7. Les mises à jour

Avec GNU/Linux, comme avec d'autres systèmes d'exploitation, les logiciels doivent être compilés avant de pouvoir être utilisés.

Au début du projet Debian (sur lequel est basé Ubuntu), les auteurs jugèrent nécessaire de disposer d'un système d'installation et de désinstallation de logiciels et bibliothèques efficace et simple. Ce système fut nommé **dpkg** et utilise des paquets portant l'extension **.deb**.

Les paquets

Un paquet contient un logiciel ou une bibliothèque déjà compilé et qui s'installe de façon automatique au travers du gestionnaire de paquets. Le format natif des paquets pour Ubuntu et donc pour EOLE est le paquet Debian.

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



Pour limiter la taille des paquets et pour rendre plus efficace l'utilisation de votre ordinateur, le paquet ne contient que le logiciel ou la bibliothèque. Si ce logiciel a besoin d'un autre logiciel ou d'une bibliothèque particulière pour fonctionner, le paquet indique quelles sont ces exigences à satisfaire. On les appelle les dépendances.

La dépendance permet une réutilisation d'une même composante par plusieurs logiciels. Par exemple, si un logiciel nécessite une bibliothèque particulière et qu'un autre logiciel nécessite aussi cette bibliothèque, une ne sera installée qu'une seule fois pour les deux programmes. Cette dépendance apporte plusieurs avantages: lors d'une mise à jour, un paquet est mis à jour pour tous les logiciels, il y a alors une économie de bande passante et d'espace utilisé sur les disques durs.

Le gestionnaire de paquets

Le fait qu'un paquet puisse dépendre d'autres paquets serait infernal à gérer de façon manuelle.

Advanced Packaging Tool (APT) est un système complet et avancé de gestion de paquets, permettant une recherche facile et efficace, une installation simple et une désinstallation propre de logiciels et utilitaires. Il gère les dépendances automatiquement et paramètre les fichiers de configuration durant l'installation et les mises à jour.

Les mises à jour sont continuelles et incrémentales. Le système offre une méthode de mise à jour cohérente et un processus de mise à jour sûr.

APT est un ensemble d'utilitaires utilisables en ligne de commande.

Il facilite la mise à jour d'une distribution Debian et Ubuntu.

EOLE utilise également ce système et fournit un ensemble de facilité :

- mise à jour hebdomadaire est configurée automatiquement ;
- mise à jour au travers de l'EAD et de Zéphir ;
- commandes Maj-Auto, Query-Auto et apt-eole.

⚠ Proxy et mise 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. La déclaration du

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

> proxy s'effectue dans l'onglet `Général` de l'interface de configuration du module, passer `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui` et paramétrer l'adresse du proxy dans le champ `Nom ou adresse IP du serveur proxy`.

1.7.1. Les différents types de mises à jour

Les mises à jour pour une version donnée permettent de corriger les problèmes bloquants, de sécurité et/ou ne permettant pas un fonctionnement normal du module.

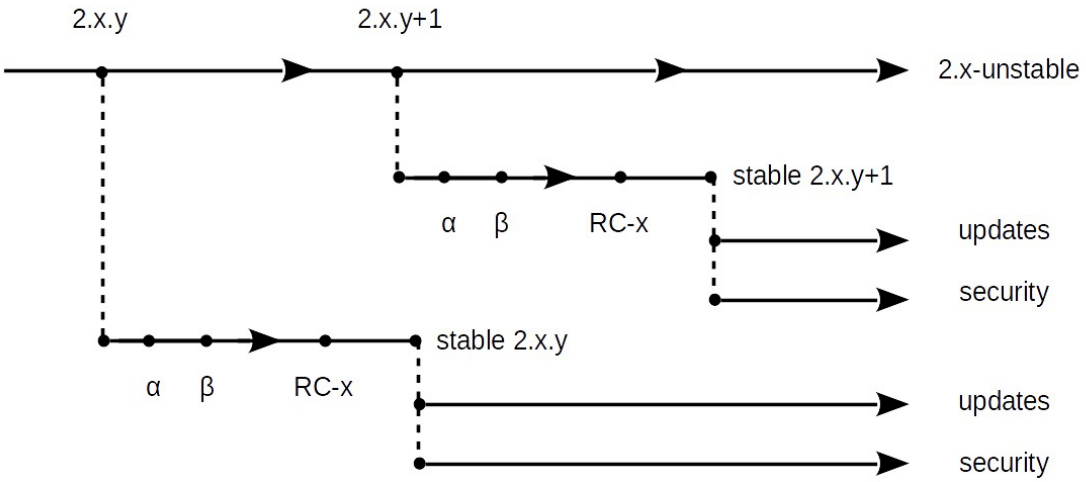
Par défaut une mise à jour hebdomadaire est configurée automatiquement à la fin de l'instanciation du module. Ce comportement est paramétrable et désactivable.

Sur EOLE 2.6, il n'existe qu'un seul niveau de mise à jour. Le concept de mise à jour minimale et complète a été supprimé. L'ajout de nouvelles fonctionnalités entraîne une nouvelle version d'EOLE (2.6.x). Le passage d'une version à une autre est manuel.

Les mises à jour fonctionnelles et les corrections sont proposées sur le dépôt de développement (Unstable), puis proposées en Release candidate (RC)[p.521] lorsque les paquets sont stabilisés et testés. Plusieurs RC successives ont lieu avant la publication de la totalité des RC en stable. Cela donne lieu à une nouvelle version d'EOLE (2.5.x). Chaque version d'EOLE bénéficie des dépôts :

- Security : paquets fixant un problème de sécurité ;
- Updates : paquets fixant des dysfonctionnement bloquants ou suffisamment importants et ne pouvant pas attendre la sortie d'une nouvelle version d'EOLE (durée de rétention en RC et publication en stable).
- Proposed-updates : paquets candidats pour la version d'EOLE utilisée.

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



Mise à jour corrective

La dénomination "mise à jour corrective" concerne les paquets qui sont diffusés en version stable sur une version mineure d'EOLE.

Il s'agit généralement des paquets proposés dans la "mise à jour candidate annoncée" sur lesquels des correctifs additionnels mineurs ont pu être apportés.

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/ ;
- 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).

Les paquets diffusés en version stable sont disponibles dans les dépôts stables du site de référence.

Ils s'installent à l'aide de la commande : `Maj-Auto` et sont également installés automatiquement pas la mise à jour hebdomadaire.

Mise à jour candidate annoncée

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

La dénomination "mise à jour candidate annoncée" concerne les paquets prêts à être diffusés en version stable sur une version mineure d'EOLE.

Il s'agit généralement des paquets proposés dans la "mise à jour candidate en préparation" qui ont été validés par l'équipe.

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/ ;
- 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).

Obtenir manuellement les paquets candidats

Les paquets en version candidate annoncés sont disponibles pendant la période de transition dans les dépôts candidats des dépôts du site de référence.

Ils s'installent **manuellement** à l'aide de la commande : `Maj-Auto -C`.

Obtenir automatiquement les paquets candidats

Les paquets candidats en préparation et non annoncés peuvent être obtenus **automatiquement** et à tout moment en déclarant les serveurs de test en tant que `Serveur de mise à jour`.

Ils s'installent à l'aide de la commande `Maj-Auto -S test-eole.ac-dijon.fr`.

Les mises à jour candidates sont testées par l'équipe EOLE, durant la période de transition et leur passage en stable, elles peuvent être installées et des remontées positives ou négatives peuvent être formulées sur la forge ou sur les listes de discussion.

Mise à jour candidate en préparation

La dénomination "mise à jour candidate en préparation" concerne les paquets prêts à être diffusés en version candidate sur une version mineure d'EOLE mais qui n'ont pas encore été annoncés officiellement.

Le détail des paquets disponibles est généralement 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).

Les paquets en version candidate non annoncés sont disponibles à tout moment uniquement dans les dépôts de test.

Ils s'installent à l'aide de la commande : `Maj-Auto -C -S test-eole.ac-dijon.fr`

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

Les mises à jour candidates sont testées par l'équipe EOLE, durant la période de transition et leur passage en stable, elles peuvent être installées et des remontées positives ou négatives peuvent être formulées sur la forge ou sur les listes de discussion.

Mise à jour de développement

Les paquets mis à disposition en version de développement sont généralement ceux de la prochaine version mineure d'EOLE qui est en cours d'élaboration.

Comme son nom l'indique, ce type de mise à jour s'adresse principalement aux développeurs et aux contributeurs qui souhaitent tester les dernières évolutions de la distribution EOLE.

Les paquets en version de développement s'installent à l'aide de la commande : `Maj-Auto -D`.

Les mises à jour de développement sont susceptibles de rendre le serveur instable.

Il est fortement déconseillé de les utiliser sur un serveur en production.

Les dépôts de développement (`eole-2.6-unstable` pour EOLE 2.6) ne sont pas versionnés.

Leur utilisation sur une version mineure d'EOLE précédente entraînera un changement de version du serveur.

Voir aussi...

Les dépôts EOLE [p.456]

1.7.2. Les procédures de mise à jour

Les procédures manuelles de mise à jour des modules EOLE sont accessible de quatre manières :

- EAD[p.500] ;
- interface semi-graphique ;
- Zéphir ;
- ligne de commande.

De plus, à la fin de l'instanciation, une mise à jour hebdomadaire est configurée automatiquement.

Intégrité de la mise à jour

Une mise à jour EOLE représente un ensemble de paquets.

L'installation manuelle de seulement l'un d'entre eux peut rendre votre système instable.

L'utilisation des méthodes listées ci-dessus permet de garantir l'intégrité du serveur.

Proxy et mise à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le

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

> 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. La déclaration du proxy s'effectue dans l'onglet `Général` de l'interface de configuration du module, passer `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui` et paramétrer l'adresse du proxy dans le champ `Nom ou adresse IP du serveur proxy`.

1.7.2.a. Mise à jour depuis l'EAD

Dans `Système` / `Mise à jour`, l'EAD propose une interface de mise à jour du serveur, il est possible de :

- de lister les paquets disponibles pour la mise à jour ;
- de programmer une mise à jour différée (dans 3 heures par exemple, ou dans 0 heure pour le faire tout de suite) ;
- d'activer / désactiver les mises à jour hebdomadaires (le jour et l'heure de la mise à jour automatique sont déterminés aléatoirement).

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.



Rapport de mise à jour

Penser à consulter le rapport de mise à jour et l'état des services sur la page d'accueil.

Reconfiguration et redémarrage automatique

Une mise à jour lancée depuis l'EAD exécute automatiquement une reconfiguration du serveur avec la commande `reconfigure`, il n'est donc pas nécessaire d'en lancer un par la suite comme c'est le cas depuis la console.

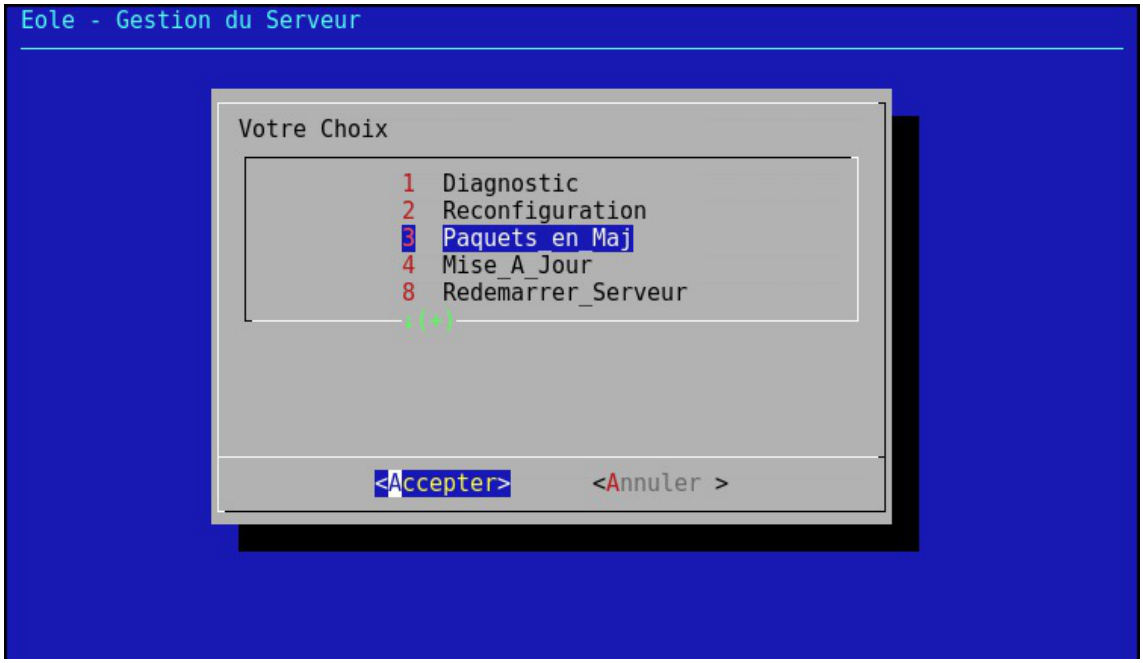
Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

1.7.2.b. L'interface d'administration semi-graphique

En plus de l'EAD, une interface semi-graphique est disponible.

Cette interface (`manage-eole`) permet d'exécuter quelques tâches simples d'administration du serveur : diagnostique, mise à jour, liste des paquets en mise à jour, etc.

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



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ... créés à l'instance, et pour les administrateurs à droits restreints qui peuvent être créés avec la commande `add_restricted_admin` en dehors de la procédure d'instance.

1.7.2.c. 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.433]

1.7.2.d. Les mises à jour en ligne de commande

Il est important de tenir son système à jour. Pour cela, il est possible de lancer manuellement une mise à jour.

Les commandes Maj-Auto et Query-Auto

Ces scripts sont à utiliser pour mettre à jour un module au travers d'un accès internet :

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

- `Maj-Auto` : télécharge et installe les paquets à mettre à jour depuis le réseau ;
- `Query-Auto` : télécharge et affiche la liste des paquets à mettre à jour depuis le réseau.

Sans préciser d'option, ces deux commandes affichent, téléchargent et installent des paquets stables, ils permettent également de tester (sur une machine dédiée aux tests) :

- les paquets candidats lors de la sortie d'une version candidates avec l'option `-C` ;
- les paquets de développements au fil de l'eau avec l'option `-D`.

Il est également possible de simuler l'installation avec l'option `-n` ou de seulement télécharger en cache les paquets `--download`.

Reconfiguration

À la fin de l'exécution de la commande `Maj-Auto`, si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur avec la commande `reconfigure`.

La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état intermédiaire qui pourrait s'avérer instable.

Reconfigurer applique les changements venants des mises à jour tout en tenant compte de la configuration telle que définie lors de la configuration du serveur.

La version candidate (nommée aussi RC pour Release Candidate) est une version d'EOLE qui correspond, du côté pratique, à la version stable. Elle est mise à disposition à des fins de tests de dernière minute visant à déceler les toutes dernières erreurs subsistant avant la sortie définitive de la version.

Tester les paquets candidats permet :

- de contribuer et de participer à l'amélioration du projet ;
- une validation par les utilisateurs des comportements attendus ;
- de faire remonter des dysfonctionnements avant la publication définitive.

Les commandes Maj-Cd et Query-Cd

`Maj-Cd` et `Query-Cd` sont les scripts à utiliser pour mettre un module à jour depuis un CD-ROM d'installation plus récent que celui utilisé lors de l'installation :

- `Maj-Cd` : installe les paquets à mettre à jour depuis un CD-ROM ;
- `Query-Cd` : affiche la liste des paquets à mettre à jour depuis un CD-ROM.

Les mises à jour à l'aide d'un CD-ROM ne se font que depuis un CD-ROM d'une même version mineure (par exemple : mise à jour de la version 2.6.0 avec un CD-ROM 2.6.0.1).

Reconfiguration

À la fin de l'exécution de la commande `Maj-Cd`, si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur avec la commande `reconfigure`.

La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état intermédiaire qui pourrait s'avérer instable.

Reconfigurer applique les changements venants des mises à jour tout en tenant compte de la

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

configuration telle que définie lors de la configuration du serveur.

Options de mise à jour

Options communes aux scripts de mise à jour

- -f : passer outre les autorisations Zéphir ;
- -h : affiche l'aide ;
- -d : mode debug ;
- -W : génère une sortie formatée pour l'EAD[p.500].

Options spécifiques aux scripts Maj-Auto et Query-Auto

- -C : force la mise à jour en version candidate pour tous les dépôts par défaut ou pour le (ex : -C envole) ou les dépôts spécifiés (ex : -C eole envole) ;
- -D : force la mise à jour des paquets en développement pour tous les dépôts par défaut ou pour le (ex : -D envole) ou les dépôts spécifiés (ex : -D eole envole) ;
- -S : force le site de mise à jour EOLE (ex : -S test-eole.ac-dijon.fr) ;
- -U : force le site de mise à jour Ubuntu (ex : -U fr.archive.ubuntu.com) ;
- -V : force le site de mise à jour Envole (ex : -V test-eole.ac-dijon.fr).

Options spécifiques aux scripts Maj-Auto et Maj-Cd

- -n : exécuter en mode simulation (*dry run*) équivaut à utiliser les commandes `Query-Auto` ou `Query-Cd` ;
- -r : exécuter reconfigure après une mise à jour réussie ;
- -R : exécuter reconfigure après une mise à jour réussie et redémarrer si nécessaire.

Options spécifiques au script Maj-Auto

- --download : procéder uniquement au téléchargement des paquets en cache.

L'utilisation des options `-C` ou `-D` entraîne un avertissement et une demande de confirmation.

Toutes les options sont documentées dans les pages de manuel de chaque commande :

```
# man Maj-Auto
```

Voir aussi...

Les dépôts EOLE [p.456]

Reconfiguration [p.254]

Installation manuelle de paquets [p.325]

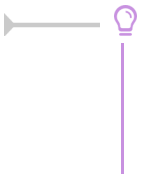
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.7.3. Ajout de dépôts supplémentaires

Les outils `Query-Auto`, `Query-Cd, Maj-Auto` et `Maj-Cd` réinitialisent systématiquement la liste des dépôts à utiliser pour les mises à jour et donc les fichiers `/etc/apt/sources.list`.

Pour déclarer des dépôts supplémentaires, il est possible d'ajouter des fichiers possédant l'extension `.list` dans le répertoire `/etc/apt/sources.list.d`.

En mode conteneur, chacun des conteneurs utilise son propre répertoire. Il est donc possible de mettre en place des sources différentes en fonction du conteneur.



Pour tester les dépôts ajoutés, il est possible de lancer manuellement la mise à jour des sources avec la commande :

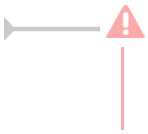
```
# apt-get update
```


L'ajout de dépôts supplémentaires est proposé dans l'interface de configuration du module, en mode expert, dans l'onglet `Dépôt tiers`.

Voir aussi...

Onglet Dépôt tiers [p.173]

1.7.4. Désactivation temporaire des mises à jour



Désactiver les mises à jour met en danger votre système. Il n'est pas recommandé de désactiver les mises à jour sauf dans certains cas et ce de manière temporaire.

Malgré les nombreux tests et la période d'incubation des paquets, il arrive parfois qu'un paquet ait un comportement inattendu, il est alors possible et souhaitable de ne pas déstabiliser l'ensemble du parc de machines. Reporter temporairement les mises à jour est l'une des solutions.

La désactivation des mises à jour peut s'effectuer de plusieurs façon :

- désactiver la mise à jour hebdomadaire dans l'EAD ;
- désactiver la mise à jour hebdomadaire avec Creole et eole-schedule ;
- interdire les mises à jour du serveur dans le serveur Zéphir.

Voir aussi...

Mise à jour depuis l'EAD [p.270]

Gestion des tâches planifiées eole-schedule [p.433]

Les actions Zéphir sur les serveurs

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

1.8. Installation manuelle de paquets

Il est possible d'installer manuellement des paquets :

- pour installer des fonctionnalités additionnelles au module ;
- pour éventuellement installer de manière sélective des mises à jour en vue de les tester.

Avant de procéder à l'installation d'un paquet, il faut s'assurer que les sources APT[p.494] sont configurées sur le bon type de mises à jour (stable, candidate, développement) et que la liste des paquets est à jour. Cela s'effectue avec la commande `Query-Auto` :

- mises à jour stables : `Query-Auto` ;
- mises à jour candidates : `Query-Auto -C` ;
- mises à jour de développement : `Query-Auto -D` ;

Ensuite il faut utiliser la commande `apt-eole` qui procède au téléchargement et à l'installation.

Au même titre que la commande `apt-get`, la commande `apt-eole` utilise APT[p.494] et permet de gérer les paquets et leurs mises à jour.

L'usage de la commande `apt-eole` en lieu et place de la commande `apt-get` est recommandée pour l'installation des paquets EOLE.

La commande `apt-eole` s'utilise comme `apt-get` :

```
# apt-eole install nomDuPaquet
```

Pour installer un paquet dans un conteneur, il faut utiliser l'option `--container` :

```
# apt-eole --container <conteneur> install nomDuPaquet
```



Pour installer le paquet `eole-bareos` :

```
# apt-eole install eole-bareos
```


La commande `apt-eole` appelle la commande `apt-get` avec les options adéquat (notamment les opérations **install** et **remove**) pour répondre aux besoins d'administration des modules EOLE :

- elle n'est pas interactive pour fluidifier l'installation, le paramétrage sera de toute façon écrasé (le paramétrage demandé par le mode interactif est fait par la mécanique EOLE selon le contexte et selon les paramètres saisis dans l'interface de configuration du module) ;
- elle permet de pouvoir gérer les paquets et les mises à jour à l'intérieur des conteneurs[p.497] proposés par EOLE.

Voir aussi...

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

Choisir le mode du module [p.61]

Les mises à jour en ligne de commande [p.321]

1.9. Les administrateurs locaux à droits restreints

À l'instance, au moins un compte local d'administrateur à droits restreints est créés.

Ce type de compte est notamment utilisé pour accéder à l'interface d'administration EAD3.

Trois commandes sont proposées pour gérer ces comptes locaux.

list_restricted_admins

La commande list_restricted_admins retourne tous les comptes locaux appartenant au groupe adm et disposant de l'interface semi-graphique comme shell de connexion.

add_restricted_admin

La commande add_restricted_admin permet de créer un compte local appartenant aux groupes adm et mail et disposant de l'interface semi-graphique comme shell de connexion.

La commande est interactive.

L'utilisateur est invité à saisir un login pour le nouveau compte.

À la différence de la procédure de création de comptes locaux supplémentaires à l'instance, le nom n'est pas contraint à eole suffixé d'un numéro.

del_restricted_admin

La commande del_restricted_admin permet de supprimer un compte local appartenant au groupe adm et disposant de l'interface semi-graphique comme shell de connexion.

L'utilisation de del_restricted_admin propose deux modes :

- interactif : exécution sans arguments, le login du compte est demandé à l'utilisateur ;
- avec le login passé en argument, la saisie étant facilitée par de l'auto-complétion et la suggestion.

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

1.10. Passage d'une version d'EOLE à une autre



2.6.n vers 2.6.n+x

Le passage d'une version mineure à une autre est manuel et volontaire et se fait par l'intermédiaire de la commande `Maj-Release`.

Consulter le manuel de la commande pour voir toutes les options :

```
# man Maj-Release
```

1.11. Passage d'une version RC à une version stable

Avant d'être publiée en version RC, la distribution Linux EOLE subit de nombreux tests.
Aussi, elle ne contient plus aucun changement qui ne peuvent être résolus par mise à jour.

Il est donc possible d'installer une version EOLE RC, de la tester, de l'utiliser et de la mettre à jour pour être au même niveau de mise à jour que la version stable une fois que cette dernière version est publiée.
La mise à jour s'effectue avec la commande `Maj-Auto`.

Les versions RC portent un numéro, il signifie uniquement qu'une image ISO a été re-générée, un nombre conséquent de paquets ont été recompilés et cela évite une trop grosse mise à jour.

2. Joindre le domaine

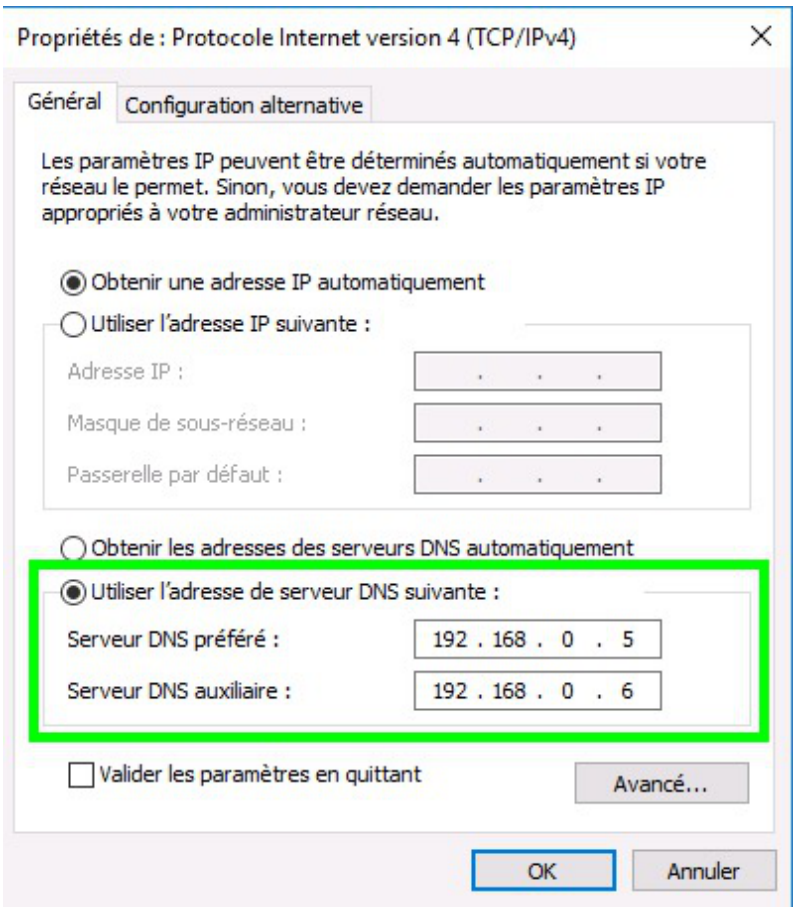
Serveur DNS

Il est indispensable que les postes clients aient l'adresse IP d'au moins un des contrôleur de domaine comme serveur DNS.

Ceci peut-être paramétré soit sur le serveur DHCP dans le cas d'attribution automatique d'adresses IP aux postes clients, soit manuellement dans les paramètres de l'adaptateur

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

réseau :

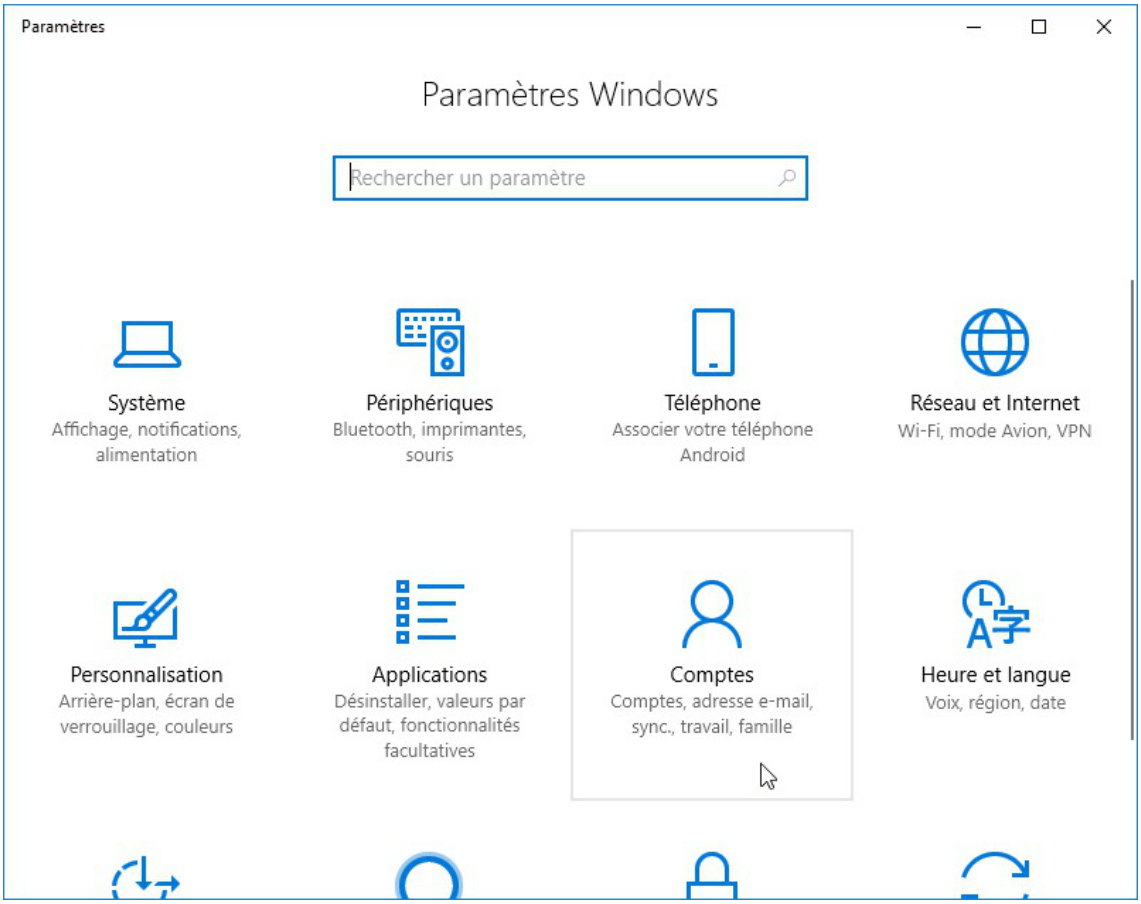


Jonction au domaine

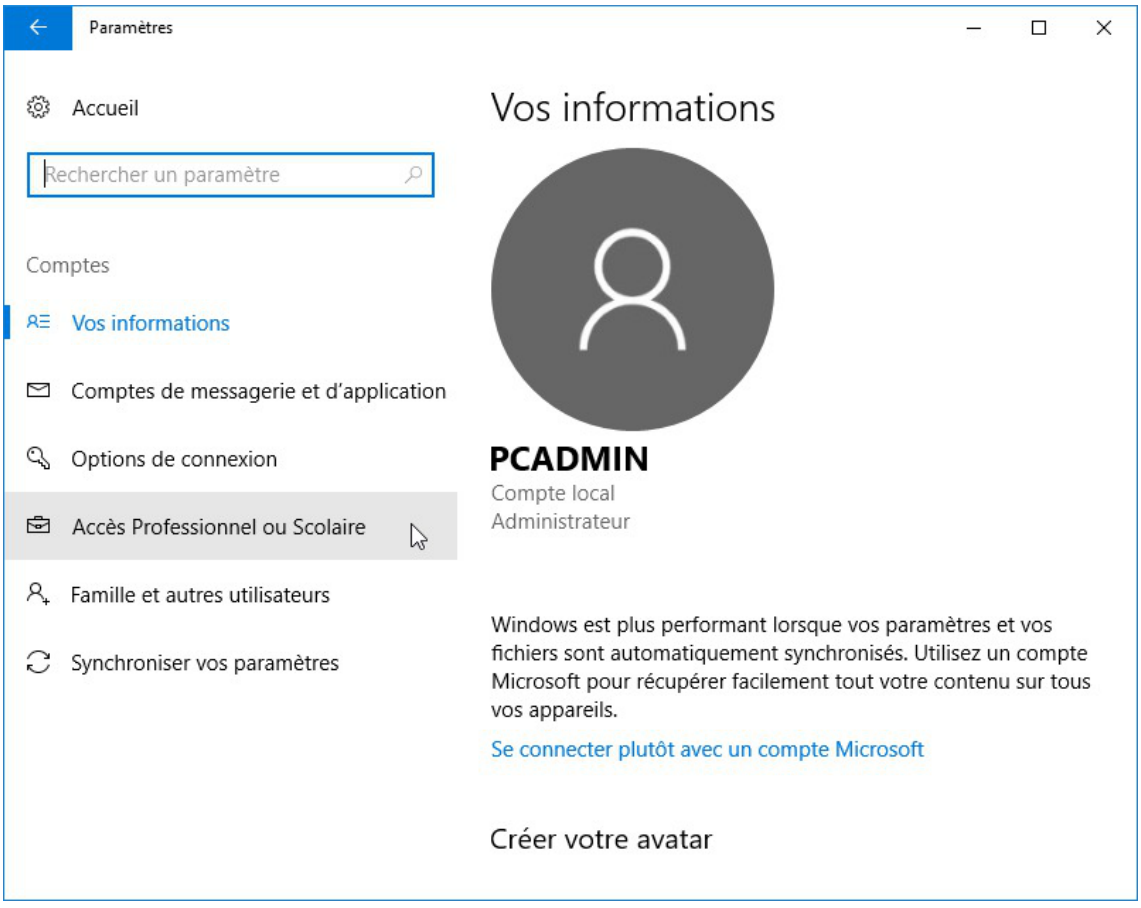
Ajouter la station au domaine de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

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

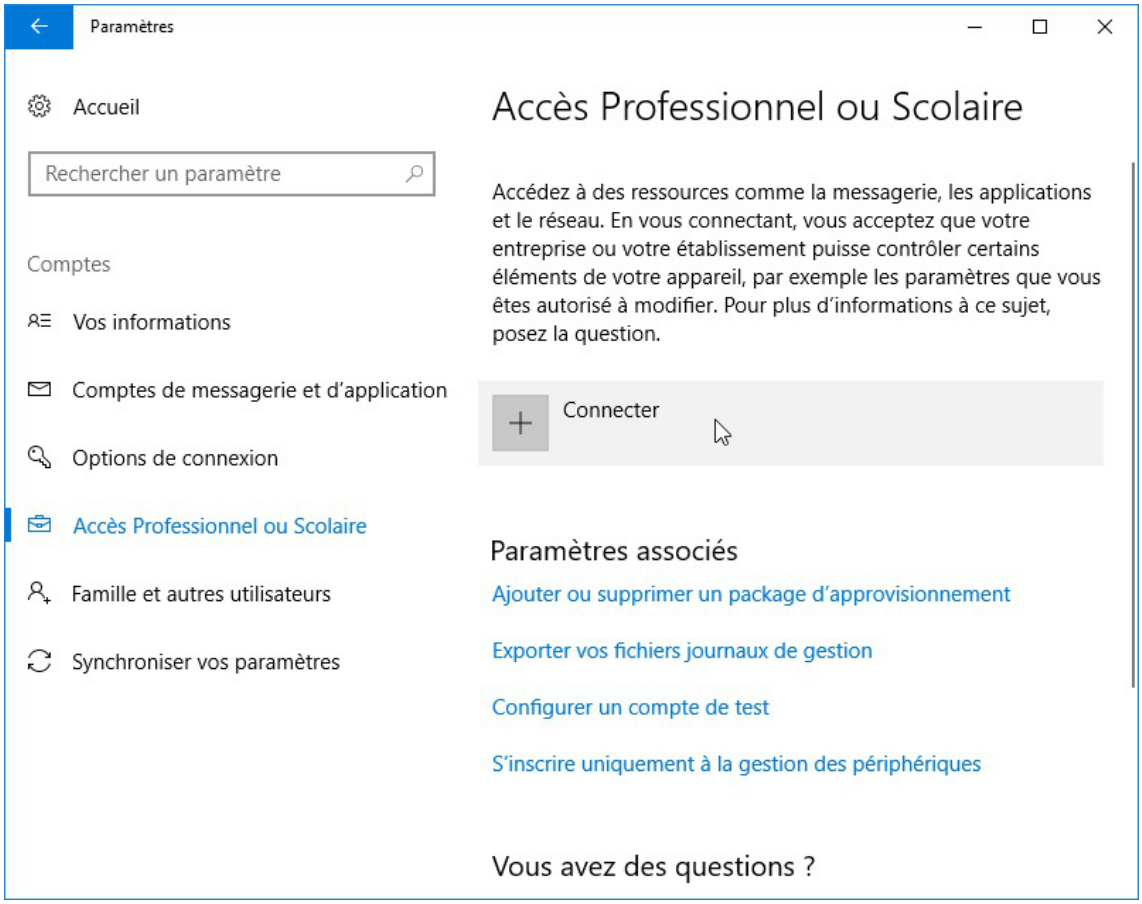


- Cliquer sur `Comptes` ;



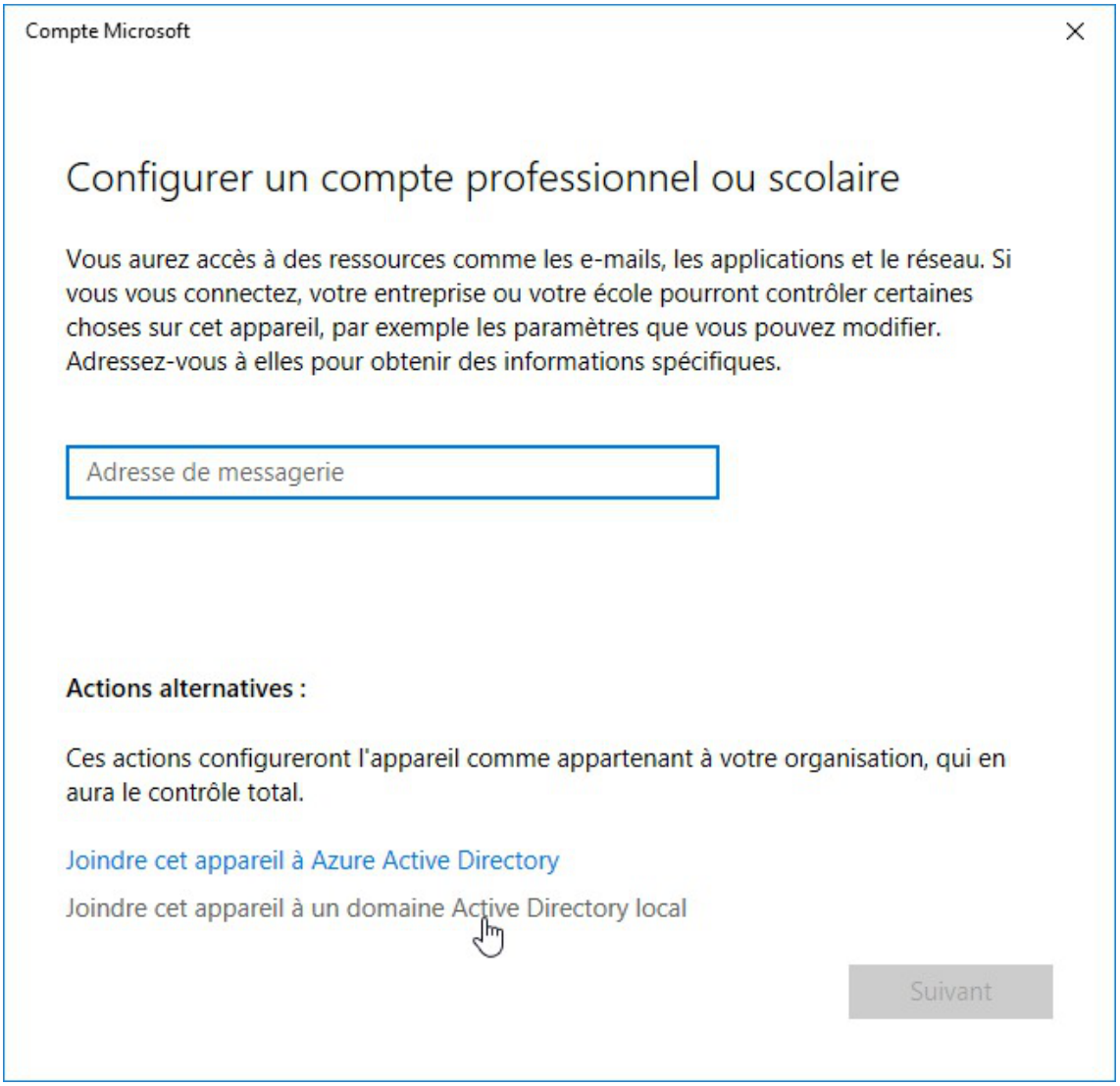
- Cliquer sur `Accès Professionnel ou Scolaire` dans le menu de gauche ;

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

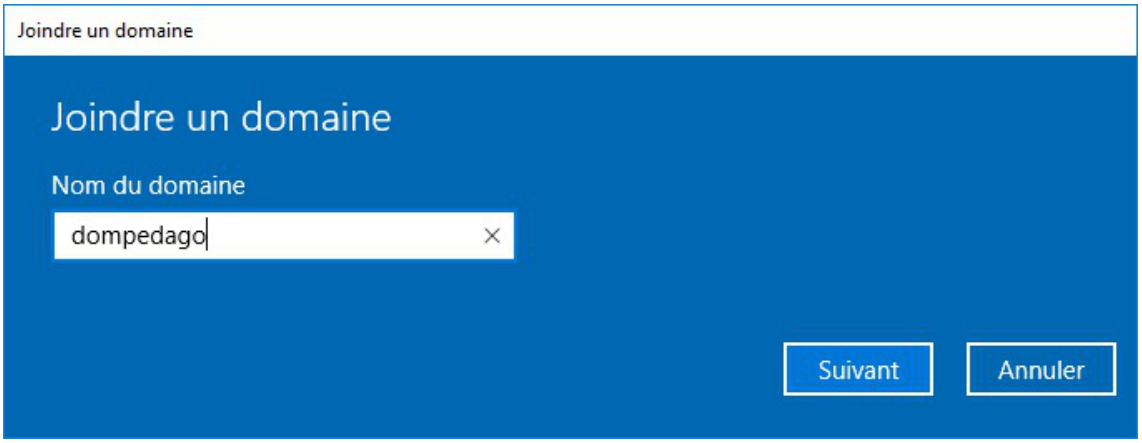


- Cliquer sur Connecter ;

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

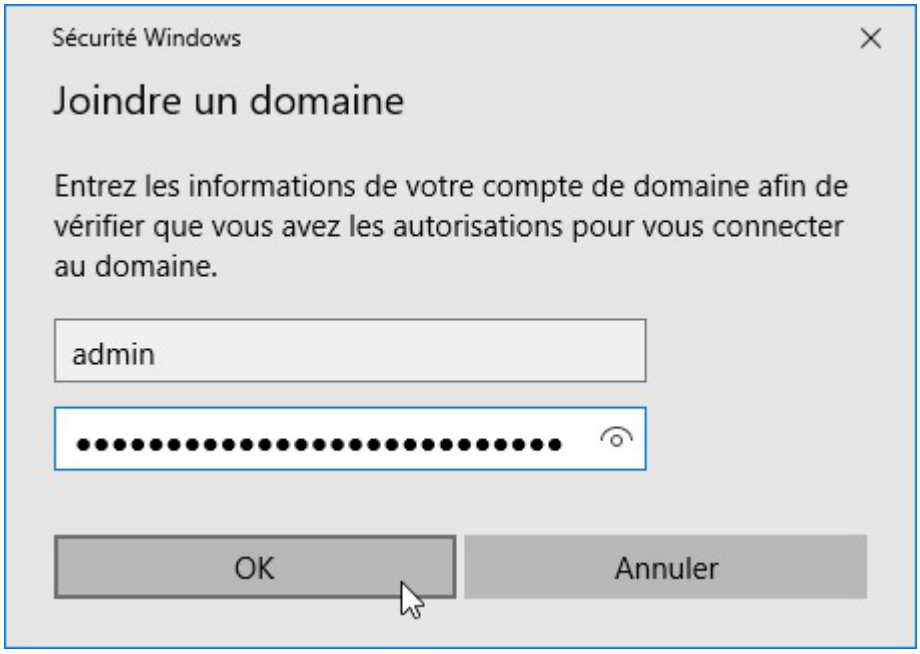


- Cliquer sur `Joindre cet appareil à un domaine Active Directory local` ;

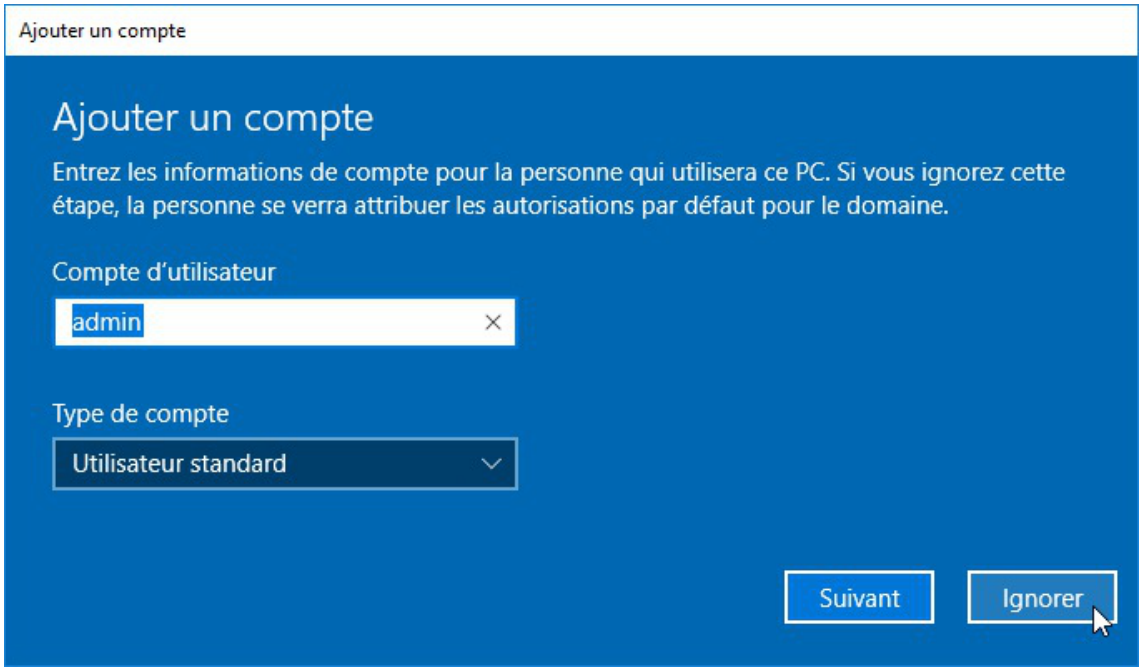


- Saisir le nom du domaine et cliquer sur `Suivant` ;

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

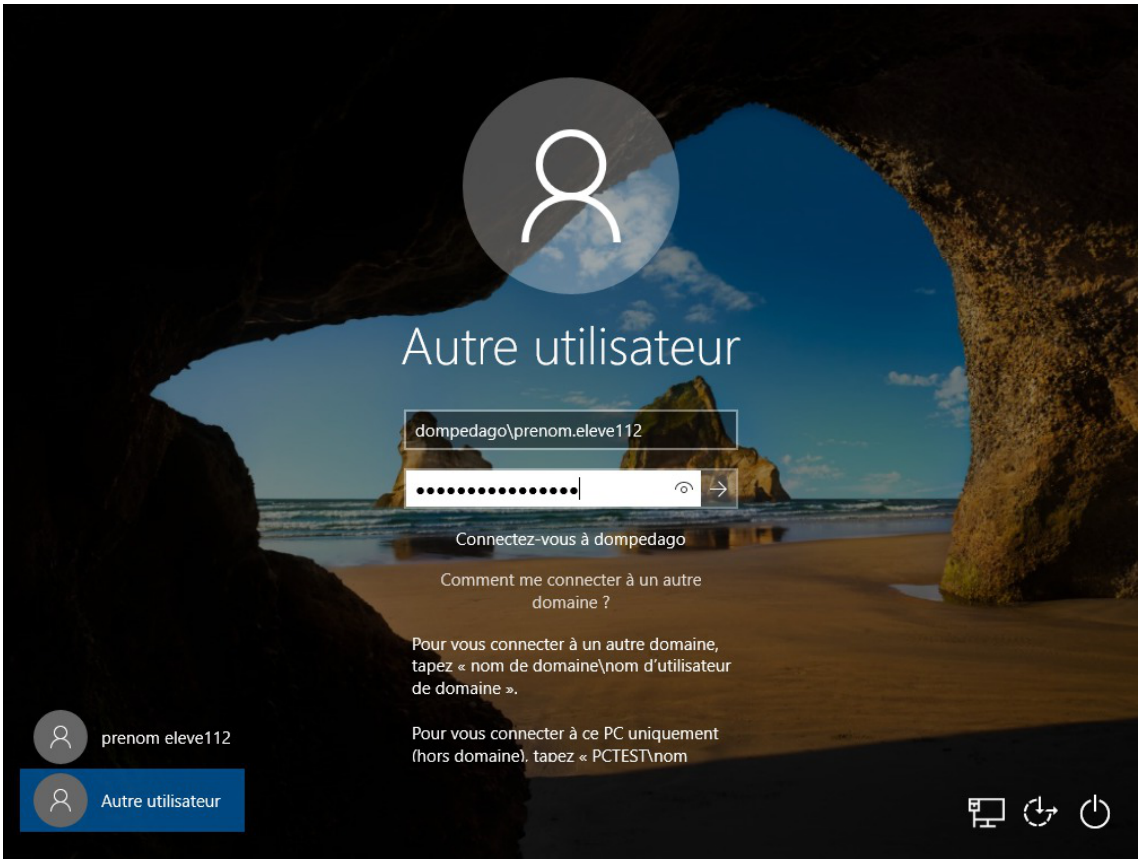


- Saisir le nom du compte administrateur du domaine ainsi que la clé secrète ("mot de passe") associée au compte et cliquer sur le bouton `OK` ;



- Il ne faut pas tenir compte de la proposition d'ajout de compte, cliquer sur le bouton `Ignorer` et accepter de redémarrer ;

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



- Cliquer sur `Autre utilisateur` et saisir le nomDuDomaine\pnom ainsi que la clé secrète ("mot de passe") pour démarrer la session.

3. Gestion de l'Active Directory Seth en ligne de commande

Bien qu'il existe quelques restrictions, la majorité des opérations de gestion peuvent être réalisées en ligne de commande sur les modules Seth configurés en tant que contrôleur de domaine.

Les opérations présentées sont réalisables sur le serveur que le contrôleur de domaine soit déclaré comme additionnel ou non.



La synchronisation des données entre les différents DC n'est pas instantanée et peut prendre jusqu'à trois minutes.

Gestion des groupes et des utilisateurs

- Lister les groupes

  `samba-tool group list`
- Lister les utilisateurs

  `samba-tool user list`
- Créer un utilisateur

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

```
samba-tool user create titi "Mot:DeP455"
```

- Modifier le mot de passe d'un utilisateur

  ```
  samba-tool user setpassword titi
  ```

  ou (noter le "\n" entre les deux mots de passe)

  ```
  echo -e "MotDePasse?\nMotDePasse?" | smbpasswd -s titi
  ```

- Inscrire un utilisateur à un groupe

  ```
  samba-tool group addmembers "Domain Admins" titi
  ```

- Consulter les attributs d'un utilisateur

  ```
  pdbedit -Lv titi
  ```

- Paramétrer le répertoire personnel, la lettre de montage et le profil d'un utilisateur
- `pdbedit -h '\\file.ac-test.fr\titi' -D 'U:' -p '\\file.ac-test.fr\profiles\titi' titi`
- Supprimer un utilisateur

  ```
  samba-tool user delete titi
  ```

Jetons Kerberos et fichiers keytab

Les fichiers keytab, abréviation de « key table » (table des clés), sont des fichiers qui contiennent une clé de chiffrement pour un service ou un hôte.

Ils sont utiles pour réaliser des opération d'administration qui nécessite l'utilisation d'un compte avec pouvoirs sans avoir à en saisir le mot de passe.

L'article suivant (en anglais) explique plutôt bien ce qu'est un keytab : https://social.technet.microsoft.com/wiki/contents/articles/36470.kerberos-keytabs-explained.aspx

Compte machine

Sur le module Seth, un keytab du compte machine du serveur est automatiquement généré dans le fichier `/var/lib/samba/eole-ad-dc.keytab`.

keytabIl est ainsi possible d'utiliser ce fichier dans des scripts, pour ajouter des entrées DNS, par exemple :

```
# initialisation d'un jeton Kerberos à l'aide du fichier keytab
kinit ADDC@AC-TEST.FR -k -t /var/lib/samba/eole-ad-dc.keytab
# ajout d'une entrée DNS locale
samba-tool dns add dc1.ac-test.fr ac-test.fr mac10 A 192.168.0.10 -k 1
# vérification de la résolution d'un nom par le DNS local
dig @localhost mac10.ac-test.fr +short
# suppression d'une entrée DNS locale
samba-tool dns delete dc1.ac-test.fr ac-test.fr mac10 A 192.168.0.10 -k 1
# destruction du jeton Kerberos
kdestroy
```



Le jeton Kerberos[p.505] permet de ne pas avoir fournir de nom d'utilisateur et mot de passe aux commandes d'ajout/suppression d'entrée DNS.

Ceux-ci sont remplacés par l'option « `-k 1` ».

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

Compte utilisateur

De la même façon, il est possible de créer un fichier keytab pour des comptes utilisateur tels que `admin` ou `Administrator` :

```
root@dc1:~# samba-tool domain exportkeytab ~/administrator.keytab
--principal=Administrator@AC-TEST.FR
Export one principal to admin.keytab
root@dc1:~# kinit Administrator@AC-TEST.FR -k -t ~/administrator.keytab
root@dc1:~# kdestroy
root@dc1:~# rm -f ~/administrator.keytab
```

Gestion des sites

Sur le contrôleur de domaine principal, la déclaration d'un site s'effectue facilement grâce à la fonction bash *samba_update_site* :

```
. /usr/lib/eole/samba4.sh
samba_update_site monsite 10.1.1.0/24
```

Recherche avancée

La commande ldbsearch permet d'effectuer des recherches dans l'annuaire Active Directory :

- Initialisation de la variable `LDB_URL`, utilisée par la commande `ldbsearch`.
  `export LDB_URL=/var/lib/samba/private/sam.ldb`
- Rechercher les utilisateurs
  `ldbsearch -S '(objectclass=user)' cn`
- Afficher l'entrée d'un utilisateur
  `ldbsearch cn=admin`
- Afficher l'entrée correspondant au groupe `Administrators`
  `ldbsearch '(&(objectclass=group)(cn=Administrators))' --cross-ncs`
- Afficher les entrées correspondant aux contrôleurs de domaine
  `ldbsearch '(invocationId=*)' --cross-ncs objectguid`

Les commandes ldbadd, ldbmodify et ldbdel permettent également de modifier l'annuaire Active Directory à l'aide d'instructions au format LDIF[p.506].

Ajouter une OU (Unité Organisationnelle) :

Générer le fichier *ajouterOU.ldif* :

```
dn: OU=etablissement1,DC=ac-test,DC=fr
changetype: add
objectClass: top
objectClass: organizationalunit
```

Ajouter la modification dans l'annuaire :

`ldbadd ajouterOU.ldif`

Voir aussi...

Administration avancée du module Seth [p.468]

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

4. Gestion sommaire des GPO depuis le contrôleur de domaine

Le contrôleur de domaine propose des commandes complétant celles fournies par le projet Samba pour la gestion des GPO[p.502].

Ces commandes proposent une couverture partielle des opérations d'ajout de règles (policies) que l'on retrouve dans la console d'administration sur les postes Windows.



Les commandes `samba-tool gpo`, fournies par Samba, permettent de créer des GPO, de les supprimer, de les lier à des OU[p.521], de les délier, mais pas encore d'associer des règles aux GPO.

Les commandes `gpo-tool policy` proposées sur le module sont fournies par le paquet `gpo-tool` et ses dépendances et complète partiellement *samba-tool*.

La commande `gpo-tool policy` réplique le fonctionnement du client en ligne de commande `samba-tool` .

Elle propose les sous-commandes suivantes :

- `register` : enregistrement d'une description de règle dans un fichier local servant de stockage à l'usage de la commande `gpo-tool` ;
- `list` : affichage de la liste des description de règle connues par la commande `gpo-tool` (enregistrées dans le fichier de stockage par la commande `register`). Actuellement, la commande `list` affiche le détail de toutes les descriptions contenues dans le fichier local.
- `add` : association de la règle au GPO ;
- `inspect` : affichage des détails de la description de la règle. L'inspection des règles permet de voir quelles règles seront acceptées par la commande `add` et quelles variables sont nécessaires.

Associer des règles à un GPO nécessite une édition de l'Active Directory et du répertoire SYSVOL[p.519]. La nature des modifications du répertoire SYSVOL dépend de la règle à associer de même que les informations à ajouter à l'Active Directory.

Les commandes proposées couvrent la fonctionnalité de création et d'ajout de descriptions de règles (l'ensemble des éléments permettant d'associer la règle à un GPO) et l'association d'un sous-ensemble des règles existantes à un GPO.

Est testé, actuellement, l'ajout des règles suivantes :

- association d'un utilisateur ou groupe de l'Active Directory à un groupe local ;
- désactivation de la fonctionnalité de changement de mot de passe en passant par l'enchaînement de touches `Ctrl + Alt + Suppr` ;
- la restriction des droits de jonction de machines au domaine, à un compte.

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

Enregistrement des descriptions de règles

Une description de règle s'ajoute au fichier local avec un appel comme suit :

```
# gpo-tool policy register <nom unique> <CSE_GUID> <type> <emplacement> <modèle>
```

Les arguments sont les suivants :

- `nom unique` : le nom unique servant à identifier la règle (passée en argument de la commande `add`) ;
- `CSE GUID` : l'identifiant du composant prenant en charge la règle dans la console d'administration de Windows ;
- `type` : le type de règle déterminant quel traitement est nécessaire pour la mettre en place ;
- `emplacement` : l'emplacement dans le répertoire du GPO, commençant soit par `Machine`, soit par `User` ;
- `modèle` : contenu du fichier à créer dans le répertoire `sysvol` avec emplacement de variables.



La commande suivante enregistre une description de la règle permettant l'association d'un utilisateur ou groupe de l'Active Directory à un groupe local :

- le nom Groupes restreints ;
- un CSE_GUID `{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00` ;
- la règle est mise en place sous la forme `GptTmpl.inf` ;
- le fichier est créé dans `Machine/Microsoft/Windows NT/SecEdit` (implique que le contexte d'application est `Machine`) ;
- le contenu est déterminé par `[Group Membership]\n{group}__Memberof = {sup_group}\n{group}__Members = {sub_group}` (la section Group Membership avec les clés {group}__Memberof et {group}__Members) avec les variables `group`, `sup_group` et `sub_group`.

```
# gpo-tool policy register 'Groupes restreints' '{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0' 'GptTmpl.inf' 'Machine/Microsoft/Windows NT/SecEdit' '[Group Membership]\n{group}__Memberof = {sup_group}\n{group}__Members = {sub_group}'
```



La commande suivante enregistre une description de la règle permettant désactivation de la fonctionnalité de changement de mot de passe en passant par l'enchaînement de touches `Ctrl + Alt + Suppr` :

- le nom identifiant la description `Ctrl + Alt + Suppr` ;
- le CSE_GUID `{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8`

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

;

- la règle est mise en place sous la forme `Registry.pol` ;
- le fichier est créé dans `User` (implique que le contexte d'application est `User`) ;
- le contenu est déterminé par `Software\Microsoft\Windows\CurrentVersion\Policies\system;Disable` avec la variable `value`.

```
# gpo-tool policy register 'Ctrl+Alt+Suppr'
'{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E82
'Registry.pol' 'User'
'Software\Microsoft\Windows\CurrentVersion\Policies\system;DisableCh
```

Actuellement, seuls deux types sont supportés :

- `Registry.pol` : format de fichier permettant d'appliquer des clés de registres ;
- `GptTmpl.inf` : format de fichier similaire au format INI[p.504] permettant de stocker des règles sous la forme clé-valeur.

Le choix du type n'est pas libre mais déterminé par le composant de la console qui prend en charge la règle.

Inspection des descriptions de règles

```
# gpo-tool policy list
Policy: 'Groupes restreints'
  - destination: Machine/Microsoft/Windows NT/SecEdit
  - variables: group, sup_group, sub_group

Policy: 'Ctrl+Alt+Suppr'
  - destination: User
  - variables: value

```

Création d'un GPO

La création d'un GPO s'effectue à l'aide de la commande `gpo-tool register`.

Le GPO admin_local est créé avec la commande suivante :

```
# samba-tool gpo create "admin_local" -U administrator%password
GPO 'admin_local' created as
{95CBBB90-2941-4AA0-BFFA-491D072EB8DC}
```

Le GPO change_password est créé avec la commande suivante :

```
# samba-tool gpo create "change_password" -U
administrator%password
```


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

```
GPO          'change_password'          created          as
{E542AB9F-626C-4045-8862-F31710A37D07}
```

Association des règles aux GPO

L'association des règles aux GPO s'effectue avec une commande comme suit :

```
# gpo-tool policy add <nom du GPO> <nom de la description> [-v clé:valeur …]
```

Avec les arguments et paramètres suivants :

- `nom du GPO` : le nom d'affichage (unique du point de vue de Samba) du GPO ;
- `nom de la description` : le nom utilisé pour distinguer la description lors de son enregistrement dans le fichier local (peut-être retrouvé grâce à la commande `list`) ;
- `-v clé:valeur` : un nombre indéterminé de couples clé, valeur.



La règle enregistrée plus tôt peut y être associée de la façon suivante :

```
# gpo-tool policy add "admin_local" 'Groupes restreints' -v group:*S-1-5-21-2447931902-1787058256-3961074038-5004 -v sup_group:'' -v sub_group:Administrators -U administrator%password
```

L'utilisateur S-1-5-21-2447931902-1787058256-3961074038-5004 issu de l'Active Directory est associé au groupe local Administrators.



La règle enregistrée plus tôt peut y être associée de la façon suivante :

```
# gpo-tool policy add "change_password" 'Ctrl+Alt+Suppr' -v value:1 -U administrator%password
```


La commande `add` édite l'Active Directory et le répertoire SYSVOL à travers des connexions ldb et SMB. L'option `-U` est nécessaire pour passer le nom d'un compte autorisé à de telles éditions. Le mot de passe peut être ajouté à la suite du compte ou saisi dans le terminal.

Application du GPO au niveau d'une unité organisationnelle

Pour appliquer le GPO, il faut utiliser la commande `samba-tool gpo setlink`.



```
1 # samba-tool gpo setlink "DC=etb1,DC=lan"
  '{E542AB9F-626C-4045-8862-F31710A37D07}' -U administrator%password
2 Added/Updated GPO link
3 GPO(s) linked to DN DC=etb1,DC=lan
4     GPO     : {E542AB9F-626C-4045-8862-F31710A37D07}
5     Name    : change_password
6     Options : NONE
7
8     GPO     : {31B2F340-016D-11D2-945F-00C04FB984F9}
```


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

```
9     Name    : Default Domain Policy
10    Options : NONE
```

Débogage des GPO sous Windows

Lister les GPO appliqués

Pour commencer, il est recommandé d'actualiser les paramètres de stratégies de groupes du client, dans l'`invite de commandes`, saisir :

```
gpupdate
```

La commande suivante permet d'obtenir la liste des GPO appliqués pour l'utilisateur connecté :

```
gpresult /SCOPE USER /V
```

Pour obtenir les GPO "machine", la commande est :

```
gpresult /SCOPE COMPUTER /V
```

Exécution de code PowerShell

Si le GPO nécessite des traitements complexes, il est probable qu'il exécutera un programme PowerShell[p.513].

L'application `Windows PowerShell ISE` (exécutée en tant qu'administrateur) permet d'ouvrir et d'exécuter simplement des fichiers .ps1[p.514].

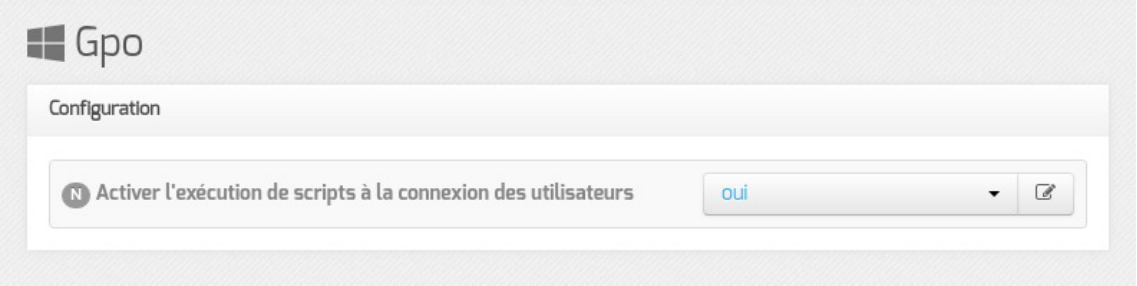
5. Le GPO « eole_script »

Le paquet `eole-gpo-script` met en place un GPO[p.502] permettant notamment de déclarer simplement des scripts personnalisés à exécuter lorsqu'un utilisateur ouvre une session sur un poste Windows (`logon.exe`).

Il permet également le déploiement automatisé du nouveau client EOLE (SaltMinion).

L'outil ré-utilise les mêmes concepts que l'exécution des scripts personnalisés par l'ancien client Scribe NT.

Le paquet `eole-gpo-script` est pré-installé sur les modules Scribe et Horus en mode AD.



Les GPO « eole » sont désactivables dans l'onglet `Gpo` de l'interface de configuration du module.

Emplacement des fichiers

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

Les commandes doivent être renseignées dans des fichiers texte se trouvant dans l'un des sous-répertoire du dossier `scripts` situé dans le répertoire SYSVOL du contrôleur de domaine.

Le répertoire des scripts est accessible par :

- le chemin Unix sur le serveur : `/home/sysvol/` <REALM[p.515]> `/scripts`
- les chemins UNC suivants :
  - \\<nom NetBIOS[p.510]>\ `sysvol/` <REALM[p.515]> `/scripts`
  - \\<nom NetBIOS[p.510]>\netlogon

Arborescence des fichiers

Les scripts peuvent être ajoutés pour :

- un utilisateur → `scripts/users/admin.txt` ;
- un groupe → `scripts/groups/eleves.txt` ;
- une machine → `scripts/machines/poste01.txt` ;
- un OS (Win95, Win2K, WinXP, Samba, Vista) → `scripts/os/WinXP.txt` ;



Windows 7, 10 et 11 sont traités de la même manière que Windows Vista *(OS=Vista)*.

Les noms de machines doivent être écrits en minuscules.

Scripts personnalisés pour exécuter des commandes

Pour exécuter des commandes il faut utiliser l'instruction `cmd`.

Par défaut, le programme d'ouverture de session affiche le programme et attend la fin de son exécution pour continuer. Un programme qui ne se ferme pas (ex. notepad.exe) provoquera des ouvertures de session très longue et incomplètes.

- l'option `NOWAIT` permet de ne pas attendre la fin de l'exécution du programme ;
- l'option `HIDDEN` permet de masquer la fenêtre.

Le format est :

cmd,commande,[options]



Exécuter *notepad.exe* pour l'utilisateur *toto* lorsqu'il ouvre une session :

Fichier *<addc>**netlogon**scripts**os**toto.txt* :

```
cmd,%WINDIR%\notepad.exe,NOWAIT
```

Scripts personnalisés pour monter temporairement des lecteurs

Pour monter temporairement des lecteurs il faut utiliser l'instruction `lecteur`.

Le format est :

lecteur,lettre:,partage

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

Monter le partage *monserveur**partage* sur la lettre *V:* pour tous les utilisateurs du domaine :
Fichier *<scribe>**netlogon**scripts**groups**DomainUsers.txt* :

```
lecteur,V,\\monserveur\partage
```

Les scripts personnalisés sont concaténés dans le script principal, par défaut au début de celui-ci. Si des instructions doivent être effectuée après (nécessité d'avoir accès au lecteur `commun` par exemple), placez la balise **%%NetUse%%** et ajoutez les instructions ensuite.

L'ouverture de session sur un Scribe NT

L'ouverture de session

6. Gestion de l'Active Directory Seth avec les outils RSAT

Depuis une station Windows, il est possible de gérer l'Active Directory du module Seth à l'aide des outils d'administration à distance fournis par Microsoft, les RSAT[p.516].

Téléchargement et installation

Les outils d'administration à distance, *Remote Server Administration Tools (RSAT)*, sont téléchargeables depuis le site de Microsoft :

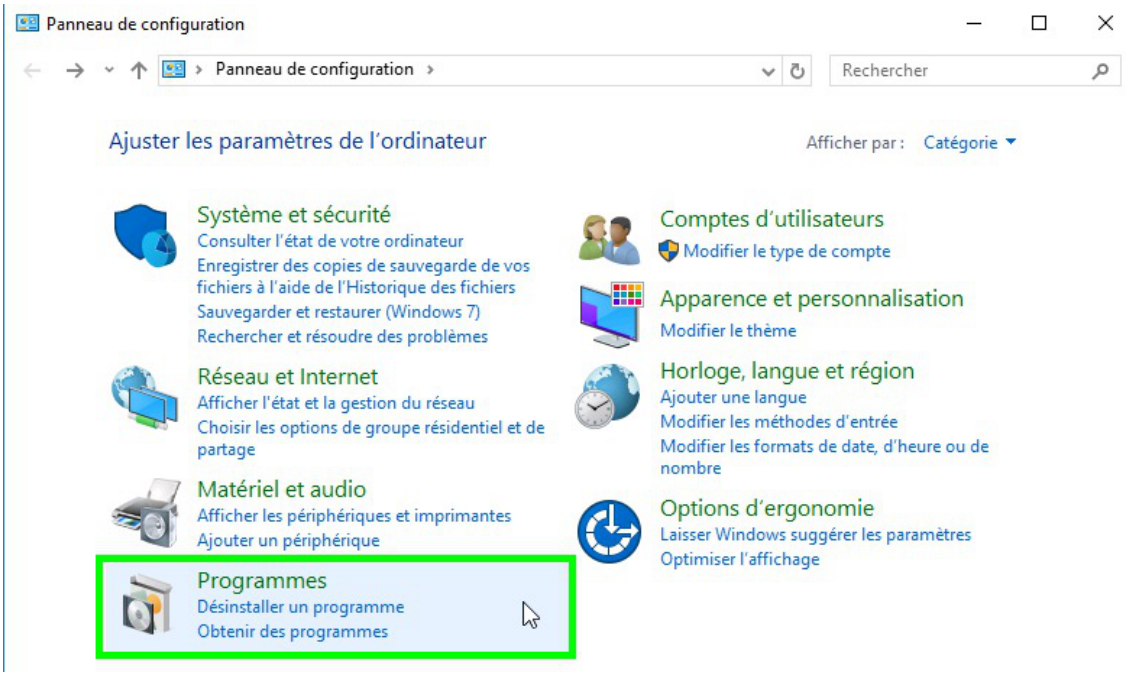
https://support.microsoft.com/fr-fr/help/2693643/remote-server-administration-tools-rsat-for-windows-ope

Une fois installé, il peut être nécessaire d'activer la fonctionnalité.

Pour ce faire :

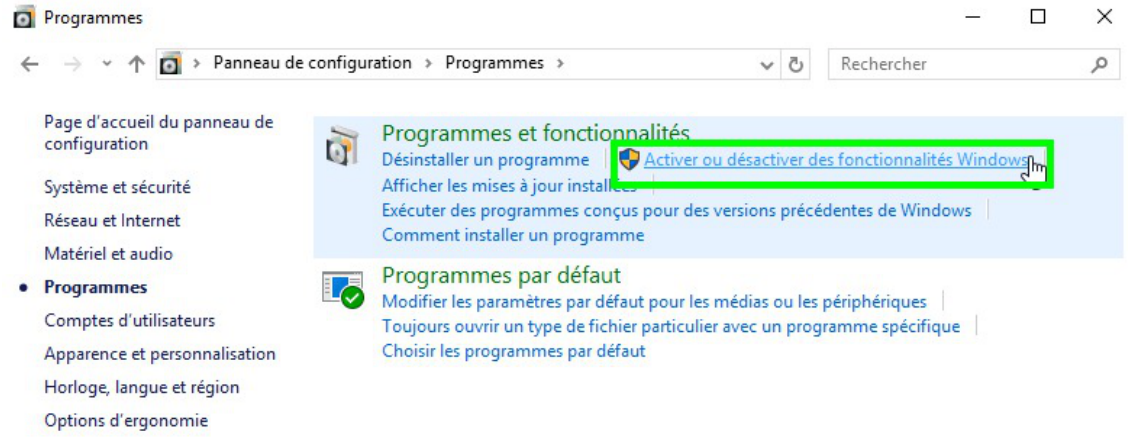
- aller dans Panneau de configuration ;

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



Panneau de configuration

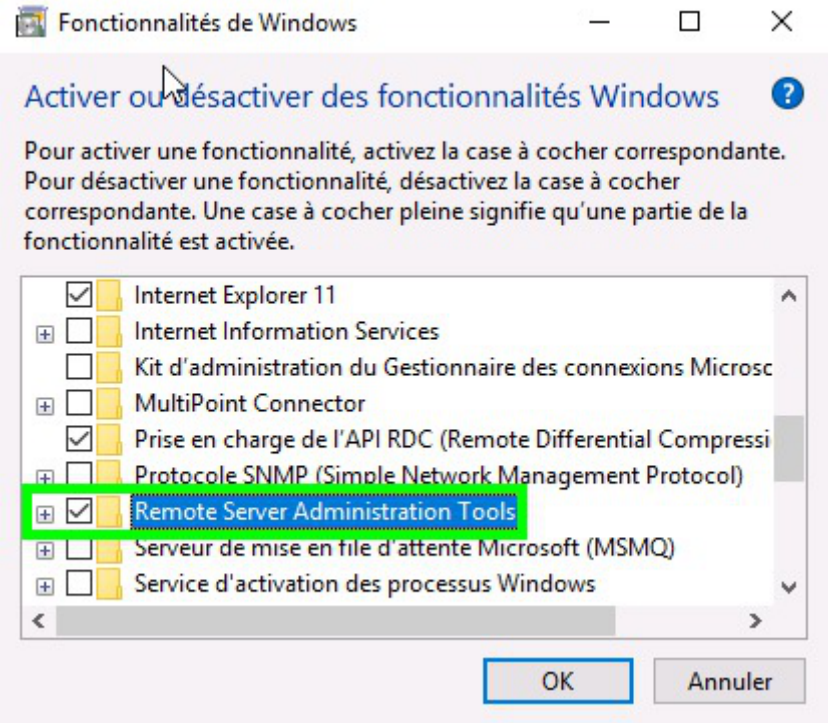
- cliquer sur Activer ou désactiver des fonctionnalités Windows ;



Programmes et fonctionnalités

- cocher les fonctionnalités à activer.

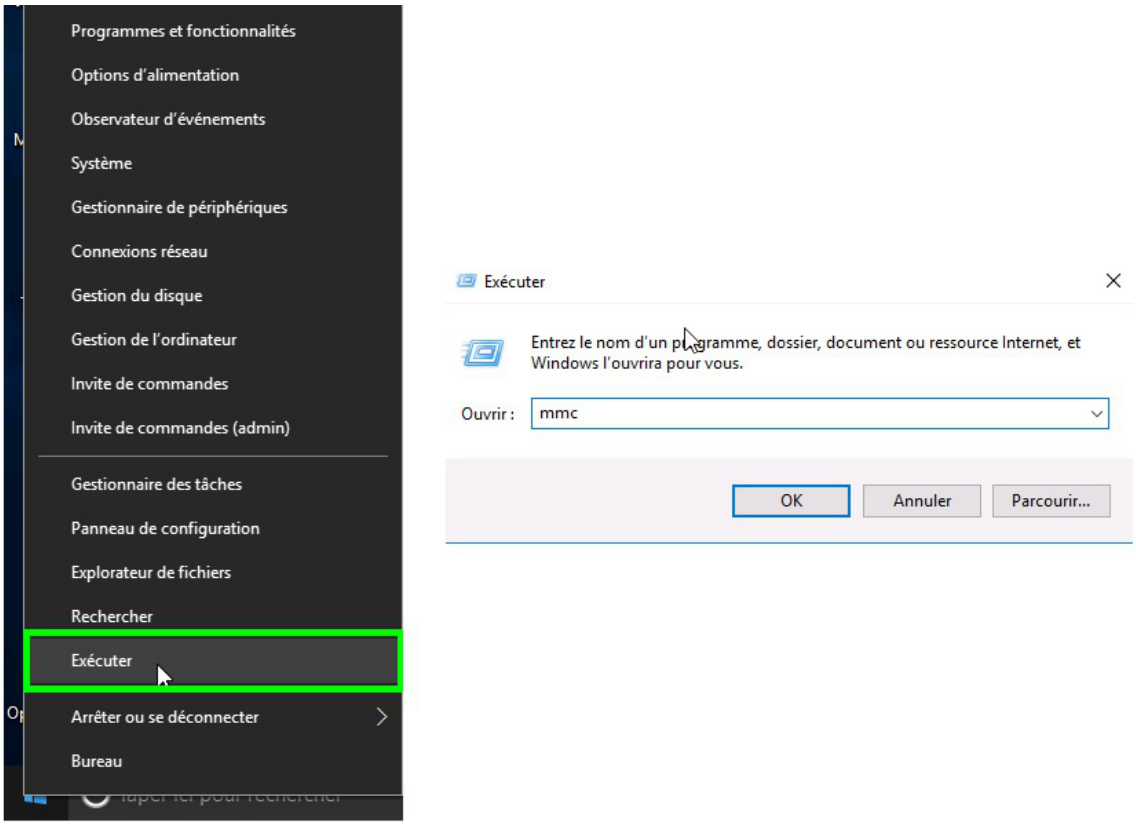
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Activer/désactiver des fonctionnalités

Exécution et paramétrage des outils

Les RSAT s'utilisent, soit séparément en les appelant depuis `Panneau de configuration` → `Outils d'administration`, soit en les regroupant dans une console MMC[p.509] personnalisée. Pour exécuter la commande `mmc` faire un clic droit sur le menu Windows et taper la commande à exécuter.

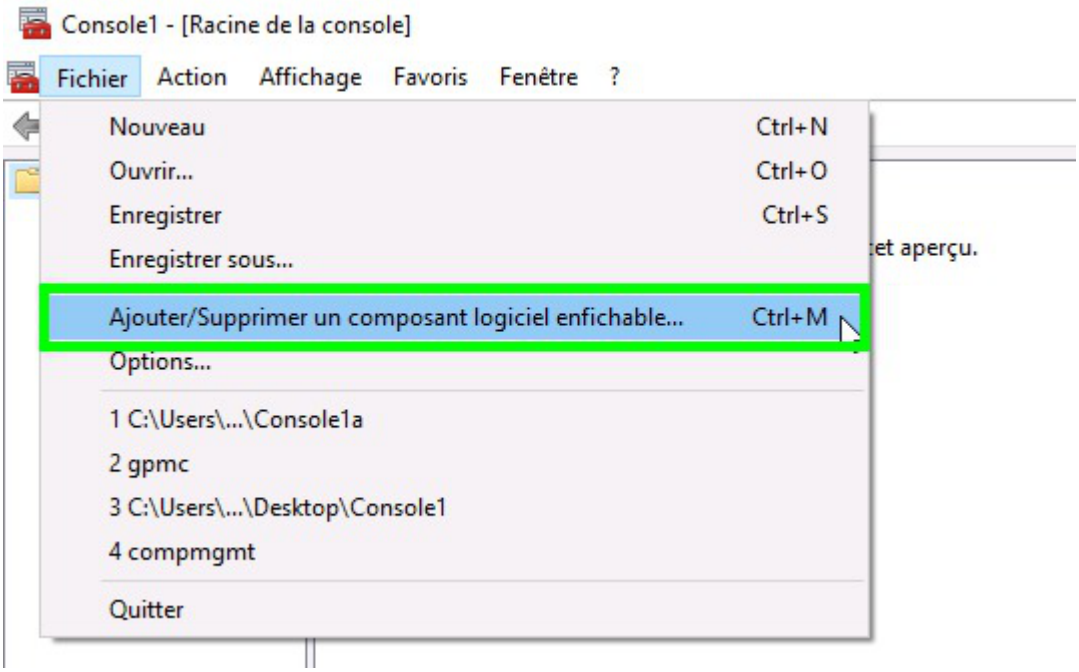


Exécuter une commande

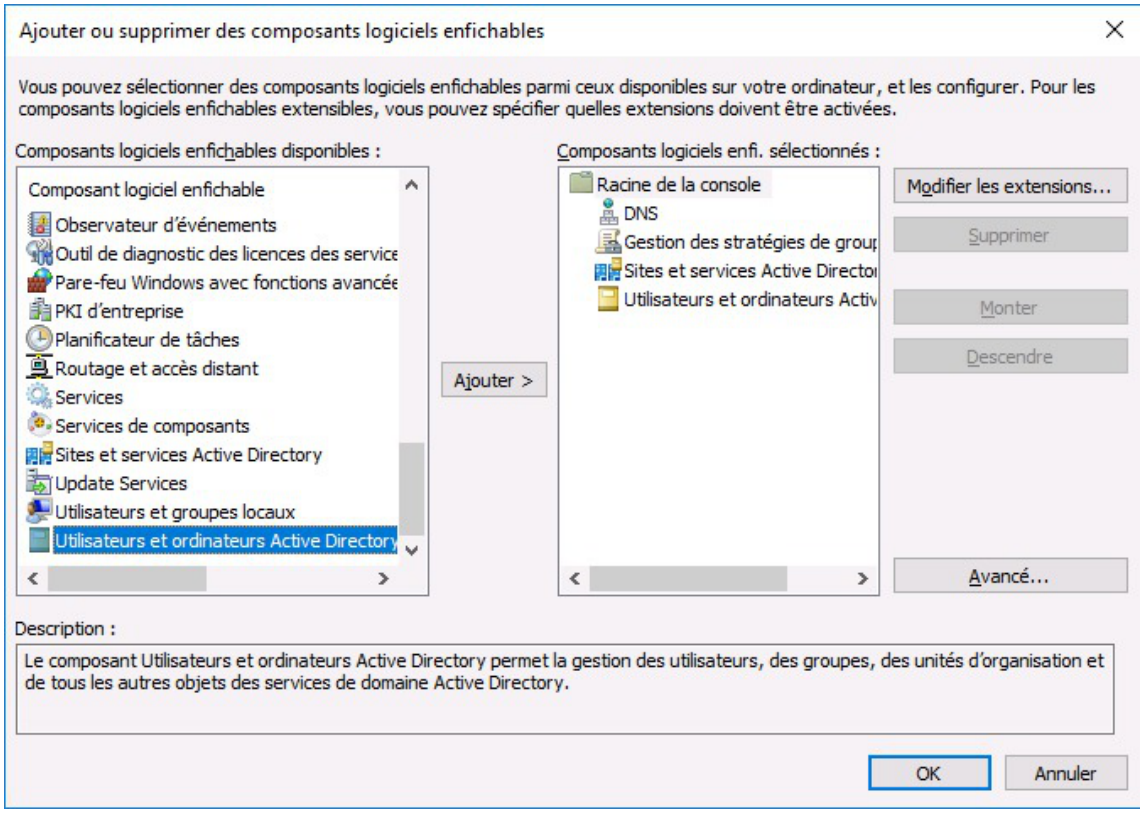
Une fois la console MMC lancée, sélectionner les principaux composants :

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

- DNS ;
- Gestion des stratégies de groupes ;
- Sites et servies Active Directory ;
- Utilisateurs et ordinateurs Active Directory.

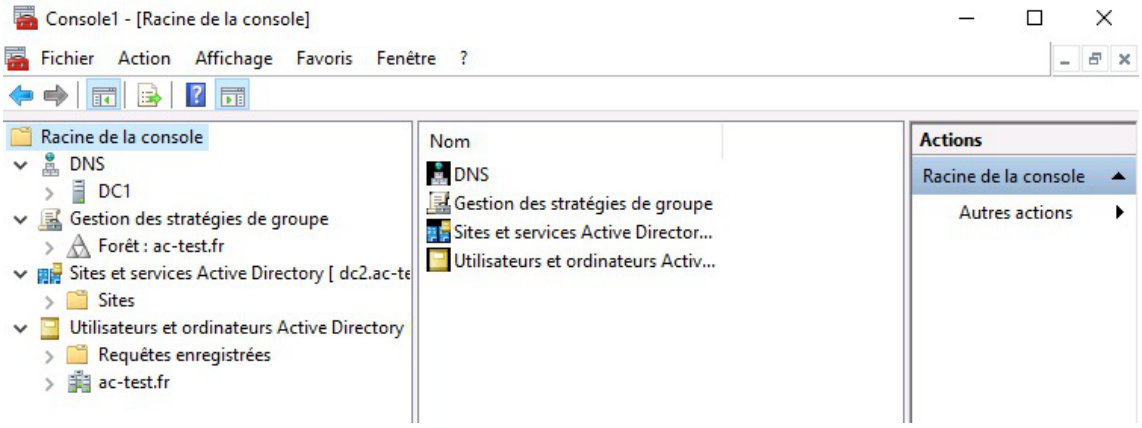


Ajouter des composants à la console



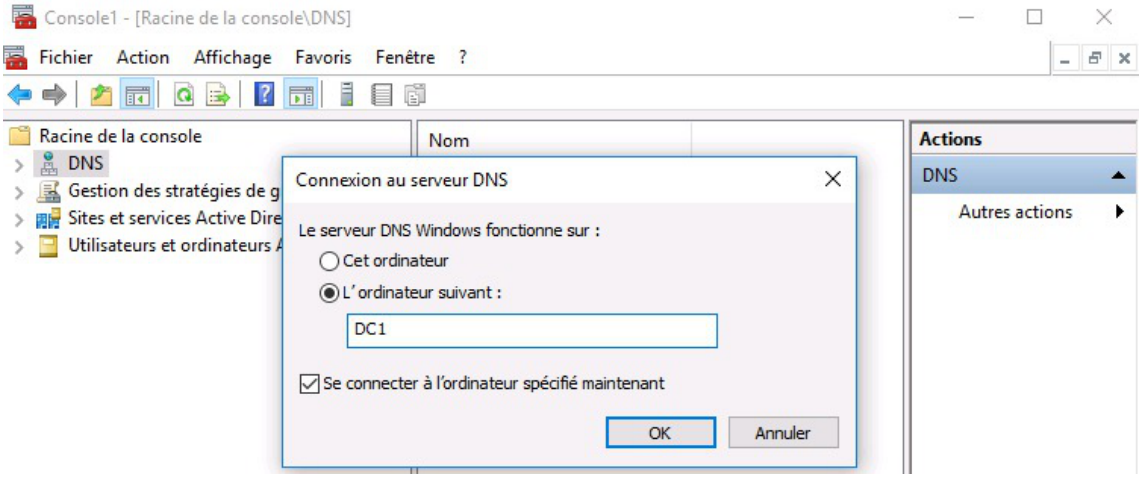
Choisir des composants à ajouter à la console

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



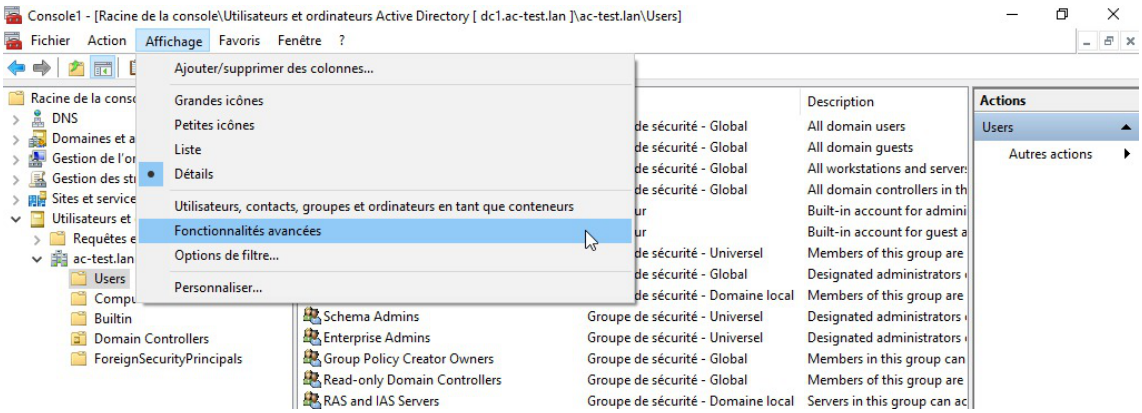
La console une fois les composants ajoutés

Une fois les composants ajoutés dans la console, lorsqu'on clique pour la première fois sur `DNS`, il faut indiquer sur quel serveur on souhaite administrer le DNS.



Indiquer sur quel serveur le DNS fonctionne

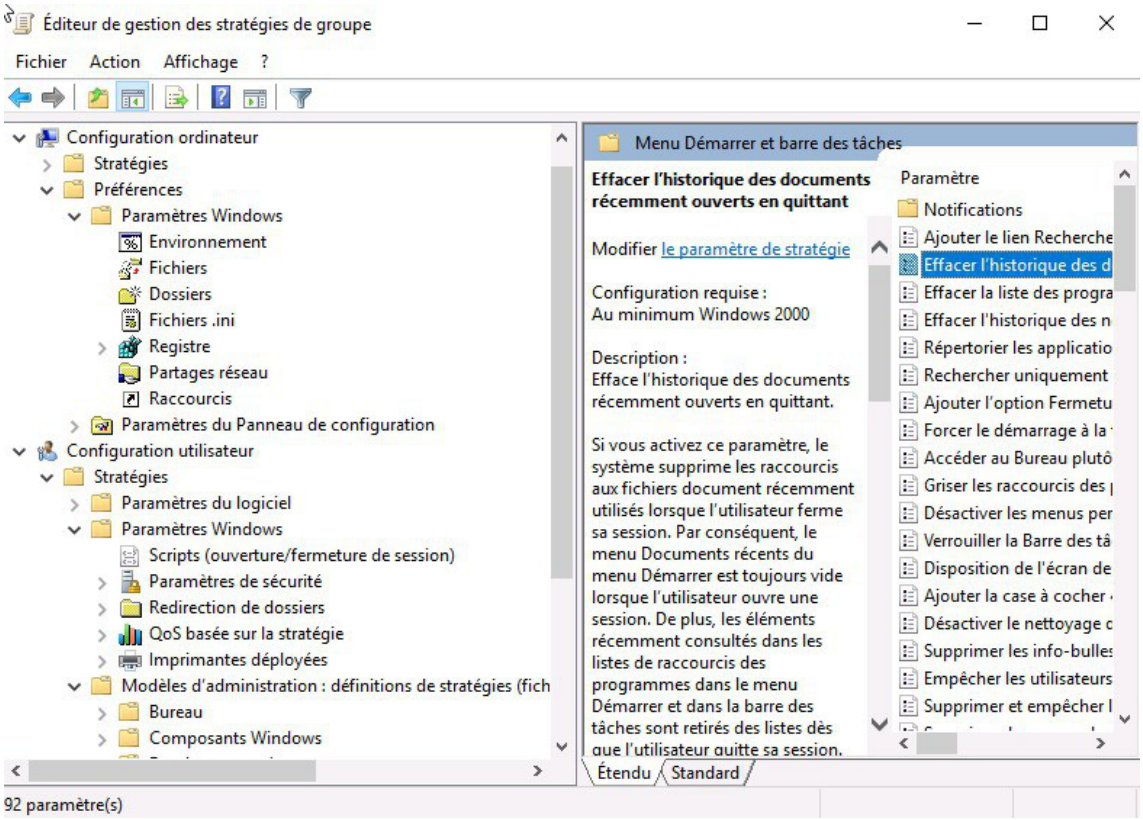
Enfin, on peut activer les fonctionnalités avancées de la console pour avoir accès à davantage de détails et de paramétrages possibles.



Accéder aux fonctionnalités avancées de la console

On peut maintenant administrer le serveur Seth comme n'importe quel serveur Active Directory, paramétrer des GPO par exemple :

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

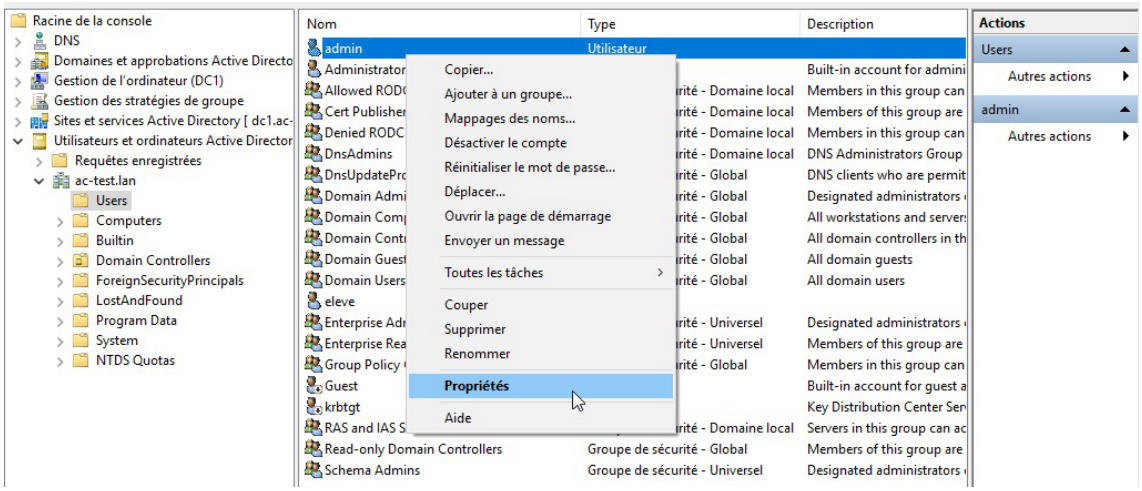


Administrer le serveur Seth

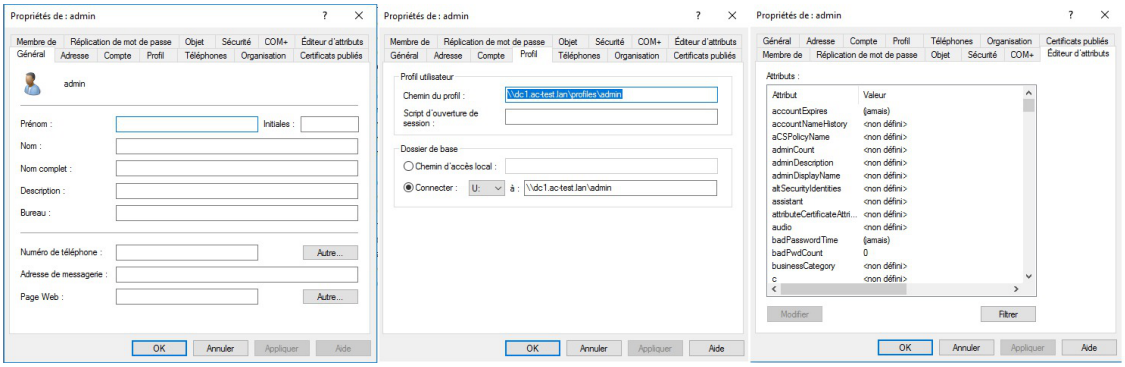
Édition des propriétés d'un utilisateur

Dans la console, aller dans : `Utilisateurs et ordinateurs Active Directory` → `<nom_du_domaine>` → `Users`.

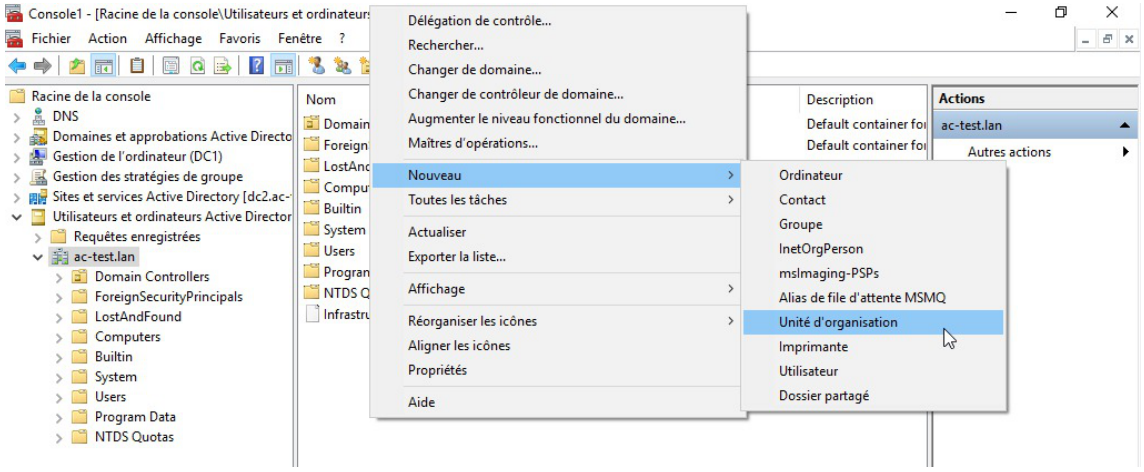
Faire un clic droit sur l'utilisateur et cliquer sur `Propriétés`.



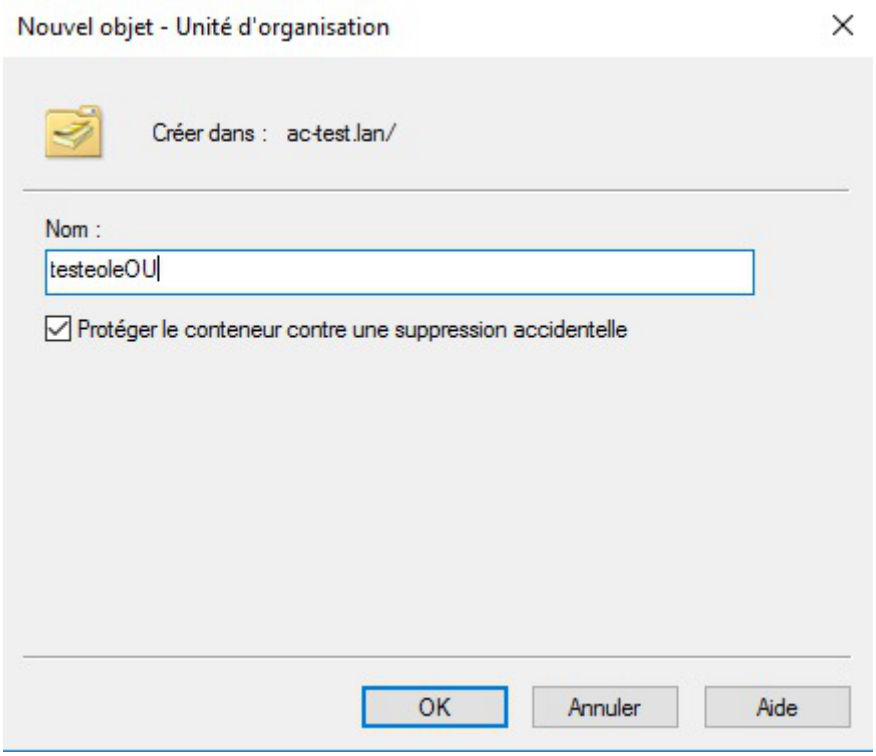
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Création d'une unité organisationnelle (OU)



Nouvelle unité d'organisation

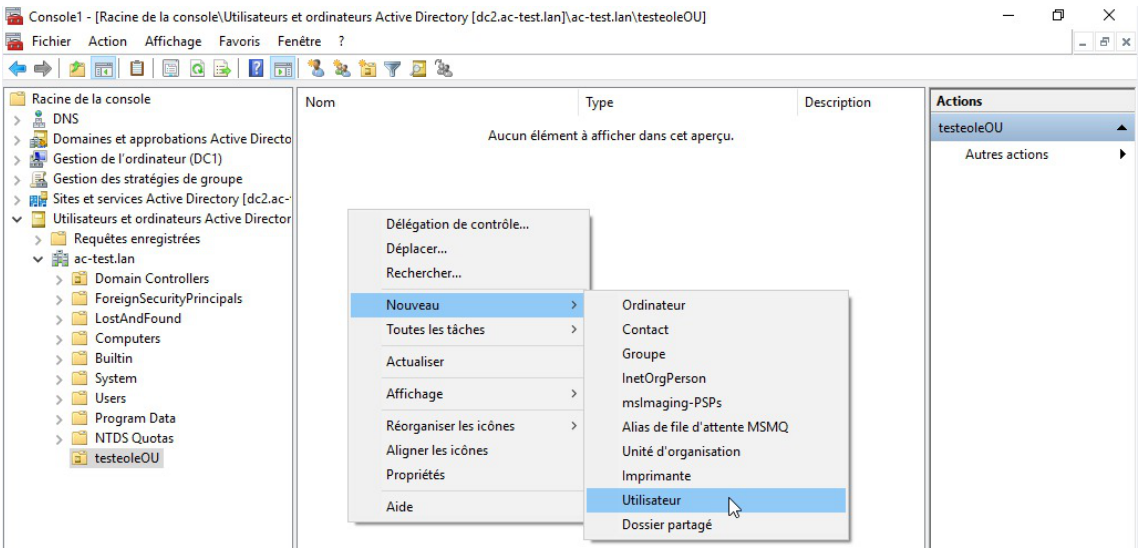


Nom de la nouvelle organisation

Ajout d'un utilisateur à l'unité organisationnelle

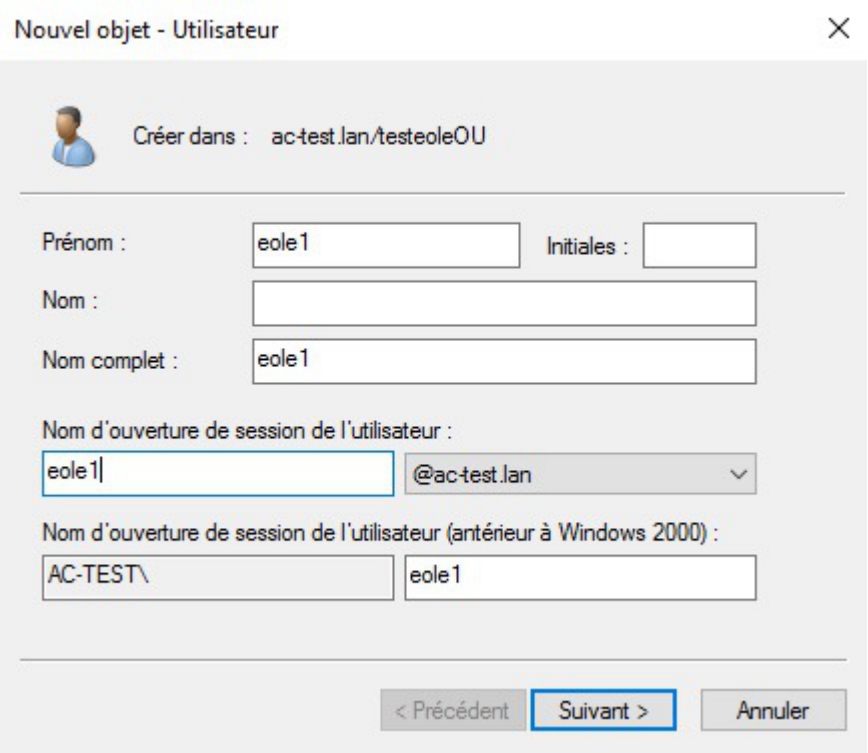
Créer un nouvel utilisateur dans la colonne `Actions`.

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



Nouvel utilisateur

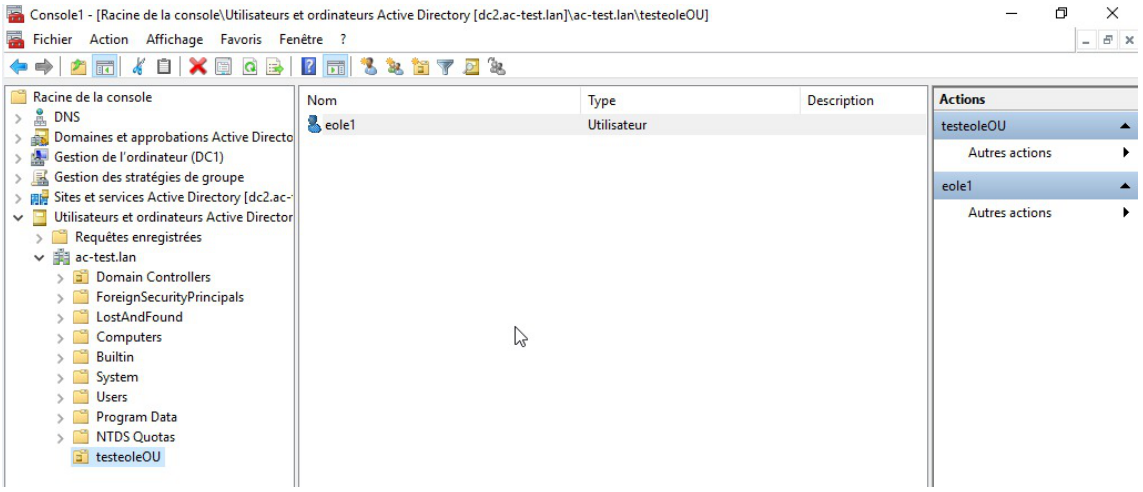
Donner un nom au nouvel utilisateur.



Nom du nouvel utilisateur

Le nouvel utilisateur apparaît dans la liste.

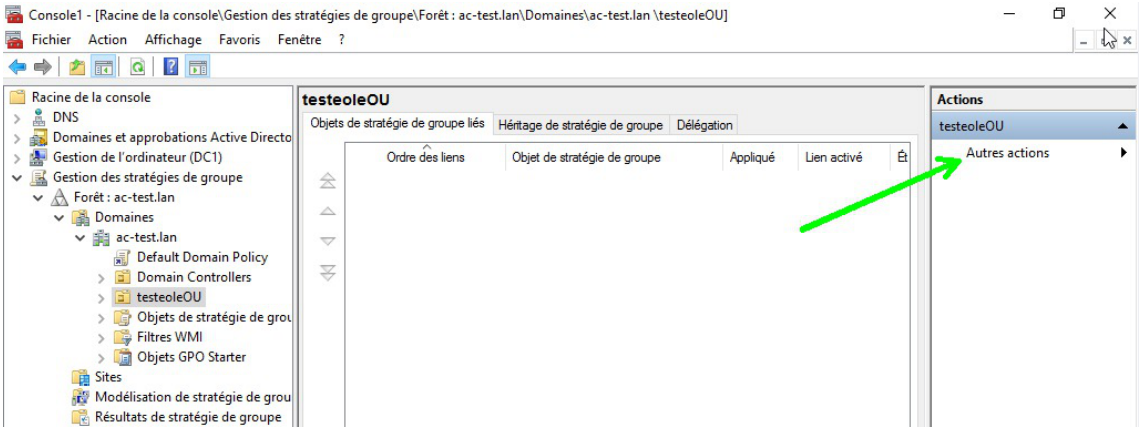
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Liste des utilisateurs

Création et affectation de la GPO

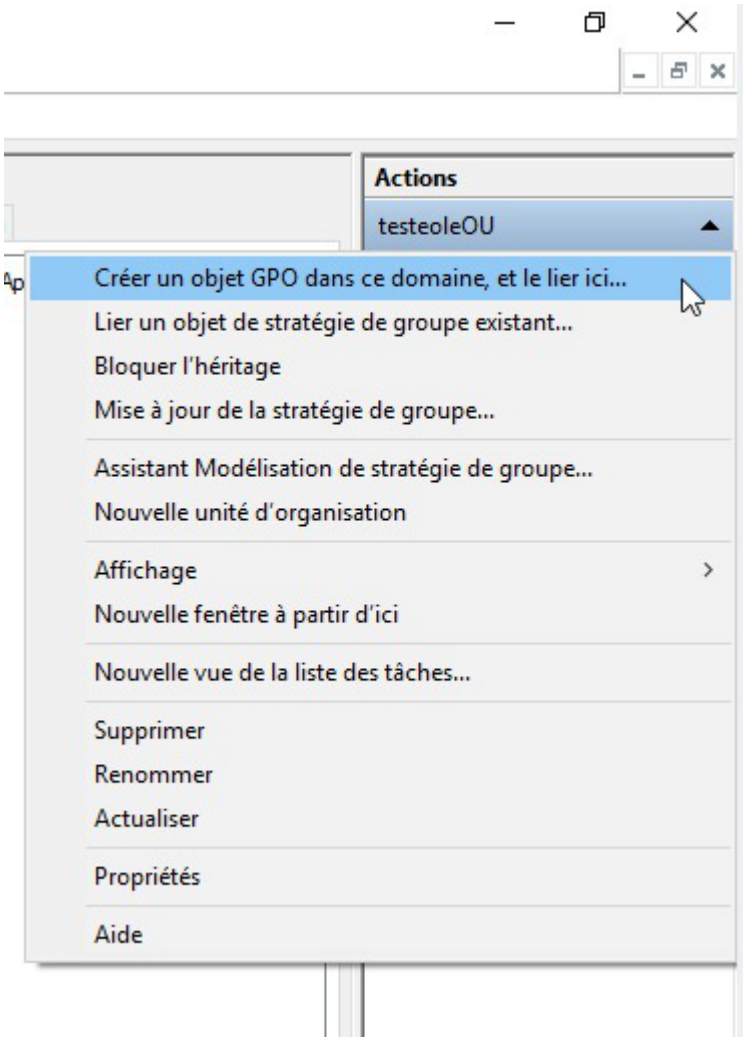
Dans `Gestion des stratégies de groupes`, développer l'arborescence jusqu'à l'unité organisationnelle précédemment créée.



Lister les actions possibles

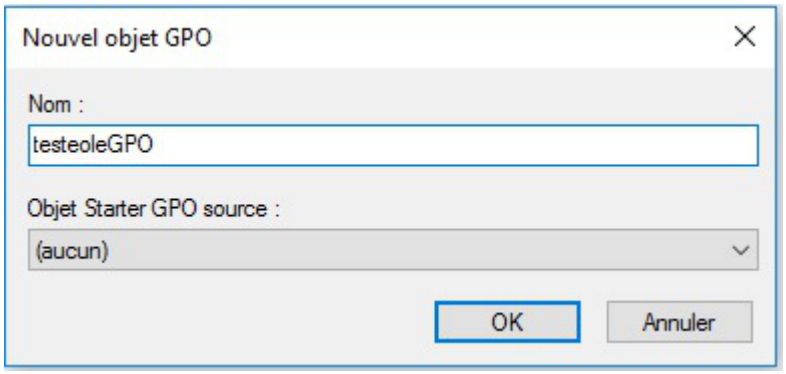
Créer un nouvel objet GPO.

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



Créer un objet GPO

Donner un nom au nouvel objet GPO.



Saisir le nom du nouvel objet GPO

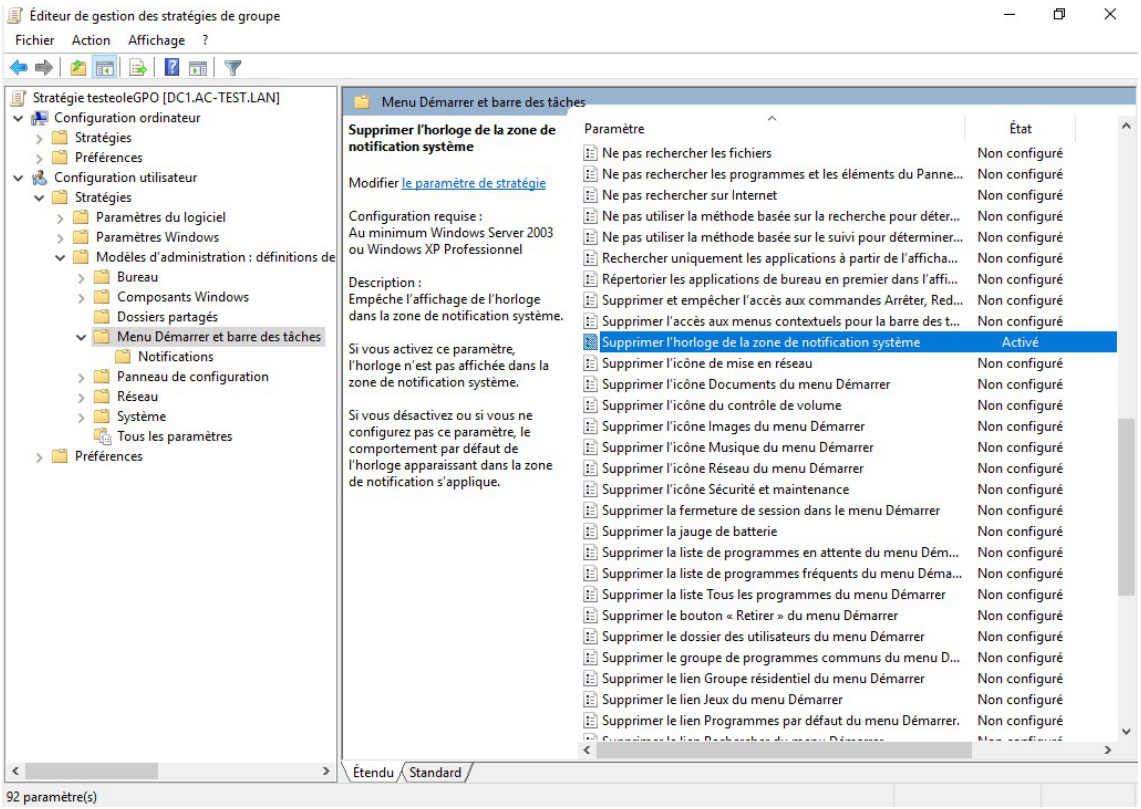
Modifier l'objet GPO nouvellement créé.

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



Modifier l'objet GPO

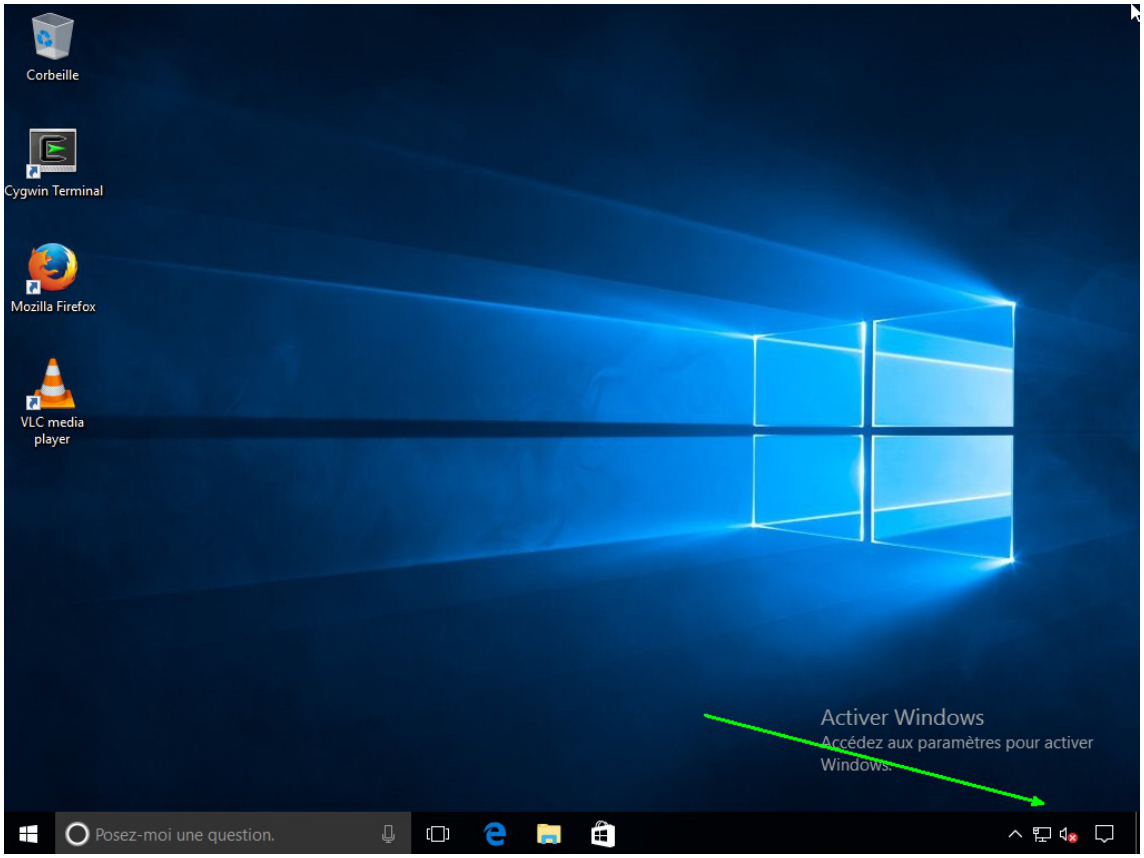
Sélectionner Supprimer l'horloge de la zone de notification système.



Gestion de stratégie de groupe

L'heure n'apparaît plus dans la barre des tâches.

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



Application de l'objet GPO

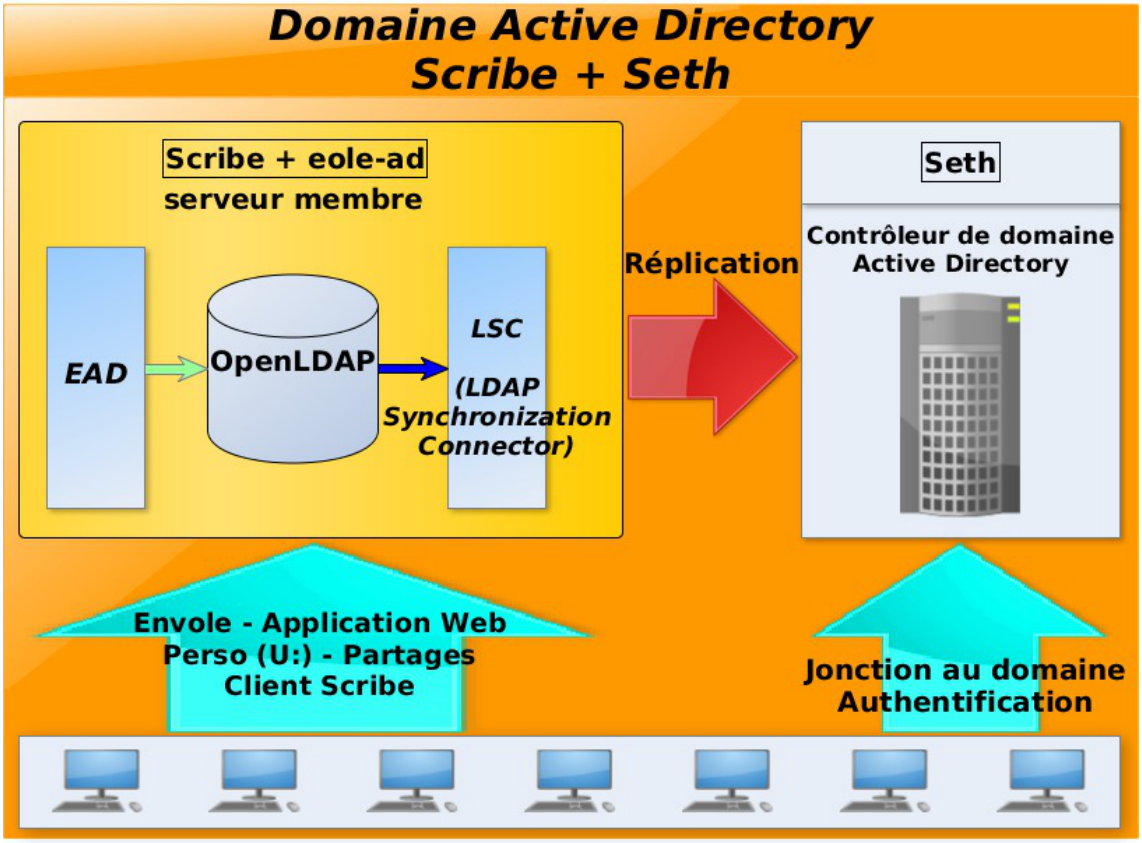
7. Intégration du serveur Scribe dans le domaine AD de Seth : Eole-AD

Initié à l'origine par la direction des lycées de la Région Rhône-Alpes, le projet Eole-AD est actuellement mis en œuvre dans l'académie de Poitiers et dans le département de la Savoie.

Eole-AD permet l'intégration d'un module Scribe à un domaine Active Directory[p.493] tout en conservant la gestion des utilisateurs et des groupes sur le module Scribe.

La version proposée sur EOLE 2.6.2 est compatible avec le module Seth 2.6 ou 2.7 basé sur Samba4. Elle est également compatible avec les serveurs Microsoft.

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



La mise en œuvre de cette fonctionnalité utilise le connecteur LSC[p.506] qui synchronise les identités entre un annuaire LDAP et d'autres sources de données comme n'importe quelle base de données pourvues d'un connecteur JDBC, un autre serveur LDAP, un fichier plat, une API REST…

https://lsc-project.org

Afin de pouvoir appliquer simplement certaines modifications spécifiques à EOLE, le service `lsc` original a été remplacé par le service systemd[p.519] personnalisé `eole-lsc`.

Pré-requis

Ce fonctionnement suppose :

- un module Scribe et un serveur Windows ;
- un module Scribe avec un module Seth : ce cas d'utilisation suppose que l'un des 2 modules ne soit pas déjà instancié. Principalement parce que le nom de domaine Samba ne peut pas être modifié une fois le serveur instancié. Le serveur Seth devra être instancié en premier.

Installation

L'installation du paquet `eole-ad` sur un module Scribe à jour active automatiquement la fonctionnalité :

```
# Maj-Auto
# apt-eole install eole-ad
```


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

Versions supportées

Le paquet `eole-ad` est disponible uniquement pour les versions 2.5.2 et 2.6.2 du module Scribe.

Il est possible de mettre en place la fonctionnalité Eole-AD sur un serveur Scribe existant mais les mots de passe n'étant synchronisés qu'au moment de leur modification, la ré-initialisation des mots de passe de tous les utilisateurs est nécessaire.

Configuration du module Amon

Résolution DNS

Pour la résolution DNS il faut ajouter l'adresse IP du module Seth comme serveur DNS à la liste d'adresses déjà déclarées, dans l'onglet `Général` → `Paramètres réseau globaux` → `Adresse IP du serveur DNS`.

L'ordre à une importance, l'adresse saisie en dernier peut être passée devant à l'aide du bouton .

La configuration doit être appliquée à l'aide de la commande `reconfigure`.

Configuration du module Scribe non instancié

Dans l'interface de configuration du module un certain nombre de variables doivent être renseignées et ce dans plusieurs onglets.

Onglet Général

Dans l'onglet `Général` le `Nom DNS du réseau local` doit correspondre au nom du domaine Active Directory (realm[p.515]) du serveur Active Directory.

Il est recommandé de déclarer le serveur Active Directory en tant que serveur NTP, saisir l'adresse IP ou le nom d'hôte dans le champ `Adresse du serveur NTP`.

Pour une utilisation avec le module Seth, la valeur du nom de domaine Active Directory peut se retrouver dans l'interface de configuration du module Seth → onglet `Active Directory` (mode Debug activé) → variable `Nom complet du domaine racine de la forêt`.



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

Consultation du realm sur un module Seth

Onglet Samba

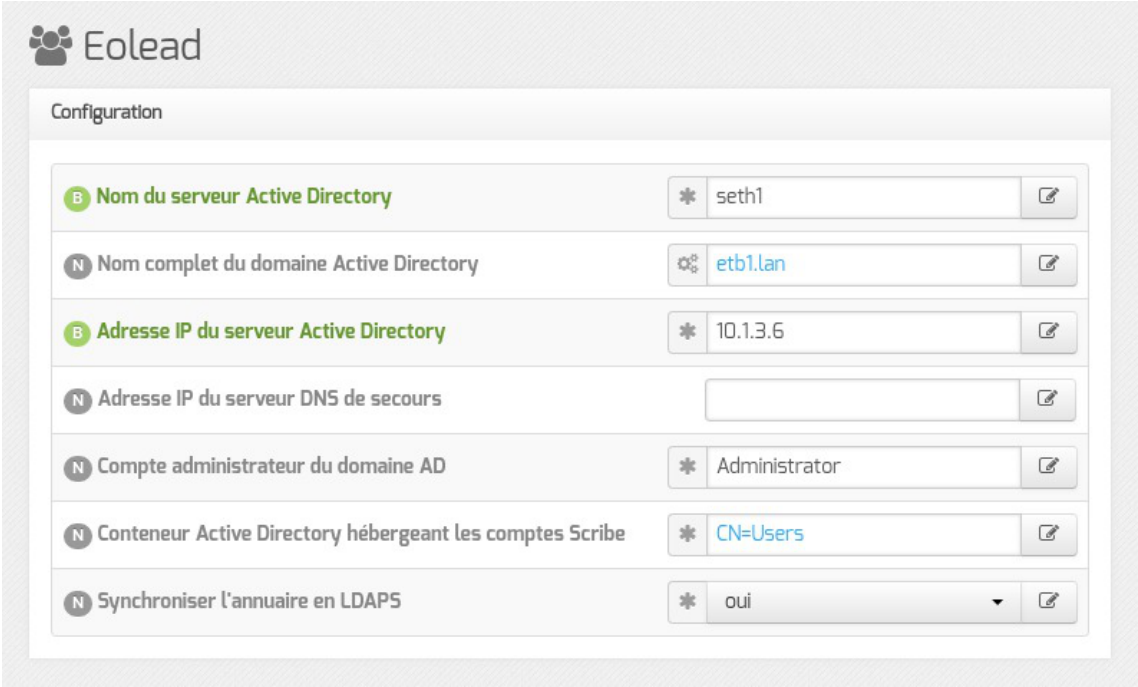
Le `Nom du domaine Samba (ex: mondomaine)` doit correspondre au nom du domaine Windows.

Pour une utilisation avec le module Seth, la valeur du nom de domaine Windows se retrouve dans l'interface de configuration du module dans l'onglet `Active Directory` instancié en activant le mode Debug.



Consultation du nom de domaine sur un module Seth

Onglet Eolead



- `Nom du serveur Active Directory` : doit correspondre au nom de la machine Active Directory ;
- `Nom du domaine Active Directory` : doit correspondre au nom du domaine Active Directory, il est pré-renseigné à partir du nom saisi dans l'onglet `Général` ;
- `Adresse IP du serveur Active Directory` : doit contenir l'adresse IP du serveur Active Directory ;
- `Adresse IP du serveur DNS de secours` : cette valeur est facultative ;

Dans le cas où une architecture de haute disponibilité de l'Active Directory a été mise en place, il est

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

recommandé d'y renseigner l'adresse du second serveur AD ;

- `Compte administrateur du domaine AD` : doit correspondre à un compte ayant les droits Administrateur du domaine, en général le compte `Administrateur` ou `Administrator` (dans le cas d'un module Seth);
- `Conteneur Active Directory hébergeant les comptes Scribe` : les comptes de l'annuaire du module Scribe sont répliqués par défaut dans le conteneur Active Directory *CN=Users*. Cette variable permet de personnaliser le conteneur hébergeant les comptes du module Scribe (exemple : *OU=Scribe*). En cas de personnalisation du conteneur, ne pas oublier de créer ce dernier dans Active Directory avant d'instancier le module Scribe ;
- `Synchroniser l'annuaire en LDAPS` : la synchronisation des comptes en LDAPS est plus sécurisée mais nécessite l'enregistrement des certificats d'autorité du serveur AD dans un fichier Java keystore[p.505].

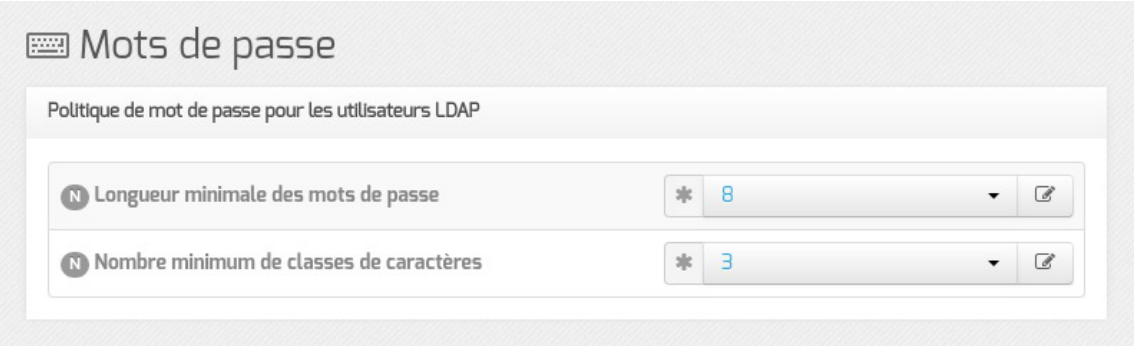
L'utilisation du protocole LDAPS est obligatoire dans le cas de synchronisation vers un module Seth.

L'utilisation du protocole LDAPS pour synchroniser l'annuaire apporte plus de sécurité et s'avère une obligation dans certaines infrastructures.

En contrepartie, elle nécessite l'enregistrement des certificats d'autorité du serveur AD dans un fichier Java keystore[p.505] avant l'instance.

Onglet Mots de passe

La politique de sécurité définie dans l'onglet `Mots de passe` doit être en accord avec celle du serveur Active Directory.



Onglet Dhcp

Il faut configurer le `Nom de domaine à renvoyer aux clients DHCP` en mettant la valeur du `Nom DNS du réseau local` du serveur faisant office d'Active Directory, onglet `Général` dans le cas de l'utilisation du module Seth.

Il faut également configurer l'`Adresse IP du DNS à renvoyer aux clients DHCP` en mettant l'adresse IP du module Seth dans le cas de l'utilisation de Seth/Samba4 ou l'adresse du serveur

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

Windows dans le cas de l'utilisation de Microsoft AD.

Enregistrement des certificats d'autorité

Si la synchronisation de l'annuaire est configurée pour utiliser le protocole LDAPS, il est impératif d'enregistrer les certificats d'autorité du serveur AD dans le fichier Java keystore[p.505] par défaut du module Scribe.

Chaîne de certificats sous Seth/Samba4

Chaîne de certificats sous Seth/Samba4

Sur un module EOLE Seth instancié, le fichier contenant la chaîne de certificats est le suivant : `/var/lib/samba/private/tls/ca.pem`.

Intégrer la CA du module Seth au Java Keystore

```
root@scribe:~# scp root@seth:/var/lib/samba/private/tls/ca.pem /root/
root@scribe:~# keytool -import -trustcacerts -keystore /etc/ssl/certs/java/cacerts -storepass changeit -noprompt -alias eole-ad -file /root/ca.pem
```

La commande suivante permet d'afficher le contenu du fichier :

```
# openssl x509 -in /root/ca.pem -text
```

Chaîne de certificats sous Microsoft AD

Pour créer la chaîne de certificats, il est possible de suivre la procédure décrite dans : https://www.ltb-project.org/documentation/active_directory_certificates.html

Intégrer la CA au Java Keystore

Une fois le fichier copié sur le serveur Scribe (exemple : `/tmp/certificate.pem`), il faut l'ajouter dans le fichier Java keystore à l'aide de la commande suivante :

```
# keytool -import -trustcacerts -keystore /etc/ssl/certs/java/cacerts -storepass changeit -noprompt -alias eole-ad -file /tmp/certificate.pem
Certificat ajouté au fichier de clés
```

La commande suivante permet d'afficher le contenu du fichier :

```
# openssl x509 -in /tmp/certificate.pem -text
```

Instanciation

Une fois la configuration enregistrée, il faut instancier le module Scribe à l'aide de la commande `instance`.

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

Spécificités de l'instanciation en mode Eole-AD

Au cours de l'instance, vous seront demandés :

- le mot de passe de l'utilisateur `admin` (du serveur Scribe) : il sera ré-initialisé par la suite ;
- le mot de passe de l'administrateur `Active Directory` : il est requis pour la jonction au domaine KERBEROS et la réplication de l'annuaire Scribe vers AD.



> Une mauvaise saisie de la clef secrète de l'administrateur de l'Active Directory rend inopérant la synchronisation des données et relancer l'instance ne permet plus de saisir la clef secrète.
>
> Il faut supprimer le fichier `/root/.eolead` et relancer l'instanciation.

Messages d'avertissement sans conséquence

Lors de l'instance, plusieurs messages d'erreur sont susceptibles d'apparaître.

Certains sont déjà connus dans le cadre du projet Eole-AD et peuvent être ignorés car sans conséquence.

```
run-parts: executing /usr/share/eole/posttemplate/04-fichier instance
Restart System V service nscd
Stop System V service nscd [ OK ]
Start System V service nscd [ OK ]
Erreur : Unable to bind to ldaps://etb1.lan with CN=Administrator,CN=Users,DC=etb1
,DC=lan (80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error,
data 52e, v1db1)
```

```
Intégration au domaine Active Directory
Mot de passe de l'administrateur Active Directory :
Password for Administrator@ETB1.LAN:
Failed to join domain: failed to lookup DC info for domain 'ETB1.LAN' over rpc:
Undetermined error
```

Si on relance la commande `instance` ou `reconfigure`, on obtient les messages suivant :

```
ATTENTION : plusieurs sambaDomainName détectés !
Des dysfonctionnements sont possibles sur ce serveur
```

Cependant, la présence des deux entrées *sambaDomainName* ne semble pas entraîner d'effet de bord.

Postes clients

Sur le serveur Active Directory, ajouter l'utilisateur `admin` au groupe des `Administrateurs du domaine` (Admins du domaine).

Les stations peuvent être intégrées au domaine avec le compte `admin` et/ou le compte `Administrateur` du serveur Active Directory.

Le nom de domaine à saisir lors de la jonction au domaine est le nom du domaine Active Directory (FQDN).

En se connectant avec l'utilisateur `admin` (U:\ doit pointer vers Scribe), il est possible d'installer le client Scribe.

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

Une fois le client Scribe installé, les utilisateurs du domaine voient leurs montages Scribe et les règles définies dans les modèles ESU sont appliquées.

Gestion des utilisateurs

L'importation, la gestion des utilisateurs, des groupes et des mots de passe au travers de l'interface EAD du module Scribe est totalement fonctionnelle.

Trucs & astuces

Synchronisation

Forcer la synchronisation manuelle des comptes depuis le module Scribe :

```
# /usr/bin/lsc -f /etc/lsc -s all -c all -t 1
```

Changement de mot de passe

Forcer le changement de mot de passe d'un utilisateur (exemple avec l'utilisateur `admin`) depuis le module Scribe :

```
# changepasswordeole.pl admin Eole123$
```

Si la commande échoue avec le message suivant, vérifier que le mot de passe proposé respecte la politique de sécurité mise en place sur le serveur AD :

```
Unable to modify unicodePwd for CN=user11,CN=Users,DC=domaine,DC=lan
(0000052D: SvcErr: DSID-031A0FC0, problem 5003 (WILL_NOT_PERFORM), data 0)
```

Liste d'utilisateurs

Lister tous les utilisateurs depuis le module Seth :

```
# ldbsearch -H /var/lib/samba/private/sam.ldb -S '(objectclass=user)' cn | grep ^cn:
```

Attributs utilisateur

Chercher un utilisateur depuis le module Seth :

```
# ldbsearch -H /var/lib/samba/private/sam.ldb -S cn=p.nom
```

Configuration du serveur AD

Installer un serveur Active Directory avec les rôles suivants :

- serveur DNS
- Services de domaine Active Directory
- Services de certificats Active Directory
- La commande `dcpromo` permet de lancer l'assistant adéquat
- Pour activer le services de certificats sur un serveur 2003, aller dans `Panneau de configuration` → `Ajout/Suppression de programmes` → `Ajouter/Supprimer des composants Windows` puis cocher :
  - Serveur d'applications → IIS
  - Services de certificats

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

Journaux

Les journaux sont disponibles dans `/var/log/lsc/`.

8. Diagnose

La commande `diagnose` permet d'afficher des informations sur l'état des services du serveur Seth.



Module Seth

Résultat de la commande diagnose sur un module Seth

```
*** Serveur Active Directory
Test du fichier de configuration :
. Syntaxe => Ok
Resolution  DNS :
. Syntaxe => Ok
. DNS AD => Ok
Réplication :
. => Actif
```


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.504].

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.510].

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.513].

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.493] 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.513] 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.501].

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.498] local et/ou d'un serveur PXE[p.514].

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.510] (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.510], 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.522]).

Le logiciel utilisé, Nginx[p.510], 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.517] Exim[p.501].

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.513] / IMAP[p.504].

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.518] : proxy cache ;
- e2guardian[p.500] : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM[p.511] ou Kerberos[p.505].

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.514].

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.506].

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.519].

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.495].

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.499] local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.495].

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.498].

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.514].

Logiciels et services

Le paquet `eole-ltsp-server` s'appuie sur les service NBD[p.510] et LDM[p.506].

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.517].

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.503].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync[p.497].

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.517].

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.515].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.519].

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.498] 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.513]** : permet de modifier un template[p.520] fourni par EOLE ;
- le **dictionnaire[p.498] 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.520] 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*.

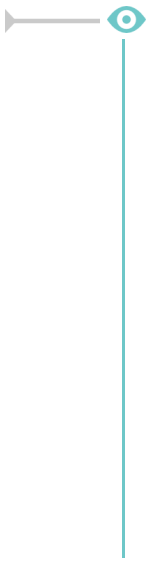
2.2. Création de patch Creole

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
```

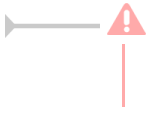
Exécution de la commande `gen_patch` :

```
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.520] 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.499] :
> 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 [p.243]

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.

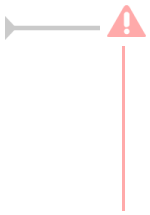
Les services à activer/désactiver se définissent dans le dictionnaire grâce à la balise **<service>.**

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.

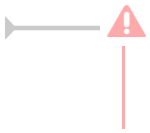
La balise service peut également être utilisée pour activer/désactiver des configurations de site web apache2 (commandes : `a2ensite` / `a2dissite`).

Comme pour les services système, l'activation d'un site peut être conditionnée par une `servicelist`.

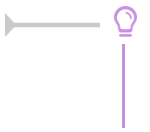
On peut ainsi gérer le lien symbolique suivant : `/etc/apache2/sites-enabled/monsite` avec :

```
<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.520] 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.61]

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 choisi 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.

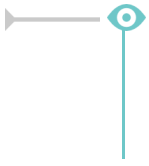
Les variables non obligatoires (`mandatory='False'`) possédant une valeur par défaut (balise `<value>`) deviennent obligatoires.

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.520] ;
- 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>
```

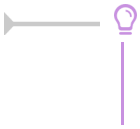
  Il est possible d'utiliser des *calc_multi_condition* avec des variables non déclarées ou désactivées mais uniquement si toutes les variables testent la même condition.

  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 :

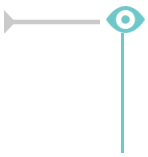
- des fonctions natives de Tiramisu[p.520] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

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.

```
<condition name='mandatory_if_not_in' source='mode_zephir'>
    <param>non</param>
    <target type='variable'>nom_carte_eth0</target>
    <target type='variable'>nom_zone_eth0</target>
</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.501].

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.420]

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.505].



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.497] ;
- `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 :

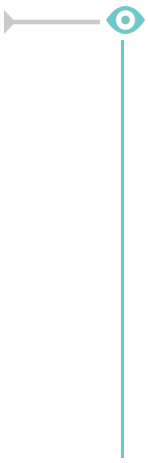
- d'instancier un seule template existant sur le module en utilisant la ou les destinations déclarées dans le dictionnaire :
  `# CreoleCat -t hostname`
- d'instancier un template existant sur le module en redirigeant le résultat dans un fichier spécifique :
  `# CreoleCat -t hostname -o /tmp/hostname.txt`
- 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.498].

- `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.497].

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.513] 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.521], 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.427]

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.427]

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

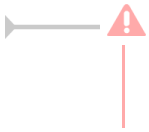


La commande `uname -r` permet de connaître le noyau en cours d'utilisation.

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.520].

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est cron[p.498] qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bareos[p.495] 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.522] (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.498] 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.520] 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.386]

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.508] (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.498]) 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.501]) :

- **<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) :

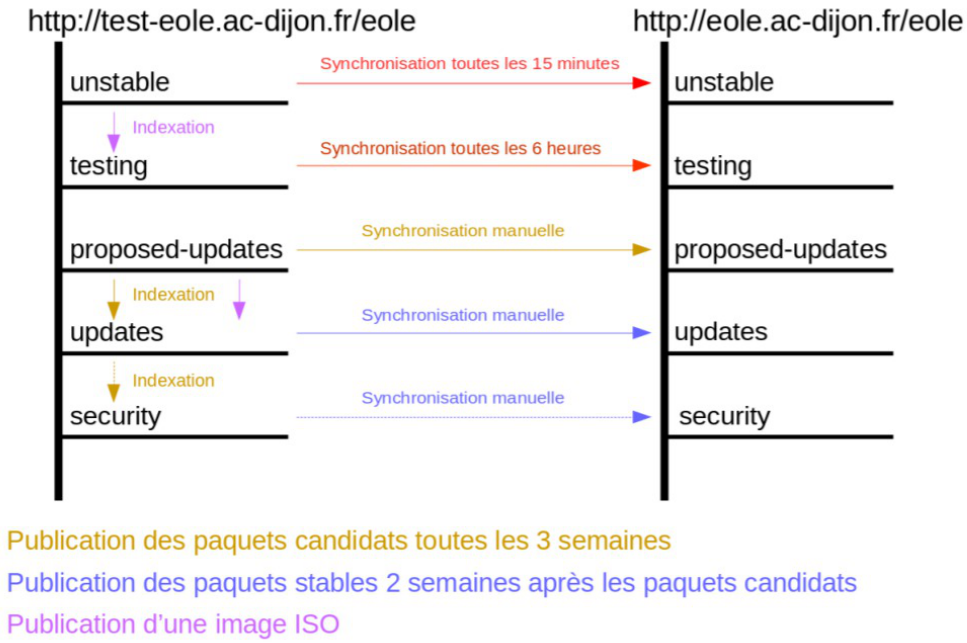
- **eole-2.6-unstable** : paquets de développement pouvant contenir des évolutions fonctionnelles, des corrections de sécurité ou de dysfonctionnement ;
- **eole-2.6-testing** : paquets candidats (correspondant aux images RC de la distribution) qui sont éligibles pour passer en version stable après validation ;
- **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.494] (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.502] 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.494] 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

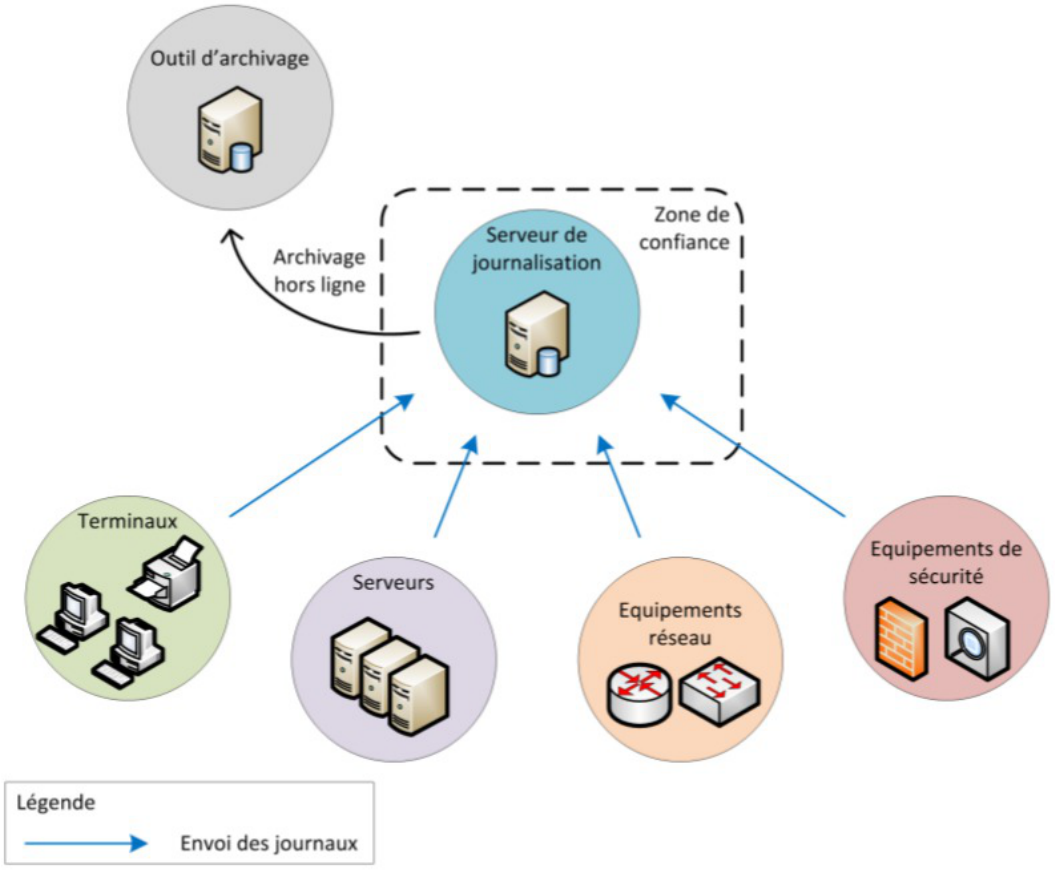
- l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux doit être prise

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

en compte dans le dimensionnement des équipements,

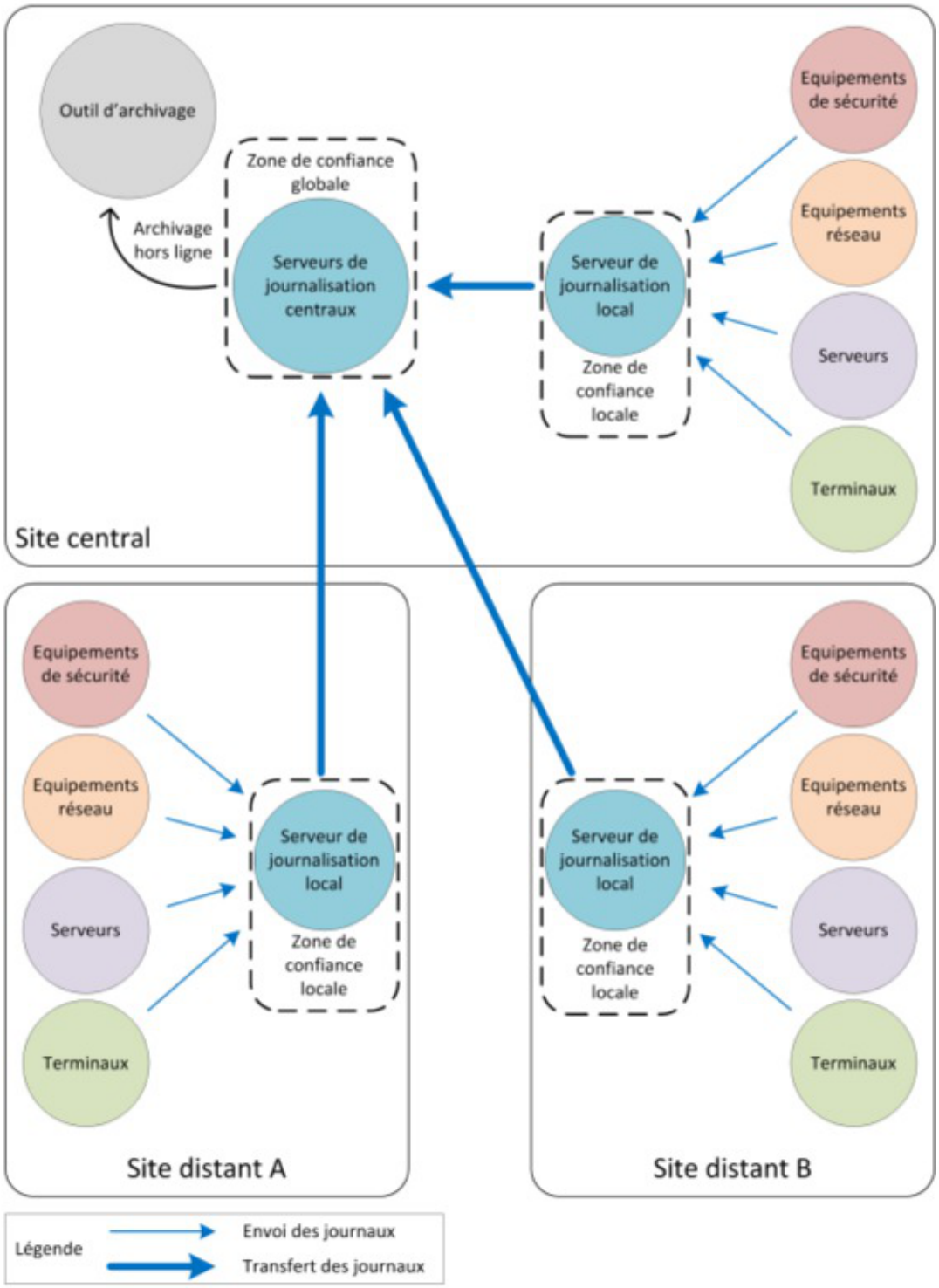
Recommandations d'architecture et de conception

- 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 Seth

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-ad-dc

Le paquet `eole-ad-dc` permet la mise en place d'un serveur Samba Active Directory[p.493] 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).

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

1.2. eole-dhcp

Le paquet `eole-dhcp` permet la mise en place d'un serveur DHCP[p.498] local et/ou d'un serveur PXE[p.514].

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.

1.3. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP[p.517] Exim[p.501].

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.

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

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. 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-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.
Le logiciel utilisé, Nginx[p.510], 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

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

Le service s'installe sur le système hôte (maître).

2. Ports utilisés sur le module Seth

Le module Seth propose quelques services.
Ce document donne la liste exhaustive des ports utilisés sur un module Seth standard.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.
Il est possible de lister les ports ouverts sur le serveur par la commande :
`netstat -ntulp`



En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 25/tcp : smtp (Exim4)
- 68/udp : dhclient
- 123/udp : ntpd
- 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)

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

Ports spécifiques au module Seth

- 53/tcp+udp : DNS
- 88/tcp+udp : Kerberos
- 135/tcp : End Point Mapper
- 389/tcp+udp : LDAP
- 445/tcp : SMB
- 464/tcp+udp : Kerberos kpasswd
- 636/tcp : LDAPS
- 647/tcp : failover DHCP, port en écoute sur le serveur primaire et port d'émission pour le serveur secondaire
- 847/tcp : failover DHCP, port en émission sur le serveur primaire et port d'écoute pour le serveur secondaire
- 3268/tcp : Global Catalog
- 3269/tcp : Global Catalog SSL
- 7911/tcp : API OMAPI (configuration du DHCP)

Sur un module Seth, les services historiques NetBIOS[p.510] (ports 137 à 139) sont désactivés par défaut.

Si le serveur est configuré en tant que membre d'un domaine existant, seul le port 445 est en écoute.

Liste complète des ports Active Directory sur le Wiki Samba

- liste des ports pour un contrôleur de domaine : https://wiki.samba.org/index.php/Samba_AD_DC_Port_Usage
- liste des ports pour un serveur membre : https://wiki.samba.org/index.php/Samba_Domain_Member_Port_Usage

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. Administration avancée du module Seth

Interroger Winbind

Les commandes Winbind[p.522] permettent d'interroger l'annuaire Active Directory que le serveur soit

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

contrôleur de domaine ou simplement membre d'un domaine existant.

- Lister les utilisateurs du domaine

  `# wbinfo -u`
- Lister les groupes

  `# wbinfo -g`
- Voir les informations d'un utilisateur

  `# wbinfo -i admin`
- Obtenir le SID d'un utilisateur

  `# wbinfo --name-to-sid=admin`
- Vérifier la validé de la clé partagée

  `# wbinfo -t`

Et plein d'autres fonctionnalités...

`# wbinfo --help`

et

`# man wbinfo`

Personnaliser les restrictions sur les mots de passe

La commande `samba-tool domain passwordsettings show` permet de connaître les règles de complexité mises en place sur les mots de passe.

```
root@dc1:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=ac-test,DC=fr'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Toutes les règles de complexité peuvent être adaptées à l'aide de cette même commande.

Taille/longueur de l'historique des mots de passe

Nombre de mots de passe sont enregistrés pour que l'utilisateur ne puisse pas les ré-utiliser. Devrait-être combiné avec "min-pwd-age > 0" sinon un utilisateur peut changer de mot de passe autant de fois que nécessaire pour enlever son mot de passe de l'historique et le ré-utiliser.

`# samba-tool domain passwordsettings set --history-length=0`

Longueur minimum du mot de passe

Nombre de caractères minimum que doit faire un mot de passe.

`# samba-tool domain passwordsettings set --min-pwd-length 5`

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

Âge minimal du mot de passe en jours

Nombre de jours que doit attendre un utilisateur (même membre du groupe `DomainAdmins`), pour pouvoir changer à nouveau son mot de passe.

```
# samba-tool domain passwordsettings set --min-pwd-age 0
```

Âge maximal du mot de passe en jours

Nombre de jours après lequel le système demandera à un utilisateur de changer son mot de passe (0=désactivé).

```
# samba-tool domain passwordsettings set --max-pwd-age 365
```

Durée du verrouillage des comptes bloqués

Durée en minutes pendant laquelle un compte ayant effectué trop de tentatives d'ouverture de sessions infructueuses est bloqué.

```
# samba-tool domain passwordsettings set --account-lockout-duration 10
```

Nombre de tentative avant blocage d'un compte

Nombre de mauvais mots de passe qu'un utilisateur peut entrer avant que son compte soit bloqué.

```
# samba-tool domain passwordsettings set --account-lockout-threshold 3
```

Délai de réinitialisation du système de blocage de compte

Délai en minutes après lequel le comptage de tentatives d'ouverture de sessions infructueuses est réinitialisé, ce délai commence après la dernière tentative infructueuse.

```
# samba-tool domain passwordsettings set --reset-account-lockout-after 10
```



La commande suivante permet de désactiver intégralement les règles appliquées sur les mots de passe ce qui est évidemment non recommandé sur un serveur en production :

```
# samba-tool domain passwordsettings set --complexity=off
```

Gérer des rôles Active Directory

Les rôles Active Directory ou types de Maître d'opérations[p.508] (ex : FSMO[p.508]) sont des rôles nécessitant un maître unique pour la réplication entre contrôleurs de domaine.

La commande `samba-tool fsmo show` permet de connaître la façon dont sont répartis les rôles entre les différents contrôleurs de domaine.

```
root@dc1:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
InfrastructureMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
RidAllocationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
DomainNamingMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
```


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

```
8 ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=DC1,CN=Servers,CN=
  Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ac-test,DC=fr
```

La commande `samba-tool fsmo` est ses options permet de gérer les rôles Active Directory.

Vérification de l'état du serveur

Vérifier/réinitialiser les droits appliqués sur le répertoire SYSVOL

Certains dysfonctionnements sont causés par des problèmes de droits d'accès au répertoire SYSVOL.

Les commandes suivantes permettent pour l'une de vérifier et pour l'autre de réinitialiser les droits particuliers sur ce répertoire.

- `# samba-tool ntacl sysvolcheck`
- `# samba-tool ntacl sysvolreset`

Surveiller l'état de la réplication

Dans le cas de la mise en place d'une architecture multi-DC[p.510], la commande suivante permet de vérifier l'état de la réplication Active Directory :

```
# samba-tool drs showrepl
```

La commande `samba-tool drs` et ses options permet de gérer le service de réplication Active Directory.

4. Gestion des clients à l'aide de SaltStack

SaltStack est un logiciel de gestion de configuration écrit en Python, fonctionnant sur le principe client-serveur.

https://saltstack.com/

La partie cliente, salt-minion est à installer sur le poste Windows. Il est alors possible de gérer la station à distance grâce aux nombreux modules fournis par salt-minion.

https://docs.saltstack.com/en/latest/topics/installation/windows.html

Le serveur salt-master est indépendant du contrôleur de domaine, il peut être installé sur un serveur tiers. Il est disponible sur le module Seth.

Joindre une station au domaine

```
# salt 'PC-124784.ac-test.fr' system.join_domain domain='etb1.lan'
username='admin' password='eole' account_exists=False restart=True
```

Lister toutes les GPO d'une station

```
# salt 'PC-124784.ac-test.fr' lgpo.get machine
return_full_policy_names=True
```


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.521] 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` :

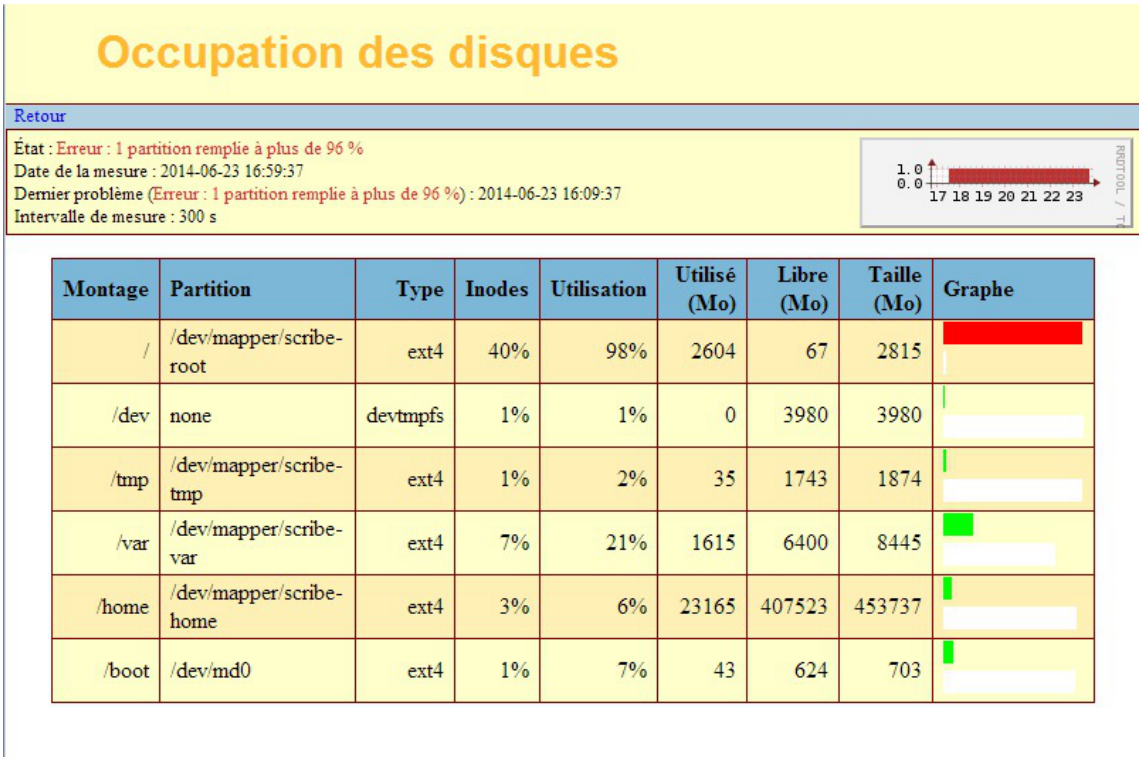
```
# mount /var/home
```



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

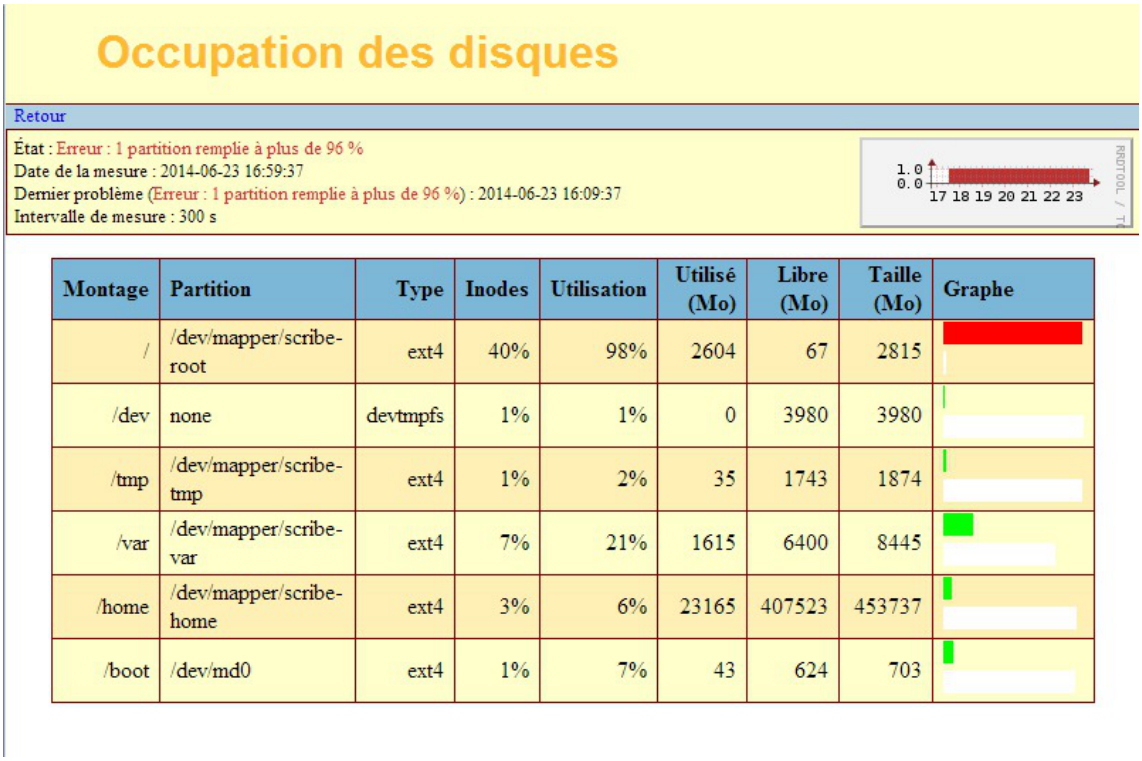
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	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 / TO

Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

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. 508]).

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. 508]).

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

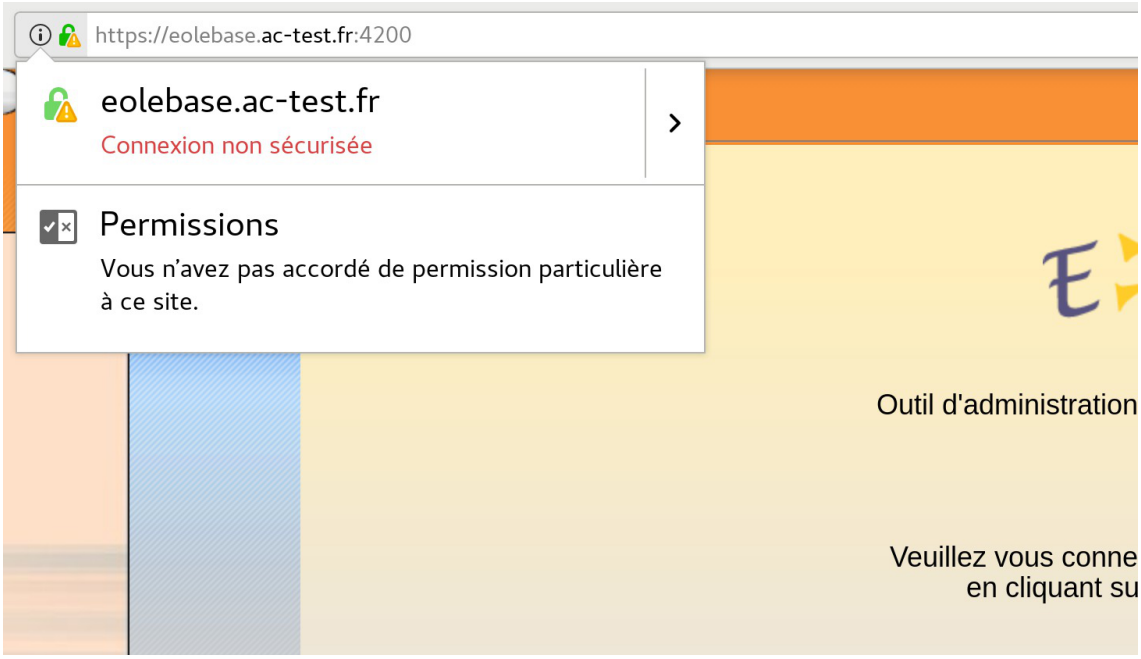
Pour avoir accès à l'EAD il faut impérativement que le nom de domaine soit présent dans le certificat SSL.

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.

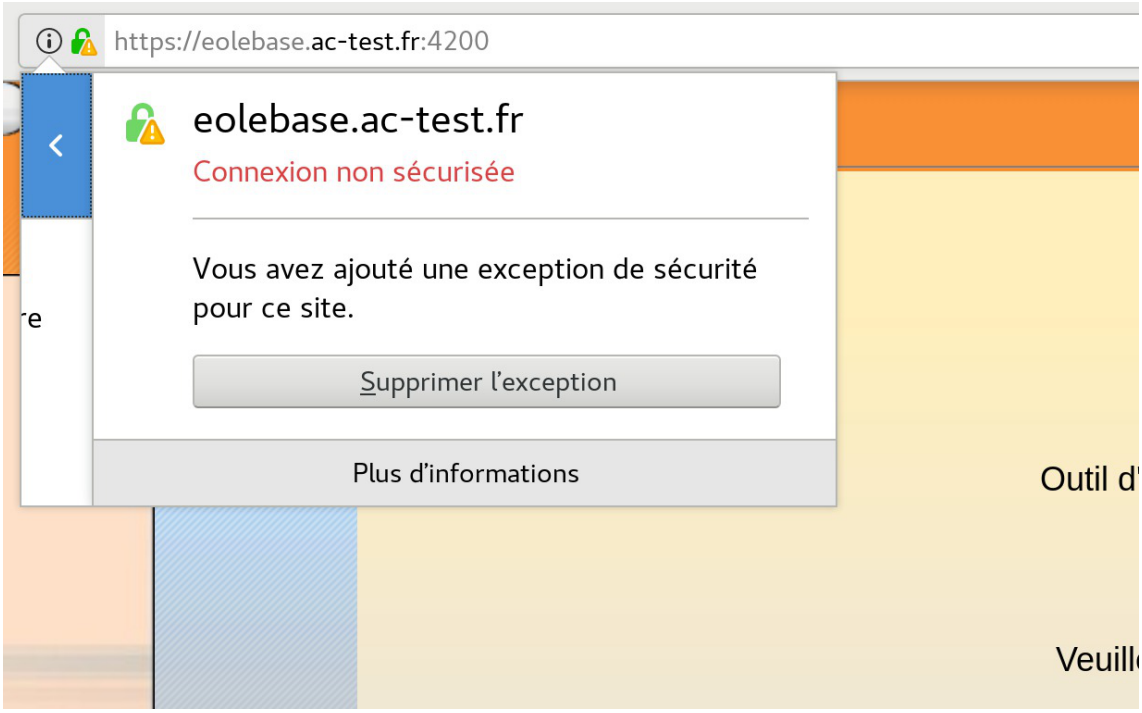
Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

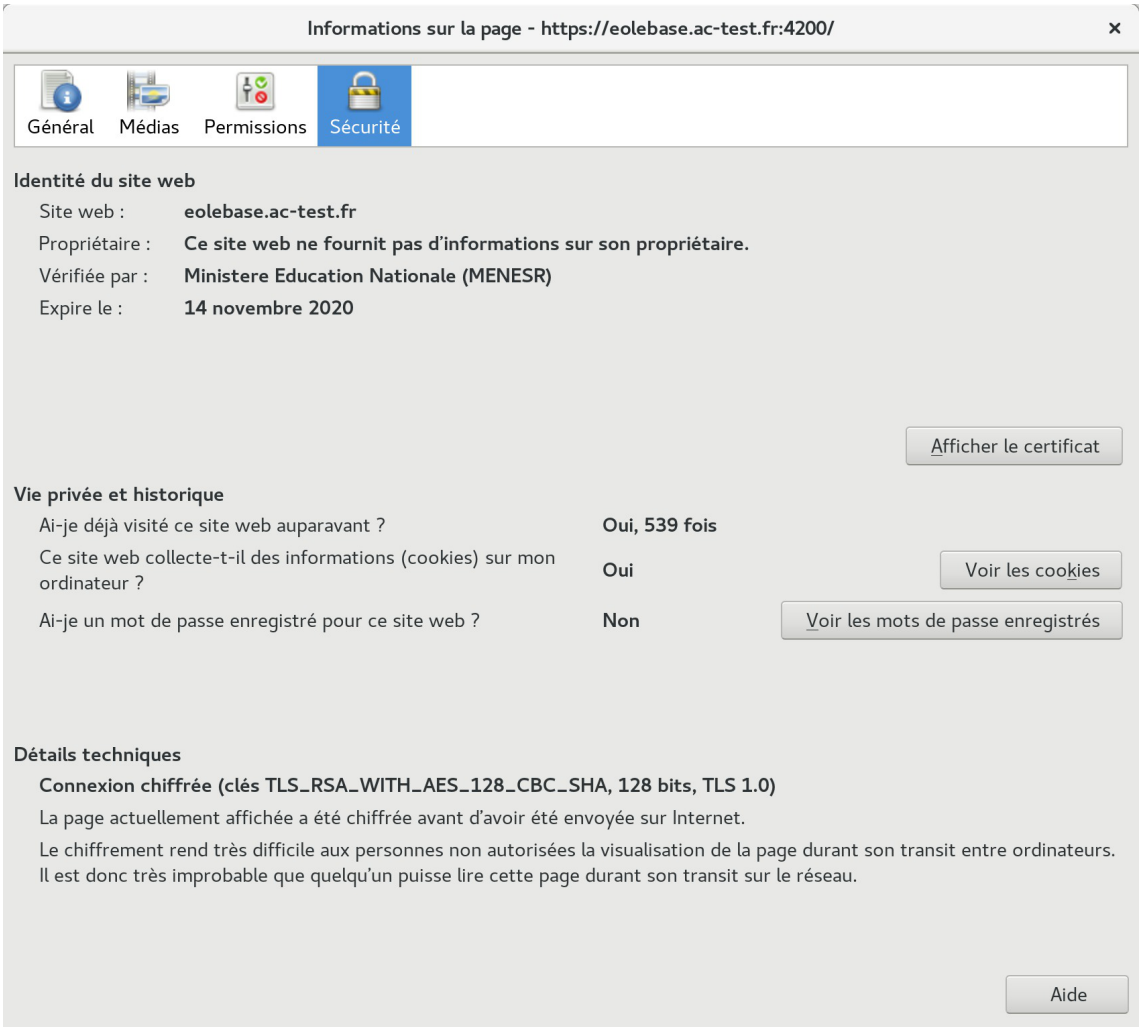


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

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



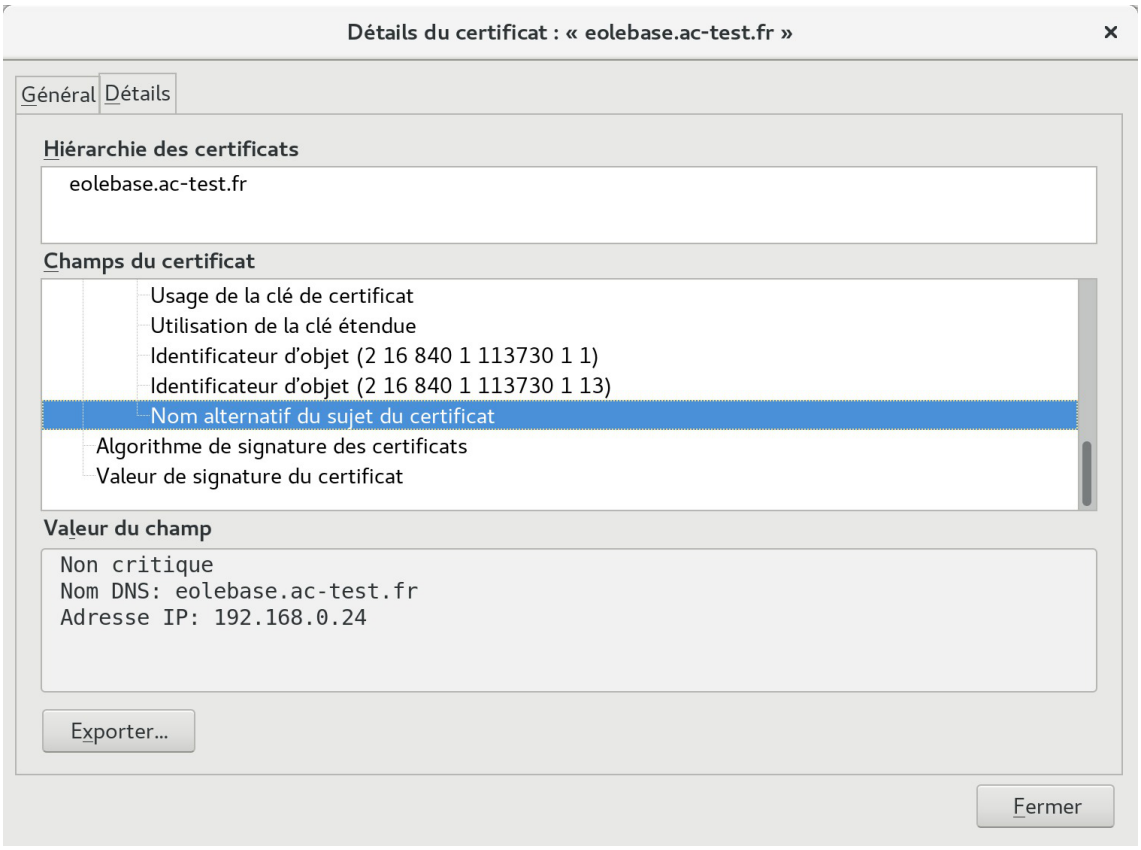
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- 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.520] 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.503].



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 Seth

Pas de question fréquente pour le moment.

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

Glossaire

ACL *= Access Control List*	Le terme ACL désigne deux choses en sécurité informatique : • un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX. • en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.
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 SSH *= Agent d'authentification*	Un agent stocke en mémoire les clés privées utilisées lors de l'authentification par clef publique (RSA, DSA, ECDSA) pendant toute la durée de la session. L'utilisation d'un agent, évite donc d'avoir à retaper la phrase secrète à chaque fois que l'on sollicite l'utilisation de la clé privée. L'agent se lance au début d'une session (graphique ou non) et tous les appels (fenêtres ou autres programmes) sont réalisés en tant que client du programme de l'agent SSH. Grâce à des variables d'environnement, l'agent peut être trouvé et être utilisé pour l'authentification lors de la connexion à d'autres machines en SSH. ssh-agent est l'agent d'authentification inclus dans la suite logicielle OpenSSH.
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

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

	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. 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

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

	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.
bastion	bastion est un service qui récupère les règles par défaut des zones réseaux utilisées par le module ainsi que toutes les règles personnalisées : • les règles optionnelles de l'EAD ; • les postes et les groupes de postes interdits ou restreints dans l'EAD ; • les règles sur les horaires de l'EAD ; • les règles ipsets (exceptions sur une directive) ; • les règles de la QOS ; • les règles tcpwrapper (host allow et hosts deny). Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu. La liste des actions du service se trouve dans le script `/usr/share/era/bastion.sh`. Le service bastion met en cache les règles mais ne les régénère pas à chaque fois. À partir de la version 2.6.1, seules les commandes `reconfigure` et `bastion regen` régénèrent les règles.
BIND *= Berkeley Internet Name Domain*	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet. 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 ;

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

	• 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 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

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

	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. 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.

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

	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.
DFS *= Distributed File System*	La technologie DFS (Système de fichiers distribué) est un ensemble de services client et serveur permettant : • de fournir une arborescence logique aux données partagées depuis des emplacements différents, • de rassembler différents partages de fichiers à un endroit unique de façon transparente, • d'assurer la redondance et la disponibilité des données grâce à la réplication. Avec cette technologie, il est possible de monter un seul même lecteur sur le poste de tous les utilisateurs, les partages existant se présenteront sous forme de dossiers et fonctionneront comme des raccourcis. L'affichage ou non des dossiers se configure ensuite en fonction de l'appartenance aux groupes NTFS. https://fr.wikipedia.org/wiki/Distributed_File_System
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.
Directive optionnelle	Directive paramétrée dans ERA et qui peut être activée ou désactivée

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

	depuis une autre interface. Les directives optionnelles le sont depuis l'EAD et les directives optionnelles cachées le sont par l'intermédiaire du template Creole `active_tags` des modules Amon et AmonEcole.
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.
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
DNS Forwarder *= Redirecteur DNS*	Un forwarder DNS est un serveur DNS qui transfert les requêtes DNS pour des noms DNS externes au réseau local vers des serveurs DNS situés à l'extérieur de ce réseau. Il est également possible de configurer le serveur de façon à transférer les requêtes sur la base de noms de domaine spécifiques au moyen de redirecteurs conditionnels.
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

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

Durée de rétention	La durée de rétention désigne le temps de conservation des sauvegardes avant leur effacement.
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`. 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.
ELF *= Executable and Linkable Format*	ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé
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).

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

	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 : 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/
FAI *= Fournisseur d'Accès à Internet*	Le FAI est un organisme (une entreprise ou une association) qui met à disposition une connexion au réseau informatique nommé Internet.
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

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

	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 Gaspacho.
GNU *= GNU is Not Unix*	GNU est l'acronyme récursif de GNU is Not Unix. Projet fondé en 1984, il vise à produire un OS complet de type Unix. Le noyau propre au projet n'étant pas fini, GNU est le plus souvent utilisé avec Linux. On parle alors de système GNU/Linux.
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
GPO *= Group Policy Objects* *= stratégies de groupe*	Les stratégies de groupe (ou GP pour Group Policy) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un

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

	environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection de dossiers ainsi que la gestion des fichiers en mode déconnecté. Les stratégies de groupe sont gérées à travers des objets de stratégie de groupe communément appelés GPO (Group Policy Objects). https://fr.wikipedia.org/wiki/Strat%C3%A9gies_de_groupe
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 de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
IDMAP *= Identity Mapping*	La méthode de calcul des identifiants Samba permet de définir une relation entre les SID Windows et les identifiants d'utilisateur et de groupe Unix.

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

	Celle-ci est effectué par le service Winbind. Il est possible de personnaliser la configuration IDMAP par domaine.
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.
INI	Un fichier INI est un fichier de configuration dans un format de données introduit par les systèmes d'exploitation Windows en 1985. Par convention les noms de ces fichiers portent l'extension « `.ini` ». Les fichiers INI sont des fichiers texte qui peuvent être manipulés avec un logiciel courant de type éditeur de texte. La valeur de chaque paramètre de configuration est indiquée par une formule : paramètre = valeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Fichier_INI
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,

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

	variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
iSCSI *= Internet Small Computer System Interface*	iSCSI est un protocole de stockage en réseau basé sur le protocole IP destiné à relier les installations de stockage de données
Java keystore *= JKS*	Un magasin de clefs Java est un fichier informatique qui stocke des certificats électroniques et éventuellement leurs clefs privées, le contenu de ce fichier sera utilisé par des applications de chiffrement à clef publique comme SSL. Le JDK Java propose la commande keytool qui permet de manipuler ces fichiers. La commande permet d'ajouter des certificats ou des clefs privées dans un fichier keystore, de les supprimer, d'extraire un certificat, mais jamais d'extraire une clef privée. Source Wikipédia : https://fr.wikipedia.org/wiki/Keystore
Jinja2	Jinja2 est un moteur de templates pour le langage de programmation Python. http://jinja.pocoo.org/docs/2.9/
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)

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

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.
LDIF *= LDAP Data Interchange Format*	LDIF est un format standardisé d'échange de données, qui permet la représentation des données contenues dans un annuaire LDAP. Il permet également la représentation d'opérations sur les données de l'annuaire (ajout, suppression, modification). https://fr.wikipedia.org/wiki/LDAP_Data_Interchange_Format
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. 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.
LSC	LSC est un connecteur open source qui permet de synchroniser les identités entre un annuaire LDAP et d'autres sources de données : base de données avec un connecteur JDBC, un autre annuaire LDAP, des fichiers plats, une API REST…

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

	https://lsc-project.org
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 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

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

	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).
Maître d'opérations (master operation en anglais) *= FSMO*	Maître d'opérations (master operation en anglais) désigne certains types de contrôleurs de domaine dans Active Directory, de Microsoft. Ce sont ceux qui jouent un rôle nécessitant un maître unique pour la réplication entre contrôleurs de domaine ; certains rôles sont uniques pour tous les domaines de la forêt ; d'autres rôles sont plus simplement uniques à l'intérieur d'un domaine. L'ancienne dénomination (avant 2005) était FSMO qui signifiait Flexible Single Master Operation ; le F de FSMO peut signifier flexible ou floating. Source Wikipédia : https://fr.wikipedia.org/wiki/Ma%C3%AEtre_d%27op%C3%A9rations
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. 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

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

	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
MMC *= Microsoft Management Console*	Microsoft Management Console est un gestionnaire de console virtuelle incorporé dans Microsoft Windows, qui sert de conteneur pour des interfaces graphiques de configuration. Ce logiciel utilitaire sert de base pour de nombreux outils de configuration incorporés dans Windows, et permet de créer des outils d'administration système en regroupant un lot d'extensions dans une même fenêtre. Source Wikipédia :

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

	https://fr.wikipedia.org/wiki/Microsoft_Management_Console
MTU *= Maximum Transmission Unit*	Le MTU définit la taille maximum d'un paquet (en octets) pouvant être transmis sur le réseau sans fragmentation. Source Wikipédia : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit
multi-DC *= multiple domain controllers*	Active Directory propose une réplication bidirectionnelle qui permet de maintenir à jour les données sur n'importe quel contrôleur de domaine. Déployer plusieurs contrôleurs dans un même domaine offre une grande tolérance aux pannes et permet de répartir la charge entre les serveurs.
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.
NAS *= Network Attached Storage*	Un NAS est un serveur relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.
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.
NetBIOS	NetBIOS est une architecture réseau et non un protocole réseau. C'est un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau. Ce service sert à associer un nom d'ordinateur à une adresse IP. NetBIOS tant à disparaître au profit des noms DNS. Le nom NetBIOS d'une machine est de type alphanumérique, excepté le premier caractère qui doit être de type alphabétique. Il doit comprendre entre 2 et 15 caractères.
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.

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

	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 : • 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`.
OMAPI *= Object Management Application Programming Interface*	OMAPI est une API qui permet de manipuler les objets distants du serveur DHCP : leasing, host, failover-state et group. Chaque objet a un certain nombre de méthodes qui sont fournies: rechercher, créer et détruire. En outre, il est possible de regarder les attributs qui sont stockés sur les objets, et dans certains cas de modifier ces attributs. Il est donc possible de modifier une partie de la configuration du serveur DHCP en cours d'exécution, sans l'arrêter, de modifier ses fichiers de base de données et de la redémarrer. Les clients OMAPI se connectent au serveur à l'aide de TCP/IP, s'authentifient à l'aide d'une clé secrète partagée et peuvent ensuite examiner l'état actuel du serveur et y apporter des modifications.
OpenNebula	OpenNebula est un projet libre et européen qui fournit un ensemble de

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

	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
OSCAR *= Outil Système Complet d'Assistance Réseau*	OSCAR est un logiciel comparable de clonage. Il permet de réaliser des images des partitions et de les restaurer en cas de plantage ou de cloner des ordinateurs strictement identiques qui peuvent contenir aussi bien un système Windows qu'un système GNU/Linux. Il est particulièrement utilisé dans certains établissements scolaires. Ce logiciel est en réalité un Live CD (basé sur la distribution GNU/Linux Gentoo) ce qui permet d'effectuer la maintenance de manière nomade, mais il peut également être installé en parallèle (dual boot) avec le système d'exploitation principal. http://oscar.crdp-lyon.fr
PAM *= Pluggable Authentication Modules*	PAM est un mécanisme permettant d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau, permettant de ce fait de rendre indépendants du schéma les logiciels réclamant une authentification. PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. PAM permet de contrôler la manière dont les modules sont enfichés dans les programmes en modifiant un fichier de configuration. Les programmes qui donnent aux utilisateurs un accès à des privilèges doivent être capables de les authentifier. Lorsque vous vous connectez sur le système, vous indiquez votre nom et votre mot de

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

	passe. Le processus de connexion vérifie que vous êtes bien la personne que vous prétendez être. Il existe d'autres formes d'authentification que l'utilisation des mots de passe, qui peuvent d'ailleurs êtres stockés sous différentes formes.
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.
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.
PowerShell	PowerShell ou Windows PowerShell, anciennement Microsoft

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

= Windows PowerShell	Command Shell (MSH), nom de code Monad, est une suite logicielle développée par Microsoft qui intègre une interface en ligne de commande, un langage de script nommé PowerShell ainsi qu'un kit de développement. Il est inclus à partir de Windows 7 et s'appuie sur le framework Microsoft .NET. Source : https://fr.wikipedia.org/wiki/Windows_PowerShell
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.
ps1	`.ps1`, est l'extension des fichiers de script Microsoft PowerShell.
PUA *= Potentially Unwanted Applications*	Applications potentiellement indésirables.
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	Une base Ramsese est le fichier de gestion des établissements

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

= Répertoire académique et ministériel sur les établissements du système éducatif	secondaires d'une académie : EPLE (établissements publics locaux d'enseignements) et EREA (établissements régionaux d'enseignements adaptés) publics et privés. Il contient toutes les informations concernant chaque établissement, notamment sa localisation, son code. Caractéristiques techniques : • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
Realm *= Nom du royaume Kerberos*	Dans Active Directory, le royaume est forcément le domaine DNS (le nom de la forêt en langage Microsoft). Le realm est le nom de domaine complet. Il est l'équivalent du FQDN pour le DNS Active Directory.
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.
Relai DHCP	Le relai DHCP est un service qui se charge de router les trames DHCP d'un réseau vers un autre.
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.
RODC *= Read-Only Domain Controller*	Un contrôleur de domaine en lecture seule (RODC) est généralement destiné à une utilisation dans des services où les contrôleurs de domaine peuvent être hébergés dans des locaux à faible sécurité d'accès. Le RODC contient une copie non modifiable de l'annuaire Active Directory et redirige toutes les tentatives d'écriture à un contrôleur de domaine complet. Il réplique également tous les comptes excepté les comptes sensibles. En cas de vol ou compromission du RODC, la sécurité est toujours assurée puisqu'il est impossible d'écrire et donc de modifier l'Active Directory. Le RPDC permet enfin d'isoler des utilisateurs sur un contrôleur de domaine en particulier. Ils ne pourront pas s'authentifier sur un autre

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

	contrôleur de domaine.
RPC *= Remote procedure call*	RPC est un protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications. Ce protocole est utilisé dans le modèle client-serveur pour assurer la communication entre le client, le serveur et d'éventuels intermédiaires. Source : https://fr.wikipedia.org/wiki/Remote_procedure_call
RSAT *= Remote Server Administration Tools*	Les outils RSAT (Outils d'administration de serveur distant) permettent aux administrateurs informatiques de gérer à distance les rôles et les fonctionnalités d'un serveur Active Directory.
rsync *= remote synchronization*	rsync est un logiciel libre de synchronisation de fichiers, distribué sous licence GNU GPL. La synchronisation est unidirectionnelle, c'est-à-dire qu'elle copie les fichiers de la source en direction de la destination. rsync est donc utilisé pour réaliser des Sauvegarde incrémentielle ou décrémentielle ou pour diffuser le contenu d'un répertoire de référence. https://fr.wikipedia.org/wiki/Rsync
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 ».
Samba 4 *= SaMBa : Server Message Block*	Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du protocole SMB, protocole standard de Microsoft. À partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Windows Server, soit en tant que contrôleur de domaine principal (PDC) ou en tant que membre d'un domaine. Il peut également faire partie d'un domaine Active Directory. Samba 4 est une version de la suite Samba développée en parallèle avec la branche stable 3.x. Une des nouveautés majeures de cette version est le support des protocoles d'authentification utilisés par Windows 2000 et supérieur.

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

	Il est ainsi possible de joindre complètement des clients Windows à un domaine et effectuer des opérations d'ouverture de session. Il inclut un serveur LDAP et un centre de distribution de clés Kerberos (KDC). Source Wikipédia : https://fr.wikipedia.org/wiki/Samba_(informatique)
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
scalability *= scalabilité*	En informatique matérielle et logicielle et en télécommunications, la scalabilité désigne la capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande (montée en charge), en particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande. Les traductions généralement utilisées sont extension graduelle, évolutivité, facteur d'échelle, extensibilité, passage à l'échelle, ou capacité à monter en charge. https://fr.wikipedia.org/wiki/Scalability
SID *= Security Identifier*	Le SID est un identifiant de sécurité utilisé pour identifier les ressources et les personnes sur un réseau Microsoft. Le SID d'un domaine se présente sous la forme `S-1-5-21-nnnnnnnnnn-nnnnnnnnnn-nnnnnnnnnn`. Chaque serveur de fichiers possède son propre SID et celui-ci est utilisé lors de la création des comptes (utilisateurs, groupes, machines rattachées au domaine). Lors de l'installation de module Scribe, Samba génère aléatoirement son propre SID. http://fr.wikipedia.org/wiki/Security_Identifier
SMB	Le protocole SMB permet le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC équipés d'un système d'exploitation Windows.
SMTP *= Simple Mail Transfer Protocol*	SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
SNMP *= Simple Network Management Protocol*	SNMP est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

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

	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.
SSO *= Single Sign On, Authentification unique*	SSO est une méthode permettant de centraliser l'authentification afin de permettre à l'utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques. Les objectifs sont : • simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent ; • simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ; • simplifier la définition et la mise en œuvre de politiques de sécurité.

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

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 *= Subject Alternative Name, nom alternatif du sujet du certificat, SAN*	OpenSSL respecte la norme X. 509v3 qui permet d'étendre la demande de certificat à l'usage qui en sera fait du dit certificat. 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).
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
SYSVOL *= System Volume*	Le partage SYSVOL sert à stocker des données spécifiques qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients. Il contient principalement les stratégies de groupes (GPO) et les scripts de connexion.

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

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. Tous les démons ne supportent pas la technique TCP Wrapper.
TDB *= Trivial Database*	TDB est une simple API de base de données développée et utilisée pour Samba afin de stocker les informations de façon rapide et sûre. Son interface est inspirée de GDBM mais, contrairement à cette dernière, TDB est capable de réaliser plusieurs opérations simultanées sur les bases de données.
Telnet *= TErminal NETwork ou TELecommunication NETwork*	Telnet est une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation. Telnet est un protocole réseau utilisé sur tout réseau prenant en charge le protocole TCP/IP. Le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.
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.

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

	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
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

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

Version admissible ou pre-release	Une version admissible, bien que le terme anglais release candidate (souvent abrégé en RC) soit beaucoup plus utilisé, est une version du logiciel qui correspond, du côté pratique, à la version « finale » ou « stable » du dit logiciel. Elle est mise à disposition à des fins de « tests de dernière minute » visant à déceler les toutes dernières erreurs subsistant au sein du programme. Source Wikipédia : http://fr.wikipedia.org/wiki/Version_d%27un_logiciel#Version_admissibl
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.
Winbind	Winbind permet de récupérer les utilisateurs et les groupes du contrôleur de domaine Windows, pour éviter de gérer plusieurs bases de données d'utilisateurs.
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
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 :

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

	• la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. Source : http://fr.wikipedia.org/wiki/Xml
ZéphirLog	ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.

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